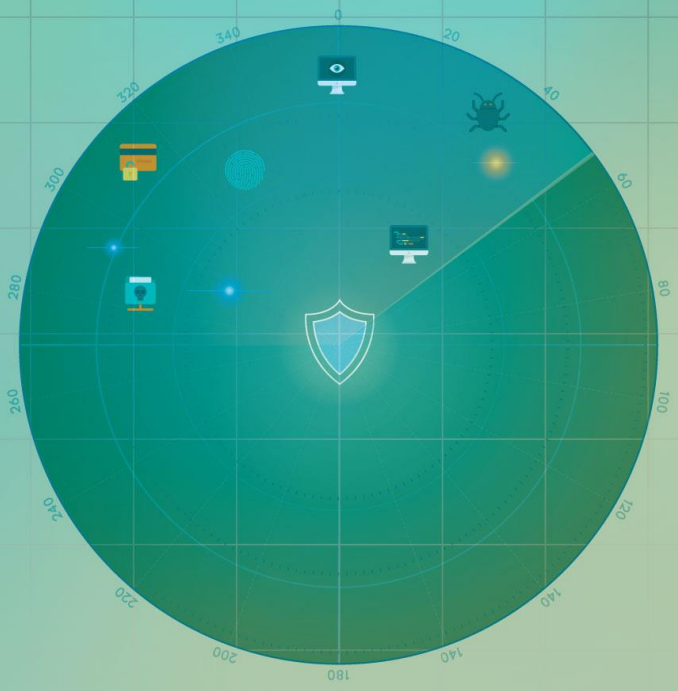
TLP: WHITE

Malware Threat Intelligence Report for Bangladesh Context, 2021



DIGITAL SECURITY AGENCY

ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

Report Period: Jan,2021 - Dec, 2021

Published: Dec, 2021

BGD e-GOV CIRT

Bangladesh e-Government Computer Incident Response Team

Cyber Threat Intelligence

Table of Contents

About this Report

The goal of this report is to provide actionable intelligence regarding threat actors and the malware or other tools they use for reconnaissance, delivery, exploitation, and so forth in order for security operations teams to be empowered to more quickly detect and respond to this specific threat. This information is also intended so that security operations teams can utilize the intelligence in this report in order to set up preventative measures for their IT asset/network/system/cyber resources.

This threat intelligence report is based on analysis from the BGD e-GOV CIRT team in which we examine TOP malware families specific for Bangladesh context for the period of January,2021 to December,2021. The malware families which are listed in this report were detected by BGD e-GOV CIRT's analysis from its various trusted sources.

Top active ransomware in Bangladesh (period of January,2021 to December,2021) are:

- Zeppelin
- Egregor
- Ryuk
- Neer
- REVIL
- CONTI

Top Malware family in Bangladesh (period of January, 2021 to December, 2021) are:

- RedLine Stealer
- Panda
- Keybase
- Necurs Botnet
- Sality
- QBot
- KASABLANKA
- Sombra or SombRAT
- Emotet
- AZORult
- KPOT Stealer
- Oski Stealer
- FormBookFormgrabber
- Loki PWS
- Nexus Stealer
- TrickBot
- Kinsing
- Outlaw hacking group cryptocurrency miners

Advanced Persistent Threat (APT) threats in Bangladesh:

- APT41
- NXSMS
- HAFNIUM
- DARK HALO
- TRANSPARENT TRIBE
- APT28
- PATCHWORK
- APT-C-61
- APT C-35 (DoNot Team)
- Sidewinder
- RedDelta
- SYSTEMBC TA
- BASILISK
- Lazarus
- Silence
- OceanLotus

General Definition

Ransomware is malicious software that infects a computer and prevents users from accessing it until a ransom is paid. For numerous years, ransomware variations have been noticed, and they frequently try to extort money from victims by presenting an on-screen alert. The user's systems have been locked or the user's files have been encrypted, according to these notifications. Users are informed that access will not be restored unless a ransom is paid. Individuals are regularly requested to pay a ransom in virtual money such as Bitcoin.

Malware (malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network (by contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug). A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware.

Trojan horses

A Trojan horse is a harmful program that misrepresents itself to masquerade as a regular, benign program or utility in order to persuade a victim to install it. A Trojan horse usually carries a hidden destructive function that is activated when the application is started.

Stealer/Info Stealer

An information stealer (or info stealer) is a Trojan that is designed to gather information from a system. The most common form of info stealer gathers login information, like usernames and passwords, which it sends to another system either via email or over a network. Other common information stealers, such as keyloggers, are designed to log user keystrokes which may reveal sensitive information.

Cryptomining malware

Cryptomining malware, or cryptocurrency mining malware or simply cryptojacking, is a relatively new term that refers to software programs and malware components developed to take over a computer's resources and use them for cryptocurrency mining without a user's explicit permission.

Attack Vector

In cyber security, an attack vector is a pathway or method used by a cyber attacker to illegally access a network or computer in an attempt to exploit system vulnerabilities.

Indicator of compromise (IOC)

Indicator of compromise (IoC) in computer forensics is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.Typical IoCs are virus signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command and control servers.

Command and Control (CnC) Server

A command-and-control (C&C) server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network. Many campaigns have been found using cloud-based services, such as webmail and file-sharing services, as C&C servers to blend in with normal traffic and avoid detection.

Dropper

A dropper is a kind of Trojan that has been designed to "install" some sort of malware (virus, backdoor, etc.) to a target system. The malware code can be contained within the dropper (single-stage) in such a way as to avoid detection by virus scanners or the dropper may download the malware to the target machine once activated (two stage).

Backdoor

A backdoor is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device. Backdoors are most often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems. From there it may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information.

Bot

Malware bots are used to gain total control over a computer.

Remote access Trojan (RAT)

A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a botnet.

DDoS

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Spyware:

Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.

Advanced persistent threat (APT)

An advanced persistent threat (APT) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

The whole purpose of an APT attack is to gain ongoing access to the system. Hackers achieve this in a series of stages.

Stage One: Gain Access

Like a burglar forcing open a door with a crowbar, cybercriminals usually gain entry through a network, an infected file, junk email, or an app vulnerability to insert malware into a target network.

Stage Two: Establish a Foothold

Cybercriminals implant malware that allows the creation of a network of backdoors and tunnels used to move around in systems undetected. The malware often employs techniques like rewriting code to help hackers cover their tracks.

Stage Three: Deepen Access

Once inside, hackers use techniques such as password cracking to gain access to administrator rights so they can control more of the system and get even greater levels of access.

Stage Four: Move Laterally

Deeper inside the system with administrator rights, hackers can move around at will. They can also attempt to access other servers and other secure parts of the network.

Stage Five: Look, Learn, and Remain

From inside the system, hackers gain a full understanding of how it works and its vulnerabilities, allowing them to harvest the information they want at will.

Hackers can attempt to keep this process running — possibly indefinitely — or withdraw once they accomplish a specific goal. They often leave a back door open to access the system again in the future.

Ref: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Network signatures/Rules

A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity. Rules are a different methodology for performing detection, which bring the advantage malware detection. Developing a rule requires an acute understanding of how the vulnerability actually works.

Threat level: High

indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems

Threat level: Medium

indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.

Ransomware: Zeppelin

Zeppelin Ransomware is offered as ransomware-as-a-service (RaaS) by buransupport seller. At the beginning, burransupport sold its Ransomware under the name Buran but lately he changed topic name to Zeppelin.

Attack Vectors

RDP, VPN vulnerabilities, and phishing.

Indicators of Compromise (IOCs)

CnC:

216[.]249[.]104[.]215
45[.]142[.]213[.]167
iplogger[.]ru
iplogger[.]org
btcxchange[.]online
bad_sysadmin(at)protonmail[.]com
Vsbb(at)firemail[.]cc
Vsbb(at)tutanota[.]com
buratino(at)firemail[.]cc
buratino2(at)tutanota[.]com
ran-unlock(at)protonmail[.]com
ranunlock(at)cock[.]li
buratin(at)torbox3uiot6wchz[.]onion
wp[.]com
cox[.]net
198[.]54[.]117[.]244
autograf[.]pl
stack-sonar[.]com
208[.]67[.]222[.]222
208[.]67[.]220[.]220
4[.]2[.]2[.]1

MD5:

0d442c4d8b4c4312840675cac8d69661
0da72fc6c1cebb98289b1efe8dd56fd9
0e06f623bc4eefa97a84ededfbb6bb7e
15bd9fe4de43bd0c418546d5e90f00be
2f1ecf99dd8a2648dd013c5fe6ecb6f5
357b149a0f40224db5d359db104a6778
386157f4cab9327d01a7210da9237ef0
5181f541a6d97bab854d5eba326ea7d9
58f53c8034a1e0ac1174595909ddf88c

68ccfaf0f453cc45faaa8f653ab9c983
79927881700955c52f113bc2d6968698
a8e670c63e257049a7bcae632c9acef6
aed10704bfb8f9eff057d5523b9ad431
bfdfd9874072b6340660b501f1bd7a33
c8823b84999ecf29f0c18c500a4e5c75
e4a50b032c527869103066212340 6fac
f8ca42285e4979fc25e1e358aaaf3ee3
fee6ba9a0d7a805b3281d4f955821c1c
968503a249052f5d214d3d368fe49e0c
c0e88cbb811aa4a59f79c392120c559a
f8a5d94ebd48bd371cb4d751507319e9
1d6ce900a8b2bf19fc993cad4f145fa8

SHA1:

871857cbf192f0fe42bfaa6bef15dd1ce0938e45
03dc1dc627fa8f7488bb7043ec38adbeb0bf69f3
c87575a3148b0e26b33b3a6b9a5f78001b10cc13
e8502ca3ba9ff85cfb7069a1f0485f9e6eb85e08
121c377693b96eef8e84861f091ef47e6fb6cae5
84768b767dcac1be745ec19031ebd188915a84c7
e82e1780847e1a889f78603ff0375cb9d9d1a545
aa8b7920718123cafa0eafa6c843b801f8c157c1
6cce64e738a001e7a1281ba0d936f762cee63ea3
1395a9377108d7fb5f90b78fe5dd7eca01e21847
b30085e5b6e7aa998582fd94e56c924d7b4497dd
0daea8972337a35f6d48eb9f9dc11ca178dd5e94
5961613e874ffcea7cd9debb8782d60b53665cb0
beac6854bcb4757a0e1d0caaf24275ac6c619d84
16d9967a2658ac765d7acbea18c556b927b810be
ff6966a1e5c4d087dc248eaec4a5f7335bb6ea8b
83bb7336deceeb094574714c1043ce9d3d420ee8

SHA256:

a72076ce30a9ddb767379ae16033e29eddf1041ae235ac8d430279d8fcbef0f5
cdeb7c9d8a737dc03c7bc81d99b72d253dc5d61f67c0796309a8285a36c73775
d76782960590abc182dba8fdcdc8bfb121b13d36be2d5d8b0960fb67960e89b1
c8738fa01d2c8a821ec660e1a039a1f827b874fdc063123eaa91821f193cac34
ddcf8ed013834b0839f58ecb3e71aeb27246d14c2e3019b5f555b01421d20a63
3e9a13f19e94ccc08138d525cc3138df642b2eca455c276be6e115c64d81294f
13DAD4E98F94568914EE55B7178E3615453007D55A186FC6CE9F188FDC78D447
4950feae35849e8f48ace0af8c7808c5ee28a9365103788fe22cb80e36d0ec7e
9df93b395c37e8387aa83da03acc0b29542778de6d89baad2659509f16307cfb

6fb05df00cf6552dcf8a0a5aef873ab7e822083d588e988815ade475e47336ee
f26e1e90b066ef235c8052c61aef0380afb68badb53351cb35cf6134bb04cf87
fd56d79a454150ba91f1e8ceb1d561a594fca21e0b40ba236769af16ea97865a
638697B2EEF0B57B4BBFB4DC23DB49B4FDC8789637E1E37D92E1C4EBB10E6EAC
4683ab92a5fd5534b13910a09b81dded8863d5cb429f50c85bf782d5cfec66d3
e15927cce83c28a01af2130765ca506166f84cadf0b8b65978a42c3e090e63aa
17777d12b6361366b4994e23d4d8597713f4772d4bbd7142f48ad4421431bbdc
c201b67cb570829122d710c2259d5342cb7c23a8e524290f0c371e68f410664b
80d61d7aaa3534e477a8e0c743bf1d715b57f140a2e68ef5d4602109285e8544
7806e02ef484826de615db972b046c4f580c69ba59f549b25f78854f8e901f3e
3437bf19502df4821f574d46bb3f9aa50770237311a8ecba6908a6dbeef9184f
BD475EEEDF26EF4CAD0ED694A57CA6ACDD09E7070E2070E766111C9D2219C7C5
7ddbd9d156f58969e172c3ecc91b230ac1dff4c185fa7db0cf07aa2c4e3ea18f
AAC0A6796CB90FEB504CD85D0313FF4B7A889EE66C1F9E9B717710397743DC44
eccf0f76a73428574beade9a692cef70e0fe1e947b4b614ba71ad36eb90420b3
be9dd97e5b63ca55c3acdeef15e8da65424d7c074effb386a1e443a85fec9d94
0BED6711E6DB24563A66EE99928864E8CF3F8CFF0636C1EFCA1B14EF15941603
4B7A2DFF949A14956A679ADB981BBEC0AEC0E198C04A454F54C5E9DCF5854B54
8d44fdbedd0ec9ae59fad78bdb12d15d6903470eb1046b45c227193b233adda6
04628e5ec57c983185091f02fb16dfdac0252b2d253ffc4cd8d79f3c79de2722
1f94d1824783e8edac62942e13185ffd02edb129970ca04e0dd5b245dd3002bc
39d8331b963751bbd5556ff71b0269db018ba1f425939c3e865b799cc770bfe4
4894b1549a24e964403565c61faae5f8daf244c90b1fbbd5709ed1a8491d56bf
d61bd67b0150ad77ebfb19100dff890c48db680d089a96a28a630140b9868d86
e22b5062cb5b02987ac32941ebd71872578e9be2b8c6f8679c30e1a84764dba7
f79ed2df72dedf4205d36e70099efad67dad726c32b11ba7b28157e532abb446
1c4643b790c17c1d2ae953b172bbf697898c1a4ae4a8961f23bac950076cd95f
442bf867c8738c7231ff09db0715ec79d0ae15c050fbd46946c45b76a040d024
148e394346c6f50193a47fdeb99bb902b3fd0f92d9171b604d8e311b76e22323
4cc4840b79f7f89db98a69209c30916560eaf4daf5befcb70f9c6f699908bec2
4f87fefc9bf667f1d60e9ac07bdcf91013d609b8222b6d1b2995706f7ece1b07
6e4459199d7fbdc4c215e595906e78fdd1c15ad3be6abed6540b80de17b63f3b
6d2e9c9249cfa6847231ce697f53e0f5d1760db2a942450c47c0c2add6308dbb
45c7c5d62ca2525ac1da111fb3388cb381c24c974eba1ca3681ef07b10ef7b77
3b332273cc839a39aa8d37a6094217e5d6d9bf02ef0e8404cd6b3a4b42489251
b7f96fbb9844cac5c7f4ec966683f3564bbb9a2f453927e1c579dcb0154f5f83
8370b5aaf5d21fdfe7052c90b1e6b8fd3e0fa0bc26007badd416b1d4a99bc3cd
c40b9b561f3054475f27423f8180c62543cdf12b3b0c1488f1b6b282b33536dd
c25da9f1e12fede333e381c548a90dcc0d348e1f7db5199cdba4cb8d6e2dfcd1
896eccdb80921e092121762ba2dafbe641ea1572018cb0152d9bd8e91ecac762
6c5a6ff90856b456e49ff35b09f4f91e692ba7ae2b798d6befb0bd9947dddbfd
f8f8f413eba06639f768ce96847d9da882c5b81c22cde6c9285dc7aa962ca164
205d2b2ebe59016c12808cf0c73277ce954bc561f7531d0dd7e9661f9685cdd4

f702e92c7e42cb476c16d1231b90e9a1a3cea00f905977dec95160098f1bf7d3
871281136a11f2db9487c8b0b061f5aab9dc7c29f554f9256e37f6093d3788f3
9959e1c41b3339501f3cfe83bd935011373bc0ff0d5517370f25d899c908bb3d
ebd5c12244445e7ef7ee72bb336145d057441d582005e83e6d7978c902de0226
09738056f37414e16a6a90e2c168c8343a7f2bef2767cdc4e2e5c8b2378ca985
dfc4ae71fc60e6546101d2c6b6795067fec6a5184a2ddf568a4f7e748e840bcc
6b96557ff35cdfcf20ae3b10365cb4db386dc6af5e36db908b2bfdefe9e081d0
dc691a5d1102ec098bd796507dd27641629e023ebcd13b14aa4aaadc7c17c975
d4d762e34d115bfa537bd3f961a969b0751e651454034c57193f8847be64725a
bf9bb73d3545be876af2093be203e0b70ce790ede8ff6569bc5b2e6c4d809d97
582c82ca828e5192f221219c978d37798c04ce32c9f79cacb0837624f8674b3c
8a43f9db2ef50873237b8380b85ac16166c8ae7105e54664d72e99c21a80996b
1322158f8ac0becc08648663279883079c4979fe7063e1849c671506ddbce01e
bb2508576dcc843181a88860679681f27debee39dfabfe99e2128d52fe1676a2
f68bec24561e484008cf17397be3484f339bd36629756e610bd4028c949c92e5
5516b8a465ec6dc78752de9f1a8addbcf1deee0bb52e7816ae807554dbb4afe1
0d67b80d3ca799483fc7037ad3a1e5b50cba6315d8c98fd82e4e44270c6fd74a
77a3ae2fffcef7b8d95a83757dd55ce5d0020d46ecc4bbf61a025d9646a29b8b
1b1222281671324ec5967333f4ee9cb5d3b649ca59a909a548c91ca26399aae9
56f54f5c5ebedda6b5b1e6ccb7da150032b34ece1b56612a662ce5ad9a364241
06089152600b091a667febae496c673bfad7e8d2f69d021785736b8b84a6e48e
931e3ec9d8765e3d79909c83ac87e3ff7ed58088d161d431c19951083d50f5b6
8afe0827823a5b044effe9e21af6e8b894f62ec203abe6c010772ab96b2eee88
25aa7d7bd388d56e4c9100db78d3c45f7cd044c3250a042529b5add584e63f08
ab7d1f99e2a948555c06675937ac6e97fc0bc2cac9b4fd06eec6f10ba3233c77
09b5f214d60f039c955036772022509d84f78c70349c9dd918b02750051d0927
9be9b5915aac3f3946fea9327c9495966fe079ee3961d3d549bc30c96a656726
4c65f326e78f01703dc8aab58cdf64b81b32cfd9c3b3de56bd83d70ecc345977
d5d950d9b3d26ba97e9d652716cd11a1c3a253ce119d13ef1ae75cc23f0edea0
df297ad2615681ba98d067d1ebeaeddcedb76a40d9adb2a121780622d11968bc
4d6b7c826b4c936222936f161a2823ad822b8653f0b60cbd3fe467c9be8ab632
00d7fc32137ee39150ac2028cb0771ab86c6a645b2ae18a93c962ba19efe51be
e7e24fd1c2e00d582ff8f1c0ad3dcd0a5ac39e4fafd2884826c98d5c636f39f5
94eda9818b5d1a68789032d5ee9a8a8648cb983019c568e20bffa817ebfc8eb3
b01e7f1eca6b45b94957cb62794f0ea0838042334f03b5b81613361ac359c912
56ba50151d543340990bb30ea0f390c1edef32cbb7b6026f2a727550621b8a7e
260f69e40abbbace9dff6115ef543308257b953a6d8a6ec0357ab270d10d4cd7
f992014855c765aea3a375d9de380714378b86c2c5bdad9d5160fa4644c7e4e1
698777eaf20e3fe8ce97cecf3be4abb12524ecf274fbf3a47b2a5def56abcd9c
38486560d06eb709b1e631b0c2f2dc8ea6ef4618c25718fb4cfe545ab9ab5dcd
b1e70925d9ea0b5d4e2453addcecaec53eef3ed611454e9fa5afec7be9b8e5f3
0c20292f4bf1598d2106c8a666c17e0e268b52363086229d8c7628c3c8e352da
ce3ffe33b8ae2e67db88c9d871936c7b51703fe432b1750f064c78b491e0e48c

Ransomware: Egregor

Egregor is a ransomware variant belonging to the Sekhmet malware family that has been active since September 2020.The ransomware organization infiltrates businesses, grabs data, and then encrypts everything. The intricacy of their attacks, their ability to infect a wide spectrum of victims, and a large increase in their activities indicate that Egregor ransomware operators have become more sophisticated. In terms of negotiating with victims, Egregor is perhaps the most aggressive ransomware family. Its operators only allow you 72 hours to get in touch with them. If the ransom is not paid, the information is made public on the attacker's website, "Egregor News."A separate chat function given to each victim is used to negotiate and agree on the ransomware payment. Bitcoin is used to make the payment.

Attack Vectors

Remote Desktop Protocol(RDP)
Phishing Emails
Software / Hardware Vulnerability

Indicators of Compromise (IOCs)

CnC:

91[.]199[.]212[.]52
49[.]12[.]104[.]241
45[.]153[.]242[.]129
185[.]238[.]0[.]233
Crt[.]sectigo[.]com
hxxp://49[.]12[.]104[.]241:81/78.bin
hxxp://49[.]12[.]104[.]241/sm.dll
hxxp://49[.]12[.]104[.]241:81/sm.dll

MD5:

16a9c2917577e732cd6630b08e248443
1cce0c0d67fe7f51f335a12138698403
43445fbe21cf3512724646a284d3e5d7
4c36c3533a283e1aa199f80e20d264b9
5f9fcbdf7ad86583eb2bbcaa5741d88a
627c2219a80245a25e4fe9843ac2a021
65c320bc5258d8fa86aa9ffd876291d3
7dd1a1a0eefc5a653a30010f475cc37c
b554791b5b161c34b0a7d26e34a88e60
b9dcee839437a917dde60eff9b6014b1
d6fa64f36eab990669f0b81f84b9a78a

SHA1:

03cdec4a0a63a016d0767650cdaf1d4d24669795
069ef8443df750e9f72ebe4ed93c3e472a2396e2
07d4bcb5b969a01fb21dc28e5cb1b7ceb05f2912
7bc6c2d714e88659b26b6b8ed6681b1f91eef6af
ac634854448eb8fcd3abf49c8f37cd21f4282dde
bd8c52bb1f5c034f11f3048e2ed89b7b8ff39261
d2d9484276a208641517a2273d96f34de1394b8e
e0caae0804957c5e31c53dd320ca83a5465169c9
e27725074f7bc55014885921b7ec8b5319b1ef8f
ed5b60a640a19afe8d1281bf691f40bac34eba8a
f0215aac7be36a5fedeea51d34d8f8da2e98bf1b
f7bf7cea89c6205d78fa42d735d81c1e5c183041
5a346fb957abeba389424dc57636edcacc58b5ba
901cee60fba225baf80c976b10dfa1684a73f5ee
a6259615ea10c30421e83d20f4a4b5f2c41b45b8
03cdec4a0a63a016d0767650cdaf1d4d24669795
4ea064f715c2a5f4ed68f57029befd8f406671dd
ac634854448eb8fcd3abf49c8f37cd21f4282dde
7bc6c2d714e88659b26b6b8ed6681b1f91eef6af
0579da0b8bfdfce7ca4a45baf9df7ec23989e28b
3a33de9a84bbc76161895178e3d13bcd28f7d8fe
f7bf7cea89c6205d78fa42d735d81c1e5c183041
986f69a43e0bf174f73139785ec8f969acf5aa55
f1603f1ddf52391b16ee9e73e68f5dd405ab06b0
5a346fb957abeba389424dc57636edcacc58b5ba
901cee60fba225baf80c976b10dfa1684a73f5ee
a6259615ea10c30421e83d20f4a4b5f2c41b45b8
4ea064f715c2a5f4ed68f57029befd8f406671dd
f73e31d11f462f522a883c8f8f06d44f8d3e2f01
ac6d919b313bbb18624d26745121fca3e4ae0fd3
95aea6b24ed28c6ad13ec8d7a6f62652b039765e
a786f383dfb90191aa2ca86ade68ee3e7c088f82
631924a3567390a081dbd82072a6fc3a185c5073
1be22505a25f14fff1e116fafcaae9452be325b1
a2d5700def24c3ae4d41c679e83d93513259ae4a
34a466a0e55a930d8d7ecd1d6e6c9c750082a5fe
2edaa3dd846b7b73f18fa638f3e1bc3a956affa4

SHA256:

072ab57f9db16d9fb92009c8e10b176bd4a2eff01c3bc6e190020cf5a0055505
1a722cde21a4338b26bc37401ef963022d97cea141c985e6615a10287f8d02ff
28f3f5a3ea270d9b896fe38b9df79a6ca430f5edab0423b3d834cf8d586f13e6

2d01c32d51e4bbb986255e402da4624a61b8ae960532fbb7bb0d3b0080cb9946
386cf4e151bc7510c3333eb1a5c96ab1b7becd8cfb94bcb76e93458078daf66f
3dba9fbef8f8a42ecfa65022b8a3c54738d15ef67c666272078b58b3c9a0a414
410afc5daebd7b39410b046286b814bb5fb5f9139167cd310bc59cc4461d4083
49b3d9c3bd6b6a13f89f0e849d80531454cc5cd259cbb7c8a806c67cd403575e
5455d104e693445dce5567236f4e047617bae7f09d5ca8699a838c2d17d37fb3
561092877e91f2741ed061cbe7a57d1af552b600c6654ccc588cb6bff7939152
605c2047be7c4a17823ad1fa5c1f94fd105721fce3621dc9148cd3baf352938e
7222c8acc69a7598989c335d528b366f801a41b434cbf928c6aef01f8e54f57a
7caed5f406445c788543f55af6d98a8bc4f0c104e6a51e2564dd37b6a485cc18
9fffabede0ef679970666f04184340437cd70bc8fe870ee8174713ececf32398
b027467332243c8186e59f68ff7c43c9e212d9e5074fedf003febcfedad4381a
b81d2293b43decd5a401487da952deb32cbb53f118882b97b457a14c67029247
c1c4e677b36a2ee6ae858546e727e73cc38c95c9024c724f939178b3c03de906
c9d46c319ed01c183598f7b9a60b9bca34b2eea989f4659e9aa27c7a1bf8681c
e3ef50749f144bfd7f5d7d51aaa9e2332b706c4d8ac130fdc95f50662525f6e0
f1ba626b8181bd1cd84f47f70838d9fa4d8117fac3bd07cbd73cb6f73b1297f8

Ransomware: Ryuk

Ryuk ransomware operators continue to strike key infrastructure and exact hefty ransom payments from susceptible groups, including a recent attack on a large health-care company. Ryuk ransomware attacks using remote desktop protocol (RDP) endpoints to carry out school ransomware assaults.

Attack Vectors

Phishing Emails

Related Tools

Cobalt Strike
SharpHound (BloodHound)
Rubeus
Adfind
Vsftpd
SystemBC
GMER
Kerbrute

Indicators of Compromise (IOCs)

CnC:

5[.]2[.]64[.]172
88[.]119[.]174[.]128
149[.]28[.]215[.]46
http://mn[.]fastbloodhunter[.]com/templates
mn[.]fastbloodhunter[.]com
fastbloodhunter[.]com
chainnss[.]com
krdgxojtymnlphxqdeec[.]com
217[.]8[.]117[.]17
uqwmftwyagxukjrhjlnp[.]com
51[.]159[.]31[.]94
ehuxktuwpkmqyqyqvrtv[.]com
imagn[.]at
lastcost2020[.]com
freebreez[.]com
exjlgnxcdadvjhkfptka[.]com
lastcost2020[.]info
advjhkfwkkhnbaetobcx[.]com
quartanam[.]com
karamelliar[.]org

rkbthfiysckqfbiqbfmu[.]com
lastcost2020[.]org
wuktmlbilrsbvsbkdetb[.]com
dogrunn[.]com
glosavrmibdlidbrcrax[.]com
omkmsefdhyngxknhtuqb[.]com
rrleuleuetijabsnqsgn[.]com
ncbdyfstrvneupadwlim[.]com
vfmawfotjeqprnvfmawf[.]com
tvlmfacgscbjlndewpxn[.]com
litlblockblack[.]com
yrsfuaegsevyffrfsgpj[.]com
baetobcxgrumftquoygp[.]com
hbamefphmqsdgkqojgwe[.]com
wdwrhikolxfwyyhwwfut[.]com
dglnvraldgkqqfognlcf[.]com
51[.]159[.]57[.]157
ehhnhaspefjhrdgcixyb[.]com
uwddrbivhweeoihvfytq[.]com
142[.]93[.]7[.]219
hconpltdkqibpgdfhwar[.]com
amagank[.]com
fkpryushemtfiekasjco[.]com
hjlomyevtehbnoossxtc[.]com
91[.]241[.]19[.]51
tpxhoiywfoxlqlcdhgmi[.]com
itqssosgjbloiuuuuumd[.]com
lxsltjemrnvfmvdonvyw[.]com
glnvrmhedrburkntpkfc[.]com
wfotjeqprnvfmawfotje[.]com
mawfotjeqprnvfmawfot[.]com
185[.]176[.]27[.]133
olpons[.]com
217[.]8[.]117[.]90
notsweets[.]net
banlo[.]org
xevgtmfndrukjftkldax[.]com
vaktorianpackif[.]com
gunzo[.]org
owxcvctdqlclytkthawh[.]com
azoraz[.]net
gnyhwaxlqowpkyewtgli[.]com
xdrnuhhhgfgfgbkbsggd[.]com

yvibvuyolrfeegaophef[.]com
lastcost2020[.]in
ujgkeowdqrptlcsnxdsl[.]com
vilfrsoycxfpcaftpwfn[.]com
obcxgrumftquoygpwkhn[.]com
xetowijhldtmdvkfpumb[.]com
hoxfqvlgoabyfspvjimc[.]com

MD5:

120cf4d1f8e624642afa69869ae1af6b
e9dc058440d321aa17d0600b3ca0ab04
097cb948a1f011f5de11579849a08db5
e8673c8a299d1647ead6f3da4565ac54
553a3cbe0b19e58c5d48e9b0396690bf
a661aeb906f044b100f557a47f6003a1
1737388ce8b0b5fc2dbc22f5b7352b7c
8b44470c7ff69ae671ff6e04550ee15f
ab52b38a4f5393e5bf919b75c0abdbdf
d99731e275a92ae306fdbb09b5bd4d24

SHA1:

5ac1c7baacbdb59c55263f0d685f54ec0a688c1b
71015f9c281038d63bf7cd45894550c1a26c6b53
15bafbd10d9bb078839da143510aacd540fab480
607f6034eae83b6546060cff5085d79b0bb0a7cd
e62135254b3a51f0180e70a11e4c3ad4a59f81c4
123f9a7487cd0fdd772f0e7bb19e70d1ee3a32e7
1fe162d6461405f7bd2c8def91e547cf85b28638
a36676950f35f1255935a0fc8467bb28ff625edb

SHA256:

ff5e6fbf14c5eb35c1b4f24e4b08b30ba2e512a4b25ab7b652f0567edb94097e
edd0675e0fcce16ae7cbb1f10fbb8407ca5e0a188eab9682f43744c95e09f1c9
e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173
d0d7a8f588693b7cc967fb4069419125625eb7454ba553c0416f35fc95307cbe
c9b06152ac1c851eaed84ee052c374341ed89d9a6e5a5d97bd0e4b941c01a274
c8076d0aa251a8c767e5f4c32c29588d46ffbed1709acaf9ca38b9d02ef7e276
c1f753047a0a5679aea0f675846364ea2f1fc4f9370f6caa89d0bfb1feb561f1
ba2a96dae66324df5bbb0751a04c538722ad49daa12d51625f8a1890608b1168
d7333223dcc1002aae04e25e31d8c297efa791a2c1e609d67ac6d9af338efbe8
9a11e1b2a6821857e1990a004447e35692d04e5b7d237697fbcc90b5198e3719
92f124ea5217f3fe5cbab1c37a961df0437d5a9cbde1af268c60c4b3194b80ed

6c7f43434e5db8703c0a47dedeeab976159d8704bfbe2e4ff65405f38d508e9d
4685e91b859b372b955c11d8d68fd562fad478520a2f4a05c46d1fe6fb991b61
3f58610586c87bb8b9f2e93768c5f289fe39ca8570902165df5d340bedc62247
32e51accf5a30da12e43b3c7f83867577fcd6fb363d7773a743ab1bbb9653d06
21cb81424dc1921344bd1cd9ad7c870fbcaadbe2e9f499d7863e9a06d7de6ee0
0d6a7a2c2d9ae89bf54f199fb63c67424d6e242777060971ee53b62dedad4096
0856b3c06805d3935b1db325c4e9c9131572b4cf09f07d989911495807775cab

Ransomware: Neer

Seems to be that Neer Ransomware is a STOP/DJVU Ransomware what uses a .neer file extension. This virus aims to encrypt all personal files on victim's computer using RSA Salsa20 cipher, mark each file with ".neer" extension and drop _readme.txt notes in every containing folder.

Attack Vectors

Infected email attachments (macros),
Torrent websites,
Malicious ads,
Unofficial activation and updating tools.

Related Tools

SmokeLoader

Indicators of Compromise (IOCs)

CnC:

astdg[.]top

Ransomware: REVIL

REVIL (also known as Sodinokibi, Unknown, UNKN) is a ransomware that was discovered in April 2019. REVIL uses a hybrid scheme, applying both symmetric and assymetric encryption (Salsa20), which stores a public key in the registry to encrypt data, and a private key for decrypting files. Presumably, it is selling on undergrounds forums as "private ransomware" by UNKN seller. Because it is selling as an affiliate revenue system, it allows other cybercriminals to spread it through several vectors. Malefactors used to exploit a zero-day vulnerability found in Oracle WebLogic (CVE-2019-2725), which allows attackers to easily gain full access to the server using an HTTP connection. Also they used a former Windows zero-day vulnerability CVE-2018-8453 to elevate itself to admin access on infected systems. It can be delivered to the victim's computer by Malicious spam, phishing campaigns with links or attachments. It is known that it was delivered via Rig EK. On June 2019 it was delivered by accessing networks via RDP (remote desktop protocol) and then utilizing MSP's (Managed Service Provider) console to drop Sodinokibi installers on end points.

Attack Vectors

Phishing emails with malicious attachments
Compromised RDP (Remote Desktop Protocol) credentials and
Exploitation of vulnerabilities in various public-facing services

Related Tools:

Cobalt Strike
Mimikatz
Crackmapexec
Psexec

Indicators of Compromise (IOCs)

CnC:

http://dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd[.]onion/
http://xsstorweb56srs3a[.]onion/threads/48608/
http://mellowc[.]sbddev[.]com/MR10[.]exe
dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd[.]onion
decoder[.]re
aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd[.]onion
decryptor[.]cc
xsstorweb56srs3a[.]onion
mellowc[.]sbddev[.]com
smalleststores[.]com
cikawemoret34[.]space
cloudmetric[.]online

nomovee[.]website
54[.]39[.]233[.]132
185[.]193[.]141[.]248
45[.]67[.]14[.]162
185[.]234[.]218[.]9
178[.]20[.]41[.]149
195[.]189[.]99[.]74
161[.]35[.]109[.]168
45[.]86[.]163[.]78
206[.]189[.]10[.]247

MD5:

06674255566d1522c27f4e269a6e97de
ec6b5973bc90fcb387f63065c5392bfb
512b538ce2c40112009383ae70331dcf
0aa7a8c026553f595305d1f1d01a5f26
843911f67cf9f70ab708372a8d30de30
9b637e90a4fcd86f2070d60a4f42cc52
c927366d400a423f890b32bce6a0aa78
b80cbbee9676aa8c647066a2e97e1d0f
7fcbb3e0b3eca4f8afb052b64cee0823
fac2cf669daebaf56f2fd4b3e0da10c0
58c390fe5845e2bb88d1d22610b0ca61
cf79091ecc42a35689672b62e7f968ec
d449ab67b3a1c5c897048152429a7695
70d38d27bb438dd5712a942bcde3378f
5a01c407a8be2ac6a004d2c40a75264e
4c49ed010405b8ce42a75645ce67aeed
898c2b98cf810791ef0bd43df742112b
85ef958ee1a5cf9ea9d84385e25cb9c5
581fc5f7185e165284acd5e17737e533
dbe2e46d3f7d2bcd0a40927a67a133dd
7d82a9c9035cae8e37a754ac77e6c8d1
524fa132dfb6611ff5bb48486274ee8f
bfa13b57730fa93e578ee65bcca21da6
6dc266627079d874d817794dc2e46d52
db8b26bc4d47e6b9e9667d22845503b5
e6566f78abf3075ebea6fd037803e176
727a6d6f23d0837dd94d85d04952b84e
784919d8dfc5a3924734802502b481d5
1a6820fec1c45cd9c928533090e7908d
54ea3dffb3907e363e8fbb4947169da0
2f10742d0db002473c128822e1e4a86a

18f64d441c8dced086e35e5bd8000dfb

SHA-256:

45f91f803de1ef2558514a8a21c279ada5bb5ad4242c2941f3c982d0bc34e3d4
8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402
dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f
df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e
1fe9b489c25bb23b04d9996e8107671edee69bd6f6def2fe7ece38a0fb35f98e
d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8
d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f
cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6
81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471
d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20
8e846ed965bbc0270a6f58c5818e039ef2fb78def4d2bf82348ca786ea0cea4f
e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
796800face046765bd79f267c56a6c93ee2800b76d7f38ad96e5acb92599fcd4
ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4
3d375d0ead2b63168de86ca2649360d9dcff75b3e0ffa2cf1e50816ec92b3b7d
d6762eff16452434ac1acc127f082906cc1ae5b0ff026d0d4fe725711db47763
C1A4878CBD32046E2FD73BBD910C62354C22BA5E53F10451420FD2F7E778A90C
CB77DC3AE2CEE170F3BD49148BF71080688E8CA3096AF1A07CC26677FB246404
1529519A30988F43B2A6ECE10F4115AB7EC282F25D3255F2A99A890E1C1C08DB
1D8D0EE5E83DA80F119E53527577A2B70D8A65282B3F9D011F178E34D3582823
1E22338DFB7BE3F01E2ACB28984039EF6381FC67AB8771E2EEF254687F3D0B96
3B5DD6038D9CB2DFD7D5089B629B1A3EFBC4A79EBDD1DC773B9790917E40849F
43AEF9C8395CB4BEBAED211E1A364CDF3074B80FF0A3150CD941A07977024B03
53178B6CF05DE5165B5B15C88426215B502DCC4C681E8C049E37E3BB503CBEC9
5DDE3386E0CE769BFD1880175168A71931D1FFB881B5050760C19F46A318EFC9
6A2BD52A5D68A7250D1DE481DCCE91A32F54824C1C540F0A040D05F757220CD3
7BE57F5067BB6DA0EF6804A49C8F4BA951E3E668E4B9C51AD492DF16C925A1B7
893FE5EFAFE1F89C93802840D71FFDA98D8F586220537CB03FA81B9F6D6044E0
ADEF0855D17DD8DDDCB6C4446E58AA9F5508A0453F53DD3FEFF8D034D692616F
BD034A6A4481AC8902E20F98350D47D06A035C57E5EA8A21D34BFE017EDB13DA
BF7114F025FFF7DBC6B7AFF8E4EDB0DD8A7B53C3766429A3C5F10142609968F9
D5F7964DC07BB3465FBC3A995FCADD623197716480F6B86518A5DFDAFC9F3AF7
E776DE801B898C65CBEF480CCEC47A60C1436E4BA1EA11F99EF2B90AB05961FF
7c7ad08931468eecb7a250a9108936976ce8b2eaae9489cf2a802580851b9f32
36fa3f72afc2dd6f206a295fc618038fef5e241bc48bd5451ac9bab9128734dd
9aec4ab2c722c0ce0a01fcb5ac05b3f3d014b3f233f4b96d8f5e0f7826011a9c
9f58b1fed5eef303f06e23f48c9359d2a74f51235677ae880bce67d76f5c827c
9fa3a004576f357b5174dd1c29ef7d13005d996d5f9fb4b86d6d978d1a4a84ae

861bc212241bcac9f8095c8de1b180b398057cbb2d37c9220086ffaf24ba9e08
90c9b6460c240177644d028458874167fedf7ca459381dde17d44446bb9ba501
6efd9aae5e112418bd43ab48ec4a1fce191c7503fcd11fdb95e89ad0217adb7a
6727edbb5d6abee908851a8c5fd7b4aca6d664634fdcdfc15e04502b960abbc5
17d153a225ea04a229862875795eeec0adb8c3e2769ba0e05073baaf86850467
c4a7f8b8046a6623cd7909bacb1cbef13471a4efd8adb4aedbf7fc1377ab502d
a3f077a4c29c522d9d70e3b22778c5a07239b6949562b37617e5ac913843076d
29e5da1f13de425e105f065be573793c41e5bf693cf874cdaac69bd85c499dfd
b613526b093b8ff750f04b920b307dbd340b1787b006a9689184d22bd348df33
cc0372ab1aba3269d4aab5a6ae0f0cb25138302dc7fa36db19fe7e1a9ad2e2d9
E8C1360A9B36EF1E4F93FC17D95963A47EC87AD3C3D85A5E0A16C29D00D53CD9
06B323E0B626DC4F051596A39F52C46B35F88EA6F85A56DE0FD76EC73C7F3851
139A7D6656FEEBE539B2CB94B0729602F6218F54FB5B7531B58CFE040F180548
26C499E3F9EC79AE91FCA43DD81F9D1302A913EE30474223F3F5320C10C4A4A0
34DFFDB04CA07B014CDAEE857690F86E490050335291CCC84C94994FA91E0160
412E951A350B84F8C0D0A2DB79029B4BBD6BE624656F2A739DB0FC00C6DBB52F
48CE9CC7A0539232C3B5C0E6D44206F145B530A108792F51143B9A3FCED446AC
7227CB2316B9E3B678698609B41BA67958D509FBF37C46CBDE714B105B71BD68
8C7E451F9D41AB36361AD516AF1AFC7ED985B7595FA77B6606775CB4686F9D1F
A376246E76EDB3F78FB5AFC32B7C250EB93AC658C75A14356644644D4FC93BAF
A9BBF8012630DC6BCD8ABAC51E45FF9EA185F4EF5FEA037A63CF36F1CCED7281
B2FF63F76AAEB73B02777C3B79022BA5A0DB2D44F61071AF808C4074E88ED6F7
1dc818f51827d89a545493921f8648299f3eb367c1e0354969ccaa9df7ce77b5
e405d4d827987638f2d8a60ebaca732dafaf9d6978187fcea12345fe24afaac7
D74CD044351030290F6AD8F70F91D51B6C39675CA3C70C45B5B0C5BD09589FF6
DDB62308575FC302245EF34D7C67EE95EEFB8A834201475DCDF490E24AA6A444
E4E83D2787545C363C909247592FA5513F6A9F330C13586A14B99D6B7BB60A99
F582A3E83181096236A5D63445CED2EA2F6F61BB9B4DDF82762DD2AE11C233A5
FB1358F4F00223FD5AA87BED22B29A65DCF7C1C26921750329EF67CBD1222B08
e281347d6faf8fa17e9bcd79d0f815187506c89e8bca9ffae78170e31ff07438
c9b04ec734151245774b54df09fc77011d703f4c93c277dbd26b998e7b6db29c
10071748cab19d1d637f24bbbb1e9fb677da5110d1cf91988436064b4694165c
4667251cbcc59ff16f6ba2ca25f78b30e88747c9d978841793265aa931119aba
7A4D05FCCC674B3E957F19E288D5149AC326C7197BDB4CCAC8055E81462A85E9
FB8B03748B617ACF0EE3B138C5B37E74EC396BC73DA3362D633862D7283742FD
6329693E5C61A2F0FA1A53BD177F5A332EF729050B3F109630B759C792F0B986
98FC76F4920BEF67830BE2D7D9C45FCFF4CA47C9003573708C5B1EDFE5A1B705
A1C58EE02858564BDBB8496EF4F9CEBAED39CF517F1C05240C79341DBD07AD95
A46B363018C0D60F3DAFE2D23341FA9D72D989CE4C35D2EC1198F98805D41B8A
A593E2CC6FE811D6BDA7750806FDF4692624E4545AA6451036769455AA9C02CE
A89E86FF5118A51337AD90686C9B5C1B986DD2BED51BBD22334D8A9D1DD89582
AB9755A71005534C3D54354BE77F304D7CB931B65A9DE9A3B0F5FF85F1118F95
ac3e29e3c35138e857bffbc8cf5f8414b71c5694e7e13abe59620d2bde408887

9665fc91d90c5381540124f8be8ad57f302875a67ee2775e5c562f022a2a8231
08E7D0E983D0220D2A8461B92A47B7F124FB1A908E96AC764DE5C17CF4752860
0ecb96d743327c4da91708d5db3eabc2de16202ccf2d90738519ebda596586d1
da2a3c7f6226de957657318994e7937e1a6fdfcd92b8dd6e2a800406e8a8247a
25ac4873ae4f955032f8f0e8ed4ec78df2e2ce814454b7b5abd9489feb4e30c3
1556A1F0240524777400D348FEF71C6CB08E6AEFCCD5E941CD7A0BBF18C0154F
34A90353EB2A9DDE073ACC7C7AFDFDA485751796263D42A3AD7826F3D2F16760
3C110B159BED84231DCE840F02698F5E0EB894B1EC5E56C2AB85EDFAFAFDA0C8
DEEC8382BC1A851A74B7261D7971EC65436AE43F51260948FAFCC794594EF77B
0C71AD6BF359A83BD638A94403CE010B27DD7562EB8DA359A4316847E41C530E
1A2A7BB050304E33C3303990C456779DF8500730F3821D2842FCFDF5B39981D4
2CDE04820DE1C7CC080B36DB54B4F48E00629326716EB4678AAB2C8EAAAC8280
338E8F24EEB38B5EF67EF662B65D592C816EBA94DFAAAC856021DAC407DAF294
3EB7FDAACCFCD2C71F527C87B55FFC40BCA2ED82728593DBD44AE31B0B389C14
60F1FC7E684C71E0203D7E6EA7FCB691B5CD723A7DA6EF4E4E462AE7F262E857
FBA829759D359DEA91DB09AC8B4674237D8DBC57EC8B76A3EBF227DA9AE96535
7bafd5de1b6724962ab920f71031978a101055f061ae3cc21db8bb9fa64c5829
2ea781140f7e86c63b636249b5fdba9828661bdd846fd95c195c5b986b84a507
89d80016ff4c6600e8dd8cfad1fa6912af4d21c5457b4e9866d1796939b48dc4
10d24ce42d973516ebec5abad7d0e927c162ba313244992d398e40716ae10ed6
C9FBE5FA6363031BD15DEE006151DDF7D9921C415421479FEC2E9732E451B584
D66F94A9FEAA7AB3C06C6AFB7E2C00806607B17C77C068539E7C5F11A0447B00
E7F9C0229C0874C069C2F3DCF237E1EE334AC4F9BC955BE8146D07941FF35790
F80527B6AD651D82B59B018C2960AB4AF31891AAB4315F325920C010CCB38F7F
a89591555b9acb65353c2b854e582bc41db2fbc0eda2210b89a877d1862084df
1501f261a66eefce47dc47cb8a426107c4b694a41b5b9fd000d0ad2ea76d8e34
d0e9cd5dbdf59931d69e28c313931fac6bef83ec9f75bd84f6cb65c43f1646e7
dd05b24610d5f9513e68201a88cdb05391bfd061346a7274062d1416e8322ff6
a389e24bf0af9bc81b8133a600a2b6c875d32aa0885964d0b9f3ac6db5fee762
1937098609fbbda1b470811a7ffe5fa044058655722d84bd029050d54f2b1496
aad3f0a2dfc2bfce8da3523cc4a4a302d44415eb14da8586c10b09752b249c39
adaee1097aa4cf10b29b41d768483a9d587fb29b85ef3ca3ae26bbabf5829b92
afbb37a3ff2187905a09403d8d42f11b64b06f2a8918ad520b202abfb5559d02
8ff6b978077a7342464d84e2ddbeb558985545980b058f5bda064de852f8d928
fd5ced03c8f056439fd6a627c5ea4b3de5a4329e0bbd5d33fc50b61359b082a3
cebadaf95ea4de56b7cda20d417b030af7d5ca7657d1670c8acecb49f6e29c78
D4E2FBCC71F4D02D01747BDAC5806DC56E59CAE4409E47867F3365FF998E8803
788e59b2fb3c80323b55cc94dc61c9d61a2d490874014591d0a8d36958b3e2f6
0DAB0428B414B0440288A12FBC20DAB72339EF72FF5859E8C18D76DD8B169F50
510EB5EBDF01D199742A98E50DD00637C6B9AF6A22DB23635BD63D4B2BF9885E
5DEB8DB611178E0858435460FC7CFF9E3F2CA23766CD5F023155C1EB6CF3E58E
720FBE60F049848F02BA9B2B91926F80BA65B84F0D831A55F4E634C820BD0848
721A6E2F7EA7C72CD76FD00DCCE09BA9038C2629FEE19A9EB8B493D2419B0CE6

7E105447D0805615ED84971CEB96B2177C050AF2A7B4E396909109D9B6A4B9F3
69f38d5d3e6f1a2d110cfff202678426e1e2007260d0fbb1d58fa5a080d40db6
45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875865
2896b38ec3f5f196a9d127dbda3f44c7c29c844f53ae5f209229d56fd6f2a59c
64076294e761cee0ce7d7cd28dae05f483a711eafe47f94fe881ac3980abfd8f
b1b00f7b065e8c013e0c23c0f34707819e0d537dbe2e83d0d023a11a0ca6b388
56de41fa0a94fa7fff68f02712a698ba2f0a71afcecb217f6519bd5751baf3ed
538078ab6d80d7cf889af3e08f62c4e83358596f31ac8ae8fbc6326839a6bfe5

List of CVE commonly exploited by REVIL ransomware:

CVE-2018-8174

A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka "Windows VBScript Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.

CVE-2018-4878

A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.

CVE-2019-11510

In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.

CVE-2019-2725

Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

CVE-2019-19781

An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.

Ransomware: CONTI

Conti (also known as reshaev) is a private Ransomware-as-a-Service (RaaS), firstly it was identified in November 2019 (test version) / Februaly 2020 (in-the-wild). Like Ryuk, it is delivered via Trickbot. This malicious software is notable for its advanced capabilities such as fast encryption, anti-analysis, and direct execution. It contains command-line options to scan for local files as well as remote files over SMB shares. Conti also uses the Windows Restart Manager to free up files that are open by various applications. The ransomware uses AES-256 encryption and requires the victim to email the threat actor for the decryption key. Also, malefactors use a website for stolen data.

Attack Vectors

Phishing emails.
RDP (Remote Desktop Protocol) services.

Related Tools

RouterScan
Anydesk
Atera
Rclone
Cobalt Strike
Mimikatz

Indicators of Compromise (IOCs)

CnC:

http://94[.]140[.]115[.]219/3/https_8443_x64[.]exe
http://94[.]140[.]115[.]219/3/win32[.]dll
http://94[.]140[.]115[.]219/4/https64[.]exe
http://94[.]140[.]115[.]219/4/win64[.]dll
http://94[.]140[.]115[.]219/3/https_8443[.]exe
http://94[.]140[.]115[.]219/3/rundll[.]dll
http://94[.]140[.]115[.]219/4/P32[.]exe
http://94[.]140[.]115[.]219/3/P32[.]exe
http://94[.]140[.]115[.]219/3/p64[.]exe
http://94[.]140[.]115[.]219/3/run1[.]exe
http://94[.]140[.]115[.]219/4/http64[.]exe
http://94[.]140[.]115[.]219/4/run1[.]exe
http://94[.]140[.]115[.]219/4/rundll[.]dll
http://94[.]140[.]115[.]219/3/http64[.]exe
http://94[.]140[.]115[.]219/3/run2[.]exe
http://94[.]140[.]115[.]219/4/P64[.]exe
http://94[.]140[.]115[.]219/4/run2[.]exe

http://94[.]140[.]115[.]219/3/http_8080_x64[.]exe
http://94[.]140[.]115[.]219/4/https[.]exe
http://94[.]140[.]115[.]219/4/serv_http64[.]exe
http://94[.]140[.]115[.]219/4/win32[.]dll
http://94[.]140[.]115[.]219/3/http8080[.]exe
http://94[.]140[.]115[.]219/3/win64[.]dll
http://94[.]140[.]115[.]219/4/http[.]exe
htcltkjqoitnez5slo7fvhiou5lbno5bwczu7il2hmfpkowwdpj3q2yd[.]onion
fylszpcqfel7joif[.]onion
continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad[.]onion
continews[.]best
conti[.]news
contirecovery[.]info
m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaidÑ…[.]onion
baron8[.]com
www[.]doloreso[.]com
doloreso[.]com
217[.]12[.]218[.]109
94[.]140[.]115[.]219
45[.]89[.]127[.]214
217[.]12[.]208[.]251

SHA256:

844cc2551f8bbfd505800bd3d135d93064600a55c45894f89f80b81fea3b0fa1
2f334c0802147aa0eee90ff0a2b0e1022325b5cba5cb5236ed3717a2b0582a9c
d21c71a090cd6759efc1f258b4d087e82c281ce65a9d76f20a24857901e694fc
a390038e21cbf92c36987041511dcd8dcfe836ebbabee733349e0b17af9ad4eb
5a2e947aace9e081ecd2cfa7bc2e485528238555c7eeb6bcca560576d4750a50
8837868b6279df6a700b3931c31e4542a47f7476f50484bdf907450a8d8e9408
234e4df3d9304136224f2a6c37cb6b5f6d8336c4e105afce857832015e97f27a
d4a1cd9de04334e989418b75f64fb2cfbacaa5b650197432ca277132677308ce
1429190cf3b36dae7e439b4314fe160e435ea42c0f3e6f45f8a0a33e1e12258f
68858814ebe2dcf21fd87ebb5fca829806307774060cb7f587f54de6625f2b02
955c113925e19feeb274b2af43403dd24d6261134e642bc7af75842f1ea150dc
0c0367006e4886fb0272033e31411f3be9ea4920fcd486c13bb48bccda74f993
6c63f028e289006218ffdfd7da4a94ef392c5893f0794133bac8d11d83233ed6
3bb6e06259d51ce88cd29e0068dcaed1d8def78281c9c4bdae6368e82266bda2
1180c0c595731caacbe4524eb1a5d19e28e0de437d02e359de70a86e3fa40446
1280098d355a5f114a23534e678191cf5e10da3794eb15c1480e877c96dbe1a4
b0f911947a82ca2c26105153f949090d99057ebd4b755e031c55f6550de0be72
a653c0455dd11a84910fdd9bd557a7555dd6cade9940fdf68cb4537004032878
b7d0a1f0e28bec456130cdd437c15b03251cbf2d9f5e9c3029f9e4fa07e086e5
db26c6c86c6fcf12d1b717d27ddaba981aa3f2e14b6b7f3dce51ce488df6e035

534880b9771c8b1b85a3c219102eda69b5d5f2f79ed4489ec71a08df82836505
63c1bfd36bd4467da1cc63e03011fe238e7abc6df035d32da892283aa0481151
0e51c1fa362ccbb122b9182b4cd6f392a6ba3f9670d4e6cf9562d94964f83d45
93a1557f49f79b55cd1f071669a7f6a333f7217fd306a6a745d1ea299599423c
ba9f4ab1cb50d3ad97eb77bad7da4fa398fd2b94182c569a64d8aa045fcb80ae
c5d7453c37e4a882bd5e7e011d8f160e90a0e036669380defa11e3d3650d00f6
e59b3ab82e876786a7658cd102fd3e8d221c36375b1eea20a0ba4c29ccdfc6d0
bd47cc015a113fae8f86975c2e59e2342c971bae162648f84a628c313caf1eca
7feb4017a1b560ce08f82eca0c79f819c5bee755882e86a5e7913977fda8c564
375642507471572e8adba9a9de5b60e5dd231210673cc14c3a875ff27d5b5aa4
49e47d31d04d670f2e4adb6c3982b458e6d7d35661be201147989a006e249fd5
2cab234781956e75d5479ebd674d5e0343c648143701b2ea20e9c2ca3f7fcdca
ca0e949d720b728e9fe5114775cde4d35a21f9ddcbba1562f66f6e1bc8d5f5ad
ca8ac27ce32b9b6b8582ed9f74ea99382720abd0338a44ad456f15cbcfff63b9

Malware: KASABLANKA

KASABLANKA

In 2021 a well-known threat actor 'KASABLANKA' was discovered to target critical information infrastructure of Bangladesh. The specific campaign utilized type of Remote Access Trojan (RAT).

Indicators of Compromise (IOCs)

CnC:

107[.]180[.]73[.]34
134[.]122[.]120[.]22 [PTR Record: vps.lap-top[.]xyz]
116[.]203[.]37[.]39
107[.]180[.]73[.]135
94[.]130[.]110[.]78 [PTR Record: vps.corona-bd[.]com]
107[.]180[.]72[.]97
160[.]178[.]220[.]194
194[.]5[.]98[.]55
107.172.30[.]213
aktel[.]org
bkashagent[.]com
info[.]v-pn[.]co
piramidewebs[.]com
c0mputer[.]xyz
zepode[.]online
mybnp[.]club
imei[.]today
corona-bd[.]com
bkash[.]club
hxxps://lap-top[.]xyz/mobile/Lap-top%20Security_Setup.apk
hxxps://av24[.]co/Virus_Cleaner_Setup.msi
hxxp://bdpolice[.]co/answer-paper-demo.zip
hxxps://isiamibankbd[.]com/tv/TPTUMC.exe
hxxps://bangladesh-bank[.]com/PBVANA.doc
hxxp://bangladesh-bank[.]com/invoice.zip
hxxp://zep0de.com/viewticket.exe
hxxp://bracbank[.]info/munafa[.]php
hxxp://107[.]172[.]30[.]213/Flash.exe

MD5:

ec8d1d6562a210daac931879acbca7c4
50ee8d6a24c1e29d184ecec1eb205ecf
afcc83d0b6bb0e71d04fb54db253a9d9

6cfc723111d7001f8c14f0cd397dbd44
c39fc85c03b20e888abbd13678f9efe7
9b6b7f85c64ca54c9f755554d5af5a47
c7dfd9ada76552be7d8a566f39066702
9a0f72cdc9a2846da937676e1efe8bf4
90387cfd4c6ebfd992e383d6d66bf458
35a3319dcba68678d4e94c039780d4c1
afcc83d0b6bb0e71d04fb54db253a9d9
50ee8d6a24c1e29d184ecec1eb205ecf
ec8d1d6562a210daac931879acbca7c4
8c8b50499149c2ad20ba39a3a607423c
461e4b3868aede5b44578441ed352268
01ee65abddc83d85f56e646a77abdf81
09600ffd3bbfad0e397b2c4bf04037c5

SHA1:

e7d5f4dc247270747a170bf6b3575f8523b5520c
0d1ae8971ec43ba43cc58ee7d3e22ffa3ad278b2
78a5dbe3c8cd70f514d1854013c30d56240e34ad
634dd186ff28247da22a9c638a117f757ba4baae
cbbcef863a6e7865027ff358cf1a6dcdeaad0d36
c01ae69b433269bcc2fd30d2b9c8576041263ce9
9bcd9a33c051d36ab0acec41e37d394025982822
f8ea2215496e6ead5135cf0ff4936cdb11208c37
acdc857fc24b72927b550e365eb4d77f385b6a4d
0239655de78351669cb0d351accb9dbe858b4347
0d1ae8971ec43ba43cc58ee7d3e22ffa3ad278b2
78a5dbe3c8cd70f514d1854013c30d56240e34ad
e7d5f4dc247270747a170bf6b3575f8523b5520c
af45e8a08dc3666996223dc4794bbdf9beff6bec
99ee00c87c5631c1d70610f42951b3acf54b4a20
dad1cb6cf834896d90f4eda7ee7d2910bd762841
3e1b9638427c9a11ad6bc55a58f876a44c0e4bf5

SHA256:

e78546bb33df88c6be3afce32f5d13084295a6e0599b26c3b380d54318170d86
cf29981bfec0f0cf2abd54ae469c8795a3cf1e19c715ded329fdb2707f982407
91b6ea9fccb4eae21335588bc83dea09780a5b7e145721f7098baafa2072286a
52b6db0fec7f587505aabfe091d8e0751acd8d4f4d120eeba5519c25a6dd8673
977a9d25972b999ae3b12d12e12978f4d116b5fb713c76c57998be15b4172def
68b221360edf4802b470fbc86493025707cf4913cc15729f4bc6ec149a4dc7ba
59f29819d223e47099ca0f00fd6bc4335d7b95188d623bf0c78c8e594c0c69c7

fbb8a86f399491ea5633df62f66bec1e4d4d5531f1dff976da1a3091b8ea4f34
4fa5525008128f77562fbb64af82b2fbcbc6c0afe71d567470380dc4476184a9
4f319b2518d855803e678713cf4b6cae975ebdd60cc1174f1609bbb9ea76f007
01f44cdc139eca65f02bfe1a8918a0d073e89bc19350262dc9d10a564863fdfd
7a55844f86b49e103564750a37604954590d27686f7f7bc8e5ae6101e8e18424
ce2276bbb6423015a4f2e80f320e068b8f53f7c19a43fb0a6f9aa5784e716d6e
bf6f5a2730ced754907e277b590959d9c734681a07a466112c392e92d008fea3
4f319b2518d855803e678713cf4b6cae975ebdd60cc1174f1609bbb9ea76f007
c3afaf555eabe5e40dcb87d2c292491e561b2dadcb1998f508088ba3bcac6836
677db7d296e4bea770f99f34e70be72b8a2b910b661804592202f3a4834ef102
cf40e1ec36f44e20a9744e8038987527027e2a6ee7e96d9044842f92ece9d7e8
f169680d8f24694e2d99c9df31988511e212e088f4dc2854ef059915019e8348
70526973e70acef4a71f474b0e321b9e600a327522903ee6bfac4e6f07935f7f
2d317bcccea4739b2deefcc3b14cf5eafe147162f62c5ff1288db3635b5c3f10
fcbaf2e5ed0b1064da6a60101f231096164895328fd6c338b322b163d580b6e3

Malware: RedLine Stealer

RedLine Stealer

First observed in 2020 and advertised on various cybercriminal forums as a 'Malware-as-a-Service' (MaaS) threat, Redline is an information stealer mainly targeting Windows' victim credentials and cryptocurrency wallets, as well as Browser information, FTP connections, game chat launchers, and OS information such as system hardware, processes names, time zone, IP, geolocation information, OS version, and default language.

Lacking an out-of-the-box distribution method, recently observed Redline incidents appear to begin with the delivery of malicious document attachments sent via an indiscriminate unsolicited email (malspam) campaign, Twitter, and Instagram Direct Messaging. Mostly targeting service or content provider's individuals such as 3D artists and streamers, financial advisers.

Data Theft

The flexibility of Redline stealer enables the variety of potential content to steal and is not bound to serve one purpose only. However, the default setting includes the following as identified from recently analyzed samples:
Browsers: Google Chrome, Mozilla Firefox, Opera and those that are Chromium-based including Microsoft Edge.
Cryptocurrency Wallets: Redline searches for the commonly used filename wallet.dat
Hardware information: Processor, Graphic hardware, screen size.
OS information: Processes, Windows versions, Credentials.
Geolocation: city, country, zip code

Indicators of Compromise (IOCs)

CnC:

45[.]142[.]214[.]200:33753
185[.]183[.]32[.]200:47859
20[.]124[.]244[.]95:7917
185[.]82[.]126[.]188:80
185[.]191[.]231[.]246:28630
80[.]66[.]87[.]53:22852
194[.]67[.]111[.]22:80
185[.]215[.]113[.]70:21508
77[.]232[.]40[.]191:57170
185[.]45[.]192[.]206:80
94[.]140[.]112[.]131:80
135[.]181[.]178[.]93:14728
194[.]67[.]111[.]22:81

45[.]9[.]20[.]221:15590
3[.]142[.]167[.]4:10757
193[.]38[.]54[.]110:25954
109[.]234[.]38[.]101:25717
5[.]149[.]255[.]29:80
45[.]8[.]126[.]9:80
195[.]133[.]47[.]114:38627
185[.]112[.]83[.]69:37026
45[.]9[.]20[.]149:42871
185[.]231[.]153[.]145:5819
45[.]150[.]67[.]236:33584
104[.]238[.]221[.]208:21732
185[.]82[.]202[.]246:81
94[.]124[.]78[.]10:23763
138[.]124[.]180[.]58:35497
185[.]80[.]234[.]61:39557
23[.]88[.]11[.]67:54321
185[.]241[.]54[.]212:4129
195[.]133[.]47[.]114:38622
185[.]112[.]83[.]21:21142
62[.]182[.]157[.]172:33718
79[.]141[.]164[.]155:80
23[.]94[.]183[.]146:43680
207[.]32[.]217[.]251:6202
87[.]251[.]73[.]109:37261
79[.]141[.]164[.]155:7655
195[.]133[.]47[.]114:38620
194[.]85[.]248[.]211:12208
179[.]43[.]187[.]40:13040
93[.]115[.]27[.]141:28269
45[.]125[.]65[.]106:51498
37[.]1[.]213[.]57:17292
185[.]215[.]113[.]67:30242
3[.]142[.]81[.]166:10757
178[.]238[.]8[.]177:4633
95[.]143[.]178[.]132:21588
91[.]241[.]19[.]213:46284
135[.]181[.]178[.]93:12952
23[.]88[.]118[.]113:23817
79[.]174[.]13[.]108:19006
45[.]81[.]224[.]6:24953
107[.]178[.]110[.]44:46230
91[.]243[.]59[.]82:52712

146[.]185[.]239[.]15:81
193[.]38[.]55[.]29:65221
80[.]66[.]87[.]52:80
92[.]255[.]76[.]197:38637
91[.]243[.]32[.]142:16969
45[.]67[.]228[.]240:80
92[.]255[.]85[.]131:44159
104[.]144[.]69[.]49:80
91[.]243[.]32[.]158:46216
185[.]92[.]74[.]32:10442
3[.]142[.]129[.]56:10757
185[.]215[.]113[.]44:23759
3[.]142[.]81[.]166:12736
185[.]45[.]192[.]75:81
37[.]0[.]10[.]21:34763
23[.]94[.]54[.]224:54456
45[.]9[.]20[.]59:46287
109[.]234[.]39[.]186:34298
45[.]88[.]3[.]225:6822
37[.]0[.]10[.]174:15466
45[.]9[.]20[.]52:35351
91[.]243[.]32[.]50:63948
178[.]238[.]8[.]1:30148
64[.]18[.]87[.]81:80
191[.]101[.]130[.]135:47895
45[.]67[.]231[.]50:49268
185[.]209[.]28[.]55:2237
176[.]122[.]23[.]55:11768
178[.]238[.]8[.]207:11703
185[.]81[.]114[.]240:80
185[.]189[.]167[.]130:38637
185[.]215[.]113[.]28:49916
94[.]140[.]112[.]68:81
94[.]103[.]9[.]200:81
147[.]124[.]208[.]247:34932
95[.]181[.]152[.]165:49234
193[.]142[.]146[.]212:7821
185[.]215[.]113[.]109:62951
65[.]21[.]226[.]115:60392
46[.]3[.]199[.]41:53924
64[.]56[.]68[.]209:25555
91[.]243[.]32[.]101:1568
94[.]140[.]112[.]149:80

192[.]227[.]89[.]116:6099
185[.]92[.]73[.]122:19037
51[.]81[.]177[.]165:6942
185[.]45[.]192[.]195:80
178[.]238[.]8[.]47:36439
212[.]193[.]30[.]196:13040
185[.]223[.]92[.]157:44160
94[.]23[.]1[.]92:12857
195[.]226[.]192[.]126:81
185[.]92[.]74[.]28:80
debiazzela[.]xyz
91[.]243[.]32[.]45:20513
jaromawanave[.]xyz
188[.]119[.]113[.]212:37572
3[.]138[.]45[.]170:12121
103[.]246[.]144[.]29:44301
137[.]74[.]39[.]29:43315
185[.]117[.]91[.]185:80
168[.]119[.]104[.]184:22192
94[.]103[.]9[.]175:80
45[.]134[.]225[.]35:7821
65[.]21[.]226[.]115:27660
45[.]130[.]151[.]74:81
195[.]242[.]111[.]44:37939
65[.]108[.]69[.]168:16278
185[.]31[.]160[.]143:51281
185[.]183[.]32[.]228:36247
80[.]66[.]87[.]32:22852
185[.]92[.]74[.]98:11734
188[.]34[.]178[.]22:5154
45[.]129[.]99[.]59:81
94[.]140[.]112[.]152:80
116[.]202[.]110[.]68:48426
51[.]79[.]188[.]112:7110
185[.]117[.]75[.]101:80
3[.]142[.]167[.]4:12736
95[.]181[.]152[.]177:21142
93[.]189[.]41[.]252:80
45[.]77[.]80[.]187:15300
207[.]32[.]217[.]185:17221
129[.]146[.]249[.]128:64466
185[.]118[.]165[.]79:61909
65[.]21[.]75[.]210:59706

138[.]124[.]186[.]113:15997
185[.]183[.]98[.]26:80
212[.]193[.]30[.]12:5176
185[.]82[.]126[.]98:80
5[.]135[.]214[.]141:53665
159[.]69[.]123[.]221:25706
3[.]131[.]99[.]219:4455
194[.]26[.]232[.]164:32592
92[.]255[.]76[.]242:1101
185[.]159[.]80[.]90:38655
194[.]26[.]232[.]163:5739
45[.]14[.]49[.]184:40979
176[.]122[.]25[.]128:49897
84[.]246[.]85[.]176:10991
49[.]12[.]219[.]50:4846
194[.]85[.]248[.]229:30260
99[.]83[.]154[.]118:80
65[.]108[.]4[.]86:21391
94[.]103[.]9[.]184:80
93[.]170[.]123[.]216:80
45[.]67[.]228[.]227:58696
65[.]21[.]3[.]192:1539
45[.]87[.]154[.]220:16714
185[.]186[.]143[.]241:12420
141[.]95[.]82[.]50:63652
64[.]56[.]70[.]117:46964
65[.]21[.]126[.]227:36202
188[.]212[.]124[.]242:58758
62[.]112[.]9[.]39:80
185[.]215[.]113[.]115:53803
185[.]215[.]113[.]29:26828
185[.]224[.]134[.]182:16014
188[.]227[.]87[.]7:10234
185[.]92[.]73[.]160:46771
136[.]144[.]41[.]178:9295
3[.]134[.]125[.]175:10655
95[.]215[.]205[.]135:8634
185[.]230[.]143[.]237:2548
95[.]217[.]123[.]66:23117
135[.]181[.]79[.]37:10902
62[.]182[.]159[.]90:21566
104[.]193[.]252[.]132:18185
viehostra[.]xyz

51[.]79[.]57[.]67:29000
93[.]189[.]43[.]32:80
185[.]219[.]80[.]146:27156
195[.]226[.]192[.]196:80
194[.]127[.]179[.]0:42417
103[.]151[.]122[.]67:61359
93[.]189[.]42[.]149:80
188[.]119[.]113[.]20:27724
91[.]213[.]50[.]135:40612
146[.]185[.]239[.]5:80
185[.]92[.]74[.]51:2378
185[.]92[.]150[.]136:7303
51[.]68[.]142[.]233:31156
91[.]208[.]127[.]220:35763
45[.]129[.]99[.]148:80
77[.]232[.]40[.]51:20166
176[.]9[.]10[.]140:50422
144[.]76[.]245[.]112:51981
185[.]215[.]113[.]121:15386
185[.]183[.]32[.]161:56024
95[.]216[.]168[.]100:38784
49[.]12[.]216[.]102:42622
3[.]17[.]7[.]232:10655
178[.]238[.]8[.]72:49214
93[.]115[.]21[.]52:45160
5[.]206[.]227[.]246:80
46[.]21[.]250[.]40:31113
91[.]243[.]59[.]56:61911
65[.]21[.]5[.]58:48811
176[.]9[.]39[.]110:23465
79[.]110[.]52[.]59:1801
62[.]182[.]156[.]188:44301
85[.]209[.]89[.]134:38190
95[.]181[.]152[.]12:44159
185[.]92[.]74[.]38:1247
51[.]81[.]139[.]72:10762
89[.]105[.]217[.]244:57262
94[.]140[.]112[.]97:80
92[.]205[.]28[.]105:5321
45[.]147[.]229[.]190:20397
37[.]9[.]13[.]169:63912
109[.]107[.]188[.]167:37171
92[.]119[.]113[.]176:1291

213[.]166[.]69[.]51:49154
37[.]61[.]213[.]242:25027
31[.]148[.]99[.]65:80
188[.]165[.]56[.]25:18225
193[.]38[.]54[.]84:20375
45[.]142[.]212[.]122:21523
185[.]250[.]204[.]166:46183
136[.]144[.]41[.]189:12208
212[.]193[.]30[.]139:57935
185[.]244[.]182[.]102:46511
91[.]219[.]63[.]223:64769
94[.]103[.]94[.]65:61473
91[.]211[.]251[.]212:59437
91[.]206[.]14[.]151:64591
185[.]183[.]96[.]27:81
65[.]108[.]29[.]209:18717
188[.]165[.]197[.]116:48679
135[.]181[.]141[.]214:11552
govvv[.]xyz
137[.]184[.]14[.]30:80
95[.]143[.]179[.]152:42556
45[.]144[.]31[.]118:31905
185[.]92[.]73[.]84:2378
5[.]196[.]97[.]178:15174
95[.]181[.]152[.]143:42599
91[.]121[.]67[.]60:51630
81[.]91[.]178[.]86:21746
213[.]136[.]85[.]189:7059
185[.]209[.]28[.]55:65401
45[.]8[.]124[.]72:80
80[.]85[.]138[.]229:4064
tatreriash[.]xyz
94[.]140[.]112[.]47:80
194[.]61[.]0[.]151:56384
79[.]174[.]13[.]108:30200
95[.]168[.]174[.]42:42482
195[.]133[.]18[.]66:51391
144[.]202[.]123[.]191:49885
50[.]18[.]71[.]252:12081
209[.]90[.]237[.]21:46536
188[.]40[.]147[.]206:56184
37[.]9[.]13[.]169:3465
138[.]124[.]186[.]65:19624

185[.]250[.]149[.]224:44031
86[.]107[.]197[.]248:56626
185[.]223[.]92[.]157:7659
23[.]88[.]98[.]112:4214
176[.]123[.]9[.]192:27934
194[.]156[.]89[.]132:22920
95[.]181[.]152[.]14:46927
94[.]103[.]9[.]139:80
212[.]86[.]102[.]63:62907
91[.]243[.]32[.]42:52075
185[.]215[.]113[.]109:44059
178[.]63[.]69[.]133:41433
180[.]214[.]237[.]105:15128
195[.]2[.]93[.]155:17354
45[.]144[.]31[.]193:5785
45[.]81[.]224[.]230:5684
65[.]108[.]20[.]184:13650
185[.]117[.]90[.]160:81
45[.]144[.]225[.]207:37828
51[.]178[.]13[.]99:44915
164[.]132[.]202[.]23:35481
93[.]115[.]18[.]158:3333
86[.]107[.]197[.]248:59530
70[.]36[.]97[.]202:27526
45[.]9[.]20[.]150:80
185[.]183[.]32[.]184:80
185[.]7[.]214[.]127:32304
185[.]7[.]214[.]8:37809
178[.]23[.]190[.]213:2602
65[.]21[.]85[.]33:8463
176[.]31[.]32[.]198:17055
138[.]124[.]186[.]108:11542
80[.]89[.]234[.]187:43303
91[.]243[.]32[.]23:12780
185[.]215[.]113[.]29:1102
135[.]181[.]141[.]214:10724
212[.]114[.]52[.]26:13575
62[.]113[.]112[.]212:11375
129[.]146[.]127[.]215:39241
95[.]217[.]123[.]17:11265
109[.]107[.]191[.]37:55005
94[.]26[.]230[.]203:48759
95[.]181[.]152[.]9:46927

135[.]125[.]40[.]67:49126
135[.]181[.]170[.]165:18467
45[.]93[.]4[.]106:80
manazyxsa[.]xyz
209[.]141[.]44[.]109:43987
85[.]208[.]184[.]233:64930
185[.]215[.]113[.]99:21438
82[.]146[.]43[.]167:80
http://82[.]146[.]43[.]167
45[.]147[.]230[.]245:34585
194[.]58[.]69[.]100:37026
nariviqusir[.]xyz
104[.]168[.]237[.]55:44505
178[.]23[.]190[.]74:23470
185[.]125[.]207[.]77:40170
95[.]181[.]152[.]143:51416
65[.]108[.]55[.]203:56717
212[.]86[.]102[.]118:22117
194[.]124[.]213[.]221:16713
185[.]159[.]80[.]90:38637
154[.]127[.]53[.]182:48463
95[.]217[.]248[.]40:30385
65[.]21[.]141[.]10:41995
185[.]215[.]113[.]109:57626
45[.]67[.]231[.]218:7527
185[.]206[.]215[.]216:80
151[.]80[.]243[.]216:31710
138[.]124[.]183[.]121:27019
65[.]21[.]76[.]42:11286
45[.]67[.]228[.]240:1026
185[.]235[.]130[.]48:44050
45[.]88[.]107[.]116:44061
23[.]88[.]109[.]42:55961
178[.]33[.]87[.]34:35291
https://maxhacks[.]pro
77[.]247[.]127[.]134:14513
94[.]250[.]255[.]5:80
185[.]250[.]204[.]246:26491
138[.]124[.]186[.]75:20481
45[.]153[.]186[.]153:56675
185[.]92[.]73[.]142:52097
65[.]108[.]4[.]86:8910
91[.]242[.]229[.]222:21475

185[.]215[.]113[.]71:16254
95[.]217[.]123[.]66:57358
94[.]26[.]249[.]132:19205
91[.]211[.]251[.]200:52562
185[.]235[.]128[.]229:20570
193[.]203[.]203[.]82:23108
23[.]88[.]115[.]80:56664
87[.]251[.]71[.]44:81
89[.]38[.]131[.]227:12236
185[.]215[.]113[.]205:65531
91[.]243[.]32[.]8:65098
95[.]181[.]152[.]141:29263
188[.]119[.]113[.]20:32804
37[.]0[.]10[.]21:53251
95[.]181[.]152[.]8:46927
http://91[.]243[.]32[.]20/verify[.]php?id=16_c774fa310032316528b50e0ae934ba5c
80[.]66[.]87[.]55:11327
94[.]103[.]9[.]167:61775
185[.]70[.]186[.]150:33967
45[.]9[.]20[.]104:6334
91[.]243[.]32[.]5:3677
91[.]243[.]32[.]14:7364
178[.]23[.]190[.]135:25442
64[.]56[.]67[.]136:55730
91[.]211[.]251[.]208:44660
65[.]108[.]21[.]21:18653
185[.]209[.]22[.]181:29234
135[.]181[.]123[.]52:21975
91[.]243[.]59[.]11:42847
185[.]215[.]113[.]83:60722
188[.]124[.]47[.]6:65098
62[.]182[.]156[.]22:36874
212[.]224[.]105[.]84:80
188[.]124[.]37[.]219:26360
62[.]182[.]156[.]184:25507
185[.]215[.]113[.]57:50723
212[.]193[.]30[.]197:34126
138[.]124[.]186[.]58:48619
80[.]66[.]87[.]50:80
45[.]147[.]231[.]161:38637
3[.]136[.]65[.]236:12545
95[.]215[.]108[.]72:8080
185[.]215[.]113[.]41:14518

144[.]76[.]156[.]28:3333
176[.]57[.]69[.]148:43862
37[.]0[.]10[.]73:23282
95[.]217[.]110[.]27:15401
18[.]190[.]26[.]16:61391
91[.]243[.]32[.]4:4249
95[.]181[.]152[.]7:46927
80[.]89[.]237[.]147:39192
23[.]94[.]183[.]146:60709
45[.]67[.]231[.]145:10991
185[.]215[.]113[.]49:29659
195[.]238[.]126[.]94:30418
185[.]183[.]32[.]183:55694
185[.]183[.]32[.]161:80
18[.]118[.]197[.]60:18345
94[.]103[.]9[.]151:31261
37[.]0[.]10[.]112:55214
136[.]144[.]41[.]101:4401
185[.]244[.]181[.]71:2119
144[.]202[.]13[.]247:33577
194[.]87[.]111[.]39:54572
104[.]168[.]102[.]108:16048
185[.]215[.]113[.]94:15564
5[.]149[.]255[.]29:81
84[.]38[.]189[.]175:18214
185[.]81[.]115[.]38:81
213[.]142[.]148[.]231:58682
185[.]82[.]127[.]214:80
185[.]117[.]90[.]160:80
145[.]239[.]32[.]179:27763
193[.]56[.]146[.]64:65441
135[.]181[.]79[.]37:52491
65[.]108[.]48[.]69:32661
185[.]215[.]113[.]46:80
195[.]238[.]126[.]94:27094
109[.]248[.]203[.]63:28517
109[.]107[.]191[.]123:52781
185[.]117[.]90[.]167:80
18[.]117[.]169[.]183:9508
178[.]33[.]87[.]34:45760
91[.]206[.]14[.]151:16764
185[.]51[.]246[.]132:8926
54[.]38[.]9[.]216:9487

51[.]91[.]193[.]177:18717
109[.]248[.]11[.]240:17314
45[.]137[.]190[.]237:27973
95[.]181[.]152[.]6:46927
185[.]215[.]113[.]51:56632
37[.]252[.]9[.]247:37711
185[.]215[.]113[.]29:36224
146[.]0[.]75[.]231:80
80[.]85[.]139[.]135:1855
185[.]183[.]32[.]230:2912
185[.]215[.]113[.]79:41465
138[.]124[.]186[.]225:38066
146[.]59[.]255[.]27:63731
185[.]255[.]133[.]25:18225
62[.]182[.]156[.]24:12780
37[.]0[.]8[.]193:26986
94[.]228[.]116[.]174:44006
91[.]206[.]15[.]183:15322
195[.]2[.]93[.]217:18524
45[.]14[.]49[.]184:55842
65[.]108[.]14[.]118:15253
144[.]76[.]183[.]53:5634
92[.]119[.]113[.]189:21746
45[.]129[.]99[.]59:80
192[.]30[.]89[.]27:6640
95[.]216[.]8[.]253:15940
135[.]181[.]79[.]37:32157
91[.]121[.]67[.]60:23325
136[.]144[.]41[.]204:34268
3[.]17[.]66[.]208:50383
45[.]9[.]20[.]182:46792
190[.]2[.]136[.]29:15554
103[.]246[.]146[.]160:6677
193[.]150[.]103[.]37:29118
5[.]149[.]254[.]7:80
185[.]215[.]113[.]62:30887
185[.]215[.]113[.]17:7700
185[.]215[.]113[.]94:35535
185[.]215[.]113[.]15:21508
162[.]55[.]45[.]65:60407
65[.]108[.]29[.]210:21638
185[.]183[.]32[.]227:51498
telegka[.]top

dogspise[.]site
homereds[.]site
dribblingway[.]site
silversun[.]site
greentry[.]site
jacksonwile[.]site
mousehoused[.]site
pilotzone[.]site
rosecar[.]site
topstart[.]site
yollowstar[.]site
87[.]120[.]254[.]33:13663
185[.]45[.]192[.]203:80
193[.]164[.]16[.]58:36882
45[.]132[.]104[.]217:12780
135[.]181[.]129[.]119:4805
65[.]108[.]21[.]17:5417
92[.]119[.]115[.]229:48282
150[.]230[.]33[.]148:17890
135[.]181[.]79[.]37:42709
193[.]188[.]20[.]94:25588
45[.]156[.]27[.]227:48558
185[.]215[.]113[.]216:4525
185[.]92[.]73[.]160:6070
37[.]1[.]219[.]52:42987
84[.]38[.]189[.]175:39222
37[.]230[.]112[.]47:26715
65[.]21[.]103[.]75:35053
91[.]206[.]15[.]183:9825
45[.]14[.]49[.]184:18458
188[.]227[.]87[.]46:51843
77[.]232[.]39[.]148:5879
45[.]14[.]49[.]66:53212
193[.]56[.]146[.]60:56554
194[.]87[.]92[.]7:22033
195[.]133[.]18[.]154:32513
45[.]147[.]197[.]123:49301
212[.]192[.]246[.]4:16972
185[.]125[.]217[.]52:8771
65[.]21[.]199[.]14:7312
185[.]230[.]143[.]38:37354
185[.]244[.]217[.]195:21588
185[.]244[.]182[.]136:51832

141[.]94[.]188[.]138:46419
5[.]39[.]42[.]4:52028
89[.]223[.]69[.]212:38637
195[.]2[.]93[.]217:59309
45[.]156[.]27[.]227:56326
5[.]188[.]118[.]163:63275
108[.]62[.]12[.]248:40746
94[.]26[.]248[.]150:17618
80[.]85[.]142[.]51:9468
141[.]94[.]112[.]3:11722
193[.]38[.]54[.]84:44885
185[.]244[.]181[.]71:44496
185[.]51[.]246[.]132:31671
185[.]92[.]74[.]21:80
91[.]245[.]253[.]52:38439
185[.]235[.]128[.]229:2187
164[.]132[.]72[.]186:18717
178[.]63[.]26[.]132:29795
135[.]125[.]40[.]64:15456
91[.]121[.]67[.]60:62102
193[.]203[.]203[.]82:63851
65[.]108[.]5[.]215:54452
185[.]82[.]126[.]114:31858
185[.]180[.]220[.]105:11915
45[.]153[.]230[.]94:52980
185[.]132[.]134[.]148:55353
77[.]232[.]36[.]199:32336
188[.]72[.]208[.]174:38430
185[.]154[.]13[.]159:34854
185[.]215[.]113[.]107:61144
45[.]131[.]46[.]129:12509
185[.]92[.]73[.]84:80
37[.]230[.]112[.]47:49799
185[.]80[.]53[.]81:15667
185[.]215[.]113[.]55:36801
5[.]61[.]61[.]168:14462
193[.]163[.]113[.]105:26203
176[.]57[.]69[.]117:21596
77[.]232[.]38[.]34:44300
5[.]149[.]249[.]178:12509
212[.]86[.]102[.]139:32600
80[.]87[.]192[.]137:27018
65[.]108[.]1[.]219:28593

193[.]56[.]146[.]60:18243
195[.]2[.]93[.]217:60468
195[.]133[.]18[.]154:30491
87[.]251[.]71[.]64:80
87[.]251[.]71[.]44:80
185[.]173[.]39[.]234:36881
195[.]133[.]18[.]5:45269
37[.]0[.]8[.]37:3799
193[.]164[.]7[.]71:22541
45[.]156[.]21[.]113:63256
138[.]124[.]186[.]42:14462
95[.]216[.]43[.]58:40566
93[.]115[.]20[.]139:28978
77[.]232[.]38[.]163:41139
45[.]144[.]29[.]94:61419
185[.]92[.]74[.]142:80
45[.]67[.]231[.]218:15411
185[.]153[.]198[.]58:80
185[.]213[.]210[.]82:4505
92[.]246[.]89[.]6:38437
84[.]38[.]189[.]175:54144
45[.]147[.]197[.]123:31820
188[.]34[.]176[.]164:80
138[.]124[.]186[.]121:45760
205[.]185[.]123[.]105:20035
185[.]244[.]217[.]166:56316
3[.]17[.]66[.]208:58281
155[.]138[.]201[.]103:60259
92[.]119[.]113[.]20:20871
91[.]206[.]14[.]151:50125
51[.]91[.]193[.]179:5048
185[.]118[.]165[.]93:4476
185[.]237[.]98[.]178:62607
94[.]103[.]9[.]133:39323
194[.]15[.]46[.]144:36848
94[.]250[.]250[.]77:32413
45[.]156[.]21[.]209:56326
138[.]124[.]186[.]2:27999
141[.]94[.]188[.]139:43059
205[.]185[.]127[.]47:20078
188[.]119[.]113[.]86:40729
45[.]142[.]215[.]47:27643
45[.]82[.]178[.]241:35141

185[.]173[.]37[.]128:40504
138[.]124[.]186[.]180:39821
18[.]216[.]102[.]251:80
84[.]38[.]185[.]103:39821
77[.]232[.]43[.]170:14614
147[.]124[.]212[.]128:45499
185[.]250[.]151[.]254:3363
95[.]217[.]248[.]44:1052
185[.]215[.]113[.]104:18754
65[.]21[.]230[.]118:16782
65[.]108[.]20[.]195:6774
213[.]166[.]69[.]181:64650
45[.]133[.]1[.]81:45269
91[.]236[.]120[.]204:20853
91[.]142[.]77[.]155:5469
80[.]87[.]192[.]249:16640
185[.]215[.]113[.]15:6043
185[.]244[.]180[.]224:39957
65[.]108[.]4[.]54:11645
94[.]26[.]228[.]204:32917
92[.]222[.]145[.]232:61157
65[.]21[.]231[.]57:60751
178[.]132[.]3[.]103:80
135[.]181[.]142[.]223:30397
45[.]9[.]20[.]20:13441
65[.]21[.]236[.]62:47186
185[.]215[.]113[.]29:18087
45[.]142[.]214[.]210:80
http://45[.]142[.]214[.]210/IRemotePanel
109[.]234[.]38[.]212:6677
103[.]168[.]67[.]29:6677
91[.]235[.]129[.]177:80
172[.]67[.]221[.]58:80
144[.]76[.]112[.]41:26462
185[.]70[.]184[.]89:52823
179[.]43[.]176[.]44:80
65[.]21[.]3[.]192:35618
37[.]1[.]195[.]84:1515
94[.]103[.]80[.]219:62459
95[.]181[.]163[.]215:80
45[.]137[.]152[.]34:4762
85[.]209[.]89[.]238:6677
http://85[.]209[.]89[.]238:6677/IRemotePanel

188[.]119[.]113[.]80:15814
45[.]67[.]228[.]93:80
http://45[.]67[.]228[.]93/IRemotePanel
212[.]192[.]246[.]10:31954
ballablaq957[.]duckdns[.]org
92[.]222[.]145[.]236:60837
87[.]251[.]71[.]14:89
185[.]125[.]217[.]185:35200
185[.]167[.]97[.]37:30900
194[.]226[.]139[.]24:7732
104[.]21[.]15[.]108:80
http://lapes2049[.]eu/
45[.]147[.]197[.]145:34595
65[.]108[.]29[.]194:20525
45[.]133[.]217[.]203:23497
52[.]6[.]206[.]192:13994
45[.]133[.]217[.]148:65255
185[.]161[.]209[.]196:57754
45[.]132[.]104[.]3:18717
185[.]219[.]80[.]221:6677
http://185[.]219[.]80[.]221:6677/IRemotePanel
193[.]38[.]55[.]57:7575
91[.]142[.]79[.]218:9781
185[.]230[.]143[.]165:52046
141[.]95[.]23[.]25:58184
77[.]83[.]175[.]169:5180
185[.]180[.]231[.]69:42875
86[.]106[.]181[.]31:38670
195[.]2[.]78[.]163:55923
95[.]181[.]157[.]69:8552
185[.]125[.]18[.]49:80
31[.]44[.]3[.]94:62655
31[.]44[.]3[.]73:60798
95[.]181[.]155[.]204:35253
http://95[.]181[.]155[.]204:35253/IRemotePanel
185[.]204[.]109[.]146:54891
45[.]14[.]49[.]232:6811
185[.]117[.]75[.]123:80
94[.]103[.]82[.]22:49018
65[.]21[.]218[.]128:42806
95[.]181[.]157[.]130:11418
65[.]108[.]29[.]202:61024
45[.]14[.]49[.]246:18015

45[.]14[.]49[.]245:61619
65[.]21[.]141[.]215:8374
51[.]254[.]68[.]139:8067
94[.]103[.]83[.]88:60362
95[.]181[.]172[.]100:6795
195[.]2[.]78[.]238:6020
159[.]69[.]190[.]155:35975
193[.]38[.]55[.]35:16777
nyamekye778[.]duckdns[.]org
45[.]129[.]236[.]6:56220
141[.]95[.]23[.]41:62480
2[.]56[.]59[.]78:14716
193[.]0[.]179[.]66:80
89[.]38[.]131[.]227:47427
45[.]84[.]1[.]79:56124
51[.]254[.]68[.]137:49913
65[.]21[.]206[.]125:13957
185[.]53[.]46[.]140:38913
149[.]28[.]252[.]135:26948
45[.]140[.]147[.]31:22127
212[.]192[.]246[.]73:10854
91[.]142[.]77[.]189:45968
45[.]76[.]170[.]221:23953
185[.]215[.]113[.]29:8889
80[.]92[.]205[.]153:60983
86[.]105[.]252[.]21:34503
34[.]125[.]127[.]142:22010
45[.]14[.]49[.]200:27625
94[.]140[.]112[.]18:80
195[.]2[.]78[.]147:59722
185[.]186[.]142[.]245:1778
45[.]8[.]126[.]18:80
185[.]215[.]113[.]60:1751
45[.]66[.]8[.]61:58416
159[.]69[.]178[.]36:37556
45[.]67[.]231[.]50:59578
94[.]242[.]224[.]231:22141
80[.]85[.]140[.]26:45198
91[.]142[.]79[.]35:13400
103[.]246[.]146[.]247:3214
188[.]124[.]36[.]242:25802
51[.]89[.]92[.]99:5965
50[.]17[.]5[.]224:40355

34[.]118[.]24[.]142:6677
http://34[.]118[.]24[.]142:6677/IRemotePanel
77[.]220[.]212[.]176:35752
95[.]179[.]166[.]29:60101
135[.]181[.]123[.]52:52101
185[.]53[.]46[.]25:38743
136[.]243[.]179[.]78:23621
45[.]67[.]228[.]114:37288
185[.]224[.]132[.]232:64354
135[.]125[.]215[.]49:54405
193[.]56[.]8[.]53:25656
65[.]108[.]16[.]40:80
93[.]114[.]128[.]144:8165
elired957[.]duckdns[.]org
203[.]159[.]80[.]180:15808
45[.]14[.]49[.]111:26475
95[.]179[.]169[.]30:6677
http://95[.]179[.]169[.]30:6677/IRemotePanel
87[.]251[.]71[.]107:34919
207[.]32[.]217[.]143:39743
194[.]87[.]146[.]179:80
91[.]228[.]56[.]223:20793
87[.]251[.]71[.]145:12427
65[.]21[.]228[.]92:46802
185[.]53[.]46[.]25:18856
185[.]234[.]247[.]50:55567
46[.]8[.]19[.]177:41228
2[.]56[.]59[.]235:7188
207[.]154[.]240[.]76:80
157[.]90[.]116[.]11:29726
2[.]56[.]59[.]35:43636
45[.]14[.]49[.]128:16334
95[.]181[.]163[.]3:46303
77[.]83[.]175[.]99:4235
185[.]92[.]74[.]36:6049
185[.]215[.]113[.]111:55066
37[.]1[.]213[.]214:63028
77[.]232[.]38[.]125:50692
45[.]66[.]9[.]19:25061
80[.]89[.]229[.]97:7479
94[.]103[.]93[.]227:17436
109[.]248[.]175[.]60:80
168[.]119[.]101[.]124:32508

45[.]14[.]49[.]68:43238
5[.]8[.]248[.]83:61808
188[.]165[.]229[.]219:31829
193[.]56[.]146[.]78:54955
209[.]250[.]245[.]216:62660
194[.]226[.]139[.]70:31846
45[.]14[.]49[.]109:54819
77[.]220[.]214[.]232:13459
45[.]138[.]72[.]167:25882
45[.]82[.]176[.]76:43679
185[.]234[.]247[.]42:15495
178[.]32[.]202[.]118:43127
185[.]241[.]53[.]200:15520
185[.]234[.]247[.]190:34363
192[.]248[.]177[.]92:6677
http://192[.]248[.]177[.]92:6677/IRemotePanel
84[.]252[.]143[.]187:38919
45[.]140[.]146[.]214:3287
45[.]67[.]228[.]128:25676
2[.]56[.]59[.]235:61159
185[.]215[.]113[.]209:14536
34[.]94[.]44[.]44:45251
45[.]153[.]241[.]106:80
185[.]92[.]73[.]140:80
95[.]217[.]248[.]44:11695
212[.]114[.]52[.]76:6261
5[.]149[.]255[.]203:32800
188[.]119[.]113[.]123:58760
195[.]149[.]87[.]79:12439
77[.]246[.]144[.]104:80
193[.]38[.]54[.]112:4623
3[.]124[.]195[.]32:80
46[.]28[.]204[.]54:27605
80[.]92[.]206[.]111:80
45[.]76[.]34[.]239:6677
http://45[.]76[.]34[.]239:6677/IRemotePanel
185[.]53[.]46[.]25:21352
45[.]137[.]155[.]31:11556
141[.]136[.]0[.]194:80
80[.]89[.]230[.]42:5461
45[.]67[.]231[.]221:42619
193[.]124[.]57[.]100:4737
185[.]250[.]206[.]122:43180

185[.]23[.]108[.]82:20793
146[.]185[.]239[.]6:80
185[.]118[.]165[.]94:15838
51[.]254[.]69[.]209:48987
45[.]14[.]12[.]90:52072
104[.]21[.]79[.]131:80
37[.]0[.]8[.]184:2305
141[.]136[.]0[.]113:80
185[.]215[.]113[.]86:13625
91[.]245[.]253[.]6:16075
109[.]248[.]201[.]150:63757
23[.]105[.]131[.]166:2112
209[.]250[.]247[.]73:64156
149[.]202[.]65[.]221:64206
135[.]181[.]175[.]182:10628
50[.]17[.]5[.]224:80
193[.]188[.]22[.]4:45689
176[.]57[.]69[.]178:59510
95[.]217[.]114[.]110:20535
87[.]120[.]37[.]152:5605
213[.]166[.]68[.]170:16810
185[.]237[.]165[.]126:25598
95[.]217[.]159[.]87:4348
146[.]185[.]239[.]11:80
45[.]14[.]49[.]109:21295
141[.]136[.]0[.]182:80
104[.]21[.]5[.]49:80
http://gimpforimage[.]com/
172[.]67[.]145[.]186:80
95[.]215[.]207[.]87:3058
172[.]67[.]180[.]172:80
3[.]121[.]85[.]109:62340
194[.]169[.]160[.]30:80
45[.]93[.]4[.]12:80
193[.]56[.]146[.]22:47861
188[.]130[.]139[.]12:23747
188[.]120[.]238[.]188:28212
141[.]136[.]0[.]181:80
87[.]251[.]71[.]78:80
185[.]230[.]143[.]16:32115
185[.]250[.]206[.]82:21330
45[.]14[.]49[.]117:14251
212[.]224[.]105[.]82:80

109[.]234[.]34[.]165:22204
45[.]82[.]179[.]116:10425
95[.]217[.]140[.]34:18653
45[.]132[.]106[.]154:6492
45[.]140[.]147[.]111:22333
185[.]81[.]114[.]75:58642
45[.]76[.]235[.]60:49976
37[.]0[.]8[.]162:7225
104[.]21[.]24[.]246:80
185[.]80[.]234[.]77:17105
87[.]251[.]71[.]145:58198
185[.]228[.]233[.]5:80
91[.]121[.]146[.]23:9519
194[.]33[.]45[.]147:46868
193[.]38[.]55[.]96:53888
2[.]56[.]59[.]84:43393
46[.]8[.]19[.]211:40857
193[.]38[.]235[.]12:29867
176[.]96[.]238[.]188:20427
45[.]67[.]231[.]194:29525
185[.]170[.]213[.]254:56663
185[.]215[.]113[.]32:14976
95[.]215[.]207[.]185:64399
185[.]215[.]113[.]45:41009
3[.]68[.]106[.]170:59223
45[.]147[.]231[.]225:40668
91[.]235[.]129[.]135:80
193[.]56[.]146[.]60:51431
37[.]46[.]128[.]40:2787
185[.]215[.]113[.]114:8887
212[.]224[.]105[.]98:80
194[.]233[.]74[.]11:39744
185[.]172[.]129[.]61:52372
185[.]248[.]101[.]142:54217
18[.]184[.]50[.]127:6677
http://18[.]184[.]50[.]127:6677/IRemotePanel
45[.]67[.]231[.]121:53952
212[.]224[.]105[.]106:80
51[.]178[.]146[.]144:59643
45[.]14[.]49[.]23:32246
178[.]20[.]42[.]11:80
185[.]244[.]182[.]34:22602
178[.]20[.]46[.]22:7684

188[.]40[.]193[.]166:43180
18[.]118[.]194[.]181:25857
77[.]220[.]213[.]35:52349
195[.]149[.]87[.]39:20170
37[.]46[.]128[.]72:29799
103[.]246[.]146[.]46:50702
18[.]117[.]82[.]8:58546
147[.]124[.]222[.]75:42864
212[.]224[.]105[.]105:80
212[.]224[.]105[.]80:80
45[.]14[.]49[.]71:18845
http://185[.]231[.]69[.]253:6677/IRemotePanel
185[.]231[.]69[.]253:6677
45[.]142[.]213[.]135:30059
213[.]186[.]176[.]123:80
212[.]224[.]105[.]79:80
185[.]117[.]90[.]145:80
194[.]226[.]139[.]106:25644
95.217.123.66:5143
94.140.115.194:80
45.144.29.134:26392
111.90.149.108:36626
86.106.181.209:18845
95.217.122.120:8374
176.114.11.244:80
93.189.40.76:80
185.117.90.158:80
193.161.193.99:55339
62.109.1.213:26078
194.233.74.11:58910
212.224.105.115:80
188.34.152.197:62942
149.202.7.96:60574
176.31.116.35:7078
95.215.207.58:16597
193.110.3.32:80
65.21.103.71:56458
45.14.49.91:60919
193.106.175.53:80
135.148.139.222:33569
193.110.3.6:80
185.237.165.42:61503
79.141.165.169:80

216.128.137.184:6677
http://216.128.137.184:6677/IRemotePanel
86.106.181.209:58703
185.215.113.63:23098
37.0.8.151:46665
109.248.11.240:18612
80.92.206.25:4311
185.125.18.50:80
185.117.90.241:80
193.188.22.226:30072
185.244.182.34:56068
46.8.19.196:53773
185.69.55.138:80
45.140.147.128:4311
185.186.142.83:29867
45.142.213.135:30058

SHA256:

28f4a775a412703de465d39a1415a671efdf4bf40f89b1fc2b35c817cd79402d
639a69507d10a69d3e4634cff299f048ea44daf93ee5eb186f5b87e03981e9b9
37d94c0ffea439a338a4c5a5267d07ac1aa1f6cf230bc2986f95e4e6d80cf365
3805dae603dcd659643f0888fe35b9bbbd0173c63ff5ce1ed5bf678e4fa5db90
6183d33fdfc6ea281c59c460d0177ff05e15a7a0baaa62f9064839ad88f5c261
0739ab90f698c1611cb646121808cda8c0a46e060a0bd8195d32812282c37fef
8f7cef2c0fa345df0232afa86eb779e189bca8b3ebaf7ff8b7000f1eeb49e448
8610e4f5fe6961af48752bd4ad6c815e4bd604cc7b489b7b4c9e55d463993ed1
f4786214620b515cec6586781ca473504d6a8558c192ac395a2d4ad5c235bc77
009d0e416fa47b7050f7384e864f2f6f26b901fe65c2673c2a345f36d966cf05
edc5b5dcc927af0b6e445c8fa70aefecb080d242cb160e44b2abdd32a32a36e7
f0e1e6986f17f286ed164f12f5f7fdffa3b445cf8603d013dc9eb38bcb175ed7
e49ec26779ee42f4130f34f73cc067e1d469f95fd7fbfcf7b746a4fb5cebb496
e72143a4f0dc2c89d4bba8ce346ec3290a189101767fe3090216adf9d81c0978
db7089144ad29efd77e49bfe299e63959f7c8cad57773447b02292e056a19f40

References:
https://cyberint.com/blog/research/redline-stealer/

Malware: Panda

Panda

Panda also kown as Panda Banker malware is banking Trojan is based on source code of the Zeus Trojan. For the first time trojan was detected on February 2016. Malware was spread via email spam with malicious document and exploit kits. Trojan targeted people working in mass media, manufacturing and financial organizations. The malware has all main functions of banking Trojan: formgrabber, screenshot, cookies, certificate, credit cards grabbers, web-injects supporting (Zeus format), and hide VNC remote access.

Platform: Windows

Threat level: High

Category: Trojan

Indicators of Compromise (IOCs)

CnC:

165[.]22[.]80[.]247
http://165[.]22[.]80[.]247/download/6126486da2966558135ab386/test34/test_34[.]7z

MD5

fc2e33ece56807a079ab12326af77b0d
173bdeb36ab02f4ff8f60e37881c6ae2

SHA256:

3d0e5d42ac1f0adad3fb5edf43d370b1c6dce6a859324b7b93bfbbe5f4bcb9a9
4b6af0a183c9a2e5b9af770742bbed36c6a0b7436d4faa27d64a414596885592

Network signatures

TROJAN GOBLIN PANDA Looc CnC Beacon

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN GOBLIN PANDA Looc CnC Beacon"; target:src_ip; flow:established,to_server; urilen:1; content:"POST"; http_method; content:"Content-Type|3a 20|application/x-www-form-urlencoded|0d 0a|"; http_header; content:"Accept-Language|3a 20|en-US,en|3b|q=0.8,en-US|3b|q=0.5,en|3b|q=0.3|0d 0a|"; http_header; content:"User-Agent|3a 20|Mozilla/5.0 (Windows NT 10.0|3b| WOW64|3b| rv|3a|41.0) Gecko/20100101 Firefox/41.0|0d 0a|"; http_header; fast_pattern:49,20; pcre:"/^([0-9]{1}(?:[A-Za-z0-9+\/]{4})*(?:[A-Za-z0-9+\/]{2}==|[A-Za-z0-9+\/]{3}=)?\n?\r?$|[A-Za-z0-9+/]{100,}={0,2}?\n?\r?)/P"; reference:md5,d432b2b979ee021c61ca02f3010239f9; reference:url,cdn.riskiq.com/wp-content/uploads/2017/10/RiskIQ-htpRAT-Malware-Attacks.pdf; classtype:trojan-activity; sid:2826030; rev:2; metadata:affected_product

Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_04_18, deployment Perimeter, former_category MALWARE, signature_severity Major, tag GoblinPanda, tag c2, updated_at 2020_08_13, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1041, mitre_technique_name Exfiltration_Over_C2_Channel, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN ZeusPanda CnC Domain (henfobuthis .com in TLS SNI)

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN ZeusPanda CnC Domain (henfobuthis .com in TLS SNI)"; target:src_ip; flow:established,to_server; content:"|00 00 0f|henfobuthis.com"; reference:md5,23c7055d6c0c09d6e9b2c68ebad95cdb; classtype:trojan-activity; sid:2828569; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_08, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, updated_at 2017_11_08, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN ZeusPanda CnC Domain (rowrorofrat .com in DNS Lookup)

alert dns $HOME_NET any -> any 53 (msg:"TROJAN ZeusPanda CnC Domain (rowrorofrat .com in DNS Lookup)"; target:src_ip; dns_query; content:"rowrorofrat.com"; isdataat:!1,relative; reference:md5,23c7055d6c0c09d6e9b2c68ebad95cdb; classtype:trojan-activity; sid:2828570; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_08, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, updated_at 2020_09_14, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Observed Malicious SSL Cert (Zeus Panda Banker)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN Observed Malicious SSL Cert (Zeus Panda Banker)"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0b|freebase.pw"; distance:1; within:12; classtype:trojan-activity; sid:2821613; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_08_11, deployment Perimeter, performance_impact Low, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_08_11, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Possible Panda Banker DGA Lets Encrypt SSL Cert

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN Possible Panda Banker DGA Lets Encrypt SSL Cert"; target:dest_ip; flow:established,from_server; content:"|55 04 0a|"; content:"|0d|Let|27|s Encrypt"; distance:1; within:14; fast_pattern; content:"|55 04 03|"; pcre:"/^.{2}(?=\d{0,9}?[a-f])(?=[a-f]{0,9}?\d)[0-9a-f]{10}[^.-]*?\.(?!com)[a-z]{2,3}[01]/R"; reference:md5,5fb74789a52b5c28a6c636facb7555f0; classtype:trojan-activity; sid:2825567; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_03_22, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, updated_at 2018_03_19, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Observed Malicious SSL Cert (Zeus Panda)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN Observed Malicious SSL Cert (Zeus Panda)"; target:dest_ip; flow:established,from_server; content:"|16|"; content:"|0b|"; distance:0; within:8; content:"|09 00 e4 02 0b 4e 94 ca e7 29|"; distance:0; within:35; fast_pattern; content:"|55 04 0a|"; distance:0; content:"|14|My Company Name LTD|2e|"; distance:1; within:21; classtype:trojan-activity; sid:2822233; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_09_26, deployment Perimeter, signature_severity Major, updated_at 2020_08_20, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Observed Malicious Domain SSL Cert in SNI (Zeus Panda)

alert tls $HOME_NET any -> $EXTERNAL_NET 443 (msg:"TROJAN Observed Malicious Domain SSL Cert in SNI (Zeus Panda)"; target:src_ip; flow:established,to_server; content:"|16|"; depth:1; content:"|01|"; distance:4; content:"|00 00 0f|gorgot11991.com"; fast_pattern; classtype:trojan-activity; sid:2821857; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_08_25, deployment Perimeter, performance_impact Low, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_08_25, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Malicious Domain Panda Banker (tontrumuchtors .com in TLS SNI)

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Malicious Domain Panda Banker (tontrumuchtors .com in TLS SNI)"; target:src_ip; flow:established,to_server; content:"|00 00 12|tontrumuchtors.com"; fast_pattern; nocase; classtype:trojan-activity; sid:2828430; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_10_26, deployment Perimeter, former_category TROJAN, performance_impact Moderate, signature_severity Major, updated_at 2019_10_07,

severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN ZeusPanda CnC Domain (linghogolac .ru in TLS SNI)

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN ZeusPanda CnC Domain (linghogolac .ru in TLS SNI)"; target:src_ip; flow:established,to_server; content:"|00 00 0e|linghogolac.ru"; reference:md5,23c7055d6c0c09d6e9b2c68ebad95cdb; classtype:trojan-activity; sid:2828577; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_08, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, updated_at 2017_11_08, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Observed DNS Query (Zeus Panda)

alert dns $HOME_NET any -> any any (msg:"TROJAN Observed DNS Query (Zeus Panda)"; target:src_ip; dns_query; content:"kuwiran.top"; depth:11; nocase; isdataat:!1,relative; fast_pattern; classtype:trojan-activity; sid:2822234; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_09_26, deployment Perimeter, signature_severity Major, updated_at 2019_09_28, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message Header Local

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message Header Local"; target:src_ip; flow:established, to_server; dsize:16; content:"|00 00 00 11 c8 00 00 00 00 00 00 00 00 00 00 00|"; depth:16; flowbits:set,ET.Torn.toread_header; flowbits:noalert; reference:url,blog.crowdstrike.com/whois-anchor-panda/index.html; classtype:trojan-activity; sid:2016659; rev:2; metadata:attack_target Client_Endpoint, created_at 2013_03_22, deployment Perimeter, former_category MALWARE, signature_severity Major, tag c2, updated_at 2013_03_22, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1041, mitre_technique_name Exfiltration_Over_C2_Channel, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Possible DEEP PANDA C2 Activity

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Possible DEEP PANDA C2 Activity"; target:src_ip; flow:established,to_server; content:"Mozilla/4.0+(compatible|3b|+MSIE+8.0|3b|+Windows+NT+5.1|3b|+SV1|29|";

fast_pattern; http_user_agent; depth:55; isdataat:!1,relative; content:!"Referer|3a|"; http_header; content:!"Content-Type|3a|"; http_header; content:!"Accept"; http_header; content:"|00 00 00 00 00|"; http_client_body; classtype:trojan-activity; sid:2020373; rev:6; metadata:created_at 2015_02_05, former_category MALWARE, updated_at 2020_05_15, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN ZeusPanda CnC Domain (mysitothar .ru in TLS SNI)

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN ZeusPanda CnC Domain (mysitothar .ru in TLS SNI)"; target:src_ip; flow:established,to_server; content:"|00 00 0d|mysitothar.ru"; reference:md5,23c7055d6c0c09d6e9b2c68ebad95cdb; classtype:trojan-activity; sid:2828573; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_08, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, updated_at 2017_11_08, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Observed Malicious SSL Cert (Zeus Panda CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Observed Malicious SSL Cert (Zeus Panda CnC)"; target:dest_ip; flow:from_server,established; content:"|09 00 ea fe 50 cb 64 b9 a3 30|"; fast_pattern; nocase; content:"|55 04 06|"; distance:0; content:"|02|XX"; distance:1; within:3; content:"|55 04 07|"; distance:0; content:"|0c|Default City"; distance:1; within:13; reference:md5,0a070be1dcbad1b5f3e50438c535b345; classtype:trojan-activity; sid:2828585; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_09, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2017_11_09, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Malicious Domain Panda Banker (tontrumuchtors .com in DNS Lookup)

alert dns $HOME_NET any -> any 53 (msg:"TROJAN Malicious Domain Panda Banker (tontrumuchtors .com in DNS Lookup)"; target:src_ip; dns_query; content:"tontrumuchtors.com"; isdataat:!1,relative; classtype:trojan-activity; sid:2828429; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_10_26, deployment Perimeter, former_category TROJAN, performance_impact Moderate, signature_severity Critical, updated_at 2020_09_14,

severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

Possible Panda Banker DGA Lets Encrypt SSL Cert

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"Possible Panda Banker DGA Lets Encrypt SSL Cert"; target:dest_ip; flow:established,from_server; content:"|55 04 0a|"; content:"|0d|Let|27|s Encrypt"; distance:1; within:14; fast_pattern; content:"|55 04 03|"; pcre:"/^.{2}(?=\d{0,9}?[a-f])(?=[a-f]{0,9}?\d)[0-9a-f]{10}[^.-]*?\.(?!com)[a-z]{2,3}[01]/R"; content:!"ad12812761miqw.xyz"; nocase; reference:md5,5fb74789a52b5c28a6c636facb7555f0; classtype:trojan-activity; sid:1003234; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_03_22, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, updated_at 2020_08_12, previous_sid 2825567, malware_family Panda, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, rule_origin gib;)

TROJAN ZeusPanda CnC Domain (mysitothar .ru in DNS Lookup)

alert dns $HOME_NET any -> any 53 (msg:"TROJAN ZeusPanda CnC Domain (mysitothar .ru in DNS Lookup)"; target:src_ip; dns_query; content:"mysitothar.ru"; isdataat:!1,relative; reference:md5,23c7055d6c0c09d6e9b2c68ebad95cdb; classtype:trojan-activity; sid:2828572; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_08, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, updated_at 2020_09_14, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Panda Banker Malicious SSL Certificate Detected

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN Panda Banker Malicious SSL Certificate Detected"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0F|107.181.187.182"; distance:1; within:17; classtype:trojan-activity; sid:2820327; rev:2; metadata:attack_target Client_Endpoint, created_at 2016_05_24, deployment Perimeter, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Zeus Panda Banker Malicious SSL Certificate Detected

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Zeus Panda Banker Malicious SSL Certificate Detected"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0d|novgeo.online"; distance:1; within:14;

classtype:banking-trojan; sid:2820593; rev:1; metadata:attack_target Client_Endpoint, created_at 2016_06_14, deployment Perimeter, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 5, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Putter Panda 3PARA RAT initial beacon

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Putter Panda 3PARA RAT initial beacon"; target:src_ip; flow:established,to_server; content:"|c4 65 f1 b3 cf a5 7e e2 c0 1a d4 7f 78 46 26 b5 86 15 f9 34 9c 3d 67 84 6a 48 aa df dc 30 60 24|"; depth:2000; reference:url,resources.crowdstrike.com/putterpanda/; classtype:trojan-activity; sid:2018555; rev:2; metadata:attack_target Client_Endpoint, created_at 2014_06_10, deployment Perimeter, former_category MALWARE, signature_severity Major, tag c2, updated_at 2014_06_10, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1041, mitre_technique_name Exfiltration_Over_C2_Channel, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Tsyrval Panda CnC Beacon

alert tcp $HOME_NET any -> $EXTERNAL_NET 1024: (msg:"TROJAN Tsyrval Panda CnC Beacon"; target:src_ip; flow:established,to_server; content:"|75 1C 11 10 75 01 14 07 12 58 5F|"; offset:3; depth:14; classtype:trojan-activity; sid:2021437; rev:1; metadata:attack_target Client_Endpoint, created_at 2015_07_20, deployment Perimeter, former_category MALWARE, signature_severity Major, tag c2, updated_at 2015_07_20, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1041, mitre_technique_name Exfiltration_Over_C2_Channel, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN DEEP PANDA Checkin 3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN DEEP PANDA Checkin 3"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"/Catelog/login1.cgi"; http_uri; fast_pattern; reference:url,labs.alienvault.com/labs/index.php/2013/u-s-department-of-labor-website-hacked-and-redirecting-to-malicious-code/; reference:url,crowdstrike.com/sites/default/files/AdversaryIntelligenceReport_DeepPanda_0.pdf; classtype:trojan-activity; sid:2016821; rev:4; metadata:created_at 2013_05_03, former_category MALWARE, updated_at 2020_05_13, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

CURRENT_EVENTS Possible Deep Panda WateringHole Related URI Struct

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"CURRENT_EVENTS Possible Deep Panda WateringHole Related URI Struct"; target:src_ip; flow:established,to_server; content:".php?v=webhp"; fast_pattern:only; http_uri; nocase; classtype:general-suspicious; sid:2018348; rev:3; metadata:created_at 2014_04_01, updated_at 2014_04_01, severity 2, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN [CrowdStrike] ANCHOR PANDA Torn RAT Beacon Message"; target:src_ip; dsize:200; flow:to_server,established; flowbits:isset,ET.Torn.toread_header; content:"|40 7e 7e 7e|"; offset:196; depth:4; reference:url,blog.crowdstrike.com/whois-anchor-panda/index.html; classtype:trojan-activity; sid:2016660; rev:2; metadata:attack_target Client_Endpoint, created_at 2013_03_22, deployment Perimeter, former_category MALWARE, signature_severity Major, tag c2, updated_at 2013_03_22, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1041, mitre_technique_name Exfiltration_Over_C2_Channel, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Possible Zeus Panda SSL Cert Observed

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Possible Zeus Panda SSL Cert Observed"; target:dest_ip; flow:from_server,established; tls_cert_subject; content:"C=XX, ST=1, L=1, O=1, OU=1, CN="; distance:0; pcre:"/^(?:\d{1,3}\.){3}\d{1,3}/R"; reference:md5,fc784d0df590fad68c1be4437ecf1ece; classtype:trojan-activity; sid:2822213; rev:3; metadata:attack_target Client_Endpoint, created_at 2016_09_23, deployment Perimeter, performance_impact Low, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2019_06_03, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN ZeusPanda CnC Domain (rowrorofrat .com in TLS SNI)

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN ZeusPanda CnC Domain (rowrorofrat .com in TLS SNI)"; target:src_ip; flow:established,to_server; content:"|00 00 0f|rowrorofrat.com"; reference:md5,23c7055d6c0c09d6e9b2c68ebad95cdb; classtype:trojan-activity; sid:2828571; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_08, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, updated_at 2017_11_08, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Zeus Panda Domain in SNI

alert tls $HOME_NET any -> $EXTERNAL_NET 443 (msg:"TROJAN Zeus Panda Domain in SNI"; target:src_ip; flow:established,to_server; content:"|00 00 0f|gloverkentok.us"; fast_pattern; nocase; reference:md5,d438cfe54ee7c4a3b31570f5431a2f33; classtype:trojan-activity; sid:2824983; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_02_15, deployment Perimeter, performance_impact Moderate, signature_severity Major, updated_at 2019_10_07, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Possible Deep Panda - Sakula/Mivast RAT CnC Beacon 5

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Possible Deep Panda - Sakula/Mivast RAT CnC Beacon 5"; target:src_ip; flow:to_server,established; content:"GET"; http_method; content:".jpg?id="; http_uri; fast_pattern; content:!"Accept"; http_header; content:!"Referer|3a|"; http_header; content:!"tagesschau.de"; http_header; content:!"ClipOrganizer"; http_user_agent; pcre:"/\.jpg\?id=\d+$/U"; classtype:backdoor; sid:2021203; rev:5; metadata:attack_target Client_Endpoint, created_at 2015_06_08, deployment Perimeter, former_category MALWARE, signature_severity Major, tag c2, updated_at 2020_10_07, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1041, mitre_technique_name Exfiltration_Over_C2_Channel, severity 5, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

TROJAN Zeus Panda Injects Domain in SNI

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Zeus Panda Injects Domain in SNI"; target:src_ip; flow:established,to_server; content:"|00 00 0b|mousisox.pw"; fast_pattern; nocase; classtype:trojan-activity; sid:2824274; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_01_09, deployment Perimeter, former_category TROJAN, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2019_10_07, severity 3, ti_malware_id 65c91fe4e3e72018680a835ed6fb2d1e57373db3, ti_malware_name Panda, malware_family Panda, rule_origin etpro;)

Malware: Keybase

Keybase

KeyBase is a spyware family that can capture keystrokes, steal data from the user's clipboard and take screenshots of the victim's desktop at regular intervals. KeyBase itself is written in C# using the .NET Framework. It was seen for the first time in February 2015. A user with nickname 'Support™' announced KeyBase on the hackforums[.]net forum on February 7, 2015. Shortly before that, the domain 'keybase[.]in' was registered as a homepage and online store for the KeyBase keylogger. Researchers also discovered that while KeyBase's control panel was secured with authentication, the folder in which images were sent for storage was not, meaning that after all this time, they could easily put together a simple script and find all the KeyBase panels available online.

Platform: Windows

Threat level: Low

Category: Keylogger

Indicators of Compromise (IOCs)

CnC:

http://95[.]168[.]175[.]16/admin/std/admin/
http://95[.]168[.]175[.]16/admin/std/admin/login[.]php
http://95[.]168[.]175[.]16/admin/std/admin/index[.]php
http://95[.]168[.]175[.]16/admin/std/admin

Network signatures

TROJAN KeyBase Keylogger Uploading Screenshots

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN KeyBase Keylogger Uploading Screenshots"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"/image/upload.php"; http_uri; fast_pattern; content:"filename=|22|"; http_client_body; pcre:"/^[^*\+\=\|\:\;\x22\?\>\>\,\#][a-zA-Z0-9-!@#\$%^&\(\)\x20_{}\.~]{1,14}[\d_]+\.(?:jpg|png)\x22\x0d\x0a/PR"; http_header_names; content:!"User-Agent"; content:!"Referer"; content:"|0d 0a|Expect|0d 0a|"; reference:md5,5626771cf6751286de4b90ea4b8df94d; reference:url,researchcenter.paloaltonetworks.com/2015/06/keybase-keylogger-malware-family-exposed/; classtype:trojan-activity; sid:2021441; rev:3; metadata:created_at 2015_07_20, updated_at 2020_11_19, severity 3, ti_malware_id 1adcf0f9b9b6c6fb363d2112e970dc20b03f6e6e, ti_malware_name Keybase, malware_family Keybase, rule_origin etpro;)

TROJAN KeyBase Keylogger Reporting Passwords

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN KeyBase Keylogger Reporting Passwords"; target:src_ip; flow:to_server,established; content:"GET"; http_method; nocase; content:".php?type=passwords&machinename="; fast_pattern; http_uri; content:"&password="; http_uri; content:!"User-Agent|3a 20|"; http_header; content:!"Accept"; http_header; content:!"Referer|3a 20|"; http_header; reference:md5,00f4601973c653ef7eeab355723b784a; classtype:trojan-activity; sid:2811365; rev:3; metadata:created_at 2015_06_09, updated_at 2020_10_01, severity 3, ti_malware_id 1adcf0f9b9b6c6fb363d2112e970dc20b03f6e6e, ti_malware_name Keybase, malware_family Keybase, rule_origin etpro;)

TROJAN KeyBase Keylogger Reporting Passwords

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN KeyBase Keylogger Reporting Passwords"; target:src_ip; flow:to_server,established; content:"GET"; http_method; nocase; content:".php?type=passwords&machinename="; fast_pattern; http_uri; content:"&password="; http_uri; content:!"User-Agent|3a 20|"; http_header; content:!"Accept"; http_header; content:!"Referer|3a 20|"; http_header; reference:md5,00f4601973c653ef7eeab355723b784a; classtype:trojan-activity; sid:2811365; rev:3; metadata:created_at 2015_06_09, updated_at 2020_10_01, severity 3, ti_malware_id 1adcf0f9b9b6c6fb363d2112e970dc20b03f6e6e, ti_malware_name Keybase, malware_family Keybase, rule_origin etpro;)

TROJAN Observed Malicious SSL Cert (Keybase Keylogger CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Observed Malicious SSL Cert (Keybase Keylogger CnC)"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0f|mattech-llc.com"; distance:1; within:16; fast_pattern; reference:md5,c10dbcdf4a651b61397aa5a66758bff5; classtype:trojan-activity; sid:2828508; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_11_02, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2017_11_02, severity 3, ti_malware_id 1adcf0f9b9b6c6fb363d2112e970dc20b03f6e6e, ti_malware_name Keybase, malware_family Keybase, rule_origin etpro;)

TROJAN KeyBase Keylogger Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN KeyBase Keylogger Checkin"; target:src_ip; flow:to_server,established; content:"GET"; http_method; nocase; content:".php?type=notification&machinename="; fast_pattern; http_uri; content:"&machinetime="; http_uri; content:!"User-Agent|3a 20|"; http_header; reference:md5,fa6f24a18ef772d9cdaa1d6cd1e24d1b; reference:url,researchcenter.paloaltonetworks.com/2015/06/keybase-keylogger-malware-family-exposed/; classtype:trojan-activity; sid:2021188; rev:3;

metadata:created_at 2015_06_05, former_category MALWARE, updated_at 2020_10_01, severity 3, ti_malware_id 1adcf0f9b9b6c6fb363d2112e970dc20b03f6e6e, ti_malware_name Keybase, malware_family Keybase, rule_origin etpro;)

TROJAN KeyBase Keylogger HTTP Pattern

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN KeyBase Keylogger HTTP Pattern"; target:src_ip; flow:to_server,established; content:"GET"; http_method; nocase; content:"/post.php?type="; http_uri; fast_pattern; content:"&machinename="; http_uri; distance:0; content:!"User-Agent|3a 20|"; http_header; pcre:"/^Host\x3a[^\r\n]+\r\n(?:Connection\x3a\x20Keep-Alive\r\n)?(?:\r\n)?/H"; reference:md5,5626771cf6751286de4b90ea4b8df94d; reference:url,researchcenter.paloaltonetworks.com/2015/06/keybase-keylogger-malware-family-exposed/; classtype:trojan-activity; sid:2021440; rev:2; metadata:created_at 2015_07_20, updated_at 2020_05_29, severity 3, ti_malware_id 1adcf0f9b9b6c6fb363d2112e970dc20b03f6e6e, ti_malware_name Keybase, malware_family Keybase, rule_origin etpro;)

TROJAN KeyBase Keylogger Transmitting Clipboard to CnC

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN KeyBase Keylogger Transmitting Clipboard to CnC"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:".php?type=clipboard&machinename="; http_uri; fast_pattern; content:"&clipboardtext="; http_uri; content:"&machinetime="; distance:0; http_uri; content:!"User-Agent|3a|"; http_header; content:!"Accept"; http_header; content:!"Referer|3a|"; http_header; reference:md5,fa6f24a18ef772d9cdaa1d6cd1e24d1b; classtype:trojan-activity; sid:2810488; rev:3; metadata:created_at 2015_04_08, former_category MALWARE, updated_at 2020_09_30, severity 3, ti_malware_id 1adcf0f9b9b6c6fb363d2112e970dc20b03f6e6e, ti_malware_name Keybase, malware_family Keybase, rule_origin etpro;)

Malware: Necurs Botnet

Necurs Botnet

It has been reported that the variants of the malware named as Necurs are spreading. The malware mainly targets the windows operating systems and is well known for its spamming and malware distribution functionalities. The malware mainly spread by means of spear phishing emails containing phishing URLs or malicious attachments and also through dating sites.

It has the following functionalities:

- Anti-detection capabilities to hide itself by disabling Antivirus driver components or other security features.
- Spread banking Trojans, ransomwares, RATs, infostealers or cryptocurrency miners
- Stop its activities for a period of time and then reinitiate with new commands for the infected hosts.
- Machines infected with necurs botnet make network connections to remote command and control server to receive commands and operate accordingly.
- Make use of victim's email IDs to send spam mails.
- Spreads malware that are capable of launching DDoS attacks.

Necurs has kernel mode rootkit capabilities, comprising of kernel mode driver and user mode component, thereby giving the highest level of privileges to the attacker. Along with this, it also has modular architecture making it suitable to spread different malwares and perform different functions when required.

Indicators of Compromise (IOCs)

SHA256:

03c770882e87585fea0272a8e6a7b7e37085e193475884b1316e14fb193e992d
b0c173e0fc28e0f1bc8debfe49de01f306d372a0516d88201b87e441f3de303e
b87e0dd9b0e032c6d2d5f0bf46f00243a2a866bf1d3d22f8b72737b4aa1148eb
00ca7e9e61a3ceaa4b9250866aface8af63e5ae71435d4fd6c770a8c9a167f22
1fbad258fa1b21723770281ee12c7fad25a1f7ee6012be842c8660f9efff7950
748e202a2c932dd43bf98f0ad611f79e1c8c1653ba03dae4416981c57a30d343
502497f5d165b64a2e287d77a06b34abcdedff227089217a874f49f58b536e92
6599a9e29bb7c607d1a13dc43d8df76c17c93449b654d4e00fb96e02eea2df32
4f9b95867b6118af70625b49760b75987e152425ab9420f83160e9cee8e79eb1
2c5d0ae2ed1596394ee8aaa2affe57f7fc62e7338d70f761c906091e00ccdfa0
e4c5422288d38cd259929177e8d2a2aedf7d6e2c16b19c437be3a36e43601b69
e8f8fec213d7fef4fe23dc28740e97e40ba5a180b6fc046f334e2971f428ca9b
2cd60385887a69f42a945006cbf418834356a5ba6e764fa2c1bea4b4336698f0
04f944284dbbe0f28902a31d1c28b11bf10b22bbff170e18b7d6a9aa213f1142
f21e070fc12eb506400bef4d5cefc52666ae53323f9dae93300fbbd3f0d25d40
de209c862d415b25c1a2b38985829c1f04513a262b11ef139930ebc7c4a82d98

c59f7216ba319749d14e097fa2a090262bf1321061e0b7794f98eebf287ad273
e22c5a72111b9037e3f98d7f7e7e3135ddb4fcdaf85e90ca0f9b3e0492232235
2535c52dad357d25e5ad05f89977c8fff622d99ca145328debf9c5559ec9f4d1
0bae076148e9c8a4c0d5f9c2080fdfe155e760daa74e14e132e5ea0b349b7280
b196bde744b8a3d28acd2bc76bca2e415f98d5544c11dc82f7d90ca25dd7c13d
e0d150a5764e1251d6dc01137419d2ac5092edb2350b6f880a2d30f59f21648b
ead15d62585d13a7f5eae9f5280db7b54f769039037a375630240a65507acf54
1b3194d6c06478e877eca6da44bda2f18715d7b9f811568e5ef5cddf86da9130
7241f86c2952fa2e1ef78c1515b919a0e0c4b934180d6a81f81bbfc075a3d2b8
77f164474edea3adf67422771b851c3b1ac6526a84d85671f72bd6e2f513df38
23a89dd8429748cec6b2250d2980dc3798bdca07367ddda0e1d8c73b0d3b4b47
b1dbb1ad6e5608a809e0ee3111aa70ca0e4f4fb8842466b55cc7c23be3aaa948
fa5f5beaac5ec303c3e9b7b3d9def7bdd676d58d38f9849a51ab304786e0de94
6fee5f477baa3b76805da4906fbc081d74c5e40a0b70e701c7ee0f174f26e354
fb14086aef4e0c707ed8ee79aed13565b738b9d2f799db94acc77ad615df4356
35009fdc37faeb343e850e21a4d3990f8e3d34fcd7b8fdf7f7246c1a9d6b35fc
6f5bf47325dfe356f86adb871d638a05b6fa1b6bb65c8f55a2749a3ba3c2a491
2e3e168c9e0d1fd9f0e7b561e370c4f2edfb49e6fd5d5c487aa8eec4035c56e1
8c9851f4dc636a7ce622b726618a603488655a3115894ba02e0d684516239380
5005de2a04c1105f8ba5c5aa1ba30fd669fdb5a39b60f41964116f7b5d6b2b37
bdd39542eecf972cf785f0a3783769596ad16f6eae61e73824ad7d6719b258f6
86a6227cf0c81a7f9221206fe5a0bef4c94df38f4b95fdb976fad0b23579fcc5
82d7cc6af7713293c0990c33035379201452ad58a0180163c4c3e40e27d9e6f3
48b0bbffebc217c584c2fe7eb3c69e82d10fb16db29accfebd220bb50380698c
14928d3f23804ed5ba0d9f7e02ee06c0d2ef2155a870c77c2b2e6cf771b00e20
b64bda5f26cb2d5566dc91860c19d39d83a9a15bc575cb84747197863f941f46
845e1fa87bcab2359bf5d03f6cf0f93717c70e25a55633b04279ffb8a08f876d
40c01bf77af3a377fa18ba34a2d07f7a8de04b6379b61511d76e17cba120a771
f93b85be0cc6ac3aaf4a8ab910af8bc9c9f148664e5ad2b6d011f50cfb1b3909
f1e8f6ba5eca8a7b8a330dd7cc25a963e98d7eb705ed1cb8daa3417f0eeff255
d7e21f661997f0b051ab47b4a85af3a549f2c877d165c597ba0899849c6dfb08
f3ec0f14efacaf71273b01976fc9c7f3c9b5be2e4e79d64b4ae6ee73a38a3e6d
135dde22e025005226470bb00df15a5882664ba7be2890e4fdf773a22d2286ff
c28dec4a1c668f2b0808b7261594f7acf158896f6b159c299a257191bec46d7f
2a4aa54359e2c472022c4adbfb44d7668fe4f09c25d5b9c8bc2485c0b29a749a
6335c60a0f66b9a0b209c8ac345423ceec98a9508b95246f4e7e2e62786b65dc
8b4b4e93c927bf9d107965b904ecfe22e4c66a12a739f16fba95f8853502d394
94a661acf172a288ecb0ddd5b97490fa13c7b9e4ee9a73321d24c5d7dbf155ba
8e8e0b905054a3320c5aa49657df54975b92da3b4fc083f2c155b109c45c25a6
9c8fc92674b4ea500f3460a8dfe01b086f0fff40c547fbde8760c96f5c046a55
2aa831dc0f27a2d747435c16990a3294f776799f0c1955c308c9b2e397a85538
956b63f7e9bf7c5b21f591d12bc12ec59ab180a7a694f5bd38b6865300b723f1
92e2ef830a1c1e282a2e3620c1a25c821ed515009779acf6b850217f557f7915

c30e8ca3173401b001de02f545870a3f25d42d892f9596d8641cc3324afe8840
2ae04579eec0f1af475d06388c8b8a13e63ccbe92474f66115fe17d3f7b902d3
298f84bdecbe3e0e23f80a76254f802f253e054c04cc3a16ed4fba08704087b7
15a0bd5dab10341655ac110644e332e8972a1a531adee278657d528d5a4acc0a
8ac824b167d9f23f02f048d9ea1657d2f070a38add1406a968255f24cd2adaf8
cd1eb34f3a45b257bed15fdafa4b6a9788b158f1dfe9b9255578595221f92973
345c3862678d7b979f8f51422aac4382532d3624bbd75bb2205d4ac32e752c17
1cefa19e1bf8cda11168921acf7e2a61750f78cbc15d375fceb26bde73f66feb
f0a137ab92846fd99fb8828d36cd98ad46f7f1dca7651d4b0b7fed3dea78b6fc
778c2dbb1da203e30394b0a923e55e35697f4432efc1f0f0c3c41d81a7a90860
a8730e6eb1ce1c0ec91fd2371d53d11feb51afcb6e25f1dcbca7efc665f50934
f1881b847abea278660466bd8eed5cfb6415909769475fb849685acc2d110f5a
8d4b317a21a7685e4066ef040d003782511be50790eb708ad26006f17cb6acee
47ffa8fea4986abfefb0de951bd3f829480209c45817b21e3a3e6cd9e27ebc0a
3a4cd03789ca51d53718508a57a2c59500ddac132c89f50fb5d95270e95a73e6
4cc82919276e65f58fe841f0da69d063fe5e196a13a19458f47b640f1689c813
d05f4d98e44d14ac64ebc1170142232912cde36eb77c0ccd2869788036761257
f1646224bfbc4d1c657bf47d7c496ac1282817484ca5a613d5a181b2ac112002
76ca7c477b0af7da335cccdd951300c26a9f13cbe7e623d94817d92e1723f53a
023baa1f2500bcf1828eae79bd49f5fae0d3e39bdb19267f01b20c84984cda5a
fcc257db11a49e1fb12658a992c04f75cd0cfa4010ae07ee10c4a8647df71791
a25f0a95a1a953013288d503bcee88f1250425678ad06161b8f7d5e85cad18e0
90ae1b460196df46aa5eceb7733348ec06907ea5e12639a97bee9a8660eeeade
0428be098c0d03f630d4eb7cda6b8694596c9eeebea17f2ce7e4136b9340d218
03e4d28308eb99a8c39ed499e4f23c8ff7580c32a399675d4895761c3791151d
e212fafdf27f579678e5ef217e79d9072562bdfaa2f571b9785218bc833e0b44
a9c4c53e851a58971d62297723de1d8cb73889c912f05341797603568ee838a6
d1d66e8a8bfd7a5abd738437dea48c2aa7e438f32e8ca953d4ea40f915cb8a9e
76c7020ff73beee56291b2b05000ae7e3663d92f3e4ec44a309a51515cc4aa7f
43cc723616d7b6c893b240db71620443ab9217cc19ae59df729fa2048a1650af
d1ee8a04e22fdff87e027f50bfb48e1f9cb20c4bce330c0e8ebef8802d5756f9
aec8ce3910920d09cd73edff6fe30b2154e3605ff5cd073b9be77dc53b5691ea
f79dd28832c3fdac339a701f73ffb2113c5e1add5dcc59643092d404c309e4e9
af12f11f6c8ad3a2d07275f4a0e9505f623c0b00554f6fa7ff25e2828ecc756e
c4f3fa4a9c84db632516d0b959095fc7b1fdf644c2f5efc32d44d48a9685c031
0f2f0756f59a70d886de0f97aac11f2f63d61502e8946f407b770fa6ce847f31
cdd343e4d903241d24997809c3b72a784cf2de36e13c8c5bbcfcad012c9ccf05
d2e701ed3cf082b1e3bf2347ebdcf71353f4dafae82a83ab23c226a8e3e7da27
c9978d21dd870699596e3ec15e2750624ea4d356fe9a94bc277f16641a41c0d8
82c4347908551bdcedced44c7608f6ce21efb254ed0203aa66223bc81da49ba4
0c1fe5ec678d9b9917212bd9d4879d6454aec7ff2d20c2057540e7af8f7c714b
2ec2c650a57e601273d5f9dacf69d7fac8c1b454991770b65f3ba4a854a70c41
bda0a0a3c8f5443c17e518910de18339240a86783464133c5bd631a776a34cdf

c29aff59dddadf5f0260f4343f123fde1be089997c16ce3c440a61506e2dfee5
a51ad34ccb701af345b6d37cb8f6a726e105d725d377cbc796b2f880d979c5be
b1d5e926016491d8bded5aaa29d8bb5a96614468e53283a6b43f008dadea6d6d
04e96c7a6bd4ce5ea57028bedf7c3abf8d961d65c65337f5297684228134e93d
928ffc036b623b0411a3d50571c1297397a0e4c72273ad1d89f815ac5ba16677
918be9a58770b65cdff21a8bc95d4be296259e545162b2c9f826bcdb7dd0b975
1d89cccec8c1c66db35e6d21866102c7cd6d0fb186b539871c76fb5e9998440f
d708c607a9de7c3f8188eaa94f0fa700eb53a6733ce7c176bc4fd99bc443f38e
7ce3785aec3d5fe4515082aed0f4fb08ef4fc65c8fc5fce5ec038fe010f7dbd3
6822d3b61544a44104e1ecba40e09bf175abe5ae1f8f391b91a45da2ef2c1812
e02ee08cad5e7835371315774c526e62afe1b754dd90d339e3c355fded3ecb5f
aeaeb874b1a73e2dd83b1be2ace8ce65cfc62c951d28dd5a46e3c8b72d99b3f6
eda46d89028298b4410fa513726149073c8fddb20c64e4e9f5b656e9cb35822b
f8b9bd23dab34e9001d2b734cca71c9915d52b6cf4e86f966ce8ed60172464be
4c6ce4083dc4d92e91b332f03605c767c246d3d2b90f4c839d60bf9bbee44301
c74ab94de5b1fa5367b15defea0952339972205ede8f940cbe19541928bf53ce
59d2111f29384fe105fffe5a58e5f367eba383297be70d82ec3dffaa89068171
4476da27b0f03d24efdaba507fee7c5eee28fd0ea7a220963bdf080f2c0542eb
99403a72a6f1913a7906e962a0d843b2298b401bbb1c46e4413d1b0abf09f81b
2f4be5d3c670ac9b1a78d389f869daf93bbda6f01125180624cae30c1b58e774
f2d2ee358841aeeefa92a01a4dcd5b1f29f19b9354b752260045aedc9ea1de58
3c24f8815e6edfe0b23fbe9ca53b98e9f2440c6547a1d520bc9282ef8355062a
360bc096f7b5f7defba0884051e246d11cee0ffd4bb630b40456fda2ef28bd4e
66434e84bf67f488de484d282aa2185277157549668a89fee73bdacfcc4ce406
409b1989f4ba7411e3c357d04522f9daebfb7a3ab3ec3064366cb14b5352506e
86218766de6d8c7035e52b94f1a2a2f8c26e8c174f6e587797f15d0b14c2a253
cafc30eee0afc6ea3010bb95fb6c24f35b6e4297f664e33be0653342524d7021
092cd0f01f5aa85b7e1b7858c515b93d6486f61da7e8ba11f4488feef9c7fd30
36b6406fe05691bd435f21a4749acc3ee42aac2aefd6c0350d689fe10a39116e
76b3437a2548d62a436f95a1fbed7b05c6c403fd2b17c72e0aaed60db5f1fd1a
bd385e70889d83897ed1099d0cc50211433a53fbb02f5685af201910f251b711
d477620d5ae3f032c819ef2ba5e67ae81d23a34e1fa9cf8a08ebd562d2adcacb
17b80212028f5ce1058664c3bd6d2dfcd7bf5374db691ca6ec3dd626af368cc6
18ad1472564629dc2e5159a9a192fdf718eca4fa7c2baff13834639f0b389256
76a97d72dfa5eda99778849e62caafb90af0bab94ba09b3aeba2e8a8930dcefe
2876e2c15453228deece2b44169c95488be1cbf8ab5a17a07d4be94483ef2c32
2a2639ded7ff98ce2412542e2da76fa336971da5b40d3f90f4739a5777ff7b0a
20ea9f2ca4d2e5e8b79af3ea438152394b1cf492ff594edb7ce3df38b45dca60
c81ed79bf3ccd44c12c23295069a12527146c788124986614cf08dc00b87a83d
bff61ca109f8a20eb19e1eb9a922c8285d079111b5b3f3f993ef1f7624963d8d
66f497c3a524c27d14fdbaae5d60b837e18fe07d4fb9c02b546e92b7f85bf0cb
2059e50a0346a707ec0a4b9fcb1bccefe444e8ae0221dd33989c5e819f83d6f5
e588a3467de8f63dfa12cf8e938ebd19b649852249f50f0e8a71fe93fc62bce0

44112222cab7a861b428a76af7067ee562a9fc8ad213d43ab83aa8f7aac4343a
f2fc2c82e4e9653f2577bec7f504f0b1d361b67cf0016e9ab18baa79621f2f79
8b1d2648e356782fd3d6c6e3b3c3dcd3b8f72e35cab6c9299f06333083e1944c
bc17ce4893e24c5faba59efeff05b0e05d7f5ad04a8f2c76844a6fe91b1a778f
143fa063ee02b9a9539455263015e9296285f97758abb5384604ed33eff744b9
7c19f6a070c1206ab7388fbfc17b805812ba17bcd753f8a3e6a357345aa99871
3fb1175af894d2b157737628169e5cd43bd489952c55ff9f255e0054223329c3
bdb33dd59e6ffc03a9ad0e58f3f280436d876dfa704c1d0e59601ebc957e38cc
ffebb94676c767fb2cbd86453e3127f7abf459c428f2d80228f2cd7e1b55fff3
ca5c4d2bb3c6c035bb0137504b17ccec31deb366757440feb832b7e0d270b487
44687edc7169d919ef0891e41487ddefa30d93744d6a9e3ecabb5d6f8d88c039
d6aa22aee572dd90161ba793b8afba27dbf50df4d23b2921d131626671e8d966
8476cf9307933499771186dfe4c397905ea2a320c488b357ba0148f862b9532e
1705d38d2ea80177963d67fd18e836326d70a239378d6b9c74d445c5e0b423d6
3ccef773a5527c7128987bb8d359726f0b3d4d84dd6526c1b3aa76fd98b68539
6eaeb3aa26dcce83342eb2ed055c623ae43c629eccd7f1d31c0380029ed9741d
65e5a0956b7e83e484b0fce962e08f1d75aefb0232d1521c97e186a746aabd2f
9008ee571b139496190f4e54d155300a1c875a8fb9096cfa27809e4e71955176
1b15c90d67e4b7522ca61e21133b155eb7f1cf32328a030784dc2d95ee7d10ad
32324fe312aba53c25a512eb81f7fe6ab7b2a44417a0cd0983c6f19cd29d5b26
1b025b5f24d42eed4eabaff15cee80fff3484d4205be2611f8dce5d4dce9020c
7e69993bfe292a72f8377d47059741f2b9ef2df1c93b2a0457ed8c1acf986e70
69ac4202505b603b490e5f2ca4e310af57a16c6c3f9a2efa928ab0d0faf7ae6b
1fc5a5831c2d880fc5e32db55adef8ad1e0f68b8e245ccaf1a3ee78f83a7da27
e4426738a8ed366f2773aa3ac9374dae6f3ad41759dd3227a8d025fac2af9b49
a0b01d5f3f41b49e07be198408910084912cc5db030aa4d0449a8bd2677596b3
06d42acee69178a161b7317c87515e4bdab647976985a1d172411b799ffbac32
eb9c6616204c358aa06ebb181cfcf8220216a9531b05006e8ed5dd714f3574da
7e73b086c5d0d693483a57847aa738e8c3b65b45f8603b5980721795af4534dd
7a6052881573bb7d976a5bbf39e1a9221dea68193f27c142bb77534a5049e5b9
f08ab6e0fc6dbff270b2d42f4412375cef3d543b311923960ab432d35754a56e
63fc82ce40ea946749e7312517b103fad96e8da6a01c63e44be93cd196aae692
2592d4bf18d83d1b9f98176ce389d6ad5dcaa399f3a549fab15cad520cd24470
5e9f7cae76f9888c732a77345326e442f56d94e8ed253eabb812fc2ba95e01ca
ff92433ae4ee90b3c6dd3cd5655302be345addd2a57bf143ee982e692ca7ca33
2881600b108ece9a1df3e7659370e3ee79cf233e9723a9acd7985452c5915eb3
f1326f8c348b6a4eb0fe0c3fcdc27e8375fd0ea7ecca54d392de790f31a9d037
cd0a031a65a10e8c549c29c1b5db87ad730c84ef9ba48041b3c4a723e56ee71f
8e2cb05dbf3375e66488f387aaebe31c51c95fea135eadace186362629988a4c
0559d32f6a20cdfa380eb1eb17fbc4aea9e39f3203f4b7818281e0fb117a6977
32325761402e0b55dd9fe8b2718bc213491eea6f57bc354e358a6edcbe584dd1
026fa1191fcf895ce375ad8f8f2bda47aa8b1cb27e6be490399a1ad47d452b68
a20ebaf8b9c14a2738795f0c38b48a712f3e9fd293a51c5475b15c959856139d

04ea10db95049ec292e712803dc87c236cc3e3e7c2dd018e84d841f9060a15ef
aa09f65734b2b6972b47b8845aa8f59737ab5a6b5469d7a6e6fdbcf12629b287
0af35bd7ffe0af328cff2cf39585b4b1b69d550c94f0b407e348085dda0b4284
ad022ea9c0bbc852806e87f8b1a2d4ffd683116876304613160e975f430bd992
10ce87f33381989373c519e2ff539f86c2a0a2a4cab0b791e82d4afece0367e6
b0ad3d8fade247b219d7a3c8fee781e26742c1733de8c00cc50254785cb71e09
1d73ce6cbc40b02c59c928238f1d316b4340c4ac1e0231f608fa7b5d2fb24836
b27fb67c5a86f65c762a8af7537c8c5d5fc27e3e2f600495d22cd39fbe82018b
24982da99435dd1a12c1a7bda53e7325b5081dff96b441287a99027a6b379309
b78dcbf395b7c934344e4f1bb3cb08628455e8d2a997dbad0bce7afdd573ff8e
2665260758371f88ca4e49dd577e885fc138651a0e2b3564309b892eea36f7af
276fd3e1e484996c7f2cd8d9b9d0125dc0d9d6488a65417fb80662616b76adc2
c411f18d2d53f26dad5275a549d288447a492487b46379fe07087f42792a1be1
2cc4ca03a31e970a020bc85bb797847abaae41af7c0734826213b4938e5040cb
c7dc067b3e6ba29ffbfc45d9c32219f3e6898142dfc6da374c752b0bc0fb4c01
350e989a917614bc2f830dbe61cbad08b444d9cfe96706ed0bd2d86e3a586ec4
d38ba2dfc9e02a2c6997901aae2197402ce7cf3e79973b81dd06271dbac17328
3a9cbdb511a5c3fad3f3d6eedaf0fe7aa61bd362d374aa8b0e7924ea1a07be48
dfb72c342d42655c6309a7496acdad721d7ab1b171e90eaef8b676ac99a06461
486a3f4053c1e44cb09a43d645227b4916a6475658f3e21ee02bae66df6a8667
e0f9cca4d7acda468bf1e8f0fab70f4b95b37cc711dae3d972aaf0c4bb0dabc6
52db4cca867773fdce9cd8d6d4e9b8ea66c2c0c4067f33fd4aaf6bfa0c5e4d62
e4ec3cdf1bb578d2740c06a0e615f4b2f08ce1ff6f925670a92630fc3daedda1
65184fbf32ef6a9e109115aaac401de7c0af797d485396091f284a262abf222c
e67599948a41876b59f09af447816391fd5d29fdebaa5b1fc344980c0b13574b
6f354a86af7f1885935f0214e663734479e560784c257fa006030fb64d9f38bb
eb822fb0d99a0b8aefcf70e484b997979a4a4c22325dfd52c4bec492e9937a03
750c0fdd43575e5110fe348f8fc46f5e5413b0e1aed1c3547bb2e216255e4f00
edb73979f8d857a35f0be95538db9bc33bc583021feca81c1a64f2da18a902d3
8424b5178273e0b5d17ae34a1bf3889b1e1d4a351246d342cad933e1e5ec7779
ee4adfcfc84afbde6180495e132a5477c8d48739051db7d996e078b33c1a5e45
8b178a3e113a14ebb0e288d610540b15df9a3c59f72667d7142782fd3ef9f370
f175ed80e667d31877ad75117f2e98a2fb83eeec8f5a523d9ed10ae6fc2dc453
8bb3c9df22203fadd942b4a4820219f88e20833f9f33ff9ae0361074dc3786f3
f3877a6e45463ebfa03b49087852572793e4233d084a64584e29f6b7c83af1e8
8e508ea5009677860b67e34af22f6706e6aa1e94c84759a43b1c9f3e40dbe01

Malware: Sality

Sality

Sality is a family of polymorphic file infectors, which target Windows executable files with the extensions .EXE or .SCR. Sality was first discovered in 2003. It infects executable files on local, removable and remote shared drives. The virus also creates a peer-to-peer (P2P) botnet and receives URLs of additional files to download. It then attempts to disable security software.

Sality is a family of polymorphic file infectors, which target Windows executable files with the extensions .EXE or .SCR. Sality was first discovered in 2003. It infects executable files on local, removable and remote shared drives. The virus also creates a peer-to-peer (P2P) botnet and receives URLs of additional files to download. It then attempts to disable security software.

Functionality:

Injects code into running processes and loads DLL files within them;

Lowers PC security settings;

Infects files on local disks and removable drives;

Downloads files;

Creates P2P botnets

Indicators of Compromise (IOCs)

CnC:

206[.]189[.]61[.]126
195[.]38[.]137[.]100
213[.]202[.]229[.]103
217[.]74[.]65[.]23
217[.]74[.]76[.]129
91[.]142[.]252[.]26
69[.]172[.]201[.]153
94[.]73[.]145[.]239
173[.]193[.]19[.]14
185[.]64[.]219[.]5
5[.]101[.]0[.]44
49[.]50[.]8[.]31
103[.]11[.]74[.]25
173[.]0[.]143[.]204
107[.]180[.]27[.]158
103[.]224[.]182[.]246
46[.]30[.]215[.]173
199[.]59[.]242[.]151
195[.]22[.]26[.]248

64[.]29[.]151[.]221
63[.]249[.]150[.]76
23[.]253[.]126[.]58
93[.]186[.]196[.]19
31[.]193[.]142[.]216
www[.]litespeedtech[.]com
pelcpawel[.]fm[.]interia[.]pl
www[.]interia[.]pl
chicostara[.]com
dewpoint-eg[.]com
suewyllie[.]com
www[.]bluecubecreatives[.]com
724hizmetgrup[.]com
yavuztuncil[.]ya[.]funpic[.]de
www[.]ceylanogullari[.]com
cevatpasa[.]com
pracenadoma[.]wz[.]cz
tehnik-unggul[.]com
philanthrope[.]in
www[.]katenilsson[.]dk
www[.]best-lab[.]org
ksaxl[.]com
www[.]akpartisariveliler[.]com
tn69abi[.]com
abb[.]ind[.]in
www[.]3pindia[.]in
1s2qvh91x[.]site[.]aplus[.]net
gim8[.]pl
acemoglusucuklari[.]com[.]tr
a-bring[.]com
aci[.]gratix[.]com[.]br
aclassalerts[.]com
elcisigur[.]ro

SHA-1:

adf205560e8bfde14378471ebee9342853781c50
d18dc8b64eaabb3047d503403f47f406ffe478b7
59bb3e745a5de05e821544522f5785d15cb65c00
a95455da6013caa421f9105b6b0aa9cc60b74cbb
29482261e903199483eba567bc082c5746526d46
97ce2e0e27397880966087225156f1bbf397c37b
7b6ef356c7fbead074c8b4643a42b3b7a5d46c8a
169492897a667322c3ffcabf96834244a4477ec8

de7347e63ebd9d060f98c96b3a2f80c52030022b
539af8bc5fb36e34ff4fe6869cdac998f1c9575d

SHA256:

02e195243af5923dae171d824b63a3d25a2538bc596a971273eb30b0a920b9e5
03232668bd0c47073066f155ac5577b0240fcff40eafac864adef86694006e43
03bc456b9c91607a9ace1f4d8121d28f51ea3177bc2198fc3a1d76aab20b3620
049d7d3d22c12f592379446b2ebb2cd2c894422379421afd4c77986a293760ed
06e4245cf5a76061587820f25a5d019663b63cca431e9bb43095d6c09b25a3ea
091eb9a5e513328d93d4e46884a210464ebbf3da71be68704bfd3bb00a842724
0a8bd011f75fc337eba89d7aa95f293999ca5aa086357abe96555266d952b883
0c0999de8b07c0e231326c88f991d068f6d56d9e85a2c386a09ccf2eb8be9ebf
0ec786687795fff9476658ca7b29a04949025cdb3fae672a6ae071520313f43c
109ec982b35185df989ef3558f704648ff4e4b9c307fba80d238dc546a5ff8d2
10c2740264a991ddd1bc1058975565eaa871803647805048c8132d169d34f5ca
11b75d4bb7cdc3938d884da59da1885e70b8bc995bbf528ffd1c02d5876214f8
13971272ef6b82c6b5ef9de3eb33f2dc439048c4eacd388faf2de37d89d25bb1
15b9de1e80e24edb459847e427edbee34734d9950db2c84f30175ba46eb5d208
168fce02cad1cfd3ac578f3ccfb023c6ea76f8c402ab160f0271863c66279af0
1692102392f7d3552307ae0b1e081b862650272d22a3823134cc9a2bfc6866c3
16e8fc998564cd4272795782a371fad13fca160f9427f85e0a8591d56c9a5248
1a93a65e01aecd981c300f7877d51c1b4907fccb4acced53c3e70bb7c1884e61
1c2479ad95ad5ec5944d10fc4222b0f7b9c40e4f3e940515c18773205a6129c8
1c7a9720df7186f3354799f5f7b17139e20d8c9233ef796c1f8a9a4a61a3eb73
1f747322ea42c2d20d19d3f0b9b2afe1f143910006163a6f08d27b97b2927ff7
2012be50bc465db1fee01bcd1183590e9d22a1fb3105efa1005f9da81adc7a5c
238f6f0376a19f92bfb2e616bac4da36f5eb922e2e93bba8bb61d0a0dfa18f18
252fe2be1234ed2028a28650daa61a2a5e90f40598c52b97226d67c8e701b97b
256fd9777738e64c2dc9279a398a24cc2382d95eb94d760d081fee71d8daa32b
007474f524c04bcfef7bff656f7d673e22496caff0490a111596b5c1a60b61ef
0abf15a831537bd86b7e16ae5032a4813c6e9e9df4f1da7c074c4daa3672c3dd
0e82ae0199228f54e8308755024fa78e0a568f1423cec3cf21d9341a7c99dcb9
18a859dee990feefdcc6196052c1d2becba64fb43d07623e1e573b0f39e63095
18bce4611a9668a2660b0471459cd070361c85d71a4989c1bc967fe04bc54795
2642e382a6a216b518471ac182891b6973a4f4eb569ad4d13cb02b8a840d3f07
5b4c4e796a0e1c9344c3165af210d2b9edd2980de25bfec656bc918809b0be4c
689bdd8a91c2bfaa00de235933b38ca9477ea9aa2eaa880cba50235641376add
865e10fa2439380d7048a0ec2eebdef487f706239e464c47dadf930b22028b11
905e701032eaaa944ccb70d3db97a200d85befefe7faf99d525c9767e5c5d615
a2ca43843f5c03adbdb03b91e4cafc162781d8c7e707c7bc161b03f4163218e2
ad68745733f455935188c0100aaf057bf1d3454a24e0be0ffff262d2318f6265
b535ea6cc31dd9f8a66fbbedb61ed021520ff74f5b42f815eb84022cfb3e4435
c38b955f4a4eee3cca1c1bf1ae0f915f75080772c4ae597c2ed76649a056a5dc

c40d8c58cc63dc606a9fa854f1774d7f17546170fdfc2679c3b8f6387fa4be6d
c5fb97f7e577795bdc7a6076efca8f09e83bd4fb9e68c40916c6784040dbb485
d0381f5c52b605b7b43c8b9dce2341b622ed2528df6bd65d527104f3fc1f2f16
da77ddf6e01c4cb2694f055a5c69f48bf6546b6831f145297a5cfbb5f64c5563
f001f25a35fb04298750c58f37ca4158085c454d784778f9a9c601d9bbbf6b40
f0d47851346c738dd836fb6f43005a57305f04e078d07af3a6d84ee586dfdfc0
0bcbac5dff686bb605adadb225fa540aab73bb3fb3251ba4226eb071cac6f0f1
0cdb71323cdf0ab4ec462f74b3830b87ae8d8212f6bfdb427ec12c06cc524220
14cbde97cb6d3df9841c8251884b664f689514d2ea8fa813fc95b323dd7ef8dd
3c419d67f98c8fd495eff616bb94d3e5de8c22d34b94124e1f3f0cfec8f3566d
3dac8250c89686244d433a9739bd59e719af950b60659d93e34b8b17cd72d0c4
7c544889d588ae668f13ff9e05eabc9ea048fa026b3a5af4882de10da8f8640c
7dc3fc8b4a572c0980b9de6ffc716fa422f627f48f8fcbc1720604e226346dff
919668829270d79de177615abf848bc09be41afd1877ef6682f8f0bbd3096880
b57206a74a8dbce03e991a5855c8c16aac2bffea69da9ebbc64c39932d886ec5
bd12db3c5dcc16b35cbb3cd42bbf9719ac8e69da6449c32659fc2a066d42265e
c85d9321a025a39c5b6facb12dd663b9623a4f43a73e2be409e9e3d04f132d4c
ea5e7e60a45331e504dcb30b29f6d9c7d438fb343aa2ae897047369b6863d712
f6efc4a323520ba88ccb8f678f3c9167010c6c575afcd8225393bc0f664fc96b
2eb74de9b3c016d03b96378e59557a6524918745c9c48df2a5a7ea5ca92d375a
513c36f4a21c7ebf125fe36b98fb2c065898b9f543a6e8dbbf3f9a041c5b86fa
33f8b063fa9eef4d6e83779a5f93c4ca9b8597c4e328ff0f789cbde0d72d24d0
4444e65841972ce81243575afa168ebbe54e7cc2db6aa34d996f53a6b2d99043
85e576aba88b0b3805d924e344feff58c27992d02675ba86126b88cb790afb7c
4ee41060b8f1c5679b10bebb8378f353ea62eb38ab27f041e3727dd8cb06b19d
f3dda8f48606c448d22a7b407f61757605acc028d3deddd0ad8c1e2742efcf86
cea7a79f688fe24df1c614bc6fdcb281c056f882307e2b9f7841dca56ae923f0
f66117bb7aff5ea3fb4241a5477edebc1f84844376b56b3c6ba6f5de7004d4c7
1e21f175cd66fe91b5ff770b1e74c61b2df04c13044388e36dfd3d0768c9e6e5
bdb1b6c2151038f1023b551d26ef4eab2d5321066d3352d5357b8bee301b67b0

Malware: QBot

QBot

Qbot, also known as Qakbot, Pinkslipbot is a network-aware worm with backdoor capabilities, primarily designed as a credential harvester. It can download and execute files, delete itself, replicate itself across network, terminate processes in OS. All stolen data will be collected and sent to FTP servers. QBot, (aka Qakbot, Quakbot) is a banking trojan first identified in 2009 as a network-aware worm with backdoor capabilities, primarily designed as a credential harvester. It is an old threat and was well-described by Symantec back in 2009. In December 2015, several researchers reported that websites hosting the Rig Exploit Kit were serving an updated version of QBot. Then in January 2016, over 500 devices at a large public organization were infected with QBot. It was the second encounter of QBot trojan. After infecting system, QBot injected into explorer.exe and browser processes. It steals cookie files, active Internet sessions, redirects users to fake pages, injects code in visited web pages, installs keylogger, steals certificates, collects passwords and logins used by user in various programs. It can download and execute files, delete itself, replicate itself across network, terminate processes in OS. All stolen data will be collected and sent to FTP servers.

Platform: Windows

Threat level: High

Category: Banking Trojan

Indicators of Compromise (IOCs)

CnC:

35[.]220[.]219[.]62
86[.]99[.]134[.]235
47[.]22[.]148[.]6
157[.]131[.]108[.]180
24[.]117[.]107[.]120
75[.]136[.]40[.]155
24[.]179[.]13[.]119
75[.]118[.]1[.]141
5[.]2[.]212[.]254
184[.]185[.]103[.]157
2[.]50[.]161[.]6
197[.]82[.]221[.]232
74[.]195[.]119[.]4
195[.]12[.]154[.]8
149[.]28[.]98[.]196
83[.]110[.]12[.]140
193[.]248[.]221[.]184
74[.]68[.]144[.]202

213[.]60[.]147[.]140
108[.]160[.]123[.]244
118[.]168[.]236[.]169
105[.]198[.]236[.]101
31[.]5[.]174[.]173
190[.]85[.]91[.]152
72[.]252[.]201[.]69
37[.]104[.]38[.]219
70[.]49[.]88[.]199
47[.]146[.]34[.]236
86[.]121[.]43[.]200
71[.]88[.]193[.]17
144[.]202[.]38[.]185
185[.]18[.]54[.]134
31[.]184[.]193[.]142
80[.]66[.]83[.]166
5[.]101[.]0[.]245
185[.]103[.]110[.]172
185[.]66[.]9[.]143
185[.]186[.]141[.]140
194[.]146[.]43[.]165
185[.]129[.]49[.]19
23[.]81[.]246[.]35
46[.]30[.]42[.]185
31[.]184[.]192[.]39
31[.]184[.]193[.]17
78[.]63[.]226[.]32
189[.]210[.]115[.]207
81[.]88[.]254[.]62
83[.]110[.]103[.]152
71[.]163[.]222[.]223
160[.]120[.]7[.]166
203[.]198[.]96[.]249
209[.]210[.]187[.]52
2[.]50[.]56[.]81
200[.]44[.]237[.]189
68[.]186[.]192[.]69
98[.]192[.]185[.]86
71[.]117[.]132[.]169
187[.]190[.]250[.]175
149[.]28[.]99[.]97
95[.]77[.]223[.]148
123[.]201[.]198[.]69

106[.]51[.]85[.]162
109[.]236[.]80[.]55
146[.]185[.]215[.]18
195[.]19[.]192[.]49
46[.]4[.]98[.]91
45[.]143[.]138[.]72
91[.]230[.]60[.]116
185[.]48[.]57[.]117
79[.]142[.]22[.]133
190[.]85[.]91[.]153
172[.]78[.]30[.]215
142[.]129[.]227[.]86
24[.]216[.]56[.]6
190[.]85[.]91[.]159
50[.]244[.]112[.]106
83[.]110[.]108[.]226
190[.]85[.]91[.]158
83[.]110[.]96[.]71
73[.]25[.]124[.]140
155[.]186[.]9[.]160
172[.]78[.]47[.]100
58[.]152[.]9[.]133
186[.]144[.]33[.]73
73[.]153[.]211[.]227
71[.]163[.]223[.]159
190[.]85[.]91[.]156
103[.]80[.]198[.]235
174[.]104[.]31[.]209
90[.]61[.]41[.]220
161[.]199[.]180[.]159
74[.]128[.]121[.]17
24[.]139[.]72[.]117
96[.]57[.]188[.]174
105[.]225[.]169[.]45
98[.]116[.]21[.]115
86[.]175[.]79[.]249
207[.]246[.]116[.]237
190[.]85[.]91[.]157
67[.]6[.]12[.]4
95[.]76[.]27[.]6
84[.]38[.]130[.]75
45[.]128[.]151[.]15
95[.]213[.]144[.]203

77[.]222[.]52[.]183
31[.]184[.]192[.]66
31[.]184[.]199[.]11
46[.]4[.]98[.]69
120[.]150[.]218[.]241
190[.]85[.]91[.]154
160[.]3[.]184[.]253
186[.]144[.]33[.]74
149[.]28[.]101[.]90
68[.]9[.]238[.]144
83[.]194[.]193[.]247
96[.]253[.]46[.]210
37[.]104[.]40[.]29
45[.]63[.]107[.]192
197[.]51[.]82[.]72
90[.]201[.]21[.]58
86[.]160[.]137[.]132
108[.]46[.]145[.]30
90[.]65[.]234[.]26
186[.]144[.]33[.]75
45[.]32[.]211[.]207
199[.]19[.]117[.]131
175[.]141[.]219[.]71
105[.]198[.]236[.]99
151[.]61[.]125[.]180
96[.]227[.]127[.]13
216[.]201[.]162[.]158
90[.]61[.]30[.]155
176[.]181[.]247[.]197
67[.]141[.]11[.]98
90[.]65[.]236[.]181
71[.]187[.]170[.]235
213[.]122[.]113[.]120
173[.]21[.]10[.]71
75[.]67[.]192[.]125
106[.]51[.]52[.]111
31[.]184[.]193[.]71
95[.]217[.]51[.]27
176[.]9[.]19[.]209
77[.]222[.]63[.]66
98[.]252[.]118[.]134
45[.]46[.]53[.]140
45[.]77[.]117[.]108

136[.]232[.]34[.]70
84[.]72[.]35[.]226
45[.]77[.]115[.]208
72[.]196[.]112[.]234
186[.]144[.]33[.]72
70[.]126[.]76[.]75
101[.]178[.]240[.]121
190[.]85[.]91[.]155
184[.]179[.]14[.]130
108[.]190[.]194[.]146
86[.]220[.]60[.]133
74[.]195[.]52[.]3
207[.]246[.]77[.]75
24[.]206[.]4[.]203
74[.]124[.]191[.]6
81[.]214[.]126[.]173
24[.]138[.]75[.]11
196[.]204[.]207[.]111
24[.]179[.]77[.]236
24[.]50[.]118[.]93
191[.]115[.]58[.]225
187[.]145[.]108[.]84
97[.]69[.]160[.]4
115[.]133[.]243[.]6
73[.]90[.]4[.]146
77[.]246[.]144[.]199
95[.]215[.]0[.]211
185[.]238[.]136[.]67
188[.]227[.]18[.]135
5[.]101[.]0[.]243

SHA256:

43abd76bebb7b2f1f1f3a11f07bb4777112aa457e27352f41a5b38a3d92ee13d
f88259c15e949773f1dfd392bcdc85274ab864744c1d9af2db5fba8cc0873ffd
81d0d5e135bedad3e95419c618871ee0a81f75b630f2d63c37e9b519998a7a7b
c4182ff4e0a245d2d665746606ac503217fdf6bb8db3628ee54f25331d605a3a
786694b1c6db525fb700a637f60ef854cfd76b98bed007834bf32beda623f102
29eacda0c6ea2660180e38df7d5f6594af73cbcf4d421d4bdd9cde1ab9275091
2965817e747cf5c74ec45d56735e64b841ba3393eef655f05fa11eb4a6636a7d
c69c328a1bafb8742b52327581af2635425e3c3ae639bbd02235c6b57159b45e
50c9401ac4fc49e14a298cf3645254884839cd3f2c13dd6502f09380b42b34db
a7c77b78afaabc7c06cb94684d72b49d3788b31a6e52c9f9a426f20e944c402c
d0de45a8b2fccf9e4e8a499519ba63e782c0b969823744be715663cd0bed74aa

a1667e9fea440141e72230f59b2d777be55dc445dfd9efce8347d647c4826329
a27c962eb6d9d7266cafd034e3846bbf2b7b90e04741154d2fe6d0ffec1f1540
bd26e07faf719c52b5619aaf634d88e5b72c765f166281d097e69640076bec61
2a57c1c324a169ac5e46196fbe19f2acff36c7e7490ec50621bdf4546e69bd3e
f51375a6e8b8242d00b7e057a3676cc9b3d61e9ab99edd4412bf19954e8e1542
378a852088474a9f6dee4eb97596e13a65ecc13d3595e2f7e228c950e4979d75
090e5de1e9e4dfde1524e351671acf0736d53b1737fafa324d4ac06cf2271f78
fd380f2e3f14f2665799b589f98cc557c9133116fd1731216815048fd4cb5912
162c07d956589b96ebb4c8c32ce50770e352a3c58613119c2954441d5ff10e31
10c27496c0a93b36c11aeea73b96dfb0220ee146afc45ed5041c6421b202f30f
6eedf6fa0d8b059e6ac541879d22e228f9218531a5dd2c73f79e226a9eaae643
3048ef7afa5e482ea0b63a241e5a16648c9a13733a6cdcbd621b38da3adf672f
8f475f3699ee5798f0364a39da6cb668aa89dd20879e41d4a394e1b66ed9f09a
7ca94f5975a02a4dc3cfe92b40e266a2a3f38639ff71e20e09e8d0343b6a5ecb
dc71cac28c729094c960230e065274fc2824cb445cb607e7b16f80081466c819
ff55279d5ef18ff4efb6cd662a7f94f4a5498ccaa2db27df946b6118a32a7c84
3214370beb6db0b1fd64c0dc3d00123f643f24463886022644247acd62d699cc
7d440094049ce035e1d9adace07691f1245ce13cc8346c13cab72f1e60cdf362
b72df5535e69fb7ea6dd6638059825c267e176baa3213a2f513d76d2455f1776
35d7b61350a2b95565a9f99c0fff4557020bbef16836a39aee6943589a9abbb9
22ef96dae6ee23654271babdccc913813e2f87dcf1bcade1c1cd0decc2f410dc
3a3cd95e61220a0f3b3a56bfc27f1bdb3bc1549e5bb80dd429a47ef6b653b2c2
21d54c69ac6bc5d653de85be3708be83242b3a74d6911e41b2fe041153ae193d
8c24dccd50347dedd38a30a87546476011e9e9c356b532cc776eded2a3c0a692
9115c5e1a4bc56983087d03c99784efbe472e81c977aaf63bebf6bbbc92c81e5
d79f644dfac8314842ef9a5245acc0a2e4947562a39b59b555c9fc9cecf91ce4
f7b1822cf7688515499b9ad4af685fc9569263236889460c9389e333b5fca5be
bab9f57bb72836ada4d3916e13db737e1c278bb006d98a96c5931281d7fdf517
9e913189f3c40230f2316dfb877a6ba90121b757e7881fe1206a4730b8e7f080
aaf5ebbe55d9262af4ea49fe8e2b9cc217c55895af6a6af035382c3fdfa98449
9c4fb8e563206a63060fd8dc31562f791bee6f40577b977a4eb52f6b87114676
32e3a352a20b5ccd0d3ff6d2cee0c766539cce60db1772a71e1239d222f4f7c7
a586179060cd43021c19930dbce6e87f22cc536825c5b9ea101416d9d3b07d69
6e30f89b5106ff9b64a223b51cd013ea6f0f7c5b9224386ac1ceccc63a35ee1a
b9535d852f6fcf52b88c004b006c7e34d4a7b40253059d635b9d55a071120a00
faa0f29ca83b538f9421d5709634abe2ae4ab0ba6af7afbcace0cd8cb6aa9a48
102e21615dab576f9c78a424061bf6feea7386bf4db149aa13cf7e3400f6728f
e3981285a7c975a192f8aa7eaf81d9e1884e74f39edfaf6a62531125a3dfe987
fdaece60ea8934e53df027df1f15ac56c3b292640d90796898170b89cc23c118
fe2cf705ddad7ab655bbdb850b6c5e87beb7f0be195fcc260bc4b78aa6de7ab9
65d9ab81778b2a753b0849f5cf1e64afc9ae98960c3db3ce874d693fd48fc5a4
a192aadf11ae8faa8fdbf7dd51291ef1f649b92b3c34a513bc6dfc22c0be9609
d662e1437b260b62d92d1193dff2a074daa80182da58bcd186ebe123dc337fab

13ccba322ba077707a60ff96f9430d7b3ac18de9afd62963f59679ebea6cb3c1
a8a458bd3c56908d78e799cb67ea681ced7057de4fd528a2887d29d6cf5ae5a3
49a7a0d67f700f5e59894f0cdf767a30a6ad768c360b729f92b12395c5a9a272
e8964e0ec21ee18ac43cd69b85f63103f1a691fa339a838748fb282380f31b51
b2cc5d29e19bad075a623cfed3aaa5d1215f9e4a0fe298921fe2e33d6c62df54
cc174bff3df014a379af4388dd57e7db845aa3f0fd09ca2b609ac345a9c25807
2e9cfd3e57f330cd6dd5d9705c8858ad5594a950b21201376c9385ad8295c69c
8b848e8e4e1e2440e91c87db130b1eb9611fa8ae0c4835f536c864472de2ca3f
4da8564def807d49cf9d45fcad3e9201344732a49aea4261ab05b8b43cb3adae
8fe5b6ec872d0c6db4e2ea14d8936c1b375ed08ffb0f2354d7a3f62214ef9650
a80e53b188293efae169cb567ef5ab81d135f35102c657fdade76d60b75b37bd

Network signatures

TROJAN Win32/Qbot CnC Activity

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot CnC Activity"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"/t4"; http_uri; isdataat:!1,relative; content:"Mozilla/5.0 (Windows NT 6.1|3b 20|WOW64|3b 20|Trident/7.0|3b 20|rv|3a|11.0) like Gecko"; http_user_agent; depth:68; isdataat:!1,relative; pcre:"/^[A-Za-z0-9]{3,20}=(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4})$/Psi"; http_start; content:"POST|20|/t4|20|HTTP/1.1"; depth:17; fast_pattern; http_header_names; content:!"Referer"; reference:md5,a74309ba974690c806ec5bc24869a549; classtype:trojan-activity; sid:2838496; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_09_18, deployment Perimeter, deployment SSLDecrypt, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_12_01, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN VBS/Qbot.Downloader Requesting Payload

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN VBS/Qbot.Downloader Requesting Payload"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:".png?bg="; http_uri; fast_pattern; content:"?os="; http_uri; distance:0; content:"&av="; http_uri; distance:0; content:"Microsoft BITS/"; http_user_agent; depth:15; content:"Range|3a 20|bytes="; http_header; http_accept_enc; content:"identity"; http_header_names; content:"If-Unmodified-Since"; content:!"Referer"; content:!"Cache"; threshold:type limit, count 1, seconds 30, track by_src; classtype:trojan-activity; sid:2833619; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_11_23, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, tag Downloader, tag VBS, updated_at 2020_08_27, severity 3, ti_malware_id

e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN Win32/Qbot/Quakbot Checkin via HTTP GET

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot/Quakbot Checkin via HTTP GET"; target:src_ip; flow:established,to_server; content:"GET"; http_method; pcre:"/^\/[a-zA-Z0-9]*(?=[A-Z])[a-zA-Z0-9]*\.php$/U"; pcre:"/(?:\x20MSIE\x20|rv\x3a11)/V"; pcre:"/(?:Cache-Control|Pragma)\x3a[^\r\n]+\r\n(?:\r\n)?$/H"; http_start; content:".php|20|HTTP/1.1|0d 0a|User-"; fast_pattern; http_header_names; content:"|0d 0a|User-Agent|0d 0a|Host|0d 0a|"; depth:20; content:!"Referer|0d 0a|"; content:!"Accept"; classtype:trojan-activity; sid:2815364; rev:4; metadata:created_at 2015_12_15, former_category MALWARE, updated_at 2020_04_06, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN PSW.Win32.Qbot.aem Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN PSW.Win32.Qbot.aem Checkin"; target:src_ip; flow:to_server,established; content:"GET"; http_method; nocase; content:"jloader.pl?is="; http_uri; nocase; content:"&ec1="; http_uri; nocase; content:"&ec2="; http_uri; nocase; content:"&it="; http_uri; nocase; content:"&b="; http_uri; nocase; content:"&vt="; http_uri; nocase; content:"&n="; http_uri; nocase; reference:url,www.threatexpert.com/reports.aspx?find=Trojan-PSW.Win32.Qbot.&x=0&y=0; classtype:banking-trojan; sid:2802932; rev:2; metadata:created_at 2011_06_06, former_category MALWARE, updated_at 2011_06_06, severity 5, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

IP address related to malware_qbot_c2_server_1

alert tcp any any <> 184.185.103.157 any (msg:"IP address related to malware_qbot_c2_server_1"; target:src_ip; flags:A; classtype:test; sid:1671681; rev:1; threshold:type limit, track by_src, seconds 30, count 1; metadata:credibility 100, malware_family malware_qbot_c2_server_1, reliability 95, rule_origin ti_panda, ti_threatactor_id 4562361a22a49bec6e4eb5c16de6aefb0809d7f0, ti_threatactor_name QBot-Group, severity 1, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot;)

IP address related to malware_qbot_c2_server_1

alert tcp any any <> 72.252.201.69 any (msg:"IP address related to malware_qbot_c2_server_1"; target:src_ip; flags:A; classtype:test; sid:1673181; rev:1; threshold:type limit, track by_src, seconds 30, count 1; metadata:credibility 100, malware_family malware_qbot_c2_server_1, reliability 95, rule_origin ti_panda,

ti_threatactor_id 4562361a22a49bec6e4eb5c16de6aefb0809d7f0, ti_threatactor_name QBot-Group, severity 1, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot;)

TROJAN Possible Win32/Qbot/Quakbot Checkin via HTTP GET

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Possible Win32/Qbot/Quakbot Checkin via HTTP GET"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:".png?uid="; http_uri; fast_pattern; pcre:"/\/\d+\.png\?uid=(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4})+$/U"; content:!"Mozilla"; http_user_agent; http_header_names; content:"|0d 0a|Connection|0d 0a|Accept|0d 0a|Accept-Language|0d 0a|User-Agent|0d 0a|Host|0d 0a 0d 0a|"; depth:59; isdataat:!1,relative; classtype:trojan-activity; sid:2030157; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_05_12, deployment Perimeter, signature_severity Major, updated_at 2020_05_12, severity 3, rule_origin etpro;)

IP address related to malware_qbot_c2_server_1

alert tcp any any <> 71.163.222.223 any (msg:"IP address related to malware_qbot_c2_server_1"; target:src_ip; flags:A; classtype:test; sid:1681705; rev:1; threshold:type limit, track by_src, seconds 30, count 1; metadata:credibility 100, malware_family malware_qbot_c2_server_1, reliability 95, rule_origin ti_panda, ti_threatactor_id 4562361a22a49bec6e4eb5c16de6aefb0809d7f0, ti_threatactor_name QBot-Group, severity 1, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot;)

IP address related to malware_qbot_c2_server_1

alert tcp any any <> 213.122.113.120 any (msg:"IP address related to malware_qbot_c2_server_1"; target:src_ip; flags:A; classtype:test; sid:1682633; rev:1; threshold:type limit, track by_src, seconds 30, count 1; metadata:credibility 100, malware_family malware_qbot_c2_server_1, reliability 95, rule_origin ti_panda, ti_threatactor_id 4562361a22a49bec6e4eb5c16de6aefb0809d7f0, ti_threatactor_name QBot-Group, severity 1, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0e|giviklorted.at"; distance:1; within:15; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022537; rev:2; metadata:attack_target Client_Endpoint, created_at 2016_02_17, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0b|marinova.am"; distance:1; within:12; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022623; rev:2; metadata:attack_target Client_Endpoint, created_at 2016_03_16, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN Qbot Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Qbot Checkin"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"n="; depth:2; http_client_body; content:"&m="; distance:0; http_client_body; content:"&v="; distance:0; http_client_body; content:"&g="; http_client_body; fast_pattern; content:!"Referer|3a|"; http_header; pcre:"/\.php$/U"; reference:md5,39c4c3a64f266dc0b2e49c4deb41a541; classtype:banking-trojan; sid:2809522; rev:3; metadata:created_at 2015_01_15, former_category MALWARE, updated_at 2020_09_29, severity 5, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

IP address related to malware_qbot_c2_server_1

alert tcp any any <> 45.63.107.192 any (msg:"IP address related to malware_qbot_c2_server_1"; target:src_ip; flags:A; classtype:test; sid:1663538; rev:1; threshold:type limit, track by_src, seconds 30, count 1; metadata:credibility 100, malware_family malware_qbot_c2_server_1, reliability 95, rule_origin ti_panda, ti_threatactor_id 4562361a22a49bec6e4eb5c16de6aefb0809d7f0, ti_threatactor_name QBot-Group, severity 1, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot;)

IP address related to malware_qbot_c2_server_1

alert tcp any any <> 189.210.115.207 any (msg:"IP address related to malware_qbot_c2_server_1"; target:src_ip; flags:A; classtype:test; sid:1663715; rev:1; threshold:type limit, track by_src, seconds 30, count 1; metadata:credibility 100, malware_family malware_qbot_c2_server_1, reliability 95, rule_origin ti_panda, ti_threatactor_id 4562361a22a49bec6e4eb5c16de6aefb0809d7f0, ti_threatactor_name QBot-Group, severity 1, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot;)

TROJAN Win32/Qbot/Quakbot Downloader - Requesting Secondary Download

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot/Quakbot Downloader - Requesting Secondary Download"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:"|3f|uid|3d|"; http_uri;

content:"WebGL3D"; http_user_agent; depth:7; isdataat:!1,relative; fast_pattern; classtype:trojan-activity; sid:2029551; rev:2; metadata:affected_product Windows_Client_Apps, attack_target Client_Endpoint, created_at 2020_02_28, deployment Perimeter, former_category MALWARE, malware_family Qbot, signature_severity Major, updated_at 2020_02_28, severity 3, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|09 00|"; content:"|55 04 06|"; distance:0; content:"|02|US"; distance:1; within:3; content:"|55 04 08|"; distance:0; content:"|02|NY"; distance:1; within:3; content:"|55 04 07|"; distance:0; content:"|02|NY"; distance:1; within:3; fast_pattern; content:"|55 04 03|"; distance:0; content:"|2a 86 48 86 f7 0d 01 09 01|"; distance:0; content:"admin@"; distance:2; within:6; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022534; rev:2; metadata:attack_target Client_Endpoint, created_at 2016_02_17, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|55 04 0b|"; content:"|16|SomeOrganizationalUnit"; distance:1; within:23; content:"|2a 86 48 86 f7 0d 01 09 01|"; distance:0; content:"|0c|root@ua7.com"; distance:1; within:13; fast_pattern; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022795; rev:2; metadata:attack_target Client_Endpoint, created_at 2016_05_05, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|55 04 06|"; pcre:"/^.\x02[A-Z]{2}/Rs"; content:"|55 04 08|"; distance:0; pcre:"/^.\x02[A-Z]{2}/Rs"; content:"|55 04 07|"; distance:0; pcre:"/^.{2}[A-Z][a-z]+(?:\x20[A-Z][a-z]+)?[01]/Rs"; content:"|55 04 09|"; fast_pattern; distance:0; pcre:"/^.{2}\d{2,3}(?:\x20[A-Z][a-z]+\.?){1,3}[01]/Rs"; content:!"|2a 86 48 86 f7 0d 01 09 01|"; distance:0; content:"|55 04 0a|"; distance:0; content:"|55 04 0b|"; distance:0; content:"|55 04 03|"; distance:0; pcre:"/^.(.[a-z]{4,12}\.(?:us|org|net|biz|info|mobi|com)[01]).*?\x55\x04\x03.\1/Rs"; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022868; rev:4; metadata:attack_target Client_Endpoint, created_at 2016_06_06, deployment

Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|04 26 98 61 57|"; fast_pattern; content:"|55 04 03|"; distance:0; content:"|25|ASA Temporary Self Signed Certificate"; distance:1; within:38; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2023013; rev:2; metadata:attack_target Client_Endpoint, created_at 2016_08_02, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_08_02, severity 3, rule_origin etpro;)

TROJAN Win32/Qbot CnC Activity M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot CnC Activity M2"; target:src_ip; flow:established,to_server; pcre:"/^[A-Za-z0-9]{3,20}=(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4})$/Psi"; http_header_names; content:!"Referer"; http_request_line; content:"POST|20|/t4|20|HTTP/1.1"; depth:17; fast_pattern; isdataat:!1,relative; http_accept; content:"application/x-shockwave-flash, image/gif, image/jpeg, image/pjpeg, */*"; depth:70; isdataat:!1,relative; reference:md5,3ceb36fc3607df3d67d9eb0f1d00fea0; classtype:trojan-activity; sid:2845945; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_12_09, deployment Perimeter, deployment SSLDecrypt, former_category MALWARE, malware_family Qbot, performance_impact Low, signature_severity Major, updated_at 2020_12_09, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, rule_origin etpro;)

TROJAN Observed Qbot Style SSL Certificate

alert tls $EXTERNAL_NET ![443,587] -> $HOME_NET any (msg:"TROJAN Observed Qbot Style SSL Certificate"; target:dest_ip; flow:established,from_server; tls_cert_issuer; content:"C="; depth:2; content:",|20|ST="; distance:2; within:5; content:",|20|L="; distance:2; within:4; content:",|20|O="; distance:0; within:20; content:",|20|CN="; distance:0; within:50; pcre:"/^C=(?:M[ACDEGHKLMNOPQRSTUVWXYZ]|G[ABDEFGHILMNPQRSTUWY]|B[ABDEFGHIJMNORSTVWZ]|A[DEFGILMNOQRSTUWXZ]|S[ABCEGHIJKLMNRTUVZ]|C[ACFHIKLMNORSVXYZ]|T[CDFGHJKMNOPRTVWZ]|P[AEFGHKLMNRSTWY]|N[ACEFGILOPRTUZ]|K[EGHIMNRWYZ]|L[ACIKSTUVY]|I[DELMNOST]|E[CEGHRST]|F[IJKMORX]|U[AGKMSYZ]|V[ACEGINU]|D[EJKMOZ]|H[KMNRTU]|R[EOSUW]|J[EMOP]|W[FS]|Y[ET]|Z[AM]|OM|QA),\sST=(?!(?:M[ADEINOST]|N[CDEHJMVY]|A[KLRZ]|I[ADLN]|W[AIVY]|C[AOT]|O[HKR]|[GLP]A|K[SY]|S[CD]|T[NX]|V[AT]|[HR]I|DE|FL|UT))[A-Z]{2},\sL=[A-Z][a-z]{2,15}(?:\s[A-Z][a-

z]{2,10})?,\sO=[A-Z][a-z]{2,25}\s[A-Z][a-z]{2,25}(?:\s[A-Z][a-z]{2,25})?(?:\s[A-Z][a-z]{2,25})?(?:\s(?:Inc|LLC)\.)?,\sCN=[a-z]{4,11}\.[a-z]{2,4}$/"; classtype:trojan-activity; sid:2834895; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_02_15, deployment Perimeter, former_category TROJAN, performance_impact Significant, signature_severity Major, updated_at 2021_04_20, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|09 00|"; content:"|55 04 06|"; distance:0; content:"|02|US"; distance:1; within:3; content:"|55 04 08|"; distance:0; content:"|02|NY"; distance:1; within:3; content:"|55 04 07|"; distance:0; content:"|08|New York"; distance:1; within:9; fast_pattern; content:"|55 04 03|"; byte_test:1,>,27,1,relative; byte_test:1,<,30,1,relative; pcre:"/^.{2}[a-z]{25}\.[a-z]{2,3}[01]/Rs"; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022488; rev:3; metadata:attack_target Client_Endpoint, created_at 2016_02_04, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|55 04 08|"; content:"|02|FL"; distance:1; within:3; content:"|55 04 07|"; distance:0; content:"|05|Tampa"; distance:1; within:6; content:"|55 04 0a|"; distance:0; content:"|1b|Realtek Semiconductor Corp."; distance:1; within:28; fast_pattern; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022714; rev:3; metadata:attack_target Client_Endpoint, created_at 2016_04_07, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN Win32/Qbot CnC

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot CnC"; target:src_ip; flow:established,to_server; dsize:<600; content:"|01 06 00 00 00 00 04 02 00 00|"; depth:10; fast_pattern; pcre:"/^[a-z]{6}\d{6}/R"; content:"|2e|"; distance:20; within:4; pcre:"/^(?:\d{1,3}\.){2}\d{1,3}\x00/R"; reference:md5,b06de4f40b501bba57903f2b4dcc585a; classtype:trojan-activity; sid:2815159; rev:1; metadata:created_at 2015_12_01, former_category MALWARE, updated_at 2015_12_01, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN Win32/Qbot Variant Exfil via FTP

alert tcp $HOME_NET any -> $EXTERNAL_NET [21,2100,3535] (msg:"TROJAN Win32/Qbot Variant Exfil via FTP"; target:src_ip; flow:established,to_server; content:"STOR artic"; fast_pattern; content:"e_"; distance:1; within:2; pcre:"/^[a-z]{6}\d{6}_1[45]\d{8}\.zip\r?\n/R"; reference:md5,fe318c2828c47e37b095731685e3b999; classtype:trojan-activity; sid:2814194; rev:7; metadata:created_at 2015_10_01, former_category TROJAN, updated_at 2018_05_11, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN Possible Qbot SSL Cert

alert tls $EXTERNAL_NET [995,2222] -> $HOME_NET any (msg:"TROJAN Possible Qbot SSL Cert"; target:dest_ip; flow:established,to_client; tls_cert_subject; content:"C="; depth:2; content:", OU="; distance:2; within:5; fast_pattern; content:", CN="; distance:0; pcre:"/^C=[A-Z]{2},\sOU=[A-Z][a-z]+(?:\s[A-Z][a-z]+)*,\sCN=[a-z]+\.[a-z]+$/"; tls_cert_issuer; content:"C="; depth:2; content:", ST="; distance:2; within:5; content:", L="; distance:2; within:4; content:", O="; distance:0; content:", CN="; distance:0; pcre:"/^C=[A-Z]{2},\sST=(?!(A[KLRZ]|C[AOT]|D[CE]|FL|GA|HI|I[ADLN]|K[SY]|LA|M[ADEINOST]|N[CDEHJMVY]|O[HKR]|P[AR]|RI|S[CD]|T[NX]|UT|V[AIT]|W[AIVY]))[A-Z]{2},\sL=[A-Z][a-z]+(?:\s[A-Z][a-z]+)*,\sO=[A-Z][a-z]+(?:\s[A-Z][a-zA-Z]+.?)*,\sCN=[a-z]+\.[a-z]+$/"; classtype:trojan-activity; sid:2830811; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_05_11, deployment Perimeter, former_category MALWARE, signature_severity Major, tag Qbot, updated_at 2020_08_25, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN Observed Malicious SSL Cert (Qbot CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Observed Malicious SSL Cert (Qbot CnC)"; target:dest_ip; flow:established,to_client; tls_cert_serial; content:"22:0A"; tls_cert_subject; content:"CN=ahbezwkftrm.net"; nocase; isdataat:!1,relative; reference:md5,79c1e7151c5f2e30a7908261aca331cf; classtype:trojan-activity; sid:2833402; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_11_01, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_09_16, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|09 00 e4 52 b4 b2 9e 40 bd 86|"; fast_pattern; content:"|55 04 0a|"; distance:0; content:"|0d|Synology Inc."; distance:1; within:14; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2023268; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_09_22, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_09_22, severity 3, rule_origin etpro;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Quakbot CnC)"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|15|whaovxeynxctdrvzn.com"; distance:1; within:22; reference:url,sslbl.abuse.ch; classtype:trojan-activity; sid:2022685; rev:2; metadata:attack_target Client_Endpoint, created_at 2016_03_30, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_07_01, severity 3, rule_origin etpro;)

TROJAN Win32/Qbot CnC Activity M3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot CnC Activity M3"; target:src_ip; flow:established,to_server; pcre:"/^[A-Za-z0-9]{3,20}=(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4})$/Psi"; http_header_names; content:!"Referer"; http_request_line; content:"POST|20|/t3|20|HTTP/1.1"; depth:17; fast_pattern; isdataat:!1,relative; http_accept; content:"application/x-shockwave-flash, image/gif, image/jpeg, image/pjpeg, */*"; depth:70; isdataat:!1,relative; reference:md5,3ceb36fc3607df3d67d9eb0f1d00fea0; classtype:trojan-activity; sid:2845946; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_12_09, deployment Perimeter, deployment SSLDecrypt, former_category MALWARE, malware_family Qbot, performance_impact Low, signature_severity Major, updated_at 2020_12_09, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, rule_origin etpro;)

TROJAN VBS/Qbot.Downloader CnC Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN VBS/Qbot.Downloader CnC Checkin"; target:src_ip; flow:established,to_server; content:"HEAD"; http_method; content:".png?bg="; http_uri; fast_pattern; content:"os="; http_uri; distance:0; content:"&av="; http_uri; distance:0; content:"Microsoft BITS/"; http_user_agent; depth:15; http_accept_enc;

content:"identity"; http_header_names; content:!"Referer"; content:!"Cache"; classtype:trojan-activity; sid:2833618; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_11_23, deployment Perimeter, former_category MALWARE, performance_impact Low, signature_severity Major, tag Downloader, tag VBS, updated_at 2020_08_28, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN Win32/Qbot/Quakbot Checkin via HTTP POST

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot/Quakbot Checkin via HTTP POST"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"Accept|3a 20|*/*|0d 0a|Content"; http_header; fast_pattern; content:!"Referer|3a|"; http_header; pcre:"/^[a-z]{5,15}=[a-zA-Z0-9/+=]{100,}$/P"; pcre:"/^\/[a-zA-Z0-9]{20,}\.php$/U"; classtype:trojan-activity; sid:2815363; rev:4; metadata:created_at 2015_12_15, former_category MALWARE, updated_at 2020_10_05, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

TROJAN Win32/Qbot/Quakbot Checkin via HTTP POST

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/Qbot/Quakbot Checkin via HTTP POST"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"Accept|3a 20|*/*|0d 0a|Content"; http_header; fast_pattern; content:!"Referer|3a|"; http_header; pcre:"/^[a-z]{5,15}=[a-zA-Z0-9/+=]{100,}$/P"; pcre:"/^\/[a-zA-Z0-9]{20,}\.php$/U"; classtype:trojan-activity; sid:2815363; rev:4; metadata:created_at 2015_12_15, former_category MALWARE, updated_at 2020_10_05, severity 3, ti_malware_id e323de16fc8162e02aad6683b0f48a0e4008cbae, ti_malware_name QBot, malware_family QBot, rule_origin etpro;)

Malware: Sombra or SombRAT

Sombra or SombRAT

SombRAT is a backdoor discovered in 2020. It communicates with a C&C server via multiple protocols, including DNS, TLS-encrypted TCP, and potentially WebSockets. Although the backdoor supports dozens of commands, most of them enable the operator to manipulate an encrypted storage file and reconfigure the implant. The backdoor's primary purpose is to download and execute plugins provided via payload.

Platform: Windows

Threat level: High

Category: Backdoor

Indicators of Compromise (IOCs)

CnC:

Celomito[.]com
Feticost[.]com
Cosarm[.]com
Portalcos[.]com
sbibd[.]net
infosportals[.]com
akams[.]in
newspointview[.]com
159[.]65[.]31[.]84
212[.]83[.]61[.]227
144[.]217[.]53[.]146
45[.]89[.]175[.]206
bd1540dda[.]celomito[.]com
5dc5a95caaaad5ce6ef4[.]celomito[.]com
b27543ffd5a3949c5d483e2b4705[.]celomito[.]com
^b[a-zA-Z0-9]{3,64}\[.](celomito|feticost)\[.]com
51[.]89[.]50[.]152
57[.]219[.]0[.]1
19[.]134[.]94[.]227
88[.]105[.]224[.]32
180[.]222[.]29[.]199
119[.]39[.]152[.]157
109[.]124[.]209[.]212
119[.]170[.]44[.]215
226[.]31[.]10[.]29
156[.]77[.]252[.]190
135[.]78[.]65[.]199

30[.]24[.]7[.]206
229[.]222[.]231[.]39
22[.]58[.]50[.]80
218[.]10[.]128[.]138
245[.]179[.]63[.]52
98[.]160[.]54[.]99
200[.]72[.]40[.]81
229[.]228[.]106[.]12
71[.]61[.]21[.]41
79[.]93[.]190[.]81
64[.]227[.]24[.]12
157[.]230[.]184[.]142

MD5:

87c78d62fd35bb25e34abb8f4caace4a
6382d48fae675084d30ccb69b4664cbb
cf1b9284d239928cce1839ea8919a7af
4aa3eab3f657498f52757dc46b8d1f11
1f6495ea7606a15daa79be93070159a8
31dcd09eb9fa2050aadc0e6ca05957bf
edf567bd19d09b0bab4a8d068af15572
a5b26931a1519e9ceda04b4c997bb01f
f0751bef4804fadfe2b993bf25791c49

SHA256:

130fa726df5a58e9334cc28dc62e3ebaa0b7c0d637fce1a66daff66ee05a9437
8062e1582525534b9c52c5d9a38d6b012746484a2714a14febe2d07af02c32d5
d69764b22d1b68aa9462f1f5f0bf18caebbcff4d592083f80dbce39c64890295
f6ecdae3ae4769aaafc8a0faab30cb66dab8c9d3fff27764ff208be7a455125c
561bf3f3db67996ce81d98f1df91bfa28fb5fc8472ed64606ef8427a97fd8cdd
8323094c43fcd2da44f60b46f043f7ca4ad6a2106b6561598e94008ece46168b
ee0f4afee2940bbe895c1f1f60b8967291a2662ac9dca9f07d9edf400d34b58a
70d63029c65c21c4681779e1968b88dc6923f92408fe5c7e9ca6cb86d7ba713a
79009ee869cec789a3d2735e0a81a546b33e320ee6ae950ba236a9f417ebf763
d81c13b094c59196ac45c5f0ec95446dea219fa2f2a1c35a25f883d2a18ab19d
99baffcd7a6b939b72c99af7c1e88523a50053ab966a079d9bf268aff884426e
61e286c62e556ac79b01c17357176e58efb67d86c5d17407e128094c3151f7f9

Malware: Emotet

Emotet

Emotet first surfaced in 2014, when we uncovered a pretty simple banking Trojan propagated through phishing emails. It evolved into a Malware-as-a-Service botnet several times over the years, allowing individuals willing to pay to gain access to compromised systems. There were a lot of them, including ransomware gangs like Ryuk and the data-stealing malware Trickbot.

Platform: Windows

Threat level: High

Category: Backdoor

Indicators of Compromise (IOCs)

CnC:

219[.]92[.]8[.]17
180[.]92[.]239[.]110
81[.]169[.]145[.]94
www[.]feetinform[.]de
http://94[.]23[.]45[.]86
http://pacificgroup[.]ws/paradisesuiting[.]com/closed_module/additional_742881396_wsvMByYwoxJJai/TmGMTw5Mc_5ydy9fKNrv00
http://nightlifemumbai[.]club/x/0wBD3/!/
https://njyp[.]com/wp-content/Nz/1/
http://www[.]escalierconsulting[.]com/wp-includes/I/
http://de[.]letscompareonline[.]com/cgi-bin/ztEE/
http://paulomarciotrp[.]com/z/y/
http://haumaguerraevoceoalvo[.]com[.]br/wp-includes/0Hm/
http://aecotimes[.]com/wp-admin/44Z/
http://rakikuma[.]com/cgi-bin/K/
84[.]200[.]106[.]120
78[.]47[.]182[.]42
71[.]58[.]165[.]119
69[.]198[.]17[.]7
39[.]112[.]243[.]65
160[.]2[.]24[.]88
139[.]162[.]151[.]141
115[.]71[.]233[.]127
http://c-t[.]com[.]au/PspAMbuSd2
http://bysound[.]com[.]tr/En_us/Documents/11_18
http://bahiacreativa[.]com/9syoe9k
http://84[.]200[.]106[.]120
http://78[.]47[.]182[.]42

http://71[.]58[.]165[.]119:443/whoami[.]php
http://69[.]198[.]17[.]7
http://39[.]112[.]243[.]65
http://160[.]2[.]24[.]88
http://139[.]162[.]151[.]141
http://115[.]71[.]233[.]127

SHA256:

d6dd56e7fb1cc71fc37199b60461e657726c3bf8319ce59177ab4be6ed3b9fb4
cb04718694115b94b4d8bde2be0a4daf802c7a4c94f9b81811872e4e7126e813
667cda76b582c0771f85ad12167238e0f4bb12f479030d99c8a15d7f08eb9975
63e348c05cd94f4488f7f1707ba901ddfa8ec04b4626a46ae2d9d0a83ae291ae
045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f9599
def2b3241d79b377518a5b1a39506ebd3018c8c8e8d611e43916cfdacc377a8a
ba154a65b97dd287b4b85191759be5cae2bfb1b663bd5f6269dea7cb5e80f3a2
afc45e7266a43b6608f6052166a07c75fdff5990d201af85ab06fc63a5e5d3d9
9f8f9470663bb4c1dca15733e1cff0e882c931ed0ca6e9eeefa0f535df501229
90c07f7976127dc85f002710eb67930cd277cefb91d4da09ab42c7de58242f09
7ece6b353421561ebb06b374497b668d84a13506ad8c6fa552b04dc3dfd4878b
7671e803b42ec6425d5f12f3a88d5fa442474e6d7ecae05e75619c9bd57359d1
707539d4c37078c936250a42e901fb5db3a9575db176edc5a3d4889b6f1ab649
6b80eeb2b9d7e86b14e12ee8858daaf12f92c0ac0340cd6b95e5691ff373591c
6a34569bf87487070e6ddd5896b403b7dffb7d9a29341fda5813151a3511aaf6
43099c7f72b6aff08e3ddb1566e32735c66b1751500fff124af6e1a761c1ccbc
34cebe5a052d2d3a5c23059350443b4e6a133983029f9f8c3d275bb8a342402d
2d5caba6f7f04cd29245bd72faa63f47964c98ce9c4b995bb7d4a8a134555d0a
207fbe9c72f12bd67b3febaf2653ae9230000a7f8e1850a0933060df72983084
0bd927dbaad1932ff73d5abacb13abed7947ad6834fd2481a5cc5ada7bab76d9
007afb6797203e525c3facbe4de7dba73b31007e58059cfc09bad8e317581249
e4ecb82fb8a2bf785c2f976c1feea57bca2ff115f5a26c00a9282f9d7f43eb43
e410c621736aa8e6b5174ad62cc2c49fc6a804dd6dac8f87fcfd35910b5734ca
d1e2d97314ab7f756f8ce799a9b578d80388f8e1365f648743183ec08a9f315d
b61113e598e002f1d9273b07d7607d858efba0cb4dcda4a8c72864885ed63376
7516af39a37c18fa7c21a8dc9b0659463886b7453d92d0082e04907e8c7cfb32
6ca9d13ba701a131d357c033e15204e7daacd1805142856c568c1289ca010656
5ab7313c5141a184d22a5c6ac325dbd3bdaf81aa448600d204914a3740e5612d
3ce80ee8433dc8ddd1459244196e687508bd564493621a45fa2df58b3e521314
3546c31ab9a6dbcf55084397ce3b5b24afe23861e2a9cc2b84f7d79b07e33ee5
1908cf7f7f3be0ea4d3221f70402947b76211dad38058a5a0bfb762f8ecdd392
0b3e6fb8bf5701aa1e13c089b2cf51bcb8c169e3d6a2e3e86a8ed9398f8f493b
000cac78f50ff38ccb4465cac82be45df87e8d0b9e28338fdd62d367240f26a0

Malware: AZORult

AZORult

AZORult stealer is known since 2016 when it appeared on underground market. This malware is able to steal passwords from popular browsers and dat files of popular crypto wallets.

Platform: Windows

Threat level: High

Category: Trojan

General information

- Stealing of passwords from browsers, email clients, FTP-clients, IM-clients: Chrome, Mozilla Firefox, Opera, Yandex Browser, Comodo Dragon, Internet Explorer, Microsoft Edge, Outlook, Thunderbird, Amigo, Pidgin, PSI, PSI + and others.
- Stealing of cookies files, data from autocomplete forms in browsers Chrome, Mozilla Firefox, Opera, Yandex Browser, Comodo Dragon, Amigo, etc.
- Stealing of banking cards data from Chrome-like browsers.
- Collecting of dat files from popular crypto wallets (bitcoin, litecoin, etc.)
- Collecting files of Skype and files from victim's desktop
- Collecting of information about victim's system (ip/comp/user, list of processes, list of applications, etc.)

Indicators of Compromise (IOCs)

CnC:

43[.]255[.]154[.]108
185[.]9[.]147[.]100
205[.]185[.]121[.]209
103[.]28[.]15[.]220
141[.]8[.]195[.]34
103[.]211[.]216[.]223
209[.]99[.]16[.]206
142[.]44[.]131[.]27
91[.]243[.]80[.]164:80
93[.]170[.]105[.]132
89[.]108[.]99[.]79
91[.]243[.]81[.]212
5[.]8[.]88[.]106
162[.]244[.]35[.]55
91[.]243[.]80[.]23
homeearlybird[.]com
sijuki[.]com
lulaaura[.]top

driverscontroller[.]com
lacdowronfor[.]com
http://baliseconsulting[.]com
hadsparmirat[.]com
rombutcading[.]ru

MD5:

59953C7BF6FD0D9AF52A483C5F993B66
3163ABA93A0292A4BB27AA52DB27C300
c8996ffafc353f1b14f2cada218f8fa5
2fe90a1d114ed4c91fdcfb5e4bbcf60d
d722759dab276601ce5a6071e282b6c4
5E876524A4BCF406D9B53FA90FE97327
E56D3607E99F3F51A8BD18267D8FC15C
19A1DDDA720F8F444BA81B1E070903F9
6081ED3388C8261E85ED1735EEFC16BE
58FBBD895301937014BA1880284DF58D
B1F988B550C4DB1411BA36773227E248
3FCB889CE9066DD811A79C811B36BF56
FDA0D12ADFB59256B3B655CFB011624F
E829B268494D6A5D53EA91803A018853
9b30f8ac97733dac0fa5a02530f2b94c
07ce7152dcb4ba99c9b05c4a959be577
f76849218adceb805e702a45b85c907c
ad3c82241cdac455de215fd0b37ac4cb
0AC55B5056364CDAC63AAF05F9D7F654
2bfe8198144d16a2bf62740a69f3816f
ed3368dbd10ed6ef74d6b65b1f35ef67
0ac55b5056364cdac63aaf05f9d7f654
60fd7028eba3bb029c0631680ff135a1
ed95fb42855312fd61fb65fb29fb77f1
b8e6efb23e79aa5889360d70f494695c;
29ed79ca7b1778274d76c7ef0304efb5
5ddac41b063bc265854f053fb026475f
f32bd9317b8dc700e899aacc554a3b50
d444350e4ea6e10285865d02982d28ee
7ff25aad4b48a2eca4237755735c158a

Network signatures

AZORult CnC Beacon

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult CnC Beacon"; flow:established,to_server; content:"POST"; http_method; content:".php|20|HTTP/1.1|0d 0a|User-"; fast_pattern; content:"MSIE"; http_user_agent;

pcre:"/^J[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; http_content_len; byte_test:0,<,150,0,string,dec; http_header_names; content:!"Referer"; content:"|0d 0a|User-Agent|0d 0a|Host|0d 0a|Content-Length|0d 0a|"; pcre:"/^(?:Cache-Control|Pragma)\r\n\r\n$/R"; classtype:backdoor; target:src_ip; sid:1002985; rev:1; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin gib, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6;)

AZORult Variant.4 Checkin M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.4 Checkin M2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|4a 2f fb|"; fast_pattern; http_client_body; content:"|2f fb|"; http_client_body; depth:11; content:!"Referer"; http_header; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,0ac55b5056364cdac63aaf05f9d7f654; reference:url,twitter.com/James_inthe_box/status/1020522733984100352?s=03; classtype:trojan-activity; target:src_ip; sid:2025885; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_07_23, malware_family AZORult, updated_at 2018_07_23;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:from_server,established; tls_cert_subject; content:"CN=linddiederich462.pw"; nocase; fast_pattern; isdataat:!1,relative; tls_cert_issuer; content:"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:trojan-activity; target:dest_ip; sid:2027799; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_08_05, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-07

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-07"; flow:established,to_client; tls_cert_subject; content:"CN=mailfueler.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,c189cdadd96c148e64912c55c5129d3e; classtype:trojan-activity; target:dest_ip; sid:2028652; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,

deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03"; flow:established,to_client; tls_cert_subject; content:"CN=worldmasterclass.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,fe9caf2568d7bbf2bb0e20b8e7dc8971; reference:md5,c5a460fd87ffd50c114fffa684688d01; classtype:trojan-activity; target:dest_ip; sid:2028653; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03"; flow:established,to_client; tls_cert_subject; content:"CN=worldmasterclass.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,fe9caf2568d7bbf2bb0e20b8e7dc8971; reference:md5,c5a460fd87ffd50c114fffa684688d01; classtype:trojan-activity; target:dest_ip; sid:2028653; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-03"; flow:established,to_client; tls_cert_subject; content:"CN=corpcougar.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,73fad17f8054d01488c3ddd67e355bf1; reference:md5,a25591dbf57ac687e2a03f94dcccc35a; classtype:trojan-activity; target:dest_ip; sid:2028654; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-02"; flow:established,to_client; tls_cert_subject; content:"CN=adityebirla.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,61b34d02bb09e5a547251a625ce81f9c; reference:md5,cab127c5b8582c1e3ea8860a239a060b; classtype:trojan-activity; target:dest_ip; sid:2028655; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-01

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-01"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, OU=PositiveSSL, CN=www.livdecor.pt"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,7baca517af0b93bd3f94910c7b8f10db; reference:md5,efb4951e11baf306f5680a041c214e5b; classtype:trojan-activity; target:dest_ip; sid:2028656; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-09-30

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-09-30"; flow:established,to_client; tls_cert_subject; content:"CN=flozzy.uk"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,6a333c3f54d7fb6efb276cf6e33315c0; reference:md5,ab578cff6c06157aadd5f324a3413973; classtype:trojan-activity; target:dest_ip; sid:2028657; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult Cnc Server) 2019-09-27

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult Cnc Server) 2019-09-27"; flow:established,to_client; tls_cert_subject; content:"CN=evershinebd.net"; isdataat:!1,relative; fast_pattern; metadata:cnc 0,

severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,c93a2d16dd0cf8dd3afa5ecba111e7c4; reference:md5,23aff33025681263adcdcb480d0e9a95; classtype:trojan-activity; target:dest_ip; sid:2028658; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Low, updated_at 2019_10_07;

Observed Malicious SSL Cert (AZORult CnC) 2019-11-18

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-11-18"; flow:established,to_client; tls_cert_subject; content:"CN=solvents.ru"; isdataat:!1,relative; fast_pattern; tls_cert_issuer; content:"C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority"; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,e54cbf645b0840c0dd1f212f42cd47fd; classtype:backdoor; target:dest_ip; sid:2029001; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_11_18, malware_family AZORult, performance_impact Low, updated_at 2019_11_18;)

AZORult v3.3 Server Response M1

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.3 Server Response M1"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|3f 36 90|"; depth:6; content:"|3f 7a cd 3d 69 c0 3d|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029136; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.3 Server Response M2

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.3 Server Response M2"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|3f 36 90|"; depth:6; content:"|69 81 60 6b 92 6d 6b|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE;

classtype:backdoor; target:dest_ip; sid:2029137; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.3 Server Response M3

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.3 Server Response M3"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|3f 36 90|"; depth:6; content:"|92 2c 36 90 3f 3b 90|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029138; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.2 Server Response M1

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.2 Server Response M1"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|31 69 f6|"; depth:6; content:"|31 25 ab 33 36 a6 33|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029139; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult v3.2 Server Response M2

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.2 Server Response M2"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|31 69 f6|"; depth:6; content:"|36 e7 6e 34 f4 63 34|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029140; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08"; flow:established,to_client; tls_cert_subject; content:"CN=superlatinradio.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,ce879fb552e7740bb2e940c65746aad2; classtype:trojan-activity; target:dest_ip; sid:2028672; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_11, malware_family AZORult, performance_impact Low, updated_at 2019_10_11;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08"; flow:established,to_client; tls_cert_subject; content:"CN=corpcougar.in"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,f7a490fcf756f9ddbaedc2441fbc3c0c; classtype:trojan-activity; target:dest_ip; sid:2028673; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_11, performance_impact Low, updated_at 2019_10_11;)

Observed Malicious SSL Cert (AZORult CnC Server) in SNI 2019-09-27

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) in SNI 2019-09-27"; flow:established,to_server; tls_sni; content:"techxim.com"; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,5c4e395fc545b5e0c03f960a4145f4ea; classtype:trojan-activity; target:src_ip; sid:2028659; rev:1; metadata:attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_07, malware_family AZORult, performance_impact Moderate, updated_at 2019_10_07;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-08"; flow:established,to_client; tls_cert_subject; content:"CN=cloudcitytechnologies.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,9a23881abe27dc70ca42597a1e1de354; classtype:trojan-activity; target:dest_ip; sid:2028894; rev:1; metadata:attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at

2019_10_22, malware_family AZORult, performance_impact Low, updated_at 2019_10_22;)

AZORult Variant.2 Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.2 Checkin"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"CWC^@GUSGP"; http_client_body; depth:10; fast_pattern; http_content_type; content:"image/jpeg"; depth:10; http_header_names; content:!"Accept|0d 0a|"; content:!"User-Agent|0d 0a|"; content:!"Referer|0d 0a|"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,b8e6efb23e79aa5889360d70f494695c; classtype:backdoor; target:src_ip; sid:2826206; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_02, malware_family Stealer, performance_impact Moderate, updated_at 2020_03_06;)

AZORult Variant.2 Checkin m2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.2 Checkin m2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"~~~~~~~~~~|3a 20|~~~~~"; fast_pattern; http_header; http_content_type; content:"image/jpeg"; depth:10; http_header_names; content:!"Accept|0d 0a|"; content:!"User-Agent|0d 0a|"; content:!"Referer|0d 0a|"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,b8e6efb23e79aa5889360d70f494695c; classtype:backdoor; target:src_ip; sid:2826232; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_03, performance_impact Moderate, updated_at 2020_03_06;)

AZORult Variant.2 Checkin m3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.2 Checkin m3"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; http_start; content:".php HTTP/1.0|0d 0a|Host"; fast_pattern; http_content_type; content:"image/jpeg"; depth:10; http_header_names; content:!"Accept|0d 0a|"; content:!"User-Agent|0d 0a|"; content:!"Referer|0d 0a|"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,b8e6efb23e79aa5889360d70f494695c; reference:md5,29ed79ca7b1778274d76c7ef0304efb5; classtype:backdoor; target:src_ip; sid:2826361; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,

deployment Perimeter, signature_severity Major, created_at 2017_05_10, malware_family Stealer, malware_family AZORult, performance_impact Moderate, updated_at 2020_03_02;)

AZORult v3.2 Server Response M3

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult v3.2 Server Response M3"; flow:established,to_client; content:"200"; http_stat_code; file_data; content:"|31 69 f6|"; depth:6; content:"|f4 22 69 f6 31 64 f6|"; distance:0; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2029141; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_12, malware_family AZORult, performance_impact Low, updated_at 2019_12_12;)

AZORult Variant.3 Checkin M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.3 Checkin M1"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|99 4c 42 9d 4f 51 c3|"; http_client_body; depth:7; fast_pattern; http_header_names; content:!"Referer"; content:!"User-Agent"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,ed95fb42855312fd61fb65fb29fb77f1; classtype:trojan-activity; target:src_ip; sid:2829890; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_03_06, malware_family AZORult, performance_impact Low, updated_at 2018_05_30;)

AZORult Variant.3 Checkin M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.3 Checkin M2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|8c 4c 46 91 5b 42 9a 48 42 9f 14|"; http_client_body; depth:11; fast_pattern; http_header_names; content:!"Referer"; content:!"User-Agent"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,60fd7028eba3bb029c0631680ff135a1; classtype:trojan-activity; target:src_ip; sid:2831079; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_05_30, malware_family Stealer, malware_family AZORult, updated_at 2018_05_30;)

AZORult Variant.4 XORed Download

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult Variant.4 XORed Download"; flow:established,to_client; file_data; content:"|31 69 f6|"; depth:3; fast_pattern; pcre:"/(?:\x31\x25\xab\x33|\x36\xe7\x6e\x34|\xf4\x22\x69\xf6)/RQs"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; classtype:trojan-activity; target:dest_ip; sid:2831936; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_07_23, malware_family AZORult, updated_at 2018_07_23;)

AZORult Variant.5 Checkin M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.5 Checkin M1"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|26 66 96 26 66 9d 47 14 ef 26 66 98 26 66 99 46|"; http_client_body; depth:20; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,aebb382b54e1521ad1309f66d29a1d1c; classtype:trojan-activity; target:src_ip; sid:2833315; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, updated_at 2018_10_29;)

AZORult Variant.5 Checkin M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Variant.5 Checkin M2"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"|41 10 8b 30 64 8b 30 66 8b 30 62 8b 30 61 8b 30 62 ed|"; http_client_body; depth:20; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,aebb382b54e1521ad1309f66d29a1d1c; classtype:trojan-activity; target:src_ip; sid:2833316; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, updated_at 2018_10_29;)

AZORult Variant.5 Checkin Response

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"AZORult Variant.5 Checkin Response"; flow:established,to_client; file_data; content:"</n><d>"; content:"</d>|0d 0a 30 0d 0a 0d 0a|"; distance:0; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,aebb382b54e1521ad1309f66d29a1d1c; classtype:trojan-activity;

target:dest_ip; sid:2833317; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, updated_at 2019_09_28;)

Observed DNS Query to known AZOrult Domain

alert dns $HOME_NET any -> any any (msg:"Observed DNS Query to known AZOrult Domain"; dns_query; content:"makak.bit"; nocase; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,78800a47adadaa3a56e533dd7abf957e; classtype:backdoor; target:src_ip; sid:2834136; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_12_28, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

AZORult CnC Beacon M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult CnC Beacon M2"; flow:established,to_server; content:"POST"; http_method; content:"MSIE"; http_user_agent; content:!"/connect.php"; http_uri; content:!"pq.f.360.cn"; http_host; pcre:"/^[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; http_start; content:"POST|20 2f 20|HTTP/1.1|0d 0a|User-Agent|3a 20|Mozilla/"; fast_pattern; depth:37; http_content_len; byte_test:0,<,150,0,string,dec; http_header_names; content:!"Referer"; content:"|0d 0a|User-Agent|0d 0a|Host|0d 0a|Content-Length|0d 0a|Cache-Control|0d 0a 0d 0a|"; depth:53; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,111665920191e273002cf649070a7766; classtype:backdoor; target:src_ip; sid:2834334; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag Stealer, signature_severity Major, created_at 2019_01_10, malware_family AZORult, performance_impact Low, updated_at 2019_01_11;)

Azorult++ Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Azorult++ Checkin"; flow:established,to_server; content:"POST"; http_method; urilen:1; content:"|00 00 00|"; http_client_body; depth:3; content:"Content-Length|3a 20|25|0d 0a|"; http_header; fast_pattern; http_header_names; content:"|0d 0a|Content-Type|0d 0a|Host|0d 0a|Content-Length|0d 0a|Connection|0d 0a|"; content:!"Referer"; content:!"User-Agent"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE;

reference:md5,fe8938f0baaf90516a90610f6e210484; reference:url,securelist.com/azorult-analysis-history/89922/; classtype:backdoor; target:src_ip; sid:2835638; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_03_29, malware_family AZORult, updated_at 2019_03_29;)

AZORult Geolocation Lookup (set)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Geolocation Lookup (set)"; flow:established,to_server; xbits:set,ETPro.AzoRult.GeoCheck,track ip_src,expire 5; noalert; content: "GET"; http_method; content:"/geoip"; http_uri; depth:6; isdataat:!1,relative; content:"api.ip.sb"; http_host; depth:9; isdataat:!1,relative; content:"Mozilla/5.0|20 28|Windows NT 10.0|3b 20|Win64|3b 20|x64|29 20|AppleWebKit/537.36|20 28|KHTML, like Gecko|29 20|Chrome/72.0.3626.121 Safari/537.36"; http_user_agent; depth:115; isdataat:!1,relative; content:"|0d 0a 0d 0a|"; isdataat:!1,relative; http_header_names; content:"|0d 0a|Content-Type|0d 0a|User-Agent|0d 0a|Host|0d 0a|"; http_content_type; content:"application/x-www-form-urlencoded"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,3a13ecf4f8ee02027cf77396bc130c53; reference:md5,fa633db0e584a35350b84560d6ea29df; reference:md5,a703ba86d3692fb59c41efc88ba98c8e; classtype:backdoor; target:src_ip; sid:2836768; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Minor, created_at 2019_06_10, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

AZORult Geolocation Lookup

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult Geolocation Lookup"; flow:established,to_server; xbits:isset,ETPro.AzoRult.GeoCheck,track ip_src; content: "GET"; http_method; content:"/json"; http_uri; depth:6; isdataat:!1,relative; content:"freegeoip.app"; http_host; depth:13; isdataat:!1,relative; content:"Mozilla/5.0|20 28|Windows NT 10.0|3b 20|Win64|3b 20|x64|29 20|AppleWebKit/537.36|20 28|KHTML, like Gecko|29 20|Chrome/72.0.3626.121 Safari/537.36"; http_user_agent; depth:115; isdataat:!1,relative; content:"|0d 0a 0d 0a|"; isdataat:!1,relative; http_header_names; content:"|0d 0a|Content-Type|0d 0a|User-Agent|0d 0a|Host|0d 0a|"; http_content_type; content:"application/x-www-form-urlencoded"; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,3a13ecf4f8ee02027cf77396bc130c53; reference:md5,fa633db0e584a35350b84560d6ea29df;

reference:md5,a703ba86d3692fb59c41efc88ba98c8e; classtype:backdoor; target:src_ip; sid:2836769; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_06_10, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=techxim.com"; nocase; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,dc6c83c65e091e3f572d6870a4d3b382; classtype:backdoor; target:dest_ip; sid:2838487; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_09_17, malware_family AZORult, performance_impact Low, updated_at 2019_09_28;)

AZORult CnC Beacon M3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AZORult CnC Beacon M3"; flow:established,to_server; content:"POST"; http_method; content:" MSIE "; http_user_agent; pcre:"/^[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; http_content_len; byte_test:0,<,150,0,string,dec; http_header_names; content:!"Referer"; content:"|0d 0a|Host|0d 0a|User-Agent|0d 0a|Content-Length|0d 0a|"; depth:36; http_start; content:".php|20|HTTP/1.1|0d 0a|Host|3a|"; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,73964217600c6a83da1110ed4df85217; classtype:backdoor; target:src_ip; sid:2834335; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag Stealer, signature_severity Major, created_at 2019_01_10, malware_family AZORult, performance_impact Low, updated_at 2020_02_12;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-28

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-28"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, CN=dicey.biz"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category TROJAN; reference:md5,76fe84b3901f697927de568f5a0dbb0f; classtype:backdoor; target:dest_ip; sid:2839137; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,

deployment Perimeter, signature_severity Major, created_at 2019_10_28, malware_family AZORult, performance_impact Low, updated_at 2019_10_28;)

Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-22

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC Server) 2019-10-22"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, CN=derek-heath.com"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,6867022e6454cc381c6e156466e53a9e; classtype:backdoor; target:dest_ip; sid:2839138; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_10_28, malware_family AZORult, performance_impact Low, updated_at 2019_10_28;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=azo.icf-fx.kz"; nocase; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,678988bffec50b92a0150e0ed0ea9c24; classtype:backdoor; target:dest_ip; sid:2833327; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_10_29, malware_family AZORult, performance_impact Moderate, updated_at 2019_09_28;)

Observed Malicious SSL Cert (AZORult CnC) 2019-11-18

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-11-18"; flow:established,to_client; tls_cert_subject; content:"CN=gemateknindoperkasa.co.id"; isdataat:!1,relative; fast_pattern; tls_cert_issuer; content:"C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority"; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,3289edad56299b031de6e6a35e93969b; classtype:backdoor; target:dest_ip; sid:2839482; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_11_18, performance_impact Moderate, updated_at 2019_11_18;)

Observed AZORult Domain in TLS SNI

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"Observed AZORult Domain in TLS SNI"; flow:established,to_server; tls_sni; content:"1d9f0a85.ngrok.io"; isdataat:!1,relative; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,5ebe08ea8d7c4f043cd0e94711b0ff7f; classtype:backdoor; target:src_ip; sid:2839694; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_02, malware_family AZORult, performance_impact Low, updated_at 2019_12_02;)

Observed Malicious SSL Cert (AZORult CnC) 2019-12-19

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-12-19"; flow:established,to_client; tls_cert_subject; content:"CN=belco-in.com"; depth:15; isdataat:!1,relative; fast_pattern; reference:md5,5306317feffae1f5d2290229e931b624; classtype:backdoor; target:dest_ip; sid:2840027; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_12_19, malware_family AZORult, performance_impact Low, updated_at 2019_12_19;)

Observed Malicious SSL Cert (AZORult CnC) 2019-12-27

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-12-27"; flow:established,to_client; tls_cert_subject; content:"CN=nsabeau.com.my"; depth:17; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; reference:md5,8390e6ceb68f2bd717d83849c4c0e535; classtype:backdoor; target:dest_ip; sid:2840141; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_12_27, malware_family AZORult, performance_impact Low, updated_at 2019_12_27;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-02"; flow:established,to_client; tls_cert_subject; content:"CN=a-vnet.com"; depth:13; isdataat:!1,relative; fast_pattern; reference:md5,8323181d5829755580d379cde3c7aaea; classtype:backdoor; target:dest_ip; sid:2840227; rev:2; metadata:cnc 0, severity 5, malware_family AZORult,

ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_02, malware_family AZORult, performance_impact Low, updated_at 2020_01_02;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-02"; flow:established,to_client; tls_cert_subject; content:"CN=aearthlink.net"; depth:17; isdataat:!1,relative; fast_pattern; reference:md5,2ddd176ca5b852ba366642447cddde39; classtype:backdoor; target:dest_ip; sid:2840228; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_02, malware_family AZORult, performance_impact Low, updated_at 2020_01_02;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-02

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-02"; flow:established,to_client; tls_cert_subject; content:"CN=ezvuer.com"; depth:13; isdataat:!1,relative; fast_pattern; reference:md5,bf716722b130148297047ab18fbb0342; classtype:backdoor; target:dest_ip; sid:2840229; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_02, malware_family AZORult, performance_impact Low, updated_at 2020_01_02;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=syndicatemechines.com"; depth:24; isdataat:!1,relative; fast_pattern; reference:md5,b1382375eafb605ab7bbf304fadfed64; classtype:backdoor; target:dest_ip; sid:2840357; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at

2020_01_09, malware_family AZORult, performance_impact Low, updated_at 2020_01_09;)

Observed Malicious SSL Cert (AZORult CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC)"; flow:established,to_client; tls_cert_subject; content:"CN=nsabeau.com.my"; depth:17; isdataat:!1,relative; fast_pattern; reference:md5,8390e6ceb68f2bd717d83849c4c0e535; classtype:backdoor; target:dest_ip; sid:2840114; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_12_26, malware_family AZORult, performance_impact Low, updated_at 2019_12_26;)

Observed Malicious SSL Cert (AZORult CnC) 2019-12-05

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2019-12-05"; flow:established,to_client; tls_cert_subject; content:"CN=cbn-cargo.co.id"; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, former_category MALWARE; classtype:backdoor; target:dest_ip; sid:2839784; rev:2; metadata:attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_12_06, malware_family AZORult, performance_impact Low, updated_at 2019_12_06;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-10

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-10"; flow:established,to_client; tls_cert_subject; content:"CN=syndicatemechines.com"; depth:24; isdataat:!1,relative; fast_pattern; reference:md5,276add022cac0382c552364a9f0793e0; classtype:backdoor; target:dest_ip; sid:2840391; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_10, malware_family AZORult, performance_impact Low, updated_at 2020_01_10;)

Observed Malicious SSL Cert (AZORult CnC) 2020-01-13

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (AZORult CnC) 2020-01-13"; flow:established,to_client; tls_cert_subject;

content:"CN=nenkel.com"; depth:13; isdataat:!1,relative; fast_pattern; reference:md5,c0ab2bcae5b3e3567fa5654ae4b0fdf2; classtype:backdoor; target:dest_ip; sid:2840417; rev:2; metadata:cnc 0, severity 5, malware_family AZORult, ti_malware_name AZORult, rule_origin etpro, ti_malware_id 83b2f363e76157386cd7c376ecbe9c8d6b6030a6, affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2020_01_13, malware_family AZORult, performance_impact Low, updated_at 2020_01_13;)

Malware: KPOT Stealer

KPOT Stealer

In July 2018 advertisement about selling if «KPOT Stealer» has been published on underground forums. This malware is able to steal passwords from different browsers, messengers, crypto wallets, FTP and other programs. It also has functions to make screenshots of victim's display and function of loader which allows to infect victim's PC with other malware.

Platform: Windows

Threat level: High

Category: Stealer

General information

- Stealing of passwords, auto filling forms, cookies, masked CC from Chromium-Based and Mozilla-Based browsers. It is realized using recursion.
- Collection of passwords from Internet Explorer (versions 6-11)
- Collections of credentials from jabber clients – psi, psi+, pidgin
- Collection of credentials from outlook, rdp
- Collections of crypto wallets data from wallet.dat, namecoin, monero, bytecoin, electrum, ethereum
- Collection of skype correspondence in format: time – sender— receiver – message
- Grabbing of Telegram session
- Grabbing of Discord session
- Grabbing of Battle.Net session
- Grabbing of passwords in VPN: EarthVPN, NordVPN
- Collection of Steam data: ssfn, config.vdf, loginusers.vdf
- Collection of FTP: FileZilla, WinSCP, TotalCommander, WsFtp
- Collection of wininet cookies in netscape format
- Makes screenshots of victim's display in png format
- Function of files' grabbing-Collects information about victim's system – screen resolution, keyboard layout, video card, the name and number of processor cores, current LOCAL time and time zone, OS version including os edition, number of RAM, IP-address.
- Function of loader – file is recorded into memory. If «resident» is chosen, file will be recorded into Temp, path to the file in PEB will be changed so that your file can be installed by copying itself wherever it is needed. If file is 32 bit, loadup will be in current process; if file is 64 bit and OS is 64-bit, cmd.exe will be launched and file will be injected using wow64ext.
- Function of self-deleting-Bypassing of firewall on the base of com-interface of Internet Explorer.

Network signatures

KPOT Stealer Check-In

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Check-In"; flow:established,to_server; content:"POST"; http_method; content:"bot_id="; depth:7; nocase; http_client_body; fast_pattern; content:"&x64="; nocase; distance:0; http_client_body; content:"&is_admin="; nocase; distance:0; http_client_body; content:"&IL="; nocase; distance:0; http_client_body; content:"&os_version="; nocase; distance:0; http_client_body; content:!"Referer"; http_header; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,7586034a638b95ddd51b60e5b9f4a2b2; classtype:trojan-activity; target:src_ip; sid:2832358; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_08_28, updated_at 2018_08_28;)

KPOT Stealer Exfiltration

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Exfiltration"; flow:established,to_server; content:"POST"; http_method; content:"Content-Disposition|3a 20|form-data|3b 20|name=|22|zip_file|22 3b 20|filename=|22|"; http_client_body; content:".cab|22 0d 0a|Content-Type|3a 20|vnd.ms-cab-compressed|0d 0a|"; http_client_body; distance:0; content:"sysInfo.txt"; http_client_body; distance:0; nocase; http_content_type; content:"multipart/form-data|3b 20|boundary=0xd3adc0d3"; nocase; fast_pattern; depth:40; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,7586034a638b95ddd51b60e5b9f4a2b2; classtype:trojan-activity; target:src_ip; sid:2832359; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2018_08_28, updated_at 2019_09_28;)

KPOT Stealer Exfiltration M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Exfiltration M2"; flow:established,to_server; content:"POST"; http_method; content:"/gate.php"; http_uri; fast_pattern; isdataat:!1,relative; content:"-stream|0d 0a|Content-Encoding|3a 20|binary|0d 0a|Host"; http_header; http_header_names; content:!"User-Agent"; content:!"Referer"; content:!"Accept"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,bba015562893c9367325057b5e725dae; classtype:trojan-activity; target:src_ip; sid:2832753; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,

deployment Perimeter, signature_severity Major, created_at 2018_09_24, malware_family Stealer, malware_family KPOT, updated_at 2019_09_28;)

KPOT Stealer Variant CnC Activity

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Variant CnC Activity"; flow:established,to_server; content:"POST"; http_method; content:"/gate.php"; http_uri; isdataat:!1,relative; fast_pattern; http_content_len; byte_test:0,>,1500,0,string,dec; http_header_names; content:"|0d 0a|Host|0d 0a|Content-Length|0d 0a|Connection|0d 0a|Cache-Control|0d 0a 0d 0a|"; depth:53; content:!"User-Agent"; content:!"Accept"; content:!"Referer"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; reference:md5,d88dd410ac0d4317a493b30442899d16; classtype:trojan-activity; target:src_ip; sid:2834774; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_02_07, malware_family KPOT, performance_impact Moderate, updated_at 2019_09_28;)

SSL/TLS Certificate Observed (KPOT)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"SSL/TLS Certificate Observed (KPOT)"; flow:established,to_client; tls_cert_subject; content:"OU=Domain Control Validated, OU=PositiveSSL, CN=chrisovunhie.pw"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; classtype:trojan-activity; target:dest_ip; sid:2836202; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag KPOT, signature_severity Major, created_at 2019_05_02, updated_at 2019_05_02;)

Observed Malicious SSL Cert (KPOT CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Observed Malicious SSL Cert (KPOT CnC)"; flow:from_server,established; tls_cert_subject; content:"CN=krtk.icu"; nocase; fast_pattern; isdataat:!1,relative; tls_cert_issuer; content:"C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; classtype:trojan-activity; target:dest_ip; sid:2836970; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert, signature_severity Major, created_at 2019_06_21, malware_family KPOT, performance_impact Low, updated_at 2019_09_28;)

KPOT Stealer Exfiltration M3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"KPOT Stealer Exfiltration M3"; flow:established,to_server; content:"POST"; http_method; content:"/conf.php";

http_uri; fast_pattern; isdataat:!1,relative; content:"-stream|0d 0a|Content-Encoding|3a 20|binary|0d 0a|Host"; http_header; http_header_names; content:!"User-Agent"; content:!"Referer"; content:!"Accept"; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category TROJAN; reference:md5,a0cfe711cd721ca486a49e31081b4e02; classtype:trojan-activity; target:src_ip; sid:2837753; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_07_30, malware_family KPOT, performance_impact Moderate, updated_at 2019_09_28;)

Win32/KPOT Stealer Initial CnC Activity M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32/KPOT Stealer Initial CnC Activity M1"; flow:established,to_server; content:"GET"; http_method; content:"/gate.php"; http_uri; isdataat:!1,relative; fast_pattern; http_content_type; content:"application/x-www-form-urlencoded"; depth:33; isdataat:!1,relative; http_header_names; content:"|0d 0a|Connection|0d 0a|Content-Type|0d 0a|Host|0d 0a 0d 0a|"; depth:36; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; reference:md5,7e3ae5d4db2e8c55dc4de98843489e78; classtype:trojan-activity; target:src_ip; sid:2838467; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_09_16, malware_family KPOT_Stealer, performance_impact Moderate, updated_at 2019_09_28;)

Win32/KPOT Stealer Initial CnC Activity M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32/KPOT Stealer Initial CnC Activity M2"; flow:established,to_server; content:"GET"; http_method; content:"/conf.php"; http_uri; isdataat:!1,relative; http_content_type; content:"application/x-www-form-urlencoded"; depth:33; isdataat:!1,relative; http_header_names; content:"|0d 0a|Connection|0d 0a|Content-Type|0d 0a|Host|0d 0a 0d 0a|"; depth:36; isdataat:!1,relative; fast_pattern; metadata:cnc 0, severity 3, malware_family KPOT Stealer, ti_malware_name KPOT Stealer, rule_origin etpro, ti_malware_id f1725b6226be26590ed6f7b0a22c11bc35f23c91, former_category MALWARE; reference:md5,7e3ae5d4db2e8c55dc4de98843489e78; classtype:trojan-activity; target:src_ip; sid:2838468; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2019_09_16, malware_family KPOT_Stealer, performance_impact Moderate, updated_at 2019_09_28;)

Malware: Oski Stealer

Oski Stealer

Oski Stealer is a malware which is advertised on undergrounds forums by oski_seller seller since July 2019. Malware is written in C/C ++. Oski uses man-in-the-browser (MitB) attacks by hooking the browser processes using DLL injection for extracting credentials. Some of the features are: extracting browser credentials and cryptocurrency wallet passwords.

Platform: Windows

Threat level: High

Category: Info stealer

General information

- Non-resident Loader
- Data collection from Browsers (Passwords, Credit Cards, Cookies, Form AutoComplete, View History, Download History, Search Engine History):
- Chromium browsers
- Google Chrome
- Mozilla Firefox
- Opera
- Internet Explorer
- Microsoft Edge
- Amigo
- BlackHawk
- Comodo
- CentBrowser
- Cyberfox
- Epic Privacy Browser
- IceCat
- Kometa
- KMeleon
- Maxthon5
- Nichrome
- Orbitum
- Pale Moon
- Torch
- TorBro
- Uran
- QIPSurf
- Waterfox
- Sputnik

- Vivaldi

Steals following cryptocurrency wallets:

1. BitcoinCore
2. Ethereum
3. Electrum
4. ElectrumLTC
5. Exodus
6. Jaxx
7. ZCash
8. ElectronCash
9. Anoncoin
10. BBQCoin
11. MultiDoge
12. DashCore
13. InfiniteCoin
14. Litecoin
15. DevCoin
16. DigitalCoin
17. FrankoCoin
18. FlorinCoin
19. FreiCoin
20. GoldCoin
21. IxCoin
22. IOCoin
23. MegaCoin
24. MinCoin
25. NameCoin
26. PrimeCoin
27. TerraCoin
28. YACoin

- Collecting following information about Sytem:

1. Windows version
2. Username
3. PC name
4. Machine ID
5. GUID
6. Processor model
7. Video card model
8. Display resolution

9. RAM
10. Local time
11. Time Zone

Network signatures

Win32/Oski Stealer Data Exfil

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32/Oski Stealer Data Exfil"; flow:established,to_server; content:"POST"; http_method; content:".zip|22 0d 0a|"; http_client_body; content:"|0d 0a|PK"; http_client_body; distance:0; content:"screenshot.jpg"; http_client_body; distance:0; http_content_type; content:"multipart/form-data|3b 20|boundary=1BEF0A57BE110FD467A"; depth:49; isdataat:!1,relative; fast_pattern; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family Oski Stealer, rule_origin etpro, former_category MALWARE; reference:md5,6c8357280b50bb1808ec77b0292eb22b; classtype:trojan-activity; target:src_ip; sid:2029236; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2020_01_08, malware_family Oski, updated_at 2020_01_08;)

Malware: FormBookFormgrabber

FormBookFormgrabber

Formgrabber of "FormBook" has begun to be on sale at underground forum since February, 2016. It is intended for compromise data which victim input from browsers, e-mail clients, FTP and services of instant exchange of messages.

Platform: Windows

Threat level: Medium

Category: Trojan

General information

FormBook can be classified as inforstealer malware that collects passwords, logins, installs formgrabber, FTP credentials, messengers credentials and emails data. It began to be sold in the beginning of 2016. The malware injects into legitimate processes and installs keyboard hooks to log all pressed buttons, steal exchange buffer and intercept HTTP sessions.

- log pressed keyboard buttons
- intecept and extract data from HTTP/HTTPS/SPDY/HTTP2 requests
- extract data from Internet browsers and email clients
- make screenshots
- selfupdate
- selfremove
- execute shell commands
- steal cookies
- reboot system
- shutdown system
- Ring3 rootkit
- it reads Windows' ntdll.dll module from disk into memory

If the malware is running with elevated privileges, it can copy payload to one of the following directories:

%ProgramFiles%

%CommonProgramFiles%

If running with normal privileges, it can copy to one of the following directories:

%USERPROFILE%

%APPDATA%

%TEMP%

Browsers hooks look for following substrings in HTTP requests:

- pass
- token
- email
- login
- signin
- account
- persistent

Malware uses RC4 encrypted and Base64 encoded HTTP POST requests to C&C.

Following commands could be received from CnC:

- update
- downlaod and execute
- selfremove
- execute via ShellExecute API
- clear cookies
- reboot OS
- shutdown OS
- collect passwords and create screenshot
- download and extract ZIP archive

Indicators of Compromise (IOCs)

CnC:

http://algreenstdykeghestak.dns.army/receipat/winlog.exe
http://192.210.173.40/files/loader1.exe
http://37.0.10.83/os/sov.exe
http://hisensetech.xyz/obinnazx.exe
http://lg-tv.tk/obinnazx.exe
http://15.165.235.203/winr/x2-29.exe
http://algreenstdykeghestyc.dns.army/receipat/winlog.exe
http://stdytheviejupcazfekr.dns.army/receipt/invoice_115521.doc
http://stdyrmtcntlenverstgv.dns.army/documenrt/winlog.exe
http://algreenstdykeghestdb.dns.army/receipat/winlog.exe
http://3.12.154.229/new.exe
http://hdmilg.xyz/obinnazx.exe
https://moorebankpharmacy.net/index.php
http://rmtcntlstdyfarmtstpo.dns.army/documenrt/winlog.exe
http://darkyardfilms.com/SAMPLE/SAMPLE+PURCHASE ORDER.7z
http://stdytheviejupcazfekr.dns.army/thevdoc/winlog.exe
https://bazaar.abuse.ch/download/7876ab3827c6d9bd/
http://wsdyalgreenkeghewsmq.dns.army/receipat/winlog.exe
http://172.104.235.192/dirkk/dir1.exe
http://18.159.48.76/cps/vbctwo.exe

http://18.159.48.76/cps/vbcone.exe
http://myhostisstillgood11.zapto.org/dashboard/docs/images/kn.exe
http://37.0.10.83/os/m.exe
http://15.164.227.23/windows/xloa.exe
http://darkyardfilms.com/SAMPLE/SAMPLE+PURCHASE%20ORDER.7z
http://23.94.159.183/kome/win32.exe
algreenstdykeghestak.dns.army
hisensetech.xyz
lg-tv.tk
wwwjinsha486.com
wenerberger.com
algreenstdykeghestyc.dns.army
stdytheviejupcazfekr.dns.army
stdyrmtcntlenverstgv.dns.army
algreenstdykeghestdb.dns.army
hdmilg.xyz
cannabisdigital.network
breatheincourage.com
moorebankpharmacy.net
rmtcntlstdyfarmtstpo.dns.army
darkyardfilms.com
bazaar.abuse.ch
wsdyalgreenkeghewsmq.dns.army
myhostisstillgood11.zapto.org
protecteddrive.com
91.223.242.222
10.8.83.10
37.16.83.20
172.16.10.117
194.226.170.31
10.100.30.200

Network signatures

Win32.Trojan Formbook Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan Formbook Checkin"; flow:established,to_server; content:"GET"; http_method; content:!"Referer|3a|"; nocase; http_header; content:!"User-Agent|3a|"; nocase; http_header; content:!"Accept"; nocase; http_header; content:"/?"; http_uri; fast_pattern; pcre:"/\/\?[a-zA-Z0-9\-_]+=[a-zA-Z0-9_+/=]*(&.+)?$/U"; content:"|00 00 00 00 00 00|"; isdataat:!1,relative; threshold:type limit, track by_src, seconds 360, count 1; reference:md5,36d5927e1992190368cb34dd1ce19658; reference:md5,0b658062652f4f4f8829cc131861a764; reference:md5,39c6f6d426252499caf2042ebaa21751; classtype:backdoor;

target:src_ip; sid:1002098; rev:4; metadata:cnc 1, severity 5, malware_family FormBookFormgrabber, malware_family Formbook, ti_malware_name FormBookFormgrabber, rule_origin gib, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4;)

Formbook 0.3 Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Formbook 0.3 Checkin"; flow:to_server,established; content:"POST"; http_method; content:"Mozilla"; http_user_agent; depth:7; content:"dat="; depth:4; http_client_body; nocase; fast_pattern; pcre:"/^[a-z0-9_\/+-]{1000}/PRi"; metadata:cnc 1, severity 5, malware_family FormBookFormgrabber, malware_family Formbook, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,6886a2ebbde724f156a8f8dc17a6639c; classtype:backdoor; target:src_ip; sid:2024436; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_06_29, malware_family Password_Stealer, updated_at 2017_11_07;)

Formbook Stealer Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Formbook Stealer Checkin"; flow:to_server,established; content:"GET"; http_method; content:"/?id="; http_uri; pcre:"/^(?:[A-Za-z0-9/+]{4})*(?:[A-Za-z0-9/+]{2}==|[A-Za-z0-9/+]{3}=|[A-Za-z0-9/+]{4})/URi"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_header_names; content:!"Referer"; content:!"User-Agent|0d 0a|"; content:!"Accept"; metadata:cnc 1, severity 5, malware_family FormBookFormgrabber, malware_family Formbook, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,72c511b5b12f8bcc1dc706a77a0e9bd0; classtype:backdoor; target:src_ip; sid:2827594; rev:6; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_08_18, performance_impact Moderate, updated_at 2020_03_02;)

FormBook CnC Checkin (POST)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"FormBook CnC Checkin (POST)"; flow:established,to_server; content:"POST"; http_method; content:!"."; http_uri; content:!"?"; http_uri; content:!"&"; http_uri; content:"="; within:15; http_client_body; pcre:/^[a-z0-9\(_~-]{1000,}/PRi"; http_content_len; byte_test:0,>,400,0,string,dec; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_accept_enc; content:"gzip, deflate"; depth:13; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a|Content-Length|0d 0a|"; depth:36; fast_pattern; metadata:cnc 0, severity 3,

malware_family FormBookFormgrabber, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; target:src_ip; sid:2829004; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_12_20, malware_family Formbook, performance_impact Moderate, updated_at 2019_09_28;)

FormBook CnC Checkin (GET)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"FormBook CnC Checkin (GET)"; flow:established,to_server; content:"GET"; http_method; content:"/?"; http_uri; pcre:"/^[A-Za-z0-9_-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))&[A-Za-z0-9-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))(?:&sql=\d*)?$/RU"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a 0d 0a|"; depth:22; isdataat:!1,relative; metadata:cnc 0, severity 3, malware_family FormBookFormgrabber, ti_malware_name FormBookFormgrabber, rule_origin etpro, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, former_category MALWARE; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; target:src_ip; sid:2829000; rev:7; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_12_19, malware_family Formbook, performance_impact Moderate, updated_at 2019_09_28;)

TROJAN Formbook 0.3 Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Formbook 0.3 Checkin"; target:src_ip; flow:to_server,established; content:"POST"; http_method; content:"Mozilla"; http_user_agent; depth:7; content:"dat="; depth:4; http_client_body; nocase; fast_pattern; pcre:"/^[a-z0-9_\/+-]{1000}/PRi"; reference:md5,6886a2ebbde724f156a8f8dc17a6639c; classtype:trojan-activity; sid:2024436; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_06_29, deployment Perimeter, former_category MALWARE, signature_severity Major, updated_at 2020_08_24, severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, malware_family FormBookFormgrabber, rule_origin etpro;)

TROJAN FormBook CnC Checkin (GET)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN FormBook CnC Checkin (GET)"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:"/?"; http_uri; pcre:"/^[A-Za-z0-9_-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-

9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))&[A-Za-z0-9-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))(?:&sql=\d*)?$/RU"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a 0d 0a|"; depth:22; isdataat:!1,relative; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; sid:2031449; rev:7; metadata:attack_target Client_Endpoint, created_at 2017_12_19, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_12_16, severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, ti_malware_id d77771f830d535a63e37a1ca8df3bcc25daf107d, ti_malware_name FormBook Formgrabber, rule_origin etpro;)

TROJAN FormBook CnC Checkin (GET)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN FormBook CnC Checkin (GET)"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:"/?"; http_uri; pcre:"/^[A-Za-z0-9_-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))&[A-Za-z0-9-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))(?:&sql=\d*)?$/RU"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a 0d 0a|"; depth:22; isdataat:!1,relative; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; sid:2829000; rev:7; metadata:attack_target Client_Endpoint, created_at 2017_12_19, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_12_23, severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, malware_family FormBookFormgrabber, rule_origin etpro;)

Formbook Stealer Checkin (POST)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Formbook Stealer Checkin (POST)"; target:src_ip; flow:to_server,established; content:"POST"; http_method; content:"dat="; depth:4; http_client_body; nocase; fast_pattern; content:"&un="; http_client_body; distance:0; content:"&br="; http_client_body; distance:0; pcre:"/^dat=[a-z0-9-_/+]{1000}/Pi"; reference:md5,6886a2ebbde724f156a8f8dc17a6639c; classtype:trojan-activity; sid:2828408; rev:1; metadata:former_category TROJAN, severity 3, malware_family FormBookFormgrabber, rule_origin etpro; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_06_29,

malware_family Password_Stealer, updated_at 2017_09_28; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_10_24, deployment Perimeter, former_category TROJAN, malware_family Formbook, performance_impact Low, signature_severity Major, tag dupe, updated_at 2018_10_11;)

TROJAN FormBook CnC Checkin (GET)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN FormBook CnC Checkin (GET)"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:"/?"; http_uri; pcre:"/^[A-Za-z0-9_-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))&[A-Za-z0-9-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))(?:&sql=\d*)?$/RU"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a 0d 0a|"; depth:22; isdataat:!1,relative; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; sid:2031412; rev:7; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_12_19, deployment Perimeter, former_category MALWARE, malware_family Formbook, performance_impact Moderate, signature_severity Major, updated_at 2020_09_16, severity 3, ti_malware_id d77771f830d535a63e37a1ca8df3bcc25daf107d, ti_malware_name FormBook Formgrabber, rule_origin etpro;)

Win32.Trojan.MSIL.Injector GET request

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan.MSIL.Injector GET request"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:!"Referer|3a|"; nocase; http_header; content:!"User-Agent|3a|"; nocase; http_header; content:!"Accept"; nocase; http_header; content:"/?"; http_uri; fast_pattern; pcre:"/\/\?[a-zA-Z0-9\-_]+=[a-zA-Z0-9_+/=]*(&.+)?$/U"; content:"|00 00 00 00 00 00|"; isdataat:!1,relative; threshold:type limit, track by_src, seconds 360, count 1; reference:md5,36d5927e1992190368cb34dd1ce19658; reference:md5,0b658062652f4f4f8829cc131861a764; classtype:trojan-activity; reference:md5,39c6f6d426252499caf2042ebaa21751; sid:1002098; rev:4; metadata:severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, malware_family FormBookFormgrabber, rule_origin gib;)

Formbook CnC script download instead of audio v1

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"Formbook CnC script download instead of audio v1"; flowbits:isset,gib.formbook.mp3; flow:established,to_client; content:"$"; depth:1; http_server_body; fast_pattern;

pcre:"/\$[A-z0-9]{1,3}\=\@\(\d{2},\d{2},/Q"; http_content_type; content:"audio/mpeg"; target:src_ip; reference:md5,7c711c9e227d455a131a223eea423cbe flowbit_sids,1003216; classtype:trojan-activity; sid:1003217; rev:1; metadata:sha1 62aec9adb0dbd955d006742f49a0285823e80f1e, severity 3, rule_origin gib;)

TROJAN FormBook CnC Checkin (POST)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN FormBook CnC Checkin (POST)"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:!"."; http_uri; content:!"?"; http_uri; content:!"&"; http_uri; content:"="; within:15; http_client_body; pcre:/^[a-z0-9\(_~-]{1000,}/PRi"; http_content_len; byte_test:0,>,400,0,string,dec; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_accept_enc; content:"gzip, deflate"; depth:13; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a|Content-Length|0d 0a|"; depth:36; fast_pattern; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; sid:2829004; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_12_20, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_09_16, severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, malware_family FormBookFormgrabber, rule_origin etpro;)

FormBook CnC checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"FormBook CnC checkin"; target:src_ip; flow:established,to_server; content:"GET"; http_method; pcre:"/\/[a-z0-9]+\/\?[A-Za-z0-9]+=[A-Za-z0-9+\/]+=*&[A-Za-z0-9]+=[A-Za-z0-9]+/U"; content:"|00 00 00 00 00 00|"; http_header_names; content:!"Referer"; content:!"User-Agent"; content:!"Accept"; content:!"Accept-Language"; content:!"Content-Type"; classtype:trojan-activity; reference:md5,a78444423e5f422eeb62c9019048f41e; sid:1002768; rev:2; metadata:severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, rule_origin gib;)

TROJAN FormBook CnC Checkin (GET)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN FormBook CnC Checkin (GET)"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:"/?"; http_uri; pcre:"/^[A-Za-z0-9_-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))&[A-Za-z0-9-]{1,15}=(?:[A-Za-z0-9-_]{1,25}|(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}==|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4}))(?:&sql=\d*)?$/RU"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a

0d 0a|"; depth:22; isdataat:!1,relative; reference:md5,a6a114f6bc3e86e142256c5a53675d1a; classtype:trojan-activity; sid:2031453; rev:7; metadata:attack_target Client_Endpoint, created_at 2017_12_19, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_12_23, severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, ti_malware_id d77771f830d535a63e37a1ca8df3bcc25daf107d, ti_malware_name FormBook Formgrabber, rule_origin etpro;)

TROJAN FormBook CnC Checkin (POST) M2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN FormBook CnC Checkin (POST) M2"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:!"."; http_uri; content:!"?"; http_uri; content:!"&"; http_uri; content:"="; within:15; http_client_body; content:"|00 00 00 00 00 00|"; http_client_body; isdataat:!1,relative; fast_pattern; pcre:"/=[a-z0-9\(_~\-\.\x00]{300,}\x00$/Pi"; http_accept_enc; content:"gzip, deflate"; depth:13; isdataat:!1,relative; http_connection; content:"close"; depth:5; isdataat:!1,relative; http_content_len; byte_test:0,>,300,0,string,dec; http_header_names; content:"|0d 0a|Host|0d 0a|Connection|0d 0a|Content-Length|0d 0a|"; depth:36; reference:md5,6f5d2b42f4a74886ac3284fa9a414a87; classtype:trojan-activity; sid:2031413; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_12_16, deployment Perimeter, signature_severity Major, updated_at 2021_02_03, severity 3, ti_malware_id d77771f830d535a63e37a1ca8df3bcc25daf107d, ti_malware_name FormBook Formgrabber, rule_origin etpro;)
Formbook CnC communication (script download instead of audio)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Formbook CnC communication (script download instead of audio)"; flowbits:set,gib.formbook.mp3; flow:established,to_server; flowbits:noalert; content:"GET"; http_method; content:".mp3"; isdataat:!1,relative; http_uri; http_header_names; content:!"Referer"; content:!"Cookie"; content:!"User-Agent"; target:src_ip; reference:md5,7c711c9e227d455a131a223eea423cbe; classtype:trojan-activity; sid:1003216; rev:1; metadata:sha1 62aec9adb0dbd955d006742f49a0285823e80f1e, flowbit_sids 1003217_1003218, severity 3, rule_origin gib;)

TROJAN Formbook Stealer Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Formbook Stealer Checkin"; target:src_ip; flow:to_server,established; content:"GET"; http_method; content:"/?id="; http_uri; pcre:"/^(?:[A-Za-z0-9/+]{4})*(?:[A-Za-z0-9/+]{2}==|[A-Za-z0-9/+]{3}=|[A-Za-z0-9/+]{4})/URi"; content:"Connection|3a 20|close|0d 0a 0d 0a 00 00 00 00 00 00|"; fast_pattern; http_header_names; content:!"Referer"; content:!"User-Agent|0d 0a|"; content:!"Accept";

reference:md5,72c511b5b12f8bcc1dc706a77a0e9bd0; classtype:trojan-activity; sid:2827594; rev:6; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_08_18, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_11_03, severity 3, ti_malware_id 8eee3e23fc03c10c1d3527bea862fc18541db8b4, ti_malware_name FormBookFormgrabber, malware_family FormBookFormgrabber, rule_origin etpro;)

Formbook CnC script download instead of audio v2

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"Formbook CnC script download instead of audio v2"; flowbits:isset,gib.formbook.mp3; flow:established,to_client; content:"@@4D,@@5A"; depth:9; nocase; http_server_body; fast_pattern; http_content_type; content:"audio/mpeg"; target:src_ip; reference:md5,7c711c9e227d455a131a223eea423cbe; classtype:trojan-activity; sid:1003218; rev:1; metadata:sha1 62aec9adb0dbd955d006742f49a0285823e80f1e, flowbit_sids 1003216, severity 3, rule_origin gib;)

Malware: Loki PWS

Loki PWS

Loki PWS (Password Stealer, aka Loki Bot, Loki-Bot, LokiBot) is a Trojan designed to steal authentication data and cookies saved in browsers. In addition, the malware can steal logins/passwords from Cryptocoin wallet, email clients, FTP clients, VNC clients, Poker clients. It has file grabber, keylogger, VNC, Proxy, form grabber (FF, Chrome, IE, Edge, and Opera) and resident loader modules. Loki PWS sends stolen information to the C&C server via HTTP POST. The Trojan was written in C++ and works with following versions of Windows: XP, Vista, 7, 8, 8.1, 10 and Linux. Loki PWS first appeared on underground forums in 2015. A seller is known as «carter» and «lokistov». The seller disappeared after Loki v2 release in 2017. Presumably, Loki PWS Control panel was leaked in 2016. A cracked version of the Loki PWS has become widespread by the end of the 2017. 10.10.2018 on the underground forum exploit.in carter published an announcement about the sale of new versions Loki Bot v2.1. An actor wasn't active on forums until appearance of Loki Bot v2.1.

Platform: Windows

Threat level: High

Category: Trojan

General information

The malware can steal logins/passwords which were saved in following browsers:

- Internet Explorer
- Mozilla Firefox (x32+x64)
- Google Chrome
- K-Meleon
- Comodo Dragon
- Comodo IceDragon
- SeaMonkey
- Opera
- Safari
- CoolNovo
- Rambler Nichrome
- RockMelt
- Baidu Spark
- Chromium
- Titan Browser
- Torch Browser
- Browser

- Epic Privacy Browser
- Sleipnir Browser
- Vivaldi
- Coowon Browser
- Superbird Browser
- Chromodo Browser
- Mustan Browser
- 360 Browser
- Cyberfox (x32+x64)
- Pale Moon
- Maxthon browser
- Citrio Browser
- Chrome Canary
- Waterfox
- Orbitum
- Iridium
- SlimBrowser
- Brave
- Kometa
- Avant Browser
- Uran
- Dooble
- Sputnik

the Trojan can steal logins/passwords from email clients:

- Outlook (2003-2013)
- Mozilla Thunderbird
- Foxmail
- Pocomail
- Incredimail
- Gmail Notifier Pro
- SNetz Mailer
- Checkmail
- Opera Mail
- FossaMail
- MailSpeaker
- yMail
- Trojita
- TrulyMail
- Claws Mail
- The Bat!
- Mailbird

- TouchMail

The author noted that Trojan also can work with following FTP/VNC clients

- Total Commander
- FlashFXP
- FileZilla
- FAR Manager
- CyberDuck
- Bitvise
- NovaFTP
- NetDrive
- NppFTP
- FTPShell
- SherrodFTP
- MyFTP
- FTPBox
- FtpInfo
- Lines FTP
- FullSync
- Nexus File
- JaSFtp
- FTP Now
- Xftp
- Easy FTP
- GoFTP
- NETFile
- Blaze Ftp
- Staff-FTP
- DeluxeFTP
- ALFTP
- FTPGetter
- WS_FTP
- AbleFTp
- Automize
- RealVNC
- TightVNC
- Syncovery
- mSecure Wallet
- SmartFTP
- FreshFTP
- BitKinex
- UltraFXP

- FTP Rush
- Vandyk SecureFX
- OdinSecure FTP Expert
- Fling
- ClassicFTP
- Maxthon browser
- Kitty(login+private key)
- WinSCP
- Remmina RDP
- WinFTP
- 32Bit FTP
- FTP Navigator
- Core FTP
- CrossFTP
- FTP Voyager
- FireFTP
- CuteFTP
- JSCAPE

Supported password managers:

- EnPass
- KeePass
- 1Password
- AI RoboForm

The malware has module for stealing logins and passwords from cryptocoin wallets

- Bitcoin
- Litecoin
- MultiBit
- Electrum-BTC
- Electrum-LTC
- Armoryc
- Namecoin
- Ufasoft
- PPCoin
- Blockchain
- Ixcoin
- Feathercoin
- NovaCoin
- Primecoin
- Terracoin
- Devcoin

- Digitalcoin
- Anoncoin
- Worldcoin
- Quarkcoin
- Infinitecoin
- DogeCoin
- AsicCoin
- LottoCoin
- DarkCoin
- BitShares
- MultiDoge
- Monacoin
- BitcoinDark
- Unobtanium
- Paycoin
- Copay
- Monero
- Ethereum
- Electron Cash (Bitcoin Cash)
- Bitcoin Knots
- Green Address
- mSIGNA
- Bither
- Exodus
- WinZec (Zcash)

Network signatures

Win32.Spyware_LokiBot Sending data (Fareit/Pony)

alert http $HOME_NET any -> any any (msg:"Win32.Spyware_LokiBot Sending data (Fareit/Pony)"; flow:established,to_server; content:"POST"; http_method; content:!"Referer|3A|"; nocase; http_header; content:!"Accept-"; nocase; http_header; content:".php HTTP/1.0"; content:"(Charon|3B| Inferno)"; http_user_agent; content:"Content-Key|3A 20|"; threshold:type limit, track by_src, seconds 360, count 1; reference:md5,1019d4a79c0c66070800b827026bb83c; reference:md5,565d6e2f8ed24de7c3d36b9c277c4cf9; reference:md5,99f29c4b4ef7f494c525018212662d97; classtype:backdoor; target:src_ip; sid:1001732; rev:2; metadata:cnc 0, severity 5, malware_family Loki PWS, ti_malware_name Loki PWS, rule_origin gib, ti_malware_id b50509a8a6bfdf5f510b38040b3a38fb311447f2;)

Loki Bot Cryptocurrency Wallet Exfiltration Detected

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Loki Bot Cryptocurrency Wallet Exfiltration Detected"; flow:established,to_server; content:"POST"; http_method; content:"(Charon|3b 20|Inferno)"; http_user_agent; content:"|00 26 00|"; offset:1; depth:3; http_client_body; pcre:"/^[\x00-\x01]\x00.\x00{3}/PR"; metadata:cnc 0, severity 5, malware_family Loki PWS, ti_malware_name Loki PWS, rule_origin etpro, ti_malware_id b50509a8a6bfdf5f510b38040b3a38fb311447f2, former_category TROJAN; classtype:backdoor; target:src_ip; sid:2024311; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_17, malware_family lokibot, updated_at 2018_04_13;)

Loki Bot Keylogger Data Exfiltration Detected M1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Loki Bot Keylogger Data Exfiltration Detected M1"; flow:established,to_server; content:"POST"; http_method; content:"(Charon|3b 20|Inferno)"; http_user_agent; content:"|00 2b 00|"; offset:1; depth:3; http_client_body; pcre:"/^[\x00-\x01]\x00.\x00[\x00-\x01]\x00.\x00.{4}\x01\x00.\x00{3}.{48}\x05\x00{3}/PR"; metadata:cnc 0, severity 5, malware_family Loki PWS, ti_malware_name Loki PWS, rule_origin etpro, ti_malware_id b50509a8a6bfdf5f510b38040b3a38fb311447f2, former_category TROJAN; classtype:backdoor; target:src_ip; sid:2024315; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2017_05_17, malware_family lokibot, updated_at 2018_04_13;)

Malware: Nexus Stealer

Nexus Stealer

Nexus Stealer is a malware which is advertised on undergrounds forums by nexusMP seller since January 2020. Malware is written in C/C ++.

Platform: Windows

Threat level: High

Category: Info stealer

General information

- Data collection of all Chromium browsers (Passwords, Credit Cards, Cookies, Form AutoComplete, View History, Download History, Search Engine History) Includes data from Chrome Browser and browsers with non-standard data location.
- Collecting all .dat of files (recursion) of cryptocurrency wallets, and also collecting cold purses: Anoncoin, Bitcoin, Bitpay, Coinomi, DashCore, devcoin, Eidoo, Electrum, Electrum-NMC, Exodus, Feathercoin, Fetch, FLO, Franko, Freicoin, GoldCoin (GLD), Guarda, I0coin, iXcoin, Jaxx, Litecoin, Luckycoin, MegaCoin, Mincoin, Monero, MyCrypto, NovaCoin, Peercoin, Primecoin, Quarkcoin, TerracoinCore, Worldcoin, Yacoin, Zetacoin.
- Collecting 2FA Sessions - Authenticator (Authy)
- Collecting all Telegram sessions
- Collect all Discord sessions
- Collect all Steam sessions
- Jabber Client Census
- Collect all profiles FileZilla
- Collect all profiles WinSCP
- Collect all profiles TotalCommander
- Collecting credentials WindowsSecureVault
- IE, Edge credential collection
- Collect all Pidgin accounts
- Collecting all PSI, PSI accounts
- Collecting sessions of VPN clients
- Collection of sessions and authorization data OpenVPN
- Collecting Steam Details
- Collecting profile data WiFi
- Collecting profiles from Credmanager
- Collect system information, screenshots, and location data (useful for spot client processing)
- Grabber of files
- Ability to filter CIS-Logi (LPG), protection against repetition

- Loader module with flexible parameters, ability to specify multiple files and multiple filters
- A separate and convenient search page, with the ability to sort by a large number of criteria, including cookies and passwords, to automate the search for the required data.
- Ability to change skin in one click,
- View log data without downloading (passwords, PC information)
- The automated installation of the panel
- Intuitive and at the same time beautiful admin panel. Ability to sort logs by custom templates (Presets), ability to create/edit/delete templates.
- The ability to download or remove all logs directly in the panel (in one click)!
- Smart filtering of fresh logs
- Geostatistical information on home page

Network signatures

Nexus Stealer CnC Data Exfil

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Nexus Stealer CnC Data Exfil"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; isdataat:!1,relative; content:!"Mozilla"; http_user_agent; content:"{"; depth:1; http_client_body; content:"|7e 3b 5e 3b|Windows|20|"; distance:0; http_client_body; within:50; fast_pattern; content:"|7e 3b 5e 3b|"; distance:0; http_client_body; content:"|7e 3b 5e 3b|"; distance:0; http_client_body; content:"|7e 3b 5e 3b|"; distance:0; http_client_body; http_header_names; content:!"Referer"; metadata:cnc 0, severity 3, malware_family Nexus Stealer, rule_origin etpro, former_category MALWARE; reference:md5,8bd8582155ef003b8a24d341d75f1d7f; classtype:trojan-activity; target:src_ip; sid:2029298; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, signature_severity Major, created_at 2020_01_21, malware_family Nexus, updated_at 2020_02_19;)

Malware: TrickBot

TrickBot is banking trojan first appeared in middle 2016. TrickBot is Dyre successor and has strong code similarities to the Dyre trojan.

Platform: Windows

Threat level: High

Category: Trojan

General information

In the first half of 2016, Trickbot was first noticed in attacks on clients of banks. Trickbot is a banking trojan using similar techniques as Dyre. After launch of the loader – "TrickLoader", the body of the trojan is installed in the victim's system. This is loaded from the host controlled by the attackers along with additional modules that are then subsequently launched. Amongst these, are modules for collection and distribution of PC system information, data intercepted from browsers, information from email clients, functionality for network spreading, form-grabbers as well as browser inject functionality.

Network signatures

Trickbot SSL certificate detected

```
alert tls any any -> $HOME_NET any (msg:"Trickbot SSL certificate detected";
flow:established,from_server; content:"|55 04 0a|"; content:"|16|Ubiquiti Networks
Inc."; distance:1; within:23; content:"|55 04 0b|"; distance:0; content:"|11|Technical
Support"; distance:1; within:18; content:"|55 04 03|"; distance:0; content:"UBNT-";
distance:1; within:6; target:src_ip; classtype:banking-trojan;
reference:md5,87dfea7f85a960bbc92b0adbf124a072; sid:1002270; rev:2;
metadata:severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae,
ti_malware_name TrickBot, malware_family TrickBot, rule_origin gib;)
```

Win32.Trojan_Trickbot Sending IE history

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan_Trickbot
Sending IE history"; target:src_ip; flow:established,to_server; content:"POST";
http_method; content:!"Referer|3a|"; nocase; http_header; content:"Connection|3a|
close"; nocase; http_header; content:"boundary=---------"; http_header; fast_pattern;
pcre:"/boundary=-{9}[A-Z]{16}\x0d\x0a/"; pcre:"/\/[\x20-\x7e]+?\.[0-9A-F]{32}\//U";
reference:md5,6ace098066b82cd4e6ad5bbdc9954b0d;
reference:md5,1a3d01fce1c387a2075f1de6a462a871; classtype:banking-trojan;
reference:md5,155106c45d76d566051cc65f77df2e55; sid:1002028; rev:1;
```

metadata:severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin gib;)

TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (TrickBot CnC)"; target:dest_ip; flow:established,from_server; content:"|09 00 e7 1f b0 eb b2 ae 21 70|"; fast_pattern; content:"|55 04 0a|"; distance:0; content:"|13|Default Company Ltd"; distance:1; within:20; reference:url,sslbl.abuse.ch; classtype:banking-trojan; sid:2023541; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_11_22, deployment Perimeter, former_category MALWARE, signature_severity Major, tag SSL_Malicious_Cert, updated_at 2016_11_22, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN TrickBot IP Check

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN TrickBot IP Check"; target:src_ip; flow:to_server,established; content:"GET"; http_method; content:"User-Agent|3a 20|Mozilla/5.0 (Windows NT 10.0|3b 20|WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36|0d 0a|Host|3a 20|ipinfo.io|0d 0a|"; http_header; depth:141; fast_pattern:121,20; content:!"Referer|3a|"; http_header; content:!"Accept"; http_header; threshold:type both, track by_src, count 1, seconds 5; reference:md5,770db932ec1807de570be1727e5ced09; classtype:banking-trojan; sid:2827992; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_09_18, deployment Perimeter, former_category TROJAN, performance_impact Moderate, signature_severity Major, updated_at 2020_08_12, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN Malicious SSL certificate detected (TrickBot C2)

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Malicious SSL certificate detected (TrickBot C2)"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|0c|421ho4241.ru"; distance:1; within:13; classtype:banking-trojan; sid:2828428; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_10_26, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2017_10_26, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN Trickbot SSL Certificate Detected

alert tls $EXTERNAL_NET 447 -> $HOME_NET any (msg:"TROJAN Trickbot SSL Certificate Detected"; target:dest_ip; flow:established,from_server; content:"|55 04 03|"; content:"|13|sd-97597.dedibox.fr"; fast_pattern; distance:1; within:20; reference:md5,3d55d71c3f0655837694ea125687e479; reference:url,sslbl.abuse.ch/intel/cf31d2f8e419d76517b0bc6c3ead1f246b950a42; classtype:banking-trojan; sid:2830188; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_03_29, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, updated_at 2018_03_29, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

TROJAN Trickbot Payload Request

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Trickbot Payload Request"; target:src_ip; flow:to_server,established; content:"GET"; http_method; pcre:"/^\/(?:kas|ser|mac)[0-9]+\.png$/Ui"; http_start; content:".png HTTP/1.1|0d 0a|Host|3a 20|"; fast_pattern; http_header_names; content:!"Accept"; content:!"Referer|0d 0a|"; content:!"User-Agent|0d 0a|"; reference:md5,2c6cd25a31fe097ee7532422fc8eedc8; classtype:banking-trojan; sid:2024901; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_10_23, deployment Perimeter, former_category TROJAN, signature_severity Major, tag Trickbot, updated_at 2020_03_04, severity 5, ti_malware_id cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot, malware_family TrickBot, rule_origin etpro;)

Trickbot Known C&C IP

alert tcp $HOME_NET any -> [200.119.45.140, 107.181.175.122, 79.143.31.94, 186.47.40.234, 181.129.93.226, 190.152.4.210, 107.173.42.177, 82.118.22.87, 195.123.213.186, 195.123.246.69, 51.254.69.233, 195.123.240.36, 195.161.114.131, 192.210.132.15, 168.235.102.16, 164.132.138.134, 23.94.93.106, 190.154.203.218, 189.80.134.122, 125.99.253.34, 191.37.181.152, 187.58.56.26, 146.196.122.167, 177.103.240.149, 131.196.184.141, 103.84.238.3, 190.152.4.210, 202.4.169.178, 36.89.85.103, 103.117.172.206, 45.237.240.178] 443 (msg:"Trickbot Known C&C IP"; reference:md5, 0cc0cbe936aadd2ba70dc0c8a901493b; reference:url, https://brica.de/alerts/alert/public/1274175/trickbot-is-using-google-docs-to-trick-proofpoints-gateway/; reference:url, https://feodotracker.abuse.ch/browse/host/107.173.42.177/; reference:url, https://feodotracker.abuse.ch/browse/host/82.118.22.87/; reference:url, https://feodotracker.abuse.ch/browse/host/195.123.213.186/; reference:url, https://feodotracker.abuse.ch/browse/host/195.123.246.69/; reference:url, https://feodotracker.abuse.ch/browse/host/51.254.69.233/; reference:url,

https://otx.alienvault.com/indicator/ip/195.123.240.36; reference:url,
https://feodotracker.abuse.ch/browse/host/195.161.114.131/; reference:url,
https://feodotracker.abuse.ch/browse/host/192.210.132.15/; reference:url,
https://feodotracker.abuse.ch/browse/host/168.235.102.16/; reference:url,
https://feodotracker.abuse.ch/browse/host/164.132.138.134/; reference:url,
https://feodotracker.abuse.ch/browse/host/23.94.93.106/; reference:url,
https://feodotracker.abuse.ch/browse/host/190.154.203.218/; reference:url,
https://feodotracker.abuse.ch/browse/host/189.80.134.122/; reference:url,
https://feodotracker.abuse.ch/browse/host/125.99.253.34/; reference:url,
https://feodotracker.abuse.ch/browse/host/191.37.181.152/; reference:url,
https://feodotracker.abuse.ch/browse/host/187.58.56.26/; reference:url,
https://feodotracker.abuse.ch/browse/host/146.196.122.167/; reference:url,
https://feodotracker.abuse.ch/browse/host/177.103.240.149/; reference:url,
https://feodotracker.abuse.ch/browse/host/131.196.184.141/; reference:url,
https://feodotracker.abuse.ch/browse/host/103.117.232.198/; reference:url,
https://feodotracker.abuse.ch/browse/host/103.84.238.3/; reference:url,
https://feodotracker.abuse.ch/browse/host/190.152.4.210/; reference:url,
https://feodotracker.abuse.ch/browse/host/202.4.169.178/; reference:url,
https://feodotracker.abuse.ch/browse/host/36.89.85.103/; reference:url,
https://feodotracker.abuse.ch/browse/host/103.117.172.206/; reference:url,
https://feodotracker.abuse.ch/browse/host/45.237.240.178/; target:src_ip;
classtype:banking-trojan; sid:1003029; rev:1; metadata:cnc 1, severity 5, ti_malware_id
cf1534c820c4cde26a2bbb078274f10db79e14ae, ti_malware_name TrickBot,
malware_family TrickBot, rule_origin gib;)

Malware: Kinsing

Kinsing Malware

In this attack, the attackers exploit a misconfigured Docker API port to run an Ubuntu container with the kinsing malicious malware, which in turn runs a cryptominer and then attempts to spread the malware to other containers and hosts.

Platform: Linux

Threat level: Medium

Category: Cryptominer

General information

- Disabled security measures and cleared log
- Downloaded and ran the shell script every minute using crontab
- Halted and deleted files related to numerous applications like other malware and cryptominers
- Installed and ran the Kinsing malware
- Killed other malicious Docker containers and deleted their image
- Looked for other commands running and cron; if found, it deletes all cron jobs including its own.

Indicators of Compromise (IOCs)

CnC:

http://142[.]44[.]191[.]122/d[.]sh
http://142[.]44[.]191[.]122/kinsing/
http://142[.]44[.]191[.]122/al[.]sh
http://142[.]44[.]191[.]122/cron[.]sh
http://142[.]44[.]191[.]122/
http://142[.]44[.]191[.]122/kinsing
http://142[.]44[.]191[.]122/ex[.]sh
http://185[.]92[.]74[.]42/w[.]sh
http://185[.]92[.]74[.]42/d[.]sh
http://217[.]12[.]221[.]244/
http://217[.]12[.]221[.]24/d[.]sh
http://217[.]12[.]221[.]244/kinsing
http://217[.]12[.]221[.]244/j[.]sh
http://217[.]12[.]221[.]244/t[.]sh
http://217[.]12[.]221[.]244/spr[.]sh

http://217[.]12[.]221[.]244/spre[.]sh
http://217[.]12[.]221[.]244/p[.]sh
http://217[.]12[.]221[.]244/Application[.]jar
http://217[.]12[.]221[.]244/f[.]sh
http://www[.]traffclick[.]ru/
http://www[.]mechta-dachnika-tut[.]ru/
http://www[.]rus-wintrillions-com[.]ru/
http://rus-wintrillions-com[.]ru/
http://stroitelnye-jekologicheskie-materialy2016[.]ru
45[.]10[.]88[.]102
91[.]215[.]169[.]111
193[.]33[.]87[.]219

MD5:

kinsing -	0d3b26a8c65cf25356399cc5936a7210
kinsing -	6bffa50350be7234071814181277ae79
kinsing -	c4be7a3abc9f180d997dbb93937926ad
kdevtmpfsi -	d9011709dd3da2649ed30bf2be52b99e

Malware: Outlaw hacking group cryptocurrency miners

Outlaw hacking group cryptocurrency miners

Outlaw Hacking Group's Botnet download Monero miner script named dota3.tar.gz.

The shell script downloads, extracts, and executes the miner payload. The extracted TAR file contains folders with scripts and the miner and backdoor components.

Platform: Linux

Threat level: Medium

Category: Cryptominer

General information

The Shellbot disguises itself as a process named rsync, commonly the binary seen on many Unix- and Linux-based systems to automatically run for backup and synchronization. This allows the malicious activity to evade detection.

File named "tsm32" and "tsm64" is responsible for propagating the miner and backdoor via SSH brute force, and capable of sending remote commands to download and execute the malware. Another file named as ".satan" is a shell script that installs the backdoor malware as a service.

In Linux, files that start with a period are hidden.

Download masscan tar file and unzip the masscan and scan the connected network subnet excluding private IP. The scan result was kept in a text file named input.txt for delete it.

Indicators of Compromise (IOCs)

CnC:

146[.]185[.]171[.]227:443

5[.]255[.]86[.]129:3333

54[.]37[.]70[.]249/[.]satan

54[.]37[.]70[.]249/rp

http://54[.]37[.]70[.]249/[.]x15cache

http://54[.]37[.]70[.]249/dota2[.]tar[.]gz

http://54[.]37[.]70[.]249/fiatlux-1[.]0[.]0[.]apk

http://mage[.]ignorelist[.]com/dota[.]tar[.]gz

mage[.]ignorelist[.]com

zergbase[.]mooo[.]com

SHA256:

rsync	0d71a39bbd666b5898c7121be63310e9fbc15ba16ad388011f38676a14e27809
ps	bb1c41a8b9df7535e66cf5be695e2d14e97096c4ddb2281ede49b5264de2df59
cron	4efec3c7b33fd857bf8ef38e767ac203167d842fdecbeee29e30e044f7c6e33d
anacron	66b79ebfe61b5baa5ed4effb2f459a865076acf889747dc82058ee24233411e2
tsm32	0191cf8ce2fbee0a69211826852338ff0ede2b5c65ae10a2b05dd34f675e3bae
tsm64	085d864f7f06f8f2eb840b32bdac7a9544153281ea563ef92623f3d0d6810e87

Advanced Persistent Threat (APT): APT-C-61

APT-C-61 attacks against South Asia: A series of attacks organized by an unknown APT were observed starting on early 2020. The target were important organizations such as national institutions, military industry, and scientific research. The APT used spear phishing emails and social engineering methods to infiltrate, spread malicious programs to the target device, secretly control the target device, and continue to steal sensitive files.

Attack Vectors

Harpoon emails and social engineering

Indicators of Compromise (IOCs)

CnC:

35[.]173[.]69[.]207
35[.]169[.]173[.]194
54[.]156[.]27[.]150
3[.]213[.]124[.]232
34[.]230[.]212[.]197
54[.]221[.]249[.]82
75[.]101[.]250[.]206
54[.]225[.]189[.]121
os[.]herokuapp[.]com
w0m[.]herokuapp[.]com
a0x[.]erokuapp[.]com
sysupdate[.]pythonanywhere[.]com
p92[.]herokuapp[.]com
fcdn[.]pythonanywhere[.]com

MD5:

512dc6478daa978b8cc1fd8886e48fcd
78f2f7f31c7a12841695d09217138d0d
9353dd2652a12f4c8b5333d11552d13d
b30cb1cfda5d401cb5352ced708c2ffd
e0231be9e17dec8d66ad50b96172153f

Advanced Persistent Threat (APT): Sidewinder

Sidewinder is a suspected threat actor group that has been active since at least 2012. They have been observed targeting government, military, and business entities throughout Asia,

Attack Vectors

Phishing emails
Credential phising
Phising Websites

Related Tools

PowerShell
Koadic

Indicators of Compromise (IOCs)

CnC:

185[.]99[.]133[.]106

SHA256:

98af6635138045cae3f29995a587d0c8a7f14446a9d10564677dd4a41372c3f1

Advanced Persistent Threat (APT): APT C-35 (DoNot Team)

In March 2017, the 360 Chasing Team found a sample of targeted attacks that confirmed the previously unknown sample of APT's attack actions, which the organization can now trace back at least in April 2016. The chasing team named the attack organization APT-C-35. The unique EHDevel malicious code framework used by the organization.

The actors use false personas to register their domains instead of opting for privacy protection services. Depending on the registrar service chosen, this could be seen as another cost control measure. The actors often used typo-squatting to slightly alter a legitimate domain name. In contrast, the registration information used accurate spelling, possibly indicating the domain naming was intentional, typos included. Each unique registrant usually registered only a few domains, but mistakenly reused phone numbers or the registration data portrayed a similar pattern across domains. Looking at shared IP infrastructure, it was easy to see the registration patterns and expand the network used by the attackers. The Donot Team relies heavily on subdomains. Nearly every domain discovered through the course of this investigation had multiple, unique subdomains and every malware sample analyzed communicated to subdomains. In at least two instances, the domain never resolved to an IP address. Instead, the malware used subdomains, which lead to active infrastructure. Many of the sub-domains only navigated to the third level, but other samples used overly complex subdomain structures down to the sixth or seventh level.

Related Tools

StealJob

Indicators of Compromise (IOCs)

SHA256:

8fff7f07ebf0a1e0a4eabdcf57744739f39de643d831c36416b663bd243590e1
d71a1d993e9515ec69a32f913c2a18f14cdb52ef06e4011c8622b5945440c1aa
f10f41bd38832596d4c449f81b9eb4129361aa4e4ebd4a8e8d2d8bf388934ca5
f331f67baa2650c426daae9dee6066029beb8b17253f26ad9ebbd3a64b2b6a37
d4e587b16fbc486a62cc33febd5438be3a9690afc1650af702ed42d00ebfd39e
62dfec7fe0025e8863c2252abb4ec1abdb4b916b76972910c6a47728bfb648a7
b874a158f019dc082a0069eb3f7e169fbec2b4f05b123eed62d81776a7ddb384
13f27543d03fd4bee3267bdc37300e578994f55edabc031de936ff476482ceb4
e726c07f3422aaee45187bae9edb1772146ccac50315264b86820db77b42b31c
5acfd1b49ae86ef66b94a3e0209a2d2a3592c31b57ccbaa4bb9540fcf3403574
57a9a17baaf61de5cffa8b2e2ec340a179e7e1cd70e046cbd832655c44bc7c1d

Advanced Persistent Threat (APT): AVADDON

Author of the Avaddon Ransomware is threat actor "Avaddon". First time this ransomware had been detected in the wild in June 2020.Threat actor has accounts on two underground forums - Exploit[.]in and xss[.]is. Both were registered in December 2019. First time he wrote a message on forums. In May 2020 on both forums - that was a task to test the administrator panel. In June he opened an affiliate program for Avaddon Ransomware.Threat actor has low activity on forums - all his activity is limited to threads about affiliate program.

Attack Vectors

Phishing campaigns through e-mails containing obfuscated JPEG or ZIP attachments (which are actually JavaScript or Excel with macros).
Remote Desktop Protocol (RDP)
Virtual Private Networks (VPN)

Indicators of Compromise (IOCs)

CnC:

http://avaddongun7rngel[.]onion/
http://avaddonbotrxmuyl[.]onion/
avaddongun7rngel[.]onion
tldrnet[.]top
myphotoload[.]com
avaddonbotrxmuyl[.]onion

MD5:

8f6e003f36c14be08558b18b7e2a80bf
043b13e02769b4ebdc679468fd650876
8e31bceb020d0cf8280052790908 76f5
4c5339d759262f9c228910067a608bb7
8ba941089eddb79337e3658d9dbe03c4
76c47ae35c6cc4ee40cbab0f81fc63e4
e92aeb5a50d6b84d47aa19cb9def7858

SHA-256:

68510adc7bd2bbc4438b4495c61ffd8a31c68fc53415a1a0ad8cbf70124a58f3
710fb650f05011b3a084d1b62c532e3f1f34cdd79c297b5394597e4bae820024
2946ef53c8fec94dcdf9d3a1afc077ee9a3869eacb0879cb082ee0ce3de6a2e7
5252cc9dd3a35f392cc50b298de47838298128f4a1924f9eb0756039ce1e4fa2
b39bfb51c0c8e2e216123ca619d45b995371cacf68d0ef7a8cd6b658aa8e68de
cc4d665c468bcb850baf9baab764bb58e8b0ddcb8a8274b6335db5af86af72fb
17396e9cf64ed18556a6510b6573b61ce0ac52428490ffdbd3e3a704e53fb7cd
2c5ecb43c0468b4724f7ea6c308531de9e0373678f611505b2f7a7ccbe03f2b8
21949184522a8258d58b90ff43cf440c713f1e62ba1491a5cd60460b4ae465c4
b8d6fd333973adb640649cab8c9e7575a17b5a8bc382e3335400d43a606a6253
fce637ff0885b82dcdb90c5625d4537d4905c2b1affce0e65cb3a5a052b35b5c

10c7127adb4ade624a3a6e3855c025e9b308c3a760a94db0b5109acdd4caa188
12bc439445f10a04b574d49ed8ccc405e2dfaa493747585439643e8a2129e5e5
f4f2a920a6f6454b3843b1ce69119ff91389ef398ba33622a1a35476aa81288b
167942b8b37615f543d58ee7ceacc174a545b5f4353ded2cb60400da729f645e
dccc689c986e357d5dbdc987e72e6b8a0e9017cbf347449b27c84b8b7b9d507a
036de5693b7e3821b0177a72a57e4ef87530c14999674a8fd967ee3cfe2aafc6
1a0753164f53de108ec44958bfa8f01a37d08e75b0436ed6b9961de9fd7bc669
50d97a35df81fc2c19b1f1893ae8ac552839b65adf662aa4dedd4923f5097608
66ebe6ca19059102193a67034f6f726783050571af484fd53c07fa5e36cdec43
7fd53917c03a9e2734abc50b43e2aabae04b440d1f88c89cf727e5e6ad9f040a
6616abb725c24307f4f062996edc5150079bc477acd4236a4f450e5835a20c62
4f198228806c897797647eecce0f92d4082476b82781183062a55c417c0bb197
9c9c4f20e4be9403e80e4f4bc09dcdcabdfcfd061950d7a226fa19b220e6d3bd
bcb69244dc69a152af4dca3849bb4f3ca634ad785926304c672dbf8a3c38e7bc
f3f4d4e4c6704788bc8954ca6f6ddc61b006aba89d5d384794f19424a3d24132
11dc4d55c095a7c2c3fe5b8e3e3612440ce9c068dd7c0d33503e62a5499e0dfc
94faa76502bb4342ed7cc3207b3158027807a01575436e2b683d4816842ed65d
7355912b1d15c772efe698fe04ac77d77e44862785b03ac3079570e9ab5fb50c
ea93ce421be8a2eba34752b8e8da4d241d671ef808a0f8e55a04ceca8ad5113f
b75f1a42db354e1552360fee17727198e3a70158ca1f78c8c41f2b92bde0114a
4a072c044993616658d1fdeddcf9ead501633fdf000cde18447301afa9b96e99
09bcfc62dd97d13cd7747066369bb5b4d9710307f718690598df79e11a196838
304945a98969e17d31a232cd7e3c42911f8ac3a33df69523dd51b5dd1cb0ae4d
6642eae47df9d87fdbe9356229989f37c6c88467ff47dfb6fde144c2563eb853
20bade9ac05d61c82189db69517bc3b7468c23818eb2470db6009dde7ac09985
a660ce6953d8c90f844efed48f30eacdaa21e872c11ab9e7dddd862ca4fdc40c
7dc1363a330c4ce09b662b84db879f0fa064378aa3d212173f64f4bd65bb0008
a481d2b64c546f68d55e1fd23e57ada80b6b4e2c3dd7b0466380dba465f3d318
a3fca43a08e02ec75524fbd841ac9908a37b05530e1d019c0defb278041660b6
29b5a12cda22a30533e22620ae89c4a36c9235714f4bad2e3944c38acb3c5eee
331177ca9c2bf0c6ac4acd5d2d40c77991bb5edb6e546913528b1665d8b501f3
46a8c1e768f632d69d06bfbd93932d102965c9e3f7c37d4a92e30aaeca905675
557809ad788cd565c7515ce150109f8bddcdec02ad383039b5401305a479562c
56835a799dde8d9ec2d34493fb7207bff069c0deac9942ece427721853709d91
aea6fc31e3a6df3fae067535ab6dc83518ef39662865ec6b1a7bd65bd640b137
0a052eff71641ff91897af5bdecb4a98ed3cb32bcb6ff86c4396b1e3ceee0184
66fdfebe84bdcef5389b066474661cfbcf5e71e6036deaa4b4b6fc1f43bf8892
94fefbae1f1c369c6fcc718d0ea40828b98f55b18c8b4fa68915ceef2d725707
4bf54e4e4c36d6509470ba7a45fd03b68f8432ca3e926b269a195196d2a01d5f
9d32616dd8061f94ff7a0fc575b9b2a9e3e111fad732c81ce8523f896527aa47
21b7b150139c8c228f2b2d342e5de08526b0758a653c23fd7bf2b4d51639f0ea
8c0d535176320f2391ff86beeed00fc3a2987b055b83c7969d8730071477b19d
75066a2982794eff05bb053ba53e7a018faa0b6151f8a47b35f4153e9e5c74ad

982d910b04625e284fc6ff5217f6708433af0939d6ac2301cd88ceea3e362b87
05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
f1be81055877d185ed1e09e8e3356d82eee388875ce9f948ebf7712c749f9819
5a47a89a870d7db244c76da43887e33c9ee4b26f9972878b1a6616be0302439f
0ff4058f709d278ed662719b9627618c48e7a656c59f6bfecda9081c7cbd742b
5266b38ad229e89f9afd2464b8f609d33c0f068dc7fe54d9cdc06624826cedc5
b08247c9c0cd3bd8f805f49e08131d78be25e9e8691aab2fab74bfee8fab6a9d
b3fa794ac8d4b8577a61109b96262fd83d9ebf6717d006cb9b5e5638cb234b70
146e554f0d56db9a88224cd6921744fdfe1f8ee4a9e3ac79711f9ab15f9d3c7f
165c5c883fd4fd36758bcba6baf2faffb77d2f4872ffd5ee918a16f91de5a8a8
28adb5fa487a7d726b8bad629736641aadbdacca5e4f417acc791d0e853924a7
d1c1dfa0117fc595419464578959feb4c459ab99a498e0cb66cee626ceff6835
fa4626e2c5984d7868a685c5102530bd8260d0b31ef06d2ce2da7636da48d2d6
4fd72c550987c7638e727c9d84b4940692bf94e101d3f5746bc4a8f377e49b37
c06e2e3fe09f92007ff589e46a57cb8efa1fe261d7b8193190eb648cf7961a4b
210c7f7330f66a248d3cb90bfeefcdb68d5771b1bfc976c7607deedf626d4391
a73900ed8479bfcfbeff20c95dfdb941aa67ea24aeebd07e5e4162d6f4ffb50d
c6add04be76ec96445a2418b6e7cc52faa4671ceea98e1f9050ced82e54df5f4
a4c73aabb9e37b06cebb95b339a24b567ee6c996d129ad9b4fcb6ac029cc2fee
cbb0d1d2a9a93464e0b77844088875ef75bb4904efa189ad7d7d15d3dde4d800

List of CVE commonly exploited by AVADDON APT:

CVE-2018-13379

An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.

CVE-2017-0144

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Advanced Persistent Threat (APT): BALBESI

This group of cybercriminals is involved in compromising corporate networks using the "Cobalt Strike" framework and the publicly available tool - Mimikatz. Based on our Intel this group consists of at least four members with nick-names: balbes; nicko; finamina; brute. This group is also known as "hancitor". Other aliases of group: TA511, MAN1, Moskalvzapoe. Cuba ransomware was found in at least one of compromised network. We suppose that they are partners of RaaS Cuba/Buran/ Zeppellin.

Related Tools:

Cobalt Strike
Mimikatz
Buran
SystemBC
FickerStealer
Cuba
LaZagne
NBTScan

Indicators of Compromise (IOCs)

CnC:

http://185[.]153[.]199[.]166/a
http://185[.]153[.]199[.]166/match
http://144[.]202[.]42[.]216/download/svchost[.]exe
torbavzubi[.]com
winsysmon[.]us
trampampooh[.]com
lajasinfoy[.]com
31[.]44[.]184[.]53
31[.]44[.]184[.]55
185[.]153[.]199[.]166
144[.]202[.]42[.]216
31[.]44[.]184[.]49
185[.]153[.]196[.]214
31[.]44[.]184[.]51
84[.]238[.]168[.]253

MD5:

a7a7f626f5808ae112fa85bc530ad724
5381a11ff3bc4ab0daaf590b61b032d6
b41df38c683ccbfe27d3e9ee4dc88e63
fc9b875bee6ea712519889a8ee68d3aa
522bc39647dd316db705de3995099f2d
53b91edd8c93cb49ff2003a87aafc1a2
5ec3aacd4c91f6d9232ce4b77b30afa9

73a8e5cf8c5e9870f459c376ff345c0c
a8d7ce3bdbebb466c06493028d9c5824
ca10d3fa3609170e675061355ee3e228
19eeed1819efbdcbc115bbec3f71e1c3
1a08104065ec8968e34dce8cfdd568ed
1dcf4b7c10c4a6263e521a19a3016ae5
42b9cdd896b72f6fdcc4fbf728064321
3ec590d5377bc6f4b0cae4a93efe5fbb
76a5b1c4ca4c02e98d6b9fbbf3ae8229
9c01d5ced2dbaf1300a30ab1cb831cde
a0d4f3fdee72c23689c9f0153401c245
02675f4692e8d057ae6457c7cc1a7716
224f383c45814dfde345ea6aebca3443
3e37d13807117228e270ddcce81f33a3
49a4724fb2fb246dc66c3f870f454627
4c32ef0836a0af7025e97c6253054bca
5ce73c5f0e006f2108f3cc941c369f37
bb9515e25c9f1c75fcb22f59874df0bf
6d29b4a62ced9ad7a2b62965d9174b12
4679ae807e28bfae312ecc3a08d49e24
7d6a9e60d582644806a5848c142aa06b
ac97736f0a17fe7c1a882f69f151550d
b56f17be50a4d03e098cc754e88c6b1d
ca2a224c04cf27ccb2d71d8db8c34330
4765e9d15bbe3ad37bc26e64f0a4220e
4b99e9a0b91ea0b7c0ec63ee162a8592
5f92234ff1b9a919765702258779bd61
726c868f05045bcc615cecb943e0b12f
9d562703fc155fd22b77526cfd3b1fcd
e308168a027836a2f792ac404e1109e3
ed04bbeed85508ddc1c4d006c4366dbf
fb5618c86e5298276608be1cded197b2
ef4685625d72ba2f3e33f5f2809bcd3e
fd977325006c7f0e7aa740215239cebf
6ce17907e6b6a965d9de304d8390797a
fd235fdc95043a3102ebd1177e6f9335
6d29b4a62ced9ad7a2b62965d9174b12
bb9515e25c9f1c75fcb22f59874df0bf
7d6a9e60d582644806a5848c142aa06b
ca2a224c04cf27ccb2d71d8db8c34330
fb5618c86e5298276608be1cded197b2
ef4685625d72ba2f3e33f5f2809bcd3e
22c166b2c803b02a46fa40fe5d954138
f07245cff132533077ea757ec74881f8
e8e98e4ee3bc8c8b0b1873c57ba0f6ac
ee4525f0933df3ead3bc9e9235b344f5
ac1094cb70c4d2a7257690311e685482

ad16a08683b01cd1c4feb955703c6adb
75973401c8a3bbb8b932d9747a9c1b4d
02e5bde0dcd1c9a966730a80a8b78a00
1017612d10f4f45ac46e7d24a759925c
3d422dc23eae2bc7b1ff5541df4ba358
16b870384d98b3a4a53be52bfe9359b6
329892fec47136dd6f6b4619eeb0a05d
343e489b8b1df522e26f3efd42d639a5
3b07d59318eaad00547aa84d4308dfeb
47c8aa7fac917a012ef125036dc100bb
4ab5f1631994378f9612b384729e6f1e
6832cc63eee8b73c851fc1d07b262847
88a725e00f5613dd3bfd023ae0fa8526
ca1ec4bcbd0361b48d32f124cd04bf53
034ae5ce80d8a314e0e787b6209610a5
07df365742fe41605b056606009e2484
e4f3456183c43a9a302f2a6dd9885eb2
5d9227fdb5b76d0207bd412873f6e85e
7ecf0136784b5f85e76f9328991eda3c
32c16bf83336bfeb806c2e6bfa6976a2
11107a24aba9cdb3a2de8634d746cd3f
d349825ccc56ddd5991a895608affc59
fdb92bc5ab549b8802adbc1922159109
babdfbb9d06290a8cb83a0937a90514b
cb8edfb71a35d4b313ae3822cf20f7ca
529ba8dd5d1bcc77069a645cd16ae47a
737c907eb26e851f9f7fead30bd2c374
b4b066c2714e7d1eec9e421624e69480
ff31679a6b7b825cbdc27abcb72a1625
812e761a3098b2ac4613385a0891bf70
4348b7c5734645e465dc51817e7ca58a
63fc7a15ec00a7b60979499bcb995a19
064089ee5995aa32412b66386540c3e0
3683294a854eb511c15296d0d223a6ec
5cf4297016fdc9b7ee930eff10247ee6

SHA-256:

b35a772967050f781181143d0822f13591965a1d06d01c469230cb0171111b44
6759626abfc08f7c0233609cae8cecdae35fd227e037a64bb62d5a5266599fa0
6caf06e33a9cda5c0f564bc8c0b4ef9e95bd043f275b02b13f4edaba90aa28e9
45a30caa46cf531121e81ee34bd6df322ae721de8a2b47a0503419faaffcf54b
79c561b8d4d2c79f80ec54fc057eac186685a1cbd2767ac27ecf4c01f2fa770d
25155d668b97e976fbbdfc1f45890403f59114e6b4323c3dcb124ec88a6e90bf
79c561b8d4d2c79f80ec54fc057eac186685a1cbd2767ac27ecf4c01f2fa770d
65f3162d46b247a9b79ace4c19e6ad81c5aa00a2229a6557f377f9ced697df01
7ce1766f2c3edff24b2278dc0fda0a311312bc2fb6dabfa91859d23d4dc119bd

5eaa77c015e6b0262ca87865d83340cd93439524f192b70e0075f1736f13622a
fb6cdb2eb3ee4dcaee54464d68f4b5ee76fa65ca2ffdddb6fc4f43d0955309f8
273bda279eb54c1f3afb45a4ecb89f26bb59efbe7cbab9e790e3f9696b625933
894405332300de6351e31591348a15495cd1ed72583f136c2a9331b85a339cc4
81d7f58b5dd232cd8f8788faf8d2ecbe8cbe48ed6b89f60f5d9f364d8b54d7eb
53ccef513983bb1ed50c8d1179dcf41a930f670b6379ab7ecd7d7c87e8d56168
31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc

Advanced Persistent Threat (APT): APT41

The cybercrime group APT41 (also known as BARIUM; Winnti; LEAD; WICKED SPIDER; WICKED PANDA; Blackfly; Suckfly; Winnti Umbrella; Double Dragon) is a criminal group with dual attack goal (cyber espionage and financial benefit) that has been active since at least 2007. APT41 specializes in stealing digital certificates for use in operations involving user data theft (cyber espionage), as well as placing cryptominers and ransomware on devices. Previously, the group's goals were also currency manipulation in online games and theft of intellectual property. The use of digital certificates issued for legitimate gaming software and obtained by compromising the manufacturer in attacks is one of the main features of this group. Certificates are either delivered by agreement with the group or distributed commercially in the shadow segment of the network. The malware was distributed in the DLL library for a 64-bit version of Windows form and had the functionality of a Remote Administration Tool (RAT). Third-party utilities and frameworks were also used. The use of malware attributed to other groups has been noticed. APT41 considered to be a few APT groups conglomerate which includes Group 72, PassCV, APT17

Related Tools

ASPXSpy
BITSAdmin
BLACKCOFFEE
Certutil
China Chopper
Cobalt Strike
Derusbi
Empire
ZxShell
Winnti for Linux
ShadowPad
ROCKBOOT
Pwdump
PowerSploit
PlugX
MESSAGETAP
gh0st RAT
FTP
Ipconfig
Mimikatz
Net
Netstat
LaZagne

NBTScan

Indicators of Compromise (IOCs)

CnC:

http://54[.]245[.]195[.]101/mess[.]exe
http://54[.]245[.]195[.]101/test[.]rtf
http://signup[.]facebooknavigation[.]com/
http://54[.]245[.]195[.]101/sign[.]exe
http://118[.]193[.]37[.]157/log[.]dll
http://ieee[.]boeing-job[.]com/1
http://ieee[.]boeing-job[.]com/0
http://149[.]28[.]23[.]32:65534/Complaint[.]rar
http://www[.]btdot[.]com/bbs/data/boot1[.]gif
http://www[.]funzone[.]co[.]kr/bbs/data/boot1[.]gif
http://www[.]gbutterfly[.]com/bbs/data/boot1[.]gif
http://www[.]srsr[.]co[.]kr/bbs2/data/boot1[.]gif
http://boot[.]ncook[.]net/bbs/data/boot1[.]gif
https://github[.]com/Yt1g3r/CVE-2019-3396_EXP/blob/master/cmd[.]vm
http://67[.]229[.]97[.]229/pass_sqzr[.]jsp
https://bugcheck[.]xigncodeservice[.]com/Common/Lib/Common_bsod[.]php
http://www[.]battllestategames[.]com/jquery
https://www[.]battllestategames[.]com:8443/jquery-3[.]3[.]1[.]min[.]js
http://www[.]battllestategames[.]com/jquery-3[.]3[.]1[.]min[.]js
http://coivo2xo[.]livehost[.]live/access/?version=4&lid=1582502724&token=cnnnidaighjjhobannhffjehgkgnmnochcecmdcoaahcheohgdndgipgmecnofjmmnmnkhlbacejlkjbloifejgiepngmlefmeijpjlpdgjebmphioaiedkddbiniomdkokbojbdlcjfgchhnnomgnmgpkbibchlehjmnaafndlapibljjmkmpooehfgghkgbjhhgmhbbaikebggpeojbglbdofgkbjkhlpoijpgfdlojgmkblhnopdfjhifaeme
https://coivotek[.]livehost[.]live/access/?version=4&lid=1582502724&token=hkmoblodbbckhkaaokfdlbfihpaodddoldbjimgjfnlhednammmhafdcleiohbemednhieigngleicfecddeikeaekjfdkeopglpjholodiicbpghlpkkkiddbadlmgngeomaobppefbmcepmelogdcafkpfbhndhmlghphaobeenpogakdojioaemeiggmdiofkaekogikecbooippdklkjnhfbepffmjdekkhaabgcmhajmapihmmnmkbjnmpe
https://coivo2xo[.]livehost[.]live/beat
https://coivo2xo[.]livehost[.]live/9jVd
https://coivo2xo[.]livehost[.]live/access/?version=4&lid=1582502724&token=dgmppklkgcahinpmmkplfbmednfekhghdnnkfglelnbjndnnbonfflaammdghgdaffdbiijpmefidhbnhjjblfjelkbglpdkgjejljakoipnjiacnoaifpgnhdeljlbpghhdgohcnigpinfoghcodhondnkeknegajcgledoejgidinjebjaifhipghnoodapdhoggbhfchjanffpphbejpanekpljllmdbbodabdkefnhebijeigdkiobhjpinc
https://coivotek[.]livehost[.]live/access/?version=4&lid=1582502724&token=acplbndbidcjjgcljecjnohgflbepglagcflhejokcfbdohbhllnmphobnopnbmcgnpipoijbamijckdjijefoipokccajodmbbbobbniildfafobllmbkkabbjikolgehgnfnehojocpjgkianjknlbgdkoakgfhjmlcicilmjjdaidlegcajaoakhiolmkfaobdmlilghgcijiipplldcebfbmcnnmibeolnaaaklcnlleokdeekdfkldgeifd

https://doc[.]goog1eweb[.]com:80/settings
http://168[.]106[.]1[.]1/http:/7hln9yr3y6[.]symantecupd[.]com/upadminx/
http://7hln9yr3y6[.]symantecupd[.]com/upadminx/
http://ftp[.]fiysaa[.]com/download/TS[.]zip
http://66[.]42[.]48[.]186:65500/electronic_resume[.]pdf[.]rar
http://66[.]42[.]48[.]186:65500/video[.]rar
http://66[.]42[.]48[.]186:65500/Photo[.]rar
http://66[.]42[.]48[.]186:8080/http:/66[.]42[.]48[.]186/QUERY/en-us/msdn/
http://www[.]yandex2unitedstated[.]dynamic-dns[.]net/news[.]php?type=1&hash=6fc29fee2b56620d4ff2ed750f5ad232&time=02:12:55
http://www[.]oseupdate[.]dns-dns[.]com/news[.]php?type=1&hash=d41d8cd98f00b204e9800998ecf8427e&time=10:32:17
http://agent[.]my-homeip[.]net/ks8d192[.]168[.]122[.]143akspbu[.]txt
http://g00gle_jp[.]dynamic-dns[.]net/news[.]php?type=1&hash=d41d8cd98f00b204e9800998ecf8427e&time=11:59:58
http://www[.]oseupdate[.]dns-dns[.]com/news[.]php?type=1&hash=d41d8cd98f00b204e9800998ecf8427e&time=10:19:30
http://agent[.]my-homeip[.]net:8000/ks8d0[.]0[.]0[.]0akspbu[.]txt
googlerenewals[.]net
facebooknavigation[.]com
cdn[.]igooglefiles[.]com
xn--360tmp-k02m[.]tmp[.]googlecustomservice[.]com
tmp[.]googlecustomservice[.]com
find2find[.]com
luckhairs[.]com
bot[.]new[.]googlecustomservice[.]com
www[.]googlecustomservice[.]com
new[.]googlecustomservice[.]com
bot[.]googlecustomservice[.]com
igooglefiles[.]com
pornsee[.]tv
signup[.]facebooknavigation[.]com
game[.]googlecustomservice[.]com
www[.]uk[.]igooglefiles[.]com
xn--360tmp-k02m[.]www[.]googlecustomservice[.]com
ftp[.]googlecustomservice[.]com
vnew[.]googlecustomservice[.]com
hk[.]uk[.]igooglefiles[.]com
lead1[.]uk[.]igooglefiles[.]com
cdn[.]uk[.]igooglefiles[.]com
uk[.]uk[.]igooglefiles[.]com
uk[.]igooglefiles[.]com
news[.]aolonline[.]cc

googlesoftservice[.]net
tiwwter[.]net
jp[.]googlerenewals[.]net
xn--360tmp-k02m[.]new[.]googlecustomservice[.]com
mess[.]googlerenewals[.]net
us[.]igooglefiles[.]com
xn--360tmp-k02m[.]googlecustomservice[.]com
us[.]uk[.]igooglefiles[.]com
show[.]uk[.]igooglefiles[.]com
news[.]googlesoftservice[.]net
news[.]facebooknavigation[.]com
aolonline[.]cc
googlecustomservice[.]com
sexyjapan[.]ddns[.]info
bswan[.]authorizeddns[.]org
pd[.]zzux[.]com
pic[.]x24hr[.]com
xnews[.]mypicture[.]info
xx0ssd[.]isasecret[.]com
ad[.]lflink[.]com
zxerbqr[.]zyns[.]com
id[.]serveuser[.]com
biller[.]zzux[.]com
images[.]h1x[.]com
sport[.]wikaba[.]com
voda[.]dns04[.]com
nxead[.]itemdb[.]com
winner[.]ikwb[.]com
firejun[.]freeddns[.]com
users[.]fartit[.]com
netsysdom[.]dynamic-dns[.]net
newnw[.]4pu[.]com
cat[.]moneyhome[.]biz
token[.]dns04[.]com
wpblog[.]dynamic-dns[.]net
cronous[.]wikaba[.]com
xx0xx[.]dnset[.]com
hike[.]dns04[.]com
remotetest[.]dynamic-dns[.]net
free[.]itsaol[.]com
happysky[.]edns[.]biz
gold[.]mrbonus[.]com
readme[.]myddns[.]com
images[.]ikwb[.]com
xnews[.]ikwb[.]com
remoteset[.]zyns[.]com
udm[.]dns05[.]com

ddns[.]4pu[.]com
faceb00k[.]ns01[.]info
patch[.]itsaol[.]com
wordpressb[.]justdied[.]com
pd1[.]dynamic-dns[.]net
forum1[.]zzux[.]com
faceb0ok[.]2waky[.]com
pachost[.]wikaba[.]com
gold[.]bigmoney[.]biz
ddxsn[.]ddns[.]info
item[.]itemdb[.]com
excharge[.]sexxxy[.]biz
pachost[.]dynamic-dns[.]net
wordpr[.]dynamic-dns[.]net
firejun[.]freetcp[.]com
mtnl1[.]dynamic-dns[.]net
udomaincom[.]dynamic-dns[.]net
vada[.]my03[.]com
vb[.]xxuz[.]com
firejun[.]myddns[.]com
wwwss[.]mrbasic[.]com
pdbana[.]dynamic-dns[.]net
purdue[.]dynamic-dns[.]net
rem0te[.]edns[.]biz
wxxxs[.]mefound[.]com
clients[.]cleansite[.]info
hirez[.]ddns[.]info
image[.]x24hr[.]com
splash[.]dns04[.]com
bschery[.]zzux[.]com
help[.]wikaba[.]com
xznews[.]zzux[.]com
linkedin[.]2waky[.]com
foods[.]x24hr[.]com
xvideo[.]mrslove[.]com
testtest[.]x24hr[.]com
l1nkedin[.]ns01[.]biz
cipp[.]dns04[.]com
money[.]moneyhome[.]biz
udomain[.]mrbonus[.]com
mxmail[.]esmtp[.]biz
dr0pb0x[.]zyns[.]com
dropbox[.]dns2[.]us
newpic[.]sexxxy[.]biz
news[.]mrbonus[.]com
wind[.]ikwb[.]com
winner[.]serveuser[.]com

bsnl1[.]dynamic-dns[.]net
spyd123[.]dynamic-dns[.]net
foryou[.]x24hr[.]com
pic[.]4pu[.]com
www[.]pneword[.]net
cigy2jft92[.]kasprsky[.]info
update[.]ilastname[.]com
ns[.]mircosoftbox[.]com
ns[.]upgradsource[.]com
update[.]serverbye[.]com
update[.]upgradsource[.]com
service[.]dns22[.]ml
ns1[.]colunm[.]tk
ns2[.]colunm[.]tk
colunm[.]tk
rss[.]6600[.]org
sshd[.]8866[.]org
ftpd[.]6600[.]org
ftpd[.]9966[.]org
pptp[.]7766[.]org
ieee[.]boeing-job[.]com
orzk[.]net
o5team[.]com
moeskin[.]com
a[.]bingtok[.]com
a[.]sqlyon[.]com
a[.]sqlyon[.]net
youfunv[.]com
heixbai[.]com
is2sec[.]com
akibaol[.]com
moegoo[.]com
010sec[.]com
exchange[.]longmusic[.]com
alibaba[.]zzux[.]com
cs[.]colunm[.]tk
www[.]btdot[.]com
www[.]funzone[.]co[.]kr
www[.]gbutterfly[.]com
www[.]srsr[.]co[.]kr
boot[.]ncook[.]net
dnsgogle[.]com
paniesx[.]com
nylalobghyhirgh[.]com
xmponmzmxkxkh[.]com
notped[.]com
operatingbox[.]com

techniciantext[.]com
github[.]com
cake[.]pilutce[.]com
pool[.]boreye[.]com
ssl[.]dyn-dns[.]com
dns1-1[.]7release[.]com
iron[.]tenchier[.]com
svn-dns[.]ahnlabinc[.]com
xp101[.]dyn-dns[.]com
coco[.]miniast[.]com
kasparsky[.]net
Infestexe[.]com
macfee[.]ga
update[.]ageofwuxia[.]net
symanteclabs[.]com
win7update[.]net
ageofwuxia[.]org
micros0ff[.]com
exe[.]com
agegamepay[.]com
ibmupdate[.]com
byeserver[.]com
micros0tf[.]com
gamewushu[.]com
bugcheck[.]xigncodeservice[.]com
ageofwuxia[.]info
linux-update[.]net
ageofwuxia[.]com
up[.]linux-headers[.]com
mm[.]portomnail[.]com
back[.]rooter[.]tk
www[.]battllestategames[.]com
update[.]facebookdocs[.]com
mail[.]nexongame[.]net
a1[.]reegame[.]net
tank[.]hja63[.]com
q[.]gasoft[.]us
versiontt[.]no-ip[.]org
mail[.]gasoft[.]us
kor[.]xxoo[.]co
nx[.]jcrsoft[.]com
ws[.]gcgame[.]info
dns[.]nhnclass[.]com
nx[.]xxoo[.]co
ftp[.]gcgame[.]info
nexoncorp[.]us
smtp[.]nexoncorp[.]us

bcc[.]hja63[.]com
wm[.]myxxoo[.]com
wm[.]googleclick[.]net
mail[.]zzsoft[.]info
usa[.]nexongame[.]net
help[.]googleclick[.]net
mail[.]jcrsoft[.]com
google[.]x3322[.]org
perl[.]mynetav[.]net
kr[.]reegame[.]net
tcp[.]nhntech[.]com
help[.]ibm-support[.]net
tw[.]reegame[.]net
ap[.]googleclick[.]net
pass1[.]joymax[.]in
zb[.]mynetav[.]net
ad[.]gasoft[.]us
ns5[.]msftncsl[.]com
winlogon[.]net
ru[.]gcgame[.]info
wm[.]ibm-support[.]net
ns4[.]msftncsl[.]com
gf[.]jcrsoft[.]com
imap[.]zzsoft[.]info
gongyi[.]co
gunz[.]gcgame[.]info
dell-support[.]org
pop[.]cjinternet[.]us
hja63[.]com
els[.]jcrsoft[.]com
googletrait[.]com
q[.]gcgame[.]info
my[.]zzsoft[.]info
id[.]naverpulic[.]com
openhost[.]webhop[.]net
mini[.]reegame[.]net
ed[.]xxoo[.]co
also[.]msftncsl[.]com
ru[.]cjinternet[.]us
nhnclub[.]com
ijj[.]conimes[.]com
test[.]reegame[.]net
ap[.]myxxoo[.]com
cg[.]apanku[.]com
ns1[.]naverpulic[.]com
ns1[.]java-ssl[.]com
www[.]googletrait[.]com

pass2[.]nexongame[.]net
bot[.]jgame[.]in
ftp[.]hja63[.]com
dns01[.]dyndns-work[.]com
ns2[.]nhnclass[.]com
xxoo[.]co
mynetav[.]net
pass2[.]hangame[.]co[.]uk
imap[.]gcgame[.]info
ball[.]reegame[.]net
kr[.]xxoo[.]co
gasoft[.]us
ro[.]xxoo[.]co
egi[.]mynetav[.]net
holleword[.]3322[.]org
apanku[.]com
wi[.]zzsoft[.]info
nx[.]cjinternet[.]us
zz[.]xxoo[.]co
imc[.]zzsoft[.]info
pop[.]gasoft[.]us
osk[.]zzsoft[.]info
new[.]nexoncorp[.]us
ro[.]myxxoo[.]com
rh[.]gcgame[.]info
swordwind[.]net
lp[.]xxoo[.]co
zm[.]gasoft[.]us
jcrsoft[.]com
service[.]googlefiles[.]net
ftp[.]nexoncorp[.]us
www[.]jcrsoft[.]com
nx2[.]joymax[.]in
dl-adobe[.]com
ns3[.]msftncsl[.]com
support[.]nexononline[.]com
udp[.]myxxoo[.]com
w[.]zzsoft[.]info
pp[.]ibm-support[.]net
isatap[.]dyndns[.]org
tt[.]conimes[.]com
btg[.]mynetav[.]net
dns2[.]msftncsl[.]com
lp[.]apanku[.]com
lp[.]zzsoft[.]info
usp[.]xxoo[.]co
pop[.]nexoncorp[.]us

haj[.]mynetav[.]net
dbo[.]gasoft[.]us
ftp[.]mynetav[.]net
us[.]nhntech[.]com
mg[.]jcrsoft[.]com
new[.]myxxoo[.]com
rh[.]jcrsoft[.]com
q[.]zzsoft[.]info
nd[.]gasoft[.]us
ro[.]hja63[.]com
ns1[.]msftncsl[.]com
update[.]reegame[.]net
god[.]zzsoft[.]info
goqc[.]xxoo[.]co
ns3[.]nhnclass[.]com
2m[.]reegame[.]net
sg[.]java-ssl[.]com
nx2[.]interdriver[.]net
a[.]gcgame[.]info
imap[.]cjinternet[.]us
ca[.]zzsoft[.]info
tw[.]java-ssl[.]com
sn[.]jcrsoft[.]com
service[.]interdriver[.]net
ava[.]apanku[.]com
as[.]xxoo[.]co
ckts[.]mynetav[.]net
kr[.]zzsoft[.]info
mir[.]reegame[.]net
xy[.]hja63[.]com
ftp[.]gasoft[.]us
www[.]joymax[.]in
ftp[.]cjinternet[.]us
qc[.]zzsoft[.]info
fm[.]hja63[.]com
e[.]zzsoft[.]info
udp[.]ibm-support[.]net
wh[.]jcrsoft[.]com
shoes[.]sellClassics[.]com
ar[.]apanku[.]com
w80[.]xxoo[.]co
ns2[.]msftncsl[.]com
ynk[.]xxoo[.]co
tw[.]hja63[.]com
pass1[.]reegame[.]net
bar[.]zzsoft[.]info
pay[.]gcgame[.]info

gs[.]xxoo[.]co
xx[.]hja63[.]com
ree[.]reegame[.]net
interdriver[.]net
qs[.]nexongame[.]net
webadmin[.]dnsdojo[.]net
dns[.]msftncsl[.]com
pass1[.]nexongame[.]net
offices[.]dyndns-office[.]com
sf[.]cjinternet[.]us
smtp[.]zzsoft[.]info
ssh[.]joymax[.]in
e[.]hja63[.]com
pda[.]gasoft[.]us
wsafelogin[.]com
han[.]zzsoft[.]info
nhntech[.]com
sm[.]gcgame[.]info
eudb[.]reegame[.]net
iyy[.]conimes[.]com
oa[.]nexoncorp[.]us
e[.]jcrsoft[.]com
sl[.]myxxoo[.]com
usa[.]xxoo[.]co
hsb[.]mynetav[.]net
docs[.]naverpulic[.]com
jc[.]nhntech[.]com
mail[.]hja63[.]com
mail[.]nexoncorp[.]us
as[.]cjinternet[.]us
e[.]gcgame[.]info
db[.]nexongame[.]net
mail[.]gcgame[.]info
nc[.]feelids[.]com
googleclick[.]net
ns1[.]nhnclass[.]com
stmp[.]msftncsl[.]com
msftncsl[.]com
us[.]msftncsl[.]com
ns2[.]naverpulic[.]com
pop[.]zzsoft[.]info
on[.]xxoo[.]co
kerberos[.]dnsalias[.]com
a1[.]googletrait[.]com
th[.]xxoo[.]co
tvads01[.]dyndns[.]tv
lp[.]gasoft[.]us

nx3[.]googlefiles[.]net
joymax[.]in
www[.]reegame[.]net
myxxoo[.]com
ads01[.]dyndns-web[.]com
www[.]mynetav[.]net
rw[.]nhntech[.]com
ka[.]jcrsoft[.]com
us[.]xxoo[.]co
fax[.]cjinternet[.]us
nx2[.]intercpu[.]com
windows[.]doomdns[.]com
ka[.]zzsoft[.]info
jjevil[.]com
nexongame[.]net
est[.]gcgame[.]info
newpic[.]dyndns[.]tv
nsqc[.]xxoo[.]co
nexon[.]hangame[.]co[.]uk
smtp[.]gasoft[.]us
my[.]gasoft[.]us
dns[.]nhnclub[.]com
jrun[.]hja63[.]com
tv[.]mynetav[.]net
ogp[.]reegame[.]net
docs[.]nhnclub[.]com
updata-microsoft[.]com
hangame[.]co[.]uk
mx[.]hja63[.]com
www2[.]mynetav[.]net
imap[.]gasoft[.]us
pda[.]zzsoft[.]info
bar[.]gasoft[.]us
apps[.]mynetav[.]net
mail[.]7niu[.]com
game[.]joymax[.]in
vtc[.]gasoft[.]us
tv3[.]mynetav[.]net
dbo[.]gcgame[.]info
id[.]java-ssl[.]com
osk[.]jcrsoft[.]com
mini[.]googletrait[.]com
tcpiah[.]googleclick[.]net
pop[.]hangame[.]co[.]uk
eya[.]zzsoft[.]info
wapqq[.]3322[.]org
aion[.]reegame[.]net

su[.]cjinternet[.]us
cc[.]xxoo[.]co
brqc[.]xxoo[.]co
wi[.]gcgame[.]info
smtp[.]cjinternet[.]us
imap[.]hja63[.]com
googlefiles[.]net
ssl[.]msftncsl[.]com
ns1[.]nhnclub[.]com
uni[.]vip-webmail[.]com
ip[.]xxoo[.]co
mail[.]joymax[.]in
conimes[.]com
xss[.]gongyi[.]co
tech[.]ibm-support[.]net
tt[.]xxoo[.]co
eya[.]jcrsoft[.]com
zzsoft[.]info
dns--google[.]com
l53[.]xxoo[.]co
smtp[.]hja63[.]com
nx3[.]interdriver[.]net
ads01[.]dyndns-pics[.]com
pop[.]gcgame[.]info
ac[.]xxoo[.]co
udp[.]googleclick[.]net
nd[.]xxoo[.]co
dns[.]java-ssl[.]com
mailes[.]dyndns-mail[.]com
a[.]zzsoft[.]info
moon[.]reegame[.]net
est[.]gasoft[.]us
dbo[.]zzsoft[.]info
gcgame[.]info
support[.]interdriver[.]net
pda[.]gcgame[.]info
cpu[.]4pu[.]com
pda[.]jcrsoft[.]com
ns9[.]msftncsl[.]com
ns2[.]java-ssl[.]com
alta[.]apanku[.]com
pass1[.]googletrait[.]com
www[.]nexoncorp[.]us
my[.]reegame[.]net
login[.]joymax[.]in
guys[.]mynetav[.]net
ava[.]zzsoft[.]info

jp[.]xxoo[.]co
ros[.]zzsoft[.]info
x64[.]reegame[.]net
rf[.]gcgame[.]info
pda[.]hja63[.]com
kr-mail[.]com
xv[.]apanku[.]com
imap[.]nexoncorp[.]us
t3[.]myxxoo[.]com
gn[.]xxoo[.]co
crl[.]nhntech[.]com
pwd[.]nhntech[.]com
hk[.]zzsoft[.]info
blog[.]mynetav[.]net
br[.]reegame[.]net
e[.]gasoft[.]us
br[.]xxoo[.]co
jp[.]jcrsoft[.]com
ga[.]nhntech[.]com
update[.]ddns[.]net
baesystems[.]conimes[.]com
ns2[.]nhnclub[.]com
intercpu[.]com
ix[.]xxoo[.]co
qc[.]xxoo[.]co
hp-supports[.]com
mail[.]cjinternet[.]us
gamenow[.]8800[.]org
sg[.]xxoo[.]co
ns7[.]msftncsl[.]com
udp[.]nhntech[.]com
club[.]cjinternet[.]us
t3[.]jcrsoft[.]com
kr[.]hja63[.]com
dns[.]naverpulic[.]com
vip-webmail[.]com
tho[.]hja63[.]com
hk[.]hja63[.]com
hansoft[.]sunsb[.]net
cj[.]jcrsoft[.]com
mail[.]msftncsl[.]com
mini[.]msftncsl[.]com
udp[.]jjevil[.]com
pop[.]jcrsoft[.]com
nexon[.]nexongame[.]net
file[.]googlefiles[.]net
est[.]zzsoft[.]info

hansoft[.]does-it[.]net
w53[.]myxxoo[.]com
mini[.]nexongame[.]net
wyqc[.]xxoo[.]co
www[.]nexongame[.]net
xl[.]apanku[.]com
w53[.]xxoo[.]co
service[.]hp-supports[.]com
gm[.]gasoft[.]us
ftp[.]jcrsoft[.]com
lftv[.]mynetav[.]net
nx3[.]intercpu[.]com
tah[.]xxoo[.]co
nx2[.]hangame[.]co[.]uk
he[.]xxoo[.]co
nhnclass[.]com
w[.]gasoft[.]us
bot[.]dongevil[.]info
nexononline[.]com
www[.]apanku[.]com
kog[.]jcrsoft[.]com
ads01[.]mynetav[.]net
smtp[.]gcgame[.]info
nexon[.]joymax[.]in
nx3[.]hangame[.]co[.]uk
soft[.]hja63[.]com
au[.]msftncsl[.]com
www[.]cjinternet[.]us
gcqc[.]xxoo[.]co
mg[.]zzsoft[.]info
java-ssl[.]com
js[.]nexoncorp[.]us
nd[.]jcrsoft[.]com
www[.]gasoft[.]us
nxeu[.]jcrsoft[.]com
sellsads[.]sells-it[.]net
nt[.]nexoncorp[.]us
www[.]hja63[.]com
get[.]java-ssl[.]com
eudb[.]nexongame[.]net
kr[.]jcrsoft[.]com
www[.]zzsoft[.]info
nx3[.]joymax[.]in
a1[.]nexongame[.]net
service[.]dell-support[.]org
ns3[.]nhnclub[.]com
wog[.]zzsoft[.]info

ad[.]jcrsoft[.]com
ns6[.]msftncsl[.]com
ibm-support[.]net
gh[.]zzsoft[.]info
smtp[.]jcrsoft[.]com
cc[.]nexoncorp[.]us
imm[.]conimes[.]com
pass2[.]googletrait[.]com
gh[.]gasoft[.]us
wm[.]nhntech[.]com
www[.]gcgame[.]info
support[.]dell-support[.]org
av[.]gcgame[.]info
gm[.]gcgame[.]info
cjinternet[.]us
pass1[.]hangame[.]co[.]uk
fax[.]nexoncorp[.]us
roqc[.]xxoo[.]co
new[.]java-ssl[.]com
tug[.]mynetav[.]net
ftp[.]zzsoft[.]info
pop[.]hja63[.]com
ahn[.]gasoft[.]us
officess[.]dyndns-office[.]com
lp[.]gcgame[.]info
web-games[.]us
sl[.]xxoo[.]co
login[.]hangame[.]co[.]uk
vn[.]jcrsoft[.]com
roap[.]myxxoo[.]com
mir2[.]nexongame[.]net
imap[.]jcrsoft[.]com
game[.]nexongame[.]net
fs[.]nhntech[.]com
docs[.]nhnclass[.]com
t3[.]nhntech[.]com
iss[.]conimes[.]com
lyto[.]zzsoft[.]info
scvhosts[.]com
dbo[.]jcrsoft[.]com
fn[.]hja63[.]com
oky[.]mynetav[.]net
naverpulic[.]com
wm[.]xxoo[.]co
vn[.]gcgame[.]info
ap[.]nhntech[.]com
l[.]xxoo[.]co

masternow[.]webhop[.]net
reegame[.]net
myav[.]mynetav[.]net
exchange[.]dumb1[.]com
ssl2[.]dyn-tracker[.]com
client[.]gnisoft[.]com
owa[.]ahnlabinc[.]com
nmn[.]nhndesk[.]com
n8[.]ahnlabinc[.]com
www2[.]dyn[.]tracker[.]com
ssl2[.]ahnlabinc[.]com
sixindent[.]epizy[.]com
zeplin[.]atwebpages[.]com
goodhk[.]azurewebsites[.]net
snoc[.]hostingupdate[.]club
sidcfpprx01[.]in[.]ril[.]com
nted[.]tg9f6zwkx[.]icu
sidcfpprx14[.]in[.]ril[.]com
sidc[.]everywebsite[.]us
koran[.]junlper[.]com
sidcfpprx25[.]in[.]ril[.]com
sidcfpprx10[.]in[.]ril[.]com
bsyu[.]dnslookup[.]services
bctu[.]dnslookup[.]services
coivo2xo[.]livehost[.]live
lmogv[.]dnslookup[.]services
wcuhk[.]livehost[.]live
coivotek[.]livehost[.]live
wvt[.]livehost[.]live
dntc[.]livehost[.]live
wctu[.]livehost[.]live
kbklxpb[.]imshop[.]in
msfcnsoft[.]com
A781195[.]gicp[.]net
B781195[.]vicp[.]net
msffncsi[.]com
kbklxp[.]eicp[.]net
upgradsource[.]com
serupdate[.]wicp[.]net
microsoff[.]net
db311secsd[.]kasprsky[.]info
doc[.]goog1eweb[.]com
d89o0gm35t[.]livehost[.]live
7hln9yr3y6[.]symantecupd[.]com
d89o0gm34t[.]livehost[.]live
ftp[.]fiysaa[.]com
www[.]alombok[.]yourtrap[.]com

www[.]asagamifujino[.]dns05[.]com
fackb00k2us[.]dynamic-dns[.]net
nadvocacy[.]mrbasic[.]com
developman[.]ocry[.]com
jeannedarcarcher[.]zyns[.]com
alombok[.]yourtrap[.]com
www[.]trendupdate[.]dns05[.]com
bluecat[.]mefound[.]com
serviceonline[.]otzo[.]com
cindustry[.]faqserv[.]com
www[.]uacmoscow[.]com
www[.]g00gle_mn[.]dynamic-dns[.]net
npomail[.]ocry[.]com
ns2[.]microsoftsonline[.]net
movie2016[.]zzux[.]com
www[.]arjuna[.]dynamicdns[.]biz
frankenstein[.]compress[.]tonikolatesla[.]x24hr[.]com
free2015[.]longmusic[.]comnotepc[.]ezua[.]com
freedomain[.]otzo[.]com
ntripoli[.]www1[.]biz
www[.]yandex2unitedstated[.]dynamic-dns[.]net
ggpage[.]jetos[.]com
arjuna[.]serveusers[.]com
gmarket[.]system-ns[.]org
billythekid[.]x24hr[.]com
daum[.]xxuz[.]com
depth[.]toh[.]info
email_gov_mn[.]pop-corps[.]com
www[.]yandex2unitedstated[.]dns05[.]com
www[.]oseupdate[.]dns-dns[.]com
filename[.]onedumb[.]com
odanobunaga[.]dns04[.]com
www[.]odanobunaga[.]dns04[.]com
point[.]linkpc[.]net
www[.]fergusmacroich[.]ddns[.]info
www[.]googlewizard[.]ocry[.]com
www[.]ibarakidoji[.]mrbasic[.]com
unaecry[.]zzux[.]com
googlewizard[.]ocry[.]com
indian[.]authorizeddns[.]us
www[.]g0ogle_mn[.]dynamic-dns[.]net
facegooglebook[.]mrbasic[.]com
www[.]g00gle_kr[.]dns05[.]com
www[.]microsoft-update[.]pop-corps[.]com
www[.]yandex2unitedstated[.]2waky[.]com
www[.]freedomain[.]otzo[.]com
ttareyice[.]jkub[.]com

agent[.]my-homeip[.]net
freemusic[.]zzux[.]com
pop-corps[.]com
application[.]dns04[.]com
regulations[.]vizvaz[.]com
server[.]serveusers[.]com
msdn[.]ezua[.]com
myflbook[.]myz[.]info
fergusmacroich[.]ddns[.]info
mynews[.]myftp[.]biz
fornex[.]uacmoscow[.]com
www[.]cuchulainn[.]mrbonus[.]com
www[.]daum[.]xxuz[.]com
www[.]david[.]got-game[.]org
www[.]facebook2us[.]dynamic-dns[.]net
www[.]nthere[.]ourhobby[.]com
www[.]fackb00k2us[.]dynamic-dns[.]net
www[.]free2015[.]longmusic[.]com
www[.]siegfried[.]dynamic-dns[.]net
www[.]inthefa[.]bigmoney[.]biz
jaguarman[.]longmusic[.]com
dnsdhcp[.]dhcp[.]biz
xindex[.]ocry[.]com
likeme[.]myddns[.]com
eshown[.]itemdb[.]com
www[.]likeme[.]myddns[.]com
www[.]ggpage[.]jetos[.]com
www[.]medusa[.]americanunfinished[.]com
www[.]yandex[.]pop-corps[.]com
cuchulainn[.]mrbonus[.]com
modibest[.]sytes[.]net
www[.]ncdle[.]net
ns1[.]dns-dropbox[.]com
ns1[.]microsoftsonline[.]net
g00gle_jp[.]dynamic-dns[.]net
www[.]yandex2unitedstated[.]dns04[.]com
daum[.]pop-corps[.]com
www[.]jaguarman[.]longmusic[.]com
www[.]xindex[.]ocry[.]com
www[.]nikolatesla[.]x24hr[.]com
www[.]nmbthg[.]com
www[.]billythekid[.]x24hr[.]com
www[.]officescan_update[.]mypop3[.]org
www[.]program[.]ddns[.]info
bradamante[.]longmusic[.]com
www[.]yandex[.]mrface[.]com
letstweet[.]toh[.]info

lezone[.]jetos[.]com
medusa[.]americanunfinished[.]com
yandex[.]pop-corps[.]com
www[.]facegooglebook[.]mrbasic[.]com
www[.]bradamante[.]longmusic[.]com
www[.]npomail[.]ocry[.]com
backup[.]myftp[.]infohardenvscurry[.]my-router[.]de
help[.]kavlabonline[.]com
hosenw[.]ns02[.]info
hpcloud[.]dynserv[.]org
tunnel[.]itsaol[.]com
microsoft-update[.]pop-corps[.]com
microsoft_update[.]pop-corps[.]com
rama[.]longmusic[.]com
redfish[.]misecure[.]com
microsoftdocs[.]dns05[.]com
ns[.]microsoftdocs[.]dns05[.]com
ns2[.]dns-dropbox[.]com
onenote[.]dns05[.]com
www[.]ertufg[.]com
info[.]kavlabonline[.]com
www[.]webhost[.]2waky[.]com
www[.]gkonsultan[.]mrslove[.]com
www[.]goog1e_kr[.]dns04[.]com
economics[.]onemore1m[.]com
artoriapendragon[.]itemdb[.]com
www[.]robinhood[.]longmusic[.]com
describe[.]toh[.]info
waswides[.]isasecret[.]com
webhost[.]2waky[.]com
webmail_gov_mn[.]pop-corps[.]com
ecoronavirus[.]almostmy[.]com
yandex[.]mrface[.]com
ereshkigal[.]longmusic[.]com
robinhood[.]longmusic[.]com
host[.]adobe-online[.]com
thebatfixed[.]zyns[.]com
uacmoscow[.]com
update[.]wmiprvse[.]com
inthefa[.]bigmoney[.]biz
gaiusjuliuscaesar[.]dynamicdns[.]biz
arjuna[.]dynamicdns[.]biz
gkonsultan[.]mrslove[.]com
www[.]stade653[.]dns04[.]com
www[.]jeannedarcarcher[.]zyns[.]com
www[.]msdn[.]ezua[.]com
www[.]frankenstein[.]compress[.]to

www[.]hosenw[.]ns02[.]info
freemusic[.]xxuz[.]com
ns4[.]colunm[.]tk
ns3[.]colunm[.]tk
www[.]astudycarsceu[.]net
www[.]indiasunsung[.]com
indrra[.]ddns[.]net
ixrails[.]com
escanavupdate[.]club
www[.]smartdevoe[.]com
ptciocl[.]com
www[.]shipcardonlinehelp[.]com
railway[.]sytes[.]net
indianrailway[.]hopto[.]org
inraja[.]ddns[.]net
indrails[.]com
websencl[.]com
pandorarve[.]com
ntpc-co[.]com
ubuntumax[.]com
railways[.]hopto[.]org
42[.]236[.]84[.]118
45[.]77[.]6[.]44
54[.]245[.]195[.]101
103[.]86[.]84[.]124
61[.]33[.]155[.]97
45[.]77[.]3[.]152
180[.]150[.]226[.]207
103[.]212[.]222[.]86
117[.]16[.]142[.]9
103[.]19[.]3[.]44
23[.]236[.]77[.]175
23[.]236[.]77[.]177
103[.]19[.]3[.]17
103[.]19[.]3[.]43
207[.]246[.]108[.]247
104[.]224[.]185[.]36
138[.]68[.]78[.]69
149[.]28[.]75[.]81
207[.]246[.]16[.]107
173[.]242[.]122[.]198
149[.]28[.]69[.]116
174[.]139[.]62[.]56
67[.]230[.]163[.]214
52[.]175[.]54[.]166
104[.]238[.]181[.]224
45[.]32[.]137[.]79

45[.]76[.]107[.]43
119[.]28[.]56[.]124
112[.]175[.]150[.]38
23[.]97[.]66[.]120
104[.]194[.]85[.]41
104[.]225[.]159[.]134
66[.]42[.]96[.]115
80[.]251[.]222[.]80
192[.]69[.]89[.]157
216[.]24[.]182[.]48
67[.]198[.]161[.]246
111[.]68[.]6[.]198
8[.]210[.]127[.]210
67[.]229[.]97[.]224
45[.]76[.]174[.]221
67[.]198[.]161[.]240
174[.]139[.]203[.]0
104[.]243[.]19[.]49
172[.]96[.]204[.]252
216[.]24[.]179[.]23
216[.]24[.]180[.]216
64[.]64[.]236[.]27
64[.]64[.]251[.]135
51[.]68[.]28[.]242
149[.]154[.]157[.]48
65[.]49[.]192[.]74
74[.]120[.]175[.]144
74[.]82[.]201[.]8
80[.]251[.]220[.]225
149[.]248[.]16[.]107
104[.]243[.]23[.]73
104[.]36[.]69[.]105
107[.]182[.]24[.]70
176[.]122[.]163[.]125
176[.]122[.]188[.]254
45[.]77[.]28[.]164
45[.]32[.]93[.]169
149[.]248[.]8[.]134
45[.]32[.]68[.]14
67[.]198[.]161[.]247
123[.]254[.]109[.]81
140[.]82[.]23[.]214
149[.]28[.]75[.]141
149[.]28[.]88[.]49
64[.]64[.]234[.]24
45[.]86[.]163[.]136
45[.]76[.]6[.]149

8[.]9[.]11[.]130
80[.]251[.]222[.]7
173[.]242[.]117[.]47
107[.]182[.]18[.]149
107[.]182[.]26[.]43
176[.]122[.]162[.]149
66[.]42[.]98[.]220
125[.]65[.]40[.]163
144[.]48[.]6[.]235
103[.]4[.]29[.]167
118[.]193[.]37[.]157
103[.]79[.]76[.]205
120[.]52[.]19[.]140
107[.]174[.]45[.]134
183[.]131[.]155[.]225
150[.]109[.]37[.]160
45[.]77[.]27[.]90
40[.]83[.]98[.]28
207[.]148[.]96[.]191
45[.]76[.]75[.]219
49[.]51[.]138[.]80
198[.]13[.]37[.]172
23[.]254[.]164[.]52
107[.]191[.]60[.]153
45[.]77[.]127[.]19
52[.]184[.]35[.]40
45[.]76[.]167[.]196
150[.]109[.]46[.]244
95[.]179[.]201[.]52
150[.]109[.]57[.]65
45[.]77[.]19[.]199
45[.]77[.]3[.]234
149[.]28[.]77[.]148
45[.]63[.]60[.]144
67[.]229[.]97[.]229
149[.]28[.]134[.]47
207[.]246[.]104[.]203
45[.]76[.]31[.]159
124[.]156[.]138[.]199
118[.]24[.]129[.]240
67[.]229[.]97[.]228
103[.]17[.]119[.]69
119[.]28[.]70[.]14
67[.]229[.]97[.]230
45[.]77[.]127[.]236
45[.]77[.]26[.]96
45[.]77[.]31[.]168

123[.]60[.]33[.]183
149[.]28[.]91[.]97
45[.]76[.]78[.]170
45[.]32[.]74[.]62
149[.]28[.]70[.]90
67[.]229[.]97[.]226
124[.]156[.]110[.]160
185[.]117[.]75[.]152
112[.]140[.]187[.]228
150[.]109[.]45[.]166
45[.]32[.]77[.]154
149[.]28[.]23[.]32
23[.]97[.]70[.]106
124[.]156[.]183[.]96
66[.]42[.]107[.]133
176[.]223[.]112[.]114
149[.]28[.]19[.]86
66[.]98[.]126[.]203
104[.]224[.]169[.]214
185[.]118[.]166[.]66
149[.]28[.]134[.]209
185[.]118[.]164[.]198
45[.]61[.]136[.]199
108[.]62[.]10[.]13
69[.]46[.]84[.]52
222[.]186[.]34[.]238
35[.]241[.]112[.]73
50[.]117[.]68[.]136
121[.]127[.]241[.]143
58[.]158[.]177[.]102
15[.]164[.]83[.]206
106[.]187[.]55[.]107
119[.]28[.]139[.]20
119[.]28[.]139[.]120
222[.]239[.]254[.]108
220[.]95[.]232[.]173
54[.]209[.]61[.]132
218[.]38[.]243[.]68
45[.]76[.]241[.]33
154[.]223[.]131[.]237
167[.]88[.]176[.]205
103[.]224[.]83[.]95
110[.]45[.]146[.]253
117[.]16[.]142[.]69
122[.]10[.]117[.]206
103[.]19[.]3[.]21
209[.]124[.]90[.]173

110[.]10[.]176[.]10
207[.]148[.]125[.]56
118[.]193[.]236[.]206
103[.]19[.]3[.]109
184[.]168[.]221[.]42
204[.]11[.]56[.]48
104[.]18[.]33[.]202
3[.]13[.]78[.]141
184[.]27[.]168[.]54
50[.]63[.]202[.]58
91[.]195[.]240[.]82
211[.]44[.]251[.]3
121[.]170[.]185[.]183
50[.]63[.]202[.]60
18[.]211[.]9[.]206
139[.]162[.]123[.]108
108[.]61[.]214[.]194
45[.]144[.]31[.]31
91[.]195[.]240[.]94
184[.]168[.]221[.]63
123[.]176[.]102[.]82
125[.]209[.]210[.]19
154[.]206[.]53[.]238
185[.]49[.]222[.]43
27[.]115[.]103[.]198
211[.]60[.]126[.]164
174[.]36[.]138[.]30
114[.]222[.]36[.]32
199[.]188[.]106[.]231
119[.]240[.]212[.]110
50[.]63[.]202[.]50
113[.]196[.]70[.]169
27[.]115[.]103[.]195
162[.]255[.]119[.]254
192[.]64[.]119[.]194
163[.]49[.]70[.]18
172[.]104[.]65[.]97
45[.]248[.]84[.]7
85[.]204[.]74[.]108
103[.]65[.]182[.]110
180[.]150[.]230[.]54
103[.]43[.]18[.]252
137[.]175[.]66[.]204
101[.]78[.]177[.]240
160[.]202[.]163[.]20
66[.]79[.]188[.]139
27[.]255[.]80[.]206

61[.]97[.]250[.]73
103[.]65[.]182[.]140
103[.]43[.]18[.]90
160[.]124[.]15[.]98
154[.]223[.]175[.]59
95[.]179[.]228[.]103
149[.]154[.]159[.]171
210[.]121[.]164[.]51
192[.]161[.]58[.]62
180[.]150[.]230[.]55
223[.]255[.]151[.]75
107[.]150[.]10[.]193
45[.]138[.]209[.]91
45[.]138[.]209[.]12
103[.]140[.]186[.]119
137[.]220[.]245[.]75
101[.]78[.]177[.]244
154[.]95[.]17[.]181
194[.]105[.]58[.]119
194[.]68[.]26[.]70
193[.]28[.]202[.]13
154[.]95[.]16[.]192
18[.]176[.]36[.]194
185[.]202[.]103[.]215
103[.]140[.]186[.]103
137[.]220[.]245[.]80
84[.]38[.]129[.]56
154[.]223[.]175[.]117
101[.]254[.]215[.]131
45[.]93[.]16[.]232
27[.]255[.]92[.]93
101[.]78[.]177[.]242
101[.]78[.]177[.]227
223[.]255[.]155[.]235
104[.]238[.]176[.]26
89[.]32[.]40[.]199
45[.]76[.]220[.]137
180[.]150[.]227[.]184
61[.]43[.]242[.]94
140[.]82[.]39[.]17
43[.]240[.]127[.]226
108[.]160[.]134[.]187
61[.]172[.]235[.]23
27[.]255[.]80[.]203
180[.]150[.]226[.]16
117[.]16[.]142[.]35
27[.]255[.]80[.]197

206[.]189[.]82[.]210
154[.]223[.]179[.]224
61[.]14[.]211[.]199
14[.]18[.]191[.]150
93[.]90[.]75[.]182
129[.]211[.]109[.]27
113[.]96[.]44[.]130
156[.]236[.]111[.]35
156[.]236[.]106[.]78
111[.]223[.]246[.]223
103[.]100[.]158[.]244
103[.]100[.]158[.]164
154[.]223[.]179[.]249
137[.]220[.]245[.]5
27[.]255[.]72[.]115
107[.]179[.]66[.]160
103[.]43[.]18[.]144
160[.]124[.]15[.]108
210[.]216[.]41[.]200
27[.]255[.]81[.]8
209[.]105[.]242[.]187
103[.]99[.]209[.]105
160[.]202[.]163[.]59
185[.]157[.]77[.]45
213[.]168[.]250[.]92
206[.]189[.]95[.]160
86[.]106[.]102[.]236
43[.]246[.]209[.]73
178[.]209[.]42[.]117
121[.]127[.]252[.]236
45[.]115[.]236[.]14
207[.]148[.]97[.]221
45[.]115[.]236[.]20
23[.]224[.]185[.]72
103[.]213[.]244[.]227
103[.]43[.]18[.]229
45[.]77[.]33[.]247
139[.]162[.]114[.]218
107[.]150[.]10[.]190
121[.]124[.]124[.]146
103[.]94[.]180[.]230
91[.]204[.]225[.]35
103[.]39[.]79[.]136
45[.]115[.]237[.]2
43[.]228[.]90[.]126
61[.]14[.]211[.]201
103[.]65[.]182[.]211

180[.]150[.]226[.]136
103[.]56[.]17[.]124
103[.]43[.]18[.]247
154[.]95[.]16[.]193
192[.]51[.]188[.]41
218[.]255[.]77[.]40
223[.]255[.]155[.]252
86[.]106[.]102[.]189
45[.]32[.]114[.]37
89[.]35[.]178[.]10
27[.]255[.]80[.]195
86[.]106[.]102[.]232
137[.]220[.]245[.]96
185[.]202[.]101[.]110
193[.]36[.]117[.]113
2[.]59[.]154[.]183
103[.]149[.]46[.]25
192[.]51[.]188[.]238
61[.]97[.]244[.]124
103[.]204[.]76[.]81
129[.]211[.]135[.]27
218[.]255[.]77[.]58
218[.]255[.]77[.]42
223[.]255[.]155[.]244
154[.]223[.]175[.]87
101[.]254[.]215[.]132
218[.]255[.]77[.]59
137[.]220[.]245[.]24
223[.]255[.]155[.]241
91[.]204[.]225[.]78
154[.]95[.]16[.]217
91[.]204[.]224[.]13
91[.]204[.]224[.]152
180[.]150[.]226[.]213
95[.]179[.]239[.]174
154[.]223[.]175[.]65
45[.]119[.]124[.]9
95[.]179[.]158[.]21
154[.]223[.]179[.]228
43[.]240[.]127[.]144
93[.]90[.]74[.]123
45[.]80[.]148[.]36
103[.]193[.]150[.]186
103[.]43[.]18[.]91
85[.]204[.]74[.]54
118[.]193[.]175[.]244
85[.]204[.]74[.]94

27[.]255[.]72[.]148
43[.]228[.]90[.]136
185[.]236[.]203[.]149
103[.]75[.]191[.]249
157[.]52[.]167[.]233
103[.]213[.]246[.]45
45[.]77[.]8[.]251
103[.]75[.]190[.]58
27[.]255[.]72[.]188
27[.]255[.]72[.]213
111[.]223[.]246[.]203
185[.]239[.]226[.]209
180[.]150[.]230[.]58
27[.]255[.]81[.]14
103[.]65[.]182[.]170
43[.]240[.]12[.]125
103[.]39[.]110[.]198
103[.]43[.]18[.]164
137[.]220[.]245[.]84
93[.]115[.]23[.]25
154[.]95[.]17[.]147
45[.]138[.]209[.]31
141[.]164[.]58[.]87
194[.]68[.]26[.]63
154[.]95[.]16[.]182
89[.]17[.]61[.]65
154[.]223[.]175[.]128
154[.]223[.]166[.]55
223[.]255[.]155[.]254
218[.]255[.]77[.]62
45[.]93[.]16[.]251
91[.]204[.]225[.]51
45[.]138[.]209[.]133
137[.]220[.]245[.]23
154[.]95[.]17[.]143
91[.]204[.]225[.]194
180[.]150[.]230[.]57
210[.]121[.]164[.]68
43[.]240[.]127[.]178
103[.]43[.]18[.]26
91[.]204[.]225[.]31
91[.]204[.]225[.]25
103[.]82[.]52[.]151
103[.]56[.]19[.]157
69[.]172[.]85[.]2
103[.]213[.]244[.]198
118[.]184[.]51[.]224

218[.]255[.]122[.]28
123[.]59[.]199[.]160
118[.]184[.]61[.]238
27[.]255[.]65[.]87
120[.]132[.]31[.]205
23[.]226[.]181[.]60
139[.]59[.]28[.]187
220[.]231[.]209[.]192
154[.]223[.]179[.]66
23[.]224[.]210[.]16
77[.]83[.]159[.]88
77[.]83[.]159[.]86
27[.]255[.]72[.]220
95[.]179[.]232[.]12
114[.]64[.]249[.]110
69[.]172[.]85[.]21
167[.]179[.]108[.]2
157[.]245[.]103[.]59
156[.]236[.]102[.]131
103[.]75[.]191[.]125
195[.]123[.]237[.]2
185[.]243[.]112[.]254
220[.]231[.]208[.]212
103[.]93[.]77[.]16
45[.]77[.]175[.]5
104[.]207[.]139[.]245
69[.]172[.]85[.]243
180[.]150[.]226[.]138
211[.]62[.]228[.]140
103[.]75[.]190[.]226
180[.]150[.]226[.]26
27[.]255[.]80[.]88
27[.]255[.]80[.]90
27[.]255[.]72[.]124
107[.]150[.]10[.]171
43[.]251[.]118[.]113
103[.]80[.]18[.]242
178[.]73[.]210[.]244
61[.]172[.]253[.]36
93[.]90[.]74[.]220
93[.]90[.]74[.]60
154[.]223[.]175[.]31
114[.]118[.]21[.]146
3[.]112[.]169[.]225
156[.]232[.]3[.]72
202[.]59[.]9[.]190
202[.]59[.]9[.]151

5[.]188[.]33[.]209
223[.]255[.]151[.]79
61[.]172[.]235[.]244
93[.]90[.]75[.]204
223[.]255[.]155[.]231
61[.]97[.]244[.]115
223[.]255[.]155[.]245
103[.]40[.]101[.]55
103[.]39[.]77[.]176
180[.]150[.]227[.]133
103[.]43[.]18[.]182
192[.]161[.]58[.]30
107[.]179[.]66[.]151
172[.]247[.]116[.]13
27[.]255[.]80[.]212
103[.]27[.]108[.]98
103[.]27[.]108[.]174
160[.]202[.]163[.]19
101[.]78[.]177[.]246
210[.]16[.]187[.]236
1[.]214[.]142[.]19
80[.]245[.]105[.]102
23[.]224[.]213[.]35
154[.]223[.]166[.]85
113[.]105[.]164[.]96
45[.]207[.]21[.]105
154[.]95[.]16[.]184
137[.]220[.]245[.]118
185[.]202[.]103[.]236
45[.]93[.]17[.]150
154[.]95[.]16[.]185
45[.]138[.]209[.]57
103[.]212[.]222[.]4
154[.]95[.]17[.]187
103[.]27[.]109[.]194
118[.]184[.]15[.]60
43[.]246[.]208[.]225
45[.]77[.]130[.]196
172[.]104[.]43[.]172
45[.]77[.]255[.]202
89[.]43[.]60[.]113
202[.]131[.]246[.]126
172[.]247[.]116[.]18
89[.]43[.]202[.]168
103[.]27[.]108[.]150
139[.]180[.]194[.]124
61[.]97[.]248[.]91

154[.]223[.]179[.]14
103[.]68[.]192[.]126
46[.]30[.]189[.]216
148[.]72[.]41[.]130
218[.]255[.]77[.]43
27[.]255[.]90[.]151
154[.]223[.]179[.]176
154[.]223[.]179[.]181
154[.]223[.]179[.]243
45[.]40[.]57[.]185
154[.]95[.]44[.]39
167[.]71[.]230[.]71
91[.]204[.]225[.]80
161[.]117[.]229[.]136
45[.]207[.]21[.]39
45[.]207[.]21[.]242
45[.]207[.]21[.]188
45[.]158[.]32[.]70
47[.]241[.]2[.]213
154[.]223[.]175[.]85
81[.]68[.]102[.]11
137[.]220[.]245[.]113
137[.]220[.]245[.]124
27[.]102[.]134[.]141
27[.]255[.]80[.]91
27[.]255[.]92[.]92
218[.]255[.]77[.]56
101[.]78[.]177[.]254
139[.]162[.]175[.]182
103[.]80[.]16[.]139
80[.]240[.]27[.]232
27[.]255[.]72[.]68
107[.]150[.]10[.]136
43[.]240[.]14[.]105
180[.]150[.]227[.]232
118[.]193[.]169[.]209
192[.]161[.]58[.]234
103[.]43[.]18[.]201
160[.]238[.]86[.]79
223[.]255[.]155[.]251
104[.]217[.]253[.]134
27[.]255[.]81[.]15
118[.]123[.]15[.]170
43[.]246[.]208[.]141
43[.]246[.]208[.]145
103[.]244[.]90[.]38
103[.]27[.]108[.]214

103[.]65[.]182[.]119
103[.]75[.]190[.]243
103[.]43[.]16[.]146
43[.]240[.]127[.]171
160[.]124[.]156[.]86
103[.]27[.]109[.]226
45[.]32[.]14[.]56
149[.]154[.]157[.]77
139[.]59[.]95[.]210
218[.]255[.]77[.]52
27[.]255[.]94[.]29
149[.]28[.]145[.]214
168[.]106[.]1[.]1
139[.]180[.]131[.]135
60[.]250[.]18[.]188
158[.]247[.]206[.]194
45[.]32[.]112[.]201
205[.]185[.]216[.]42
207[.]148[.]99[.]56
149[.]28[.]152[.]196
45[.]32[.]37[.]243
158[.]247[.]219[.]236
205[.]185[.]216[.]10
66[.]42[.]48[.]186
45[.]158[.]32[.]63
61[.]97[.]248[.]161
23[.]224[.]108[.]51
27[.]102[.]101[.]42
61[.]97[.]248[.]74
144[.]48[.]125[.]133
27[.]255[.]72[.]233
154[.]95[.]17[.]140
27[.]255[.]65[.]77
198[.]55[.]103[.]157
64[.]233[.]167[.]99
61[.]97[.]250[.]89
107[.]150[.]12[.]121
96[.]44[.]158[.]122
61[.]43[.]242[.]78
154[.]223[.]179[.]223
118[.]184[.]51[.]183
154[.]223[.]179[.]25
180[.]150[.]226[.]10
223[.]255[.]155[.]238
180[.]150[.]226[.]216
223[.]255[.]155[.]237
27[.]255[.]94[.]21

223[.]255[.]155[.]247
27[.]255[.]92[.]83
101[.]78[.]177[.]252
223[.]255[.]151[.]85
218[.]255[.]77[.]60
210[.]92[.]18[.]132
218[.]255[.]77[.]54
223[.]255[.]151[.]74
223[.]255[.]155[.]243

MD5:

1a0752f14f89891655d746c07da4de01
1d05380f3425d54e4ddfc4bacc21d90e
a283d5dea22e061c4ab721959e8f4a24
128cecc59c91c0d0574bc1075fe7cb40
a4b42c2c95d1f2ff12171a01c86cd64f
a76a1fbfd45ad562e815668972267c70
1e091d725b72aed432a03a505b8d617e
98908ce6f80ecc48628c8d2bf5b2a50c
9d86dff1a6b70bfdf44406417d3e068f
a17cb9df43b31bd3dad620559d434e53
1b95ac1443eb486924ac4d399371397c
a9c750b7a3bbf975e69ef78850af0163
212784cf25f0adfaf9ba46db41c373d5
fc208a4d04c085edcea1ec5f402057f9
5528bb928e02926179fca52dd388b1f0
20aebf6e20c46b6bfe44f2828adf3b91
559b7150d936fffe728092b160c14d28
9337952aa3be0dacfc12898df3180f02
83e6da9cd8ccf9b0c04f00416b091076
7b501402c843034cd79151257aca189e
69f5c5f67850acdb373ddd106adce48c
b8ecab09b7bfb42b9ace3666edf867a7
b6b06a95cfeeee0efe8bc0cd54eac71d
b071a62d2dd745743c6de5f115d633b1
a00ab8ac0f11c3fcd5c557729afcbf89
143278845a3f5276a1dd5860e7488313
83249cff833182b3299cbd4aac539c9a
d414c7ede5a9d6d30e6d3fe547e27484
019122b1d783646f99c73a3c399cc334
c4be6b466807540a22f62ffa6829540f
9c027648dc43b5a69dc1044d632ffadf
b1dd7ebee1ed9cecc650005bde302287
d0e98866d8b0bed5212ae27314ab2e31
e36160b7060c753eda6c086ff9a1c61d
611cb8decc2b260ba0344898e3ace34f
81aa9b58ad1d7b9981951d4557ca49a7

826547b7c6dd7d46297123f07edae30e
df49b7e640a55b6712762b6c90c4033e
87399e912ffc6ca13d1476a0172b76c1
1b29b173eee6126cf94147a1f45b0319
2b081914293f415e6c8bc9c2172f7e2a
e171d9e3fcb2eeccdc841cca9ef53fb8
7d1309ce050f32581b60841f82fc3399
eb3fbfc79a37441590d9509b085aaaca
6ae7a087ef4185296c377b4eadf956a4
c8daf9821ebc4f1923d6ddb5477a8bbd
f6004cfaa6dc53fd5bf32f7069f60e7a
c5d59acb616dc8bac47b0ebd0244f686
e19793ff58c04c2d439707ac65703410
c0118c58b6cd012467b3e35f7d7006ed
e07b5de475bbd11aab0719f9b5ba5654
1c30032dc5435070466b9dc96f466f95
51e06382a88eb09639e1bc3565b444a6
3ca2a13f646690481dc15d78bac6d829
155e98e5ca8d662fad7dc84187340cbc
582f84b21978cab7d190aef663a268ea
0996b71f1364acde317881810c5912f0
B0BD6C215A7C20B23FD23D77FA26F3BA
1b56416fefa2d2c863f3b46dfb6dc353
1716889fcee461e7cde5128c14d206cb
4ce57dbb210aea361aac3256b655437f
442cc6da5d2d9de50ee25fe88ad0de11
aa3e35e4808a1c0dd4a83314b8e57725
8342dc2a6bd63dd6a8e434463ffa70d7
aef8d6815054088ddfc489f478a7fe65
5d401e159ef4f7208c9512a374c7599c
212cc6078dc128105a75aa609788736c
072dc4cfe40a837205c9bff92791a5ef
83ddda78cc36aa1c3a4811d9805c00cc

SHA-256:

86b174eca149ce9c985c7d8da632515cc1c174cf9d5a8753302441d83de03939
2ba66cf4483c96f744540bc84a968efe982864ad2b185bb5a5fbae12f29e5835
7de282100c554a8cefb63001969fe25fc232bb83c3a2d9248306217b07d65b0d
c5e46e80c790be6997798241b852c8dbcd88e823a765a581dae228430114a8d4
efe1c1bfe07981069d17102b8e5c313f769625fd86d95fedc32525518d4cb2de
a0b2803aa9967c7d725ad1c29df129a2dae70ed93bfca4a80ea297aa66095e64
fb3b782b68f102f67b2d908ecfe8da9395519177d6fbdcba672ead2dc2f22716
bdc5b6fa35bcddb52e404512a824a97756fbc09c0303000a31f9278e6a607aa0
3c3ab6f16bf64d50941afefe4829b09d6628ecb67d962b2204c395a370e0917e
24f85e480bc3c7f733f0f2334f5d14c5893638af60c780ea9bd5fa9acfe423c7
eee4b1c4621b0ca355dc677652dfd6449f1f230565da8cb5db59fa195e8f553f
7fbf5efd35ca300537949c16d9ce68b7f7b98e82bba1f95a265b8d46324d7f2c

d7323a226c34aa76a3c25dce33250102648c49038affaf49bea1da46c9c0d695
12258203236afed3b293ed2a9b5f657cfd5b8d8a0fb9bed6200666c379d758c8
1ada845dbf89024f4eee8409880ce21ece2262db3ad5129d2eed33a76d177d39
6d64319843f4c26c757c104b636aab4e08e1ecd1d947f1beb6ef2419110e97d6
06211a1415b9bd765dcebe7583076ac1d581e00ef64c435199de1cbe23afb455
a911bec0c307f542990016ed3cb15bae7a61d489278800f111794387f7995e2e
b08accc9ed7474f5eb165fecf2026ea1b7660d5f7749e50163aa105b5f639f8f
9bac5ef9afbfd4cd71634852a46555f0d0720b8c6f0b94e19b1778940edf58f6
bca9583263f92c55ba191140668d8299ef6b760a1e940bddb0a7580ce68fef82
e05dcadd44a2c948f0d7a3dc47cf392a75d41ad9c50f3b71e2766416716e76eb
13e4bda99c359789ced1470a9d6869efe90a18eef5e57de7097fd79627fc5619
7b7e5b915af6a8c07c228f348313579b90409893365993df50ed7b572d54f5c1
993d14d00b1463519fea78ca65d8529663f487cd76b67b3fd35440bcdf7a8e31
b7fcc7f99bd5c440ead40ae26ddff95d5160a248345b27bb5daa5a0a3aa87814
306a7818108c10882e32403f5d77007d670110bf832726c1e18bb7069a263757
8c46d9e8529d9702df61c3e5f3a365248b3215b00f1f3a58433f7c106a851cdc
682fc8ccfc9316c54f02ae7865eee553ad0211031d4d80bb9c4365fbbc74049a
bebb16193e4b80f4bc053e4fa818aa4e2832885392469cd5b8ace5cec7e4ca19
dcbff3dbd8a3b0ed066a717ee8b74c28a4a2392a92008dd024717f96d137942d
bc90535f3412fce0092c69424700a36e4f006ee79729897a5f443752301850ca
2669f90ce96af374d13bab2e0e83c46fb8f3576d30f649512d41689188cf3c69
8510fc293227ea7b7d4b20073302e015b616aa8af90d30549b5b118034036111
c59509018bbbe5482452a205513a2eb5d86004369309818ece7eba7a462ef854
4f51eb7829b97d4a5ba5cdc9d909f484a0e412340fc68d3cad0e1f2e8972640d
fc117650688065deeb54e686f873359c2a56d23165567ab3f2a3b62498199fa9
5a151aa75fbfc144cb48595a86e7b0ae0ad18d2630192773ff688ae1f42989b7
a8e5a1b15d42c4da97e23f5eb4a0adfd29674844ce906a86fa3554fc7e58d553
03b7b511716c074e9f6ef37318638337fd7449897be999505d4a3219572829b4
e93a9e59ee2c1a18cee75eedcbe968ed552d5c62ec6546c8a1c1f1ae2019844e
ae000f5cef11468dde774696423ca0186b46e55781a4232f22760a0bfbfb04f0
3b70be53fd7421d77f14041046f7484862e63a33ec4b82590d032804b1565d0d
531e54c055838f281d19fed674dbc339c13e21c71b6641c23d8333f6277f28c0
5ff2196bf8e0c1cf4da84a2095a0f0090a5d6cddb5160ee0d3d0b7aecf3880e0
1f64194a4e4babe3f176666ffd8ee0d76d856825c19bfcd783aec1bacb74fd05
42beb91ccc7a6c0768f3d134842026ebfe5199e91a3f57787eb0b64852cb853f
a1fa8cad75c5d999f1b0678fa611009572abf03dd5a836f8f2604108b503b6d2
37be65842e3fc72a5ceccdc3d7784a96d3ca6c693d84ed99501f303637f9301a
f53639989aae3239f6da834d765a7e3a92118d5096fbc9ea315991f01e4d98a0
94ea23e7f53cb9111dd61fe1a1cbb79b8bbabd2d37ed6bfa67ba2a437cfd5e92
b59a37f408fcfb8b8e7e001e875629998a570f4a5f652bcbb533ab4d30f243f7
e54b7d31a8dd0fbab1fa81081e54b0b9b07634c13934adaf08b23d2b6a84b89a
52b966d2b80dfc406f6d5c95d90a39cec0e1a524b6de4c56cc6d812d054fd472
b2028fbc366d79d52acc761a8e075dab072ff79238f5d5e363843b405d2b96d4
ac5b4378a907949c4edd2b2ca7734173875527e9e8d5b6d69af5aea4b8ed3a69
ccdb8e0162796efe19128c0bac78478fd1ff2dc3382aed0c19b0f4bd99a31efc
18a14cec1abcb9c02c1094271d89f428dec1896924a949ed760d38cd0dea7217
0a76c55fa88d4c134012a5136c09fb938b4be88a382f88bf2804043253b0559f

0423258b94e8a9af58ad63ea493818618de2d8c60cf75ec7980edcaa34dcc919
75d573d1e788590195012a1965cfcaa911c566aee88331b7718ddc638028c175
a02258fcb3694893b900f10f0f9bb1d0d522ed098b1cc8eab59f2f70209b3a0b
655c21fc31967282d8517b3c845f775cd0a80595f90c5c85b6027110532a1cf9
d0686f44fb7e77ce0f68cc91c4cef12dbd691bb99b0b7be77103b7b17eec3753
0d6a5183b903b1013367b9a319f21a7a3b7798d9565a0deee52951f62a708227
1bd0f0fbd7df99c41e057f6d6c7107812ef1370609ad215a92227ca79ce6df70
9afb78e9be08041f849563c4fd2777a373ffc76c3eccd638b1f6f846b847b968
325430384d642ab2a902fb0e268e85808b6cbf87506ccdc314e116e7d1b8239e
9ad808caa0b6a60a584566f3c172280617e36699326e7425356795b221af41dc
eb9c850b1e8d8842eb900fa78135b518fb69da49c72304b5b3b4b6f4fa639e57
e10046b86fe821d8208cb0a6824080ea6cd47a92d4f6e22ce7f5c4c0d9605e4b
420dc77afe28003f14dfe6c09fbf8194ead8a6e8222b6ab126e7ee9bf4b63fd4
d6a05e20da5012c0cfc491b0044f7fded9322f5bbc664092c4b481709c3472e0
e935699b31707ecf9e006940f31f09514688cb45e078a66724603ee7fadf84db
fad80dc36a59d1cc67f3c4f5deb2650ca7f5abac43858bf38b46f60d6bb4b196
8308e54055b45eb63dc6c4c6a4112310a45dec041c1be7deb55bec548617136f
d30dd7d82059dc34e72c3131dd7ea87f427cabe7225bbf59aa69e01cd761a1fe
e0b675302efc8c94e94b400a67bc627889bfdebb4f4dffdd68fdbc61d4cd03ae
2fdef9d8896705f468f66eb8c20e5892d161c1d98ab5962aa231326546e25056
1e29e07b404836c82cd9b75e44a3169195a335dc494ba27f744f6605666c26aa
f69c6e8fe1188a461bfe249ba7afefbd7a787fcd0777c008f9580f6976118898
0187d3fae2dfc1629e766d5df38bdabf5effcb4746befceb1aaf283e9fe063a1
ca0f235b67506ed5882fe4b520fd007f59c0970a115a61105a560b502745ac6a
4da733bbf7d585ee5b5a58c0ad77047ce640a4512a84502ad5ae9240ee2fcdb0
bef3f87c6582813e23b0c8c8db9ca9ed65bc802445187378f4e62a7246133ae2
e4df8634f5f231fae264684e63b3e0c6497b98dd24ba1b0c6f85c156d33a079c
1968f29b67920fc59e54eba7852a32f20ecbf3f09481c09ddbee1dedc37f296e
a7df8143a36638de40233b141919d767678b45bf5467e948a637eaafb2820550
6867f3d853de5dfe8adbd761576c29ad853611d8d1c7fdd15b07125fd05321f8
0c6c6ba92661c119168a5486faa1af94673bd4d770c13c2b49d7a0651f798857
0041b28d1f076e196af761a536aa800ebe2fcaea9084a8e17d2a43c43765efdd
46f03ddf74c47960a3731de18f123b2110153ed668f9bf6ed3badd7fd099ccb6
d879b6cac6026a5418df4bf15296890507dbaec5abe56dafda54266975488cf2
3d38dfd588fc98de099201fe9f52feb29bb401fc623d6fe03eb8f0c959ffc731
5347c5bbfaec8877c3b909ff80cda82f505c3ef6384a9ecf040c821fc7829736
a4b2a737badef32831cbf05bfaa65b5121ddb41463177f4ac0dbc354b3b451d4
0756216ea3fea5b394e2fa86e90a75f05c3da2b4b47d61110559bd28f51da8e6
34aeaa89aab983318ed8f6da32556faf3057a92dc045fac1f960f3aaad3a1ba1
40101054d18eb50b65c2ce32b00352d2486008f67c63baec5ef93cac9d5c81ed
4665280d4b34c5388edeb51a6d5e808d2942c364017a42d3f1fac186b21eb571
4f2d8c437d32dc075074f01d10698f6d4dfc4d4bd8a595dabaa2519c6a025c8e
9bf32bf4a4bc1d13bddaa6402595ad76d2d9fcc91a988313f13ed990ccb1c4c1
9c3280bc1ebc239de86523a7046b45e9bb7ce7a40a869dda6ea92fcee727366a
bfe2673b02c54be9093cff8fd564b630109175c608f07d94e4a2ac65028a6eae
3454d87b2ce0eab44c07774c7b56318710f9a63626d6d2aaf898922178bf2792
b447a7bb633f682058d4b9df5caabbe8c794f087b80bf598d6741a255e925078

ba03feb351825029426e84c2f74e314f27b56714a082759650a455dfb1a946eb
be7ba33fcb2a19bb2d1fe746f49c39fb1b8bd5d9e46d5b6610f8a2ad3f60b248
d1a548b9ad6b4468ee3c5f6e1aaaa515021255fb13e45ff34fbff5ad88bf4de2
6a10027dd99f124cd9d2682b6e7b0841d070607ea22a446f3c40c0b9f9725bed
abac7a72b425ff38f8a7d8b66178da519525dc2137ca8904b42301fb46a8983e
afb5e3f05d2eedf6e0e7447a34ce6fd135a72dad11660cf21bec4178d0edc15b
81ab37ae3abce3feabdefde6a008dec322e0168ce4f0456ee737135025399400
71a965d54c4b60f7ae4a5e46394bfca013d06e888ec64f06d5ec3d8a21eccb55
283302c43466bdc6524a1e58a0ff9cc223ab8f540a1b0248d1fcffe81b87d5d6
01c8cc07a83ffd7ac9ee008685eb360c9934919e86847c50c8843807b9d9c196
de648c21b4fae290855fdf0cd63d9e6807ced0577bdcf5ff50147ba44bf30251
be70b599e8d7272e8debf49e6bf6e5d8d9f1965812f387a9f1e75aa34788a7c7
8fb8134bf40ad6bddd60ea77b78c30dab72c736bf29172f89d03505b80c3ae8d
c93999f7622caf63cbcfb26966ff11719a4e26bca7d90a843461f44a3c982a30
e7f5a30d4bf7915cc97374e0f6a29573d4640961166b5c9b942030e8c10949d8
645b14df1bd5e294ec194784bc2bd13e0b65dac33897c9b63ad9ed35ec6df3a8
7fd19347519ec15ab8dbce66722b28a917b87ad034282ef90851e1b994463644
adf52650ce698e17d5ff130bc975a82b47c6c175ad929083d757ec0fe7c4b205
b55812f35735e4fb601575072f1b314508b2dafdcb65aa6c1245a2e1f9d80bdd
f6085075e906a93a9696d9911577d16e2b5a92bc6b7c514d62992c14d5999205
43fe07f9adeb32b20e21048e9bb41d01e6b3559d98088ac8cd8ab0fad766b885
6e7052562db5f23c2740e9d094aae2316f77866b366eb4ef59c157e112172206
f91f2a7e1944734371562f18b066f193605e07223aab90bd1e8925e23bbeaa1c
e886caba3fea000a7de8948c4de0f9b5857f0baef6cf905a2c53641dbbc0277c
a783edae435c6fdf55e937b3246b454ed3b85583184b6ffc1b2faba75c9165cf
b83534071bbcacc175449faadbb1d6b0852fe58521da0fefd5398a4a9b1fb884
06210a1f9bc48128e050df0884f9759e4d202bd103aa78e6b6eb3cec1a58cdb5
29233eab65960c2da4962e343a3adab768673012d074db35ebc2abe2142ee73c
8f0538a18c944e2a98f1415d5528a0dab4367cd8689f598ab2da266c36403252
025e053e329f7e5e930cc5aa8492a76e6bc61d5769aa614ec66088943bf77596
0ad8ee3fe6d45626b28c0051c4c4f83358a03096ad06fc7135621293e95c75ae
f54cf6d9a5d77a89c4a2d47b02736d746764319e02ad224019db8de78842334a
86100e3efa14a6805a33b2ed24234ac73e094c84cf4282426192607fb8810961
e398290469966aff01a9e138d45c4655790d7a641950e675785d0a2ab93e7d28
47d6a1e163e65287087d2bb4c18fde9e2bce349cf7315be874c5dba1c8e1f2f8
0046df35f66a3b076d9206412be2f1f7ea4641d96574e7b58578c0c0995d1feb
9e27f110fc824d8b85855538c3320e8ea436e82737d686fcecb512b6f872e172
bec68bcaa80bb00274ef7066ddc8de1b289fb5f8b8e8573f3a961664f41da9d7
3a9bbf4ee872904e729466aa50d570b43451b0945a41b5d9d114f8c24683c21e
faca607b43551044fda3c799ce7e9ce61004100544eeb196734972303f57f2ae
f36a0b99973a837d5e4d542edd739df7cac10e207be538d47a106c4edf7cff54
45d175f3c1cb6067f60ea90661524124102f872830a78968f46187d6bc28f70d
6b4b9cf828f419298cd7fda95db28c53fc53627124224d87d2ad060185767957
8add31b6a2828e0d0a5b3ac225f6063f2c67c56036ff3f5099a9ee446459012a
21dd261e5fe46b86833cd69b299ae5ee5f24da3d4e87de509eddda4d2f63d591
79fbb45d0041933dce16325b87b969db12b7a8dedc918929615104835badc80f
fc5c9c93781fbbac25d185ec8f920170503ec1eddfc623d2285a05d05d5552dc

8f8ee8d2bc6c559a0a09ce3958727dee2f30880c615b2788d757917ca55d43ef
8b515bf88b3f7ac77861fdea61f82fb0c941bc5569922cadca254a79a744ae99
012d8d787c6e7a5f3dbe1e9cce7c5da166537a819221e210ef4d108f1a0a24b3
fb707094673a48408f9ba5240019cb502b9367fb380bb1734e0243e90b9399c3
5841a4302fcbd63f66fc2afd41f8671744454aaa7e1ed834e935bfdb007a9a83
7ed5cbeb6c732aa492762381033ff06d0c29f1c731530d4d27704822141a074a
8c962ddbb515e73ecfc5df9db35a54c8c9d15713a04425298f2d89308e2a47bf
fb23c7fc2e5e8ae33942734c453961da9ed4659368d19180a8f1ecb3b9b8e853
49e338c5ae9489556ae8f120a74960f3383381c91b8f03061ee588f6ad97e74c
62bcc4c3c74dbed9dd9fcd85ab5a479a26e06818d93e3fae649038e24054ac27
1229ddc6e928a803c3a20f13a948d943df9eda81db89a94857acfd271fc829d1
5d24f7135ec60c3f96f333d2030a3b23af333738f236ac1e2b3ca28987078d09
36eca485ebf5a08252edc00d090ebc9f173b1dbff3611c3ab2da793f1cadf09a
3e20ba0187bd31217ff98d8bf4dd89d116187d49e0925b5825cc4101c183237a
96b33f498ab8b4894fac4da41e0e7f11e9f3eb32b03e5a2213e1c47c497cb852
97f35f6ce242fde9f8aab7fbd3e94d8f530d563e7c5d177bb1ce274f3ac34e58
a6b75d222ab2930f4e20f2832dad51aca8a47c922e10108b962f5aa24434aa4e
fa9400f7d8e5555adf782d05487028346725b432f6ddd77bf136d79284bf3f2a
8a25bc0be3f0a6f8df5e1a6af88c56f45d2d0f1308f454b5ce1dafd4564e675e
62bd2c7098510cee6ea980c04f6df5c2ec740e8af91dd3c46a83d7d90524444f
28b726fb77a5981330cfd9f3667a6e12e0e6381d859f7f2eff7a3bccc3397f17
b03623e4818e60869f67dba28ab09187782a4ae0f4539cef2c07634865f37e74
094426e065ddc2a5caa15bf4a1fe7f87059e085d86192c9a8c3d80de4a5468a1
6c33d285dd0458a5b4c9e7fc76c818679ee06009f40792a6fdf070f38f8e6639
35f01d00cf986e9ec44e86fba0c45498d8ffcbf3a9c549c150d2bee95e55efb0
d6459e851fda540159a78aa901b46cc2e921c57952e961edf4d817b4f5a82f14
800ad41d6e951f0b5ac00501a6bee233c51ee4aa6ffcb899a4839f42715496d3
40933d429fad3375721d4374939e3bf0d79390e47709207cb2a0848f01670cf7
740c97728889fdc407049eadf46ac67c35db70e72b6cf5dcba5ffa43364cda8d
ae41108ad801edf08f96a77c41edd0b4ef6a3ff40575848faa85dd5a73cb4043
228a0c7f01f7198719eb03a02839147c0ab1fb4dfb30ccc364184a873bd562e7
28cdf2fd3175c8066e6c3d10a0ba5423c9dad35c93e8ca2c2bac706e9ce9119f
db866ef07dc1f2e1df1e6542323bc672dd245d88c0ee91ce0bd3da2c95aedf68
300519fa1af5c36371ab438405eb641f184bd2f491bdf24f04e5ca9b86d1b39c
f6d0cd5b6aa6ccea3ba3cb63b26420f6579d4a07164944e1013e093c521c5687
9d0ac935b9e0d6c86fc2904477638af6e4b68d020c2956912e5109cc6219c08f
12c02b62f14cf5675e2453cbc4e884735a7c25d6288551152a0e8545b70f936a
5455af6789342055aa04055934cca7d1873cbddf735e771130e40a9431a7c656
d4513b8379610116bfc17e0b694e3aa93f8eaf52758e1dc3afa4be7ba12d1215
ac546bd38ad2e56b42fd3e35f27048ca9c86203153868944188e6fb6822d9f63
0f6033d6f82ce758b576e2d8c483815e908e323d0b700040fbdab5593fb5282b
d29254ab907c9ef54349de3ec0dd8b22b4692c58ed7a7b340afbc6e44363f96a
6a9f16440b9319f427825bb12d7a0cda89b101cf7b8b15ec7dd620b4d68db514
ae5c7cfd8bbfb38b38772083bae721c77ac5698b2339148605e46756f0619da0
2590ab56d46ff344f2aa4998efd1db216850bdddfc146d5d37e4b7d07c7336fc
85297097f6dbe8a52974a43016425d4adaa61f3bdb5fcdd186bfda2255d56b3d
c2a88cc3418b488d212b36172b089b0d329fa6e4a094583b757fdd3c5398efe1

99c5dbeb545af3ef1f0f9643449015988c4e02bf8a7164b5d6c86f67e6dc2d28
493574e9b1cc618b1a967ba9dabec474bb239777a3d81c11e49e7bb9c71c0c4e
6943fbb194317d344ca9911b7abb11b684d3dca4c29adcbcff39291822902167
dfb4e0c176ba0cdc60bd8b58e9120b41e7927f0962338be3fd394e0ec97d9ef2
0531bdbe53e67095aa729809a6608be8cd04b7fc5b2cc3f6a610084cca062ff4
4d887bd577541437f0572a7dddbcb3dd94ad259a52f9f57807011939854a207c
3103a27193561218be83d26071701bf1900aecd3a3994fc4d12e7521acf97ec1
96c6ae72dc2d8ef45c0c7842780ba01f0c51280423ce8f11d49fa9c9053e6dff
21d66715f809593c277f43947d7005697bbd4f0af3c2fe16685cbab639aab4ea
ebd359fc107fb644c4f8a04e8b490b6a8e06eca648223d1bb06f2b25a7464cd1
1ac8477c5deb33585f0333298dac61537cb23f59226c685618f1e91cfa629171
7a265dc00f5a5a7401c56021190bf3345d7e39eadcf49d4c36f1e63654b021db
23bb555d3039ac59c5c827aefd46b70acdf7ebd284dd8fa2e05282774478f94d
a9a8dc4ae77b1282f0c8bdebd2643458fc1ceb3145db4e30120dd81676ff9b61
e3f47d6588b94507619acd51188d798e1adcb9a611960a2b231eddfc853a8ead
7af2ba8b7ece6da2844fd988bc01a3215839c8a79f43288e2126bc6f05953aed
4cf451ff2c5c7bae19edaff5cfbdd0d73084d8b18197070fc30df48e08040405
9cd2ae02c9ab9da01f0d3513efe6941a380eb4e13a3d8daf578a3dd716e29527
310b0f2973e969306b1652638338a19dacdc2429e7dc85d8e474780d86a407cb
57d38b0803db74fa388bb5fc4334d596a80f760d3551108d83703c722980eb4e
462a02a8094e833fd456baf0a6d4e18bb7dab1a9f74d5f163a8334921a4ffde8
ee41a4a58114ccdcbef0c424176ed267b10fc137136185b07d7710770d4dea27
f86fa8fc2f2428ed145e782894ef3be32b9ea8d60b68b805d8fbd1c5e7af427c
d484b9b8c44558c18ef6147c6ca8276a462fccf2acb2863be4ee9bf37942f11e
b4a07a3218fe80b8da2f0f470ab327cc3622155adeef8a3d1fd0c43dff4aa130
7049bad2755ae8b8a6945a1f323b1bc14551c9ee664b8573910ffbbe6bba97c8
dc52bdf5e3f71fb9ab3b1730d445287d16d3a3c81f026861247086d7e228792e
c297a74e3d2706ea033161043afd7c208499c5e46ff00e8e6ee7d646b8f9c761
a41edcd01e79c95f23c6d11aa6560a2ef02ccb5dafd5644f3082fc47cb0897e1
4548bbd713d94e2fb078a5c036c929b410ee706337a8303035f9b4605d341c8d
427a0860365f15c1408708c2d6ed527e4e12ad917a1fa111d190c6601148a1eb
6d41ec99b441408f29531d203818c93bb107f49b64bec9458d8bf3d11e542917
e2d7e21cd384a45f7fa37eb8eba7ea163d38cf6f663acf440c55defbc40ee2eb
7f8af64b082942f0469ce9b23c225dd9f06ab34724ed0d0e0802dbbf95ad5ccf
b96bd7c7ddaab860f78983520d7e1a40ff3712e8fe61e6dfca2d4d2d3b4a35d0
439c4818d04f6591bc2e0e4aabf6cee5a767b67ee32d8bf02ece9866d31bccea
eced97254f1ece17f3c8b6c1b4d34db13524f20600cd4234f36646e3cf2ed940
5b0b754b24c324f7b53f256e9612ddd5a422e57ae235acf4c757efdedf795f38
a0f01aa1fae705fcb45d16b7759d011badc8e9360807cdde2bfe9e2b5b522b6e
09258b138a8e2cab383a490041429961634545af559affbcbf35a128b1663d96
5d971ed3947597fbb7e51d806647b37d64d9fe915b35c7c9eaf79a37b82dab90
9439dee1dd20edd96bfa3908cda3bf49cb0e50f2a471f5657a2e974508acaca4
0055dfaccc952c99b1171ce431a02abfce5c6f8fb5dc39e4019b624a7d03bfcb
13aed842a6b43e61fd8e076cdfa9d96ec9ad917e073740bbd99ccb395eb3c9fe
eedeca88eb4cc1f180bbbe30b8997b68fa909c6e9f134a6c113bf9e3d12df47e
e6a51821b73e13b70a22d1d5f1736b2091af50a69cd03aec88e11b38b00d7af7
3e6c4e97cc09d0432fbbbf3f3e424d4aa967d3073b6002305cd6573c47f0341f

ae26e3507b81b5816f9c7557785e73d3391176dfbed3392cd3c6116365d99dc8
a32bda4bdfe8d04b4f53d5adc82f9bbdb6dc5c7b439ba0bdc02faadd6e16550c
0881cf8aa07b1381d4bfbaa43510fcb6f6db182b1fb899f50a1c1425dad04cf8
e038450d226cc02529a34a0c89cdd3af4c033066bb9db57274d0cadb52bb1065
f39cdc437f4c8d7d4d80b8d1d17c9c75e54340df912a56afc1f9a4e7ce5e4cfb
7c09b14a34114e5b6861530ac19ab1aaadf9e8c9a7fbbde96542c21175b094e0
14f40d1ca0019f38bb80e9d772952efbf643c34a2e236440e2e03ac9be1c5442
02a7dd784a87fd08b50515aa5ea7db5bebe95d13ee8df1e75d903c744827e01b
4f18df68ce89ba55b1bff0b1aac72a54c19862241f0fac9f957f8626114db418
38136d8d4146e75f03714f14d847777bf1cd17ddc942b95446b72954dfbd9f3e
555413c77e8d97df2e26522984baef65b09269825fb80a6bffb5b456e009211a
1865013aaca0f12679e35f06c4dad4e00d6372415ee8390b17b4f910fee1f7a2
9c770b12a2da76c41f921f49a22d7bc6b5a1166875b9dc732bc7c05b6ae39241
cc1455e3a479602581c1c7dc86a0e02605a3c14916b86817960397d5a2f41c31
90c5c715e6f1e61b02b56d70aa273898eae526c6b0caf303935763fc8b363e7f
4d3ad3ff281a144d9a0a8ae5680f13e201ce1a6ba70e53a74510f0e41ae6a9e6
3c6d304c050607a9b945b9c7e80805fc5d54ced16f3d27aaa42fce6434c92472
02f5cb58a57d807c365edf8df5635263f428b099a38dff7fe7f4436b84efbe71
fcbd7ab82939b7e0aff38f48a1797ac2efdb3c01c326a2dcf828a500015e0e83
3c8049bd7d2c285acc0685d55b73e4339d4d0a755acffad697d5a6806d95bb28
5d549155b1a5a9c49497cf34ca0d6d4ca19c06c9996464386fc0ed696bf355a2
34acd44b3c913f6437adee6df451af2bd5d8f2ab30bc8a7b044c2662faa80278
05e2912f2a593ba16a5a094d319d96715cbecf025bf88bb0293caaf6beb8bc20
3cd42e665e21ed4815af6f983452cbe7a4f2ac99f9ea71af4480a9ebff5aa048
74e348068f8851fec1b3de54550fe09d07fb85b7481ca6b61404823b473885bb
1419ba36aae1daecc7a81a2dfb96631537365a5b34247533d59a70c1c9f58da2
ef3cce62cd2ca9a48bdb2c1c53b02fe86988a8c3ce6bb114ff243ecab99fba1f
58a9e1a0558d77473c4bce16f75e403f3ace83910002f8beb233f7ff7cbf5e0d
19eec7cc74f2e111af5af8bf8af524306f9b18a53896279ffd3af70e1cf61b6a
801a64a730fc8d80e17e59e93533c1455686ca778e6ba99cf6f1971a935eda4c
67811f70e72693b266938c3a15a2a4b2634550e5934571e80e163c4313833d9d
706b927576e03f13daac88ad2a00b981e479302103948704fe20af21b6c6146c
719989e438d7bb37a2ab4aa6cb39df259aba33ed058d474909bdc100dd76a201
fb1ef3b5e0a3d4f50e550b0cbec0006484a4fa8f9f94556f0e42e31b147f9ca5
48f0bbc3b679aac6b1a71c06f19bb182123e74df8bb0b6b04ebe99100c57a41e
b3e1969261ef289fcf5401964f59ebadfe1408b261237a7443f84d540c96db66
b87f1023c6ea63c4e2c688f386b5cc278b89de6c3dd52ad2dd3440887185bdd6
5475ae24c4eeadcbd49fcd891ce64d0fe5d9738f1c10ba2ac7e6235da97d3926
a415d5f8eb12b55ab525b79869b00d037a66bb01b780b4cb6b987e5fa908cb90
ff9392032400659d7b1ba510eaf41efdcd02379e16c33b8621419d3ba489b4c4
4e8dc34e7b93faebc05c43efcee6a1d6b7f619c569a3e029e81a0006a3573ca2
6a5a9b0ae10ce6a0d5e1f7d21d8ea87894d62d0cda00db005d8d0de17cae7743
854b64155f9ceac806b49f3e352949cc292e5bc33f110d965cf81a93f78d2f07
63e63ffb95be2d5b8b7989a87c18aac16bfd0621209cfec55f8f63decc8a371e
e3bfb5443b2f36b61ba7a2cf95d2a24452559fafee85c47751f66438ac523d59
dc8441b4aef281e20db5103977b9a131b22eda8d5937923672e55d44d3951fe7
ae616003d85a12393783eaff9778aba20189e423c11c852e96c29efa6ecfce81

d8df60524deb6df4f9ddd802037a248f9fbdd532151bb00e647b233e845b1617
8da5d78b59ef78673d54d5178bebaf924589b95b9a1ad6004c456d7d9b1ca31c
adb9c2fe930fae579ce87059b4b9e15c22b6498c42df01db9760f75d983b93b2
3cdc149e387ec4a64cce1191fc30b8588df4a2947d54127eae43955ce3d08a01
9acbb8bed33a99664cc74d2d85f6db0dfba921f221b67392793f047b6aaadfb8
a026b11e15d4a81a449d20baf7cbd7b8602adc2644aa4bea1e55ff1f422c60e3
f1feea63da7c0f3a9d6eba3e33f10bb884ffda1b68525edf569798c1d9aa0b9f
a26a0b52b46d9ccafd023eae8cda960d8c1682f12136fb1e95076801b5d07358
a48483ba46e070c34b11c3b34e22b44d1bf783ae3e07c43d48eb6fb276690eab
16bfdbbea405d961db3e57bbd3c90111a62a0b1aaeafcc996bd5b26f08f31418
6aa8a859fd6d30d544269056930f6528dbd840fdae098842bf674e8d62bc8c05
b8350ae1e30b3705c8f388784bc40ffcba1279513014f98385047a485073b5ec
324e28d86e20b48cefc080e9464c652a4d25f8a1119eecb95b320e19d4c10a8e
236ba1b13c148c496198607fb1ae1f2efeccdb90f56fee813de8d96876731503
1e1fd03d363949f90909580947fe8de4657b540eb2e990b8f0d7bfbad426aabc
c55cb6b42cfabf0edf1499d383817164d1b034895e597068e019c19d787ea313
c8f83bf5e9f247d6ab52a87a0e59180097a74630d448b6ceb9d7290d99a24b1d
d1e7845a7ca3cce01597b6bb11d87fd19d330cf4474a6f27ec46dc7fc50b1640
ff4e12cf344ab0de04dac358e841907d4e9dc7cc286fd77f65e3246053ba3f8c
5fffdc8fb72d60f873d8693f2ae0218d7341ed0bcd390dde448e0c4b4c4139f0
9cc38ea106efd5c8e98c2e8faf97c818171c52fa3afa0c4c8f376430fa556066
c74a8e6c88f8501fb066ae07753efe8d267afb006f555811083c51c7f546cb67
d31374adc0b96a8a8b56438bbbc313061fd305ecee32a12738dd965910c8890f
9800f150260e81623b067ea82b7fc07119f6a587ad39e1572d611612b5737ba2
02815b72ed3449fd6004e007940ea8a8ab09bae4132739a4c7c705c2db0a1f89
902b1ec33382c0d4c941e005693c0ee83a9e0b46ab1a994171202c93d636ea38
a5565fc347a6040ec5e25acda630046a5c685843cc14ef14804852cff651e8cc
c3bec1a9a407bc8b3584e6166281e78ef15db4b303aaaac9aa5c71e9777f6f95
99e81931c35bf855974b6625100c645b970b2f6307f27aaf78f636469ef00957
75ca2c792d1d92b1d0888cb9b8d59b90c86a455ec251d5bf24dcab33525f02db
f3ed954f36b8982de337ced97c7b62b8eb2a0ede988ea11fad6193294ee0e5a0
a2977cebda62d687d1a0dde3b4c92295500ffd0ed35dd04b81ad59371ff03604
a4ce3a356d61fbbb067e1430b8ceedbe8965e0cfedd8fb43f1f719e2925b094a
fcfe8fcf054bd8b19226d592617425e320e4a5bb4798807d6f067c39dfc6d1ff
197c5cc9bbdeb6643d808d908eb9db078eb9b23c96299cbafaa4b7313eb6bf4a
3ed9ae6e596446f33dd13e44f3d54c8d1ca210242fc3b38b2d6398b1d0a97763
27a7768c45cf418b5aa057c0721e5599869390ba2e794b7bd03aa6fadff9d87c
f36d88b50ca2c6baffdadc8afc025d6546c6e97afb9456f9de82bc06c6d5db8c
be6bea22e909bd772d21647ffee6d15e208e386e8c3c95fd22816c6b94196ae8
237b74d3fd84f91aba3e541a34dd92c02b3625e61bf7ee0c01e691dd56004e15
448f0c371357c5a893190b36fe3dc5219fb557b0eba1b406d688538d00151305
baa39feabd3bf2524d658396f006a6fc8c9a0b669c828e91de17147f0a1053f3
32144ba8370826e069e5f1b6745a3625d10f50a809f3f2a72c4c7644ed0cab03
61761832dbb347cbaa778d8067f2ab2b0e7670b46f6c8287ca6115e6a6a2372d
6ef10bc47a361ece5f1019be5c3d47a0f36b5113a5cfb9541cf04fd2ae5783f6
1da13de2fea970749141cc8069f9082b2128b9af1518c2c50b91fb2c62480e6c
a7b6df70e23250a6cc2cbc032c7015eff9425725b5e85d1534c84f89e8ff8dea

66dc249bcd33189aa07a1c8fe294e4031b5954434b6747b24a7993985bb7a51b
d0522f0573ed16176bfa46057d9d3b9126bc0b3878dfc2df353bf8f118d12d82
356e1ab823280da9bb70bd8453f318e22cb7de956917d6eef419db274a3fb590
9729465c25b363968275329923cb040d80c30d323ed2dbf2eb959a0f7744163e
0af40318da9910510f8c3a4ae107f0b02ee7b80b5b16356b25715314ddc04fe5
f4b6c1f87091686d5462bd4915ce8f4c9844d2806553edd3fdf6e2038a489c99
a4c87cbb65b9c500ef54a5f201e1e7d02373465853c63397d7db6f2020c7c068
f7f6249ba423d1ce70a79621e1092ce37be7c4ad7dd768e0f3f6eafdd18d610e
72a8fa454f428587d210cba0e74735381cd0332f3bdcbb45eecb7e271e138501
c236559a5328d9d7106b224f2ee2f1a4e9e6dc5b25bba9d0c615ed74eec3d269
70992a72412c5d62d003a29c3967fcb0687189d3290ebbc8671fa630829f6694
73270fe9bca94fead1b5b38ddf69fae6a42e574e3150d3e3ab369f5d37d93d88
0608254fb22e5657e505763c901844bf83268e9df7a282758d56f37725e8abe9
253bf6847c709f28b2c5a7ac8c38e9be783722997ba7b0a356239cf325f6aa15
b2aa9bfc781973a766cf275836f9fa1cbc43b48e34c46e1d7e1774fc4db3cb6e
e7bbdb275773f43c8e0610ad75cfe48739e0a2414c948de66ce042016eae0b2e
a8bfc1e013f15bc395aa5c047f22ff2344c343c22d420804b6d2f0a67eb6db64
90b0888d5494476318067d736d4240c22c93a963eb5efb78f97d239d428cd162
4dfc539ef568e1a3cff0841fbf08756c21117e6451e142b77da18a5f41970877
2a93cf9550f3622f65b837c97ce2b2415f1c5f8cc764b2d634a5936feb73ce14
fb9af24eaf2e67595921aae2d13df25d8a213fb4f180174331c41b6c83a647f1
b3648697a00b6571e71f9d4cee07fdffbe7aaec0acb79bfe2322ae840eacc036
2b145bfa3c126c9b737cdd6316a67b0eb5f4d703b3ef80e7ea5810269d2b760b
ecd61a6ccdd01c030daa42928b2c8b82146d07dfc613e33560ed98a4e8546cc0
fe632654420af2189f6389f53e5c6b99d80b66c02db180f87b21a36ba4afee8c
d892cac17339fcfe4aca03980b590bd029e519e4f92f46623bf4e862b9483fd3
58bb3859e02b8483e9f84cc56fbd964486e056ef28e94dd0027d361383cc4f4a
fa380dac35e16da01242e456f760a0e75c2ce9b68ff18cfc7cfdd16b2f4dec56
7ea4591a4ba94d2be4346b3af502bf6d34bcf98ae05a040907c8d7bac28cbc01
be9254b2156e1f7089d86949cd314c42970640e1512785e735a2e753870ceca8
23f28b5c4e94d0ad86341c0b9054f197c63389133fcd81dd5e0cf59f774ce54b
73744ef6fb9654197abf083f060acecd306e891933940bfc88c77950ca14b2ba
1fe28cf9c65befa32eebcacc03a7c2605b7319457b8dc40278669d47c79c5dec
375985290d157cc90b5c61a4892caf55886f0ecd6279677cc8f9d659b97fefd2
dc9b5e8aa6ec86db8af0a7aa897ca61db3e5f3d2e0942e319074db1aaccfdc83
c7f9dd66ba7c924046569e437a63667489bcfdb32e065f42f80a5b8eaf2537f1
770fbe9d6fef71b7d7a9f07d9eae6dca9ce8b3178989fae0ed32d2d10651ab57
11c4e1b0af8bfc4ee951ccc794cc6e7d61e0533dcd4dbd780998414702b71ff9
d854f775ab1071eebadc0eb44d8571c387567c233a71d2e26242cd9a80e67309
d781794dc6d639a00e1ea587f3c7b928776848d515a991fa7b9c58a1b51f9bdb
de9ef08a148305963accb8a64eb22117916aa42ab0eddf60ccb8850468a194fc
08677a3dac3609d13dc4a2a6868ee2f6c1334f4579356d162b706a03839bb9ff
771fd0653bb5683d32ed7d98f38ffa8532e064ab0be010fe71e7ddb5c7cad225
6ae214bf4f815f05e27467fa0c8f1a6b24b5fc84c735d3d426da16bf6435d37c
c5108344e8a6da617af1c4a7fd8924a64130b4c86fa0f6d6225bb75534a80a35
2b373d4f4a8929cab247a84ea1c378c8c3926cb8d1aae8475639368fcffcaea0
063029a54743b98f556bad751ea8b331e2a27033f9e85e80ac3192c095ff1586

945d0a9f35e0e8e10c4c9e52d3257d43ca9a63ffc419ad84a492b764125fd59c
975b3f17c4e06136f5d0f3db074bea78326a6d8ffbf0c7971056845a3daa7ffb
be6ea2d9aa284b7e8cc7c8946a17708677300f43d57f325788b179e0210fef6d
84b8bfe8161da581a88c0ac362318827d4c28edb057e23402523d3c93a5b3429
41a1b059b5e75c75f9978b1384a555fe30a6f32448687d59613f38f19d1798f7
8e6945ae06dd849b9db0c2983bca82de1dddbf79afb371aa88da71c19c44c996
df999d24bde96decdbb65287ca0986db98f73b4ed477e18c3ef100064bceba6d
c0a0266f6df7f1235aeb4aad554e505320560967248c9c5cce7409fc77b56bd5
50d081e526beeb61dc6180f809d6230e7cc56d9a2562dd0f7e01f7c6e73388d9
dcd2531aa89a99f009a740eab43d2aa2b8c1ed7c8d7e755405039f3a235e23a6
c3a45aaf6ba9f2a53d26a96406b6c34a56f364abe1dd54d55461b9cc5b9d9a04
1074654a3f3df73f6e0fd0ad81597c662b75c273c92dc75c5a6bea81f093ef81
c613487a5fc65b3b4ca855980e33dd327b3f37a61ce0809518ba98b454ebf68b
7eab62e542e59e2e0c41a46f46c742da571f09b2e5bf79eca4532310b0362af0
4209b457f3b42dd2e1e119f2c9dd5b5fb1d063a77b49c7acbae89bbe4e284fb9
7b2ee37915d9e4325d5372a9524b543919c3698abf735e0c61e0e5cdb81f0cc8
9061f16b2213a4278838416199d0b6839a92d9673477dd24ed119be297792d8e
4cfb1243e8b9e64424f3de3d2144ee512dadd07ba921e0ced38e58e836347c7e
3235e64e6bd9e0d6fd152859a258fed7fe189eca7539a335a6e9f2833fe34820
60e20c926a37535af2dd7af42366791a2c25bb444b2148afef247a7feef98631
7d80715c889029c2926ec76f991e999ec71063c657eb6912cff302737c5549ca
38051b399f29a0c39c22668d62c110a5bb8ffbc8d0ef4b59aca13e8d6c18d2eb
d49b9e94187add8acf9c64583aa313c198f070e2b1f8ca335a21024e6d33f161
1496d62ba1b6fd6cfb85546fbfab57f75b0b3c6915dcce22cfaea9c51a9bd85e
b5331eea1d13abaa13cdb56f0bb1fccdd335b8223a09f8eff3f68ef655568fa9
c0d2aaf266866900552c681ce63bfd4a3b09442a7742d7f20dcdbdd3ec9763aa
c3bb9d1f748d0b1b78dc525039c7a2ebab610a4f0ab7f43d0c5600f2262a62ba
c465238c9da9c5ea5994fe9faf1b5835767210132db0ce9a79cb1195851a36fb
b123d7e7c18f0d3e87f3ffb49b6113c119fd3c4b0c1ba83ef93c06e3dfce17f6
0845bfa3b949b34b94376f62a033e4ea4ab21aedadd82608f3295831877b3bfa
22562716be013e3114c79ffe69a7b19e2e0275ef2aa74e5bf518b225c41dce76
4af18b2314609db33db030b963aa1d9a43cbb627472ed8f9235ef476236ad7b6
e40bebdd65b66ca2afa076fd0f5e4010bdf16b4e326f8c53b6c8871cdc0eb20f
f3a36a3bf1e05c8425cd5d20883dc73c6a678fac07eeaab91b820e422b9fec45
f18a6d3cf01c2f0d46fb23df3ed1e49c7e185b2796f8d54e184a6ea168da0bbd
b6ca88618cca588b11f38310c7455923fc16558c4b34b7644c006d6cd7e749d0
ac96863726364ee362d7ea1c603bd3236c31d5092b918b698bef1b206ed954f1
8b4a4918b9eac70478310878450dd6d2d12c3bcd7203f5c3ce59079cd0dfc95e
d89197e13ab9d93ae56a591d108558c7a20b343b2f143e453fb948cb07949579
b43805374da8cfedbc592cc8fd6c32609a437f0031d1469e72a8c7ca99486461
a203fefc5b72f4c8806d92c32b980e899f874f25f96a9d652e5faf5ff30cb964
0d2c333e089fd28fda0060e8c1ab910e4a91d4225823e33a200f831e8c93d770
650619946a36ec2a6bb74c95a69cd485b60e38656b67f7d814692492bf51c409
65d4414d56fa929464760cf6edca352934cd4f56b0a4daf057008c0615896bbd
f8d11c2dab4587af8236ec6907cf36ed6fa05f4ab75aed9c5347c52fd134a793
373d538c75193ce514cd9ee6315dc30726a5caea3fb78ce4787465c9cf4a10eb
02835ece100bb06ed759f9fa434151870e39c3ad1e429c6aace838e918b43a1a

48dfad0b351d3d6d9db71738b1258a6b8bc598e8f1db0b4a2c13b82e85b37510
0cb82719fc06867ca9a896eb878474efe4245fc9c25f8c9d5b38eddde3c2a5f6
e8926a2c9a1413dd0f63824ea6c76c346705093f29b035b480e32d160f8fe9fa
0832ec4e7a6e59fe03fe7d7614eadd67ceea3f330b309cadb4aacaf05d46ba61
15439972eb851827c3d7643acd4193929c0034b5ce1ba2b977858057c9795fe6
d7c6926938c6eb47fa1faee887dbd103c761392c35f2af82c2fec308b29b53ec
2c7321d8b9905d4b8671c9e16c14665cd29f88460f0c8ec503fc3398b8e642c8
e00b052e63b503507d6b35636d9685cb14114ff4c81ce1fb0425b4b843350f8c
4365fb820df115343e160d8b32be23615a032d1409ce881d4445a4b9261d79ad
7bb5bcc1cb2f8ab248ed20e717d42fdafe6ee107e112e1356af51866212c3642
1888cd56b21a6571193b67166cf61980e3e976f0bb6e9439e6502461260e383b
d7276a9cbe2aa90649b3f7e7bed97f6cc99efcd689036b3f77b82a2849cf53a9
8d587560c2e7448179625d563831e7d98ae27fa722918eef0e0485045181560e
4e0c1f1a705891e28b63aa4bdf1c51a24b635a72e81432cb331daf8b33a944eb
63e8ed9692810d562adb80f27bb1aeaf48849e468bf5fd157bc83ca83139b6d7
7b108c9a51643faa140edcad8b13b00c30c6fefdd21667318a24474cde44f796
40bd6a44c7de50545623a8c9709c1fb2b62e3f1ec4e1571d3b0a68c944a957ed
692abc19ed30132d3d8b5ba2b31268677641ca24a3902d2cfc97497f2b7b5b85
9c6e9d790af34a1cb79be16ef683a4bc5af317dab4b6ef93d6cdb78121720fa2
619513c03d1cd8d0302ba564d6e4252316a3c265110fd0452d018f43f7e72fb1
7dd27691487411149e7392314ece911f62867b894f61e5a706f9a9ac60a4f7a4
5a4980a432703e964c8cc07f6a02b7723a2be2070e0ec7f98b2f5a2623b8dcb7
4ff7a702221ebf66c6d143067eb2a2d2339ca6b65e1d5df388b270fc7b44101b
bcd74869fed12192e15d27254f6736621a82fbdcb555f7a258d0f2fa99eed36e
df3554b884ebc1e8ada4329fcc9677bfb6f7db73b5f17ff279e5d0cce6005c5c
b1167965062b1c63eba259669a898ff1bfd1395f4e9a4ad23e6004bafc10e597
2fb2b9c91ed2da4a80190f15d0b62bd5c0c1708dbcac52f7b4b8b0f5fb43cd17
d701d7d7db2536cc21ca3710872e9d86cba52d409eb4f88ae22b6c75ea924ecd
9d4230faf28fc2ca29ce216c33e1aebd572689d437b135f8aa7a80312227f6fb
0f1b1cb23adb81c4c4fc3f876d3299526c631c9bd97b9bbde7f321b6ac2c7c51
f4f49c5ecb63c21355ee1d212c340c6cc2dafb2a5d95a7494cf4a5d3b2a315d6
c4ba06c532ebfa09645211030b898ac4e14f1dd9ba48d4b94b23c6ded49d54d2
cc930bbc91462a12b75bad92fe916d8fd4b15a471171394e3efc3f8512cc4348
e5dad9637e84732d1e8b0c9973d4ef14365f4f300a966a4a3af6ec1c45cc5683
8fa3a56e3cfd923c32cb3c524bfd9525c7ea6e4dfa27872ed92cdd28474062e3
b7872290479a97f86d1f2e4d2e8a9d0041ac201178ec54a3b1b9345e849b60aa
6fd47d689537c5769ccb8eccdd541e3501789973701d91cbaad3883a875cb8e7
165aec991a1e1be2960d796b3c3fe8b5e0fcbc6e4b72c3182cc719e518fe0ecc
85873815509f47a6027d2ac3b736d62c1c4dc7747bba67e7438f08dc30406241
2c1613c2a9387151854b398fb8d104abe684bd57800857512f068fb84152d355
f7e683987d0e9c80ac75e031765bac0bb9df6fa5b5ea351d2b5850b05c89c9b6
732a026d8c1b9f4f67b700086b4803776f10a8b6e27e82e0c7d1a5873ccd4212
13c4b244bd9f0e609a60e5dd9062006fc0f845146756f3ec74ea2c4a48d58485
76b3f7186bd9e6b24b708fdcd9283b824c1b42f562979e28e5d1291e56090770
c6dc46d2d44d08dbde58abe5f68a338647e34a94f53b0af6fad4cbb0b9e56b97
ed855200be3f4068841654085718f43b1bf94dedb1c791b1d6aa5ebf1b957126
a0c1e35d61b70b0f0ce59e019750617e5f3ab9add117abf3a33ab7b0d784c2bf

d97434c33e8a669772703f14ba9b0be90976596b9972715bedb09c397924954e
dd67ac938272603c1c3141a35deee82c9bead6e60e96331b49427ba121d37bc0
b80e02e5b77e414d73c5863cd23bd9f4ed0107f936083ea53a820decc61d1903
89163d1ab3a2153e12be3d24fbc0469819eb68d79a570a06f5ee20180b8cc442
efe4e1c1517095c36503aecd3ec5b7c9d6c3f9e23cdf23afc358b28fb6602221
8657b3b7336d5c3ac6463eac74bebb482daab30b4f80852cbabf0b86c823d5d1
1bc3f6d84f664dc255d5e34afeb92aee49f842e56897f8eae786efae003ec3ad
83cee698d64d11076ccbf7a2fce301a1b55b52620edf7dd126a8cbedc7283530
1de19b37601d32beeeaec7b5342a84ade05a8e6c500f77d13877e07ca1a1d6c3
be3eaef592009dfe26c8768c143c5734343db823282b8f15d1d71f73c3ce66ad
0b41a1bc8d3b6e90c7d62b82b0bf5a496d34292f4d44ad7d1d4e1ceb3ccb46ee
2b7e99541a29d17c541c31d9b24e4e888350b0a64c43bc87e6955e45cc507793
1d3b5c607bd32db223dad4f647b8fb5265ef89948ff349f2a1776094b2ba8671
255b94fd32d1343188a9e0504aeb4b55e4665689fec7b6778fa9121eddb7a0a0
825bfea146d8e72b09912947f27e6d7896750457ff0a598c87ed9fa7a880e15c
a6f36429189b308c0506a99acef7c8133619aaeaabfcbf378468116ed304b4f1
5f5fac89d925a12972206f346245ba317b027f107a500f1bdbed01e40c065e9b
9797217360ad367d7a0114f79897aba388d6aba4069394baed744dce2d4267a9
6cdb65dbfb2c236b6d149fd9836cb484d0608ea082cf5bd88edde31ad11a0d58
1b449121300b0188ff9f6a8c399fb818d0cf53fd36cf012e6908a2665a27f016
e27fb16dce7fff714f4b05f2cef53e1919a34d7ec0e595f2eaa155861a213e59
75c3b22899e39333c0313e80c4e6958d6612381c535d70b691f5f42afc8c214f
50174311e524b97ea5cb4f3ea571dd477d1f0eee06cd3ed73af39a15f3e6484a
6804be0689bbfbb180bb384ebc316f50cb87e65553d0c3597d6e9b6b6dd8dd3f
4554aa6c2fdd58dfddebdb786c5d23cd6277025ab0355ffb5d8967c3976e8659
8ea275eee557037ab6626d15c0107bdcf20b45a8307a0dc3baa85d49acc94331
45513f942b217def56a1eac82a4b5edca65ebdd5e36c7a8751bf0350d5ebea39
64d7d4846c5dd00a7271fe8a83aebe4317d06abad84d44ffd6f42b1004704bd5
e6020eb997715c4f627b6e6a16947861bce310aa31fcf58448a5beba11626d36
07d94726a1ae764fa5322531f29fe80f0246dd40b4d052c98f269987a3ee4515
4622f8357846f7a0bea3ce453bb068b443e21359203dfa2f74301c7a79a408c2
49baf12f50fec772fdfe56c49005efb306b72a312a7dbdad98066029a191bfaf
3817388a983d5ee1604a8eec621b5eb251cb8bdeab9c8591fe5e8c90cd99ed49
5909c1dcfb3270b2b057513561b2ab1613687a0af0072c51244ff005b113888b
2063fae36db936de23eb728bcf3f8a5572f83645786c2a0a5529c71d8447a9af
b45baac2ae9c5fdfbf56131451962826a95d56f641af8ca1b74738c2eb939a76
9f540ee7ffae3ff53687e08ba2200710980ce5494f55454b406d7b04f6c1d2a4
568298593d406bd49de42688365fdc16f4a584119858352 7a35f6a7d518a6b0e
fbc56623dd4cdfdc917a9bb0fbe00fa213c656069c7094fe90ba2c355f580670
90db021aa59df940e081d55b07a7cde9ac75c5d55450928adb5639af1019ad61
ff0527ea2f8545c86b8dfdef624362ed9e6c09d3f8589f873b1e08a895ef9635
fb0fdd18922977263f78becdedddab7a03c8de16a5431c7b4602e5be13110fa3
d4a6f4a56710ab1f7f41e406b46fdb91c681359b9156eb04ac6e8f4fde896be2
97da4b36fc3cbdd56ea94eecddcf3b6e2a1b7b06d62566b035b20906c0d1303b
4f2ff60e150ef0e0e0a1f21dfd2569ee082e2f470ad5ef774777e8df80739a61
23dfce597a6afef4a1fffd0e7cf89eba31f964f3eabcec1545317efeb25082ed
84b141abbce90a5d7ae71b52dadaa3156586b92a944a1625f6f6edb55085d819

d81ba465fe59e7d600f7ab0e8161246a5badd8ae2c3084f76442fb49f6585e95
8ac21275d0db7f3e990551f343e16ac105d6a513810ff71934de4855999cc9c5
2c2b1d9b34df9364fd91a6551890b0fdc58a7e681713c682221a674d1116089a
87a57f5bb976644fce146e62ee54f3e53096f37f24884d312ab92198eb1e6549
169c24f0ad3969fe99ff2bf205ead067222781a88d735378f41a9822c620a535
3ff1cf65dff231f05bd54df3fecad2545b159094ce59ce4bf4c668c904d2a5d7
79f0e0a0f9c79a9206b9c2af222f026c384d3e0d761b0b42815453991bc05294
9984d5b554b8dbfeffdb374e1c8eaf74af7109a0e6b924b00ad5b878d0188895
bb28528e76649fb72e069b15a76f7c6ef520ae727408b3439856880a4488aa1f
d7786504a09ae35a75818c686b6299870e91d646bdf20609fbee0d86c94a5ff5
ec801e3baa02c7ad36a9b06512ac106d30ab3a2207a7cb1e543fbd076995d43d
06d20fb5894c291fca07021800e7e529371372abff6db310c0cbc100cf9ad9f9
319a06a39e5a1394710ec917f281a546d850386e80fdb56238456b68d5207a99
e114dd78f9acafcf7e93efe1c9e68a29e4fe52c4830431a4aa5457927bef7c5e
1d59968304f26651526a27dabd2780006ebd14925c9e00093acfa2443a223675
a9db9751fe1c9fdad17b289b845bbf87221ba8e4b3b707f7d16b64a957c4bcb9
aa7b1d13a96f90bf539455f25ef138d5e09e27b7da6bf7f0c2e48821d98cf476
ece7f411ed1897304ca822b37d6480ff0b9505c8e307ef152fef8ed183b001c5
63a74b66685fb94d685cfdfadd10917c805239ea079b9431bb5e9c8a58e0ea4b
831212d40c5120824508a645e54bf1b86f3be0cd19f87b8067e8b2fdea5c844e
be7b1f7f0b73b77fc8fe4c109ae5a675cc9f3f6c16d3a1d7b2a9c6ba5a52ef9a
9843ceaca2b9173d3a1f9b24ba85180a40884dbf78dd7298b0c57008fa36e33d
f7231082241d9e332b45307e180f20e11041f59196715749c6a79a8be17fcdc0
b5227a12185a6fef8bb99ac87eefba7787bbf75ff9c99bdc855a52539b805d2e
59759bbdfc1a37626d99dd260e298a1285ff006035ab83b7a37561e2884fd471
a77613cbb7e914796433bf344614e0c469e32a1d52fbaf3df174bf521a3fc6b7
85b0ada2836c76cc49b886dfe59d950a073e9d6d761581075bf904238306e8c4

List of CVE commonly exploited by APT41:

CVE-2017-0199

Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document

CVE-2013-0633

Buffer overflow in Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code via crafted SWF content.

CVE-2013-0634

Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32

on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted SWF content.

CVE-2019-11510

In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.

CVE-2019-16920

Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise. Later, it was independently found that these are also affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825.

CVE-2019-16278

Directory Traversal in the function http_verify in nostromo nhttpd through 1.9.6 allows an attacker to achieve remote code execution via a crafted HTTP request.

CVE-2019-19781

An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.

CVE-2019-3396

The Widget Connector macro in Atlassian Confluence Server before version 6.6.12 (the fixed version for 6.6.x), from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x), allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.

CVE-2021-26855

Microsoft Exchange Server Remote Code Execution Vulnerability.

CVE-2021-26857

Microsoft Exchange Server Remote Code Execution Vulnerability.

CVE-2021-26858

Microsoft Exchange Server Remote Code Execution Vulnerability.

CVE-2021-27065

Microsoft Exchange Server Remote Code Execution Vulnerability.

CVE-2019-1653

A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information.

CVE-2019-1652

A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker with administrative privileges on an affected device to execute arbitrary commands. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious HTTP POST requests to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux shell as root.

CVE-2020-10189

Zoho ManageEngine Desktop Central before 10.0.474 allows remote code execution because of deserialization of untrusted data in getChartImage in the FileStorage class. This is related to the CewolfServlet and MDMLogUploaderServlet servlets.

CVE-2017-11882

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability".

Advanced Persistent Threat (APT): NXSMS

The cybercrime group NXSMS (also known as Desktop group; SilverTerrier) is a hacking group, which uses red teaming frameworks and publicly available versions of RATs for conducting attacks on various organizations. All servers are hidden behind dynamic DNS services, Frooty VPN, Your VPN, several anti-abuse hosters and mobile Internet. Since 2020-03 the TA got access to several financial organizations. At least in one African bank the TA gained control over SWIFT controllers. At least infrastructure of two banks were used to attack other organizations. During the lateral movement stage the TA deployed Metasploit teamserver there. On the final stage the TA gains control over payment system. Then with help of exfiltrated account of payment system operator the TA makes thousands money transfers to mule accounts. Then in few hours mules cash out money from ATMs.

Indicators of Compromise (IOCs)

CnC:

update[.]mcafee-endpoint[.]com
news[.]afrikmedia[.]info
news[.]coris-bank[.]fr
covid[.]ocitnetad[.]com
download[.]nortonupdate[.]com
winsec[.]senegalsante[.]org
update[.]microsofts[.]download
reply2host[.]duckdns[.]org
driver[.]eimaragon[.]org
info[.]senegalsante[.]org
queen2012[.]ddns[.]net
contact[.]senegalsante[.]org
boa[.]eimaragon[.]org
winsec[.]ddns[.]net
winsec[.]gotdns[.]ch
cobalt[.]warii[.]club
wari[.]warii[.]club
wa[.]eimaragon[.]org
gemalto788[.]ddns[.]net
info[.]warii[.]club
bac[.]senegalsante[.]org
warima[.]warii[.]club
lofl2154[.]odns[.]fr
bac[.]eimaragon[.]org
winsec[.]warii[.]club
176[.]9[.]193[.]5
45[.]15[.]16[.]228
160[.]155[.]0[.]199

108[.]62[.]49[.]249
154[.]44[.]177[.]192
154[.]44[.]177[.]192

MD5:

2aa09843321aeced3befa5f7ceca5f52
2c5dcd5c42ece2a91e53914f10b10270
2d03e001d92c099a002692c1669432b6
2d17eb61660c1e4390fe88c9ddefc6c7
31fa90a98da6fc1276662ab5862b01a4
368653e74934b6d649c8d08d66341177
093ba856381c9e17e29a5fc2aadfa9f9
0a11428c5f4cb64bea4905576d30044d
0f304bd73274a6fd4a5b05eb5f0657f7
1be74532a1cd57f5c7c02de4549384dd
017ba3cb35528108f6c4e05db99f3572
0258f4f0319fa77b10978dd92edf87c1
71621e1a35137ea2a7c48db9bde0298c
7444684c7152c6089e68305c36f585e3
782e17672213b22dae0a20397ffc3dae
7ddee4ec4650bf7836478ca8f286ac10
7e2801b8d44eb6bece5b3b5467242111
809f42059da3058a1e62fa7ba56ce66b
dda2894e76da57dca989e37f4a210d34
e37e9402a3a63b60065eaee7c552f514
e8848f591f9cd537e1feb84a54fe18ff
f1bef120cb72066000e67171ed5193a7
f39e284c2fcf02f7aea3ba7ff47349cc
f63d75f66574c346ccc2a2f6b7f3f01e
f7533a09f0bc3b7e9317c65050f987d2
3cbe2c4d95d10a0d5f1d33db3e752df0
44069f273916002a782a737fca6c140f
47777cb7a44e587e1c39eb4b7aec6ac4
49237e35bac0a1625fde93ebcadeb58c
5501196c0134a5a9eac0dfe250acd055
ac4c38200c6b668ea188d92f9f526b7f
af67701a6387834d2195282719ef6636
b180eecc6beb4998bcbe40b226538026
bace201a0f9bc25dda6b288e22023f61
bb592a79fd934e30df6832b67b918923
bcc73790f7b2d37704976cd78095a9e9
c4a0b6076fdd71b6dbcf3125434cb8e3
c9194a86915eb04b8293183dada19e79

ce89231981dc64542c76f64979639826
ceb73b19f731fa24fca9a6b55ffe910c
d1d1749cc28a05873b26594e6742f228
905b386750d2977f116ac8805c030492
92de907d5d84361487288088b0b28c40
a0873962bca482a7d14dafbeaf5346cb
a9ab4f14d339eb15d8209b13a51ce989
5aa2bc6132915f9ddd56b7fd17f992e6
5f9e1eb02be8edfe26d480fd78f065d4
63417ec71d3c7670c2306afc4164b0de
fbec4459fbf7018db2a0148406d8196f
fd4f43af4b47683256b31e74d5bdfb9c
f7e6e117024b8936cf0f3ba1ac303a3b
fb6c7eb4f64f699511380721e9c8cabb
ffea49fca3098180dc03037ea5f87138
4f06d98642b9a8c000128c66bea6207d
4fbf342ef3e828fe28ed4afd7dd955d8
58c6fa3caf152bf781da8da64ab52799
5a4fa5c58234034800ba1a929c18d278
5d9d7de37e423d33aec86617a750662d
2178d1efad5f2a1f7400e0d6d0a263f8
218ccd13162c76f4a251164917b8c7c0
2b83d157f134a0388d6b48a4fbb85bd0
2e5af496face122157e459e84e5fe14b
2f53f7e0e4dc0aebd7c73abc1460bea2
306447863f89c6962fc5c16517c8fb9c
67caabf197df108e2a5707f198146ac1
72902ec0df95a7dcfb3b66f9b02ef7f3
7584fa7ded7aed3b38635274719b7966
8061ba44ebc7cc1adb5dc61c903f541f
351cbc60e73886519a8e1232adf80f28
40340722aca5dc78ab182ada40f01bc2
49ad6020376caba051b4d6a6578efc1c
4e14c0aeb2e3f660f3dcd831fe5bcfbe
92492bbeaecf7d28bb9f3e52d845ebb6
9810a7e072a97aee69126d751afc3666
9d5696758c45cceb3405a62af931c11d
dda5a9d262181339921c04902bd77173
f24a401dc5974e995a2cf98f03a42e17
b1de80dc4a1d8122909f53a101802449
bdbe1fbfb2085e6a3d1a5659da5bd409
0e695222e2244eb32c461ae50ea05174
13c07511ff89f1567a8f39a5215bc884

cf7d3cdb8806d59c9e3b4a64d46df62e
db37a5c00a956bb8d6cc18974992a2dc
dc33c287ffa253bc5af591e7f40877da
e4e6b52047e6b3873497757160753930
e8e6362100d9cff8152221c5fcad20d6
f7b0cf59a52e2c03a38bd6d04aab47fc
80c0cd9971c1d458c40a10ffc54ec35d
834d61aa653f8503aa36fffc9774b2b6
85d11ce9d46580ddc993b5d34fec5bea
88fdbd552303bd33e75c37c7b13cffab
8cd17229113b8f57d7db6b2719f93f4d
91ea7988b73f38bd6ad80dc127eb0c46
97bfda8cede4baec095f0f24b4c47a56
9bbf6882f33bcdddc34fb7508ee68b31
9d61b753e7073a70fb6f4b577c9270f0
a3dfc62d3739990c96912cc3b92aa56e
bed4f32f0d6f97feee6c03f287e1832c
c1523055a02b61e0f4ba87547b29ec0c
c9a5a794de0c80f844549555ce399118
cb3ba453d968d027e975e43296e9bc53
64e61ec18ab4336798f667c4465a7b58
670a05010ba9c97e7451e1d7896801ae
67f6cea5ce043f1e4872c357d2752379
690d63a3dd05649f330df67b072df337
7efe472be826bf387545117b3e463fed
a963112260daf1fcf30f394a21e123e1
ac40121e057c198e64d5fc2e29169787
b0ec0169142b1c63f4e34ac18371ce3f
b17079b1169f9a0017eac2c21800b6ce
b24780ce45ac7bec621729dd46d06c27
b6c707729ac8e7fe2f6d358b5dd2736c
ba6d2148ecff70e2134953df18210c15
5ecc4ad7475caef78f0e035aa277b51e
612a09cbcd247344fd4bd5854242a241
62fa2fd8ddd36330840c643259ae52f1
63c7f3e2eb52298bdb9641b8ac319882
043956a214b56a2efd323ec305a813f2
12ac5d447435c45fb53f84b299469922
1df5c1f71f3cb82b697e4170cc81b188
22fe5107805f9c5f1ce8051c9796df18
24aa5d597961bc1d902c5462052a1250
3c1e90e8b5d180ff0f5455dd92bdb412
3d79e91b1382280535596ce7eaa5e29b

0ca97bf824c3bf16818f9830c0ba83a5
144aa70f1c115d4288aab5970e1d2c5c
21bf477dbc9eaca77e0d7e77856bddd7
223269efa93bc8d4d3ab3ec1e5438f16
2fc48496711a25b875808162a5b0c51e
34499495a77a34ce3a58899089f97062
df88175fb96cad1ca9605db2352ae063
e2b0d44be0970b740afc27ff82bb29bf
efa80d8591424baf4020f6af6d31264b
f58ccfae8b60f37e8d612532395170de
f61a31de0f8478b9b4332ae321b03c1b
f80d3f12cc2625e3ea4448429ffb7520
f82e14c44a62e332b539e3347dfc5461
fafd580a4c5faae28a82a2c2487f0b66
c872af5d1182e865dc72e23fed938b5c
d1b2d809addb30c85c8344336f3bc6ff
d440dd5375fd1dc90858cc4d2415b5f9
d6a3f830a51ec64acaab361e056f5e0d
d75b86a6ea82cb86cb050fa5508617df
dbd7a7cc06ca8e4c5ccc5fb901271d80
8dad3becaaac2e3a9224a9de5bb860cb
9425024fe2b94a9c7cdf8ea60a1fbdb7
9768250c8ad2861dd46c1a2d5f9b0ac3
9c38991c3770b0c2917659bdb7091ed9
a69f9a26f8cf8abddc0e105328198766
a7927c6b141eb7ec51eda967f17a67e3
692170776b27e820f7efe4667783afa2
6ccdc868a729510a1c2f3ce447e1de05
73a7a35cd9dc8d219b1a48a8c8251908
81866c3973dfb844c9e648c97b5b55f5
83666313229db6be218d11cfec325ea2
8416149a694a4ad8b54ae06579f56908
37502ecc7f8575055873f92719e1c7b6
39b914a406e30d93b0e41dbdfa4039b3
3a60017847cf09f334fd8a2d0b001543
41192fa3d772ce5659e3b544b941398b
4b78df00aa863bc8b581b33289031500
b4e0f7eb8cea6ccb43820330f19762a2
b9943a25caed8e251a9580ebb6148137
c2a287fae215fa3c4ae4accf5186d014
c2f14513b0080e13c4fa20ef5c1ce8fa
63649943c1ffb9d650d73bc375b6f224
6414928547ef254886331378cfb97be1

036605bb349eaaa2516170e4e90e0eac
044e0bb14076e83bcd38c537ff328f73
10260f016285a196e245493a0e50681a
1305f4fe0f5032c82e3dd5ca4ecae235
13e7c5ad329a3e3c0568d27cc2242af6
14bb5b6f4f94285c366b456ee5a65bc0
2c13a45f665e4123ae590f08dfbf4274
330cf14b15f441462554917d66f4c4cf
009bcdb4cb4784df7e366921c523db16
9e770404e3b0636846aeb0b89523f472
a50622b8f9c48a28627dcf3df63460fb
a7ac14fe5391a94fe5c6bd7fcb2c60ac
a822a9c8655ff10488655bdcae619524
aae20b78c9bcba19e95fc56a630228a0
5920d3b1b09e132f6a0f4c2e43e828d5
5bda2488ed7628af8b068811258f5e10
622bfef24d3278eef4ca0f50af8d777f
6474ce389aaa84ee9ea3f5209a9609ca
c5821ff549fa52fe8df8d43a03fbd32f
ce83775b68686c01d1c45fe47d8e5325
cebbd06d6dbf99ab1eb868310f642027
dc1e1506c0c03663233911f4d0a22c70
446a6e8c3876959ba1695899fe3584a7
472873942f0e7750ced3bc42c0b469f7
4f27b4322117484847c7021a5325814d
588afc20615b110b8bc0365397c3dbbf
bb431f144ae22c06662fcb0d64dd6b7d
c01c90d7d742108055078b657250cb80
e89790f614197291933982e26f9214ca
f2060ef4f0e02bb9f96f4f0ac295c03f
fddf19d5410019b32d26ccf6763f2a40
fdfe13661dd743d884e5b92775c89102
75549471ec54ba39f33ef636ab3dd700
3ae956f12a7a0d43aea8c6819d4a4d61
37240381d523afd3f81117fa811b12c2
3671872f33a75317254ce80656ee6da7

SHA-256:

9c27d8cbcd2398e8f20ce60d12164e165945486249c554e706f43f576ec817b0
c7d3fe9a84e891a05ecdc6b117edb75cb3c10bb18a611a08ebd519f17beb50d2
e8a6e7c538c293b0ec26e0ac3d24954dd7412c153567c9dede0c1f74b3dd6b9a
07191e65af30541f71e876b6037079a070a34c435641897dc788c15e5f62f53c
f689ee9af94b00e9e3f0bb072b34caaf207f32dcb4f5782fc9ca351df9a06c97

4b91c28dcce545ddb71906d6002f550cf1d46cea0c29bb3e21ee027c82f2e3ea
011ff6f5a205fca08b44b216bd67519b7f8ad1c995b92eb5712b3fc8a971d829
644985bd33d378f4ca9fde53e472652a6d175cc14e202e4703a265daac774a24
0f56c703e9b7ddeb90646927bac05a5c6d95308c8e13b88e5d4f4b572423e036
85bd47cc708f80a3e9aebc5948404017053eec1c316f2c3b527011f19597ab1f
ed86e53cf17911199047a01de6fec851f36aeafd403e3e548e6f3473d053be54
ad6b98c01ee849874e4b4502c3d7853196f6044240d3271e4ab3fc6e3c08e9a4
65f2bf2bf25524b4b9c41e4ff55ede002cc527aab0840c5bcbeb06f7c245227f
79e54e56e37504b49ba64374acae3339974339a6217bc7b0ab57754fa0dbe0ae
f4072066def52ca1473ab460108b53f30efdd8fc3935740773bcec88a643372b
1db91e71006a6cbf71e32cb7451089f6adaba1883a203ea9d079abcc9d9bb82b
598002e121633a6f9a39bd2f6848b1d1e01055685f3b7915eeb54aafcacf0f56
a5e470bf946c8f2b70d6fabcbdb2a817d44bba2a02dd7e98c483550b7161900e
b135ffb7df2742e0558ea1b44d3f4fbfe2165061c01e0367af5f977c9dbc3356
117c66c0aa3f7a5208b3872806d481fd8d682950573c2a7acaf7c7c7945fe10d
7d5e7ae8a7f40468938956f23e664e3eff2e32fd434e20df1f152fac95bc00a8
120d278f1849f462ace6bd00aebae7110337ed76bf580f81b60bf7b338bfaede
aa58aced5c9eb9018ba2c16635ca702f4e1f12fbcd0f6aa61b3901c0c0ba7824
45a92acd42405ff1ece0e1cb3a8a4f5744ef52d1b2ffba9e8b454f0a5ae98a06
4c7413ebe361f24b945a61011b4841762aaa261c5462bdac7a53f4d027a062ff
12435df15a836c3d34cce9b4b13d696e94014a9fc9cd5f1914d36fe81fd37319
c1cb02c3dd98f7895467dbbdc9222e2e50a18f6813c38b97f8e4e70d18889e20
5b6703c8d6dee6919c7daec1f56a8bf43c5a7dcca30a84964790f6e71d4aeab8
e0a3539495ee5caead28edbb008d21b9676518ee75a2cea523dedef6baf73ca1
69f9d65de13dc3c8244b2b3301bb6fc2f6010820eb7ed838e16cc242e0cee9be
148ce41bf5adbd59f5b472e04add09ae7a9e8e72b4d6a370599f695c308a2a9b
ad39123a6867487b2a8bd785f78a9e094820b6963298a4e11d1b97220119ce35
1db98f39f4613742185f76e1da9e1fad82ac537be7af0621f594a157039566f2
6eed2122af8b437db0aad59f6eb3c817aa84e9047c7043d7fa60cf171fe63463
503a78b4323f2db34f2da78833ae191803cea4827b9b931ab77a7feffc275eb5
368b40cd95a5e5fbd6b81c8d064ab6d6476d80baddf162cecaabed39323d6b73
1c470e31be680117034815393b4a0ff8b8c46d97b0e7c0076f93ff32c1ef26a8
d6859dc3fd641ad6569bcf207b04085e5a17612460adfb96ddec79cffd525a66
b6a4d7d59bbd9e2f914e36d6b2146f5293d308882900656e75f2d3046a64c360
6516eeb8b47307826abe8a1edabac1f86290df84412c5f62427c49e0cdee1d6e
e80166fef57fddbb2f17966ea95802ec07560d0b902a5ca86df366b36d2d7d4b
c56c915cd0bc528bdb21d6037917d2e4cde18b2ef27a4b74a0420a5f205869e6
13c04aec50077624a7f9fa72d848a160b72a88ae5ec5fd2d2882777238d8f619
a6e6b44c41e3b659df057e7f02e5ec4c7eddc13b20748c66261653e25a5c88f7
1ed1b3e607c00c06d6fc0de65ef368448f6b0bfa415fc10f0e3e78bcb1b652b3
73b7e029804027045d85e9c1447a6a741ec026bafa746dc742738348a8e6f463
1baa3d58bb56b56bda4bedb2a86c4d75a61dfb140d40ff61bb5bc6f0773b05bb
4948bbce41be2d6ef71d4e7130f3c20b645fdc52fadff920a9ebc2fcbde38a9a

e9022acaeb28b9660c46198989e9fbfad998a2ba9e32cf53a1e009505c07f983
461a6b154aec27488c61635e5a4379590fe0cd953e777875acb0bf97f270c245
61c4d908df19d8e4a92083b55e11264ba6f15fbe0fc3747a49b2458ec71db436
f0c947dc52ef25ec5ae2dc9ea95e1b068ecb5869cfe6a894babb0dee690a1ac1
7af7b083ccaf83c1b1b4c7083b4c121472846f1b7343a0a83c883a8561fc62dc
b8f7f9119f2a8e5cba174d32da0ac9481f262971e0b5c0f5827da89a2315cb3d
83d1b796c474245c077eae07daf47ee996632dad12295fd366e6f8b4e3c86dfb
72adc4390e3cebb01f946fea4c9021b0fdc993ea27d836836a3cfe5c4469ac09
eab5a2a023f676cf2182b41c6f66d18931ece859fd7ceac241e321c72070c7bf
83e2264e6f9b27e081c6e93c5a05b08d3c9f072330cab02533d7e30ff0415380
80b9a4980ba13d6fe1e108bb035f46cd4bf09213a75f17f8288e92b20184fc5c
26d62fb1ca77910b4ae35e3868c4c1e45fc58b9261a14de8a39fb0ba3144d943
6a482d0ce43833040aeecfd4cf1947bcc803004d5ec6adad6f74deaa81d346ac
b8ed318330c822cbe1fbc25ceb197006d836facb1d8a079e1397e48e24b9531f
20c48e607351969eb0c639e7d26e47a598c229455ba277c0be66b47801f9f98d
32d7779dd310728b8ef1037fbd58448d07a19131422e7ee8d8ad2e8684a09e24
b47213e2ff24ebb55506a92f473983e98690c0ec6e151dab912b35d6b6e70980
d6d5c9d7f6e744830cad4dc27f12b036e384475d63880a6a369bdeea4fa662b4
5fa560ba956e965558dfedd5af72a3d7a7946f830c5e82f9f1dbbf0b768950e3
1e77ab61e139f4d681aaeb72a339a3f2ee88b68638f6f846051297dea229702a
570b1829935e3f94a0fa3ca0fb40465bd89209e5972bcd5d99182bf783844d4c
19da52ee67a0d40ed8e82db7d8f5265b71821c73dde2957c688e166f4dd81c76
611308b920be55b8ab0d58d9109ea3de428227babc81c850552627f8cd9f3b39
f092a0f4719ccbb78b250e9374fa908face33f836c713df00863042feb7a3bd8

Advanced Persistent Threat (APT): HAFNIUM

HAFNIUM, a group assessed to be state-sponsored, based on observed victimology, tactics and procedures. Its primarily targets entities a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. This group has overlaps in tactics and technique with other hacker groups.

Attack Vectors

Exploit public-facing applications

Related Tools

China Chopper
ASPXSpy
Covenant
Mimikatz
ProcDump
Psexec
Nishang
PowerCat
7-Zip
Nishang
Psexec
PowerCat
ProcDump

Indicators of Compromise (IOCs)

CnC:

http://p[.]estonine[.]com/p?e
http://188[.]166[.]162[.]201/update[.]png
http://cdn[.]chatcdn[.]net/p?hig210305
http://cdn[.]chatcdn[.]net/p?low210305
p[.]estonine[.]com
cdn[.]chatcdn[.]net
192[.]81[.]208[.]169
203[.]160[.]69[.]66
182[.]18[.]152[.]105
167[.]99[.]239[.]29
157[.]230[.]221[.]198
165[.]232[.]154[.]116
5[.]254[.]43[.]18
104[.]248[.]49[.]97
45[.]77[.]252[.]175
86[.]105[.]18[.]116

161[.]35[.]1[.]225
13[.]231[.]174[.]2
104[.]250[.]191[.]110
161[.]35[.]45[.]41
167[.]99[.]168[.]251
185[.]250[.]151[.]72
5[.]2[.]69[.]14
80[.]92[.]205[.]81
89[.]34[.]111[.]11
45[.]155[.]205[.]225
45[.]76[.]110[.]29
103[.]77[.]192[.]219
104[.]140[.]114[.]110
108[.]61[.]246[.]56
149[.]28[.]14[.]163
211[.]56[.]98[.]146
91[.]192[.]103[.]43
161[.]35[.]1[.]207
5[.]2[.]69[.]13
110[.]36[.]238[.]2
114[.]205[.]37[.]150
209[.]58[.]163[.]131
58[.]190[.]46[.]175
90[.]230[.]190[.]92
121[.]154[.]50[.]51
121[.]176[.]145[.]25
161[.]35[.]76[.]1
188[.]166[.]162[.]201
103[.]212[.]223[.]210
110[.]36[.]235[.]230
130[.]255[.]189[.]21
34[.]87[.]189[.]145
46[.]101[.]232[.]43
46[.]23[.]196[.]21
49[.]36[.]47[.]211
78[.]189[.]225[.]136
1[.]9[.]2[.]18
103[.]135[.]248[.]70
113[.]173[.]3[.]225
185[.]65[.]134[.]165
46[.]244[.]29[.]17
200[.]52[.]177[.]138
213[.]219[.]235[.]158

218[.]39[.]251[.]104
112[.]168[.]90[.]84
119[.]231[.]129[.]222
122[.]213[.]178[.]102
123[.]16[.]231[.]247
1[.]36[.]203[.]86
1[.]65[.]152[.]106
108[.]172[.]93[.]199
211[.]177[.]182[.]80
23[.]95[.]80[.]191
128[.]90[.]21[.]223
159[.]89[.]95[.]163
124[.]5[.]24[.]161
167[.]179[.]67[.]3
104[.]244[.]92[.]215
31[.]28[.]31[.]132
39[.]123[.]17[.]120
58[.]126[.]135[.]235
89[.]147[.]119[.]227
104[.]225[.]219[.]16
116[.]49[.]101[.]143
117[.]146[.]53[.]162
119[.]197[.]26[.]38
185[.]224[.]83[.]137
219[.]100[.]37[.]239
219[.]100[.]37[.]243
31[.]182[.]197[.]163
170[.]10[.]228[.]74
185[.]171[.]166[.]188
108[.]61[.]171[.]184
185[.]65[.]134[.]170
34[.]87[.]113[.]30
139[.]59[.]56[.]239
172[.]105[.]87[.]139
179[.]1[.]65[.]54
182[.]165[.]53[.]4
201[.]17[.]196[.]211
201[.]208[.]18[.]226
202[.]182[.]118[.]99
110[.]39[.]189[.]202
121[.]174[.]31[.]220
61[.]82[.]150[.]49
78[.]188[.]104[.]84

104[.]223[.]89[.]147
139[.]162[.]98[.]150
219[.]78[.]205[.]63
5[.]189[.]162[.]164

SHA-256:

31a750f8dbdd5bd608cfec4218ccb5a3842821f7d03d0cff9128ad00a691f4bd
508ac97ea751daebe8a99fa915144036369fc9e831697731bf57c07f32db01e8
c0caa9be0c1d825a8af029cc07207f2e2887fce4637a3d8498692d37a52b4014
5e09ea8b70a386f0812a8cafb94e2d2365849ce67fda42377389f18e56d860d0
5ac7dec465b3a532d401afe83f40d336ffc599643501a40d95aa886c436bfc0f
0c5fd2b5d1bfe5ffca2784541c9ce2ad3d22a9cb64d941a8439ec1b2a411f7f8
36149efb63a0100f4fb042ad179945aab1939bcbf8b337ab08b62083c38642ac
1e0803ffc283dd04279bf3351b92614325e643564ed5b4004985eb0486bf44ee
d9c75da893975415663c4f334d2ad292e6001116d829863ab572c311e7edea77
c7e1b386b472a26a36632f4ccc25e37458546b9c864b7ef0ec5ebece5e8cc704
ee883200fb1c58d22e6c642808d651103ae09c1cea270ab0dc4ed7761cb87368
d637b9a4477778a2e32a22027a86d783e1511e999993aad7dca9b7b1b62250b8
bda1b5b349bfc15b20c3c9cbfabd7ae8473cee8d000045f78ca379a629d97a61
71ff78f43c60a61566dac1a923557670e5e832c4adfe5efb91cac7d8386b70e0
c8a7b5ffcf23c7a334bb093dda19635ec06ca81f6196325bb2d811716c90f3c5
be17c38d0231ad593662f3b2c664b203e5de9446e858b7374864430e15fbf22d
138f0a63c9a69b35195c49189837e899433b451f98ff72c515133d396d515659
eb8e4845bab4a3ca0b85f3c659ca39c8719d928d0269cf8d977eaf4d10c49557
0bec4813ac09bb0de24725afcd62b44e0075031730186747f743329f64a2280a
94512C434290405BEFD159FC3C4ED01F18722F966D53DAC45760DD36C4D9B918
0D648339C975CF04F6C8DC99CD09EA508F16C553A47847B522341CE5857424A2
EE91A2ADF1581CEEAEB690125A60A3CCD94B98ECE545679D1E95E609AB9666F9

List of CVE commonly exploited by HAFNIUM:

CVE-2021-26855

Microsoft Exchange Server Remote Code Execution Vulnerability.

CVE-2021-26857

Microsoft Exchange Server Remote Code Execution Vulnerability.

CVE-2021-26858

Microsoft Exchange Server Remote Code Execution Vulnerability.

Advanced Persistent Threat (APT): DARK HALO

The cybercrime group "DARK HALO" (also known as UNC2452, SolarStorm, StellarParticle, NOBELIUM, NobleBaron, IRON RITUAL) is active since late 2019 with espionage aims. It has compromised organizations across the globe via a supply chain attack that consists of a trojanized update file for the SolarWinds Orion Platform. They used following malware: sunburst, teardrop and cobalt strike beacon.

Attack Vectors

Supply chain compromise

Related Tools

GoldFinder,
GoldMax,
Sibot,
China Chopper,
VictimTotal Sandbox,
Koadic,
Sarasota script,
Cobalt Strike,
Sunburst,
EnvyScout,
BoomBox,
Sunspot,
Teardrop,
Raindrop,
NativeZone

Indicators of Compromise (IOCs)

CnC:

http://jenkins[.]findfwd[.]com/sk-jspark_init[.]php
http://alertmeter[.]info/sk-jspark_init[.]php
http://176[.]10[.]118[.]136/pwrvw[.]ps1
http://185[.]43[.]220[.]214:80/Invoke-SocksProxy[.]psm1
http://185[.]43[.]220[.]214:80/pwrvw[.]ps1
http://38[.]135[.]104[.]189:80/46tt83y6[.]ps1
http://roofingspecialists[.]info/file
http://test[.]directfwd[.]com/sk-jspark_init[.]php
http://188[.]138[.]71[.]62:80/p0fd798[.]ps1
http://securesearchnow[.]com/sk-jspark_init[.]php
http://173[.]232[.]146[.]12/Invoke-SocksProxy[.]psm1

http://179[.]43[.]141[.]188:81/46tt83y6[.]ps1
http://185[.]189[.]151[.]178:80/Invoke-SocksProxy[.]psm1
http://185[.]189[.]151[.]182:443/pwrvw[.]ps1
http://185[.]99[.]133[.]129:80/p0fd798[.]ps1
http://freeresultsguide[.]com/sk-jspark_init[.]php
http://179[.]43[.]141[.]188:82/46tt83y6[.]ps1
http://179[.]43[.]141[.]188:83/46tt83y6[.]ps1
http://185[.]189[.]151[.]182:443/46tt83y6[.]ps1
http://185[.]189[.]151[.]182:80/46tt83y6[.]ps1
http://91[.]219[.]239[.]43:143/46tt83y6[.]ps1
http://91[.]219[.]239[.]54:81/46tt83y6[.]ps1
http://91[.]219[.]239[.]54:82/46tt83y6[.]ps1
http://coloradospringsroofing[.]info/file
http://rtfv[.]info/time
http://185[.]14[.]29[.]246:80/Invoke-SocksProxy[.]psm1
http://185[.]189[.]151[.]182:80/pwrvw[.]ps1
http://188[.]138[.]71[.]62:80/Invoke-SocksProxy[.]psm1
http://91[.]219[.]239[.]43:80/46tt83y6[.]ps1
http://91[.]219[.]239[.]54:80/46tt83y6[.]ps1
http://141[.]136[.]0[.]4/46tt83y6[.]ps1
http://179[.]43[.]141[.]188:80/46tt83y6[.]ps1
https://bigtopweb[.]com/wp-admin/admin-ajax[.]php
https://panhardware[.]com/files/documentation_076[.]pdf
https://panhardware[.]com/wp-admin/new_file[.]php
https://bigtopweb[.]com/files/page_306[.]pdf
signup-now[.]com
tanzaniafisheries[.]com
twimg-us[.]azureedge[.]net
admirer[.]onehourcfo[.]com
freespace[.]givingprofits[.]net
group3[.]pulsedesigngroup[.]us
phpmyadmin[.]xsunx[.]com
flowers[.]thegardnerco[.]com
moreofit[.]cn
combat[.]strategyforgood[.]com
context[.]septemberyears[.]org
daddy[.]stlouisdemoday[.]com
defender5[.]coachwithak[.]com
joke[.]webproduct[.]info
joomla[.]lifepath[.]site
pixelapn2[.]adsprofitnetwork[.]com
plkiu[.]daniyalmedicaltech[.]com
snuff[.]mybabyrose[.]com

time[.]suehyatt[.]com
roofingspecialists[.]info
coloradospringsroofing[.]info
robotvice[.]com
champions[.]gdtc[.]org
lamarfish[.]com
d3ser9acyt7cdp[.]cloudfront[.]net
bmlor[.]750[.]credit
gallery[.]wineadam[.]com
inferno[.]bigpurposebigimpact[.]com
method[.]nonprofitsustainability[.]com
q[.]promossupply[.]com
rock[.]core-thought[.]com
standart[.]sdtranspo[.]com
flowers[.]netplusplans[.]com
pixelapn[.]adsprofitnetwork[.]com
printing[.]laminatesandthings[.]com
promo9[.]promossupply[.]com
prompt[.]powerofpartnerships[.]net
zombie[.]susan-hyatt[.]com
pointers[.]ecostratas[.]com
popcorn[.]net-zerodesign[.]com
40ort[.]750[.]credit
fanta[.]swofficefurniture[.]com
moreeu[.]cn
adagio[.]betterworldshopping[.]com
backup[.]awarfaregaming[.]com
builder[.]visionarybusiness[.]net
inspirer[.]cartsandmowers[.]com
lion[.]vipjoyeria[.]com
rtfv[.]info
test[.]news[.]pocketstay[.]com
sense4baby[.]fr
eyetechltd[.]com
megatoolkit[.]com
nikeoutletinc[.]org
7hpaqi751fqoei2fdv8m[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
globalnetworkissues[.]com
solartrackingsystem[.]net
deftsecurity[.]com
kubecloud[.]com
seobundlekit[.]com
thedoccloud[.]com

webcodez[.]com
freescanonline[.]com
virtualwebdata[.]com
digitalcollege[.]org
lcomputers[.]com
usaid[.]theyardservice[.]com
dataplane[.]theyardservice[.]com
theyardservice[.]com
worldhomeoutlet[.]com
cdn[.]theyardservice[.]com
static[.]theyardservice[.]com
bgh8g52s8toi9ppqun022dioho7r1p0i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
j8cctvevmnkrbl7yun022dioho7r1p0e[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
vrh5lnjsgqo2hhnaun022dioho7r1p0e[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0ms9s6cmpd7s3mhcun0c2dioho7r1p0g[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0vu9666cp41semncun022dioho7r1p0i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1mc0ar8vrdk4o79dun0b2dioho7r1p0b[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9bdhkuc4n9mufe5lun0c2dioho7r1p0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
sjs8jtah96r4mbf6u30o2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0m45lsmf43lrf35bu30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
28rc1mao5cs2ru9du30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
4gncu8sn0lo2q4rfu30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
7vehkko1bf1lhfniu30t2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9vp0k6bgsfjihepku30b2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
agv3v4qvhhlbticouhu15o0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bi8d3md8ptapmapquhs0oe2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gmpla9g4rlfkm1hvuhs0ce2sd02ovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nbkg2k5i60gl4rv2uhs0ce2sd0govir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rlnjt31g18d5h1c66iu550eire3vo2v0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
hmq2rp92qtfss85w00h4dkr20fgaaobd[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
s6l0iu24v2j1s796urso2ve2sd0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
q3vcrhhcmddh7rl5oi602ou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
qipotpf1jic4gav5oi60eou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
r69ncekf56jlkkr6oi602ou6iuir02rn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
s131pfib6s2q5dv7oi602ou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
vb9u8elfnbj6nknaoi60cou6iuir0orn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1bsem60k5hc76tldoi60bou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
6gk48cm1q8t4ih0h6hr60b2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
hm4tpjrvee033stw6260lun0i6iuir0i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
birhrvj80ukmt1pp6s20ewr6i52s0bnj[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bjkjagkfb84tob6p6fdrso2s0b12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
m38bgi18f5jo7ad06qn0g12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
uidpastj7df8i9p8vwonou0ee2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com

6os7i8v1ah9p0cnhsee50bsf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
t3ekv1k8omhjq1p7srd6sw0ge2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
hlosr7obo8ml8uvvsodiu0oe2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
81jsr14f06rvqrbks6i0iui1uvio60kd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3h05ngfoghciciup07g12qn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
j2pk60f7g1mmbk81gmclr30[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ajhlj8sfkjigtrrpho11rntrwo11r0t1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
q8vmaei8n3dpeui5vr2d32i2voe60be2[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7cbtailjomqle1pjvr2d32i2voe60ce2[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
i71nka0t074lcp1xoi60eou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jftn02th7ba7ru3yoi60tou6iuir0orn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
jjg2q47bfg7ode1yoi60tou6iuir0orn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jljm963j1kbtuu0yoi60cou6iuir0irn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lr3gsae383m0mqe0oi60bou6iuir0orn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bt19h4euuk925fgui3ugma0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
4ivorp1rr9p41krfiwb0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vfu4rlfpmrfkd159fo60tjrvi02rnf[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ivkg3dh4ghpj52mwfveoip0enj[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
97gbn1m22jleff3loi60eou6iuir0ern[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
afub5rfnofv2j80poi60eou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ggjq9c8j8nb8ut0voi60gou6iuir0crn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
0eke91jkeq78b5dt6cpqml0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
tvt2f17hnoh0106800q49s2of12ql2o0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
bclkdenuvgbekmcq00q49s2of12ql2o0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6aos6mvt2k3ncngt9or7mc0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
6cgiqb15s82mdnti0024l6bvvgjtdi30[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6r2prvobs5q5bbdh0feaaso[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
6uf4bacj0cp4ss858303[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8dpdidaujmnltutej6l0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
3dkshcl4115b13t24gu0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
3eppf9a5gmjktotjbjl0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5ig5c6csfj4mdgkh004udkr2ftq4qnfm[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
avn0o2schlrh9ocp00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ebb5h6ad0cu9bs2t00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
f38tp3nd09pr2c9u00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6fgvmc6q9lrdt51i00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
6orv98cc9cgd10ri00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7l3nb77le9idv0hj00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
h6qtppelj3tjlbkw00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
j777r2f04t42bsny00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2odoa9fkjffh7g9dmnmove0ivri[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
02m6hcopd17p6h450gt3[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
b1imfaabnfvur00p0ee2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

6gc819kpm58pmggh5u0e1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
flhrl95764f8arnt5u021e1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sobu56rbhn49ja965u021e1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0m5v1trnfqd7j71cq22nsf550k6uqprs[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
qo046rspifbl4k04e2mvri0ge2m0te2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
sj2h2et2iv8i4rm6e2mvri0ee2m0ge2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
610ol17ptgqa9i5he2mvri0ee2m0ce2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
dgg9g9ls8gvqepgre2mvri0ie2m02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o63cev8obs41d0f2e6u0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o7ccffjub0u1b5n2e6u0c12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
u6i3eqc3ss9vdc08e6u0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
viq0bl2gfpotfdr9e6u0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9fs9rj4nhh8e32lke6u0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ardfbas1tdfmfmpoe6u0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
blqco7jgoko1v9dpe6u0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
i1cafiour5u5bnlwe6u0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
jc18hh8e6ak7419xe6u0o12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lg9toko1gni0vrlze6u0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
66p07i585li1urdhou0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7luke58qlplnhp0iov50one0ovri[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7349o3up6eu17qijoi60iou6iuir0grn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8b6vf62og4o56udkoi60gou6iuir0crn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r7kqk893t5lu82j6uhs0ie2sd0iovir1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
pmiagmur2r6nmkq400h4r4f19uh4tor3[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sgl76n6her02qkc6cic0bu7[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9oc14sgc4n0pt71lexr08ovirsvu10ee[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r1q6arhpujcf6jb6ervisu10odohu0it[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2cd00j4gv060m1lde56o0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ugrh86s478m9tjq9nhw0c6iuir02vw0i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
6j1ba655onr4ic0ircr0ge20ts2uv2jr[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
dcb9pmrldv38fk1r5i5ef0be2sd[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
8o1nl8uqrceig9gkt12fer6irswu0ivr[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
u3ucl3ff87ugh478tvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
1lq9urk5noq2mhkctvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
b31375voq71rpl7ptvef0e12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gvaqkil158apf9lutvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
q8g11thobvg6d604tvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
8g6ef235pp9h073k00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
arl4spn3psoerc4pwh60tun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
bc3ngb7u197025qqwh602un02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
d1binvi2tegvou6swh60iun0iwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
djsk60v5e51jvohswh60oun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com

e1piosdphv9qv3ptwh60gun0owusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
131apen9992i2a1d00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
38s32qaknb226frf00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
4l4fmlv6ju7svipg00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5fg73t47qgdfd83h00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6c579uiq25o2q4hi00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
p8kf9ap03fvmll94wh60iun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qbj26i5jnkrqdac5wh602un0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
tmrj1i0jkdekoa08wh60oun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
0ljdf3k3aic3bsncwh60gun0owusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
2ckh9sn0fvvql7fewh60eun0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
3bcb845tr9npi1vfwh60iun0bwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
3rauajkilshav9sfwh602un02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
3v3b52n3r4dp27pfwh60iun0bwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qb45pba45cj9m4s500mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qjm8h5t6lm8u7cp500mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
u7lvrpv0btqubkr900mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
0fkqf50afqmg39pc00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mrftop7md6n0t3n1wh60cun0owusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o6tn8j7g7d90h9e3wh60tun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o6tn8j7g7d90h9e3wh60tun0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
olh5mn0vhbgas8k3wh60cun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ivhub0gpo1d7fiixwh60gun0twusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
jcvi7o1j7k24b0hywh60tun0gwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
kgovb3hbcot3apizwh602un02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mva8fjhsterd3bd100mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
nvu2f35sbk5soef200mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
6oc69if8l6j5201iwh60gun0twusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
773k3vnecfb8rndjwh60cun0gwusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
a5rrvn4gnl0vnfaf0l9v[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
be8fptn47bsa8gggpmq0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
cv9a0989o06ebg5r00quksbsvggtquo0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
oguoekruvv6fp3t300gsqjr31uru9oii[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
v75r3enf4k83ikha004sdjfefgee76o0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
lhdjpf749dng4efelm70q6r[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nbj2n5htt2epur31u0if6[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sf6pf4m0qd401k260f8j5snmah[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
avau7h3em6svmnmpnotoiu1srue3ove0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
i86iegbrro6dh53wuehrneis02un[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
b808u0eb8n6imdvqun022dioho7r1p0i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ogf81h2kct2idnp3un0b2dioho7r1p0b[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
qfnf6ab6u28je4i5un0c2dioho7r1p0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ao4vk8mq2hv6fo0pun022dioho7r1p0e[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

0olcrtj4bsjtulfburso2ve2sd0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
d1o12ctcc9r0lnnrurso2ve2sd0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
olthhiq05p0vcqg2urso2ve2sd02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r7j506qtdp6joj35u30c2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0ru5sub54iiremgbu3022st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
q10ncmprl1d7tv04vedu0t12e[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dj8ao3dos6ld11grvri0ewr6i52s0enj[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ng0tet912lupnh11vri0cwr6i52s0tnj[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
hranipdbjh6tmf8vvwonou0ie2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
cihtrlnj36c63hlqvwonou02e2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
idchijm6kdlf6nii2f0np2p[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
q0me4k7cgtk85ba2d1kfq0n[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
j39qr5fhk9kks1cxtvef0g12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
kv6a0jg8786niapytvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mgvft0du4bvbbgg0tvef0212eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
m1pcq3emvaqsjm60t650cee[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
blan01m0ngp2nn7ptp1nrvnu10c12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8j6lopo0j4ngi5djov50ine0gvri[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9iq1i2obrorl9b0kovv2fi0ge2sd[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
0v9gi5pk4mpn3kicoi60cou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1ij9hctjjpb1sthdoi60cou6iuir0irn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2cv8mnbeha1qglreoi60gou6iuir0crn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
41qsrgg00826m7pgoi602ou6iuir0trn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
u5g20o4i08sj2j6hgv0r4vk[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
8fal4r2nbims506jj0ee2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
n8mam162tt83g0d2oi60gou6iuir0crn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
nmsi7h45aiu9d522oi60cou6iuir0crn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nr2ia9qfa349b0q2oi60bou6iuir02rn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
r74br8r0cce4m6r6oi60eou6iuir0trn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
rc0n7qkh5colsnr6oi60iou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
rlsbbcr7c6t4vjk6oi60tou6iuir0orn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
qgdubroda1vph414srd6sw0oe2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
e8cucug2t2ln8p1ss60i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dmdb4di02rq9r16r6e0idohu0et2w[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hlgrfnhmqc8qevcv6e0odohu0ot2w[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
evf1enqtp979klvtoi60iou6iuir0crn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
jg3lsj9jqgkn7v1yoi602ou6iuir0trn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jjg2q47bfg7ode0yoi60tou6iuir0orn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
kl2daf5gfl7il60zoi60bou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
so3s7kn3ldflpsk66refsworq0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hfe34nk4htdhc6tw00q49irp95gu9nfm[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
g8lvv11ho5musgnuovirv6owr0oovi[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
61ofp3rbssea545ioi60eou6iuir0crn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

bo0bishlre42vupp6o6jop2f60grnf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
s8l5ios8jpj89r566g36ut2w0g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
d8lfdqpamf9m7rhswh60cun0owusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
gmqs4715j821hphvwh60gun0twusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
h3bs1h984phgo6hwwh60eun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
73ccpvrss141140jwh60gun0owusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8b7o8b5ul9udi5hkwh60oun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9fg3iqfqb8hv5rnlwh60eun0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
vloefu4bsf6o0l9a00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0fn7oe4cegrf933c00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1ovvh0e9m851b7bd00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2lphmu5vfb1qs1kewh60eun0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
4clhd4navv9q7vhgwh60gun0owusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ofhjbkipi7d0ffk3wh60gun0iwusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sijbvor3klchoak7wh60cun0gwusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ogtclgitm5ali6c2i32ft3i6d2i0tovi[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
mmqbgu51idip3v11wh60eun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1i06atdfbue8vrsdwh60tun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
kjdcdqmq23g33m6z00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
s0q69bope17och6f0r81[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
sdncbs9k54hqt86h7f30[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sman43ms6uuhdi580g8qlnok71gtsob4[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
tbhjpg088o87e4c7071mqtkrm1gheap[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
u9tndt8r0p42hl73ffo0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
elqienlbfhrlsrdt00qu7lbvf1qe7jo0[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
eqhnnlpnnm2733kn08m3o97[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
h5sqsh3ldnu7959p07ge4dr[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hlc3g293751a3niv0oo1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
obrd90372tf0qsv300q2rofmgjrql2os[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
r8p6o3htj2d8osr52v0ceu[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
q9q772a490qkum02tg0oe0l[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
j673t7242re0i89xvg0all49711e[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
leajiq7s79krdeitlvb0m67[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
cbkq88d8nqqbqr4q5i5ef0ce2sd[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5fjujoold6af000gtj6h0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
61o333t53ubv3fdhtj6h0g12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ojrn1gtg0vpl5js2tj6h0i12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
8r64v4ivgve6qfijt1f0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
tvmsmpr9nrub9ml7t1f0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5336qh70uos4vb0gt1f0ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h7vc3vcgj9s7aumw00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com

lbufdtueqsf3grb000iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
lrsfrtttqkv3nr8000iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
m8pq26ooke896hu100iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
o3i9qb2i5ttq854300iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
o3i9qb2i5ttq85j300iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
u335qd4fftnt884900iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mai8mje63ah68qtuc8583a0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gjaggu9tp478kbnv002u9l4p5554q6ro[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
060mpkprgdk087ebcr1jov0te2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nvkevlgqeq5bn151c2j0te2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7ve1vmv7kblqirlieu6ov202dsw[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
u1emrh79c839hel8e30g12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
n1lef2btk559bjk1e6u0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
fba157qr9i4r5uft00isdorp9ujh9bi[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
l7ihn112h60bpl0z00isdorp9ujh9bi[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
e1i5647kn3d2f5otnrihos07ts2fd0cs[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
57m839c1o9k1aj8h00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bon9dj220u3qg94q00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3ffv0vjjgvtnpnpeu30o2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
5rhqup3g159rvdtgu30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
7riatumj05rlrstiu30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
fvf90rojjftgp5dtu3022st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
gck0l44pn2n6e2uuu30e2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
hreeui31f5qivrmvu30e2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
sf0q84qdutb323q6eo6e202e2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
4j6cjhk8mc73b28fe2sd0onwn0te2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
v3671bokobrb5ts9e2sd0t6uvu0ce2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
toqfpaaqcfvo5pu800esau3m9j0qtovm[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
njiee4m3ku99d691e6u0o12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
gr5ioskgsa7rbbpvuhs0ce2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ji5poadgkt7dbmgyuhs0ce2sd0govir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
lr1i34kjua0rm6p0uhs0ce2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
qgc2gj97t3sop4i5uhs0be2sd0govir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ui0d72v648lr96i9uhs0ee2sd0eovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
2cjmh3c24aaf4thde6u0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7f05rn251hga3ikie6u0c12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7f05rn251hga3ipie6u0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
fo30qreov24tpk9te6u0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
3juu5ipmcf8jfk5fuhs0ce2sd02ovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
e1q28b9aaoboeugtuhs0ge2sd0tovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7rcfm22r7tfq3kfi0oo1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
84foosm8s82rscttfc0q[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
aqr078go4nad5201o80l[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

bivcd4mcdvofqe9pu0grnf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
cj17b39ca729ujjq01qqtobmv1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
aiopjm31bum5oktp7oddrsifcovt0oe2[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0dv6fsons11r6hqh0657[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
14fhos08sq2r26etoc04[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
93ueh1k419flevvl00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9clddtg984cnq8pl00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9i4e3706147lffkl00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
t3tcm2p69a7ocsl8q535z0i3rq1rii0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1muqmhk6mtluc0ldq535z0i3rq1rii0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
7rbqd00d3npukh7jq535z0e3rq1rii0g[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ao3crspkhs9ol2ipq535z0i3rq1rii0g[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jgrasd5o4n1q0oiyq22nsf55096uqprs[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
3m88popdahpd261f00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
81tgvivs9pnrbp7k00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dv85mko4cgmgtj0s00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ebo32rdrcp5kpg7t00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
n74ejupohk2grmn15u0i1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
49a4p4fqchtddi7243bfq0g[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bf148nfa1t55n1gp5u021e1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ggm0p8dn9ab55fsuu1h02csuvn0gnj[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6ogkkniro15lrrhiuhs0ce2sd02ovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7l1om4ljtq0b36njuhs02e2sd0bovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9666qr1339ujekfluhs0oe2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
aggum9ij1eks37npuhs0ie2sd02ovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
egusb7i1ve6uo9ltuhs0ge2sd0iovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
fc2jtvnq7r3u355uuhs0be2sd0govir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ajdmlq30e8o6msipeo0gnfc1ov0beu0g[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
o3c181q66o5iiig3eo02nfc1ov0geu0i[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
blqtnhtren4tdhkpeo6e20be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
p6sa8nd1f80emte3e2sd0enwn0oe2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jcfda1fpkvrdhi4xe2mvri0te2m0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
n6fr769sh71lspc1e2mvri02e2m0ie2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
mgkqij3ukpm9k9c100iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mjnqpjo2k239l94100iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ofr9mbeg55aqt5q300iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
1c6l472227ihucucn2ie2hh0o2st[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
b88ig0re7h0qfc5q00i2rori9u04t4i3[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
6ja3j5thv6vsmr0hu30b2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
8i8fahjtirhk2lnju30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
bg5mu1un7l3uqdppu30o2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
dcdag6qia86ovevru30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
i6456o4fpe2jhb4wu30b2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

0i17b61bsutd80dcexr09ovirsvu10oe[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
d138iu5qqeh271nsexr08ovirsvu10ee[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
vijfbk7mbunn8cnaexr09ovirsvu10oe[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r8stkst71ebqgj66ervisu10bdohu0gt[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ooad2c9fd58p4qh3uhs0ee2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pbsl2l5fb0jg4df4uhs0ie2sd02ovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
uinno0pgltlkbvi9uhs0ge2sd0iovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
38q4d8vh9p32peffuhs0oe2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5667k3rv2rubelthnrihos0kts2fd0os[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5688hh6ho4p176oh00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
632h4s239t1ejf6i00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bik9rjeu0nmqn9aq00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
qvot463cl5rcg5r4urso2ve2sd02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
vb096g3p6omg3979u30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0rfqtn3j75vrrkmbu30c2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
tbifqqa3a49mpc17e6u0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7f05rn251hga3iiie6u0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8bf1q9t3c4dcp77je6u0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
q3b8h3lm9q7eoqa56260kun0e6iuir0e[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
d1s9qaucac0fkmpriu0o2st[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
cgkp6q0u8gvv0tjqi32ft3i6d2i0eovi[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vtl46o0dhqmj0ueui6pu3s0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
aj96unpachpelllofo60gjrvi0grnf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dmank7g6rkuvj5grfo60ejrvi02rnf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sot05l3noituaq97wouh0lovwrvorvi0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gmovu3cjdvookn9vwouh0lovwrvorvi0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mm7tpdlad7d01m71wh60cun0gwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lg90ma1cps6ovek000mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ljh0qagmpkjo9e7000mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lv8ui10k2kg435h000mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
p1j8m8blsi4mptm400mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
tghcifuviv0skq5800mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gjq7q1dlti686uhvwh60tun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h3k3hai0o1vvgl7wwh602un02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
73f6lq9to5c84gajwh602un0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9fbokvp2utgmbuulwh602un0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9f1bipv24b31grol00q49s2of12ql2o0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r83ggmvu8h772nc6wh602un02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
23do4svnpch9h31ewh60bun02wusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
kd6590n43hks8rvh0fj2[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
labcvlinm51jbh310buj[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com

md5p22a3ub4r56upo7v0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mpqcemiip5vpm9up0186[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
uokn20hil5gk4v59uhs0ie2sd02ovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vc8dk0u83a179ic90e2st[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
n0ueo899p6784gr30ipf[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
r0bs4ljom79j6koitvu0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
fahdplckrrebmnpn08jub4f[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hlfobsupm8c59e2vuj0esf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
s1bvlrpo8tbeelo6rsvuio2vu10if7[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9tn2mm06vjpsidqu0cf23kh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vl0k73rpbnrscs6a1u6rs60g6iuir0e1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
qem0uje27t36fvsuuchf30h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
b31cb2bqdb6fvqnqun021ocsusp0efe1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mf5160o6j2joedl1un0c2dioho7r1p0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
qfnf6ab6u28je4d5un0b2dioho7r1p0b[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ebpjshc01131vbstunhov0oeu11onf6e[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
v77h5nkjd374r7d9tvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vc1h1n0odf14d779tvef0212eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
07ttndaugjrj4pcbtvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
16e9jr0hnie2qh5ctvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
17a9nik1n3a2v9rctvef0g12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dv50krctfobl2i8rtvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
e1k1nepgomk6vbrstvef0g12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
e8fh1ravufms0qpt00gudir2951udivf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mmvl9dhqj5v0crd0vues02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8odjhiq5l11122nkvr2d32i2voe602e2[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ip0o7efrui75clii2v08d2i[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3f4teb3to5bffaredu12wrsnr0i12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
nb07n2hkshm204k1re2cuvj0cts2fd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
eiug79kqm69riq1srd10ee2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1lcm3vikgahl1nfd00osr2i50fgsqorp[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
o7rp3opdfl5gh9i2t1f0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5o869977u344mohgt1f0ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h6p5j45piipsq3vvtvef0t12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
o3qer1fpd9sns5m2tvef0g12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
q80cgv4eolosbfo4tvef0t12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
28j5sl2eknfre96d3twe0ge2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jga7cjdpauatposyovi0t1fj2o10kovi[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
vinhpqt1bpd7a3haoi60oou6iuir0irn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1v8snc7udvdj8i0doi602ou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
2g57e0i9oageug9eoi60eou6iuir0crn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
2jri6np3cjtd0qpeoi602ou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
4jdicppf8j8dkaigoi60bou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

7m3anm7jn931mctjovi0c1fj2o10zovi[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
617stsr6ntep0auho2v60be2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
bgs4b6l77jtbv8dqoi60eou6iuir0trn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
dce6d1f9a74sqlfsoi60eou6iuir0trn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
l89ru8n7tq1m6ngzsuo0ce2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
dr5hpngivq2l7k9rsee50csf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
i7vv7q8lvooaeqow6eo50be2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
m3rmre9cqd957bd1oi602ou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
m87sgjjuil18hoj1oi60cou6iuir0crn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
g72hhjlrnu3cna0voi60tou6iuir0brn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
k79jr5ikqcpumklzoi60cou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
og0cg7ke855dbpp25u0i1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
s1b38eniqnonv6p65u0e1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
4tfnvnohonj9j46ufm9ii01[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
2jnmnc5tttkk42vd5u0i1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
fb50klvtgq0b2h1t5u0o1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
hmp9sjf8n4d6pq5v5u0i1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
b36fqacs06op81rq00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
cv59opucflv59icr00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mrtv6930a6vt9ed1004udkr2ftq4qnfm[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5igutvd2sealpupg02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1ofa2qnv9duipt7d00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6iivv86m97ld50hi00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gmk94bm0ejprjppv00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
616v2nvri9ngud0iq535z0i3rq1rii0g[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1rndq7kt61lqd2qc0fju9nf[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
n7vjvhiseciubdd2oi60cou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ojvg6ud3ajuk09d3oi60bou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
pbdrcv4gqfph47o4oi60tou6iuir0orn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rc0n7qkh5colsnd6oi60iou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
t1u25pchk6sminq8oi60tou6iuir0grn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
tmm73g42nq8hlkg8oi60oou6iuir0irn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
sgfbfjtg0hat2k8700gudir2951udivf[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
gs9cuvo0tmp7sho1vo30io5[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
s67olf26av187hp6vwonou0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
agrnc0oen313l99ovwonou0ce2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5s4fo7e4877a2vd1a82qii0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ib9lcm2gmfh54csxoi60tou6iuir0grn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
km6il54ttij99h2zoi60tou6iuir0orn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
l6qkc3kih6ggklk0oi60cou6iuir0orn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
lljh2bl4kttcte90oi60tou6iuir0brn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
rcd88oj010cgbfr5s2phrs1ov0ge2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0m1mrqllcde2u30c00qsdsi5f5jha6b9[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

8buuqki79g4jlp0j6es22i0ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
s3e0tg3gofeu0e97wouh0lovwrvorvi0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mv1tid7qdcp05mr1wh60cun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o695qnk7hrla68v3wh60cun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1oqce1rlug61ju1dwh602un02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2ljladle9a0ud8kewh60eun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2lphmu5vfb1qs1newh60cun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ujbr6gpomj5p0ml9oi602ou6iuir02rn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
3inmqad9eq15sj7foi602ou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
7obj2bi86vlvu2qj00q49s2of12ql2o0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
g1ugvjhh86pm7sbv00q49s2of12ql2o0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
og62jqmjt812f1126hr60t2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jchk1s75v9a5efcywh60tun0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
kb597umaunsal2tyw6d0ee2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
l80m4h3moof8ffb000mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
gbasd111jju1ed9vwh60oun0ewusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gge7m19rtoj8sugvwh60cun0gwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
jchk1s75v9a5ef8ywh60tun0twusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ebo32rdrcp5kpgvt00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
f38tp3nd09pr2cvu00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
krpr3dl0i3479vdyqro255oer0ee2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3rauajkilshav9jfwh60eun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5fdb00ph4tu3mobhwh60eun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5i2m38frjj8funkhwh60tun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
73f6lq9to5c84gmjwh60iun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
a8breb9t0m3edt1pwh60gun0owusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9i4e3706147lfflI00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
c1gm3csqdrr4a59r00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ol3evljklvaa2kc300mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
u6ra9sc9dmneo66900mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
276frivk6t9sblge00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
77gq364q4irban5j00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
u8p6ki08450s3f580bwu0of6[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
vm05sk8bgd6239vaun0c2dioho7r1p0g[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
tb26sfckf1f7v4j8unhov02eu11onf6e[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h3nukdm78l85m3bwunhov0ieu11onf6e[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
3rte9im0nn0m8qpeurso2ve2sd0ge2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
bl8hpgqa0p7v6arpurso2ve2sd02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h348mmjvjapa5pfvurso2ve2sd02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lg1vp5asqdch66nzurso2ve2sd0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
n1p7eqtl39457ii1urso2ve2sd0ge2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qrjtdj3alnlcj0k4urso2ve2sd0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com

nb5skp5mht7pn2u1ut12uv0gun6[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
r6b5cj43deojp665u30c2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0ru5sub54iiremrbu30o2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1v3h0do8of5lp1lcu30o2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9bk06jmpsobi3qfku30t2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
j8k7lqspu4nseeuxu30i2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
kvigfpnujsdlvgpzuhs0oe2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
o7rc6mr3vtmhpcq2udf0ghv[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lli0auqjkhr6istzu30i2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
bfbn6lf0jjqg4pkquhs0ge2sd0tovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
e3p0d7aaeks8p3rtis0gire3vo2v02ue[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
8fqc16riseq54bukovi021fj2o109ovi[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ngf7qcl12uj2l6f1ovirv6owr0iovi[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9rp2th11grcbgs0loi60eou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
afub5rfnofv2j8fpoi602ou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ao4b8iiioo12ncrpoi602ou6iuir02rn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
b37kljuufr119o2qoi60bou6iuir02rn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bifks6tofmv1mbqqoi60eou6iuir0ern[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
e33khi5qnfbl2vvtoi60cou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
07605jn8l36uranbtvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
76398l0eki32451itvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
76398l0eki3245vitvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
a16758p86m6jrsiotvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
c1u3nqeuu6v24etqtvef0t12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
cj7939h35krs5veqtvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dv50krctfobl2imrtvef0t12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gmtqli7f51tph90utvef0g12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9i5qv0gsn99hdvukre2e2sd0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2oat8rs0rki2qrld5i5ef0ce2sd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7ro74qnpv7t21ibitj6h0t12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
13obqe10joasvr7ct1f0ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
479nogd49lgipapft1f0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
rb3a857o2bd1gnd5tvc0212eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ir9esdlnhj9d3fdwtvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
lrmqallt0jmpo5lztvef0t12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
m81f159o4v1bdl90tvef0t12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3gghuskn9ncd2jre3r1omquirs022st[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3rh4p9atjlem05veovt20tjt[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
hmpe5011r9pvb93wovi021fj2o103ovi[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
kbt1d5semsi8gbjz00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
kvq1b0a8m0l8uoez00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nrc1vha53kd856m200iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
uo859p4hfupt1cj900iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com

38iqeboinet9c56f00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
he2qr7p28cvsjcdnr80ebd7[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
p6jg3t892pl69bf400h4r4f19uh4tor3[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
eb5f9dd8rlmuap2scj0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1fng0b6inl37m6tcc2j02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
d8m8punaqh9201vsexr08ovirsvu10ee[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
57bmrk1as7nv0n0geu16c0t2st[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0ij93ftklciddelb00esqjvi0fju0n3[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
b6605db6jomt93mq00e4r4ii5nj9quiu[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
n6eng19tquuq7562e60i3up6ium0212e[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
u7l3fe6ts05vb8l8e6u0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
82a9t1io21hh5ru1e6a6m30[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
sgm7psfdpdhin257q535z0i3rq1rii0o[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0m8abtnlet026qkcq535z0i3rq1rii0o[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
33n3midc7a66clkfq535z0g3rq1rii0t[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9v7t485vt5t4sm9lq535z0i3rq1rii0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
j8uv3pr6rqlg8kpyq535z0i3rq1rii0o[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
aqf4iscuscnrsua18600[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
bqvbvhg02p17vhjub301ma5[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
d56g8g5s2h1dfvridr04[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
dim24hdrb0dst7pr071mt0im00feaaso[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
ncd0dudrutavm6q1vw0bf6[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
olc62cocacn7u2q22v02eu[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
q9f2a667bb6p6t02s1a3e0l[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
r5ta59un17jqldii5v0o[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
mfgsshts56t2qjn00ie2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
uc1p7naijbe7a6880ce2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7dsclk69i6r5ish30lrs9jg[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
jtmeu6cslgk39pg89mf0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
lu8f6rmceral1vo85og0fjv[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
m9q27ja0deq1lgn25lajea0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1vm0vetvdv46lcgc0be2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9i96cr8o78dhv7tk02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
28pmu858tudkd4vd5u0o1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
2sr38c6i7nh5j86udo0u[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
3qb1266564omnctj0jtv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
52h7rr1b7f4psu91kcc4ii0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
amfijpui0mgfr6ep00nurl25vn82vimd[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
14aa15h1o55d8ne1p8j0iov[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
gnfm22ldl9ainmif0rb0por[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
3o11qb2ksonusuff2sorvi09rmdsr660[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
cfjusftah654qukrun0cu7usi3soio60[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
cioukvtchch49sgrun02u7usi3soio60[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

kcsqu6amhk7kmm1zun0c2dioho7r1p0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
pjs1f3u984n0ad93urso2ve2sd0ge2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o8vm1vto1caurn72u30o2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0bvq8noo7tfrdksbu30g2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1r8hapotoihl27dcu30e2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
i1efeva7t99972nwurso2ve2sd0be2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
jl59hpqkhpafcmdxurso2ve2sd02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
l1fv20a6q9mhljpzurso2ve2sd02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
28aflvuho4t2ef2du30e2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
48dcgcai0c62v25fu30t2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
aovm85jocafdd0uou30i2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
efhc95pv34ihklftoi60eou6iuir0crn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
efmkfinan3olovktoi602ou6iuir0trn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
er11hkq8pdv9sg7toi60gou6iuir0crn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
evf1enqtp979kl1toi60gou6iuir0crn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
gluhe6ldnt8cut0voi60tou6iuir0brn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
hrcl3vpcubjkiinwoi60cou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ljsqrmjicu288eg0oi60oou6iuir0irn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1cmge6dsclrtfejc6e0gdohu0et2w[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
p8sqj81kv6f3kc636eo50ge2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r761pv5v4sdk6hi600qsdsi5f5jha6b9[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9rm34379mq04gqll00qsdsi5f5jha6b9[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0lu3cu7c9r45ujnc6ruii1r0eovirsvu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0c6og5btugjqhhocoi60cou6iuir0crn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
1bsem60k5hc76tddoi602ou6iuir0irn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
4ord6lsjhvifqrbgoi60bou6iuir02rn[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5b1ge9hb2rlnpp7hoi602ou6iuir0trn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
trr24hh4h7664ar7guswo60t1uc[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
68bfi3v6skqa14pioi602ou6iuir0irn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
8i36ujvj4iku1v5koi60eou6iuir0ern[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
9o05i9sf42hvcfkloi60iou6iuir0grn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
bifks6tofmv1mb3qoi60eou6iuir0ern[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
cij34md4aqt0a2vroi602ou6iuir0irn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
k7juuhg3btk63b9yf2vi0ee2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
mjne0sq5tgndtv01wouh0lovwrvorvi0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mm7tpdlad7d01m91wh60tun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mrcusokogsfar0j1wh60eun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o8dvftv72kvtg6p3oi60bou6iuir0grn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
pc369ffqt7bs4r14oi60tou6iuir0crn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
r75n0q0557bl6nv6oi60cou6iuir0orn[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
s7ec4imn00ae5df7oi60cou6iuir0irn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
rmgf4i3ea0pq1lh56s20gwr6i52s0gnj[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com

6g58ps634jn2jqshiup12s5ush60ee2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
nbm5cn6i7fngfk21tvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
q8g11thobvg6d674tvef0e12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
fvnv0hkcb27mg4cu00qua2o09jd4l2b9[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
o6me9l8dlmtaok4300mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qb45pba45cj9m4o500mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qr433l96827kfil500mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r1a5v81snarbmmk600mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
tghcifuviv0skq1800mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
tml0euav96phrjb800mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
uf2bb6rhn7qhfep9wh60iun0ewusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
uf2bb6rhn7qhfer9wh60oun0ewusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
13ach7rku1b1gs9dwh60iun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
17eko7nh8f48vpidwh60gun0iwusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
27nhvs59fmfqk7kewh60gun0owusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qrieo21mr659tfk5wh60iun0bwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
s3bbqbvtkc3hptf7wh60bun02wusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sfobmbrek7mhitn7wh60oun0ewusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
slo9bo5b7bteahn7wh60cun0owusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
53l7etqvqjpfr82h00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7ohaeanmhdjihefj00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8m1cp2p9qh2p2svk00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
978t3k246imjaj5l00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dbl29e7j4j1v269swh60iun0ewusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
djsk60v5e51jvo7swh60iun0bwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
g8a797dktfb8lsfvwh60iun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
43roq4vudcf9p80gwh60gun0iwusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5c4d2c05t3e392fhwh60gun0twusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
6oc69if8l6j520fiwh60bun02wusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7omc2fr6sgs1829jwh60cun02wusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8bqaegllnl65jthkwh60cun0gwusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
blf5bp0m9bnaa3gqwh60cun0ewusouv0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
kvo4mmles1mfiuizwh60cun0gwusouv0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nji949lvrktjd57200mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
380l9prq02si4ipf00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ult052kct4j60fo900h24orh1nq4tofu[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
dlb69er4rl5ijoasu11rts2vri02e20b[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
3ig87v3r1sfo1hmfuhrsoeu60ed32rvo[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
8j024avi0h142m5kuhs0ge2sd0iovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9c3ouck95r22oevluhs0ge2sd0tovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9lj6mrg83qsj3kiluhs02e2sd0bovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ajluq9fo1hnse7vpuhs0ee2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
fc2jtvnq7r3u351uuhs0ee2sd0eovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com

jc18hh8e6ak7411xe6u0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mmt7d1tp3q68ehv0e6u0c12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
n73qmque1f470r11e6eo01wu0be2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
km4mld3hb340b9ky00isdorp9ujh9bi[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
uligade12dff1ta8nr1iun60trvi[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6ouhdu2e9ufegvsi00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ajttpnber2i5lmop00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gm9ipu0pskfrdo1vuhs02e2sd0bovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nrngokng6allbri2uhs0oe2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
qj82njdvtfuoi455uhs0be2sd0govir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
t1pur5in72rsifl8uhs0oe2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0l7bgt0lhmk4pmrcuhs0ee2sd0eovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0lgjmdgj8qk63ldcuhs0ce2sd0govir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
2f2ki1p5rubnrhleuhs0ee2sd0oovir1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
06o0865eliou4t0btvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0catgds2ggijbpjbtvef0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
2ostbcvirdqpka8dtvef0g12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
agb7tcpt6bbjbulotvef0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
drrtasguvjrko8krtvef0212eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vcmk5dukadr7t4ha00esau3m9j0qtovm[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ebkf2n2qo14ivj1s00esqjvi0fju0n3[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o63cev8obs41d012e6u0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
rjea2l3iiub59d95e6u0g12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r14ptgkl7qacucu5chsv0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
pja8e4n7ep72svv4exr09ovirsvu10oe[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
icdqul828khf1qcwenu02e2sd[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
66av2e6hb14vn6shenu02e2sd[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
oog99o2p5ueq104300iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
4i00rgqu7nbanq8g00iesdb0vfhe0l45[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
8tnr4hlq3ooaq755n6jcbm0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3r39tt6cfobih8uf5srh2vi0o1uhse0c[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lgsrianmc13k2ggzt1f0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6c2d2uha76cli7hht1f0ee2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7f05rn251hga3igie6u0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8rv1m9u8cdpci7ije6u0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h3j99oq29eae2u9ve6u0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9o41pmq4t8jvmq2l00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
agfcf1umrv7s0ahp00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
blq1m6f6uul4volq00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
d1shv17sgav6mvrs00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
d8s843mbuoomfess00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
4glm1mnha5gkmukf5u0e1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
a3ofae1g42buh61o5u0i1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

dllq1bph00glmtgr5u0o1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
efdv68g3uppsi4gs5u0i1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
il0aglde105rbhnw5u0i1e1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
f3cfe1ercje7r54u00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
fomfh7edc8t7b0uu00mudofi75f4tjvh[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h7ttod2djiqjsofw00mudofi75f4tjvh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nlq0hq144pfp5t12q535z0g3rq1rii0t[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
tf79n272mhi0trn8q22nsf55096uqprs[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
61ka0n5p25hqs6liq22nsf55096uqprs[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
gp27ssesmvnpkgff7rc0eok[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
96dlh905bab82unk0f8jha6b9fgge[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
crjo68nui2fg30dqc3a0g1uv[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
s887ouilpq0ij4n7q535z0i3rq1rii0g[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
sj37isikp49ig2k7q535z0g3rq1rii0t[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
67rjs2cgl778pljh01qqtobmv1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6tgmn6evib1vpq1tb3273c0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
10hea7samrh2bo23lg70[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
1h14ptc2k6kdku238g90[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5d098eoerilg4qqegge0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
f338llosltnmqhpt05j5e7n3mrgit7p[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
hli7vmi9nfa17q4w0090gdearf95t2qh[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
i0hpm6d7rq5df03p0fpn44i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jhq70ih8gaduf9g30v6c[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nvj83eprhg9c83630fqe72osvgj9ag3m[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
q9iul80l3e6qurk2k7uoq0r[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
rb9b9q15qqmf4ni6004sdjfefgee76o0[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rv0dn8nf5tls0fq600o4vgimd18ak2ob[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
surk8jj29gqbh475ob0t[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
uvc9m27b5brbqns80gfj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
k7eb5975hja9eaty02ue0io1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ls0va7msea08l9o8tb60fjf[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ervsystem[.]com
infinitysoftwares[.]com
techiefly[.]com
financialmarket[.]org
gallerycenter[.]org
aimsecurity[.]net
mobilnweb[.]com
datazr[.]com
olapdatabase[.]com
swipeservice[.]com
mhdosoksaccf9sni9icp[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
k5kcubuassl3alrf7gm3[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com

solarleaks[.]net
solarleak[.]net
uo8igvgkvslrh9b9e6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vlks0s9quptur6eae6vi0tdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
07q2aghbohp4bncce6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
16julbdk427s94jde6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
38i66ek7kqmjq34fe6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
cjuj7cksp406da4re6vi0bdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dr0d5kfq8nupil8se6vi0gdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
e8fb6hn7lqboqfute6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hl5ttenpk6mi8vrvcussor0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
1btcr12b62me0buden60ceudo1uv2f0i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
gce7o7o4ctchtooven60eeudo1uv2f0t[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
vvv8q9e0oh5q6u3aen60oeudo1uv2f0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
gl63mjuecaqvsv6v00eu4sihv504tori[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0bv6kouis4gtgs1be2sd0tdieo0te2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
irdu1l32ub0que1xe2sd026iovtsupno[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ef4j59ohojpulg8te2sd0t6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
a6t9c7ufd2ekhfpoe26ts2wr60i12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
oillnq790k8gfm33e6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ogne61tecb993802p2sji2v02e25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
vgkhu50lq3q77j79uit0c12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
382ss75vrn3fr82fr08on621fio2v60e[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
tejsi18ur65nkna8tj40[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ra4ovrb531jjc33gvbj0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
sif1gorsk090nes6mvri0tj7[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dnfmqavi0tr44qbp7f06[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ufqiaderpv6o44886d6n0i6j0teu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
16uu1e6k3j3nihuc6d6n0c6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
1c2u8q6l388no9uc6d6n0b6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
23hrcr27nmgbbbud6d6n0t6j0teu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hb01ujbtkgpcqgivp2sji2v0ee25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
lljmcpepfomfo20zp2sji2v0oe25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
o3plcb47gm16brb26d6n0t6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
tgao5p3dhlbip2m76d6n0g6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
tca1u6slgg74bli7e2q0c12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
18shu72lull6bclce2q0b12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
1g2hg1educi6d87ce2q0o12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
2f9dj160un1hhpfde2q0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
6i6n1qj6b520269he2q0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9jv05e4ab7qovhdke2q0b12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
f36hv0ad2n3dnabthom2v3o110ge2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
rbcu5i6ptab72jm5sr6ds2n02e2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com

dfdg889mkr8233qr6ne30i12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
jbd3d1luqjashtqx6ne30g12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
vgve6mdppbgpt289ir0ev7[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
jgfatv4l3s3l8mqxim0c2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
fq3o26m3484isc2jf7a0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
4og2ki2t8s31t6dfep60i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dm3mulrt5kj6f0rsnotoiu16rv6r0ce2[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
4t4bhjpfuvh8o3lur3if307[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
nj6pv3s53meviit100osv6imi5r2[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ciepcqqog816s6urtt6t0kf60ceo6e20[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
97v4u78ma1kdecek6d6n0o6j0beu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
a1mouk3b97siesco6d6n0t6j0teu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
a1mouk3b97siesto6d6n0t6j0teu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
agconn349l4ihueo6d6n0t6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
db1dl1uasop4v8jr6d6n0c6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
g1gqh760t2v2lc3uhom2v3o110ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
r8sei9c4qpe40q65hom2v3o110ce2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
cbdvbiqmk05itobqhom2v3o110ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
e8ueb8kp9vo6aitsscr0t6j0eeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
53to5l3lo2nud4ugce256u0te2h02us[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
irnrin44ue7fgh9wco0ge2sd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
c6aeorrprknv98pqc2d0ce2h0tdj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
5vsivtapld93b9ggoid60bfj0bvri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
im55nuau5ptq6inwjed10ee2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
a1fon7mkjrkm2vephutv21ouo6n0t12e[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
r8p6o3htj2d8osr6nf55rsove2fvip0b[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qegmhsh6v9agpo0udjtom0f[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1on45q99h4i7bg0cdae2sd02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
irklg6o7g0i1eq5we2q0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
krci1db6d0ev277ye2q0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
m8isa3tqc2ktrup0e2q0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
77buuacbm1ane0ai6d6n0e6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7couja66m8tn304i6d6n0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
814jt4mrf7cg2dmj6d6n0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
97v4u78ma1kdecak6d6n0c6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9cf4j7jca8nd3cbk6d6n026j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bogllj4albh6vgup6d6n0g6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ibnk73s0jofsrfsw6d6n0g6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
kb8pl5us4o22vtsy6d6n0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ofdlabqvgv764rt26d6n0c6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pb5d7fu0uoi4r3436d6n0c6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pv9davtvufl44me36d6n0c6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rrlkk8aq6i9s91c56d6n0e6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com

vb9jst38pt1h1ugaovirsvu10t3q60i2[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
vbbm5rktqh88hvcaovirsvu10c3q6022[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
nl3u27u4qu181192f60tnr12oiir0ie2[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
mb2v3cgjgmohahg0f630te2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
4tqj85ig0aa1756umogii07[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
rvrkscam6f0sq7356d6n026j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sicikne4dr4o9u366d6n0b6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
uiai0pedprbod2886d6n0b6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
174utqcr31cn293c6d6n0o6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
lljmcpepfomfo21zp2sji2v02e25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
5o62p6s87utijjghr0lon621fio2v60c[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1llms3vh0q0cb39dtsfd2cu7us0e12eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
do1b13iike88fsnror60ce2h[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
hi35qtulot6kj5qvhom2v3o110ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
dv6feovu284kj1orscr0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
039n5tnndkhrfn5cun0y0sz02hij0b12[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
hj1ccqesdulojdow00hu0imrfggqtkbm[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
so1dl53jrofi71o700esqlr575gu4nrp[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
oct7dd5e8ggcqft2e2sd0odieo0oe2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
m1lg6fti08vv0s11e2sd0i6iovtsupno[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pm52tjbjjvpag9p4e2sd0i6iovtsupno[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
33eo1qm52g92kjufe2sd0o6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
hv4u5djhi6pjl18we2sd0t6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
2rn2ddllc4bmtjiet36huovz0ott30et[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
aih4cvusn1fhgg2ojed10ce2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
l2dkplid39dfhn38j3o0vj1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
crnt92r0q52ehubq1f5jovirmu60tvri[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
s8rrone0hbta63j7h2fvi6ovuo0e326d[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ev3i3ekbbqgj0hptds2n0e3uho1i2v0o[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
0fhdojdvgeuskgkcds2n0i3uho1i2v0i[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
08amtsejd02kobtb6h07ts2fd0b12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
lt5ai41qh5d53qoti3mkmc0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
m69dja7eprpf5p20f6nl9l0g2st[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
elgaesftnsc1rh1sc2d0te2h02dj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
0ftd1sok8kjdkp6beuheoip0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mbdgt1cvhtvg6ma0euheoip0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
pjv2soembqd28le3euheoip0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
uccbkqt4l2sb15e8euheoip0t12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lobe0fosavdlf3lze2q0o12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
ovnm6k8vhojn2sv2e2q0c12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
s33pthc44ua9igk6e2q0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sv88cbcb7o5derv6e2q0e12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
7jbh5f2ss7d6v3nie2q0e12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com

tivhrvpredt9rr78vrinreo6o2v60212[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
5jb9cmvm9pjj8vlg261rs3e022st[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
4ltorald3spgu0kgds2n0o3uho1i2v0c[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5i1dfbdql2osardhds2n0i3uho1i2v02[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
e1vbsh5vl9oomfete6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ej1bl9n0l46o9v4te6vi0bdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pj9o66fr5s7jgk145o63rscusi2vove0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
5ba54io0m6ureoph5o63rscusi2vove0[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jojggmlk9s7lhquye6vi0bdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
s3ei81g6fadr2527e6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sfqit11bf0pro537e6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
96547kpaj2s2dl2le6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
n7f3h0fgnlgk2uq2wo11r02irssrc2vv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
0b0fbhp20mdsv4scwo11r0oirssrc2vv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ugri0juovl9hh9l8uosafu1oip022st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
6rqj6h3nhg8kgjsivrqnosreio2v60gj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
f39s3d02vksn1lhtv6q3ru1i30cvri[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lf8aqc64b7skp2azv6q3ru1i30cvri[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
18f5phqbdbg6etec26c0g12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
q8bps26mocuq6re4dutru70ct2w[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
46aoda7k3kdgj07gds2n0e3uho1i2v0o[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ab0rpc00jd4667vpds2n0i3uho1i2v02[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
icbcfcrfi6cpog2xwo11r0oirssrc2vv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
d6amofiedc4nfbbswo11r0oirssrc2vv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
drm1vig56j36hfisqscuf6isu1ou0tun[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hehgiqetn3tdt1qjpj70[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
766o9im0q5tm01gico0ge2sd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vj0mo9lh6nuh9un9c2d0be2h0gdj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
oj4t2iih6dejuen300eu4ivhvu52v2ea[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
rv67lm38o3jti405e2sd0cdieo0ie2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
8f9b5mbpuje4lutke2sd0t6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
g65dcoag5varua2ve2sd026isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
g79d0bsp5bergteve2sd0g6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
28phos6q9al7th2een60eeudo1uv2f0t[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
33htbkuqrq7maeofen60oeudo1uv2f0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
133bocmjd8ppsa8d00eu0los5jhea4vo[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
9jmb3qd8ugt495uke3e0gn2h[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
vi3f2e8c4oevdto9orc0ot20eon[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
dae7jsoakoq01kmugmmpm0b[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
7jbf1c0fqp8drocijrpuv20212eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
ooglgql00scghm23e6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
1cou6odl4evsq2bde6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5fl9k0dd4qlv4ibh5onr1oipe2hh0e12[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com

cbh7c256iph0vctr5onr1oipe2hh0i12[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
qg0unjs2fe8a1ud50042rsimd18ak2ob[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sfmiskebdvsoqsm66d6n0t6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
tgao5p3dhlbip2e76d6n0t6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
u3eicd2lpmjob4b86d6n0t6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
u3eicd2lpmjob4u86d6n0b6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
uoti7p2kpboor2j86d6n0o6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0c32j0j6q8up3a4b6d6n0t6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
3jn61ob016fliibe6d6n0t6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
4i7rkgeqkrdb9jqf6d6n0i6j0teu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
4o1rlg2akbpbvj4f6d6n0o6j0beu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5ce289jle8jpoq2g6d6n0o6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rlg3cieh1ovvooh5p2sji2v0oe25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
mrlf027vaikgov10co6e20bovi[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
io1v9ddpo72r4t6xee6efssoef1fh0te[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
sjfbapmchlbiap2700f2vorkkfgaaobd[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
j32gc44lim8jbdbx6d6n0c6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
jf4ga4qrivcj4dmx6d6n0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mjg6gjba76hlfg206d6n0e6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pmhdcvu7u3g4bm636d6n0t6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rbgkl8sa6ohsv1s56d6n0t6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rmik6csc635sm7456d6n0c6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
difa7emqmmeihh1re2q0b12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
kb0o2bs7bbnbkaayov6run0g2st[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
drkc9o966vk900ar00tsrl2o75eudki[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
rj4eohcbqht4ae45hom2v3o110ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
kr0ugestl213degzvo0ee2sd0bvuiov6[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
814jt4mrf7cg2dej6d6n0e6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
9cf4j7jca8nd3c4k6d6n0c6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
a83ojko69cui3sjo6d6n0o6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bogllj4albh6vg4p6d6n0i6j0teu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0oqdtu3r8abd6d8beuheoip0t12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ggos6p46s9estsoueuheoip0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
nftt6cmr8b1r2791e2q0b12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
a6m15ossl194vinoe2q0o12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
1ch1ndtjj2u8mi5d6rswoiou0bovirsv[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
mr2k2ao5up1oece16otvuifsrcuvj0c1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6ghau746mseljcthim0e2st[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
p6cm31ihpcbni624wo11r02irssrc2vv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
qit94i5tqf2j9mq5wo11r02irssrc2vv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
j4pnl4m823on6tj1boa7i30[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gefcu1q076qb27o5lo50ob1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
eb86erv58g4hmbgsuv6e0it2c0cdr[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com

ojesc10gakqt4bm2uv6e0et2c0tdr[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
7f000qp4oq07qj6j5onr1oipe2hh0g12[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
ra8sbj8jq6hokk3gtmq0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
eo5talvjhsjtgtcs3iquvhthi0c12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
1rulnov28l330v0dovirsvu10igi10ce[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
04spiistorug1jq5o6o0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
icpk5r0mvd4uh8awjed10ge2h[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ufenocumi4b0jbv8co0ce2sd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
uitni8uqiq60go18co0ce2sd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
2c8ff0an7hnj4nsdco0te2sd[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
sv25dohg9q9c37f6c2d0be2h0gdj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
amar5a8d1u6rlheoeuheoip0i12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
6cd64117t0arg8hids2n0e3uho1i2v0e[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
dja2dsvkfndnjk7sds2n0e3uho1i2v0e[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
i8buqpf6957p12hxds2n0i3uho1i2v0i[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
k8944jv715skgg1zds2n0o3uho1i2v0c[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
o7ojmhgbqa1i5ei3ds2n0e3uho1i2v0e[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
4v1cc4cmvotped1fe2q0c12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
cg6u7qu6mh2a46hqe2q0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
go4ek1oktvrli8rue2q0o12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
cbfr07jrtrhqcklrnrvo70enrvo7cuvj[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2o1rg9g07s6ihvsee6vi0gdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7c2ucjd62e9s4u4je6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
a8eoc1n6iqdb456pe6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
q882csbrq5oa58d4r6eud0i2st[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
b6e4e15hg35e2blq001sqoimd18ak2ob[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
8c1sd3hddsdtbntjh2vei2v0b12e[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
cppkbbrs1j1j8h53v7o0h8d[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
ulavlp89rts1ffs8d3ucu3uhu60e2st[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
63103hgeg7hiuuahscr0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
882j84blfc8god6j6d6n0g6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hifpjoocm0ppal6veuheoip0b12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
4i7d1v6cs5hh2k5fe2q0i12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
bj8i6tq8qf7ptboqe2sd0g6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
jg0ra34it3tdjsmye2sd026isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
l7vdk6s20b3r1e80e2sd026isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
g68mkujrpetovivv00esqnv21ur29uit[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
gr6nnbvdqn1kf48ve6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ibgkg4r0aucnhb2xe6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
sfqit11bf0pro587e6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
21dh2sca90g78hqeen60ceudo1uv2f0i[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
fmh8b02qbe7qa2ouen60oeudo1uv2f0c[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
g7q7273sc58h8omven60eeudo1uv2f0t[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

qg1e4bctbk3gdkr4e2sd0bdieo0be2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dm12uobg6via10dse2sd026iovtsupno[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ir61lpf3khg9murxhv30gst011uq0oue[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5cc19c6bgu6jn6fh00huauo0f1qtkgb4[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5iat8b7ub86lr0egcuveervisu10te2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
p7ij6im26ncmc5q4002sdoimd18ak2ob[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
db1dl1uasop4v86r6d6n0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ivdkamavjf7s4vcw6d6n0c6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
jisg02qdirmjdp3x6d6n0e6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
nmepc9ul23j2bqs16d6n0c6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
oikl0oq9grv6dit26d6n0t6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pv9davtvufl44m336d6n0b6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
pv9davtvufl44mm36d6n0b6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
qj1bggoa06prfj646d6n0g6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
t8eo8dolhcjio4276d6n0c6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
56t21hjkejopieug6d6n0c6j0ceu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
48vt0ms1tvg0pvlfp2sji2v0ee25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
mv2r1g9h6u4nh8l1un0v0pz0ehij0o12[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h3mkn3ntnk3iii7wun0y0yz0thij0c12[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
3gvl2qm6a9f8mu6euvj0ee2h[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hd010rekkecceq4iu71epp0[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
e8h2vel9711jjcpte3so6iore1ovoe0t[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
48ogl0etmirn5isge2sd0g6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
96o3vbdoeiusk7ekscr0t6j0eeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
lm173piej1hput3zscr0t6j0eeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
6i6gkuq4rrqj9n8h6d6n0e6j0ieu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
8juj12bkf63gipjj6d6n0c6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
7rjv8p3pijm3b25ip2sji2v0oe25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
aoc0te6n2lot4hkop2sji2v0ee25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
r7i37ref137vib05p2sji2v02e25p[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
2sn98d96h9pqmlcg0b6fih5[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
cjjjgubsv6egfnuq6d6n026j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
dmfd67ucs3n4mc4r6d6n0o6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
gm2ncqslo38ub9ju6d6n0c6j02eu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
hl045f89tgrdp3tv6d6n0g6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
ufqiaderpv6o44e86d6n0o6j0beu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
vllsn8cqcg9kh1a96d6n0g6j0oeu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
0c32j0j6q8up3aob6d6n0g6j0geu[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
jci7gmkna15jb2lxdfc1o6rs0ooi[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
gv2iol4m22mvjv7uco0ge2sd[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
4brcv81m4dt0b0mfco0ie2sd[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
58b8f8go25f04rpgc2d0be2h0gdj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
6rth4r9nv4kmf80hc2d0ce2h0tdj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com

91pcpe11stq5mk0kc2d02e2h0tdj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
jmmhvgdof9im2mixc2d02e2h0tdj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
sru54bhn940cf1f6c2d0te2h02dj[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
erfij3jcv5pia7sseuheoip0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
fiinjibcq0hna6uteuheoip0t12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
orpqk4rjns0ohtu2jrpuv20212eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
gec3qrvfjmnioco513e0fb5[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
7mlobqm86f3dieniv6q3ru1i30evri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
li18fvb2rse3keizv6q3ru1i30bvri[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
1cghgocfgcik9p1cv6q3ru1i302vri[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
r1qshoj05ji05ac6eoip02jovt6i2v0c[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
v292digu3l858vhj50etvuh[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
6gp98d4asbjpu4gh53e0i12eu1[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
s7jrsqlefsc11q265hiv0gun[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
lo9jctj7lggmbbvzovi02veu360tvri[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
ggokp42htrcg7m8uos2v52sh02e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
s718c2inl9aosjo6jed10te2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
d1ddjl7g30lugkrrde6e20ge2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
h3mpe296rhlu7pfwds2n0i3uho1i2v0i[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
mv2go5nr2q5oktr1ds2n0o3uho1i2v0c[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
tmvre30c69667f18ds2n0e3uho1i2v0o[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
q1b91c4fdd7q4td56rswoiou0govirsv[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
5ge5g8qdjcfbd11ge2q0e12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
fjd9n52027bjrtkte2q0o12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
igoee56leec46t8whom2v3o1102e2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
1ii9q1s7ut7pj88chom2v3o110ce2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
2788hsokf4b6lkadhom2v3o110ie2h[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
a8eoc1n6iqdb454pe6vi0cdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
agao0754idnbr0epe6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
f6gsl4d0s2cu9boue6vi0gdsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
fllsk499sp8uvbcue6vi0edsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
qb9it88vftri6v84euheoip0e12eu1[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
n3atscbl8r7ro7i1e2q0b12eu1[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
oikkgcj7j5i5e412e2q0b12eu1[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
i6tpc2a1hv0iucjxe2sd0o6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
u8pl7ven8i4knnu9e2sd0o6isuif6vri[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
s3ei81g6fadr25s7e6vi0odsovertr2s[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
6jef5kkueau1hv8i656o0c6irusv6cuv[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com
websitetheme[.]com
panhardware[.]com
mhdosoksaccf9[.]sni9icp[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
6a57jk2ba1d9keg15cbg[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
ihvpgv9psvq02ffo77et[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

incomeupdate[.]com
databasegalore[.]com
zupertech[.]com
7sbvaemscs0mc925[.]tb99[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
gq1h856599[.]gqh538acqn[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
k5kcubuassl3alrf7[.]gm3[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
highdatabase[.]com
virtualdataserver[.]com
srfnetwork[.]org
onetechcompany[.]com
bigtopweb[.]com
autonetonline[.]com
actualityworld[.]com
mappsglobal[.]com
assetdata[.]net
diamondglobalnetwork[.]com
datatidy[.]com
limoservicecompany[.]com
ioxmesh[.]com
gdbcloud[.]com
productpitfalls[.]com
webpp[.]com
websitesline[.]com
gnadptech[.]com
topwebservers[.]com
softwarelaunches[.]com
ipadsreview[.]org
ebbcloud[.]com
armrvrholo[.]com
computerrepublic[.]com
xrlinks[.]com
techforefront[.]com
storagewithoutborders[.]com
securitysystemnews[.]com
graphicscodex[.]net
globesoftwares[.]com
vmdisk[.]com
microtransito[.]com
ryaxtech[.]com
softweblinks[.]com
rollver[.]com
1cloudserver[.]com
apexwebtech[.]com

digitalphotohub[.]com
bigdataanalysts[.]com
globalsection[.]org
ebookstorelive[.]com
fqtel[.]com
appsprovider[.]com
domainingdirectory[.]com
38[.]135[.]104[.]189
37[.]48[.]84[.]156
185[.]122[.]57[.]238
81[.]4[.]122[.]101
79[.]110[.]52[.]140
178[.]249[.]69[.]35
23[.]106[.]61[.]74
185[.]163[.]47[.]211
130[.]0[.]235[.]92
188[.]120[.]239[.]154
149[.]154[.]157[.]248
185[.]189[.]151[.]178
185[.]43[.]220[.]214
84[.]38[.]183[.]45
91[.]219[.]239[.]43
179[.]43[.]169[.]32
104[.]128[.]228[.]76
176[.]10[.]118[.]136
179[.]43[.]141[.]188
185[.]99[.]133[.]129
188[.]138[.]71[.]62
91[.]219[.]239[.]54
141[.]255[.]161[.]180
179[.]43[.]169[.]30
81[.]4[.]122[.]193
79[.]110[.]52[.]139
179[.]43[.]169[.]31
5[.]61[.]57[.]152
74[.]72[.]74[.]142
185[.]163[.]45[.]150
141[.]136[.]0[.]4
173[.]232[.]146[.]12
185[.]189[.]151[.]182
79[.]110[.]52[.]138
146[.]0[.]32[.]16
185[.]185[.]117[.]15

46[.]32[.]252[.]175
45[.]89[.]106[.]3
158[.]69[.]243[.]52
18[.]220[.]219[.]143
34[.]219[.]234[.]134
13[.]59[.]205[.]66
3[.]87[.]182[.]149
3[.]16[.]81[.]254
54[.]215[.]192[.]52
54[.]193[.]127[.]66
18[.]217[.]225[.]111
13[.]57[.]184[.]217
162[.]223[.]31[.]184
83[.]171[.]237[.]173
192[.]99[.]221[.]77
198[.]12[.]75[.]112
107[.]152[.]35[.]77
93[.]119[.]106[.]69
23[.]92[.]211[.]15
135[.]181[.]10[.]254
199[.]241[.]143[.]102
172[.]97[.]71[.]162
45[.]150[.]4[.]10
192[.]3[.]31[.]210
162[.]241[.]124[.]32
34[.]203[.]203[.]23
204[.]188[.]205[.]176
5[.]252[.]177[.]25
5[.]252[.]177[.]21
51[.]89[.]125[.]18
139[.]99[.]115[.]204
66[.]172[.]27[.]175
185[.]225[.]69[.]69
144[.]217[.]174[.]58
45[.]10[.]21[.]121
149[.]255[.]35[.]187
172[.]245[.]92[.]219
212[.]103[.]61[.]118
104[.]168[.]165[.]76
162[.]248[.]245[.]79
94[.]158[.]244[.]32
45[.]66[.]156[.]171
24[.]132[.]243[.]118

51[.]81[.]0[.]3
107[.]175[.]96[.]36
193[.]70[.]109[.]24
79[.]141[.]162[.]41
103[.]124[.]105[.]87
89[.]44[.]9[.]70
54[.]177[.]231[.]23
51[.]161[.]59[.]32
185[.]62[.]58[.]210
23[.]145[.]80[.]43
104[.]217[.]8[.]116
192[.]3[.]255[.]190
202[.]5[.]24[.]181
198[.]23[.]206[.]4
34[.]217[.]37[.]240
216[.]189[.]145[.]128
158[.]51[.]87[.]108
38[.]68[.]50[.]174
158[.]51[.]85[.]116
38[.]117[.]105[.]187
91[.]189[.]187[.]189
192[.]250[.]230[.]158
185[.]186[.]247[.]34
45[.]149[.]114[.]106
192[.]243[.]97[.]109
140[.]82[.]3[.]156
45[.]76[.]2[.]102
144[.]202[.]84[.]65
104[.]248[.]255[.]207
63[.]141[.]224[.]90
172[.]106[.]86[.]13

MD5:

4f2eb62fa529c0283b28d05ddd311fae

SHA-256:

3cae987fd99950a299b690a1e03a09a15adc9eb556f7f2901afd3bc06719f4db
dbe2d877924c7b650d380d86cb46bf5d91a44ba03f30f6eee93c621c23a852f9
24d1bd110c0bf7f21f75c9e99ddbb29bd0cfebf5577b4202d35e4ffe36477de6
59a779046e32940c08f4c723143134a1b14d6855de3482e8503fca47aea9413e
e6ff50bdcc7b57fbc52ab203470fa388487bf92412c59b2678d57dde701ba985
0afcd12924eed83f0e3f33c51a0766849df661ea2220b4a919297b0ef742b7c3
d5c4d94bb747555921469eff6a3660456d0c048c735de4bb9099c303d713e73e

65226d59bb790120af2ad70d48736a8a223f6122d6ee5dd6b48bd5c47ff94b0b
5ed2e0bf353cfee15e50f2e4188fed20c79cf2c6dc517c34069570ddca9c92f9
c418acbe45ccaa7e66eb9db8fd595a89c8215c9ac5e2d151dd3389641e81b50a
67ff5c5fd19b23fb92cb0a395c9e12729c3a31ae21b44bfccde671f84e18f9c5
3aff515be9c17e3e6a46e891e10a2e807e9595111049b1d7c229e1f920b680c0
61d50f4a45cde3234e612016fb6816b47ebf4b6644b759365ffd53eb6bb1e5e7
4d4f0eb982a52768e1195e4632a0de4f2671c99cd2ce2acbca6442de5f25251e
7cfb684fb46e9b66881d213fa212a39b770a7820c627c7ce2073d397dead9430
f2a8bdf135caca0d7359a7163a4343701a5bdfbc8007e71424649e45901ab7e2
4e8f24fb50a08c12636f3d50c94772f355d5229e58110cccb3b4835cb2371aec
e9ddf486e5aeac02fc279659b72a1bec97103f413e089d8fabc30175f4cdbf15
88cd1bc85e6a57fa254ede18f96566b33cee999c538902aefc5b819d71163d07
ec5f07c169267dec875fdd135c1d97186b494a6f1214fb6b40036fd4ce725def
0d770e0d6ee77ed9d53500688831040b83b53b9de82afa586f20bb1894ee7116
6e2069758228e8d69f8c0a82a88ca7433a0a71076c9b1cb0d4646ba8236edf23
5f7d08eb2039a9d2e99ebf3d0ef2796b93d0a01e9b8ec403fec8fcdf46448693
112f92cfecdc4e177458bc1caebcc4420b5879840f137f249fac360ddac64ddd
a45a77ad5c138a149aa71fb323a1e2513e7ac416be263d1783a7db380d06d2fc
b81beb17622d4675a1c6f4efb358cc66903366df75eb5911bca725465160bdb6
dcf48223af8bb423a0b6d4a366163b9308e9102764f0e188318a53f18d6abd25
2836e5553e1ae52a1591545b362d1a630e3fef7e6b7e8342a84008fe4a6473a9
cf1d992f776421f72eabc31d5afc2f2067ae856f1c9c1d6dc643a67cb9349d8c
0acb884f2f4cfa75b726cb8290b20328c8ddbcd49f95a1d761b7d131b95bafec
776014a63bf3cc7034bd5b6a9c36c75a930b59182fe232535bb7a305e539967b
c4ff632696ec6e406388e1d42421b3cd3b5f79dcb2df67e2022d961d5f5a9e78
136f4083b67bc8dc999eb15bb83042aeb01791fc0b20b5683af6b4ddcf0bbc7d
6d08b767117a0915fb86857096b4219fd58596b42ccf61462b137432abd3920e
ca83d7456a49dc5b8fe71007e5ac590842b146dd5c45c9a65fe57e428a8bd7c6
2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
9059c5b46dce8595fcc46e63e4ffbceeed883b7b1c9a2313f7208a7f26a0c186
ca66b671a75bbee69a4a4d3000b45d5dc7d3891c7ee5891272ccb2c5aed5746c
cfb57906cf9c5e9c91bc4aa065f7997b1b32b88ff76f253a73ee7f6cfd8fff2f
98473e1b8f7bedd5cfa3b83dad611db48eee23faec452e62797fb7752228c759
2ebbb99b8dae0c7b0931190fa81add987b44d4435dafcf53a9cde0f19bb91398
3c86859207ac6071220976c52cef99abf18ae37ae702c5d2268948dda370910b
0585ed374f47d823f8fcbb4054ad06980b1fe89f3fa3484558e7d30f7b6e9597
23e20d630a8fd12600c2811d8f179f0e408dcb3e82600456db74cbf93a66e70f
b0bfe6a8aa031f7f5972524473f3e404f85520a7553662aaf886055007a57db5
7ed1b6753c94250ad3c1c675eb644940c8104ff06a123252173c33cc1be5e434
74202eed181e2b83dd0ab6f791a34a13bd94e63e86b82395f9443cb5aeddc891
7a3b27cf04b7f8110fc1eee5f9c4830d38ac00467fc856330115af4bffaf35b6
69f0d85119123f3c2e4c052a83671732aced07312a05a3abf4ab0360c70f65de

d7c05bd68e8bde3d13aa7dbd6911461104d06715da15d3ee7f75136fa8330cc2
a4f1f09a2b9bc87de90891da6c0fca28e2f88fd67034648060cef9862af9a3bf
d19ff098fe0f5947e08ec23be27d3a3355e14fb20135d8c4145126caa8be4b05
24caf54e7c3fe308444093f7ac64d6d520c8f44ea4251e09e24931bdb72f5548
6866041f93141697ec166fe64e35b00c5fcd5d009500ecf58dd0b7e28764b167
065e9471fb4425ec0b3a2fd15e1546d66002caca844866b0764cbf837c21a72a
f9a74ac540a6584fc3ba7ccc172f948c6b716cceea313ce1d9e7b735fa2a5687
1f5a915e75ad96e560cee3e24861cf6f8de299fdf79e1829453defbfe2013239
279d5ef8f80aba530aaac8afd049fa171704fc703d9cfe337b56639732e8ce11
8199f309478e8ed3f03f75e7574a3e9bce09b4423bd7eb08bb5bff03af2b7c27
94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916
ad67aaa50fd60d02f1378b4155f69cffa9591eaeb80523489a2355512cc30e8c
2a352380d61e89c89f03f4008044241a38751284995d000c73acf9cad38b989e
4fbfeb7a0bb6b9841b92fa4e6b5a7bdb69c2a12ed39691c9495ff88cd6f58836
117317d623003995d639975774edd1bfe38cec7d24b22d3e48d22c91cf8636bb
0c14a791f8a48d2944a9fa842f45becb7309ad004695e38f48fca69135d327c6
1c17c39af41a5d8f54441ce6b1cf925f6727a2ee9038284a8a7071c984d0460f
656384c4e5f9fe435d51edf910e7ba28b5c6d183587cf3e8f75fb2d798a01eeb
6df1d7191f6dd930642cc5c599efb54bfcc964b7a2e77f6007787de472b22a6a
f006af714379fdd63923536d908f916f4c55480f3d07adadd53d5807e0c285ee
749bf48a22ca161d86b6e36e71a6817b478a99d935cd721e8bf3dba716224c84
9301e48ea3fa7d39df871f04072ee47b9046d76aa378a1c5697f3b2c14aef1d6
292e5b0a12fea4ff3fc02e1f98b7a370f88152ce71fe62670dd2f5edfaab2ff8
873717ea2ea01ae6cd2c2dca9d6f832a316a6e0370071bb4ee6ecff3163f8d18
d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142
f7e8c9d19efd71f5c8217bf12bdd3f6c88d5f56ab65fea02dc2777c5402a18f1
b295c5ad4963bdffa764b93421c3dd512ca6733b79bdff2b99510e7d56a70935
89016b87e97a07b4e0263a18827defdeaa3e150b1523534bbdebe7305beabb64
f5bc4a9ffc2d33d4f915e41090af71544d84b651fb2444ac91f6e56c1f2c70d5
7bf3457087ea91164f86f4bb50ddb46c469c464c300228dba793f7bfe608c83e
f88530bc87cf2c133c0a50e434ce0428694901fe7860abb42737097fdea56b30
bca5560a9a9dd54be76e4a8d63a66e9cfd731b0bd28524db05cc498bb5b56384
194f4d1823e93905ee346d7e1fffc256e0befd478735f4b961954df52558c618
e41a7616a3919d883beb1527026281d66e7bcdaff99600e462d36a58f1bdc794
0819db19be479122c1d48743e644070a8dc9a1c852df9a8c0dc2343e904da389
c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168
6ff3a4f7fd7dc793e866708ab0fe592e6c08156b1aa3552a8d74e331f1aea377
7c68f8d80fc2a6347da7c196d5f91861ba889afb51a4da4a6c282e06ef5bdb7e
948bfdfad43ad52ca09890a4d2515079c29bdfe02edaa53e7d92858aa2dfbe4c
b348546f4c6a9bcafd81015132f09cf8313420eb653673bf3d65046427b1167f
c5a818d9b95e1c548d6af22b5e8663a2410e6d4ed87df7f9daf7df0ef029872e
cdd9b4252ef2f6e64bccc91146ec5dc51d94e2761184cd0ffa9909aa739fa17e
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07

c7924cc1bc388cfcdc2ee2472899cd34a2ef4414134cbc23a7cb530650f93d98
c96b7a3c9acf704189ae8d6124b5a7b1f0e8c83c246b59bc5ff15e17b7de4c84
dbd26ccb3699f426dc6799e218b91d1a3c1d08ad3006bc2880e29c755a4e2338
118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51
327f1d94bc26779cbe20f8689be12c7eee2e390fbddb40b92ad00b1cddfd6426
5cf85c3d18cd6dba8377370883a0fffda59767839156add4c8912394f76d6ef0
cbbe224d9854d6a4269ed2fa9b22d77681f84e3ca4e5d6891414479471f5ca68
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
2a276f4b11f47f81dd2bcb850a158d4202df836769da5a23e56bf0353281473e
674075c8f63c64ad5fa6fd5e2aa6e4954afae594e7b0f07670e4322a60f3d0cf
915705c09b4bd108bcd123fe35f20a16d8c9c7d38d93820e8c167695a890b214
b35e0010e0734fcd9b5952ae93459544ae33485fe0662fae715092e0dfb92ad3
c741797dd400de5927f8b5317165fc755d6439749c39c380a1357eac0a00f90c
e60e1bb967db273b922deeea32d56fc6d9501a236856ef9a3e5f76c1f392000a
1ec138f21a315722fb702706b4bdc0f544317f130f4a009502ec98345f85e4ad
3985dea8e467c56e8cc44ebfc201253ffee923765d12808aaf17db2c644c4c06
557f91404fb821d7c1e98d9f2f5296dc12712fc19c87a84602442b4637fb23d4
5f8650ca0ed22ad0d4127eb4086d4548ec31ad035c7aec12c6e82cb64417a390
f61a37aa8581986ba600286d65bb76100fb44e347e253f1f5ad50051e5f882f5
f81987f1484bfe5441be157250b35b0a2d7991cf9272fa4eacd3e9f0dee235de
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d
b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2
ad2fbf4add71f61173975989d1a18395afb8538ed889012b9d2e21c19e98bbd1
c20fd967d64e9722d840ec4292645b65896d0ee3ebe31090e15c5312d889c89e
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8
acc74c920d19ea0a5e6007f929ef30b079eb2836b5b28e5ffcc20e68fa707e66

70d93035b0693b0e4ef65eb7f8529e6385d698759cc5b8666a394b2136cc06eb
b9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8
bbd16685917b9b35c7480d5711193c1cd0e4e7ccb0f2bf1fd584c0aebca5ae4c
0e1f9d4d0884c68ec25dec355140ea1bab434f5ea0f86f2aade34178ff3a7d91
f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c
247a733048b6d5361162957f53910ad6653cdef128eb5c87c46f14e7e3e46983
0affab34d950321e3031864ec2b6c00e4edafb54f4b327717cb5b042c38a33c9
611458206837560511cb007ab5eeb57047025c2edc0643184561a6bf451e8c2c
240ef5b8392b8c7a5a025c36a7e5b0e03e5bb0d0d1a28703bb22e6159a4fd10e

List of CVE commonly exploited by DARK HALO:

CVE-2021-1879

This issue was addressed by improved management of object lifetimes. Processing maliciously crafted web content may lead to universal cross site scripting. This issue is fixed in iOS 12.5.2, iOS 14.4.2 and iPadOS 14.4.2, watchOS 7.3.3.

Advanced Persistent Threat (APT): TRANSPARENT TRIBE

The cybercrime group "TRANSPARENT TRIBE" (also known as APT36, ProjectM, Mythic Leopard, TEMP.lapie) is active since 2012. Transparent Tribe performs cyber-espionage operations with the intent of collecting sensitive information from various countries based on military and diplomatic interests. It mainly relies on both spear phishing and watering hole attacks to gain its foothold on victims. The phishing email is either a malicious macro document or an rtf file exploiting vulnerabilities, such as CVE-2012-0158, CVE-2017-0199. The attacker used watering hole websites for deliver a remote access Trojan (RAT) dubbed «MSIL/Crimson RAT». The RAT allowed attackers to steal data from infected devices, log keystrokes and capture screenshots. In the past, the group has also deployed different types of RATs, such as BreachRAT, PeepyRAT, DarkComet, Luminosity RAT, and njRAT.

Indicators of Compromise (IOCs)

CnC:

198[.]46[.]177[.]73
193[.]164[.]131[.]58
5[.]189[.]145[.]118
193[.]228[.]53[.]0
193[.]111[.]155[.]137
173[.]249[.]14[.]104
173[.]249[.]42[.]113
45[.]32[.]151[.]155
209[.]127[.]16[.]126
104[.]227[.]97[.]53
198[.]12[.]90[.]116
213[.]136[.]73[.]122
192[.]3[.]157[.]104
172[.]245[.]87[.]12
13[.]78[.]188[.]237
134[.]119[.]181[.]142
173[.]249[.]22[.]30
185[.]174[.]102[.]105
5[.]189[.]134[.]216
185[.]136[.]169[.]155
107[.]175[.]1[.]103
64[.]188[.]25[.]206
79[.]143[.]188[.]166
213[.]136[.]84[.]43
80[.]241[.]221[.]109
185[.]136[.]163[.]197
88[.]150[.]227[.]71

193[.]22[.]96[.]100
176[.]107[.]177[.]77
209[.]58[.]149[.]88
87[.]247[.]155[.]111
64[.]188[.]13[.]181
64[.]188[.]25[.]143
5[.]189[.]131[.]67
5[.]189[.]167[.]220
79[.]143[.]181[.]21
213[.]136[.]69[.]224
173[.]212[.]192[.]229
173[.]249[.]50[.]57
107[.]173[.]204[.]38
23[.]254[.]119[.]11
23[.]254[.]119[.]118
185[.]136[.]169[.]139
66[.]154[.]113[.]38
89[.]249[.]65[.]206
5[.]189[.]167[.]65
5[.]189[.]152[.]147
5[.]189[.]167[.]23
178[.]238[.]228[.]113
64[.]188[.]25[.]176
139[.]28[.]36[.]212
185[.]161[.]210[.]111
193[.]42[.]105[.]40
212[.]90[.]111[.]12
104[.]161[.]42[.]234
151[.]106[.]14[.]125
172[.]245[.]247[.]112
64[.]188[.]12[.]126
104[.]144[.]198[.]105
151[.]106[.]19[.]220
167[.]160[.]166[.]177
134[.]119[.]181[.]15
45[.]77[.]246[.]69
http://sahirlodhi[.]com/usr/api[.]txt
http://iiaonline[.]in/9999[.]jpg
http://iiaonline[.]in/111[.]jpg
http://iiaonline[.]in/DefenceLogo/theta[.]bmp
http://larsentobro[.]com/mbda/goliath1[.]bmp
http://larsentobro[.]com/mbda/mundkol
http://iiaonline[.]in/merj[.]bmp

http://iiaonline[.]in/sasha[.]jpg
http://iiaonline[.]in/timon[.]jpeg
http://iiaonline[.]in/camela[.]bmp
http://iiaonline[.]in/111[.]png
http://afgcloud7[.]com/logs/ssc[.]mcom
http://cynqms[.]com/3RanD!0rTt_ooN/_Clientere03Lop/_B0e4oRa1@llpP_0agEs/
http://bdrive[.]club/14[.]5/record[.]php/
http://bdrive[.]club/14[.]5/connection[.]php?
http://bdrive[.]club/14[.]5/record[.]php/?USERNAME&#x3D
http://cloudserve[.]online/14[.]5/syncfile[.]php/C/Users/SNk72CS/Downloads
http://ezeescan[.]com/_isolated_codes/C0n_eections/checkfonts[.]php
http://ezeescan[.]com/_isolated_codes/C0n_eections/Lad!esFirst[.]php
http://tprlink[.]com/needo/shake/c0_nCussi0N[.]php
http://tprlink[.]com/needo/shake/iLln_Ess_is_0k[.]php
http://kmcodecs[.]com/A1L5C3endRa@l/b2sp-inutor/completenod[.]php
http://ezeescan[.]com/_isolated_codes/C0n_eections/de_pTa!Ls[.]php
http://kmcodecs[.]com/A1L5C3endRa@l/b2sp-inutor/motos[.]php
http://ezeescan[.]com/_isolated_codes/C0n_eections/Prob_ab3ili8es[.]php
http://firebasebox[.]com/tootie292/reboshw/1Inter-view_Call[.]php
http://firebasebox[.]com/tootie292/reboshw/iLln_Ess_is_0k[.]php
http://firebasebox[.]com/tootie292/reboshw/c0_nCussi0N[.]php
http://bdrive[.]club/14[.]5/working[.]php/?USERNAME&#x3D
http://cloudserve[.]online/14[.]5/record[.]php/
http://tprlink[.]com/needo/shake/1Inter-view_Call[.]php
http://ezeescan[.]com/_isolated_codes/C0n_eections/_inpo_dent[.]php
http://peechtrees[.]com/BudDH1!$st/0bJ3ct0R!3nTed/
http://pbxmobiflex[.]com/new_tg/smeshapp/registration[.]php
http://pbxmobiflex[.]com/new_tg/smeshapp/upload_file[.]php
http://pbxmobiflex[.]com:9090/imsignup/
http://pbxmobiflex[.]com/new_tg/smeshapp/uploadcontact[.]php
http://pbxmobiflex[.]com/new_tg/smeshapp/verification[.]php
http://qhavcloud[.]com//northernlights//JobTCP1[.]php
http://qhavcloud[.]com//northernlights//JobTCP2[.]php
http://qhavcloud[.]com//northernlights//Uninstaller[.]php
http://qhavcloud[.]com//northernlights//PingPong[.]php
http://qhavcloud[.]com//northernlights//JobWork1[.]php
http://qhavcloud[.]com//northernlights//updateproductdownload[.]php
http://qhavcloud[.]com//northernlights//postdata[.]php
http://qhavcloud[.]com//northernlights//JobProcesses[.]php
http://qhavcloud[.]com//northernlights//JobWork2[.]php
http://f3cloud[.]com/P0urWa1t3_r!es/iptonps[.]php
http://isroddp[.]com/rEmt1t_pE7o_pe0Ry/hipto[.]php

http://mail[.]gov[.]in[.]sites[.]default[.]files[.]attachment[.]maildrive[.]email/?att=1569817404
http://email[.]gov[.]in[.]maildrive[.]email/?att=1581914657
http://email[.]gov[.]in[.]maildrive[.]email/?att=1579160420
http://intribune[.]blogspot[.]com/2015/11/army-air-defenceengineers-and-signal-to[.]html
http://intribune[.]blogspot[.]com/2015/09/sc-seeks-army-response-on-batch-parity[.]html
http://intribune[.]blogspot[.]com/2015/05/seniors-juniors-and-coursemates-please[.]html
http://cdrfox[.]xyz/
http://intribune[.]blogspot[.]com/2015/07/awho-defence-and-para-military-forces[.]html
http://intribune[.]blogspot[.]com/2015/11/4-sikh-army-officers-being-trialed-in[.]html
http://intribune[.]blogspot[.]com/2015/11/seventh-pay-commission-recommends[.]html
http://www[.]avadhnama[.]com/latest/batchparity-command-exit-policy[.]doc
http://www[.]scan9t[.]com/aegon/JobWork2[.]php
http://www[.]scan9t[.]com/aegon/postdata[.]php
http://www[.]scan9t[.]com/aegon/JobTCP2[.]php
http://www[.]scan9t[.]com/aegon/PingPong[.]php
http://www[.]scan9t[.]com/aegon/JobTCP1[.]php
http://www[.]scan9t[.]com/aegon/JobWork1[.]php
https://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Armed-Forces-Spl-Allowance-Order/html/
https://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Images/8534
https://demo[.]smart-school[.]in/uploads/staff_documents/9/Sheet_Roll/html
https://demo[.]smart-school[.]in/uploads/student_documents/12/css/
https://demo[.]smart-hospital[.]in/uploads/staff_documents/19/IncidentReport/html/
https://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Defence-Production-Policy-2020/html/
https://demo[.]smart-hospital[.]in/uploads/staff_documents/19/ParaMil-Forces-Spl-Allowance-Order/html/
https://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Req-Data/html
https://drivetoshare[.]com/mod[.]gov[.]in_dod_sites_default_files_Revisedrates/html
https://demo[.]smart-hospital[.]in/uploads/staff_documents/19/Sheet_Roll/html
https://mediafiles[.]live/aditii
http://mediaflix[.]live/files/skype-lite[.]apk
http://mediadrive[.]cc/?a=W1550558721I&fbclid=IwAR1PzHnHCOjDqfpqaBqxnY4o1xMX6ibdgXAComUmJuHFYHgtCBHFq5NlYug
http://social[.]medialinks[.]cc/files/hot_song[.]rar
http://filelinks[.]live/files/Note%20Verbal[.]doc
http://filelinks[.]live/Details-and-Invitations

http://drivestransfer[.]com/myfiles/Dinner%20Invitation[.]doc/win10/Dinner%20Invitation[.]doc
http://drivestransfer[.]com/files/Age-Review-of-Armd-Forces[.]doc
http://mediaclouds[.]live/files/attachment[.]zip
http://mediafiles[.]live/files/khushi%20pics%20all[.]zip
http://cloudsbox[.]net/files/new%20preet%20cv[.]zip
http://hostflix[.]live/files/my_new_pic[.]zip
https://shareone[.]live/New-sonam-cv1
https://sharingmymedia[.]com/myfiles/Immediate%20Message[.]docm/Unknown%20OS%20Platform/Immediate%20Message[.]docm
http://armypostalservice[.]com/myfiles/file[.]doc/win7/file[.]doc
http://cloudsbox[.]net/files/sonam%20karwati[.]exe
http://cloudsbox[.]net/files/sonam
http://cloudsbox[.]net/files/nisha%20arora%20sharma[.]zip
https://sharingmymedia[.]com/files/1More-details[.]doc
http://filestudios[.]net/files/Nisha%20Doc[.]doc
http://10feeds[.]com/temp[.]dotm
http://sharingmymedia[.]com/recordsdata/Standards-of-Military-Officers[.]doc
http://sharingmymedia[.]com/files/Criteria-of-Army-Officers[.]doc
http://drivestransfer[.]com/files/Officers-Posting-2021[.]doc
http://drivestransfer[.]com/files/Parade-2021[.]xlam
http://cloudsbox[.]net/files/cv%20ssss[.]zip
https://cloudsbox[.]net/files/sonam
https://datacyncorize[.]com/
https://datacyncorize[.]com/INDISEM-2021[.]ppt
http://file-attachment[.]com/files/fauji%20india%20september%202019[.]xls
http://mediafiles[.]live/files/my%20fldr%20for%20u%20diensh[.]zip
https://datacyncorize[.]com/INDISEM-2021(INDISEM-2021[.]ppt
http://social[.]medialinks[.]cc/Case-Detail
https://cloudsbox[.]net/sonam11
http://drivestransfer[.]com/files/My-Resume-Detail[.]doc
http://mediaclouds[.]live/files/cnics[.]zip
http://mediabox[.]live/anita-resume4
http://file-attachment[.]com/files/pfp-73rd%20independence%20day%20gallantry%20awards%20[.]xls
http://cloudsbox[.]net/files/new%20cv[.]zip
http://mediadrive[.]cc/?a=W1549544649l
http://shareflix[.]co/larmina-circulum-vetae-complete-2020
http://drivestransfer[.]com/files/Special-Services-Allowance-Armd-Forces[.]xlam
https://email[.]gov[.]in[.]attachment[.]drive[.]servicesmail[.]site/New-Projects-List
http://cloudsbox[.]net/sonam11
http://filestudios[.]net/
https://filestudios[.]net/Sunita-Singh1[.]html

http://filestudios[.]net/files/sonam%20cv[.]zip
https://cloudsbox[.]net/My-Pic
https://cloudsbox[.]net/sonam-karwati5
http://mediafiles[.]live/files/for%20u%20krishna%20my%20pic%20and%20video%20fldr[.]zip
http://cloudsbox[.]net/files/sonam%20karwati[.]zip
http://templatesmanagersync[.]info/essa[.]dotm
http://social[.]medialinks[.]cc/my-100-pics
http://mediashare[.]cc/?a=W1551315913I
https://datacyncorize[.]com/NDC-Updates
https://studioflix[.]net/my-social
http://social[.]medialinks[.]cc/files/scan0001[.]rar
http://email[.]gov[.]in[.]attachment[.]drive[.]servicesmail[.]site/files/Coast%20Guard%20HQ%2010[.]rar
https://emailhost[.]network/National-Conference-2021
http://mediabox[.]live/files/nisha-resume-2020[.]zip
http://cloudsbox[.]net/files/sonamkarwati[.]exe
http://shareflix[.]co/files/lkgame[.]apk
http://cloudsbox[.]net/files/preet[.]doc
https://mediaflix[.]net/BHC-PR
http://datacyncorize[.]com/
https://7thcpcupdates[.]info/downloads/7thPayMatrix[.]xls
http://newsupdates[.]myftp[.]org/lee/vbc[.]exe
http://sharingmymedia[.]com/files/7All-Selected-list[.]xls
https://sharingmymedia[.]com/files/More-details[.]docm
https://datacyncorize[.]com/INDISEM-2021(INDISEM-2021[.]ppt)
https://datacyncorize[.]com/INDISEM-2021
http://tryanotherhorse[.]com/config[.]txt
http://212[.]8[.]240[.]221:80/server/upload[.]php
yepp[.]ddns[.]net
micrsoft[.]ddns[.]net
timesofindiaa[.]in
afgcloud7[.]com
cynqms[.]com
bdrive[.]club
kmcodecs[.]com
firebasebox[.]com
admin_USER-PC_v1_225061&amp
cloudserve[.]online
bdrive[.]space
ezeescan[.]com
peechtrees[.]com
bbmdroid[.]com

eastmedia1221[.]com
kssync3347[.]com
student3347[.]mooo[.]com
winupdater2112[.]com
mustache-styles[.]com
winupdatess[.]no-ip[.]biz
thefriendsmedia[.]com
ordering-checks[.]com
99mesotheliomalawyers[.]com
eastmedia3347[.]com
kssync3343[.]com
kssync3347[.]co[.]cc
ad2[.]admart[.]tv
bbmsync2727[.]com
facemedia[.]co[.]cc
eastmedia3347[.]co[.]cc
mahee[.]kssync3343[.]co[.]cc
lolxone[.]com
vhideip[.]com
wisheshub[.]com
dvdonlinestore[.]net
onlinestoreonsale[.]com
bhai1[.]ddns[.]net
Mpjunkie[.]com
Idnnews[.]net
smeshapp[.]com
Vdjunky[.]org
idsadesk[.]in
idsagroup[.]in
qhavcloud[.]com
f3cloud[.]com
isroddp[.]com
mail[.]gov[.]in[.]sites[.]default[.]files[.]attachment[.]maildrive[.]email
cdrfox[.]xyz
intribune[.]blogspot[.]com
vmi22485[.]contabo[.]host
hussainibuilder[.]com
Bluesync2121[.]com
Eastmedia2112[.]com
pradahandbagsshoes[.]com
Mvssync8767[.]com
Applemedia1218[.]com
Avssync3357[.]com

knockknock-jokes[.]com
www[.]scan9t[.]com
tasnimnewstehran[.]club
Datroapp[.]mssql[.]somee[.]com
uronlinestores[.]net
newsbizupdates[.]net
mediaflix[.]live
social[.]medialinks[.]cc
filelinks[.]live
drivestransfer[.]com
mediaclouds[.]live
mediafiles[.]live
cloudsbox[.]net
hostflix[.]live
shareone[.]live
sharingmymedia[.]com
armypostalservice[.]com
onedrives[.]cc
digiphotostudio[.]live
filestudios[.]net
10feeds[.]com
millitarytocorp[.]com
servicesmail[.]site
vmi433658[.]contaboserver[.]net
systemsupdated[.]duckdns[.]org
bjorn111[.]duckdns[.]org
tgservermax[.]duckdns[.]org
india[.]gov[.]in[.]attachments[.]downloads[.]7thcpcupdates[.]info
datacyncorize[.]com
file-attachment[.]com
mediabox[.]live
mediadrive[.]cc
shareflix[.]co
mailout[.]pmayindia[.]com
urservices[.]net
email[.]gov[.]in[.]attachment[.]drive[.]servicesmail[.]site
mailer[.]pmayindia[.]com
clawsindia[.]com
sharemydrives[.]com
maildrive[.]email
awsyscloud[.]com
templatesmanagersync[.]info
mediashare[.]cc

studioflix[.]net
vmd41059[.]contaboserver[.]net
shareboxs[.]net
emailhost[.]network
mediaflix[.]net
7thcpcupdates[.]info
newsupdates[.]myftp[.]org
mail[.]clawsindia[.]com
larsentobro[.]com
tprlink[.]com
pmayindia[.]com
email[.]gov[.]in[.]maildrive[.]email
tryanotherhorse[.]com
173[.]212[.]234[.]57
206[.]81[.]26[.]164
157[.]230[.]112[.]219
PASSWORD&#x3D
207[.]154[.]248[.]69
46[.]101[.]131[.]249
80[.]240[.]134[.]51
95[.]85[.]43[.]35
182[.]181[.]239[.]4
193[.]164[.]131[.]225
91[.]194[.]91[.]202
178[.]238[.]232[.]44
178[.]238[.]235[.]143
173[.]212[.]194[.]214
165[.]22[.]86[.]11
198[.]54[.]119[.]174
199[.]188[.]200[.]93
93[.]104[.]213[.]217
213[.]136[.]79[.]50
82[.]196[.]13[.]94
185[.]174[.]102[.]105
185[.]165[.]168[.]35

MD5:

5A27D092E4A87554206F677B4EADC6F5
ddd4f8ba3190cfa1f813e79864a73fe1
7e42de66eee8d280a3ba49d5b979c737
428371be27fc057baac3ea81a8643435
ddb66b231ab63c65a8ce139e73652aec
4e9b81e70227575f2d2a6dd941540afa

8a991eec65bd90f12450ee9dac0f286a
edccbc7f880233de987ba4e917877df2
ca48224adce9609dc07e50930dd1afae
ccc6bb98a2629338d49587d186562fd3
ca77af41cbd8c2fd44085d0d61bac64b
9fd2838421b28674783b03eb46f4320f
84c30675b5db34c407b98ea73c5e7e96
53a60acc6a09a7fa2eebf4eb88c81af5
8c713cffdc599930a9236c2d0d0ee91a
53c10ac66763739b95ac7192a9f489ad
9d4504cdb7b02b9c9fffefcf9b79101d
3cc848432e0ebe25e4f19effdd92d9c2
3a64e2d3558a28c4fdb0f076fa09e1a1
6409930f39cd6c17fb68f7fee47b1cdf
801f94eedb9481fb65709457c1f4c47a
c411ee81c34e14a1ace7e72bea2e8d12
04e8404f1173037ba4e11241b141d91d
438031b9d79a17b776b7397e989dd073
a6ef041311497bcddb8818b5a4f6c90e
858a729819cc082f2762b6d488284c19
0e3e81f4d2054746f74442075f82a5c5
27ca136850214234bcdca765dfaed79f
4A22A43CCAB88B1CA50FA183E6FFB6FA
4B733E7A78EBD2F7E5306F39704A86FD
F5375CBC0E6E8BF10E1B8012E943FED5
E7B32B1145EC9E2D55FDB1113F7EEE87
CAC1FFC1A967CD428859BB8BE2E73C22
2dc177b5be8f770a415ce18d2a11047a
f220c793ed46f4f38beea8fc55e74877

SHA-256:

9acf62d22e93d6ea68b8d04a174fcd0c4e53d0f14fe1e7fadfcef4dfcc57f480
98894973a86aa01c4f7496ae339dc73b5e6da2f1dbcd5fe1215f70ea7b889b85
8eb61e3d802869e45e2ee94176dd7dbb0ab5fe8aec980104a7b16b1f0dde13d6
e394ab8a308e92ca6cf10ffbb951b3225685278b55a4b00c68c4c763d0601efa
dc8bd60695070152c94cbeb5f61eca6e4309b8966f1aa9fdc2dd0ab754ad3e4c
f0e5e130852f91d815632d159ce1979ba997a14af9c26d164ead9f6c2bb71854
68253af6013d22553f3e87b8fd59dfade5c7f120b07ea679b041dcdcb845885a
b732193b2bbbc9c89dfd2e788a3a0f27ea54bf2868474c290fdeaa368a3a028f
24eba94fa7e03d688c27bef6b4f47c4109192abf8baeb25e93e2005f01994b20
19e58e6767d3e7772b559f5ac3ef2a5c7572143b5e28cc7f4b8f32ad22a763e2
9f50b0f990b7f89b105ab2c6d99b6bee93c3963f265ee41176d1854996069a40
bb3e132763ec034a5f022ce503d12fc50c324009d4268293f80ae66b6c07b7ab

29c00601e4b7a5c77d5beb80d68787a9f5ed140c2104fce2c8c3884362e04721
5215618bfcae4b572c635c2a2cb93b58b10afe417af9e8fc7b01e766a2276ba1
221913be6d35172556fd4444b15b70f921d3fc8f4b3c786be693eefde744d70d
67c60606a3fa28cbf706c1b52be123fd798df3f30c938e5eb294e8344aca40f5
7237c1052e25fccbf4ba53bcb1853618a92cbf8709d2d6906024e03ea4cceea9
fe048bb499a85f51a739a773664d0fa0474c15eba527ed9031f544e6e9710d05
f147494780e6faa095b352183be5373de023e7d71fc127dacb00ad953577ebb7
175fb973539f32da8bf44d376d2e581b29eae088fafe75c22dd889aee8d67be7
0de80caf5f1369419852d26f28f7a4abff53d1f7861cf639c25ab20a67a3c7d7
5481af07cff7edf221b3c05bb24780e58b321595c40b776da4fb7cde4693dfba
9aefdda207f4ee5d8621b25eb605bbe6bdd861e56f8de1b885f08d090b86338e
3a819fca00ea6e20bd57b9f186759565c81b11c2386fa5ab0f6476c385cedf78
d541c249a98d852905273efeaa046db4dbc70ca0151fc70f1a8abd298191cb6a
fe515a4689e39592af94244c1a3a6e07d20b6d7b579afbe16899e1db0f6d4552
0a7d73216cbbd156abb9b3a21a65b3070a21ffb643e220e7ca24c01e5e9c23dc
140ba40d2a33c67b38a909ca076a0989632fbefc17da9574e727925f066d8e91
8afab5e9affcbee1249b40391bd1de97a27095637bf3a2951e72c710787c05c7
934b8ba0d1adbc33f453dcfb9f469dd984387efcef06b03c2c4ce7e83485abf8
2db4365498a82081bce864196207c9478da3466167291ff7f36f93c9483fa624
df4d782afee2345a92cf1c0d77397ca6a0bed391049c630bf7867281b1debb5e
e05d31b46feaa752fda5fc43dffb22bf8be669e6e3aca3ad050e42f1984b0028
892d6bb277ab45d1a65c07bc4712f133c1194002ef6f1d6d9ff04564016e1e7b
f5ebfbda54c3ab58798eb1d436271546bc7ea9aea8e25b688489a0313b55c67c
0ee399769a6e6e6d444a819ff0ca564ae584760baba93eff766926b1effe0010
143d1dd302d05455f6e250e7b745ea2481ac5b780dfb6d8dff15d6cc72f2a144
64f72f1237410ae4bd54220de443b9266bef5eb6e2a058c418a9989754236e4e
dd3406409f33590aabf9bdfa7e55b6872f1d42ef96f1dec24072328072f54cec
2326ceea09f9313075eb61259c127d230e7f97641181624445f4138a9e9f4c51
91d21c69d7fa3cf605321f4c631e83b8db57270b3317c274bb473002ff38b8c6
e392cb3d3b4dae9aabf84d90d5c53fb465c119596f870fbd3e03dbde06736ee5
9b59554c61ed649e1d9de14fcd3281098156769825a6a17811ec644faab36214
b1e19b637dc7c677d8d80de7b62220b2c92299acfc99246d369c6fd0d04472f0
4ab67af94e60a67fc42462bd42d82530281c12d1ca7ccf1ecc8baaa832cfdb4f
bef7fe1a58535d2f940b8536ff6cf311d85a20288e83fb4fd3a7b4ab1bf2b69c
af1d568b78976782a6692ebedbe6449bff5afeeb07d3f8445cb5b2a2289ff79c
adf87e5e72e29fb1912db9aa2b5f72a86ce3cbe8484ff998cbd7d4ebdbb3c92f
cede5730a0155749a2a36ae72c7eb1813f8d124da00c2dc3c70fbf78fb8f7cb9
01c8d0efc53a616e898816f99d3d3965a9b03ac4d8f4b2f1f4ea64d167b4d7fd
3260a82398b8147c49d608295ff1a21e54a64aafb6b62c855eb4b2062f4ab6ce
c071dafa7928ec9107a5d9f0266ae00c9d11a85e77f318229c310d2733c7ef63
e5cddafda19dd75320436e0ace046a983bd356e0d9a9684ee2b503979841338b
e75eb656871bff48794c06f3c34cebc6238436229cd2c8ecebde7cdebebf0e0d
d81648a2066c0ed6830125333ab0ecf2eb2b87f2d9720061920338 1d7e9b069f

17e005dd7a902324e050ffa5014b31ce780d24ce92ef8969826772a05d34961c
1a8c9e2967f7a3a5dcc7115657a78caf9f0ab089634bf1f70253285e4b583416
62f55a2761a4c7acbb1001ac89b07216a511f941a08666ac4d55e092d599a861
7b3e71c2a0c0d725e13244e976a19a3661471ced667af58b22ad70671baea0fe
6a69cd7a2cb993994fccec7b7e99c5daa5ec8083ba887142cb0242031d7d4966
4c8e0459524380a9f00ffc58913f461c3e1d8737dd18252881f09e2d416e4f73
538594e61929ba9fd81f7ad21c083078ec86a5cc3fdc4be2207997de0c282d89
582ec7ab3f31b9d5ad45bc792e4097e6b4377cceabc7b626a548491b9ff8b406
2cb1404a9a348363296112fb70dbfb884da8a0bf931f5c7eca4660e1a7a2a3d3
dc7dfbdcbc85a53687aab5badf1ba72a3de0f4f408ee1d6a617e70f8a0366093
9c9951f90355f7b9ddb7355fa9c813c326bf4ae4cc895d1c9eb31de48cb36417
ae8bc3e3663e8c17eae7cea68b4c1eede0fff2866b2f23b239c8f967c1e92974
3dd14366762547c4aa2307489c6248dec4a57bec2231433b58cdf8c5e830785a
06f277d1d69550e345a08b34c034e257d5923b9d62a3cb00719aae96debd2332
02283ec4ecef511350c644689aadf37e5eaf1f4d0eac249e16baac0b1298ac8d
e147645b3216c02d1bdd6f99292cf6efbfe447430c3a3ec2d48cc99722cd4b4a
f972091af73ef029b1ea53c6dfad96dbe61c66fbd869b213644750ce9ffaf86b
22d41b74d2ec8028c4e7e7d60e59bbb209523a943ec50581a7b3ae4603c64fba
1866f3ce039a8fda70bc2f906bd3e9e8479be85d5430373fd085e9ebca073b1c
246cb6ba041aa51c07affe89237916b5fb49c60b5ca8835cb7730bac9f7bd999
e1134cbff0420854e6a84105f4dd5dea3b07ec77e120ba98df3bf1310afaff99
819a689239d1354c4cc4fadb398d42fee4a066af0235c7d2af997a4d1617e3d7
f9b4f7954f8d3b96b49b79ac3dd8e4489d23eab0cf8e6ee27cfdab1fa54e0233
dd56146ce07f793e09134f18e62968159ab26690a7742f12e52d808d3e2fc032
f5e7b8dddd4137ac008186a4c5e9cb644dc1bbddb61612c29c2087b1efe48974
afd21ef5712ffcbe4e338a5eb347f742d3c786f985ba003434568146adedb290
d2c46e066ff7802cecfcb7cf3bab16e63827c326b051dc61452b896a673a6e67
0784ed684da628c9bcfa402384bdd976583088b2c33e21194a4747863af80777
ecd7d7a27a2a043919a233bb91e3b009c05b7c81ff132a7c29228e1c45d2b6a6
47b99e50430e9abad7326d1837ecdda5f995112b0b12406d23df5ef603d52a4e
5a449782c6d286a5af7fd5cbab5d5d46dd4dd153cbc46e4aeae0ea54f2785980
48f662986a80c5c73a878b0f46cd7e3a548e556ad9c3f76c4eb867968b240eaf
dac2dc97d581f2cec688fe577096b60d9e525a807d239c1cc003ea9ef524bbd8
b56073581d6f2863688d779c800b2cc884a2e40e72c681b419bc3fa9c9814956
91fb5a6a40eef74971092a1c9c503d4bba5ed446fe4af843237590689f593c41
f37b1af1fede5f78b9fcb1f7ea3cbe030c7ee6604c65fdb37cc5d82a512122c2
32958285dab08e205b01e87a6b501ba11347786d09a9ac45f59fcb800d422a3f
17a1cec5b8ce358f8a0c43ac7a16292e2b455a79ba62aec1e24ac0a51427cf48
813f4d0dac6ee943f7583baaa1727a53927ec0fb11226663d04458181f4feb1d
50de9dfa7fda82584acafb9ef9ed816587316006865092a00c56b4b3177c2786
004936678c928e5945abc599e913e96f663fb81eef6e5d6970feac378181cccf
0ec8a952ab213091f04b02cc763ff13a3edb054dcdc33876c18e8b14b3570478
a7a642165c905652e45b473c59ad191624ba6726f092831bd21062fb4ae349ea

180925df10e301723d51700e3b62c28a323c6b25d1e62fd6ce3ee3a431b4401c
901284810daf81a6130eda3d35878acbf84af10324bedc4e1ea8059f15cb665b
9262613b8a407e538462aec5902d6e8d84ad9f1345e350be3ed45098fd9a8d1b
29a5b5cce3804e231654d7c3d2007590c59e8ff5633593d767cef09f16457fe8
05aacd2eb90c77fd747e32148b4cc34dc9b0c1ee061cc6fd972428569285d546
8a20bca39e9c61120ec2c2d5730e4945ec9c092fc2cd0c9e778937d3dfa0a6b5
52215e39337aefcdceb1000bdb40de70eb20e0148b01bdf80eaa47f8fa2ee7b0
57a162ef2bac41b885f8072e0b2a23ee481bbdeec870251e5e26d076f3a890ae
cf8c45fcafd11c10b4239dac1c4bac85b0e432b2912587b45c924acf9c9078ad
5e6199f7cf3ddc4f16bd57a3bd2f6e97616067b6c355e422db689c08022c32f7
c6c44689d2b3b671b8a61c410bfe56ef63b68f64ba00925d97f092d661c2da97
9544bb44a22d6b3d15429fd0658cc6acc1e9379f0dcd659f9847f15b1effa934
91d09b8deb1d6a7e545583c130f035b5d442f3c76ea9436bbd3f7227427eda9d
a168f0d23858657671ade1a151551dade4ee9d1f91e42fe40b614a456681d849
7150ed7a0b12a08183bfec3281b1f3b8d4f01577bc24811a03a9d6223d0e6d8a
808c43ddb13b876699a8d0914b100b4e4a52bc4f2f5a3db7f55939743257d239
a6f88de9a16a46e0d544594e6024a0cf93d67fc00e5750b7c144d963226777cc
6b3f41e7506591ba95f9a2bb62bb7c11112abebb3acb8efdfb71db3d86f528b1
0f66919cd7a98bbcdc8010d00e16c1883217e11739ecfc4a5a67f5741e9d2399
8151c4ebf2308d94df5f68121d1a507025bbfe9407d670c380a45adad587d9dc
6ebce511f734ef292f88889c599b391ecbf5992eabc76a4c429270e98af4b299
60b85eb25885b36cb8082259126c87e3bd48c2e1984ad1a70e2eeea6154c4da1
1a87713da4005f37c669d7a6d78417634b06352b1aba6d9237a8afaf22e6b09f
ca06db0d34fefb5c881fbd86ed30d1a4e3a8ba9c890551949eb748c1180a136e
6df82c49ba1f37d76a88e118d14c5ade2985df33c61203d0c41be100d686a0a2
e75bfa3a577483ea019ee51a2650c532fd6f234ccc12e93e9512d24a0b094272
c130b2c00964cbfc943c25fca131de6ba5885ff5d4d5c33ff1c3821cd0e7da8b
67211a50cf30a7304ed396a704e8ed8a0ddb68380d84a2cead2dd7a84bc49b92
d611e5fc28b7de9d560de544b14542ba667214d53d0969046872d9309f1d3325
1c5c4aff54a1ed64e92827063608e7d07302740a209e4461897a1772683a2a6e
d228c1186003ae37e6c9e26222782291fa97580a254e77f290b46c2376b712e4
be8ad3c1c5d51fb5d29815a1b589f821ccb079649e4921c5925393c5a71b4540
bff6270b7c6240c394515dc2505bb9f55d7b9df700be1777a8469143f78d0eb6
20209d23c45ffc377d09a53439af30f516ee833d78fb16f4eb9c74752c343fca
75c62fd62a7a71ab357c578ed8af5a9e8b6fbcd6706242192f6012b83758993a
4db52d468cede61e288f0fe0b1faaeb19b1e109299dee737b133c3a8a40f094e
6d77ec735345787c611367717c8e5eb70f24e0b6f4c25ed2073f1750caa79419
9c5186016229c89364544973423cc47b28c0c1ed47da267c54e5f1a80a76363e
d143ceb1a3e33d3eb56baa4b3a050ae9595ad4c4c65c7f804a5323e27924f903
fee91b1424ddd161cd089a71a86649c83284ec2eac793b3666ce31e524dd7412
3ab63085b9266b3c3a3f6160ad6322bf7fbd463c3e6eb368f0597a2d20ad6010
ba298f10531c462f507a1e1c8f9fd80a938531a637e0bada3fa8a068f7febd80
97d3eadbe9b85aeb07a0ad9fe11ff36fb34d60d4968917f9c8e3e89688e3c437

ce2c414abbe3eb98971ffb9653da8784ceb6ba29c20147001e9b2bcf8ab90f5e
fc99fcd3144d45c80a0acde670b201c2a1f0f0649806422e4344be66c61c5bc0
cc313e826027ee065bfc538881230bae7cac21b59313bcce637fa25784b8feaf
9b700a05d2abf489f830b6649e9f6ab0b570b3b1472b48f34ad122d90560bdbd
eb8407cfd7f94bebb6e354562a64c4024a05f200bd62d7546c8594f7b61387a8
dc9b11b602e4819a29b5cf1e4545da0ef097d1fe63e8a96b3aae5fd9542a30d0
e9879c927b43e65f7a9cab8c8f7aee73bfa9dd29db5920df7cfd05ad3ac3581d
49096cb1914b4e9cf0088d60185a48e0242f3b3e4c3a7aab2cfc25aa98270025
a013a3cf086847e1b1c36ff14d23e5d9b65627d4997b6b68381c6d6f729b85e6
a321a6679171831d0e8e0e0b4216893171bfdd113b7aa7ac975fa424c92873ce
375e903d8a81e9cd84c452884524f678b1d3bb9c828882860315415037fb861d
1a48342db5e148cb698753080788702e37b98d8d9439cfd050b4896a61db3b50
7baac6f22c24ce505c0b34855d073b4f9808b6f627559015c623a6fdec35bf21
51cb06da2422a76bc707333f5d09a4216014771b8f1f00c24c7194fd60acf4d1
ab57298c39d88cb1296f53509214872bfb810317238b77aa8e5d8820f32c28cf
95a9643bbedc2145c9c8b60e36796dc4ebfeecd1bad00edd07c8fc720894bc7b
f4fe3854a8d06be608e46d3a13ce13cbbaf078959a6973673139ad2b686e2577
c38f6542a2680afa1063a1c4ab2d4556a4d716ca4711d1565c02b3ba149fba2c
bd4e0a30d74f4537f29a6a603427489e1d3f7d6da030afc5c199fe6b1a4d271f
bb646023c9b9b910d8f6ba267d920ecf68e1d328be209770af284441f5799577
9c60ae5309f1f70035eea7446365d8ee678aad77ec47403ea1fb2471a606e28d
42fd86674abbc793aa1baeae6bc67d6d565dd95f730e8ed7b4311603a9381c81
d408c3394cd27d60a14aea5c008a88e83ba4f98a88e6ceda91476ef8385e02c2
ccf111b2116d7897365d716db2b3d63d8164fd3c236b747f5026b64b4f4cfd94
c254e35f28045b68249b57b5d09942fee823a3e459d7f47b0ccb1b3b3b9f419f
cceef110cce627efc934e35638a0b2bc0aa7a8d3effa6bd2744d0e7be4ba9749
61fec7d90f2313f1a0fe12453c0b41481ea6d327b5275b144d1938ba296a914d
ef97cb5e25f77ea34878cf6e9161d6065a14f0bacf28a815e3231da479838586
e4a91f80d9a84e6efa7fe6664075c04f1953dec5fc4177a4e8187e4d01888148
dfa54dc6c171740352006b7125219b1fd9cd1403be4a3440c1ad1acb1b42d37e
bc3ff3fb73736649a9aad6ccb811819a912c03aaa9ec81c6fa733f1459e66af9
bbea096ceb3c94454a5b92e5f614f107bd98df0b9d2f7022574256d0614f35c8
f87d8b4376bdb341964801a836bb7ae4843351ded70801d401e951cbbe05d613
e16df177681e356ab8a9491e841fa1a757bc40069e2f42493b9238f0584cb9f1
5dcb736bf556729b30654fe97da034c1ccd7471f7587cb82dc33f4aef2248b9c
453c6fe9e176af08b176430630a4eec6f1de09f7f147248dc905dc9823af1b91
b67d764c981a298fa2bb14ca7faffc68ec30ad34380ad8a92911b2350104e748
3c7eb76db2a503d495d1332dc50acbcf511d56a6ff5a7f1a5f9c16c5efc10b5d
10e2e486cf8ac63c12c9b50bd2e5222bc8e05b5a4d43ae2dc17dcc9ca81a78d0
78175b44c1cbedb79c179c33c3def3ea140b209f15dde8fa3f8c45004394a76e
56ec7c81e26fbbab76fa82cce7b9efc16722bb0ff918cde091559b2d2dd7ee2c
f23142e54092231ccc04960598d8d17f3a79a5bf0719a9a0cb73c588afae3808
4a9224b07d715556e1089fcaed3166b66269217780d6cdca74507f1b956b6b36

40945842f4cb5844b7b8aba26d30c7ed5b95f483b6df66ec4bb6e10f37092303
bc91b92518ba7222a26f7df7cb2c79c89c7f3fa6476dfc4dae6863e09c67d75a
90c51f81c853a6433fbb400d17e64affc7cb3e7e79d0f7cd1ff3906c286dd30f
088b89e6cc86ef074a3edacc6d47096137e88a6d8d69669e637f33abcc9d0a8c
486c073aec65fc0d8db15e0695f1a88a0c852768884d6762b71feeb583222ab0
4fb7d5887a8305738abf81fd51d585cc0ab3816e7a54da57591797bbefab7509
ac9d6c79646a6603072e17e8514e70e416cff60abccc0ca45b61b8b8a69f6d20
a86e18190270888e9b8703a05c08588ab7fa841fea08ee667accc331c92e642f
03a7db447d1aee326293ab9e122573a37aa73e7de1464a821eb462657e9a5924
a84e601a20980bd8605eb1fce0f4f14b9d5408a9bfa2465bcff31ae254e44c1a
c0e35d03b416060062a28c3c671378fb41f9ba9bb5b2805a9b452f001d07e043
06158ea9684f86faee3e0d09810f78f1c9be304f92a9d13cf908995dec12741c
f847f12ac1196ea30fd0e9bba5e270853f10db21221a4e463a3050b1bdac653c
6a7ab6636f0fac6c917dbe8107615d5078b39b74a39f5139d41499d9cb1d46c2
3f3ce0a46fa764a24a196b8bc2e5df05824f15b7a9450acbd6f380aa6c5212da
efd31813e98ef1e2b9598b5026870272477ea8291235353e7fb58bc8534b72d6
1b36599fe98c0fa9a417d4c8527eb3b2a6b83c39e79096c3ba7cca258e986f94
70f9cb076e00542cb7e762f34df5ca50b1166bb6cf7d5c4b25a71450e5e5a025
3f7e8f181a6d5bc4888135aed6bf14817cbf9fe28984ace484943069c051909c
86f6bdf40e132a9788415f6bda100f20fdaa07638c0ddc80ded99c59e8f0fd83
05a1efc7bbe2d533e945e3facb2ba308c48964fe68f6058b1cc87854cb0ace7b
f2627e172eb2a55138a4ce8c849dab3ac9991af7382c74b22308e1fe7c9f6b97
338920c50a0fbccf537f07c78eaaa0a8665b96131bedc107a74be6124a06d370
cfec185523d81d275f3523f08a5f10ef5c6b8a6f7fdd97acbcbbb15c2e23110e
2fdf600893705a96d83407832de49aeb18ebab51876cfe450d8680ce80b0b303
a68219383dd7e7dfd4142adac8573f89a5f6efe2feeb83c871d45c989376b8a0
7cbc5b2a6f2a3523a49ad13fa49ab08b521bd99a3f1e887daee4bfdcda622baf
d7a86b8d6eea87143053609050e48b0bdfee1069efc30a05e57122c1909dc33b
28f457b4582701907d1cdaabbd9fdbea169185dc3e97925fd48589ef44e72812
7a865f17ce37cc71427deaf200f4e632b51ea202db8c5099ec2f9ca6ac1b647f
a74d8d6ecf4f1fd66fcc83fd76125296ea9cdffbfbacd10b04fba4dbfe9aa2f2
82a82c5e89825d8c84216d579c9dde9e42a125a8394de60f682e4c2474498ba8
2042b4c5ee7ebb4253d59dc084742f2d2c3c102aa9983333e0785de4d689e6fc
09f7d02a3c2382199458c98a62b045145ee54ab6aba86166aecf3d10c3c1444c
26a4d9bd2961d724ef07aaec5cbbd120891c600ab7932e5e4ddef38aa3ee9700
4dfe62c4d3401b386b693509bcccfc0b91c72bc8365fdc68df9f7c050e35409c
5a425372fac8e62d4b5d5be8054967eabe1e41894bcb8c10e431dd2e06203ca0
926d3f258fe2278bd1d220fafb33f246f9db9014204337f05a25d072bb644b6d
b85536589c79648a10868b58075d7896ec09bbde43f9c4bad95ed82a200652bc
ec85e270c5cb159255a3178117197d275a6a90295fd31248b397dc03bcc4f3e4
47bed59051a727911b050c2922874ae817e05860e4eee83b323f9feab710bf5c
0196bc9ac3db6f02cfa97323c8fce6cc7318b8f8fadb3e73bdf7971b3c541964
553502bfe265a7e75a1d2202776fd816cabccfcdb200cc180dc507f4d45668d2

23577ceb59f606ae17d9bdabaccefcb53dc2bac19619ce8a2d3d18ecb84bcacd
bdb184f4c8416c271ad2490c1165ee4d6e2efcf82a1834ba828393c74e190705
2ad362e25989b0b1911310345da90473df9053190737c456494b0c26613c8d1f
a9d9d7f6dd297af2bb3165ad0bfe3bbb88969393a3534bd33ef9aad062aefd05
0ade4e834f34ed7693ebbe0354c668a6cb9821de581beaf1f3faae08150bd60d
a25e5c9206952632a52e92caeb43fd8994af96aa39e99b0753f1023d80720f5a
84aa777badab889d066e3a57c6a3d2096bc978c01499ea3dd8dd65fe44a3c98f
2f9d44ea900adc43863608810f77b53d4fea7a3ad6d06dc7be81d837271b309f
6c36554956617d2996a89a0ff7f867ee9b70769e4f1b70943fbf2babb8d97bfd
7a9436c496079a8ba2ad3bda32c34085182dcd45e0d23f75b0cb218865ae1c53
1f8518dc6ff3544f02317f8c12ea8615dfbb74e13e48a2852bda317db34e701e
aa1f12737595860819e912a245cb971f794e60260d710593c1df98a3e5bcce2f
b63f375f43a852f24f55ef3000b5a9bc3563cc5f00abcf4bea12e033348ec93b
6608389f584ef9dcc1ac9044965cc85400cd2f16ecff5116bb88f6320fcc6748
386ed7ba502e7bf0e60c546476c1c762cbc951eb2a2ba1f5b505be08d60310ef
69f998bd67a5dbfd79bcc44f0cf2284ed61fac9bfaba3d3b4dfb19a57baa29c5
ff4c5f6a1a5b68b956970751d56ee7905ec48ad39cc05416ee8ee958ecd0c40e
b080305e5124688eb4cb9cd914eea83e5ef70dd8e0a85f41d21f7a3fa8720936
5bc32ad6ca2b8c6107c45715d61521acc0abca6f5da135161ef374f68ea3dcbd
bce7888704887f2a8b3f658f24852af3dcc41bf83a47c3e66fe6b123b20df930
803b976d53cbb7ce9f19709f240e7a19abe82f13823d8e3ae3b44c660a957d6f
c8dce10228ce82fafb1338b61384b44f377366367ca2704a74bd30f8f2b35ca0
ad3b604a0e190419d5934f3b74ffbbe799cb837a2d055c5d62097a945684df4f
071c2ac354452d484a37e7af15dd4685061dd4af93abad4308f41df673132ff0
8f7178ed8265cc0d9f7e7402d4d632c1f5e32c3501add571504bf2cd0065460d
b80635fed8c7fce92385ddb66fb6f58337a8a150c4a1d158888adaa8db0cfebc
9072e1af4382183be07719286f8017f6eddd9460b2e6f8a47fb042ec17aeb569
d3ab7bb031c5d6bb2e0b7105580cc9e965f98ed766f6c3036aba6603697c18d9
ebeeb6b28c9d4589601a0ed5fd4801c8fe2db0717a6f05b170766e816d8003c5
0711d640eaa4b1b176134a741622f90618380509f27cd60d06bada4bbd781c3e
a8064e327b0c3e6085c464db2a47edb16b89ca2cc1af1507a95e1adcb5228434
3cd83c4798816ebf208eb2a57cf09bf224ec57e5e35bd70d49885d61a242f39b
3e3f7b53d719f3d2397817cb7b93ecb288f84e0e7aa11d190d4a8dd5416025e1
bf34be94275f5b05d82b3805bccb30f217020d88f501d156324f98b5eda9ba7e
3C17F3D21FDDF3A1A902247D48BFBE291C2267FE7F7CE9DE364AE7DFF81C2EAF
03911D1A1AA0B3A2632C25D647FE8FB98E71F3F533AB49B437B90F48AF016CE0
8142d4e6908d773d8241fcb54f04ff033b1ca67f8e474ef09ce2ce22b85474fe
7ef0043c19e126203afbe14a3b15657e63ec15ec18c92aa9dd346199aa9a9f1e
0e6341a1a8530196b8b4d9bb0a3d8a42cba663ab6684204423ff84cf3e2df5a3
e533575676bc71ea17cb951cb3a7fd7cbe510c346cbce74685dd37595512c9cf
fa72b66dc74ff7e3f8531bf835c2d61d298410fdcb0eadbf874068b9bc05c2b1
26efeda05a25a72a8bb9abf0a334ff5724f3f9921c7444b1ce50c92f8776d4f0
2650d426bc3565559f05c6bdbe48e87f764d1862b82913140f3c95adbd40d9ea

5c2cb4405d9def8e24ba05819ab1ccefbf56046e0bdee162749e258b15efd966
f52e06b7a163f07b48f32e5f4420dc488f5a0452abcbed5fbf259af37c7989f1
852b7f7e4dd82c9b6a57b66f52c3839fa590e3979a53a37642acb57975cabc0b
f1d9abcc7a9aa4b5982eee5101fe702ecfcb05f03192d0591822b712cd4aaa5a
805d356745cb242419de83f20f5c2e15864a078bed4d9ddc781b5c749914c7f8
c2064e96a39d269820e50ff0df63aa4791141bc1a6d145846694e8cd11e715cf
07239cd6b23b16164251ca229d4f9ce15248d45a13642ada6aa5936ccd0228f3
d1b45a3651bfa2af1186894fc579784a5b92997d8124a1bbde8725fe259f19bf
70228e18bdd79a8dca8d5d518cf50c29ee6e8286e1a2fb67a41cf18f6eda49e9
dc77b6a04697f82002d0e29a8c3cbdc676aa2d6c6d1123ac04401173aad1cf2d
096bca0c665b5eb0075112b18729efb85c67597a8699e79427b1fa2961c6e700
fd17b3af93efc13a7801fe1eaf94ad35791a06cb84d773376474ced60657f482
b7b22712d01821d03a6f5631a126b4caf52d4bc1c7c95a83702f95b1f75227ec
7761193ab931db800772708912b9455e687b6df8112a674fac4fba45c3e8ee3b
97f931ad60edbe7599838cae8bcb219b56be3260896af62210407d88f870f340
98cdd9e8efc6859c717407a8f765f5cf780b16aecb93d2b791b27a13db9d3a1f
b9bac4e6bda22e8d65011aee0205f92bdc92d2c8f2db6de08cc50daafaf3890d
42d5f609c0143ec808b45b247f2cbf8decce5bee0572a30c2437ecb6bf8b37b4
2e6ac815d4c2aa909d48f6cfdaa00c0c64b27e7e545c38674d82351c27a1e6d7
1db8c4a926b414e6fe1f87793f602e3e899c677ed5aba7dc66bb403bd2c704bd
e9549a3eef49c56a00ac3bce5efcfeb4e97e3db47395c69f9156470a558d484b
83ec2f75a8209636e68dba62c46d6a818fe5da8a4edb50c2703dac9b04dba897
4c5a58925d5138d9228c598690e5d082afd0929786808810ae5a60bca915356c
b8173915d86ac9712895f10b9be95b5987fe49c5d0971e34c4405bd40e8cdb32
97ec77e95b984282d925275b2da7a355887926727fe05834cb67f4085a538d8c
81c0ddfe0e7cba1c5bdd875fe3a8c44fe3b07e6f1c743daf4860db96419b3cc2
dddc8b703f69d0fb7323e1cf0ef64b1e8468551e9110a3ec1c8efcb7514ada57
63275154c99227e3ae277590636accaaca7efcc0f8a7838312d66d4c30685c22
643f9cf9f9d05f2585236f93946038a628d6f02d96cc44310d55e717354aa2b4
17b98bd8212b1aeb803255986862db90777c7339f8016f92e80e4a593ee8b77b
bfe5aa095b074b3a62443566be27056549b63a461f11e9d1563e994fc645bca9
986854540603b2a47d4498f9f384827f8452cd738b4abd4c4e6222ea541df177
9556f9f6ba102b92d7c63f128251777a35c8d286bfd6ec49a96730a74dc3d921
b75b227458b2cd9c68321fe42f9d1a50898b7805150240e51a6b247f7222b19b
9cccd499953a753ef1cc064bd0be4178a2c027c58319d95da43e9f298e1c1929
cb89c7f28bc19040b5d01a774c1d35152e232bcc979ea5326c13d3aedd6fa23f
546ce68250c10c9173c896576519d199c642bdb3237b6289608fe61afa1939c3
60b2526b2dbe7c5b0d7b9f43d3dabf52042b5c6567fa042c7e4cc2cddc154faf
c331e243a557258aa8f6d3f248bb2c12df855ef664512bfec9468c549e5dba5d
1d0914df98b13d3f7fbdcb493b2dfa624c80d511f6029171097187868d732d3c
ff8bfd57726d6138f4e15ee87a4f2670745f52d57b23252bb41f7dbf97c7e9b7
ef36cfbc2a273884035357390ad1092351dca6e4a3b773459bb3807d09c30a3f
159f66960010b415cd7105984a2d6b4d40f83d4add4ca84428640f32d2b76efe

ea75a5fdb8837f17d63e468134396d10dce6c3160166d1f007d83705e8a03242
01fae9dc21c49e23417af27843165b5b1d9dde9d0dcd6ab524a34a552e923f21
1ecdf49da74cd502fe10fc145eadcc1a72987dffae187f06507c797380949d78
c8ae3bc242d003787798705b4fe3641417760259ecb7495323338d30adff34e1
fcf3cef74615da287365c2daf79f41bd063dc80d79fe321463e62aaab4acbdc5
7927fb4016f3e4bb4118e3eb0e58593b9642e5b709d7ce2936c719c4fe2f9a69
d97ee2b4edb9e1af5e054fd880c13401a17d68886cf9edf99c7eb5efc1fcd5c8
a41205eea1fe9ecb2061439518e54f76c28bb24a74f899f15b408f17f28ed491
5f5ff374738b97ab0b644e803d4125e28de8c08d43276769a4262948db52ac91
ed5d951ab1dc4aac6e675d5b54fd52b8f3078040b145954cd84aa1903b3ce36c
ba8a8105e2b4438d41315e57f19c73fc1c9cb3920d94175d136b39dc813b4f45
89b7defaf72e59480ddf76d6f5a8e9f3ba2ef4664da763c9fb8314ee88b9619c
be9664c7ebe6bbd0e45778033e6f5df07801b4a553857900a3dc98ce6a6516d1
ffd73874741bbf82c6cf26fc57002b4672bb3c9a625fca30d1a4f31180d86475
e0589e289673eced96cbb06e5985170778c84de5f092cf2fc50921990f67342d
1c608103de01265eec33f4a22e9f7dd51f1679b7527f7c2af40510d24b3963d0
f530b0ffed4dbbb83184970dc889a56dc374057699b3861795d93c4234f9338b
62de46db67941d90148a69f999dc79e0f2dece1f5aa4996566b021e43bf2e7ed
c160ee1a5ece22d04bc1368d2d36b4c143e0e33083da5cb0bdf56d872255cc9b
a8573c8e62c67a1783c0f65833b9b455cb96ce62b7bba7101554545e5a8cb9ee
2f01012c5751c45ecdf0804445d16a9112a8485c755c1c00e018943dfd0f19ee
5bbcd8a7856e037418c0ac1c0c987476e3210f577beffcdfe2eceebc19c5644d
8babf68a96861c8495580b5ecf54d8e9e1c76fc89fb72a322c94e74796db4e19
1f97ae393d45549054d2e8b6ec9e25acbd8ce727b2c1c5f01022c48c9b997af2
2908ad45670f6e7acafe0fdba1e400ea91deda96cd585c0ae4d923f0c9dc5c91
d78a6c2015b9a4a71cc2645bc904345c2bae5b78c65dafc4f430657f5243f820
8cfb47cd446329cb69d1adde062231b903fc0700f54ba48e721b7081df3f0578
e344ae25471c31f0c3533b69561314e56a12b9c96cf632f17d21126ba5c5521b
659f1dd67213c636d1c2afaef812e6661a3c44ad9c7a55b35bd8ec451cf0320c
31a852e7e9bd7de6e1dfa32d39cbeb820c5dd02fbd2421e3295caa77aba3869d
c42c878090519025c700849e3d599ec8a55689d8a337047a9698181fa8f4da4d
23bf51e4e0392c53b8df049a02dbe4b1fbc93af589f2ddae9cad230760c313dc
60aa9cda7df540b7a6e5d4d78469c929f41d462f8d4bfe3955018d93090acb9a
ef123aa59d1449178a0f7d713cb8fe239457750aff45a8b934fcfa560dc2e37a
7daac29c23ead8866f1f16a425ffae3bbfd157aef3ac013ca2f8c371704c74e5
21eed752e7ea7610d9b0354adb037833c4ab34b9b36a9cea7c9c8b6089edc02d
17e78f63f7c69dba83202e04d4733d2b76a96005547f5e24007e6979110fba41
e61aefcdeb1e5bd3855279e5e5fd676d3fdb78d1f9d6963694508e521115ea1d
2C8E8F6B205E0583CC8B66533AA15143ED580509097BC857DEFB1ECB6EECDBAE
2d6e9bdcfb534edb88ce4ea1947770dc08afe42796d7e928b53df561ee1d671e
f261a7107c752cb5051c5908e9725113c1328b627388e8102f7d62731890bfe9
8273c669505a9349528222b797151c6b2cd0db576f42075f02be1670f09af44f
a1b911629007d7b1d3e9bc227db8bab926246b0e51c10a4a9f8bab143b54adde

b92890e6da84c381330319c80ec0112cba70f50ce7f9748f8a438f2c99225cd0
6078b55381e39779f915032533a93d725bab98982b303998fa8ba2ecfc675737
20da161f0174d2867d2a296d4e2a8ebd2f0c513165de6f2a6f455abcecf78f2a
258376acf84d01e1def55c6ca303d920c80e7184b1a2d9cbbb21730ada198190
965b90d435c1676fa78cdce1eee2ec70e3194c0e4f0d993bc36bfd9f77697969
08c541896f505ba87ab3a148fbf1413f51e3b9c380b5ecf4396259974777f7a0
b29691ac40b8bbb12b13e84641ad20583d1387ca356850aa7b5e76b0f6c76806
876939aa0aa157aa2581b74ddfc4cf03893cede542ade22a2d9ac70e2fef1656
7de78f7c806f828ef071a103b7be87636414635e008ea2463bf33077a466140a
2ebcad09b11759bb64968ea3d0d73f7e6c89e21054388d80d6af9514a5d52789
4710d1b4feab4e2a66bb0f19f9a0b274a74ddaca72e684bf7ef8b8b9bb05e8a8
1bdae8e9de00a8deb386f195a087f56b8b66e5c9d2b59105b6a1a3da22eb0858
567b82c892f10a5cc6d0286c5777e7462cec7182eba81db7dd7de53d1e8d3274
c9cdd5a5b0701a4d311e0264f5bcec49fa500dde81ff8dbaa081be032b0c0446
a22f6dc3eb0001c2be76d261721a1c1f419e15f6b5bfff95c5b8a5f633ce1956
1bf6dc9af6dd730120f598d02f139f5a7776993afe29679f83a3d2fda3599736
93f2358f631d4bf5a1f16b40c5bb9479dbda492d6e96c2fd9760854d219faab1
e7dbf1eacfbd73576b0e410099898e4c7e2d51d76fe3095314dee1b54860bf4f
a5e6752aa1b9689201a98c92f8077b8f483435f0d8d38da1dfe74bb12b47dc74
9a8ad801d1b9c97eb38ed7b829968fce71723ccf4b1087b283863996efbb6e89
24c1b3bf391fa6f55fffa6dca01eae3e7c5bd0eb583d8ad16cff3d92cbd0687e
cdf920e271b6c8e638eb26a2f0e4b213035d3994249b60ffb093bca87ad4149e
4ec74ac2463b96b2948e7d6eaea7a17e3335dc973d656a152381192e947aab3c
ce8aa33c042ed777ab66721d9d387aefdfe7dd918f5100db67134acdc835952d
5c1f7c4ebf49ebcc1e07309d90049ffcc47a83318ae041330e777ad9a3befc52
97329752b4a2f48fed6e10ec54492c31413fe7148bfe6152bffe49ab4a9c7246
0638cdef52fd46ad9f6d9064be686e6aecf48b0ea26db6eb28c2954a510479c7
86390160b1e83c37a1707cce4c854e743254e1d32028a44010285ab379fa633e
b51f05bc7a55494b0d24a8e81a906d2704b90673fb37f8e26029ed27aebea415
4ed6ed9736c0213e175761a058716a9c700b83a48a8ce58e144b7efb1c8f7a4e
d6a027b99eb946ae215cf495ba124e9f97bc58e857844e9d406bc1bb9d4f5dac
815055f537d912c1e51989b818824dbb9dd21296b5ac3bfb9bde81b16657f5bb
9c439d584e7298863640ec32adc171bac98f2f239163c31755a8c919a8d433d9
bd1746091ff430fbb749fc11ae3374b45375303840379f98b2576ad5bfc94104
8a57ff67453ba40ebfeaba564c95f855b307f2f322c02d04de569ade58ffd0b0
b6615097e0d7428028d98b5fc7fe63474fe10b3ef5a2cfeafbc71315e280ccf8
1cb8ca75dbc6c42d9f76281c7cc73333a146832f444f69c0ebf47ccb9bfdd010
f6b04fa9a85ec6d7a02ae072cdc6fd30e485c6154ea242588c152b17f9aea058
4d2ea7e21dc01b1f09eb9a407f375a118b2ffd4b42300ec601832a30eb0d089c
3e894a4dde25f7967004664ac7a01077c8ffa8eb8c5e19470391441739249fb4
4be5eabe47a3d5ed1fb9c7ed8f3374f5ddb58247598d1a71d4131549e6faeca8
887c3b26bdf3bdbbb4281dced992bc7ba8632efb7526835ff1b5b21f6d6bb3aa
49608d42dd02db2c7b94268cdeea587c07b7586608f12ca1fe2b45ff94ebf12a

5f688cf7b9b960d15f208ebd6af7614f2b7793cdb7f5766074f525d8ed007278
a88967fdec2b2d21a766be305df9daf8c0d719f5de191b6cae659aa258ed1714
375be6a07745d99002bf6923c71036e9814e48835f08c1dec81785694bcbca1b
76e2ad3fdaf9b3cf089e3f3743fde96bbcab215ab44579c06f644eeb7e361ba0
ed5a60a0e3db1545bdf8e5418a62c4c0a7d8802728e7c2e48590831e727c0bb9
839569f031a2cb6e9ae1dc797b1bd7cce53d3528c8b5fbec21cecb0de3f5ac88
ca21481a6d7c16ad87efaf83604da8e9b51ff783d8f123cdb8aa3a17bfbb5d23
3df271bc8eead20c1c9ca59f5ff5ff69221dbff9945e2f2c5b8430a801513064
4071f8d9b084209a30c58608d7f07e05855955de74b49ae57f17cda53ecb3ce6
0ccb062ea14e7a7c622f988553d2a81a43e6e572d6744f1bfa4fa917b27ec735
89aec94464cfe94778e236733c0c2b91c9de79490e8ce40a26b212f5f169f079
7f470cedb72ebb46fc952f0d75be621bdfda4bb9614850ee14816bc5193bb8fd
534442b1b0f319d0aca34644378535bbb8ff16dcc0060e33e36907d4a649c354
f5950107efd6ea23bff4a17c0855cde5dc80f59b337b43cbe92801e24039d5d4
6844afd2266ffd25e6647c2306d0e75e81798c128cdf215107964993243975a0
4f163bbdb90fa72e8fb87aee7e2853754977abc1a3118170ebd63a7058aaf113
a6f8b4b528d67fe5b985ad0a394e46f5c116bb80b7cb8ca9a094d92f4dc614c1
6509788606fd69882b1c470dc0d3ee5579cc7074c68971ddeae3af5ea63b5f36
3711819b67d8bef318aaaa6a364288f919b1f08e15ae0e72add627da2b44825f
d037bc88a0823efdd1aeb930f8e61f88107281363df386cf7dc04d1c55664293
4a0728a48c393a480dc328c0e972d57c5493ee5619699e9c21ff7e800948c8e8
4c0b74954692a7dba196bcc0b4ddf761440541187d2e0bd79ecfec8fcf67f406
e71fc2a8fabff0161d82731979c4dd4c2d8c1c698161c2354374c7402eef7fea
66446ae2392316b7278007490a9e5ca81efbd949419fb175ffb22fcd1b5ea4cc
1fdb547e39569d1e4db162f2739138e471eb43c936636cfd698a37cdd8803832
464260a1d72bc3ce079353ddec92e05339253ab577956f3736d94b917bcda91e
84b3c94d98ff57d10f265f2c1a4f5b5923c5746e5e18b7b505348cf6d01b390d
43e973e87611c27c40b131a880a1718ce9c689dabc82c102aa918e1b920eea89
84fb5d99db36d869cf03b6b3c559fa976d0ea17e112e91596ddc0b0079a6b2e0
523b6dc8b48f56860e338718e9e202804d516e09b0d7b59d07276a1abe0eca7e
eaac9ce3a76ac2324c3e217ab3d5ec0025ccfc35aa804380bb2c2800505730e7
c0398f10fda0501073d3d87cf413f7c185fd65badd1210d27e5b1f25a105b0da
2f0ed2224fc36162f89147e5303a9bd5dfdd9a3c39d64035cef0840a4926b0a3
fff6108603e65fc999432695744f404e77eb86d783b62a80ee73317c46e4d432
0597dc8096146ebe49f7ca4bbc275856dd08ad2b69351095a94321901e6ae9dc
2ad32f3d0310d51ab22356bd7c994c57bcdaff5b9b6c043b137f84316916b0d4
869a9bf4a98221be8111d3185880eb2f8f859a418d7485fb60147552fb657b92
45a7b08f35b4eb9e553073819cbe6822a02ebd90c8861bc9ee3607d535726ebd
191be51494ba626d039470f78dc140b41c3d81ff71dd069ef118b5a8c76b0714
156dad889b4b84ed06106d3a6e76162927358f15e6115cd98601cab6f478e3bb
69a3c67c646cfc968eb4de63da40087b8a65c23bd348ceb164a641c84936cd8d
bc375b25eee594650541f178dea9f53c10e50bd88e64a3d508ae397b9d92b4e6
a8f286d1a7db81b3b11893f34b578e3659580fe77939d2c111aa238dea06ff04

92b6b2701a668204ae9b0dadcd6091c4917ccc9cb73955f50dea685db5834c8b
52d8aeed7f179a9936766ecca2ad9863eb25ac744c5740a047de1192caccca11
c90982564b22fbbd5ea9e4ec3fa30cee825bb2a5705ee5605345f3df6ba55bff
6c1c1bf1489a031dedc17861567e2c6fc2cab497d0dfa964ba3557b0f6add58b
1cb726eab6f36af73e6b0ed97223d8f063f8209d2c25bed39f010b4043b2b8a1
2aa160726037e80384672e89968ab4d2bd3b7f5ca3dfa1b9c1ecc4d1647a63f0
3cbb07af5c85a539ba970bd831de6ad53473afe6d99b3cdbb963711e2b1ee9c3
856f656d41dae458a3c2a78dfa48537028b5f1e2101992dbc87bb5fe42feb821
fde8b0e2ce949e09070d6788194f63131070afab0ebd479bedd545091e7cc8aa
6c9c6966ce269bbcab164aca3c3f0231af1f7b26a18e5abc927b2ccdd9499368
d4b36731cb37ad05b0b9678b568c10a56f2e84967b393b626afb19d2df41c9b9
b31d0161e87bf4f0f4d9251995a064df5bcdec48c3396ba856796560ade9af87
4546bf50e116c0cc49d206b2be2815f2724944ba7aa0b305837f90dbddd863c7
bac64033bd2acfd0a87444325b1a09ddd03a871135bcd9be108adc38ef35201b
953be93ce8fd78d09ecb6e2e72dd07a3ba25e9fc876def541a4cc1d323ce3c9d
2de20700d943981ad1bdb2f6b4d03b7c65633c1a7e1bc504ba20ec5f417eb69b
9e305566f7d342adc8eaf30471aa3eb95c049acffc742ae23a5830a44f96e51d
384105ffee918b362ed92133d3f1ec5617e20a0a2148508a5370f883eff3ef89
6257ab26547f390bfd67d60766a708a95998452eb487d6d7208a52dc3e9840e0
b9446d663f2aef34efdb579ae02e62923b5c3bc02b9d0fe537f5974ae439a422
2714b12d0c65cb6fe783571a2d103866c4059f40b2905f58a6cd5de80eefeb73
70e2236e467d2b453e6c412d32d0bd0ab256603e50339b644d064de18dbcb539
5bc838b11eadb3fec80a7e6bb46183b868096d8c2e499bedd9c976f3d70d41b1
cb136924562c2e70a5e3039ea3cd6713f4bd980df2795f6cdbc67d3364b5e79b
709d548a42500b15db4b171711a31a2ab227f508f60d4cde670b2b9081ce56af
8C6AFF2224FDD54615EF99D32A6134C961B6D7D576B6FF94F6B228EB8AF855AF
92E9CEEDF28C99F90F8892AEC9D2FA413FF0F4F17C5B0316D05871E95993C3FA
8b11db3a20f447b31cfc6a6af626c037b8f77ed0f96f7210f9d58a21f83e6eda
38A5E825577B51EEFE4C571D29B34713B4FD2A2B09A013DF4803110D5CE553E8
7B722C66602E53D173163537FA66056A78E3043BFDDDCB6FC06F31F1F7F25ED8
27AF16554281F3DD773E76768F13B099B41624BEC5AB0405A09C26595A49E80E
7EAD6660510AA9A7E58094F05A8655DF23FE680B57D51141E6E6D124C9A678D1
f889d2358eec85212659b0d273e5e892e610e114c990bfde93c9d607d85f58b0
c2e4f6d9c6afd91e6f85d2bc96c6096346bbcbadd6e1ba7192a9b226b17e67d8
1a2cf862d210f6d0b85fbf71974f3e1fbe1d637e2ef81f511ea64b55ed2423c7
B0279CC1FDE7B18C0632585EA0BB48C3F3140D0A4FF4CCB3B35EAEE27C12751D
87E5AB38B3E2BB5F63FD40D97A225F9DEDB724B07038521EE4766A233F718CA2
A866800A90A404FEB4A96813C487BFD7114A5EC521516EBA8C0178FB3F08F74A
1d09e91d72c86216f559760da0f07acdc0cff8c0649c6e1782db1f20dcc7e48f
36c9022b8d2260b360dc9390c146636a97aa984cdf5176036cd4e444840216f8
029feed08a935ba7ec5186c3ea8ae7114910ba95011395f9a097bf2b069da342
234defc7e28089ce81141907ceb16f3c80b12b6c19a4516d97f049ec66af633d
9d7edfa9834f4c5b5b35c04c7906993c330fc0a29382a69f9601793211ccf253

DD0762FC58ACB30F75B0A2A14DBEF2CCDA553EA9DDE08A180C60CD4113E1A506
C4A75A64F19BD594B4BB283452D0A98B6E6E86566E24D820BFB7B403E72F84E2
FB761A2DA4841F8739D33A682C5F2F39A033C7BA16430CE5785F7D51AB5D1537
A8D8A56CDA7E29DD64CF28B2BDAD19E8DCBF78E5900CF9CA53F952E9FD2452EB
0A6D33BDC0B70A45626211393D67566E1C9EBFFF020F7FF1EF23DC93EDE0C27A
26ca6af15ff8273733a6a386a482357256ac4373a8641e486fb646bc9c525afa
43d469f38545b63389712eba636e87ad483308eb6ce609c1117a2fdddcefe1a2
1e36dc2d6ca94e14dc7acc7c183d1cca3e05d6f01813c9a1918ef99f9caae693
e4d1f8ff1282ac60adc0134aec2420aa652250ac8ddafe866e56d2fab165a132
4b5d179531cb4baf74b8e45102c89ffe3a237bf75e80498c7982576b6557c897
1dea5c3fd77956115521e97309e5c07e220229acb142c920db996a85c018ca0e
cc8e42372ef2df10f26bc075cf3b3ca73cad573bb0eb3dfa67991e79df9d5ccd
d2cc95b72c3e72b3888e9fa35f6fe0563f9dbbd08b76d0c3546065ceca3c5961
bfc20b00bb5b9223db2b631061d6a5d8ba989fc5572323737a7019b9013eb89c
87bc6a307aa0a8e1a62a4bd90487653a8ce3a79239edc763875adc1b5ec60121
d768aa4af126995bea32bc5cee3cad6341fc9495b47b5e20f26caa19addcacc6
cd0c624ff748d78e41c851356fbc9cc6945b426f65f64df08c7648eecc88c481
8bd2a1aa58cd9fb15ce499be7131e810abbdcc7770806ebfbd83b8e8f701c5e4
fc3dd043b795a1cedb8b7e1e5471f15c0b5c17c237f634c60c4e0a92d980914b
c8f27a014db8fa34fed08f6d7d50b728a8d49084dc20becdb23fff2851bae9cb
230705996b567af8b2ed884e6c06cf2cf49a2cf5b4166a01c30d81de857627af
fb083468d19aa0ac7948c63e771890743575df1089691262fdc7963748b348a2
be860e8882e334cd01f628e00d4e0379e7ee15468517737d3b1c984a7e4d94e8
1283da4519c11d20a9c535d2886d6e60706d62aaaa8fcdbc55eeb0ee84f9805a
0ec4af0779080f9b0b534a6b1b6f1f09ee205cf49a4334046d683d1cce84d3a0
9e98fd3ad7527503b255a70ee461c02a3c9ef9aabdee3173d2f8fbb8c93d2d50
0497e0e927adf2d0079f4e0f93dfc349bf1a2321843f8c33efe89e705900d3ba
b01449db6a81203583e9226c5a4c4883abaeccb3fdc5bfda2d190bfeaf2d24b6
0afb5b3572320c62a1cf10f98cea1f27ddb67fa4b8453f41c7a43faaaa48042e
2ac34da22b6ea2d1f2c3e41c9ce01d69b16abbad9d562a238d95086c245d1762
e881c562ad195b51c9800bc32e8f170db651a7a97a9b3cc1304e80661e156c9f
1a8903d201f01608fba5c48f0f9d6d0546a0534c8af6fa61ecf28b2f484e77fe
9f6ee25ada84e57739fe3e29306bbc45b9df667bd1628e3dd1a0c2891c3deb92
502c7793e4f6e5186e4ce075704b901ba053a1f99446feec4f7d16ce450880f3
07444839822a1b1a93dec11bb03e1d26444f1471eab4fd15dd0096d075ac8db7
34d47a3999a36741bfb267b4429a09f0ad910b6196a298362c5cd688b2cf4d54
aaa461c983c495c8be4bc9deaaec43ab0ce533b55e0688f6e7dbbd91f48c71b9
9da1a55b88bda3810ccd482051dc7e0088e8539ef8da5ddd29c583f593244e1c
7a07fbc4903e443f237fc7c99976a8cdb751a983860ea17b891a8c617a820ad0
e3844f43afbc510d0b5c6f77e482711bbbb3dcae8e04b2f7200a11eff27c029d
d40b8c55edf7d7f118650135ee37080e8e296e635af5481e1a2850088524196c
057da080ae0983585ae21195bee60d82664355a7fd78c25f21791b165c250212
950532180701f8ac033a8796238d7e5b6900bc2652f28e2a44645d3cdabdeded

2cef1c6ead6c8faebf201a1e2b24a8e89b27e946244cf2116c607810b5e4f658
143cd3d5e7fbbfef8a63ccee0072a47a55872bec0da514248385ead8611543c0
92717c8ecbf6524a9fefb57a346872292daa2132aeb492ccf725208474ad9179
905fb292dc983a9d731f4716aa2e1ee289975330d11e82df95491f5a9dd7e3ed
de1356539a38d545dd557fdb63fb1f0b3a0c348ba1570c99720cfdd59b0e2007
ca79a32fa92a7c3eb6a2997dc90410da5e1c3d8638a5e7486cad3eee3aa12fb1
15c87b1820b67d4d2b082e81fd7946dd00a1072441b7551e38fccd5575bf18c2
1b70f0a55b1efadd896c8b2979663f6720f702b579127a72c1c68aad259def6c
87f51b4632c5fbc351a59a234dfefef506d807f2c173aac23162b85d0d73c2ad
15c45d634c70f0604cfe30806320090c66a65d8f8a26303db3c9c15bf3cc950c
aa6413bec5d0d549cec702430120be5bb230d36bad1a8809193ed77eea6275d6
437050e782d14bc29504ea38cd1ba01a5f6bca7b64fc80e16e241112fcb275c2
207397bdcd9b5818f82dc4ff9638dfee35b62b56e6e2fb7e158f13950093ac72
84d9b74b7002de7f49bb7624ea63bf815497c51701bb3ec9124a0ec702178ef0
7afde436f24f7faceb786554857c0fef6ceefebd1be0fcd4e68542e5a2ff0c8e
01ec30dcacc8d6ca290ae7977bf40e07f1cb29d69ea55d2f31f41ebf5240c6ff
36b57a7ff126d0f2c11e7d53d405e578dd2cda64538120dca80482c5779accdf
fe716cd97eefa66582d3a5b33b61df6760b4b6d69a68fd2bc5b2a93d6dfa11ae
def8ada059c5d8017bf912990f1f9dc961c7e143822b69007411a97086f0967d
bf6705b2148f8f49bfd231de2de8939ad4686f34c0e0f6db7168be3dd8269689
55a08e78689b58ba3b4bf7ea6d3a2420b15ccd7b4fccc97892b5724c538fb6c8
d3190b5007d433e875039da72ef507a1c6e7c15cdcf7ce4409e333d89c9050ee
6f571bbee189b20d4e845e2c81d0043f9ba6141f4032a0232752e87c9549ca73
81b67f89ebe7923e97582e3518272a49d94599107e147ff85babf231e053cf63
bfcb56e41871cf6668c2699c3b0697913d0780bc0195a51ae036db7b991797d9
aa980e29a43487d2d6af607de7d9e3dd0b8fa0cfc3960257aec7e303e689ab56
f26998a89d011af5860fa5c9cccf3ee09c81b14156824bdbee21e3229c7cba4b
8840ac6cbd448b00849f9c84ae104a49fb3464f530cf9b2aad76f04ccb0ccc78
e60ad9543b873569432bc05cbfc8dd0f72a618f26eb256f15048b820e151846e
37c7500ed49671fe78bd88afa583bfb59f33d3ee135a577908d633b4e9aa4035
ad17ada0171b9e619000902e62b26b949afb01b974a65258e4a7ecd59c248dba
d17453505cada182f346b9a3033276cf509277de4a2356fbb000abf347147a7a
deeb84b07542eaa9efd4db44bf8e9ab15b9056930962352d458852410c57e3b2
f6bec3c2d0503978f88734c6d52f2a01552c1d24b8e014ab835827ba3c9cc548
d27474625cdc0c3456918edfa58bfaf910c8b98c6168a506ac14afc1a41fb58f
17742a3ca746f7f13aff1342068b2b78df413f0c9cd6cdd02d6df7699874a13a
662c3b181467a9d2f40a7b632a4b5fe5ddd201a528ba408badbf7b2375ee3553
6333e9f091e0f605b91d2fbae9a7040800837bdc9418ccda9bd91e894b610a20
3e9d94714c78d02eedc5f9085982edd5b840950e65702d8ee1544b643733570b
dfad2a80dac91e7703266197ebbf5d67ef77467ab341dd491ad25d92d8118cac
f6e7fe318a66289722770cc1786049364774464d0ff879e284b8a3fa3630e74f
e507cc17eff228f9b04780e1fbef37fb7f90910cef4c32c3b9b01d3140773fdb
8f01ae46434e75207d29bc6de069b67c350120a9880cc8e30fefc19471eaac4a

72b1b30e4b34a0267f7386974ee024c02a3b3aa62c409de18a497ca23ade20e1
52dee9632229ad8f163edce75e564c91b6c60c4656dafac134a4433b8d4de546
2491caddf4445d9297404493c7707b54591c989b94fd4634a7afdf54c0d22e9c
1eb0d373cea19124687ed4bffb0da3f80f98a18b9e0bebd3c12443f0a3d81689
b658afc63bac3f28c7a70b9162480c3a8bbe7263a5f8cbb36f1430abba8fe441
b2d533b84e0d3c2acc98767db3eec2888d44f12317ece1477bdb2c56e4d7a71c
e5531fcf015db455a4c8fe6cb57fb5c7e179c84bb6b80194527c8ac581e055c9
8d537e68f562d89434f84ceb78f40fc74911b711bc1460cebf8fd1896bc9d5a2
d70138bbb3687aa31b35ff4aadac1ffe6569de225981f299b8853bc69c0fc39e
114b6330741d974e1c97e42cff843247e7261b222ac716ea972fe59a7dfd09a1
2c13ef00c1f17df9e60d650c5476e8212036c1496a7d48c85a475df5e2336ff7
9523cf5e690302198c39e833e01f9d070f803a8445a0b40a8e33c2edc1771c3b
fd8ced785e918da29bebe5f49a909794594fec7564477d8db4aa9a170681ea39
8e1c701bcc16001a3f579ac0531187478c8b96ebc3c354f4ba170c75c33e52e0
d68ff2f6937ea8a66a68e26b41112f8db006115e7c966e28ce67029f0317992b
5dd8a5779aa0e2b27baf9a059f1b668323ada1da2aabe640960b518cfb1b18a3
d7317a96f983a73cdccf319bcd4461cdb736e9b6b5232927861499494db957f2
8afd18b6729181aa21c14ebfb869fb97c2b02099b7a832aba5d2aa22a758b694
316b295483f59fe6b6690a3c3a889916dfb9e56375c687c48125dea601097204
dbb9168502e819619e94d9dc211d5f4967d8083ac5f4f67742b926abb04e6676
877b64590533a9545d160acb720138d9a675a7c97dc3c48005a3edae0a44c8df
9fc84eadba969bd12cda144750cef361bcdff224026eb3921d8d46a5a424da5b
1c2b18560f086f01541e5f2616c9faf6df4a47b878fcc2ac72ec41a7f6f30915
b0ad4f3310261549c5a6cc13aadd8d7525c3cec9ef944c2b8762992360643b87
691d80e4b5411a15961eeacc08b6594bfa546c646301467dc31cd470d10d0191
047f76e6674abf3887162158ec0ea1de324236402fba9698cec204a2d7d8dc92
7b97b902236d07307789391174cd07de4cf4225aa1e1e738ab1a9e046a431b04
c6dbdf2978bbadb222f2f03cd745f884226472531fd7aa96bc23c55735009ff5
a5f02bb70acdf335bed9c0fc8439ab3a220027a28c7eb44f459afda0ec7b62eb
02fddfee4928270827be0b6be617661543eb59f4a0807047eacc05c8507d188b
979f7952dd2225c149f1766b4bca020b680364a77ddb6006cfa462543e0a6440
5d558a9df7802486977851c704c37ce168259df48de3cac8714b496b69da2bc8
2e58c371711034249cad252bbff2d49ca5ff527892ba936c007302536ff50b40
c57089745a418cfb8cda224fa9faf383e72df19e5bd9e1cf83f7bfd4a5c819dc
8acc17f38e5bfab577927b2477a5842517370959d35d3a80328d58bc7238e3f5
46cad0e0ca3b2d6d9d3ce691ca2887b18abc80acf0e81799fbb290cce104c8eb
2f8e2c8300b7854ff204375f5116854cee7c4ef11f9b080dce89713867fd7066
9ec58c011d7efbc2272a0403cd90cb4640858da7b080819737af6f1dd6b6f1e0
3ce8cba4a3271721f7e2f5cab90aff56a4a6d2364d5ecbf789aa951fae7c4572
56331a4bc845b9ce0f2ad37f9c28d7c629e629d51349db0e5c5859b189c04ba1
936f2cc6458164daab71d9319cea87138f07b3845cc06ba37788c99ea5ff404a
96c730f25ee6e5a552e27b0c040f85e81a00d1c504e9f5250af60f842c6185d6
e2200fa8b8c4757039e3f78536d9442817331f530e4348e08f02af753e7ae024

68baf2a2d97213cb0d50bf9305e27c180dce6f2fd71f405143fa8f3cf775b588
fe04712df428e50a363a85db3bfe4503cad0b67449175f12a1a5eaff656348da
a7712b7c45ae081a1576a387308077f808c666449d1ea9ba680ec410569d476f
c22c8d74daac7596b4816de5b7549927a01f65669aed7f52e382d151deb76080
99b24003e4d5a19430653760db6492d920dfda94194ba8aaa9e82d2949aab740
ac4214f8b674686ea5ec51946b36290367965f3f53d93a2627b5fb0ed27f6e3a
6c917faa1a5ea5ae74525ace0c39c4a9208cb48f64372b8cd97c2e6e96a957db
08b8ab37fd019b2c9d33d278eeaa16e9c50ed4c7c66ef7202eb0537ec9465a07
577b92a3a23917f55b1156d87ae4d4824894a3b15ae687ffa8b8af125a10438c
feda78f1dff8bd9d850a154a627bcfb4041dc36c325be0db436ca85fe565f767
48c1e890c831ce2ea0bfae2bc498f42434c1c6c9d481893fa0e57285dc3dc729
e0e33f6a80bd4bab7ea7b21d64e2632d9d769aa8994ece8fae9fc358b85514d5
e5570713f4ff9c3e064c136de4e0bde2b845203b1cf330db40392cc985c13cc8
874501a8b8244ac00f3e2c54cbf02350c4eb7e6ce0ddeb53caff89538bc75b07
11ae7e7ab4d36dfe0bc33fd7719eaea5acd0ecbe17b32943660acb7647c33c34
9f5265056373d64e816c502cc3018550b3dea1ae4eae081b0631242a29a74faf
4a25e48b8cf515f4cdd6711a69ccc875429dcc32007adb133fb25d63e53e2ac6
97945ecc788f71ac05fd4eb54a41bc5704583f6928c73265dff92d4012858bad
f3148fc69a57b3b3e18ab435875ef68dac3e147d2fea4875657bf828adf09e52
9b4932af4003a11929da44d1181e9c5d9414b2c510cc601accc1691d36a21649
e38ff03d54d40f4e10292d7cbd614f26f3af13d01ded95dc7c363b317a5d6dd4
6ee76407efa8157b7f2b80a3a7ccc41581851aca58ab10cb8caf0243ce6fa436
9af6127a75b3cde2c5b459e5cacdd78bbfa8584dc892a93fb8b77bbb85a42731
c388dfa6a1e1c861c8a2301644c985d9352c43b0a41604a4385ad1a4a88fdbd3
57572d520359e209357776fa2d52455dccd64999d1f3ca7a6b90bcbf11535c0a
11c45925b64777eaa401a6c0f6a6f847fb80e82d8da8fdfe1156d28663fd9396
74e41223ec6359a9bd05bbce36b452fd046aaad64617f459ba262a5210925942
1259ddd540300dbec4d76b5909dad475fa56b3b1837b6c7097d9b42e28d3182c
108a5035ab40b13b489f8a1fb8fd8bdb5880368c9c18e1d244df23b8d5a26d67
e63cd1c60fd8d9f2ab6714f371958621f9d500bb09ba3569d0435f8f38960584
b4d6964b27f9090031589b2764efd1539d05eb24fe0a9330ff0f4da69725a780
6d3982d6c6ca753d6d1daa71d88678c07718dd1919a874959a0c7975619c37fc
20ba3c06faf0f600e0615889a4721eda75d76982b16dfdb9e4a716a46e87c0f1
6a8a022c8f234dd8cbbdb9f5b4dccd80fe0410652aacf0b00bf8d962f484ae37
5ba0618abff351a051f3abc3b4831376d478ca38c10e6165453c14cb3b19590f
6c85c0c30888891e6acc548af91139955b0c669181d7c2b8eaf1dd40dd3293dc
814ed2b9ae0770d727a8cd83581b4865b2abe16f8190240c5c1e821e22a280ab
871cab3256acdbc3c27650adde878658568a85b87e85d3e3c137bdeb4592fb2c
3281e70706cee21cc83bdeca9eb426157898232cab366042cb84e192e58b91a4
e903e54fed007ee14305bc21219b3fab69385e4df16714d737da5953f7f3c170
a7c5f87bf0a01fb12cfe8fa6da2b828e11f18ff52adbde7ee49f0b1d9ce5e40c
198871b96e9fc0bfc23204ce6a861b7fc3d9c0070e1c947cb50267dc5d454477
a7aae62be1b876e8bc70f963879ff7dd94427780adc8942691a3959172bdda0e

777679db2c9f756a37f3092b8e3bd0c662cb05ac308f852d457c2cb71b50be96
e3825a91ea1387e4247f7960afb62320a438d453df955a3ec25f590843782f38
26e79b8af50583503b0c6bb5dc3e430ca9fdeff1e4c809ca5fea0057de7470e0
87f41a32b67c7e15827dbb83d48a7981f3d72156d61436d6b063b0429567613f
90175ddb90358838ea74267524d749e17a20b483b20b74d7f76fccb171226da9
0283c0f02307adc4ee46c0382df4b5d7b4eb80114fbaf5cb7fe5412f027d165e
736b42c2f35d046855d49b4e60e25100a5a3d3fd184b0d8ac3791f79bb37419b
689c049facd73d1f133f3a2aa7941f5d19ffacabf119d449643f12246a5e4d2a
dc31e710277eac1b125de6f4626765a2684d992147691a33964e368e5f269cba
1fdb5dd192e813f337adc21dfe4a31e1de10bd2bbb5b58ca51a6836b7e108953
e4fd6452566102631a74d55b5a74b3fc5a2b7431144fb0ecf9f9fe64489a7409
706ca8e074ad04777a408b845ed56c1d675902cc2ef0aa6cca29430e967ba7af
f29895d3fd197101aa284f5076a40e4e951614a7faaf214254488879b2e235f3
ee84f4b188c1c76e1b98ec4821ef90bb600a3ea89c2a84ee44a1f89712565a22
8cb3a0af0bd6a9560c0eb1b197ae94542f7b479c9d3c2d9eb17ca6b9902a1959
ae24a9da37633e7812b3ce01a0716c1f0c64e0d70a9664afa04a0c1576554a74
887cea81fe4be74bf61a61a37d6ce93d86474ecd3fe15a0370edc672a3292cf4
3945c3bd02420f6c1b0ea2b436d09f614a4389c3ebfe97f8ae17401d6c2ae925
45385d371ba32d1f17b746a338fc11bb7f1acb7b66928359e1dffc7b6510051e
49def44d066cfa46fe21be29d74c0698e944f5e6911a8180aaa296d47f19366a
a860ba3861df2ae0add2b695071c04468f83c0973525519d62679dd4cd4d0026
02e10231a6a383ff07fd6d25b3dc8dac57b077d7f27d712887a897fb6064a0c8
425266fcaaba1204d6be8bd5e4033b6dda22d29f53c53eb88601e45d32623922
d0a5ffa3b9c40eb1e4277e7c41a100b0836c9424b36fb9bbe281711c0b116883
682dcf03ca8d0e1af60b06820f904802f09422717d7a3d6f396a23983814e431
dd47cf8ec70658af85e0cd23922462ac788305034fe78ed725bb90c1a3fa04cc
137c059adda4df22eb29785fada54ebc00a22d150bfdc423f87ff1f6093bd827
152e296998d9376c13c0ea29d191e01622ddec754484b5eefd795989b8a44ab6
26218ad353f0ef41ccecbd1ac0367177274422e18a98487d381be4e0741a9d6a
c7dbca435039a6148dc25208f04b734465e8b7c92010ede1401d88f5f8003f2d
4c21c88399d95a3602aaacf85a83c8aaac5ae7b6bf192c4c25cef4f9224b6f7b
3f77b9266f6fe2ead71fd17f86e88ad4623023349540604a56612949808acc71
e91836bbf90b1eafd5cdcf8868408309470d4a06c5239dfee7dd74eca1a7f222
8b1fe0fe0a20f8ce383a2713e170f91791ee6f62915dff86fb9e070965a7be23
ce591810b667c31c37c856b56b277ae839a71cffe0b79e757f9105ed0208b9e4
67da24711012366322f2e6ab3534d62c064d24dc6e113b6077354c792cc56b71
d035e96f54abe59dcdbc2156e55cd0135ec420f8e97aca7f109ee8d062baa755
d32a88349a7b10db3ba40619237009ab2fd5ec8351f3ebf3ca6865f576105a96
5a7a7c94eed3eea9fbc9ff1a32ea3422b46496e405f90858b1b169bb60bdbac6
ae1ce8b298ab6c7630e20f15363c7e572fe08460bd848faef5696c883298589b
0172bec4d945add9f12ce4d7d23f0e0da1ced677e89bfc132b000d444876cb41
4eca66552e8c2161adf3b10eed1082f0f18b98e4526851c8da5f48d976288890
144d8dcc78075b2f35eaf1392018127a1ff775c2a8053b91ea6837c1c246f2e2

0335de8eadbbd5dc7cbe92ef869bcea6f6596ac39a38680142c982ec6e97ecde
577a101dfe7db05c29570a1971e1a26e46f2f979d8ad99d51bb47665042614a5
6638dd6ec6c31b49c913747340fa1b2839dd9e525ac3984542669d01e8ec4ec1
3a824bfd2a90a97365f945f965a7b2afb8a52e93a0ae4215a99a61f93aec87a1
108ea9a83499004c3b618a2d547bdcdd470a7012ed0eba1dcf5bdca93beb4bb3
ecad65cf452d0f7586c8d08bc15576e5ac85ade2565e515485574cdae979bd3e
b5db0dd322656c19a05bc78f3ce1d8bed30e72fb8c1ac5071fce4afa720f2696
59c6721a5ec5f97ef9b35e17057a5edb4f0075d1430c0cbd3eecfd44ccfe272c
ea4466015415499acb68e205595adf8e22a19f86097d62b9de473d4ee24a6986
812539ebfba481c1cde1fd4db7f523b6819e4dde7d0130f5ef60fac7de67fdb7
bccfcbb8097dd32f0870621fa6d33f993f2d180a874eccc69b97815f3052d5c1
497b143d5cfcda0f409ffaf51c84bd9d8e2dfdbb22500dd17420f76b4b94c55d
774ffa99aaf6cf5bc9c2ef4744a2d595a3b84a9b6b4a4efe3394fb1cfdd8e782
7b455b78698f03c0201b2617fe94c70eb89154568b80e0c9d2a871d648ed6665
245EA1A8DC32622AE18FDC7DACCBD9EE29C244FAF8F6D99D332B513E5A951D26
39567c9bbbc038574fd1cf569f4f7cfd68403cd817984186b83098ded2433b2c
2d2ee85092147f08db4ab93b2952e42a971c6c7491985419ac375feda8674c60
b0dfb366cc63b4051bd100e5f8d132c400f4c0845d142c723d9c83efd1c52c1f
90a8515c195733e4c605c4daab50076f168d4e92da35622cefd067fddb1e913f
8e170fab8cdf11b83089706a2bf4a1748844693f4c6f465e7ba89131df089b48
113776d3cc8409da498e898bc5e0cafc1762ce1d49e1a86c56b4d841b06efdf8
98b5b30988dcab7b83ef1ca6d28a6800b70a51217a8a175701ca334669a642fd
08c0c431f7f63136091854af58cd7f9e6d229f90a9b0fda813c52232c030f6ea
58643719af0f271b87c51665c2e8c904db70155b8c6f514d6e5f44c0828a4a53
451cab3d5b5a1c699f1b9b3d8a4ddf73c48f891cbca88e4e1a829e2442116efb
ccbe720fd059610227d478578a5a4019c96885de8fd3e83984f9c1c5fe850ad6
c598f7956b1d0d6514ade39df05c9fcad70f970957c980d15f6d019e5ca04df6
1d806466896998a6c4ac962d6e5381fe704670e3fd912db98e13c2a5482b9a7e
81ca347465f28d093a27caf3d83fe5c4fb50c5e48cfd851a06784d431fa8c2cf
cee88ffae63cd95e4f9f7008a86a8d7818a47b62608d28a70bbe8d73c6d2b042
5ce6d273df4fcad8953dd4f37e7f4a0390f9da52978f0227b021b6a724b59313
e158b20c400cb2c24ce4223bb947dee86e3717b18446b76911389a9a1fcc2260
53e3d197e9d6ac3f23f8da64ffb1a1013e84d1ebf52864f5b0f8b79006f1ddc4
72aa69be5cd46220e1509c040ceb6e3cbb3c676a6c464a811370d688f45f26ec
2e103dd8eda4750fd5fe99c0c5fbc987ae7712bea7c08db4db240e85a0ee1bbf
fadc0fe0714d9e95904ccaaf16d895ac71c1337e92b8eb51258fed9fb8fb4620
012eba6182006cf9772ff509896fc2a929b5fe3062f29ed70c451c8ebd393d27
86d43578ba26f02cf845f16a38ab29a48ad86c17f4a2ec3b69fc0d5fe82b4af7
04f2a21072bf11e8cf9e06bc9e0d8102f07df92b8af6bf2431ea33be098cf0ea

List of CVE commonly exploited by TRANSPARENT TRIBE:

CVE-2012-0158

The (1) ListView, (2) ListView2, (3) TreeView, and (4) TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Controls in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0 Runtime allow remote attackers to execute arbitrary code via a crafted (a) web site, (b) Office document, or (c) .rtf file that triggers "system state" corruption, as exploited in the wild in April 2012, aka "MSCOMCTL.OCX RCE Vulnerability."

CVE-2017-0199

Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."

CVE-2017-11882

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

Advanced Persistent Threat (APT): APT28

The cybercrime group APT28 (also known as Fancy Bear, Sednit group, Sofacy, Pawn Storm, Strontium, Tsar Team, TG-4127, Group-4127, TAG_0700, Swallowtail, IRON TWILIGHT, Group 74, SNAKEMACKEREL, SectorC01, ITG05, APT-C-20, SIG40) has been operational since 2004. Most of the attacks targeted political and military institutions, while a smaller percentage took aim at media and sports organizations. At various times, defense ministries, foreign ministries, and other military and political organizations of various country were attacked. In 2016 and 2017, in addition to standard targets, APT28 attacked the World Anti-Doping Agency (WADA) and international Olympic winter sports federations.

Related Tools

Tcpdump
Responder
WinEXE
Remcom

Indicators of Compromise (IOCs)

CnC:

http://msrole[.]com/office_con
http://supservermgr[.]com/sys/upd/pageupd[.]php
http://45[.]124[.]132[.]127/action-center/centerforserviceandaction/service-and-action[.]php
http://185[.]221[.]202[.]35/software-protection/app[.]php
http://185[.]86[.]148[.]227:443
http://45[.]32[.]129[.]185:443
http://23[.]227[.]196[.]217:443
http://86[.]105[.]18[.]106/apps[.]update/DetailsID/clientPID-118253[.]php
http://86[.]105[.]18[.]106/versionID/Plugin0899/debug-release01119/debug-19[.]app
http://86[.]105[.]18[.]111/UpdateCertificate33-33725cnm^BB/CheckerNow-saMbA-99-36^11/CheckerSerface^8830-11[.]php
http://93[.]113[.]131[.]117/KB7735-9927/security-serv/opt[.]php
http://rammatica[.]com/QqrAzMjp/CmKjzk/OspRkzmG[.]php
http://185[.]25[.]50[.]93/syshelp/kd8812u/protocol[.]php
http://185[.]25[.]51[.]114/get-help-software/get-app-c/error-code-lookup[.]php
http://213[.]103[.]67[.]193/ghflYvz/vmwWIdx/realui[.]php
http://46[.]102[.]152[.]127/messageID/get-data/SecurityID[.]php
http://80[.]255[.]6[.]5/daily-update-certifaicates52735462534234/update-15[.]dat
http://86[.]105[.]18[.]106/debug-info/pluginId/CLISD1934[.]php
http://89[.]249[.]65[.]234/guard-service/Servers-ip4/upd-release/mdb4
http://89[.]45[.]67[.]153/supportfsys/t863321i/func112SerErr[.]php
http://93[.]115[.]38[.]132/wWpYdSMRulkdp/arpz/MsKZrpUfe[.]php
http://rammatica[.]com/QqrAzMjp/CmKjzk/EspTkzmH[.]php

http://213[.]252[.]244[.]219/client-update-info/version-id/version333[.]php
http://222[.]15[.]23[.]121/gft_piyes/ndhfkuryhs09/fdfd_iunb_hhert_ps[.]php
http://86[.]105[.]18[.]106/data-extract/timermodule/update-client[.]php
http://86[.]106[.]131[.]177/srvSettings/conf4421i/support[.]php
http://86[.]106[.]131[.]177/SupportA91i/syshelpA774i/viewsupp[.]php
http://142[.]0[.]68[.]2/test-update-17-8752417/temp827612480/checkUpdate79832467[.]php
http://213[.]252[.]245[.]132/setting-the-os-release/Support-OS-release/ApiMap[.]php
http://185[.]25[.]51[.]198/get-data/searchId/get[.]php
http://185[.]25[.]51[.]198/stream-upd-service-two/definition/event[.]php
http://188[.]241[.]68[.]121/update/dB-Release/NewBaseCheck[.]php
http://194[.]187[.]249[.]126/database-update-centre/check-system-version/id=18862[.]php
http://213[.]252[.]244[.]219/cumulative-security-update/Summary/details[.]php
http://220[.]158[.]216[.]127/search-sys-update-release/base-sync/db7749sc[.]php
http://89[.]249[.]65[.]166/clientid-and-uniqued-r2/the-differenceU/Events76[.]php
http://142[.]0[.]68[.]2/test-update-16-8852418/temp727612430/checkUpdate89732468[.]php
http://185[.]25[.]50[.]93/tech99-04/litelib1/setwsdv4[.]php
http://185[.]25[.]50[.]93/techicalBS391-two/supptech18i/suppid[.]php
http://185[.]25[.]51[.]164/srv_upd_dest_two/destBB/en[.]php
http://185[.]77[.]129[.]152/wWpYdSMRulkdp/arpz/MsKZrpUfe[.]php
http://213[.]252[.]245[.]132/search-release/Search-Version/crmclients[.]php
http://46[.]183[.]223[.]227/services-check-update/security-certificate-11-554/CheckNow864[.]php
http://80[.]255[.]6[.]5/LoG-statistic8397420934809/date-update9048353094c/StaticIpUpdateLog23741033[.]php
http://86[.]105[.]18[.]106/ram-data/managerId/REM1234[.]php
http://89[.]249[.]65[.]166/int-release/check-user/userid[.]php
http://89[.]40[.]181[.]126/verification-online/service[.]911-19/check-verification-88291[.]php
http://93[.]113[.]131[.]155/Verifica-El-Lanzamiento/Ayuda-Del-Sistema/obtenerId[.]php
http://185[.]234[.]52[.]168/categories/buildings[.]php
http://185[.]205[.]209[.]172/sciencedirect/development/AAF-Progress[.]php
http://stratforglobal[.]net/weekly/51586/ruthless-and-sober-syria
http://89[.]37[.]226[.]148/technet-support/library/online-service-description[.]php?id_name=
https://support-cloud[.]life/managment/cb-secure/technology[.]php
http://194[.]32[.]78[.]245/protect/get-upd-id[.]php
https://www[.]c4csa[.]org/includes/sources/felims[.]php
https://www[.]xbhp[.]com/dominargreatasianodyssey/wp-content/plugins/akismet/style[.]php

https://109[.]248[.]148[.]22/orders/create/new[.]php
http://89[.]37[.]226[.]123/advance/portable_version/service[.]php
http://109[.]248[.]148[.]42/agr-enum/progress-inform/cube[.]php
http://145[.]249[.]105[.]165/resource-store/stockroom-center-service/check[.]php
http://185[.]203[.]118[.]198/en_action_device/center_correct_customer/drivers-i7-x86[.]php
http://185[.]217[.]92[.]119/db-module/version_1594/main[.]php
https://190[.]97[.]167[.]186/pkg/image/do[.]php
http://45[.]124[.]132[.]127/company-device-support/values/correlate-sec[.]php
https://91[.]219[.]238[.]118/zx-system/core/main-config[.]php
http://89[.]37[.]226[.]148/technet-support/library/online-service-description[.]php
posta-hurriyet[.]com
mail-hurriyet[.]com
sset-aljazeera[.]com
mail[.]arnf[.]bg
mail[.]moda[.]qov[.]sa[.]com
webmail-mfa[.]am
accounts[.]g00qle[.]com
webmail-mil[.]dk
webmail[.]exerclto[.]pt
mailmil[.]ae
mail[.]dca[.]qov[.]my
mail[.]g0v[.]me
onedrive-en-marche[.]fr
mail[.]hm[.]qov[.]hu
dansa[.]bg
mail[.]bostondynamlcs[.]com
link[.]candybober[.]info
mobile-sanoma[.]net
web[.]mailmil[.]lv
fortele[.]ro
account-aljazeera[.]net
login[.]accoounts-google[.]com
myaccount[.]google[.]comchangepasswordmyaccountidx8jxcn4ufdmncudd[.]gq
mail[.]university-tartu[.]info
inside[.]wada-arna[.]org
mail-navy[.]ro
mail[.]armf[.]bg[.]message-id8665213[.]tk
qov[.]al
mail[.]anadoluajansi[.]web[.]tr
webmail-hurriyet[.]com
ssset-aljazeera[.]net
mail[.]byegm[.]web[.]tr

myaccount[.]google[.]comsecuritysettingpage[.]gq
mail-skupstina[.]me
kasapp[.]de
mail[.]kuwaitarmy[.]gov-kw[.]com
mail[.]mod[.]qov[.]af
webmail[.]mfa[.]qov[.]ae
webmail-saic[.]com
privacy-yahoo[.]com
account[.]password-google[.]com
mail-isea[.]ru
fkit-mil[.]dk
mail[.]rsaf[.]qov[.]sa[.]com
mail[.]wada-awa[.]org
tas-cass[.]org
mail-aljazeera[.]net
url[.]googlesetting[.]com
e-post[.]byegm[.]web[.]tr
e-posta[.]tbmm[.]qov[.]web[.]tr
webmail-cdu[.]de
mail-gov[.]me
vpn[.]onderzoekraad[.]nl
poczta[.]mon[.]q0v[.]pl
mod[.]qov[.]al
poczta[.]mon-gov[.]pl
webmail[.]mofa[.]qov[.]ae
mail[.]mofa[.]g0v[.]qa
mail[.]academl[.]com
mailpho[.]com
mail[.]fach[.]rnil[.]cl
webmail-mil[.]gr
sset-aljazeera[.]net
eposta[.]basbakanlik[.]qov[.]web[.]tr
support-cdu[.]de
actblues[.]com
sftp[.]onderzoekraad[.]nl
mail[.]mod[.]qov[.]es
email[.]mfa[.]qov[.]gs
anadolu-ajansi[.]com
login-osce[.]org
mail-pims[.]org
mail[.]rnil[.]am
Uniquecorpind[.]com
Postlkwarn[.]com

globalresearching[.]org
Joshel[.]com
Appservicegroup[.]com
Apptaskserver[.]com
Versiontask[.]com
Securityprotectingcorp[.]com
adobeupgradeflash[.]com
Akamaisoftupdate[.]com
globaltechresearch[.]org
researchcontinental[.]org
worldpressjournal[.]com
worldpostjournal[.]com
microsoftstoreservice[.]com
appexsrv[.]net
defenceglobalnews[.]com
politlco[.]com
globaldefencetalk[.]com
abc24news[.]com
servicetlnt[.]net
windowsdefltr[.]net
pressservices[.]net
washingtnpostnews[.]com
portal-office[.]fr
mail-en-marche[.]fr
accounts-office[.]fr
en-marche[.]co
Cdnverify[.]net
msrole[.]com
mafra[.]go[.]kr[.]jeojang[.]ga
biathlovvorld[.]com
iihf[.]eu
mail-ibu[.]eu
fil-luge[.]com
webmail-ibsf[.]org
fisski[.]ca
supservermgr[.]com
appleupdate[.]org
software-update[.]org
baltichost[.]org
servicecdp[.]com
blackpartshare[.]com
contentdeliverysrv[.]net
space-delivery[.]com

mountainsgide[.]com
netmediaresources[.]com
sendmevideo[.]org
webviewres[.]net
satellitedeluxpanorama[.]com
rammatica[.]com
adfs[.]senate[.]group
adfs-senate[.]services
adfs[.]senate[.]qov[.]info
adfs-senate[.]email
chmail[.]ir[.]udelivered[.]tk
wmdmediacodecs[.]com
soros-my-sharepoint[.]com
esco-plvnlch[.]com
dpkshodnya-my-sharepoint[.]com
cubenergy-my-sharepoint[.]com
hudsonorg-my-sharepoint[.]com
transparencyinternational-my-sharepoint[.]com
kub-gas[.]com
kvatral95[.]com
ssl-icloud[.]com
storsvc[.]org
www[.]tabsync[.]net
wscapi[.]com
munimonoce[.]com
accounts[.]google[.]com[.]rnil[.]am
mx6[.]set132[.]com
server[.]mx4[.]set132[.]com
mxx[.]evrosatory[.]com
accounts[.]servicegoogle[.]com
mxx[.]us-westmail-undeliversystem[.]com
mx1[.]servicetransfermail[.]com
mvtband[.]net
mvband[.]net
osce-press[.]org
theguardiannews[.]org
worldmilitarynews[.]org
aljazeera-news[.]com
military-info[.]eu
militaryobserver[.]net
nato-hq[.]com
natoint[.]com
pakistan-mofa[.]net

politicsinform[.]com
ausameetings[.]com
bbc-press[.]org
cnnpolitics[.]eu
dailypoliticsnews[.]com
defencereview[.]eu
diplomatnews[.]org
euronews24[.]info
kg-news[.]org
militaryadviser[.]org
shurl[.]biz
unian-news[.]info
worldpoliticsnews[.]org
worldpoliticsreviews[.]com
dailyforeignnews[.]com
defenceiq[.]us
euroreport24[.]com
politicalreview[.]eu
unitednationsnews[.]eu
virusdefender[.]org
nato-news[.]com
natopress[.]com
osce-info[.]com
reuters-press[.]com
stratforglobal[.]net
thediplomat-press[.]com
trend-news[.]org
kenlynton[.]com
microsoftdriver[.]com
softwaresupportsv[.]com
symantecsupport[.]org
updmanager[.]com
ciscohelpcenter[.]com
cloudflarecdn[.]com
nortonupdate[.]org
updatesystems[.]net
intelmeserver[.]com
microsofthelpcenter[.]info
updatecenter[.]name
microsoftsupp[.]com
timezoneutc[.]com
1oo7[.]net
akamaisoft[.]com

driversupdate[.]info
inteldrv64[.]com
windowsappstore[.]net
advpdxapi[.]com
myinvestgroup[.]com
ndpmedia24[.]com
peacefund[.]eu
unigymboom[.]com
vsnet[.]co
moldstream[.]md
secao[.]org
remotepx[.]net
rpcnetconnect[.]com
ntpstatistics[.]com
oiagives[.]com
rdsnets[.]com
msfontserver[.]com
treckanalytics[.]com
oiatribe[.]com
hp-apps[.]com
visualrates[.]com
support-cloud[.]life
www[.]c4csa[.]org
www[.]xbhp[.]com
apple-iclouds[.]net
itunes-helper[.]net
login-csis[.]org
csis[.]exchange
csis[.]events
csis[.]cloud
photopoststories[.]com
www[.]acledit[.]com
www[.]biocpl[.]org
aadexpo2014[.]co[.]za
tolonevvs[.]com
itec2014[.]co[.]uk
sofexjordan2014[.]com
gdforum[.]net
mail[.]dansa[.]bg
natoexhibitionff14[.]com
www[.]sofexjordanx[.]com
eurosatory2014[.]com
counterterorexpo[.]com

vice-news[.]com
mailmil[.]lv
novinitie[.]com
standartnevvs[.]com
kavkazcentr[.]info
updaterweb[.]com
getstatpro[.]com
213[.]251[.]187[.]145
62[.]113[.]232[.]196
81[.]95[.]13[.]60
86[.]106[.]131[.]193
86[.]105[.]1[.]13
193[.]109[.]68[.]87
95[.]215[.]47[.]207
94[.]177[.]12[.]155
89[.]45[.]67[.]20
86[.]105[.]1[.]121
130[.]211[.]96[.]168
178[.]32[.]251[.]106
191[.]101[.]31[.]119
154[.]16[.]138[.]62
23[.]227[.]199[.]104
95[.]215[.]47[.]114
109[.]236[.]87[.]83
45[.]55[.]91[.]45
151[.]80[.]74[.]167
81[.]95[.]5[.]148
93[.]113[.]45[.]100
93[.]113[.]131[.]14
154[.]16[.]138[.]77
185[.]25[.]51[.]198
185[.]25[.]50[.]93
92[.]114[.]92[.]102
185[.]221[.]202[.]35
82[.]118[.]242[.]171
167[.]114[.]153[.]55
94[.]237[.]37[.]28
31[.]220[.]61[.]251
128[.]199[.]199[.]187
191[.]101[.]31[.]112
185[.]86[.]148[.]227
23[.]227[.]196[.]217
45[.]32[.]129[.]185

185[.]86[.]150[.]244
142[.]91[.]104[.]106
86[.]106[.]131[.]141
86[.]106[.]93[.]113
185[.]216[.]35[.]26
89[.]34[.]111[.]160
213[.]252[.]244[.]219
222[.]15[.]23[.]121
46[.]183[.]223[.]227
80[.]255[.]6[.]5
86[.]105[.]18[.]111
93[.]113[.]131[.]155
213[.]103[.]67[.]193
89[.]249[.]65[.]234
93[.]115[.]38[.]132
89[.]249[.]65[.]166
89[.]40[.]181[.]126
142[.]0[.]68[.]2
185[.]25[.]51[.]114
185[.]25[.]51[.]164
185[.]77[.]129[.]152
188[.]241[.]68[.]121
213[.]252[.]245[.]132
220[.]158[.]216[.]127
86[.]105[.]18[.]106
37[.]72[.]175[.]151
185[.]25[.]51[.]64
40[.]112[.]210[.]240
104[.]254[.]99[.]142
185[.]206[.]224[.]45
91[.]132[.]139[.]155
184[.]164[.]139[.]238
94[.]158[.]245[.]28
87[.]236[.]215[.]246
191[.]101[.]31[.]6
198[.]105[.]122[.]187
46[.]22[.]208[.]204
155[.]254[.]36[.]155
95[.]153[.]32[.]53
89[.]33[.]246[.]117
89[.]45[.]67[.]144
185[.]234[.]52[.]168
185[.]221[.]202[.]36

185[.]86[.]149[.]125
185[.]205[.]209[.]172
70[.]85[.]221[.]10
131[.]72[.]136[.]165
81[.]17[.]30[.]29
192[.]95[.]12[.]5
46[.]183[.]216[.]209
185[.]106[.]120[.]101
104[.]171[.]117[.]216
80[.]255[.]3[.]93
5[.]135[.]183[.]154
141[.]255[.]160[.]52
92[.]114[.]92[.]125
176[.]31[.]112[.]10
176[.]31[.]96[.]178
80[.]255[.]10[.]236
95[.]215[.]46[.]27
89[.]32[.]40[.]4
93[.]115[.]38[.]125
167[.]114[.]214[.]63
185[.]86[.]149[.]223
31[.]220[.]43[.]99
69[.]12[.]73[.]174
193[.]29[.]187[.]212
185[.]183[.]107[.]40
103[.]41[.]177[.]43
185[.]86[.]151[.]2
46[.]21[.]147[.]76
185[.]181[.]102[.]201
185[.]77[.]129[.]106
93[.]113[.]131[.]103
169[.]239[.]128[.]133
162[.]208[.]10[.]66
185[.]86[.]148[.]184
179[.]43[.]158[.]20
94[.]177[.]12[.]150
185[.]86[.]149[.]116
169[.]239[.]129[.]121
52[.]237[.]74[.]41
89[.]37[.]226[.]148
80[.]90[.]39[.]24
195[.]191[.]235[.]155
193[.]56[.]28[.]25

194[.]32[.]78[.]245
205[.]147[.]110[.]238
185[.]10[.]58[.]170
185[.]217[.]92[.]119
91[.]219[.]238[.]118
109[.]248[.]148[.]22
190[.]97[.]167[.]186
45[.]124[.]132[.]127
86[.]106[.]131[.]177
185[.]86[.]150[.]193
95[.]215[.]45[.]189
52[.]45[.]178[.]122
192[.]111[.]146[.]185
87[.]236[.]215[.]132
143[.]215[.]215[.]205
67[.]207[.]90[.]187
58[.]158[.]177[.]102
5[.]149[.]253[.]45
194[.]33[.]40[.]72

MD5:

52775f24e230c96ea5697bca79c72c8e
3514205d697005884b3564197a6e4a34
0311cec923c57a435e735e106517797f
47e67d1c9382d62370a0d71fecc5368b
567d379b87a54750914d2f0f6c3b6571
3803af6700ff4f712cd698cee262d4ac
7f20f7fbce9deee893dbce1a1b62827d
170d2721b91482e5cabf3d2fec091151
eae0b8997c82ebd93e999d4ce14dedf5
a5cbf5a131e84cd2c0a11fca5ddaa50a
e3100228f90692a19f88d9acb620960d
6e1effd8de77a10f315db1109c5e73e3
0a00f0ff2b69df91c1b83772a0f1b160
e9bf5ce92b9d286fdc66616ca2cc5c68
1ce718ba64b85b58a3dfbd3a7b207990
82e0597f56653a8788bfb531af460eb0
961952e4873d9572cc356cb2425c1552
cd0aa9b954010b704f741debf46ade5e
0b803922a629f440f3a34e168d4639e2

SHA-256:

02de72e43d578c45d9d6359299cb2d47771081617ff01363b736414eb831deea

af9c1b97e03c0e89c5b09d6a7bd0ba7eb58a0e35908f5675f7889c0a8273ec81
45a4a376cb7a36f8c7851713c7541cb7e347dafb08980509069a078d3bcb1405
f5d3e827c3a312d018ef4fcbfc7cb5205c9e827391bfe6eab697cc96412d938e
1f81609d9bbdc7f1d2c8846dcfc4292b3e2642301d9c59130f58e21abb0001be
c42a0d50eac9399914090f1edc2bda9ac1079edff4528078549c824c4d023ff9
1579c7a1e42f9e1857a4d1ac966a195a010e1f3d714d68c598a64d1c83aa36e4
137185866649888b7b5b6554d6d5789f7b510acd7aff3070ac55e2250eb88dab
cc68ed96ef3a67b156565acbea2db8ed911b2b31132032f3ef37413f8e2772c5
73ea2ccec2cbf22d524f55b101d324d89077e5718922c6734fef95787121ff22
fa8b4f64bff799524f6059c3a4ed5d169e9e7ef730f946ac7ad8f173e8294ed8
5dd3066a8ee3ab5b380eb7781c85e4253683cd7e3eee1c29013a7a62cd9bef8c
a7938d9ba4415d2e05fa4eb22b8cff69dfb3a8814d97ccc25255c013435f8315
c993c1e10299162357196de33e4953ab9ab9e9359fa1aea00d92e97e7d8c5f2c
23411bb30042c9357ac4928dc6fca6955390361e660fec7ac238bbdcc8b83701
0CAB912409CCD2A5D90FB82B02376A633EC09F1DCF33480720E35E9714068C2A
ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8
12e6642cf6413bdf5388bee663080fa299591b2ba023d069286f3be9647547c8
cb85072e6ca66a29cb0b73659a0fe5ba2456d9ba0b52e3a4c89e86549bc6e2c7
bdfb1a9f59be657b5375689b357ef8e70e1e7332f52c2e79ab3be796e06858d1
eb766983a8a05ad16b15e356df43f4e00f36092b8c6effdff3a580c2de2bba8f
3e27b6b287f0b9f7e85bfe18901d961110ae969d58b44af15b1d75be749022c2
28858cc6e05225f7d156d1c6a21ed11188777fa0a752cb7b56038d79a88627cc
d934cb8d0eadb93f8a57a9b8853c5db218d5db78c16a35f374e413884d915016
8d92931af98496c2281553325fb9baec822ab33620b2bb9f1745d42ec64722e0
31c2be5fb8eb3b3610fbb5862211c4807387a6842175713c7203da3aaa451fe1
edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f908ee13eb9
d2e43c41acd40324813d51df99fa127b86d8e384671dcc77f748d86afc3993a5
f188abc33d351c2254d794b525c5a8b79ea78acd3050cd8d27d3ecfc568c2936
a7d6dcdf5ca2c426cc6c447cff76834d97bc1fdff2cd14bad0b7c2817408c334
a58b5f2e8172be31e3d1fcc046d044bd862393f3d3e12922287bedf6f8c18e39
ae9a4e244a9b3c77d489dee8aeaf35a7c3ba31b210e76d81ef2e91790f052c85
19ab44a1343db19741b0e0b06bacce55990b6c8f789815daaf3476e0cc30ebea
ab5bf79274b6583a00be203256a4eacfa30a37bc889b5493da9456e2d5885c7f
32efb1eb360cda726f0eb7647d1963adf37dada4b1a4b5ec486c88bfa1f21471
a5f59327be5e45f47fb37c1b4922cb2edba8fe0bde657acf1a1502ae34816cb1
e4e1e3c44e01c60fd433c6283bd8cd15a9941e1cbaad72e6409cc92e2e91263e
5d85fba3ff021b35bfba30d5d56b957ef084d818778ff77550bcf65755aa7849
b8e2e8666c4fd6cd7e1826dab3b2ba3e72a0c5c3530d1d612cef46089b0fa159
7103c7e2924c3f4261d538662fa27266ba535bccefd16dc74f61219660a22b2d
23e5bb2369080a47df8284e666cac7cafc207f3472474a9149f88c1a4fd7a9b0
a52af66a4438c5517870c503ac1e0515af44d3994aa62c7d818b6eef46cfbb2d
9085926d0beacc97f65c86c207fa31183c5373e9a26fb0678fbcd26ab65d6e64
952503b3f97d76cc211604f09ba210b8884c6c60d40dbea82d8c7ed222a64615

abbad7acd50754f096fdc6551e728aa6054dcf8e55946f90a02b17db552471ca
115fd8c619fa173622c7a1e84efdf6fed08a25d3ca3095404dcbd5ac3deb1f03
f27836430742c9e014e1b080d89c47e43db299c2e00d0c0801a2830b41b57bc1
25f0d1cbcc53d8cfd6d848e12895ce376fbbfaf279be591774b28f70852a4fd8
8cf3bc2bf36342e844e9c8108393562538a9af2a1011c80bb46416c0572c86ff
85da72c7dbf5da543e10f3f806afd4ebf133f27b6af7859aded2c3a6eced2fd5
cba5ab65a24be52214736bc1a5bc984953a9c15d0a3826d5b15e94036e5497df
b677cce4a844495a20eed2486ef71f4782c06630df34a6ce085880a045a07902
f3fadcb721f30568bc5b79dfc66e4932165be1e7a3799d146cf5a9232898425d
aeaca9985b50ebe1db0fcda9b3fbf02275d17737b748963b63c14da3e988d801
e05de3e4a03369192856a167f2865eab3062a102b23bfdde5c0f622b39cd159a
04db00bae17828654d1901b7ddbafbf16cca462675d8dfface7b2bc4f7d173f0
dc64fec5e951acf298184be89cf89128550b318d719dcc8e2c3194ec3bdb340b
2b657e2926d52a9550ece4590075dcf3cc2bcdcb331bec9b66f6ee85d2a1214e
3652c16479540afe3e4da18e32e93f91a9357e81f170296af99bdabbf527afb2
82120b08d8a6342f14243b84ffb0cbe8298fa7ef118897206b3fe3e07cf7005c
5c366ef31c5036d3a4aa0baecffcec5ec89106cc5b94989c192877721676105a
11097a7a3336e0ab124fa921b94e3d51c4e9e4424e140e96127bfcf1c10ef110
c8087186a215553d2f95c68c03398e17e67517553f6e9a8adc906faa51bce946
adf344f12633ab0738d25e38f40c6adc9199467838ec14428413b1264b1bf540
ce554d57333bdbccebb5e2e8d16a304947981e48ea2a5cc3d5f4ced7c1f56df3
566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092
5130f600cd9a9cdc82d4bad938b20cbd2f699aadb76e7f3f1a93602330d9997d
730a0e3daf0b54f065bdd2ca427fbe10e8d4e28646a5dc40cbcfb15e1702ed9a
73db52c0d4e31a00030b47b4f0fa7125000b19c6c9d462c3d0ce0f9d68f04e4c
dc2c3314ef4e6186b519af29a246679caa522acd0c44766ecb9df4d2d5f3995b
40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f
fd39d2837b30e7233bc54598ff51bdc2f8c418fa5b94dea2cadb24cf40f395e5
4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976
416467f8975036bb06c2b5fca4daeb900ff5f25833d3cdb46958f0f0f26bec82
25f983961eef6751e53a72c96d35448f8b413edf727501d0990f763b8c5e900b
11cd541511cc793e7416655cda1e100d0a70fb043dfe7f6664564b91733431d0
759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6
3ac11a74275725a22c233cd974229d2b167c336da667410f7262b4926dabd31b
9ae72114b4cd0b293dee6c5edda7ef5e4d57a3aedad9c71c0e9de659d000e045
c8f39b13b5d6952c853c4b9fd63d1a1cc2acaf01fd97185761894d1634ba0a38
1d23f9189364f4b938eb298c625c5da21020d51fd08470bc83ba13b9db186e84
f22f6d8b198d38c1b9cc1b37fe7627f7d4422e6d105a157d6baa62e943a9de80
53aef1e8b281a00dea41387a24664655986b58d61d39cfbde7e58d8c2ca3efda
b036212a83d8fc3935bab35fdaee804b5e6e3fb5324efa9469fef4e31f8615f0
73bea810827bcf071190cfa4c6046b846be8f2745c88f974606aad8428ecd9f6
5162470ebb9bb040d646a371be5cd421b21f3d3278cdb48199f1bd2bbfb43bd5
4140ccb52192cab46aab4792eb6106e88f83bbe29837771dcf0ef072c22749eb

9a061e3322aecbd9bd3566ddd46b7bd89569f380896f2cc118bd2d34171be99a
1a64c805739aa64b2e38f00c7887e80afdaaf82e719d892d08aebf72e3a52760
56186b228b86bd92de3263d04036a17b22d89bdaa230e6cd61c16bce7a52c8b0
bbadbdf1e0ba6303b581b8b55cae125da47f922744731db533a020284f7f41c4
24b295dd5f5a10d318844170911b127f1d3a7a95bacabc11c26241f7d29b0c3f
e9cd6bf375c2ff5b1f6baa2cf04b11c65f1472ed27302275f68445a17001a38b
af80b82b14b7c18ce184937620078f3703a9b3a71299bd4de7a5b0cce06b98a1
0b6e96edab66aaeb9b3912cd511b6aeea852e33453796226db36dce7bdf0f38d
27f8bab18136a805d4e1efa88bb4546929862c1ef7c6ad307a6662e18af939cd
cd220cdffe907283ee8c722d50367da8dd190a289135225e2fef8bf322e6d6b2
018a3fbea5a8a5c0d2680428ae48ba865c4c88cb809e6875208368f5d016a51b
7f4e4cc382af5d87b5d74fc7c3226652ee5748bd1de55466b5d36a70018b2460
d7c12acb306b5100a5497586942b68a8f6d5deb353083da594caba2523c3171f
1d3970df043761627f2ac63a01550074a0ef137d408c0f029fecb1481b820f93
e1a5637cf7c8a41a53fa5e6de9d623bf1f12fecacd295a80ab79134e1da158be
cb5e9eea00406d53f6620ca94fd2014f5fe54f74013115ff984ba97a4e6bbcf6
9e20d9d1b59370ac0d1d0f0f8c8a0927569e0b4219765d58aacdc4817d130bdc
dcc79262d318874ead4ea331dffe0eeac32b191733dfbd2f1aab97c970419c1a
331b06ce8b9d06f01102e8fccbf0205576feaff65803102b17a7e95233ca2d7b
7d2dd600a6255780aef39717b9dd500ba3eea25dca8cf332247abf18479f608b
8c128664ccbdc245969f541f406109295fee661622d507079c5bc31775ce5dcb
979c14f993a1cd91f1b890f93a59ab5b14e059e056b9cf069222f529e50a4d5f
11fab8361a942e46375bd5ac259146fda20608594e265bcc1d3c011ab4c17226
e355a327479dcc4e71a38f70450af02411125c5f101ba262e8df99f9f0fef7b6
030e1f6b82a8c4a63b9754585b73a8f98c129234707ebdbd401020c068838262
0f3c57f3944563c8a653b1a828f494c599655f2af16b57cb131bfd00ec993f45
32a45243118ef2ff15b0055c046f77d53c43ca958383d235e00ae3f29aeb4944
6e3f2b4e69a2e88ef13df8697c12187c482044367e4f1930e70d78a5db0628af
38949635b0d6de1388df80c2d3d45e9c877ff1b796d50929f213c5736b3872dd
ecb835d03060db1ea3496ceca2d79d7c4c6c671c9907e0b0e73bf8d3371fa931
be95e21f1a04b9d41101afb9cb43ea239a8d8cd11772be1681ee2c16fffdf5a2
99c84b8e063bdfdd07f39f2fac1fee4a68204e97283c60c7524cdacbf392729d
72aa4905598c9fb5a1e3222ba8daa3efb52bbff09d89603ab0911e43e15201f3
142287861c2322646c185b5092a1e7176a63a4d4909f03ae88446c7ff1fde105
ac9aea57da03206b1df12b5c012537c899bf5d67a5eb8113b4a4d99e0a0eb893
378aaaeaf2dcbaf5e2247b0f94ce8e584cec7645817a4df2e8357d0c7c41fe72
9e38d9831e52968e919a298830c169f89940ee1303ec4ea62fe8cc11c0e8072a
bb9a40db67fab5fcc89f5f90fb7c00f515a997cd46b5be378660017bbbd0b45a
8ac4e164b463c313af059760ce1f830c19b0d5a280ec80554e8f77939143e24e
06d4289b929b7aee66fa19baada10956535123c22cf6a6371ff4fbeac9a0ed9b
9080e7503e637ad4bef5a3f0232e31ad9a8ce4e498e5f53c2a55dede26fbfed5
6a01538e8dfa294f1b67e09e8f8b3e6bc13e14496b892d26b8390b8efb36464f
1aa4ad5a3f8929d61f559df656c84326d1fe0ca82a4be299fa758a26e14b1b27

eae62bb4110bcd00e9d1bcaba9000defcda3d1ab832fa2634d928559d066cb15
269908e1b76afaf1d837bce28640a1066808aaac29e6bc6575581dcc907065d0
d2aaadea32c3bc0b8cc43afe20e7be6aff1b3c8949edee51a765e7d464fbad4c
9e7adadbd6d7e3ebf79d81c822156073dcbd22119bcbcbe21d32f33fc16cef00
c717752733bf64c08ed9b32fb91719ad3e58910301d5511822a2ee5458c8f579
463dfc9ce5587504d8bb659cc350be919e20bb24a005f1572309a3b45ad00764
d558fa8a78a2e87e0665bf721f46b47b056f00f8097d0d5e1257b392f223010e
e68185412a5127d2a942ad2d6ff7b7ce7a0e4cabc35ecb01e25383f0b9552ac5
1932665c71ad9b0b0bfa8166dbcd874b1c1766101a4e8cb92945c9271a7c6eda
b155f2f6dec39d9a37cf91decc8e43eb62c9b5ece7ce293dbb7d219eb28d7a22
47b1e69cffc3fd4ce44b2bff72323366e0f25c3aa50caca399933372f9b7d172
d90005bebaf62fcc2056e9368ac3dcdc8b278cdbb2185079c3f5a81d2285815f
97564a1984159320080a4d2dd1e877b1906b18ae36e3d13290fb49171b61eabd
c662ef7f25deef5387f904ae303c395db061ab3d10c945349b513ae31637235b
68b1974d3bfe4b85f25b157467c7a9e036628dd104e454ba4b008ab78a844b2f
e8e78cc9fec87983a6bd1ab6c76347c6ffd91729d3dd629646391ee9e55f94d7
6fcf4592f9261d5734fb3b8534f6839ab65f68fd9ff14a9005225135e743226c
5fab4d08348b4ef080ba91bdb0d769d31797f5092bff3b24b3c23d091fccc8a7
4305214c4d9cf9e3c44962b5903db0032a9f4e4b4a2ee3d497887abed3b4ffe1
9fb79a84500d44f03dd849fc488993e92096a03366c94c04a980ec88eeaeb61c
10a9a217d3b53a3e43ec03b81a026f7a70350a062b900d672353690090e1ade6
8000fc697902cf7763f1fee2a5913f24371ad2ea62b5ba73f41c3d718a2cfce8
244813c64d5e5c350ca47e5792971c7aaa787fc86b7c88cf5b09bf900e78b794
e4b1669e99bb75af5c1cf01c0e5055404cf86f74be10af58df38deb559816cdc
84d24309d43d7daf0ef253b8c1ab779a7055c78119acae3c77b7487697457599
aa971a55dff2b37dc3cdb133fb50f7065644daa221902e2250df94e058145495
7c0132c7d0ce7ca0f0edb6c84ec93278b44eb05882af43759ffcdc07f7e4b96c
32a72f7acd9425035e68c53d4033abd27403344ec44bafbdf9e311acc436ce3f
5bd8475916ad66d317211e307664c1949e0e9496e441133571a0e28cb5982e00
786dbd28d1c94e28f8bae3e34c3cd7fefdbe4079c7f6fddbb8088dcd03bcd939
36261291ea15cccb3924615851f18f2047aeaa3858b3d1b90d8223e4f295e1d4
24a5d0dc380cec89040050838706354054 7d45851cbf2f0a0bda3d2ab6300890
e9ea627e7a6d5e79ca9568504796091c136435159000ec7966f0eaebd935c306
657c83297cfcc5809e89098adf69c206df95aee77bfc1292898bbbe1c44c9dc4
c07d30c0b69e11bae9f700187f2ca2473918142905fa258f1c6b52986087e3c7
b89f62041e18ec400082084017d084174abfdc33150c8a6e6b92642c778eb02a
9da9bbe505ab7bd45cbefadb96b21d5a8e7e7e9abdf5597e937a8ac3ba32f7d6
b94a24b922ef634da3d220015ca5b86219c04990a3906d65122cb3c566f851b9
d7f863bf1bec7cecaf08fb9871a3025f0d0e93b325b8735f53021401022e3efc
6f72632394b89daff89f08488081f782d63c1f01e0033cec693fd5c895965b80
6b57c77a9f2d8501f34097b60ae0d455186eeecb615e40df1bf48e597ba0a729
8cccdce85beca7b7dc805a7f048fcd1bc8f7614dd7e13c2986a9fa5dfbbbbdf9
0a842c40cdbbbc2bf5a6513e39a2bd8ea266f914ac93c958fda8c0d0048c4f94

25ff92ed61208513c0aec27cd3b4864f8f4604960a58d59310ec64a8706fb6f1
87cb32ed90846db823b2c1a8711f91d023dcd165f37302e3a648acda033ca1fd
340130ef9b7faf101e0d901d8eb9181a8165ba1b0a346376a59067286b7d26af
bb6adcc061e950dc0e3d524b191f2eebf38d16619cdbb16cb62e8960995b0a4f
21103415da2ec9ffc792e91f54468f86bc79d9784b33a3dff79c6a6f2cc8b120
b4064721d911e9606edf366173325945f9e940e489101e7d0747103c0e905126
5a414a39851c4e22d4f9383211dfc080e16e2caffd90fa06dcbe51d11fdb0d6c
69940a20ab9abb31a03fcefe6de92a16ed474bbdff3288498851afc12a834261
57d230ddaf92e2d0504e5bb12abf52062114fb8980c5ecc413116b1d6ffedf1b
03cb76bdc619fac422d2b954adfa511e7ecabc106adce804b1834581b5913bca
c2551c4e6521ac72982cb952503a2e6f016356e02ee31dea36c713141d4f3785
dfa8a85e26c07a348a854130c652dcc6d29b203ee230ce0603c83d9f11bbcacc
aeeab3272a2ed2157ebf67f74c00fafc787a2b9bbaa17a03be1e23d4cb273632
fbd5c2cf1c1f17402cc313fe3266b097a46e08f48b971570ef4667fbfd6b7301
be1cfa10fcf2668ae01b98579b345ebe87dab77b6b1581c368d1aba9fd2f10a0
12572c2fc2b0298ffd4305ca532317dc8b97ddfd0a05671066fe594997ec38f5
a4a455db9f297e2b9fe99d63c9d31e827efb2cda65be445625fa64f4fce7f797
b40cbf38284e6a1b9157002ad564e40fad2d85ba36437cf95c3b6326ad142520
B8CEB1EF2AA64B0C1FA7F8E07D903AD61590D5879B1AF4F0AABA40576875D648
c261a90bcc8b2e3810c1d2db6379a6a8e74b942bfecfe79e8815a5cd025e6455
58b223f74992f371cab8f1df7c03b9b66f2ea9e3c9e22122898a9be62a05c0b4
8c47961181d9929333628af20bdd750021e925f40065374e6b876e3b8afbba57
80548416ffb3d156d3ad332718ed322ef54b8e7b2cc77a7c5457af57f51d987a
b40909ac0b70b7bd82465dfc7761a6b4e0df55b894dd42290e3f72cb4280fa44
1422636dd3e4abdb0a9f89b9c14069e4ab4cdbfdc543cd65e1712c4f384b0181
0cac1ecffbd281f570196257f1e49993a640f757df43aed20b64277b034a9ffc
12879b9d8ae046ca2f2ebcc7b1948afc44e6e654b7f4746e7a5243267cfd7c46
18b5f5098747530e39570f5230cfbb1298c2a5a136c22150e2bd4322584e1bac
2631f95e9a46c821a701269a76b15bb065764cc15a0b268a4d1eac045975c9b8
0be114fe30ef5042890c17033b63d7c9e0363972fcc15a61433c598dd33f49d1
468b11cbd5710e6a2c7b9ff9409f8310f1cd59707e39b73cf21cb690cca8b287
8f88f1d0670e0db0b2ca1f73cb9b8008b4e581745148d7b084932507f69471f8
7f698295230f59c7ca8193322eb48d71cd203f3675139f2da99e326589bfdad3
6449d0cb1396d6feba7fb9e25fb20e9a0a5ef3e8623332844458d73057cf04a1
d5d9210ef49c6780016536b0863cc50f6de03f73e70c2af46cc3cff0e2bf9353
d61350d77b7762bfe9ecb1d0a660c69d9854192ab69967743c3d86cd2623b7f9
3c93800b31bf6c2897ce2d8ce363c33f3a9cf468adfaa5b0c507de6084970b49
1c12cf14d3dbdefd069635d57673258839bf95407674bea01f8d8f9801560dde
07e0b509288c501c57cc8f11b88ac8c06e379b01b74cd910d93cfdff1f9dd7ec
e39aa9b3c9b95311fe951541f733972858fe724fb5265247f2b6b37ff97356ef
7dd063acdfb00509b3b06718b39ae53e2ff2fc080094145ce138abb1f2253de4
1b3dd8aaafd750aa85185dc52672b26d67d662796847d7cbb01a35b565e74d35
0cccb9d951ba888c0c37bb0977fbb3682c09f9df1b537eede5a1601e744a01ad

cb630234494f2424d8e158c6471f0b6d0643abbdf2f3e378bc2f68c9e7bca9eb
91f750f422fd3ff361fabca02901830ef3f6e5829f6e8db9c1f518a1a3cac08c
fc2dbfda41860b2385314c87e81f1ebb4f9ae1106b697e019841d8c3bf402570
bebe0be0cf8349706b2feb789572e035955209d5bf5d5fea0e5d29a7fbfdc7c4
02c7cf55fd5c5809ce2dce56085ba43795f2480423a4256537bfdfda0df85592
fb3a3339e2ba82cb3dcdc43d0e49e7b8a26ced3a587f5ee15a256aee062e6e05
99d3f03fc6f048c74e58da6fb7ea1e831ba31d58194ad2463a7a6cd55da5f96b
24e11c80f1d4c1e9db654d54cc784db6b5f4a126f9fe5e26c269fdc4009c8f29
4dd8ab2471337a56b431433b7e8db2a659dc5d9dc5481b4209c4cddd07d6dc2b
5f6b2a0d1d966fc4f1ed292b46240767f4acb06c13512b0061b434ae2a692fa1
b23193bff95c4e65af0c9848036eb80ef006503a78be842e921035f8d77eb5de
07393ac2e890772f70adf9e8d3aa07ab2f98e2726e3be275276dadd00daf5fc6
ea957d663dbc0b28844f6aa7dfdc5ac0110a4004ac46c87d0f1aa943ef253cfe
378ef276eeaa4a29dab46d114710fc14ba0a9f964f6d949bcbc5ed3267579892
6bbec6b2927325891cc008d3378d30941fe9d21e5c9bd6459e8e3ba8c78833c2
37bf2c8118429723145956434449fd294e793b43c1a7b37cfe41af4fcc07d329d
ba1c02aa6c12794a33c4742e62cbda3c17def08732f3fbaeb801f1806770b9a0
a9dc96d45702538c2086a749ba2fb467ba8d8b603e513bdef62a024dfeb124cb
8c488b029188e3280ed3614346575a4a390e0dda002bca08c0335210a6202949
a979c5094f75548043a22b174aa10e1f2025371bd9e1249679f052b168e194b3
c6a9db52a3855d980a7f383dbe2fb70300a12b7a3a4f0a995e2ebdef769eaaca
1c8869abf756e77e1b6d7d0ad5ca8f1cdce1a111315c3703e212fb3db174a6d5
d2e947a39714478983764b270985d2529ff682ffec9ebac792158353caf90ed3
54c4ce98970a44f92be748ebda9fcfb7b30e08d98491e7735be6dd287189cea3
68065abd6482405614d245537600ea60857c6ec9febac4870486b5227589d35c
e031299fa1381b40c660b8cd831bb861654f900a1e2952b1a76bedf140972a81
8bca0031f3b691421cb15f9c6e71ce193355d2d8cf2b190438b6962761d0c6bb
2c81023a146d2b5003d2b0c617ebf2eb1501dc6e55fc6326e834f05f5558c0ec
c19d266af9e33dae096e45e7624ab3a3f642c8de580e902fec9dac11bcb8d3fd
d0e019229493a1cfb3ffc918a2d8ffcbaee31f9132293c95b1f8c1fd6d595054
715f69916db9ff8fedf6630307f4ebb84aae6653fd0e593036517c5040d84dbe
dd8facad6c0626b6c94e1cc891698d4982782a5564aae696a218c940b7b8d084
fd8b2ea9a2e8a67e4cb3904b49c789d57ed9b1ce5bebfe54fe3d98214d6a0f61
d403ded7c4acfffe8dc2a3ad8fb848f08388b4c3452104f6970835913d92166c
20ac1420eade0bdb464cd9f6d26a84094271b252c0650a7853721d8e928f6e6c
a2c9041ee1918523e67dbaf1c514f98609d4dbe451ba08657653bb41946fc89d
1289ee3d29967f491542c0bdeff6974aad6b37932e91ff9c746fb220d5edb407
ddab96e4a8e909065e05c4b6a73ba351ea45ad4806258f41ac3cecbcae8671a6
dea4e560017b4da05e8fd0a03ba74239723349934ee8fbd201a79be1ecf1c32d
94c220653ea7421c60e3eafd753a9ae9d69b475d61230f2f403789d326309c24
972e907a901a7716f3b8f9651eadd65a0ce09bbc78a1ceacff6f52056af8e8f4
82c4e9bc100533482a15a1d756d55e1a604d330eff8fbc0e13c4b166ac2c9bd3
ec2f14916e0b52fb727111962dff9846839137968e32269a82288aee9f227bd4

d2a6064429754571682f475b6b67f36526f1573d846182aab3516c2637fa1e81
c9ef265fc0a174f3033ff21b8f0274224eb7154dca97f15cba598952be2fbace
60ee6fdca66444bdc2e4b00dc67a1b0fdee5a3cd9979815e0aab9ce6435262c6
ef027405492bc0719437eb58c3d2774cc87845f30c40040bbebbcc09a4e3dd18
c4be15f9ccfecf7a463f3b1d4a17e7b4f95de939e057662c3f97b52f7fa3c52f
522fd9b35323af55113455d823571f71332e53dde988c2eb41395cf6b0c15805
e5511b22245e26a003923ba476d7c36029939b2d1936e17a9b35b396467179ae
efb235776851502672dba5ef45d96cc65cb9ebba1b49949393a6a85b9c822f52
87bffb0370c9e14ed5d01d6cc0747cb30a544a71345ea68ef235320378f582ef
1228e9066819f115e8b2a6c1b75352566a6a5dc002d9d36a8c5b47758c9f6a45
e7dd9678b0a1c4881e80230ac716b21a41757648d71c538417755521438576f6
15486216ab9c8b474fe8a773fc46bb37a19c6af47d5bd50f5670cd9950a7207c
e53bd956c4ef79d54b4860e74c68e6d93a49008034afb42b092ea19344309914
0cd9ac328d858d8d83c9eb73bfdc59a958873b3d71b24c888d7408d9512a41d7
539cdc37c34eebb28a74f0dceeee0331e6ac6f4682e55fddd69d6f9de7ab9b77
3f48dbbf86f29e01809550f4272a894ff4b09bd48b0637bd6745db84d2cec2b6
6d626c7f661b8cc477569e8e89bfe578770fca332beefea1ee49c20def97226e
06976912957d4c0c7f5d3a478fc8f3dc2ef1057537bc1548554d6569add2ba3d
060448ffd71fe2edbb5fe7c6298ad2b077e57fa6ed6d4250fbd799dd85488843
7ea33696c91761e95697549e0b0f84db2cf4033216cd16c3264b10daa31f598c
fa8de430fb491d898ee4e557977f036f2aae5f019c3b0552c9e0223da748fc27
fc28ad61fc748c08e8714cb247e741b736ebf0d9dfbcc3579f66fe3168326f61
430cbf950f9cea3f77374145f488a104f4ab664edca448effacbf2f8ba01b901
a97b1a792f7b53929a1c01bad9fc2bd606a15e8e32755daa15570e356baa0112
634795a3acbae8964bb31e3ebed7f29208844978a512fc26a8b9a51901f9cab9
37f15647c26d475db805048d6592aa153533ac5f4373145c75e24012a51ad9f8
27dd9de09e22efa2ef12e9e2f462fa9da83684bdb4ec900dd86439c5758107d9
aa5b25c969234e5c9a8e3aa7aefb9444f2cc95247b5b52ef83bf4a68032980ae
e029ed8cfe34185c94b15c74f52d6fdf9bf9b635853c466b2589c1d9f3639200
a6d83fb30af84c18edf829ae4cc29c8c1bfb5eaaf61f9579d2d79c27bd37db59
81e96c07e6c9cb02f72c0943a42ff9f8f09a09c508f8bbaa1142a9ee4f1326cf
0860f29226069a732f988cb70ea6d51057d204d421bb709b8e759376b0c4d201
eb4e174db15646f71cb1d2c471e5794a8429ca29369c8eff6042122cc6dc6845
500f426f98d4c00d29825f976b9457a274aed781a560a60e89cba4805cd47186
d0e9f0c79da838bd71a1c4ba6c5c9382569941dc38e7fa2c92009b364673d498
dcbfd12321fa7c4fa9a72486ced578fdc00dcee79e6d95aa481791f044a55af3
fcf03bf5ef4babce577dd13483391344e957fd2c855624c9f0573880b8cba62e
d77eb89501b0a60322bc69692007b9b7f1b5a85541a2aaf21caf7baf0fe0049e
b6b2f6aae80cba3fa142bd216decc1f6db024a5ab46d9c21cf6e4c1ab0bbe58b
88570857cd702409c712aa6e35513ea3a9de91ac42f8f1268faea46d34bc6874
a84852f83beed2db7772c5d9705ac5546623e1bf39e096900dd7d2b3f5b38914
e6e93c7744d20e2cac2c2b257868686c861d43c6cf3de146b8812778c8283f7d
f36a0ee7f4ec23765bb28fbfa734e402042278864e246a54b8c4db6f58275662

43c65d87d690aea7c515fe84317af40b7e64b350304b0fc958a51d62826feade
61c2e524dcc25a59d7f2fe7eff269865a3ed14d6b40e4fea33b3cd3f58c14f19
d444fde5885ec1241041d04b3001be17162523d2058ab1a7f88aac50a6059bc0
2060f1e108f5feb5790320c38931e3dc6c7224edf925bf6f1840351578bbf9cc
e3894693eff6a2ae4fa8a8134b846c2acaf5649cd61e71b1139088d97e54236d
83fbd76d298253932aa3e3a9bc48c201fe0b7089f0a7803e68f41792c05c5279
fe00bd6fba209a347acf296887b10d2574c426fa962b6d4d94c34b384d15f0f1
4c1b8d070885e92d61b72dc9424d9b260046f83daf00d93d3121df9ed669a5f9
770206424b8def9f6817991e9a5e88dc5bee0adb54fc7ec470b53c847154c22b
31577308ac62fd29d3159118d1f552b28a56a9c039fef1d3337c9700a3773cbf
3fd45b9b33ff5b6363ba0013178572723b0a912deb8235a951aa3f0aa3142509
50b000a7d61885591ba4ec9df1a0a223dbceb1ac2facafcef3d65c8cbbd64d46
c4a61b581890f575ba0586cf6d7d7d3e0c7603ca40915833d6746326685282b7
cbd9cb7b69f864ce8bae983ececb7cf8627f9c17fdaba74bd39baa5cdf605f79
b61e0f68772f3557024325f3a05e4edb940dbbe380af00f3bdaaaeabda308e72
abf0c2538b2f9d38c98b422ea149983ca95819aa6ebdac97eae777ea8ba4ca8c
3384a9ef3438bf5ec89f268000cc7c83f15e3cdf746d6a93945add300423f756
6fb2facdb906fc647ab96135ce2ca7434476fb4f87c097b83fd1dd4e045d4e47
c8b6291fc7b6339d545cbfa99256e26de26fff5f928fef5157999d121fe46135
faf8db358e5d3dbe2eb9968d8b19f595f45991d938427124161f5ed45ac958d5
0b94e123f6586967819fa247cdd58779b1120ef93fa1ea1de70dffc898054a09
45bf0e2037b43478e39a06ab23ac5d7a7156c37f8dc38e8da482078bdfe672c5
eb81c1be62f23ac7700c70d866e84f5bc354f88e6f7d84fd65374f84e252e76b
fae335a465bb9faac24c58304a199f3bf9bb1b0bd07b05b18e2be6b9e90d72e6
e6e19633ba4572b49b47525b5a873132dfeb432f075fbba29831f1bc59d5885d
b45dc885949d29cba06595305923a0ed8969774dae995f0ce5b947b5ab5fe185
aac3b1221366cf7e4421bdd555d0bc33d4b92d6f65fa58c1bb4d8474db883fec
3b548a851fb889d3cc84243eb8ce9cbf8a857c7d725a24408934c0d8342d5811
2bf088955007b4f47fe9187affe65fffea234ff16596313a74958a7c85129172
07b2d21f4ef077ccf16935e44864b96fa039f2e88c73b518930b6048f6baad74
ee7cfc55a49b2e9825a393a94b0baad18ef5bfced67531382e572ef8a9ecda4b
d9e7325f266eda94bfa8b8938de7b7957734041a055b49b94af0627bd119c51c
1e8261104cbe4e09c19af7910f83e9545fd435483f24f60ec70c3186b98603cc
1dd03c4ea4d630a59f73e053d705185e27e2e2545dd9caedb26a824ac5d11466
c213b60a63da80f960e7a7344f478eb1b72cee89fd0145361a088478c51b2c0e
a442135c04dd2c9cbf26b2a85264d31a5ac4ec5d2069a7b63bc14b64a6dd82b7
d494e9f885ad2d6a2686424843142ddc680bb5485414023976b4d15e3b6be800
96a19a90caa41406b632a2046f3a39b5579fbf730aca2357f84bf23f2cbc1fd3
1f22e8f489abff004a3c47210a9642798e1c53efc9d6f333a1072af4b11d71ef
227b7fe495ad9951aebf0aae3c317c1ac526cdd255953f111341b0b11be3bbc5
45a93e4b9ae5bece0d53a3a9a83186b8975953344d4dfb340e9de0015a247c54
2a06f142d87bd9b66621a30088683d6fcec019ba5cc9e5793e54f8d920ab0134
cffa1d9fc336a1ad89af90443b15c98b71e679aeb03b3a68a5e9c3e7ecabc3d4

c1b8fc00d815e777e39f34a520342d1942ebd29695c9453951a988c61875bcd7
4405cfbf28e0dfafa9ea292e494f385592383d2476a9c49d12596b8d22a63c47
651d5aab82e53711563ce074c047cbaa0703931673fa3ad20933d6a63c5c3b12
68df0f924ce79765573156eabffee3a7bb0fa972d2b67d12dd91dea3ec255d24
d06be83a408f4796616b1c446e3637009d7691c131d121eb165c55bdd5ba50b4
cac630c11c4bf6363c067fbf7741eae0ec70238d9c5e60d41f3ed8f65b56c1d1
ecc5805898e037c2ef9bc52ea6c6e59b537984f84c3d680c8436c6a38bdecdf4
65de07fc6b821d9fd3497cfa64212df2d39935dd515a86eda80d08086b183a3f
cd925e2464d251f02b4d425e301acf276e13eeccbbf5996ade5a6f355802abb7
4a4ccda8e1832c6dec2d4f4adbf6a087fab86b8c316719e5178c3cf9bef4e1ac
8d10fd18de90829eccc33e79b92987bc33999403a1f7e2766903d21d38a247a9
f93b89a707c647ba492efe4515bb69a627ce14f35926ee4147e13d2e030ab55b
ca8087d1ec75ac6fcbad918c8f6559612b7cf8633e29bbcb3bbc8a9cbc793801
02e6eb920ed21a73c7d7d0dc3758b434f541d02939d9aa8458227761e90f6162
b9f3af84a69cd39e2e10a86207f8612dd2839873c5839af533ffbc45fc56f809
87f363afc9778efc78dd3e0ced112d8d66a09a8924091f0927ed02a7b64850d2
90926500594d9cdb194bd10da8b62e37591ad92ca890846594de35e952919bcb
34bdb5b364358a07f598da4d26b30bac37e139a7dc2b9914debb3a16311f3ded
346e5dc097b8653842b5b4acfad21e223b7fca976fb82b8c10d9fa4f3747dfa0
07646dc0a8c8946bb78be9b96147d4327705c1a3c3bd3fbcedab32c43d914305
c20e5d56b35992fe74e92aebb09c40a9ec4f3d9b3c2a01efbe761fa7921dd97f
0d7b945b9c912d205974f44e3742c696b5038c2120ed4775710ed6d51fbc58ef
2cfc4b3686511f959f14889d26d3d9a0d06e27ee2bb54c9afb1ada6b8205c55f
f1e2bceae81ccd54777f7862c616f22b581b47e0dda5cb02d0a722168ef194a5
6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a
abfc14f7f708f662046bfcad81a719c71a35a8dc5aa111407c2c93496e52db74
86bb3b00bcd4878b081e4e4f126bba321b81a17e544d54377a0f590f95209e46
7b4193ea92ddf122a03e51be4645bc72cbd8ad427e992cc61ac594f8d1450261
03ff895c99555f00792a41e3b014f16ef6b4bb0c74d1fa2237a6a9275e2b2109
3d2a7dc27d2b8d4ea86a1eab74877acf7d2768354f1a76d99ee98589b2b7e2bc
5173721f3054b92e6c0ff2a6a80e4741aa3639bc1906d8b615c3b014a7a1a8d7
9a0f00469d67bdb60f542fabb42e8d3a90c214b82f021ac6719c7f30e69ff0b9
b41480d685a961ed033b932d9c363c2a08ad60af1d2b46d4f78b5469dc5d58e3
40318f3593bca859673827b88d65c5d2f0d80a76948be936a60bda67dff27be9
a23261e2b693750a7009569df96ec4cf61e57acc9424c98d6fe1087ff8c659ce
77ff53211bd994293400cb3f93e3d3df6754d8d477cb76f52221704adebad83a
e5aece694d740ebcb107921e890cccc5d7e8f42471f1c4ce108ecb5170ea1e92
b48b3d46ebfa6af8a25c007f77e6ed3c32fe4c6478311b8b0c7d6f4f8c82de76
93680d34d798a22c618c96dec724517829ec3aad71215213a2dcb1eb190ff9fa
fc69fb278e12fc7f9c49a020eff9f84c58b71e680a9e18f78d4e6540693f557d
5a02d4e5f6d6a89ad41554295114506540f0876e7288464e4a70c9ba51d24f12
ed8f52cdfc5f4c4be95a6b2e935661e00b50324bee5fe8974599743ccfd8daba
af77e845f1b0a3ae32cb5cfa53ff22cc9dae883f05200e18ad8e10d7a8106392

50d610226aa646dd643fab350b48219626918305aaa86f9dbd356c78a19204cc
3c7fb61f0601f9facd3c2a1b319039a3fad6535b33359493b8a8a3f24dea00e3
56e2221cddc9b12cd1021f4da804e52658e515082c8600b6ae77fe628247e002
427b9130cca7217692673fb0e9017cbc61dc295fcde381360cc893f6e96e4092
001cf7af29382f4f784fe45df131ca9e14908c6c0717899780f9354b8a5f0090
ceeb9b227d6ac68aba1fdd18625d3b8e87d4bc1c2aa50a5ad106b093225ed651
215f7c08c2e3ef5835c7ebc9a329b04b8d5215773b7ebfc9fd755d93451ce1ae
2da5a388b891e42df4ed62cffbc167db2021e2441e6075d651ecc1d0ffd32ec8
c91843a69dcf3fdad0dac1b2f0139d1bb072787a1cfcf7b6e34a96bc3c081d65
861b6bc1f9869017c48930af5848930dd037fb70fc506d8a7e43e1a0dbd1e8cb
174effcdeec0b84c67d7dc23351418f6fa4825550d595344214cc746f1a01c1a
79bd5f34867229176869572a027bd601bd8c0bc3f56d37443d403a6d1819a7e5
72227c531de0c8198399f712157d2039c9cb205b507dcc67c03f43b480e1f34c
cda841969847c626f9e477b5edfb6522ebbeabe055c4a0acce570d9d2922bb94
78adc8e5e4e86146317420fa3b2274c9805f6942c9973963467479cb1bbd4ead
054c5aa73d6b6d293170785a82453446429c0efc742df75979b760682ac3026b
5749eb9d7b8afa278be24a4db66f122aeb323eaa73a9c9e52d77ac3952da5e7d
de660457cab011deedf4c1a142021b8702ab94ce71dc5e0c75300253e7db3ee0
7cb0bb528dca188ae73d66d8739bd9d2bf04a6c7e5c805e9b3b92858eb118bf4
04bd6c3d9fa30b4d9410b89ba44c9e29aab22a1345115e8eef9cddc86d1eea25
e8b59ff8c1d206d42b89b4d7e9340526ad2d1c5c85d75ff9bb62af1a9ef40362
1803cca4f6a77dfbd5891d691cb89582d8d7d95c10c90b75fee2cab1ea59d726
d21318282e6c8d888b686fb61d87891fff4df575a8a84ea1d2784c0445409cdc
2832b7000869786e94dc3314f0e69d0129aa2925bca54cfd64858a2d71e12efa
6519c4a26c589ec30d4b9d6212d8a7b9046ab7ec377ff2ed6a1d2a64e139c527
d93f22d46090bfc19ef51963a781eeb864390c66d9347e86e03bba25a1fc29c5
3d13f2e5b241168005425b15410556bcf26d04078da6b2ef42bc0c2be7654bf8
3f2d8744205b59f7bee5a8f13e6a15201f04663ce2c6f33b1684968778e44349
461f5340f9ea47344f86bb7302fbaaa0567605134ec880eef34fa9b40926eb70
b0f1f553a847f3244f434541edbf26904e2de18cca8db8f861ea33bb70942b61
7313eaf95a8a8b4c206b9afe306e7c0675a21999921a71a5a16456894571d21d
41f222b8bb932e177cdb833e941158fcaa142fbc0e33df2991828337a99ce47b
81f0f5fcb3cb8a63e8a3713b4107b89d888cb722cb6c7586c7fcdb45f5310174
9392776d6d8e697468ab671b43dce2b7baf97057b53bd3517ecd77a081eff67d
684f4b9ea61e14a15e82cac25076c5afe2d30e3dad7ce0b1b375b24d81135c37
b3d624c4287795a7fbddd617f57705153d30f5f4c4d2d1fec349ac2812c3a8a0
77166146463b9124e075f3a7925075f969974e32746c78d022ba99f578b9f0bb
342e1f591ab45fcca6cee7f5da118a99dce463e222c03511c3f1288ac2cf82c8
970cbb11516643a714a92db4d981f8ca9c7398313d86bffbdbe227c91c290067
dd2c989e93ae3d0ab9f43991eee33c7e4cf8794ab469196dccc7c26dd2a1411a
c3b2c7bbd2aa1e3100b9382ed78dfa0041af764e0e02013acdf282410b302ead
2e75deac828111d224c2e6f08662a25e6ccf1c2b7aa938d8d35ae08560ae278a
91acb0d56771af0196e34ac95194b3d0bf3200bc5f6208caf3a91286958876f9

2a652721243f29e82bdf57b565208c59937bbb6af4ab51e7b6ba7ed270ea6bce
ae0bc3358fef0ca2a103e694aa556f55a3fed4e98ba57d16f5ae7ad4ad583698
12331809c3e03d84498f428a37a28cf6cbb1dafe98c36463593ad12898c588c9
04e1772997b884540d5728a2069c3cc93b8f29478e306d341120f789ea8ec79e

List of CVE commonly exploited by APT28:

CVE-2016-7855

Use-after-free vulnerability in Adobe Flash Player before 23.0.0.205 on Windows and OS X and before 11.2.202.643 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in October 2016.

CVE-2016-7255

The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."

CVE-2014-1761

Microsoft Word 2003 SP3, 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT; Word Viewer; Office Compatibility Pack SP3; Office for Mac 2011; Word Automation Services on SharePoint Server 2010 SP1 and SP2 and 2013; Office Web Apps 2010 SP1 and SP2; and Office Web Apps Server 2013 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted RTF data, as exploited in the wild in March 2014.

CVE-2012-0158

The (1) ListView, (2) ListView2, (3) TreeView, and (4) TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Controls in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0 Runtime allow remote attackers to execute arbitrary code via a crafted (a) web site, (b) Office document, or (c) .rtf file that triggers "system state" corruption, as exploited in the wild in April 2012, aka "MSCOMCTL.OCX RCE Vulnerability."

CVE-2016-4117

Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in May 2016.

CVE-2016-1019

Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors, as exploited in the wild in April 2016.

CVE-2015-7645

Adobe Flash Player 18.x through 18.0.0.252 and 19.x through 19.0.0.207 on Windows and OS X and 11.x through 11.2.202.535 on Linux allows remote attackers to execute arbitrary code via a crafted SWF file, as exploited in the wild in October 2015.

CVE-2017-11292

Adobe Flash Player version 27.0.0.159 and earlier has a flawed bytecode verification procedure, which allows for an untrusted value to be used in the calculation of an array index. This can lead to type confusion, and successful exploitation could lead to arbitrary code execution.

CVE-2015-3043

Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in April 2015, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, and CVE-2015-3042.

CVE-2015-1701

Win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2, Vista SP2, and Server 2008 SP2 allows local users to gain privileges via a crafted application, as exploited in the wild in April 2015, aka "Win32k Elevation of Privilege Vulnerability."

CVE-2015-1641

Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, and Office Web Apps Server 2010 SP2 and 2013 SP1 allow remote attackers to execute arbitrary code via a crafted RTF document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE-2017-0144

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

CVE-2013-1347

Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly allocated or (2) is deleted, as exploited in the wild in May 2013.

CVE-2013-3897

Use-after-free vulnerability in the CDisplayPointer class in mshtml.dll in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted JavaScript code that uses the onpropertychange event handler, as exploited in the wild in September and October 2013, aka "Internet Explorer Memory Corruption Vulnerability."

CVE-2014-1510

The Web IDL implementation in Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allows remote attackers to execute arbitrary JavaScript code with chrome privileges by using an IDL fragment to trigger a window.open call.

CVE-2014-1511

Mozilla Firefox before 28.0, Firefox ESR 24.x before 24.4, Thunderbird before 24.4, and SeaMonkey before 2.25 allow remote attackers to bypass the popup blocker via unspecified vectors.

CVE-2014-1776

Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::IsConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code leveraged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, effective workaround to help block known attacks."

CVE-2014-6332

OleAut32.dll in OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted web site, as demonstrated by an array-redimensioning attempt that triggers improper handling of a size value in the SafeArrayDimen function, aka "Windows OLE Automation Array Remote Code Execution Vulnerability."

CVE-2015-5119

Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.296 and 14.x through 18.0.0.194 on Windows and OS X and 11.x through 11.2.202.468 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.

CVE-2015-2590

Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2015-4732.

CVE-2015-4902

Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60 allows remote attackers to affect integrity via unknown vectors related to Deployment.

CVE-2010-3333

Stack-based buffer overflow in Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via crafted RTF data, aka "RTF Stack Buffer Overflow Vulnerability."

CVE-2017-0261

Microsoft Office 2010 SP2, Office 2013 SP1, and Office 2016 allow a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-0262 and CVE-2017-0281.

Advanced Persistent Threat (APT): PATCHWORK

The cybercrime group "PATCHWORK" (also known as Hangover, Dropping Elephant, MONSOON, Chinastrats, Quilted Tiger, Snake In The Grass, Viceroy Tiger, APT-C-09, TG-4410, Zinc Emerson, ATK 11, Neon, Confucius) has been active since at least 2013 and attacks organizations in industries connected with diplomatic missions and governmental entities. The group's aims are espionage and information theft.

Indicators of Compromise (IOCs)

CnC:

http://176[.]56[.]238[.]177/testing4/download/reg[.]exe
http://games-playbox[.]com/winone1/download/sppsvc[.]exe
http://176[.]56[.]238[.]177/testing2/download/winrm[.]exe
http://176[.]56[.]238[.]177/testing2/download/reg[.]exe
http://games-playbox[.]com/testing1/download/reg[.]exe
http://176[.]56[.]238[.]177/testing2/download/reg1[.]exe
http://176[.]56[.]238[.]177/testing2/download/sppsvc[.]exe
http://games-playbox[.]com/winone1/download/stisvc[.]exe
http://techto-earth[.]com/eastwing/download/sppsvc[.]exe
http://internet-security-suite-review[.]toptenreviews[.]com[.]infocardiology[.]biz
http://mail[.]telenor[.]no-cookieauth[.]dll-getlogon-reason-0[.]formdir-1-curl-z2fowaz2f[.]infocardiology[.]biz/01084204_Telenor_New_Satellite_Client_Agreement_30032013[.]zip
http://feed43[.]com/3210021137734622[.]xml
http://www[.]webrss[.]com/createfeed[.]php?feedid=49966
http://feeds[.]rapidfeeds[.]com/88604/
http://feed43[.]com/8166706728852850[.]xml
https://r0nald2017[.]wordpress[.]com/2017/02/16/my-first-post/
https://github[.]com/r0nald2017/project1/blob/master/xml[.]xml
http://mu5[.]ignorelist[.]com
http://d0nald2[.]strangled[.]net
http://www[.]webrss[.]com/createfeed[.]php?feedid=49297
http://185[.]82[.]217[.]200/@lb3rt/dqvabs[.]php
http://www[.]webrss[.]com/createfeed[.]php?feedid=49321
http://r0b1n[.]crabdance[.]com
http://80[.]255[.]3[.]96/r0g3r/dqvabs[.]php
http://overthemontains[.]weebly[.]com/paragliding-stuff
http://feed43[.]com/5787707581531238[.]xml
http://r0nald[.]ignorelist[.]com
https://musicall12[.]wordpress[.]com/29-2/
https://raw[.]githubusercontent[.]com/Zunaid-zunaid1/project11/master/xml[.]xml
https://robins0n12[.]wordpress[.]com/2017/01/31/my-biography/
http://feed43[.]com/0414303388550176[.]xml

http://d0nald1[.]strangled[.]net
http://d0nald[.]strangled[.]net
https://raw[.]githubusercontent[.]com/devonkearns/cricket/master/xml[.]xml
http://maxx[.]crabdance[.]com
http://80[.]255[.]3[.]96/max1mu5/dqvabs[.]php
https://yetwq[.]twilightparadox[.]com
http://149[.]56[.]80[.]64/u5b62ed973d963913bb/u5a3ewfasdk9[.]php
http://146[.]185[.]234[.]71/Ms3f3g45thgy5/f3af3fasf32[.]php
http://185[.]203[.]116[.]58/d394d142687ff5a0/dfae43rsfdgq4e[.]php
http://123[.]57[.]158[.]115/shujing/ghsnls[.]php
http://43[.]249[.]37[.]165/kungfu/ghsnls[.]php
http://94[.]156[.]35[.]204/22af645d1859cb5c/sg4gasdnjf984[.]php
http://81[.]17[.]30[.]28/th0mas/dqvabs[.]php
http://46[.]183[.]216[.]222/0racl3/dqvabs[.]php
http://176[.]107[.]182[.]24/f0357a3f154bc2ff/sadk9f043ejf[.]php
http://188[.]165[.]124[.]30/c6afebaa8acd80e7/byuehf8af[.]php
http://185[.]82[.]217[.]200/d3m0n/dqvabs[.]php
http://91[.]229[.]79[.]183/b15d0e30a7738037/j8fiandfuesmg[.]php
http://45[.]153[.]184[.]67/window[.]jpeg
http://45[.]153[.]184[.]67/window[.]sct
https://185[.]193[.]38[.]24/cnc/register
http://185[.]193[.]38[.]24/windows[.]sct
http://185[.]109[.]144[.]102/DistBuild/getExecutables[.]php
http://docs[.]google[.]com/uc?id=0Bx9cf6a5Mapaa3g4MII4T244SlU&export=downlo
ad
http://185[.]109[.]144[.]102/DistBuild/getExtensions_doc[.]php
http://185[.]109[.]144[.]102/DistBuild/getExtensions_rmdrive[.]php
http://185[.]109[.]144[.]102/DistBuild/getAllFiles[.]php
http://185[.]109[.]144[.]102/DistBuild/getExtensions_nondoc[.]php
http://tes[.]sessions4life[.]pw/quiz/WelcomeScrn[.]exe
https://45[.]43[.]192[.]172:8443/OxGN
http://socialfreakzz[.]com
http://194[.]63[.]142[.]174/Mussmal/ghsnls[.]php
http://85[.]25[.]79[.]230/tesla/ghsnls[.]php
http://russell01[.]servebeer[.]com/
http://russell02[.]servehttp[.]com/
http://www[.]webrss[.]com/createfeed[.]php?feedid=47449
http://5[.]254[.]98[.]68/Tussmal/ghsnls[.]php
http://updatesoft[.]zapto[.]org/Tussmal/ghsnls[.]php
http://ussainbolt1[.]mooo[.]com/Tussmal/ghsnls[.]php
http://www[.]chinasmack[.]com/2016/digest/woman-discards-her-food-on-
shanghaimetro[.]html
http://43[.]249[.]37[.]173/yumhong/ghsnls[.]php

http://asatar[.]ignorelist[.]com/tesla/ghsnls[.]php
http://blog[.]chinadaily[.]com[.]cn/home[.]php?mod=space&uid=2392255&do=blog&id=35101
http://overthemontains[.]weebly[.]com/trekking-lovers
http://captain[.]chickenkiller[.]com/quantum/ghsnls[.]php
http://feeds[.]rapidfeeds[.]com/81909/
http://info81[.]com
http://lujunxinxi[.]com
http://greatdexter[.]com
http://www[.]webrss[.]com/createfeed[.]php?feedid=47448
http://www[.]cnmilit[.]com
http://www[.]militaryworkerscn[.]com
http://miltechweb[.]com
http://climaxcn[.]com
http://cnmilit[.]com/index[.]php/?f=China_Security_Report_2016[.]pps
http://www[.]newsnstat[.]com/index[.]php?f=Report_Asia_Program_New_Geopolitics[.]pps
http://www[.]newsnstat[.]com/index[.]php?f=CEF_Chengdu_July_2016[.]pps
http://www[.]newsnstat[.]com/index[.]php?f=Limits_of_Law_in_the_South_China_Sea[.]pps
https://raw[.]githubusercontent[.]com/azeemkhan89/cartoon/master/cart[.]xml
http://t[.]ymlp50[.]com/bjyapaejesjaoawsqaaaujwes/click[.]php
http://milresearchcn[.]com
http://nudtcn[.]com
http://chinastrats[.]com
http://www[.]repeatserver[.]com/Users/sports/news[.]xml
http://www[.]webrss[.]com/createfeed[.]php?feedid=47444
http://forum[.]china[.]org[.]cn/viewthread[.]php?tid=175850&page=1&extra
http://russell03[.]servehttp[.]com/
http://wgeastchina[.]steelhome[.]cn/xml[.]xml
http://extremebolt[.]com
http://www[.]81-cn[.]net
http://updatesys[.]zapto[.]org/Tussmal/ghsnls[.]php
http://www[.]chinasmack[.]com/2016/digest/chinese-tourist-bit-by-snake-inthailand[.]html
http://www[.]travelhoneymoon[.]wordpress[.]com/2016/03/30/tips-to-how-to-feel-happy
http://wxkysteel[.]steelhome[.]cn/xml[.]xml
http://wxycgc[.]steelhome[.]cn/xml[.]xml
http://modgovcn[.]com
http://epg-cn[.]com
http://43[.]249[.]37[.]173/quantum/ghsnls[.]php
http://feeds[.]rapidfeeds[.]com/61594/

http://rasheed[.]crabdance[.]com/quantum/ghsnls[.]php
http://raw[.]githubusercontent[.]com/azeemkhan89/sports/master/sports[.]xml
http://hostmyrss[.]com/feed/housing_news
http://tariqj[.]crabdance[.]com/tesla/ghsnls[.]php
http://whgt[.]steelhome[.]cn/xml[.]xml
http://www[.]newsnstat[.]com/index[.]php?f=CIDEX2016[.]pps
http://www[.]cnmilit[.]com/index[.]php?f=China_Security_Report_CN2016[.]pps
http://www[.]cnmilit[.]com/index[.]php?f=China_Security_Report_2016[.]pps
http://10[.]30[.]4[.]112
http://www[.]itpub[.]net/thread-2055123-1-1[.]html
http://milscience-cn[.]com
http://miltechcn[.]com
http://letsgetclose[.]com
http://www[.]cnmilit[.]com/index[.]php?f=The_PLA_s_New_Organizational_Structure_Parts_1_and_2_01[.]doc
http://www[.]newsnstat[.]com/index[.]php?f=China_plan_to_dominate_South_China_Sea_and_beyond[.]doc
http://ussainbolt[.]mooo[.]com/Tussmal/ghsnls[.]php
http://www[.]chinahush[.]com/2014/12/27/can-common-views-of-chinese-women-be-changed
http://feeds[.]rapidfeeds[.]com/81913/
http://javedtar[.]chickenkiller[.]com/tesla/ghsnls[.]php
http://85[.]25[.]79[.]230/quantum/ghsnls[.]php
http://feeds[.]rapidfeeds[.]com/81908/
http://raheel[.]ignorelist[.]com/quantum/ghsnls[.]php
http://microsofl[.]mooo[.]com
http://databig[.]akamaihub[.]stream/pushBatch
http://bigdata[.]akamaihub[.]stream/pushAgent
http://bigdata[.]akamaihub[.]stream/orderMe
http://bigdata[.]akamaihub[.]stream/pushBatch
http://46[.]165[.]249[.]223:80
http://5[.]199[.]163[.]51:4343
http://91[.]210[.]107[.]106:80
http://adhath-learning[.]com:4343
http://46[.]165[.]207[.]108/appstore/appservice[.]php
http://truth786[.]com
http://tweetychat[.]com
http://freeintrnet[.]com/
http://simplechatpoint[.]ddns[.]net/android_connect/insert_sms[.]php
http://cloud[.]tweetychat[.]com/TweetyChatx32[.]exe
http://simplechatpoint[.]ddns[.]net/android_connect/insert_account[.]php
http://simplechatpoint[.]ddns[.]net/android_connect/insert_file_list[.]php
http://5[.]135[.]73[.]109/abc[.]hta

http://adhath-learning[.]com:8080
http://mofu[.]tech/useregistration/newuser[.]php
http://5[.]135[.]73[.]109/cpt[.]jpg
http://cloud[.]tweetychat[.]com/TweetyChat[.]exe
http://cloud[.]tweetychat[.]com/TweetyChatx64[.]exe
http://mfone[.]net/strength[.]php
http://91[.]210[.]107[.]104/search1[.]php
http://94[.]242[.]219[.]205/bookmarks[.]php
http://91[.]210[.]107[.]109:80
http://91[.]210[.]107[.]110:80
http://simplechatpoint[.]ddns[.]net/android_connect/upload_file_content[.]php
http://209[.]58[.]185[.]36:23558
http://mail[.]ifenngnews[.]com/8888-91-2018[.]doc
http://mail[.]ifenngnews[.]com/ADiCON2018[.]doc
http://ebeijingcn[.]live/update/software[.]php
http://saicgovcn[.]xyz/systemdb[.]php
http://www[.]nationinterests[.]org/index[.]php?f=Python_Strategy[.]docx
http://www[.]sinamilnews[.]com/cp0000412[.]rtf
http://fprii[.]net/Systems-CW-and-DW[.]doc
http://www[.]mericcs[.]org/GPPi_MERICS_Authoritarian_Advance_2018_1Q[.]doc
http://www[.]worldpolicticsreview[.]com/ChineseNuclearThinking_Final[.]doc
http://sz81orgcn[.]com/autoupdate[.]php
http://mericcs[.]org/SouthChinaSea[.]doc
http://ebeijingcn[.]live/templates/software[.]php
http://mail[.]ifenngnews[.]com/Strategic_report_ZH_2018_A01[.]doc
http://tiebabaidu[.]live/CSBA6318-GBSD_QLRSO_Report[.]doc
http://planews[.]live/China_Coast_Guard[.]doc
http://msoffice-updater[.]ddns[.]net/universe/blue[.]php
http://iexplorer[.]ddns[.]net/premium/product[.]php
http://windefendr[.]com/description[.]php
http://syspda[.]com/Loader/ccpost[.]php
http://pcupdate[.]ddns[.]net/mercury/heliocentric[.]php
http://microdigit[.]info/microservice/micservice[.]php
http://msword-updater[.]ddns[.]net/pyrimon/directory[.]php
cnaas[.]org
gffbzbgov-cn[.]org
googlemail[.]support
sinamilblog-cn[.]org
crazywomen-dating[.]com
gloalfirepower[.]org
mfagov-cn[.]com
sinodefence[.]info
tiexue-cn[.]net

milstar-cn[.]com
dwnnews[.]net
googlmail[.]cloud
ifenngnews[.]com
invitingholes[.]com
neteease[.]com
pla-report[.]net
scitechtrends[.]com
militarypeoplecn[.]com
tecchweb[.]com
brokings[.]org
ciis-cn[.]net
clep-cn[.]org
cpcnews-cn[.]com
euuwebmail[.]com
stripshowsclub[.]com
zhiihua[.]org
zhouangjiabing[.]com
militaryreviews[.]net
qzonecn[.]com
rannd[.]org
sinamilnews[.]com
mileastday-cn[.]com
randreports[.]org
servicelogin[.]center
servicelogin[.]support
bdarmy[.]news
iisdp[.]org
loweinstitute[.]org
ustc-cn[.]org
yahoomail[.]support
serviceloginmail-process[.]com
servicesprocessing[.]com
websourceing[.]com
techto-earth[.]com
games-playbox[.]com
accountsloginmail-process[.]com
alertmymail[.]com
manufacturing-minds[.]com
onestop-shops[.]com
westdelsys[.]com
worldvoicetrip[.]com
alertmymailsnotify[.]com

newsfairprocessing[.]com
cloudone-opsource[.]com
communication-principals[.]com
knight-quest[.]com
necessaries-documentation[.]com
download-mgrwin[.]com
devilcreator[.]com
internet-security-suite-review[.]toptenreviews[.]com[.]infocardiology[.]biz
torqspot[.]org
wreckmove[.]org
enlighten-energy[.]org
gadgetscorner[.]org
infocardiology[.]biz
mail[.]telenor[.]no-cookieauth[.]dll-getlogon-reason-0[.]formdir-1-curl-z2fowaz2f[.]infocardiology[.]biz
researcherzone[.]net
yetwq[.]twilightparadox[.]com
unique[.]fontsupdate[.]com
linkrequest[.]live
matissues[.]com
tes[.]sessions4life[.]pw
blingblingg[.]com
aaskmee[.]com
revoltmax[.]com
office-rb-support[.]com
yue-lao[.]info
dailychina[.]news
haiwaipengyou[.]com
nutcn[.]com
cndailynetwork[.]info
mozarting[.]com
nduformation[.]com
numeronez[.]com
majidalfuttaiim[.]com
webworldreq[.]com
wikifedia[.]space
newsnstat[.]com
qqgroups[.]info
alfred[.]ignorelist[.]com
outlookkz[.]com
xmachinez[.]com
securematrixx[.]com
sinodefprog[.]info

telemediaz[.]com
extremerebolt[.]com
junshiyuehui[.]com
pizzahomez[.]com
you-yisi[.]com
matrixrevolt[.]com
asiandefnetwork[.]com
eyescreem[.]com
163-cn[.]org
annchenn[.]com
expatchina[.]info
xbladezz[.]com
nextraload[.]com
symantecz[.]com
microsofl[.]mooo[.]com
extrememachine[.]org
bluebirdrestaurant[.]co[.]uk[.]infocardiology[.]biz
alintiqad-newsonline[.]blogspot[.]com[.]continuelogs[.]info
ezservicesenter[.]org
onlinestoreapp[.]net
openhostingtalk[.]com
mailtranet[.]com
sonification[.]com
follow-ship[.]com
macsol[.]org
cmegroups[.]net
cryptoanalysis[.]net
crystalrepo[.]org
armordesigns[.]com[.]webmail-login[.]php[.]web-mail-services[.]info
account[.]istpumpenunddosiertechnik[.]de[.]continuelogs[.]info
skylarzone[.]org
redgolfclub[.]info
server721-hans[.]de-nservers[.]de[.]continuelogs[.]inf
forest-fire[.]com
lynberrg[.]com
casinoaffiliatepartners[.]net
chkpoint[.]info
mobnetserver[.]com
competitveedge[.]org
deltaairlines[.]com[.]config[.]services[.]data[.]sesion[.]24s[.]digitalapp[.]org[.]evitalcare[.]org
sonificaton[.]com
systoolsonline[.]org

databig[.]akamaihub[.]stream
bigdata[.]akamaihub[.]stream
supportsession[.]live
mailsession[.]online
requestupdate[.]live
serviceupports[.]com
sundayobserver[.]net
conf[.]serviceupdateres[.]com
upload[.]cloudsekurity[.]online
qmails[.]org
abodeupdater[.]com
linkspectra[.]com
livesunshine[.]info
liveupdatesonline[.]net
mail[.]enrc[.]com-attachment[.]download[.]infocardiology[.]biz
mail[.]joymailserver[.]org
nitr0rac3[.]com
novelseller[.]org
opendocs[.]info
mozilaupdate[.]com
mpale[.]org
msoftweb[.]com
mymyntra[.]net
naclpro[.]org
mailcache[.]info
mailoff[.]org
makecmag[.]info
google[.]com[.]accountsserviceloginservice[.]info
google[.]comaccountsserviceloginservicemailen[.]serviceaccountloginservicemail[.]inf
o
kungfu-panda[.]info
lifelogs[.]org
hycoxcable[.]com
idsconline[.]net
gxongame[.]info
mildstone[.]net
www[.]email[.]t-online[.]de[.]accountsserviceloginservice[.]info
www[.]fonografia[.]pl
www[.]login[.]oriontelekom[.]rs[.]accountsserviceloginservice[.]info
www[.]login[.]yahoo[.]com[.]accountsserviceloginservice[.]info
www[.]mail[.]houseofjoyltd[.]com[.]accountsserviceloginservice[.]info
shreadersupport[.]net
smackdownfanclub[.]eu

smclog[.]org
smurfprotection[.]org
sochglobal[.]net
systemcrack[.]com
testerspoint[.]info
undertaker[.]no-ip[.]org
webmail[.]juno[.]com[.]accountsserviceloginservice[.]info
webmail[.]stevens[.]edu[.]authenticateservicemail[.]accountsservicelogin[.]info
webmailaccountservicemail[.]info
worldread[.]net16[.]net
worldtourismnews[.]info
spiritlog[.]org
sportswomen[.]biz
starcrunch[.]org
starsoel[.]org
supportanswer[.]net
shopping-hub12[.]com
softmini[.]net
buildyourinfo[.]org
cablecomsolutions[.]net
calling4you[.]com
centstat[.]org
cheetah4u[.]net
com-mailservice[.]com
facebook[.]comaccountsserviceloginservicemail2[.]serviceaccountloginservicemail[.]info
file-easy[.]net
fileshreader[.]net
fonografia[.]pl
ftp[.]alr3ady[.]net
downdossiersup[.]net
easyhost-ing[.]com
elementspro[.]org
enetebookstore[.]com
connectopen[.]info
crowcatcher[.]net
cupzon[.]org
dexlab[.]info
acc0unts[.]g00gle[.]c0m[.]srccail[.]com
accounts[.]facbook[.]com[.]continuelogs[.]info
accounts[.]you-tube[.]com[.]analogwiz[.]org
accounts[.]yutube[.]com[.]continuelogs[.]info
get[.]adobe[.]flash[.]softmini[.]net

global-blog[.]net
advnotifier[.]com
autowid[.]com
ftp[.]r3gistration[.]net
pharmamkting[.]eu
piegauz[.]net
plus[.]go0gle[.]com[.]servicel0gin[.]gxongame[.]info
random123[.]site11[.]com
researchhunter[.]org
outgateway[.]com
ozonerim[.]net
serviceaccountloginservicemail[.]info
rackitupstorenew[.]net
securingyourself[.]net
shopingcenter[.]net
ritownship[.]net
share-home[.]net
zerodayexploits[.]org
zolipas[.]info
alr3ady[.]net
analogwiz[.]org
appinsecurity[.]com
approvalclub[.]org
appworldblackberry[.]info
autowidge[.]org
avandtotalsecurity[.]com
bbc-news[.]com[.]influxlog[.]org
bbupdate[.]net
cr3ator01[.]net
crestboard[.]org
currentnewsstore[.]com
devinmartin[.]net
digitooldeals[.]net
braninfall[.]net
callersview[.]org
chroniclesupport[.]net
clamerword[.]net
config-login[.]com
divinepower[.]info
ezxen[.]org
fasttrackagent[.]net
filesassociate[.]net
fiservtech[.]org

activetalk[.]org
add-on-update[.]com
addoup[.]com
adminassistance[.]net
fuzzyfile[.]net
global-internet[.]info
ftp[.]currentnewsstore[.]com
ftp[.]devilreturns[.]com
ftp[.]nvidiaupdate[.]net
groupskm[.]info
www[.]server721[.]han[.]de[.]nsserver[.]de[.]continuelogs[.]info
www[.]shoperstock[.]com
xylotech[.]org
youtube[.]comaccountsserviceloginservicemail2[.]serviceaccountloginservicemail[.]info
zeusagency[.]net
zonalsky[.]org
vall3y[.]com
vkspoke[.]org
vstrend[.]org
wearwellgarments[.]eu
webjavaupdate[.]com
woline[.]info
workspacecz[.]net
worldcitycenter[.]net
www[.]alintiqad-newsonline[.]blogspot[.]com[.]continuelogs[.]info
taraanasongs[.]com
tmkstore[.]org
tollmart[.]org
tourtime[.]org
speedaccelator[.]com
spidercom[.]info
spstack[.]org
www[.]google[.]com[.]accountsserviceloginservice[.]info
www[.]mail[.]luckltd[.]com[.]accountsserviceloginservice[.]info
support-tech[.]info
docsforum[.]info
picasa-album[.]com
mailssh[.]info
mailtechsolutions[.]org
matewiz[.]org
matrixfanclub[.]net
mcosine[.]org

megamediafile[.]com
newamazingfacts[.]com
newsgroupupdate[.]com
news-report[.]sockzon[.]org
onlinewebmail[.]net
jasminjorden[.]com
joyfulhalloween[.]com
keepawayfromfire[.]com
h3helnsupp0ort[.]com
help-e[.]net
heritage-society[.]com
hifisure[.]org
mobiappword[.]com
mobilemyown[.]info
mobiletechspa[.]org
momate[.]net
mujahidtarana[.]com
myscreenname[.]aol[.]com[.]srccail[.]com
mail[.]myorderbox[.]org
hycoxweb[.]org
i-dim[.]net
opnsrc[.]net
rigidphotography[.]com
s0pp0rtdesk[.]com
s3rv1c3s[.]net
server721-hans[.]de-nservers[.]de[.]continuelogs[.]info
serverrr[.]com
pfv6jyg1rdo9ptku[.]mxsvr[.]net
searchports[.]info
secure-solution[.]net
programmersheavengroup[.]com
serviceagent[.]us
sh3llypunk[.]com
re-buke[.]com
sockzon[.]org
linxauth[.]org
login[.]yahoo[.]com-config-verify2[.]woline[.]info
m[.]ymail[.]com[.]continuelogs[.]info
mail[.]carmel[.]us[.]exchweb[.]bin[.]auth[.]owalogon[.]asp[.]serviceaccountloginservice
mail[.]info
mail[.]wildenstein[.]com[.]accountsserviceloginservice[.]info
hotbookspot[.]info
hotupdates[.]com[.]sockzon[.]org

influxlog[.]org
infoteller[.]org
mgclog[.]com
mjtag[.]org
mobilessoft[.]net
mobiltechsoft[.]org
mail-attachment[.]usercontent[.]evitalcare[.]org
mailexservices[.]com
mailservicesupport[.]org
internet-security-suite-review[.]toptenreviews[.]com[.]avandtotalsecurity[.]com
l0gin[.]y0utube[.]acc0unts[.]srccail[.]com
hangovergroup[.]com[.]coolservice[.]continuelogs[.]info
host-stuff[.]net
gamezoneall[.]com
geonet[.]org[.]sockzon[.]org
google[.]com[.]acount[.]database[.]updates[.]services[.]web-mail-services[.]info
ftp[.]forest-fire[.]net
systemupd[.]com
test[.]enciris[.]eu
thedailynewsheadline[.]com
tow3r[.]info
traderspace[.]org
trend-mico[.]net
www[.]produkte[.]web[.]de[.]accountsserviceloginservice[.]info
ymadmin[.]net
you-post[.]net
zonalon[.]org
starshome[.]comeze[.]com
store-fb[.]net
supersolus[.]org
supertechnoclub[.]com
www[.]espressoday[.]org
www[.]m[.]youtube[.]com[.]accountsserviceloginservice[.]info
www[.]mymail[.]bezeqint[.]co[.]il[.]accountsserviceloginservice[.]info
we-tour[.]net
wizcheck[.]org
www[.]ebox[.]co[.]il[.]accountsserviceloginservice[.]info
signaturedz[.]com
slamburger[.]net
visordan[.]org
wagonact[.]org
softwaresupdates[.]info
srccail[.]com

coolhostingwebspace[.]com
csfserver[.]com
customerpbr[.]com
deltadegger[.]net
denismoble[.]info
analysishunter[.]org
anoniemvolmacht[.]com
blogpublication[.]org
bluebird-restaurant[.]co[.]uk[.]infocardiology[.]biz
c0mpany4u[.]net
cabcardinc[.]net
callvoipnow[.]com
chiccounty[.]net
downfilesup[.]com
educatediary[.]org
esnucleus[.]org
espressoday[.]org
f00dlover[.]info
filesconnect[.]info
footwallfanclub[.]com
my[.]screenname[.]aol[.]com[.]accountsserviceloginservice[.]info
n00b4u[.]com
net4speed[.]net
netmosol[.]info
new-agency[.]us
secuina[.]net
securedmx[.]net
sendsh33p[.]com
server003[.]com
researchwork[.]org
rghsv[.]com[.]accountsserviceloginservice[.]info
nexterchk[.]net
osservices[.]info
saboresnativos[.]net
scrm-ail[.]info
pajerolive[.]com
parrotcatcher[.]com
servetools[.]org
serviaccive[.]com
shoppingspawn[.]com
shopingcard[.]net
applehostpoint[.]info
bkltmc[.]com

bluecreams[.]com
brandsons[.]net
addon-updates[.]com
alreadytrue[.]com
accounts[.]ymail[.]com[.]mailcache[.]info
islamic-teacher[.]org
itechtoys[.]org
joymailserver[.]org
khalistancalling[.]com
leicesterhigh[.]eu
linked-in[.]c0m[.]srcm-ail[.]info[.]srccail[.]com
mktserv[.]info
mobilesoftwaremanagement[.]info
msfileshare[.]net
login[.]facebook[.]com-confg[.]verify[.]login[.]src-ym[.]mailcache[.]info
mail[.]download[.]influxlog[.]org
mail[.]google[.]com-attachments[.]mail[.]u-01[.]infocardiology[.]biz
my[.]screename[.]aol[.]com[.]mjtag[.]org
mymail[.]bezeqint[.]co[.]il[.]accountsserviceloginservice[.]info
myvoipp0wer[.]com
secure[.]metacafe[.]com-account-login-token[.]accountsservicelogin[.]info
secure-copy[.]com
secureplanning[.]net
nlsec[.]org
nvidiaupdate[.]net
opendocxsupport[.]net
pizzapalace[.]org
primaaltus[.]org
martcas[.]org
maxtourguide[.]info
mexchange[.]info
r3gistration[.]net
filesforum[.]net
filetrusty[.]net
fistoffury[.]net
fitnessapproval[.]org
forest-fire[.]net
frameworkup[.]org
continuelogs[.]info
cpbatch[.]org
downtimesupport[.]com
easyslidesharing[.]net
endemol[.]com[.]mailcache[.]info

evolvingdesk[.]org
ezservicecenter[.]org
ftp[.]global-internet[.]info
ftp[.]kungfu-panda[.]info
ftp[.]matrixfanclub[.]net
ftp[.]s3rv1c3s[.]net
google[.]accountservice[.]adminassistance[.]net
hangoutgroups[.]net
cppblog[.]net
devilreturns[.]com
gauzpie[.]com
gnuvisor[.]com
hostmypc[.]net
imagebar[.]org
www[.]insing[.]com[.]accountsserviceloginservice[.]info
www[.]login[.]comcast[.]net[.]accountsserviceloginservice[.]info
www[.]mail[.]rediff[.]com[.]accountsserviceloginservice[.]info
www[.]mexchange[.]info
www[.]my[.]screenname[.]aol[.]com[.]accountsserviceloginservice[.]info
tradeobjective[.]net
tulip[.]net[.]inforguide[.]org
unisafeservice[.]org
vkverbal[.]org
voip-e[.]net
wakeupindian[.]net
whostmrage[.]org
wizsplit[.]org
workinglab[.]org
softservices[.]org
sped0m00d[.]com
service-secure[.]net
shoperstock[.]com
zendossier[.]org
server006[.]com
picasa-album[.]net
linkedin[.]com-uas[.]login-submit[.]account[.]session-full[.]login-3a5077708027557787984-csrftoken[.]buildyourinfo[.]org
login[.]live[.]com[.]continuelogs[.]info
login[.]live[.]com[.]mailcache[.]info
login[.]oriontelekom[.]rs[.]accountsserviceloginservice[.]info
logstat[.]info
m[.]ymail[.]com[.]mailcache[.]info
mobileappsupport[.]com

mobileappworld[.]info
mosglobe[.]org
motsoul[.]org
hangoutshop[.]net
hardwaregeeks[.]eu
heavenaffiliates[.]info
herbco[.]document[.]digitalapp[.]org
hintover[.]com
innovatorspool[.]org
jerrycoper[.]org
kyzosune[.]net
l0gin[.]faceb0ok[.]com[.]srccail[.]com
l0gin[.]yaho0[.]c0m[.]srccail[.]com
fapize[.]com
fb-time[.]net
foxypredators[.]com
ftp[.]braninfall[.]net
go-jobs[.]net
google[.]com[.]accountsserviceloginservicemaileng[.]serviceaccountloginservicemail[.]info
inforguide[.]org
infraswap[.]org
ftp[.]net4speed[.]net
megafairclub[.]org
webmicrosoftupdate[.]net
wedzon[.]org
wolfensteinx[.]net
wondersofworld[.]eu
worksmartplay[.]com
www[.]analysishunter[.]org
www[.]cytanet[.]com[.]accountsserviceloginservice[.]info
www[.]foxypredators[.]com
www[.]go0gle[.]com-serviicelogiin[.]autthserv[.]gxongame[.]info
www[.]microsoft[.]com[.]chiccounty[.]net
www[.]mlogin[.]ymail[.]com[.]continuelogs[.]info
www[.]mobilesoftwaremanagement[.]info
viewerstalk[.]org
viragenonline[.]com
web-mail-services[.]info
www[.]secure[.]metacafe[.]com-account-login-token[.]accountsservicelogin[.]info
youtube[.]com[.]accountsserviceloginservicemail[.]serviceaccountloginservicemail[.]info
trustworthyinfo[.]com

sports-interaction[.]net
starmobnetservice[.]net
stretcherservices[.]net
synergyrealsolutions[.]net
shopertock[.]net
shopie[.]net
secure-s[.]com
cellgame[.]org
clienttreasury[.]net
cmxgrp[.]net
cobrapub[.]com
codetesters[.]org
dosendit[.]com
easternsoft[.]org
evitalcare[.]org
ezyvalue[.]net
amaxgrp[.]net
avatarfanclub[.]com
bikefanclub[.]info
bmcmail[.]org
crvhostia[.]net
digitalapp[.]org
accounts[.]yandex[.]ru[.]continuelogs[.]info
myfilestuff[.]net
mysharpens[.]com
neverforget1984[.]org
oliveglobals[.]com
omg-pics[.]net
opensourceforum[.]eu
reliable-global[.]net
servicesonlinesupportinfo[.]com
servorder[.]org
privatemoneyblog[.]org
racmania[.]net
ritualpoint[.]org
rockingdevil[.]net
packetwarden[.]net
periodtable[.]eu
pics-bucket[.]net
securitytable[.]org
datapeople-cn[.]com
ebeijingcn[.]live
saicgovcn[.]xyz

sz81orgcn[.]com
sastind-cn[.]org
tautiaos[.]com
msoffice-updater[.]ddns[.]net
aarynews[.]com
windefendr[.]com
thenewpk[.]com
philions[.]com
fuddiduniya[.]com
mfone[.]net
microdigit[.]info
mericcs[.]org
mailcenter[.]support
179[.]48[.]251[.]4
5[.]101[.]140[.]220
209[.]58[.]163[.]44
5[.]8[.]88[.]64
93[.]115[.]94[.]202
94[.]185[.]82[.]155
209[.]58[.]183[.]33
46[.]166[.]163[.]243
94[.]242[.]249[.]203
176[.]107[.]177[.]10
37[.]59[.]175[.]131
46[.]32[.]235[.]162
81[.]4[.]125[.]90
176[.]56[.]238[.]177
213[.]229[.]64[.]222
151[.]237[.]188[.]167
185[.]203[.]118[.]115
94[.]156[.]35[.]204
185[.]82[.]217[.]200
80[.]255[.]3[.]96
185[.]161[.]208[.]252
185[.]203[.]119[.]184
23[.]106[.]123[.]87
212[.]114[.]52[.]148
149[.]56[.]80[.]64
185[.]29[.]11[.]59
146[.]185[.]234[.]71
185[.]203[.]116[.]58
199[.]168[.]138[.]119
85[.]217[.]171[.]138

178[.]33[.]94[.]35
123[.]57[.]158[.]115
91[.]92[.]136[.]239
185[.]156[.]173[.]73
185[.]206[.]144[.]67
193[.]37[.]213[.]101
43[.]249[.]37[.]165
164[.]132[.]75[.]22
193[.]22[.]98[.]17
185[.]116[.]210[.]8
81[.]17[.]30[.]28
46[.]183[.]216[.]222
139[.]28[.]38[.]236
176[.]107[.]182[.]24
188[.]165[.]124[.]30
185[.]36[.]188[.]14
91[.]229[.]79[.]183
139[.]28[.]38[.]231
185[.]109[.]144[.]102
45[.]43[.]192[.]172
178[.]162[.]210[.]246
178[.]162[.]210[.]245
91[.]229[.]79[.]181
91[.]229[.]79[.]190
46[.]165[.]225[.]66
91[.]229[.]79[.]185
91[.]229[.]79[.]189
178[.]162[.]210[.]247
95[.]211[.]205[.]164
95[.]211[.]205[.]165
94[.]242[.]231[.]244
94[.]242[.]223[.]24
212[.]129[.]13[.]110
94[.]242[.]219[.]203
94[.]242[.]223[.]19
95[.]141[.]34[.]245
95[.]141[.]34[.]246
95[.]211[.]205[.]161
91[.]229[.]79[.]184
37[.]58[.]60[.]195
46[.]165[.]229[.]9
46[.]165[.]248[.]237
212[.]129[.]7[.]146

91[.]229[.]79[.]187
43[.]249[.]37[.]173
37[.]48[.]77[.]215
46[.]165[.]248[.]236
178[.]162[.]210[.]242
212[.]83[.]146[.]3
46[.]165[.]248[.]238
46[.]165[.]248[.]239
46[.]165[.]248[.]240
46[.]165[.]248[.]243
91[.]229[.]79[.]186
46[.]166[.]163[.]244
46[.]165[.]229[.]7
46[.]165[.]248[.]241
178[.]162[.]210[.]244
178[.]162[.]210[.]248
212[.]83[.]191[.]156
95[.]211[.]205[.]166
93[.]115[.]95[.]132
95[.]211[.]205[.]142
94[.]242[.]223[.]28
95[.]141[.]34[.]242
95[.]211[.]3[.]135
10[.]30[.]4[.]112
46[.]166[.]163[.]246
91[.]229[.]79[.]182
37[.]48[.]77[.]214
46[.]165[.]229[.]8
178[.]162[.]210[.]243
91[.]229[.]79[.]188
95[.]211[.]205[.]163
185[.]236[.]203[.]236
176[.]107[.]181[.]213
89[.]33[.]246[.]99
5[.]135[.]199[.]0
46[.]182[.]105[.]41
5[.]34[.]242[.]129
8[.]22[.]200[.]44
88[.]198[.]86[.]172
72[.]44[.]81[.]88
75[.]127[.]91[.]16
79[.]142[.]78[.]112
79[.]142[.]78[.]76

79[.]142[.]64[.]97
79[.]142[.]64[.]99
79[.]142[.]64[.]32
79[.]142[.]64[.]36
69[.]43[.]161[.]180
79[.]142[.]64[.]177
79[.]142[.]78[.]109
46[.]182[.]104[.]83
141[.]8[.]224[.]25
173[.]224[.]215[.]230
173[.]233[.]80[.]146
173[.]233[.]80[.]147
173[.]233[.]80[.]152
173[.]236[.]24[.]250
173[.]236[.]24[.]251
173[.]236[.]24[.]254
176[.]31[.]53[.]166
176[.]31[.]53[.]167
176[.]31[.]65[.]125
176[.]31[.]79[.]48
178[.]32[.]75[.]192
178[.]32[.]75[.]197
178[.]32[.]75[.]198
216[.]24[.]202[.]100
31[.]214[.]169[.]87
31[.]3[.]154[.]116
31[.]3[.]155[.]106
37[.]221[.]166[.]53
184[.]154[.]254[.]54
184[.]22[.]69[.]109
184[.]82[.]180[.]105
188[.]165[.]148[.]70
188[.]241[.]114[.]160
109[.]235[.]49[.]158
109[.]235[.]49[.]236
109[.]235[.]51[.]100
199[.]204[.]248[.]107
199[.]71[.]212[.]164
37[.]59[.]208[.]94
178[.]33[.]187[.]74
89[.]207[.]135[.]61
89[.]45[.]249[.]129
91[.]214[.]45[.]187

94[.]185[.]81[.]153
95[.]143[.]42[.]218
109[.]203[.]110[.]103
109[.]235[.]49[.]147
173[.]233[.]80[.]145
176[.]31[.]4[.]130
109[.]235[.]49[.]43
109[.]235[.]50[.]215
89[.]207[.]135[.]120
89[.]207[.]135[.]239
89[.]45[.]249[.]136
79[.]142[.]78[.]120
79[.]142[.]78[.]79
79[.]142[.]78[.]83
75[.]127[.]111[.]143
78[.]46[.]129[.]193
94[.]102[.]49[.]55
94[.]185[.]81[.]151
79[.]142[.]64[.]181
94[.]102[.]49[.]203
95[.]154[.]237[.]11
8[.]23[.]224[.]90
173[.]236[.]117[.]205
178[.]33[.]154[.]52
216[.]24[.]204[.]243
216[.]24[.]204[.]245
31[.]170[.]161[.]136
31[.]3[.]154[.]117
37[.]221[.]166[.]49
192[.]210[.]203[.]181
199[.]119[.]203[.]86
199[.]71[.]212[.]183
213[.]5[.]71[.]20
213[.]5[.]71[.]31
37[.]221[.]166[.]55
37[.]221[.]166[.]61
37[.]221[.]166[.]8
37[.]46[.]127[.]79
37[.]46[.]127[.]81
176[.]31[.]53[.]165
176[.]31[.]79[.]50
176[.]31[.]79[.]51
176[.]31[.]79[.]56

178[.]32[.]75[.]196
178[.]33[.]154[.]49
178[.]33[.]154[.]51
178[.]33[.]154[.]54
178[.]33[.]187[.]76
5[.]39[.]97[.]57
66[.]148[.]67[.]20
69[.]43[.]161[.]179
178[.]33[.]214[.]194
184[.]107[.]159[.]18
184[.]154[.]254[.]51
46[.]182[.]105[.]60
5[.]39[.]36[.]58
5[.]39[.]36[.]59
5[.]39[.]97[.]58
64[.]120[.]135[.]137
65[.]75[.]243[.]251
74[.]117[.]62[.]170
75[.]127[.]111[.]100
94[.]102[.]49[.]204
95[.]143[.]42[.]217
78[.]46[.]129[.]194
78[.]46[.]169[.]168
94[.]102[.]49[.]199
94[.]102[.]49[.]202
79[.]142[.]64[.]183
79[.]142[.]78[.]111
96[.]30[.]46[.]216
109[.]235[.]49[.]148
109[.]235[.]49[.]188
109[.]235[.]49[.]193
109[.]235[.]51[.]153
141[.]101[.]239[.]128
213[.]5[.]65[.]24
213[.]5[.]65[.]31
213[.]5[.]71[.]27
213[.]5[.]71[.]28
216[.]188[.]26[.]235
173[.]199[.]145[.]140
173[.]236[.]24[.]252
174[.]120[.]28[.]61
46[.]182[.]105[.]43
46[.]4[.]187[.]60

46[.]4[.]215[.]38
37[.]46[.]127[.]78
46[.]182[.]104[.]85
46[.]182[.]105[.]40
31[.]3[.]154[.]115
37[.]221[.]166[.]36
178[.]32[.]75[.]193
178[.]32[.]75[.]195
188[.]241[.]115[.]127
178[.]33[.]210[.]30
188[.]241[.]117[.]163
188[.]95[.]48[.]99
199[.]119[.]203[.]102
199[.]119[.]203[.]103
209[.]85[.]51[.]152
213[.]5[.]65[.]20
213[.]5[.]71[.]24
213[.]5[.]71[.]26
37[.]221[.]166[.]9
37[.]46[.]127[.]75
37[.]59[.]175[.]130
37[.]59[.]231[.]161
188[.]165[.]148[.]68
188[.]240[.]47[.]145
188[.]240[.]47[.]220
188[.]241[.]113[.]27
141[.]8[.]225[.]7
173[.]233[.]85[.]134
176[.]31[.]4[.]129
31[.]3[.]154[.]110
31[.]3[.]154[.]114
37[.]221[.]166[.]42
109[.]235[.]50[.]191
109[.]235[.]50[.]233
109[.]235[.]51[.]50
176[.]31[.]65[.]126
176[.]61[.]140[.]119
178[.]33[.]131[.]34
5[.]39[.]36[.]56
79[.]142[.]78[.]102
79[.]142[.]78[.]107
79[.]142[.]78[.]110
94[.]102[.]49[.]56

95[.]143[.]42[.]195
74[.]117[.]62[.]181
75[.]127[.]91[.]118
5[.]39[.]36[.]57
5[.]39[.]36[.]60
95[.]211[.]131[.]144
89[.]45[.]249[.]139
89[.]45[.]249[.]41
79[.]142[.]64[.]47
79[.]142[.]64[.]49
79[.]142[.]64[.]98
79[.]142[.]78[.]101
79[.]142[.]64[.]178
79[.]142[.]64[.]34
79[.]142[.]64[.]37
79[.]142[.]64[.]39
94[.]102[.]55[.]80
94[.]185[.]81[.]152
89[.]207[.]135[.]242
89[.]45[.]249[.]208
88[.]198[.]86[.]168
94[.]102[.]49[.]201
79[.]142[.]78[.]80
5[.]39[.]36[.]61
31[.]170[.]161[.]56
31[.]170[.]162[.]23
31[.]214[.]169[.]86
31[.]3[.]154[.]111
31[.]3[.]154[.]113
37[.]221[.]166[.]15
37[.]221[.]166[.]47
37[.]221[.]166[.]48
37[.]221[.]166[.]58
37[.]221[.]166[.]7
37[.]46[.]127[.]76
37[.]46[.]127[.]77
46[.]182[.]104[.]70
46[.]182[.]104[.]72
109[.]235[.]49[.]157
109[.]235[.]49[.]235
109[.]235[.]50[.]246
109[.]235[.]51[.]254
109[.]235[.]51[.]51

176[.]31[.]65[.]124
176[.]31[.]65[.]127
176[.]31[.]79[.]49
178[.]32[.]75[.]194
178[.]33[.]154[.]53
178[.]33[.]187[.]75
178[.]33[.]187[.]77
178[.]33[.]187[.]78
173[.]236[.]68[.]99
176[.]31[.]4[.]128
199[.]119[.]203[.]85
213[.]5[.]65[.]223
184[.]154[.]217[.]250
5[.]39[.]11[.]72
46[.]165[.]249[.]223
5[.]199[.]163[.]51
91[.]210[.]107[.]106
46[.]165[.]207[.]108
45[.]76[.]33[.]53
5[.]135[.]73[.]109
199[.]101[.]187[.]54
91[.]210[.]107[.]104
94[.]242[.]219[.]205
91[.]210[.]107[.]109
91[.]210[.]107[.]110
45[.]63[.]43[.]29
209[.]58[.]185[.]36
94[.]242[.]249[.]206
185[.]130[.]212[.]252
221[.]121[.]138[.]141
221[.]121[.]138[.]139

MD5:

6d6fe7d36e1c43aab534644378d56dfb
acfada8e91eda6cca2da66bbb032d924
00bd9447c13afbbb7140bef94e24b535
1579467859b48085bdf99b0a1a8c1f86
82837a05f8e000245f06c35e9ddc3040
85ce84970182be282436317ebc310c8e
bd52237db47ba7515b2b7220ca64704e
62b702a15a762692eda296b0aea270f9
10d8d691ec5c75be5dbab876d39501f1
61abb92f0fa605c62dab334c225ef770

05c983831cad96da01a8a78882959d3e
a25d1e14498dd60535c5645ed9f6f488
ca26ca59bafa3ae727560cd31a44b35d
98ce593bfaeddbbbe056007525032e0d
ecc8b373e61a01d56f429b2bd9907e09
edc4bdfd659279da90fc7eab8a4c6de3
1676ded041404671bfb1fcfe9db34dcf
21a52fedba7d5f4080a8070236f24a81
1b41454bc0ff4ee428c0b49e614ef56c
551e244aa85b92fe470ed2eac9d8808a
d807fb3cb1a0687e152d288171ab9b59
e7ba5c209635607b2b0e38a00a822953
17d5acf49a4d65a4aacc362576dbaa12
3c68ca564595e108920a0f105728fded
8c21aee21b6bfa12ecf6070a4532655a
9c9e5d09699821c53d68e957044ec6e8
a0177d2fd49d835244028e98449c77a5
1e620679c90563d46aa349e991d2e0f2
2c70e1f152e2cb42bb29aadb66ece2ec
2158cb891a8ecbaaa70a641a6529b787
a1940b31af27139a13dff852cb012a22
915e5eefd145c59677a2a9eded97d114
a8b9a32723452d27257924a737ec1bed
f16ee3123d5eb21c053ac95e7cd4f203
543fe62829b7b9435a247487cd2a9672
7660c6189c928919b0776713d2755db2
dba585f7d5fc51566c663bd738de2c33
409e3368af2add71265d2811aa9d6817
7f50d3f4eabffe7225a2d5f0c91009c8
da29f5eeb39332a850f04be2906315c1
3a83e09f1b751dc08f4b719ed51c3fbc
165ae88945852a37fca8ec5224e35188
d01be8c3c027f9d6f0d93542dfe7ca97
fa94f2843639f7afec3c06799a8d222e
2c9b4d460e846d5814c2691ae4591c4f
dab037a9e02978bcd275ddaa15dab01d
79afb3f44172447015578b8064c1dda0
89963d5aac8441b0febbe5d5a0ab7629
90af176bfdf248d2899b49316458e4b6
6b335a77203b566d92c726b939b8d8c9
fa2f8ec0ab22f0461e860394c6b06a68
61f812a1924e6d5b4307313e20cd09d1
d5a976cc714651711c8f067dd5e00709

6f327b93279f3ce39f4fbe7a610c3cd2
4d2bde1b3985d1e1088801d92d1d6ca9
c4f5d6ed36c3d51cb1b31f20922ce880
1fb7eece41b964517d5224b57073c5d4
70c5267c56ded521c6f674a6a6649f05
36581da1d10ba6382a63e7046c21dd8d
b5e5e428b31a8affe48fdf6b8a253dc6
7c4c866cf78be30229b75a3301345f44
a4fcf3a441865ae17f2c80ff7c28543d
f7905a7bd6483a12ab36071363b012c3
eb0b18ecaa6f40e48970b08f3a3e6803
9f9824e9a4d7d3073aebbcc781869660
6abf60e9e2f6e3fa4c8020e1b2ef2867
6d8534597ae05d2151d848d2e6427f9e
4595dbaeec06e3f9b466d618b4da767e
ce1426ffe9ad4439795d269ddcf57c87
fe78c037844ad08a9a79c85f46e68a67
657e9333a052f593b7c51c58917a1b1f
141a8b306af8087df4feee15f571eb59
122d7dff33174e532063a16ae526208d
58179b5cf455e2bcac396c697cd43050
036a45983df8f81bf1875097fc026b04
0d1bdb45bac3b09e28e4f0cb09c97194
f017c65c7b5d14df11c5e0e4f0406562
dffe28c9c4dc9e2e865e3237f4bc38c4
86edf4fab125d8ccba85138f43b24def
bc08d1bddf72369adceffbfc36f848df
57377233f2a946d150115ad23bbaf5e6
9a0534772ac23ff64e3c85b18fbec596
d1c864ae8770ae43a0e59a31c0788dc2
24c722f3d0770ede82fa3d6b550098b3
08a116efce7d947257ce94fc8f3e276e
eefcef704b1a7bea6e92dc8711cfd35e
d64efa0b8c091b8dbed3635c2b711431
98e7dc26531469e6b968cb422371601a
3d01d2a42450064c55574d853c086f9a
ffab6174860af9a7c3b37a7f1fb8f381
3a2be243b0c78e8689b34e2415d5e479
098c74c23ed73ac7bf7581fec2eb088d
1c5b468489cf927c1d969484ddbdd8ea
f5e121671384fbd43534b8515c9e6940
72c05100da6b6bcbf3f96fee5cf67c3f
ebe8efbad7f01b76465afaf474589c2f

631d44688303be28a1b825aa1c9f3202
d049a6f9e527a72a4b917eec1acbd6f9
09a478efd8c5aeef3a5395e3988f5059
d791f8d9495d5d5df0cedb8b27fb3b49
040712ba00b32cc19e1938e14e732f59
3b0ca7dafb94333234e4f1330a1699da
8aae16b5e64445703d939bc7923ae7b7
807796263fd236a041f3633ac578140e
5a89f11f4bb3b5637c731e206f807ff7
d79e1d6302aabbdf083ba89a7c2f34fc
71d59036f84aba8e60aa8785e3883372
e5685462d8a2825e124193de9fa269d9
f7ce9894c1c99ce64455155377446d9c
2c0efa57eeffed228eb09ee97df1445a
61e0f4ecb3d7c56ea06b8f609fd2bf13
3cd8e3e80a106b0590a7b5eedddf4715
d273f090b96eca7c93387a03d9527d9b
533ce967d09189d27f38fe6ed4711099
8c875542def907312fd92d10746c230c
e98b1ed80ba3a3b6b0809f04536e9753
9a7e499d7abfcbe7fb2a78cf1d7a2f10
40ace1c9394c95d7e9e1e80f24bd1a73
04aff7c333055188219e290e58313d78
ae27773e49fea122e3f8ce7a27e6c555
a8022594e81c74b22abca772eb89657c
884f76542f3972f473376c943daeaf8f
4ea4142bab2b90e5779df19616f7d8ca
8a350d3f6fb359377d8939e1a2e033f3
e08bbed0aa4b21ae921d4dc5350789c7
71ce64fee9cd323828a44e9228d2736b
7eb1b6fefe7c5f86dcc914056928a17b
1538a412fd4035954237c0b4c135fcba
14eda0837105510da8beba4430615bce
b47386657563c4be9cec0c2f2c5f2f55
2565215d2bd8b76b4bff00cd52ca81be
4ad80ff251e92004f56bb1b531175a49
4e8ab2aa18c6607c40f27948d3d85be4
4a0e5f3c3d70dc287202eb0e342ca632
4abe3fae79903395a65a95c8af3738eb
282ef2ba0cc14bb94f363374537d0eaf
2902c48a767753d8e6a998c1c8efc77f
3fc11cd60c9e2bb29efe560e485abab9
423519ae6c222ab54a2e82104fa45d12

3666f0ff389747774c6d8f8338cbba7b
3a89f05c09425f03fe74b2242b119cce
3b9d65134b6529cf2d8d3cea22fe2fb7
1a1bc6e47d9dcbf6e3e7ce22d18b3628
25536cdacdcc7867d4feb1fbf7e5e172
2729de09c88071bb71b55be98801e2c0
7aeda30a2824ab86717cd3f6f09f5adc
7d42db873cae7b2ee156766e9838808c
7e74334c1495a3f6e195ce590c7d42e5
7edab76693800fd1617ba23c7a6aad88
8dad164966fb17c3c1f3e068c73080e0
8459fa25b7d93ef2f687eb0901bc94b0
859820011b21e57de55c22dabd227f11
862becc13747aafba8bfd755869251bb
78b8006cc9fc6ca45f8e7c8300e39dee
cff2e20f9ec8e4cda4957ec3136bb9f9
c4f1247cc0b5ed8adb94a51030eb473a
bc348a63e08fce9831241681f40db925
b51cbbbab70a7b89b0957b2fff4994e4
f37dd92ef4d0b7d07a4fbdcd9329d33b
f70a54aacde816cb9e9db9e9263db4aa
007d63bf9eb50c6e55125c00d32abdb6
5bda43ed20ea6a061e7332e2646ddc40
620f234fda7eb6a1247c2da6a8e5da83
6de00ae0bd81fead3fdf5c791595c8bd
6d84c91e0f46e76c4bb4245d5b1a5118
770fc76673c3c2daadd54c7aa7ba7cc3
9678089aacaf3e147e50662c82c11d19
990b640a93cffe65f646d6584f82a4d7
9911f5b52f0177e26e3fd0a671bf370e
aadbf8103cec7e5e5280befdd12c1e64
addcd1e1f20c237ccf3fa5cf7528ce33
a25568a3048cf6b83d72c5e9aae5ea75
d5bfa0a259deb8abd7e3cc3aebd52afb
e3da83cb528fd257103685443f6fdf1e
e40205cba4e84a47b7c7419ab6d77322
def441fb6719cd322389e3f594bef270
e14b7985764e737333d531daabf55970
d6f8df14da5750a75b3e5ebe2c76125c
e7d9bc670d69ad8a6ad2784255324eec
dcdae3149e91b3e8e037097667218528
00978e4b81ac577f328d6add75d0890e
36b3f39e7a11636adb29fe36bea875c4

37207835e128516fe17af3dacc83a00c
3ae40259e505b5335b72879db4db3df0
3c03b8436e9937ba3cfe18443b4c73b9
649eb3db4159411ee6ec0d849274a825
46ef141f709b2f6e3445bc2f09dd9c28
7a0f03c202c719994cbf0b62c1859e5c
82bba197bc3f1a1e1f0ae0ba1de16565
ba42eaebdedaf4f11aded2be2e352a7e
a2ed2a5dfc3954a815cf165c2f07dfd6
a53aff4075891c17ed9cdbdfcc124a1d
bd75bf1fe26f92ae2cab6beba0390d9e
bf8c0fff3269a84204d5bbcf08747c3d
e5479fac44383ca1998eb416aa2128f0
e74ce9ca4baccf2204ef6fbdf85e9817
e8197e5bca1db7ffab1f073f6300004a
ecf86588df072d4c574ee092e999e6a6
22588c6920f80398ae54e499b657f02d
232f616ad81f4411dd1806ee3b8e7553
2479724f3d62c71fe64a1d2b3535d661
02f3a2752b9a79ffccd99a1da8fb875c
0538fce0581b9233d34c6ad61a8f8139
2c5454f991fcef2ab42b899209dd4922
9ca4b7fae929a361c383cc9d5bbe2edb
9e3611e55f892cd58e2759ff482b6b54
9e5540383f78652a17b8efb7f454bc7c
87693d2559e369472fde254c1b410904
95d2e0f6ebf675069b656857eb238399
961d6de08e0417b11c40e93940fc0918
a24c34fd4244f73fc94eaf6e52b7c350
9fab73462e197ffe2263476a4e84eb79
8ed7f7ff05fe0c29874b738a7099a4ee
c9e01b48800dfe10dec2bd985c36c05e
cc8e5734532115ba77c2c906e86711f7
d534ba2ff2be9f1511d9e6ef9160bb53
d62d941d86169f6feb64bf950805bcfd
e4d710b3898dfbfb46cd65b5215ee3ee
d67418ddd0df67b3f77581ebde2df269
d75f75edb30460c7e156eac0274826b2
de75038bae500ba981147f256102c83f
dafc6646d38269656755ac004d72ccbd
3105b020e2bd43924404bc4e3940191b
331db34e5f49ac1e318dda2d01633b43
34b834d70bfde92f095a9c529b1dcc48

6521ae44e485f811e9ce25913675161c
4f82a6f5c80943af7facfcafb7985c8c
4008e61496b011e29b6343ad886e8f6d
84a2b843578c883a3fa59597c14cf709
915028829c8d64ad875c95cc916700ce
8eac188d2818dd22b857b9cffac50c12
cee292420bf0639773e6b2831bfb2e5e
c122f2b9a66f1689b92f547d3d32f455
c487aa1c2ea83fca899d8afe4de9a6fd
d4a373c4fb39471d07808b6d0a6140b9
dc39585d0c78a2dbd65afac5ef5c826b
cc3d271204c73b90a7b346121d381892
d9c3b4e5faa03bc8d83396837bd7e23c
e2e61074624f8e644b39aa0789823813
e6b45dfbd2c1e734f672e7a32fa6f9eb
f778c3fb1b2ccd5a4556f84442c6640c
f9150f1e82c2aece498da6293f50319b
f21ca71866a6484a54cd9651282572fd
06ba10a49c8cea32a51f0bbe8f5073f1
09947ba52932d10d3c859511a6d31e8f
0a0bcd8beb77e67a28a325d8d2a00254
0f91c1d4ef8b239bb9a94d5546f071dd
04c2068c132f2c4af31f905f220503d6
0680b9e247b2779799d4b32582f566c8
1ee4bd29caf6aed2f3c7e263fa025468
24f22d1391377249f21bfec81c3ea031
26fe2770b4f0892e0a24d4dddbbfe907
1972ae990751fa1b1532aa792bd5c160
7108bf3948226cbe0667607c17df8c12
7550db173b1beeb7e6c545b97f2cce02
76643813358b9198b6aed437eb7b5210
9b6305ee30004c72076e10b81c0847fb
9d959939bbf20bd582fc70f9e7b3a1e8
9de74a6b09858009766e5b9de510a764
9ec2c49fd9d1a1d8bea263b399e047af
a5452bae7a46923c75acac2fc4f00df9
b888df619bf503a014f2358d0180076b
ac5b7ac2c177125d192045e0a2ead278
acce099dddc2538e2c102b72bcf80759
a06fa6ce10b76b2d23d580cc7132fa33
bc588bed14699e30de569ee6e5f3578e
bdab33e31f27578eb99332c6c3104cd3
0b88f197b4266e6b78ea0dcb9b3496e9

33840ee0b45f31081393f4462fb7a5b6
3475cb096dc082eaa92a7825726c7b8d
13107b9455561e680fe8c3b9b1e8bc37
312892649a2be80704f1601451246308
1be309eb99298c128b97649dcc7c9ad6
18bc477fa12048fab8ec93d5ff942cf5
168f2c46e15c9ce0ba6e698a34a6769e
7a10c2c0581d01f3d4f8101bbf6468b1
7c37c6d89ed05fb264d8fe0acd795fd2
716b1c26faa3f674023aae670d3980f2
7244aaa1497d16e101ad1b6dee05dfe3
7655868c4a3ed2cd978a84971b7aab54
8017684a46d91f59e7316594c877911d
d5ff9201464048441963cdd60f54df9a
c3bd5e3d49627aae106c0e21631deb70
ca07a6e21204c72c14bc9429a6d33a71
bcec4c74fa790f3ddbbb165ad9e99ca7
ce00250552a1f913849e27851bc7cf0a
c0a53e093be2c2cc2ed6145da8aa123f
bda1967f2491e5d792fa66e672951119
d9a8709ed2e45503c94599c718d467fd
e4e851b679333928ceff068b5664efef
dde215945d217d8c97dcc498f43cfa86
08f7ead1513bb921c9cdee334a370866
41f83c83a9ae8d5558d2823cb00b4842
46110a31e7c579285ff9c2339c8e9dbf
46416847e3f92d1ef8237fc29167b9a9
3dfcaf660bc44ef3858ecb8685ec4f4d
3f4e20175a0492658fb36bf4d5cf98c2
681757936109f7c6e65197fdbb6a8655
519f62c558ebc127d18c3fef60e62349
4f634b5a1e8065f72e6e4547d016c1fe
6bc80227468c9eb692d2438774a292c0
6bd5fa275f86fe88435be26fe7db0d23
b2d892c0950643f85c059382960fda8e
a7f44192b9509d693e887407f1a51ae6
ad6968de16778610382de7d0d817c6ab
994c26013a352f808b86e95ab8e3fcce
9cb05c69ddfd3d0c66b070fe1fde554a
a229cdd723b1bfda03d371d880fbcaf8
8e861c37a592b136cf88ef71f7686d0a
9073b3db88720a555ac511956a11abf4
032c4698839a52711cb18d6bc712d5b2

410c36c79525e257c64e061b4074d7af
416b170d4d72b29f39dfc08450e8b406
444cbc26f924a2be1b65140932e8f216
451b862c56aae581e0834a483eb9c8bd
54435e2d3369b4395a336389cf49a8be
549fed3d2dd640155697def39f7ab819
3a404a2a3e5fbf4c6bb5afb374730fe4
6b666b91284d1da0b35b5584798de7cd
9d4d45ce7bcf796cdfcf03c554c465fa
9d724c66844d52397816259abdf58cea
9ef0cd655f1095ccfd591badc7e8c5bd
95c1c18003006c72d80e9e80ea1de4a8
96c0f2e8bd66759ea74fecc8843a8981
8b73fc88cc33a12a5de219aa511c7326
a017c6c90011a574bc8aa3bbd5756645
cc0d483ea30ddabe8ba03a570065b7b7
e2f5b669f7de05dd964385adef52508b
d6f40e2fc74139ec12dec16a57ac738e
1eb7e455580a0e0d6296a00e81e31818
1370e187a12403ebf40d43285a23fed8
18b9e5fad0f015a0cf792818e9e0591c
8386891ad94d249454b8c27130d34858
7f11ec3504cb4564ffadfae4807a1dcc
75d981ff0b6be08fb9b32a3c1cda9ddb
761acc13816a6840bb5f52fb43df45b1
7261d3d4d2cbd08f620ebaff827c91ef
7302c6cb4c6ed4bb560d2019087434c9
6fc6214a9cc6bb1ed442beda98fe47e6
78b754304b0998ba58c54a4d0cb7c81d
7926abf8d804792985898080542a42a7
79f3b5230012e5dde7657292f7e7d5bd
c7f4610b6d91c32b46e5051c4f8055a0
bb9974d1c3617fcacf5d2d04d11d8c5a
c147843560520bde0bb4c713084fff1f
af8979c31b5656ebfe82a68b2581256e
ff3f1c3486c852cc20daac4e97963e1d
ed7907cf7f4469976c936a73067ad0ad
f9a2bc7d3838b886be8269f5aa7eb0b6
e42a8cef2e70d4f3c96c2b8073e7d396

SHA-256:

92be93ec4cbe76182404af0b180871fbbfa3c7b34e4df6745dbcde480b8b4b3b
a34d60d00ac67e8ccce6c5b969e86e969272af2e2479e17b5bfd0b25650504c4

889f1f6873a090162356109f0f3984c044094ea789028ec3e20ba2238d269160
a6abfb56c25c06c5c12c08a8098f427fd0da11c5930a02ebb51ebc117ff63b1a
34399b371c44e52dbd17c6b4e46619f7c7131af20f66fd7a2c7f92c081d78276
a0c9b6a77dd3e6738a9f5c1a6704adeef904831d29392cf2c24a5628afecf563
e80a97b02bf9c43b8d288097caa38ab85a03ec1f8dbbc7cced1198274f60f6f6
4c8202aa414622c84a6fe32bb0402c30de964e84dcffef452e830c6f3b6c8467
667992e8c195664ad87fed3e715f0a52efe79a7c83f67d031c3a1affc6411e5f
d0d63189a28406914d9d49e8164dc716326f849cd35195ad56bb7e7ea0196ad8
dfe0e2cad843ee66f7bad85e62accb76ae54993eb057041e6f81315a3c99d522
b43bd22295f8287e5f8126712f0db11afe8b2bdaf918ed361c0d0865125a585b
0c09c662699c507c553317a909665952562bd7e2434c4a719470f672bdada700
3dd9814aeae5530e514915c6f73125188a692d0df2e56788c4302cb63d406e03
47e0886ba064156d7914db02dec46fa8f497b20373c7f2d4bc8f3f13bd8fa455
ab608d1adb169040b6fad2029ae56c07fa8d45ee9e03f4b9dfebce2b7d92b1d4
72d71b91ceb7dda82db0ec8ca3aba476d01b1011057ae71425e34fa31af2ee6b
dfc469d0cca07e83e58c6266dcd6ac67c5d5dacd6c6ef2543b3ebbbf6d35a280
801b101bc935ae3c4a8b9bf964ddc30fc5132da2271a23b9727f2b78187c62b4
ae5ecf3889c4bb1838cca1b644c16cb32e815fc1e2fd0db96aa6ca6fffbf30b6
4a21f18ec5e65b77a9c826991d6c51c45001d2b013d317096fb5f1417da88d74
e5af968a8eca77ac64862db3f6c92d7d64db24a999d0ded30f272f2a220cdb70
0345ecfb3b26acc072a3a423a9bc6aafe8750e65234e5d1f820c07cb61a2fcaf
0cddd9288e87db957b3517ac201f2da309e782a8f127d49e1dec2c7a7312d911
7535cf27ca99f8f77c8ae918ca07e8365289f27d252283444b1e6a5dd8bf087b
145551d6ad9f6e6d825393342561407f9f663a43471bb1738f741addf4dd6d82
7d6fa3046a4e558b2ef40ae0a96001a50eb3fcaed9b00e4d7bd235d1d83be01a
cf7adf8ed9b779e62f603a2f23af72671eb331e79586c46b75bd95644a62039a
684523927a468ed5abea8f6c0d3dc01210ec38aa4e0a533abc75dc891d3b0400
b6e9a1ab662304ad11ffca314fcf3d29bf7bd8cb2ff06d9b9727eaed576384b6
7317867ee5207f6b7195930d0ec3938130cbd2dc00adc8ba0cd3eca7114f4b26
260fa4d0680272feb537aac722466e58eb26c5de2ac858c10d3a244655544313
d9cdaa649b7ca7b9f61121d269801dbbd68551488c8423ae3a3e95233d6ee99d
0aeda32f977c98c8160491358491d0ad0898dcaa3366bde60c0a3bf8541e7b3f
bc8e469ac8515a23a3073a41099fde8420b8a40bb71abaf965c9031bd0a084e3
10112aab7bc43c9c138aad9b75ed6a69d7305ea2f04b5cfaa14ecfcddfaa4c7a
f1a45adcf907e660ec848c6086e28c9863b7b70d0d38417dd05a4261973c955a
c1227e575553f06fca469d43d02eda006033e5d88acb9b516f5ba64c030772b1
647b7a619b3ef6fa76b3e710a3f20b78a0a8ab6299b9245a893052d7b94b62fa
8a6a2027099e8a4d68f4c9931a8050b89aa587f8de47244af4ff399dfc0930a2
6535696186395b02608f16d86ce9b918e45012a217c11352b9d2904bf6a30c6c
ab70ef16e625291df6dc33903ec23dbc7b505c25e2e894bfbfd0110550d7664e
de22772c655890a73c7fe13d6cff49b1a560d19df04271e4bc3adcd5402158c9
f2c6effbbb203d5889f75b7d445f1a0f73c479e4a977fd7da3bd923f5b827762
283e3e8a651b87e055944e9b132f087f88181331bec1194f354eccf085d1bfe2

e4f66bd9eb1cb01f103c9a0b0616c3b073c658c1248f0e0f6faa06a629d7b06d
bf94a8f82f9b3ec1ad36be72a27813a661654bc5215559bf10b9eddfd49021b4
4fbfc64623700615410ec2caba6b931494990e1c0b210d76819edc95a8d1d8b4
328d98944555f83357c099208c3be597f5a0af0c05a3384dfbd419822177ad08
f24546590ad97b60b3c99a0bcacea4e405ba3884b57393ecf47b3463c8936a45
244d8dccd179a94b91e51f94be1e8ace42835b5b204e94e3f77f52dc866d8209
48b68a5ab219d7917dbe818e00ddbae889cf8655faf02639e4a3fbe4e46ef9b2
f0766afdaf89181401b1cbcf012f8e3bf7af8dde10f11407e23ad867e1b2922a
90218e24be373a8a8a3452d5da59d551a3b1936e7c3210cc9cb83995be3d2030
890f88af1756ce3296ca58f26f3e96fcace00048bc5f1c13a62b896e90ddea26
dbca56975506d64af911199f5510ec47c20d1fa22e505d0a157ec81fbce526b4
3a3574e202762e02ff701a9828dbd5b32a7072d3cb4814d96cc1daed0ca06a3c
2a6951077b1d0482e2dc35d2bcc9e28fe37e8e689736e89a989cb6d1696d729b
0cac3d4d2124b37e2498e251cc5faed05ebab4627ea5428e20cd75b286cb392c
bf125ba48088bb424781e01c63ec28ee37ff205c4bb65d8aaab7ae54d7c1260a
948cdb28649b547e980374179a93cad9408f2824e9be22c56ad2046d6df20a24
c66db0445702d00429bb23667afeef81f48b7424801df5f566b0fdcfc2e86e92
01334100f29c2d0fe2d37d037988b7d71a1b3aa767e99967ac1d5f8ad649d51c
8ec3f8a831074c5edb4d315b6e5d579bb2425701a13541c20729e6f13ab24d22
25c31149a906143527802034cc0084bfe787f6a996524c24a414c7c2e9e23abb
5eb471f31067ca3a13253d934f31422cfdc75a247f32d919ab527a43ca667ac3
b0d08102ac8bd55caba3aa479092c69461516a9f14ae0bcd60f457ec8f9c4e68
a88c1924ad3808521d5c62710d993f8831ce3ead74350327a5eab653eb7f7486
e6370e6438261cd7664383a784580c891d9e583a996506a0d951a4158a7dbd63
347f501484da36485b4533d14523bca6cb354287e10135922df6ce6d4704c9d8
7d9b3702c60ad79dcc3a1a6319e9575a38ed248d21ec78548f1db649687d7dcc
7cb1e226e9ee209672804a816f9532a607b1cc39384a5e7bb81648eaf0e8d80c
5153f190248a8507b38b6ae3e5661f56b2c4085776f09c02d8e67f1896ef46b8
2b1770ebdd429382ffcabeffe5799fb2b4afe684b68ed2e7c3f9c984c1191552
73acf81d65e59ce238db85b2e3ab8ce3bb9623aee426e6f4c1afea421f05797d
4b7dbc077260a677f7a6471bd331152213464bb4cf7701d390a3715131274cd6
909bf6916c2981a0a925b6ec66f341ca6a92d9b7862c3fd6680ef6b74189e08e
ed026685697d34152f153a09787fda9fee01a1c6ca434121446ee0bf2e520620
d1960d8c03fca7ae82fea6d04ca4c2c599038cbe7a775b6117b10a6a85a51ba2
5829ef8caba217f82769fe756f60c14d3ff62f444654d71c741770b1a1ebaeb6
a80caec4458bbeb2ea6b39e952d975485a0ae457921fb46d3ee91c26c64e37d9
12e225c4917624a5b363fdb1064c1f8e45578236aaa263190f352891ccca4f22
f67e87c65ac023fbae8dca2d204d729c2fd59c75a7b0cc78e8edfa5dee049bed
d9cfbf2201b24443b796c150c1138076f75607f1f6158a0093f0f3a5da06cdf6
7263106c58dce07aec8170039de94a108fc662293d9734f65cc5418fd02a7a62
24fa6e276ccebf7739403bc0c84692c8f3f42994cfffc1d14a0ac873eff00d90
8ed1a42e697f5ad80bd9c42b354a43a4fccd100a23477a7cf5c1a356261d9ac8
93a2fbb44e582a36a86020c5960c7cbf467395ac9aec9877362ff1314a3cc4db

3339ea3334e0b9a034d2ef403c9130992ccbe05ddd85e6d4e6d4524123c88194
94b153696fc74083d9d9b7e4fbf9f98a9fb74325617553f791151b53ade62aec
eae7095ad2d9ba61315f79915b3a40527dab38cfd24b810dfd2a90b91f0b0435
bae21adb236194caed6bd6180a8d33e0bfe9b7ce4c6c1ce53142a3645c2f1c4e
07d5509988b1aa6f8d5203bc4b75e6d7be6acf5055831cc961a51d3e921f96bd
ab4f86a3144642346a3a40e500ace71badc06a962758522ca13801b40e9e7f4a
b8abf94017b159f8c1f0746dca24b4eeaf7e27d2ffa83ca053a87deb7560a571
d486ed118a425d902044fb7a84267e92b49169c24051ee9de41327ee5e6ac7c2
a67220bcf289af6a99a9760c05d197d09502c2119f62762f78523aa7cbc96ef1
fd8394b2ff9cd00380dc2b5a870e15183f1dc3bd82ca6ee58f055b44074c7fd4
290ac98de80154705794e96d0c6d657c948b7dff7abf25ea817585e4c923adb2
bf93ca5f497fc7f38533d37fd4c083523ececc34aa2d3660d81014c0d9091ae3
17c3d0fe08e1184c9737144fa065f4530def30d6591e5414a36463609f9aa53a
8e0574ebf3dc640ac82987ab6ee2a02fc3dd5eaf4f6b5275272ba887acd15ac0
f61aa8c6590926533b67467603d2f42cdb1d5e1f20a5439d7e58fdaf81710711
0c63ef29d5a9674a00bb71a150d2ae6f3dc856a43291e79260992f08fdcd53d3
c9642f44d33e4c990066ce6fa0b0956ff5ace6534b64160004df31b9b690c9cd
722e8909235ae572c7baa522a675ce45ac7e10170be7428de74d04f051f473c9
5f5a1af57872610aa692ee3d0fba4a0171c2ec1a8cc3cf45f21f52caa2ab9041
167062593cb9e42a404dc9c8a0347e74888712a1256731724417e6f1d411cbbb
31c913899d50d78f2d7d9657e7534bd36819ec9571566216f1c963bf605417f7
6b656dc98773255cbc3592122db6487326e39b8e01966cca174dde87e72f82ec
750fc47d8aa8c9ae7955291b9736e8292f02aaaa4f8118015e6927f78297f580
952d4a9891a75e25e1c31a0514b97345ca0d8f240cdd4a57c8b3ff8a651a231a
31faeefb4dc4e54b747387bb54a5213118970ccb2f141559f8e2b4dbfdbeb848
4104a871e03f312446ef2fb041077167a9c6679f48d48825cbc1584e4fa792cd
677d4982d714bb47fab613ebe1921005509ed0d1e8965e7241994e38c3ade9f2
91c67c1cda67b60c82e14a5c32d79a4236f5a82136317162dfbde1a6054cf8c1
4a4bc01b20dd2aaa2a2434dc677a44cc85d9533bed30bc58b8026b877db028d5
74885df8801590c8be813c3dd841fb1b1b604723f6f9d4ee97472869751e4725
8892279f3d87bcd44d8f9ac1af7e6da0cfc7cf1731b531056e24e98510bea83c
4bafbf6000a003eb03f31023945a101813654d26b7f3e402d1f51b7608b93bcb
6a35d4158a5cb8e764777ba05c3d7d8a93a3865b24550bfb2eb8756c11b57be3
5292f4b4f38d41942016cf4b154b1ec65bb33dbc193a7e222270d4eea3578295
f64dbcd8b75efe7f4fa0c2881f0d62982773f33dcfd77cccb4afc64021af2d9e
02c306bb120148791418136dcea8eb93f8e97fb51b6657fd9468c73fb5ea786c
b18697e999ed5859bfbc03e1d6e900752e1cdcd85ddb71729e2b38161366e5b5
0f11fb955df07afc1912312f276c7fa3794ab85cd9f03b197c8bdbefb215fe92
18ce3eebbb093a218a8f566b579a5784caee94fadcda8f8c0d21f214ce2bd8b9
15109962da4899949863447bfdf6a6de87a8876f92adb7577392032df44ec892
D87b875b8641c538f90fe68cad4e9bdc89237dba137e934f80996e8731059861
021b030981a6db1ec90ccbd6d20ee66b554b7d8c611476e63426a9288d5ce68b
87e8c46d065ace580b1ed28565d1fddaa6df49da1ba83f7b3e9982cd8a0013f1

56349cf3188a36429c207d425dd92d8d57553b1f43648914b44965de2bd63dd6
922d6e68ecac6dbfdd1985c2fae43e2fc88627df810897e3068d126169977709
f79ebf038c7731ea3a19628cb329cada4ebb18f17439d9c6cf19d361b0494e7b
84e56294b260b9024917c390be21121e927f414965a7a9db7ed7603e29b0d69c
07c97b253452a2a8eb7753ed8c333efeaa3546c005ffcfb5b3d71dc61c49abda
167c7d7c08d318bc40e552e6e32715a869d2d62ba0305752b9b9bece6b9e337e
c1923226d58186c7e0735e058be80022a57e7e819e1e41b4c6e03065252be11f
ed638b5f33d8cee8f99d87aa51858a0a064ca2e6d59c6acfdf28d4014d145acb
752c173555edb49a2e1f18141859f22e39155f33f78ea70a3fbe9e2599af3d3f
98d27e830099c82b9807f19dcef1a25d7fce2c79a048d169a710b272e3f62f6e
29c5dd19b577162fe76a623d9a6dc558cfbd6cddca64ed53e870fe4b66b44096
abe82ffb8a8576dca8560799a082013a7830404bb235cb29482bc5038145b003
de5b670656cbdbcf11607f01a6f93644765d9647ddab39b54946170b33f7ac9a
e28f1bc0b0910757b25b2146ad02798ee6b206a5fe66ce68a28f4ab1538d6a1f
a1cd89a684db41206fc71efe327ef608652931e749c24a3232908824cea426bb
306fe259a250b2f0d939322cfb97787c4076c357fc9eb1f1cc10b0060f27f644
be3f12bcc467808c8cc30a784765df1b3abe3e7a426fda594edbc7191bbda461
0aa5cf1025be21b18ab12d8f8d61a6fa499b3bbcdbdced27db82209b81821caf
C94f7733fc9bdbcb503efd000e5aef66d494291ae40fc516bb040b0d1d8b46c9
d3013204f1a151c72879afc213dca3cada8c3ea617156b37771bdd7b7b74057f
9e141fe67521b75412419a8c88c199c8ebd2a135c7a8b58edced454fbc33cb77
6787242a810f8a5e1423e83790064a0a98954ab0802a90649fdd55a47d75695e
28bedd938ba05a172ea32a008d418e455a60267d7492dba66b940ef26964d37b
4ec1856bd5819a7edc96ec40c51acaa9d3045e2d0ea5f83459a4901371caf074
c596c7af09035e1b3555305a861266c9c1d6b34f3daa87c0005799a3fd89f056
adf577d079c772245f291bf2c94e4266a23a152cf7b2e7e2bda7aa1686fb389f
d5e026fc38c837b254e3bece40654ce528155db6d7ead7e4c5d0bde0c150ccac
7293693a6add51eaa809fa3dbd56f04ace26ca786ae3e125c3a84a1b743b297a
7ef4e92b0da2718fab88b8c3568a65dd9bff73d15f0ad2dca2a0297646b5ac0e
a9cae59189567f4763401a5908521d24f13043f7208d43639c0a052858cdb01e
9c77de35399621db98cb6b77bb3e08b43e2f11bff03c19aa0ba3dea0e9dac838
cfce402dbc338bb0b8e912c5dbbd031071c90a943441f572bed842315753ed53
dbcc4c05a350f44904d95e0a4f975008892bc8f599f6a14267771d28d6de0057
4ab46122d9b70ad0015d50cc15c1cf887cce28e844eb68e080940d77f784c64f
a6243b2a7cfb11cdca828ad7d08043ac9573c8ce2ca0e13487e1aae408d1c694
9fb8cc70b544c1011186df888f31662bea291ec6ee001dd85c5ba06f03b2de31
e8b55acf0db1518b70e2e007718d5756050b4e64a44cb911d12b52c4d359d5ad
1da99f69735d203a3d52ff1bb2ede75fe69601259efa6c5a080024ddf9276297
6fa84f3aaba12557129a59501d71f3a9a690e099ae8e3a4a9ec3c4a25c37a493
77c234943878d1e16d508f439b3e4bc2eab17eb68df9a297940dfd58ae0c7300
53429895e699445a717e75ce3539c5b0b3be42b375f518d5c7759bd1c8b48291
8b486336c770a5fd006b4d56c11d58a3a878ff8978c8c97470eec9819f975a60
e0d32df8cc527f8a183550456e3ec5bac6d4aa86576605bb1b770648b1c101b5

34cdfc67942060ba30c1b9ac1db9bd042f0f8e487b805b8a3e1935b4d2508db6
6f46cdc5d3af821b84c31d2c221e79f2d75c1750d39227aacf0cc5fd059a687d
037e92c575949a3570ba5097ee058a96deb1be72d521bb18905c9c33d856a100
2f6ed134adf8d29dd9e25b8f8f863389742dd5ff6d9104329c2fecb66b9e1604
20785552d82d461f5b4e480dcf51180e3f7b5d3e7286720f861e7ccfe8a2b067
0f245244a86a8b36292bc8b0a12b982e2ea366f36256223f8f9bcba37f335fc9
d20ac3fc362e022c7d09ff6808172fd0dce4e90aee4890455723f638ebff78bf
e9a930f839dbf4a7bdb72278d14fb8d18f5d56a492e4f9aa60b7b79777d3b2b7
8f2340f45861dbc36f8138f5be25ea9109368a31b2d577631f96ff9fff65b26a
887cc8220cd9722d114cf575f1cb7758c2e10f3d8904121dc9fe0b749c6955bb
20cc3da5bb77332fcc782e830ebd7fdcdc681b650716bcea943bee6736351534
cd677242197cdc89d7b8e2e3056030fe2bb9b384c95a7a027a7eee8182b8426f
96853c063cae2383cd47dbe417b892249c862e9112ad7177498384adab0c6a03
6acf5a78c38e220ff16277110f469ce725c304abb0e13d797de6c3ee203f2775
8e7367758f9cceacfab979457647880cef4ede8a55952e562c80ca291306ae4d
c126471d35f0fcff4ebafd8fb331e328b67e07312fbaa60c8a131e318b41a839
9dae4a24095b9a3870579a63c94c73fe8de205c70d95dfdb0dc9c87709215953
13b0f3b63ce276f8d30ac4f95b03485a6fe532754494f9848e875c460b121b28
09d7cd078a46a33750b002594eb7340af55a1cefe5f4451a8bdfcd6af97449bf
4d041a1bfd8dda989faa6a5a37ba49f988478dadaa110cdf9a98002f12a4b931
770f78c2633530293f6966d0c50b58dddc50e7d0a7522b06c1f4e4784cd40e97
f65eeb136e23d06b54b15834ad15d4bcd2cd51af9e8c134da32da02bdcb68996
558429867c4669ac1c367695de5eb18bd3bf49ac5f3a9462fb55d8db501cfabb
0b55cd286bf1199252f223a85039373872915317b2cac234a6b98ca819e8c85b
076aa7f5f6a5bdd9acdee55c6e3de54e6e8d5fd6fe2a03c165a23861e315f3f5
e48c5d26028815956956144c9c7ff71676e4e77297e9e60666babd18925dcee3
67d89c788f6c06ef6f8d8d40687b8a2cd611d3990443df58129428bd7b1c7ecf
ea1f4678e075a3fa4a096dcdf06fa91f1758365525ce47bc5ec580c63f0b917b
075f2ebf135b93bf3ecd6dfff0e34a2b7d524450fd419e51b3d91a81b58a3935
c03cccb7021f7660785a19e079bd2cd68ebd63504868eb7b4aaf23cda6457822
56bad93d98a01a820555357beb03a691f523ebb289b9c821ad85ee65137d29f9
962ce88813913c907d16b30a1c9f54e6d7281d9c901aa0e11bf6deb9b5ff659a
b289c674bac6ffd9c75f7d873165220a9ee78f3acae03406fcf32f9cf8406f1f
460b6796655f10713d4254651c15dc2255cd43f22ced0fa19f7493f5e66aef6f
29926c2c132b29b5f203184d0f5a2ecd83b4b89c34e4e1408c4cc66ff3034ce6
ebd4f62bb85f6de1111cbd613d2d4288728732edda9eb427fe9f51bd1f2d6db2
79293f3cfa2af27b9d5d2d7afa1d3febb8a02f7480491b0a8afb6eea0d10faab
f671bd2a4f5a4df475c6860bbc8198bcce0e2cf229a596ea169b38cb318a012b
bf3861bcd044d505c17f2e9293e961bc6075e4dd0c316230f792bdf52899137d
f5e4d5d5fde978968dce4db4120ecbb68898d5fdf55860e61058d91db29b7d91
53a30dfd90bd1208dcfe534ccd0b798d629aa989ccaeae952384cfe9ecb17369
39a5d6e5bff260474155e3bbcd33226af77f5f08a6c8efb99e345e4c1bec9681
49d08ff05bbe4a77e748dc8903b9d976a9b2176054ddfaf684c5699e84204f30

5b7fdc320e108e58045f210360c0f9486beab37860df605da01deddca9950f1d
8fd5cb42cc06f27de209fb1dca2d7046b40081721e39f2b974318d0ce9a8b293
db9ecff4368cf87406a0d64ccffd0df72ab875526acf1d1fe0957c9bacacbdeb
da1711fa9744e805389d5d17b776d8865626956d1dde8f7fa25cd5077e4ad8a5
a042affc1c30c55b22245fd5e84ba9c78c55b1c1ae1d32d941b63d3f68173a8a
607454369fa5d96fab6fec7a52a518eefed5136e4ebd4cfed238ccbb0f5b180f
446c3ee493fe127c2782748bf05693ae1bc7ccaf96d078db81a22403ff936815
6fe2f0646c13d40709fc322917d0fd9f38a2b7258d5475649e76d38ac0299301
3bfb3020c2fe3fdea274e7a318fce7af8bcb691ace35d72790b991ccf47ecdf0
dc782f3b38bcf3a0def70c89f61bd075dcb1d6328b2505f363de78188f9336c8
3026b25c0b76e9341cf894f275f5222462b799c6439a1920555d09e97b92760a
90c1ac407ceed31a17b43feda754aaf6f3e88cb86ea26bd70d7cd4d0dd195d91
d01b752163040535bf3da63d3445a2278abdffd09f137887bfbc0dc6c63b86a9
fd871ad5cf4f2690214fbbea4a27c551de845c8ddeb9149a670fecc9c282c45e
74163c0f602a12d4bacd0c94ceb307be976e23d2390d76373c86a89e0cff54d4
933e3f4451174514e299c1003c6dd66eff78b61e67ea52b662345a3194180296
1efc8b171b216298acd5ee57008dba55284e8741389cd456a0055d1cdf9b3c63
dcd03e22cd1fa86fa7fd4a9ead9cd459847a3d3b269981d8cff3189bbc232ede
cf4015f9c8f33185bf1f0da9a664e5ed8de08a06bdde98bd9135026bf8f7b0d2
f460554a43a2c884b9d3d76c9afa68667182bf55f42e13eee72b71d4ec80a90a
7099e2c8ab7cf2118a5477376be14c3c36101144e5361b396c7b77bb6a5b22ee
523bb70a77591394448b7ee6ef5dbbb150e3cb16bf77ce090ab6c04df037df3e
7e1419045c5dae0c0dc752f3096370bb59541e4ce6ed65579de6e9d9530c33ca
6ad05ba3f9aae47c3297bcb76fad76f7df4c384d344bd81cf3b7e17a42d45545
cc5f23669712ce42efa66054acefbe29a967c53e59206fbc78670672ea3978bd
ef1efc723a943b593fc88c5b6a02d33584223780a1befbbc6a791426247a5331
6a2ae67f900988a51d585d0c13eb5f5bcf5852de89890c093e9c4a538a427e33
a471f63151fe1eac42d320ed8d64122b169105845527273129342 2d570f42f33
c65d2fc5524f2456fe9da3a19a12e3a47dad3c20d5d13fbbdd6d23cf08635cbb
d2073c68f1ac5789d6cb1cffafa08ea89340794349967e1ff9a5b19a0fb2658b
9e2aab094e38c6072027fbdfa3cc384bbb2e5a189add8490232c3ac518eb1acf
fe2b3c0d05a7afc1574eac98bc16753dfa547750b24ff2097036dc1fc600f9c6
374a743f5629302301fba84e12c12e17bc59e80d80935cc5b59b02f893357c8e
95ea070bbfca04fff58a7092d61527aad0474914ffd2501d96991faad1388c7a
e9f36eae8b72b09a70df7b2d6882c591dfc4456ec0bc569343a875695c5d97b3
1af13122e13472b5a2ebd9b55fae172b5183f1379dc06d3fea775bb671f5412e
8894d01513b0125e2e23059d3e15b0973d26446c2b9d3fd6ced029e92ecd95fa
33802b1aa3931b8c63a7ad8851c6ab248f8250c0f6e61ee570e2200f84eb0ba1
a06a5b1d63ca67da90ba6cd9cbc00d6872707a1b49d44de26d6eb5ce7dd7d545
474abaa5ed31e7cc1f33c10ce8ae063a716724466017972f5293f34c9fcc1a99
497dcb807d3127aa6d9947b735977e50ec21c25d40c66e5ef3babd76bff07bf5
bbe17e6776f26d399515c0ed6cbebd3b7e3999c03186d32b33cfc0a5595a55dc
def0dd0b4c6dbd9e44fe2da8d241224b818780180d626f5ba106ecc81237480b

5d0224c0811bd91f30b282646e9442bc373896354f681611c0cccdcafd947085
be85325fb5c7b18bf0f5f27df6a51d39bc5ce5885b9ddc7c4872131d3a05bd3e
febc9d12ee6cebc3bab4cc1cbd612685949361519103e0b97505ea4e4fda64be
9b525433b7582998bdb98b1e0a74245a46026e309fbff984697045560eb11a70
7fb7944fb452d8588194ea746910ed782865efb991fa02479e429f8fba677d3b
79b3453196841d01f953bdf8aa5eddd69aa66c92387bcf2584341794ccfd3b89
446e00a53014006804135ef1c31dac6837c0cf635c26426e396b3067764f956d
600e7cfeea0ef8bd23cf95602a6b873898aa51848909aad1a7e8d4c5403797af
7d893d4f077e8e76a44a7830c5c3806dc956a6ef1a06c9f2dc33477c70f8cc9b
6bbd10ac20782542f40f78471c30c52f0619b91639840e60831dd665f9396365
a2e9d9a00e7e75ab1d5e96dd327a89b55608a0319461f2866aadada5bd50e728
4d0114b1292714a13d43a4c0de3ea4498fa752354ad4f5b73a8ba441af6064ae
50281cdd1b22f2b85de5809bf69ebd10e399410f519e357c1cb941c5dc7c95e1
e3fb0ab2f3d11f12c11b3ee1e1781eaec5581def820afe7e01902f31ba9e1936
9ce56e1403469fc74c8ff61dde4e83ad72597c66ce07bbae12fa70183687b32d
8d7eb0b7251bc4a40ebc9142a59ed8af16fb11cf8168e76dca48a78d6d7e4595
7fdace59ba9f8cd15a21e5b34bef75f153cfd0f5976e5cee14065544ac434d0c
0d8e8723bf5a62c207f8c7e03bc05db832090c7360c0e6db67b71d96ae4fbf74
f8c96e8ba8ce62ecf5cc506ba08213514a363687e095120ea121dd4d5bd0cc03
c7b233d41fe818ee95b869b0f4c92105117328f859819b626782b91fd549a39a
81f84722878270535fcc73e14298a9dcb8812b15f1bf6564eb8c64af8320e689
a407810865bb369ddb256a1b43e6871e62d3d1620e69bdf4f76bd80e2a7338b2
7090d5304e3018293196f50380490733616be12785300034ea7e3309a14761f7
8524a95c431a3b33934f9a0525c1799762cefdea8dadd97d3f244e65881b76e1
61c2dbab2a90512689ac11e724bd8d2923a30780bfb9cac884ba4eb390e8fd40
9c4e56d1b69bdb2512f77b7eec49198b854f443d86240a6eefd6463f2773f304
e3f2be0a6d44d5f85664b83021cf4343c09d706483022d4196303ffad6998ac3
0b89198b8351aee8b1c38e35fc1447164f7416c492978e9351f51a52553ea400
b9fe6916a9d01a68c2e7e5e7e2cd18b9740c6901d5dcf18bafa39e3566772ad4
02cc6b7221789989e548f8595a2de8f2d5eae436e5da9cfc643a78537496631e
8a57b906e5c6a098439a55820c866b2171cf04584b85218cffb03e989e3ae531
24f8b2adf1b5010bd6174399a62b965f672634db0abe03c01c642fd7a53d3305
576bef233b1956b6d418d61f393cf3a67c567954b6fa7776ced1e8e582b6b847
457d80b92ae27b11603695c1dc750f88ca77d4332462956d8934b421a98ded2a
f639eb3176848fba1354ba17010eab95d1e46a33afd752c76cf79ee7a487bfd4
2977b39fafe2f5e0ef9faa0e35392d8af1bb3fee35435dc964e1b14eb7dd2135
b152692a0d69346f06be23c114e76383c2798f72e3bdd2f248302cc14b85fffe
353833bf0451942428b1bb9643b59bb7c5fa27850433b1e1b6f96337b5daa844
fc37fb36a8df2c04fb06bf5648dfb4a672180f2bcd8f3d174d93cfe602f3ebf8
7ef45380dcaeac418b63e2984153b91d64b5f1a57091450d83ec1edda2f38341
372c8859b43884ec0ebc76d40216c29fd8b1229c06148a2b1fd7df6f66cdce37
12f05811ecdc44d40b613efec6d9ada72752e76a39eb47e000bfb17ac4f0ebfe
b1f02b5557b6987be726cc85b1b57b9e695ac3f1fe11b799b281df3aef9c2792

085fa0a03112b3db44d5cf756b5cc7ed5e0857a08da0dabb850ee10cdbc3de90
6f04d4410866cfe143b01e0c38b4e9c22b767ded0647392460c1aafd1b653642
ebdd59f14bb47ec4d2f2b150f8729965599c359e35df5eea2f6ba2544d6de31f
43dbd757f5024ac19ed6b85609331505d9eeaec4e06d2262ba441f2f202a9b0e
6563ca08295211caa67101ba8e53c7a4f65a0ad5af7bda4499f7ff0e781b2b34
5a14fcc3baf684b01dbff197b9d647da761b31b8577881e1feb0635cfc2bfb32
6bc0e722060b544ced0d0aed81b5809255971f50acc897e3220cf9d299f0445a
34a1e6ea880757ab8324db12544acaf4011214bf6fe7549f3a3e543dcb4e59c4
fe5746cc1fd72d8335b3f73653a3402c38921e6710a029a933be2caa7b86d61e
d4ed9522d417e0a4f11ab20c3cdcd8ff6afc6a136151a0311259c5038ca569d2
327fda502df4d048bfc6f9d0c869a727686b3e6aeaa60bb3e94b47e6300c203b
ada76741df6eed1cfa0fa587a41232714f13375a467a7f02cdd53fd800079755
82a93e80620a33497c7028471b7836d23cbb86c0d99414a31ed378a5422aca22
15e9a85190a253c038e1e3907d062d11014a0189e43eebe35127fab17e216030
084be1258d89249a4ed96baa895b4704bc09624ad90cc0c94f036ee8a09bcb96
fd76947f22d1fff4fada0343714ba61bcdff659efa929475840e88643ec07efb
648d7fede4397c0a7d1aaace0c18787306724a8cd85b54e5df8f95e16f95ae83
04f22fe1b482ebf7725826c89aa78f0952cd788d2dd5ac2ee35bb5f1f041afdd
d3830ea4509152b2c569df21dbedf3e925042bd8d390bddeada4b8d6685dcdc4
a9b05b86c4d04206fdc433b35a3a6dd20e73d591b03d073ad8b7084e797c5783
427f61e8e4d021d3dcff0df93bcb03e2747aadd8af3b6eee99707a227b8072be
58c5634fe61846e6f4d866ca959f4c25b98e83de362ce5f2bd4cf044d3b8e273
953319061c0e03e5b15859b8bbb5ec750ae60761c1fe90d48a69ecca95cda1ce
89cfc0314523d71a7641efe980908bd5c1ece2a15ed21d22ccf940ec40b97f64
6727049bdb444e784e41df078d2c08386c8a686f8a1f693b53ed867c655637ed
adb2995540ae902b7be4eb2f4ba0147db2326bdd1ed7a361fa9b666cad06258d
18f3bffa21c975886f3e3e5a5fc6284470883f9f7b89c5d6c553ade6e743e153
e8702eeb9341ba3358f2367ea3d321fd337a6efc11e3e648be3634bc5e990d76
9f886c8d95a36428d17377dd06f2bbb37d6470897621456f4f1352b6f2c157a0
32696554015d6433b2ec8155bfad3e6519530ca89226724f5ac257f5c6135763
a316fb26c422f5f94cdfb43c3819dc7bc40d157efdda57562b36d1782be283e9
4e7557d43c21d5502baeb39e41a197dbde0eb3bfee5f82c463a6c3565cc74aa9
0f2c54f1e2460a8968fd418c3bedfe285ba4dbcc5415721a8efca6322dee9ae2
354302e538ded150d97a3750be2a0a3b00b8cd5c80ab73816c7ea5c81ea0046e
94ada57c3823aeeeba9be4a5c2098676e785c4048b44adcdd0bb6608a9d83aca
31c38a9cfb1d92b8239a8d01f5b8ee9af77a70093a9664dbb6ddd917e98bf690
e4079e8eb93b6209cdc06f3a2ab4b97547035cabbd17bd0ada89cd2b740b8df9
f038e880056a096c74bec67ac8df39dc4beebe72332bf03d7dec57a9e851cf00
29cca2ab3db3c2f476c37cf0a8bb12e5afc5a8810ecebec14d6c37ef1ded26d3
78f33acdf770c6439f85aad95c3ae6578533dc2de912e2f7397260d8849c8d06
02cf51121a54c5fd6b952e2c16dbc0bdc947eb9ee14f5d1553b244d14f7de488
73f9aa545c9157487118d4901acacb2d9d085aa63d7a7fe5787c576bba163668
397c6c71201aa7c2fc14ee1928144f85d1f7842b5c471bec5aa2dee42c4ce7d7

f80d0cc6dc483aba3298254bed9063d510ffadc1abfb145868f56db1e66c2489
1ade9cb3e600184d654af1063ba733a77282d8dbb807b2166050a4c1da22e2d1
f8605dba534be40c4a968ac6e112768f464d002d9ea35cf4ad587b27cec78418
e905ecd5d76e0a46d706624120632c7c7614b14572ffcf71757756bc99516a00
2ff1024e9065187aa41f8a33e87ed07f8cb35ae2c6654430dc47389a9a2729d6
8f15d2c3cd2e8a46cd5046cea5eb6fc9d28f0a69d452fbd2a39dab5c9906c833
69645817113af8bc1fdbea2b88937255ac1fba1123442773bfa6c48df1ce030f
b948377fe2abe2ee5fa7939967185aef5b392fbc26d15c262d97ad1c21252ebe
28701f8a3579d4f38a08d6bb8ad11e8c827fc14816bbfe1f5e6f5c8628fe2172
8b396b629e3ff24d7151895d2649048d99ad235c1cf79b20c3fd954dedd1861f
70e3f6f428f4ff15e991a0b8c1fde01900b8a61fffaa2cdef37b1b9a334e9103
dcf5cb14d4f41bfafe9fa534226c48274b74976f5f4b257fa853a411688d6132
9f929f612d6b30c85ee7018c07fa57a462891bd04aa56c595e32fe6362eef267
173da45fd93c51f51c5631a54688279cac7ece9429a80999aa950377b4c26d25
d8396b77b4ab2525f74e2ceac774083dad25e3e5f3be752251ae3d8213df02ef
e9641cf0d4d25403e0a7ad2c622d744fc6436e3ecd5ebd02cc1e1eb2fdbff8ed
7f83a381cd27e5b9a016a664d8ac957dc57bddb727733f6159ed6b54e428035c
5043eea8f3bdbcd6326851a951c54ccfdeea4bb8f12e7e7f36bb7145c5956dfe
a93b70f827d4a48fcbbd6c9018306fa37de95e4a7a32d5d6d47f44b52769c94b
a8d521cc23c0383559f6ed5d3d7e320b1bee43a6ffdcabbff4053c6441538e8b
0775278847098221e987886ace76a3b62baa1900604c6dcfabb5cbc20a49e52d
fd890b9dfdf1aab95d5e38cde887bfc12be3d6d30a649b5c3fc52725b85a82ab
619c707672fc36279f7983f95387e5fdcaff56c58620b23e6dc47dd200add9b7
93ca053622afb121a1b74076558d37a2bde2841625d24a78e3f552939562c8ef
8b3237e5e41fca16e69f715f22b42973c0ca80aafabea8e9a1d285bfa51a5cf6
fba6bea5d5da214a70c7387f538b33184519c0b584aeb48be9f7fc471272e70c
a5f5dd52afca9d86d620f10abef9610a0555e525d33799dad2bcfe1a6bdb6ac5
b5aa40a19abd273321e9f0019bf57b27da832d2609cd2569d1073affd4db08c3
2ef9708e32e96adc4b830dd07aa867b49c7eedafc81a81bfb9985af5c2e86670
d5453fe94a07115f3f340e5029d81f46f9af706bf2d079c829fa86e6bd972233
46427cebd7bb779bf02911280bba2f4a4def92008d6d71842abc4bcae4ebce0e
b0036e9143ad336b23ac33ebd8fab5bd5cdbf884090683e927bafce31e314f4a
b3c10e386f9c88b584809cab9b6ff097c3435d365ce3ca38b61df2436113b15a
1a957fd82067e6ada61652f5118e02822b50dbb515e13048609a3415bec49d22
b1343bc27a5db200206afa1c14fb402a263482bf2f532f1215e88f3dc49c54ef
39bbc283ce079ed5adcd1b913b2c780e05480a5316083047424746f4b671f649
cb461f92f8747c758f49fa38485fe22a401849f6460cf7a6a783ca3b558b5e8a
62fa446ddbd9e7d7324fe7fe662c5382dbce8c71b3c10778371d8621b727d4d9
751328177c83aa67e73284bad4841696b7eb5e0c2b211a6c4a45881f15d79340
8a46f03d8d7a60e09977db1c468bf1f64493cc412836ee515f9a0e8325184336
a3367e9744f801862f1e5028763b0f5ded22d3da9125a3338eb14f8b3330ba1c
1083637f5a5aee1d0ea9768c372533da4fe28096eac35e71dd568429ee4086c3
8258738610d6b6c538333e1fc3b2a309c37198e45670d78284880b21cfe06905

63b7a3b648520c46d7f9beb060a7e96be517db3753811b3050128e2db1f805b7
41c7eeeadf543b7a9cc551a0a69eebed5648ba1659776511397c76051c74bf1d
977c648abba0aa99e61b7c4e90778ae9f09e820cac8aaa15228652ee8565b556
80da13e4b4365248bf0ea0c0244becf5005c70ab9d83ee16f38cffa97b8d05c6
44f3e506edd39939240891b1a32adadf6b7433ace58a8ff075ce9fd0e2df993b
7a735a6b027cd45a30e09ef52d4c31ac20cad89e8150a5967bbbdbe1c1b13acb
62bdf11506a620ec1b3069536c837fa8017fb57ce0f6a1c3c81acc5d5a94f237
8a207366a994fa90a5cbd19e7ae3d38b0cae1af7d4079c857373349801644f2b
24b37c95f61bf78566caa97f3dce549cc9e905e2bcd79c0906bd5394570afd66
c41e6867b6dd21f77f57717a10f18c97ebad08de1eec88167108c24c196cbf21
be8557250c4ef21e20ffc014523236401b24c2cf9a8142a7a1b1dfcc533d2d26
dc892687463cabea95456106c5d1b66ce0821c1b133eab4c38a45f0327c18e91
b6bff66d9270a239d9221195b0bb65c675d8bed5872374ab9f292cc8dd661832
985d30f2beaa76d6ce891b891656700e2ef14fb33820254670f32fa6b27b8ee4
3c97150cd36883cbdad28e05516cb63b1e490b9b5107bfc7545d5f770927a2cf
3411150742d47a826872af9b6d816777f3abb5a2fc6e11f0c13b81e422168ae2
f1027a8ce507b864f2ae2c6b70b8692037375129656387 2babd9767fbb059fc7
bf590551b76a76dbbb3608f336837ce06697c53f0fd35838d306bf60925bab1e
94ab06876227f50fa1056d9e827bfda7a1663d564cb0c06c71ea538e98f21c56
5cb86fe5666aa806f7d653782505c428e9e9f10b6aeff40ad8415c1910ebdc7b
c6d577252a56fcd42ba37317c894ea15026aa4b7771b619b003161e95b54dc7d
4b3381bb21c2d1d73861b8aa0c045fd8af62c137bf8457f5fb5f8a51933141e5
20f09ab75ce4298915a72047e339040f0a416a99fd33cf5a1fa1c8bcd9869c06
b8e956a800d27254ff9e32580c927b0647336970b1926b65a04d3d385b770777
be029eda6121e34078b62f7bf41b032bf7dbac47038118960d371ec53fb76136
648da7fef56097b4e0ef51c8a5d503ec6a078bf3df0671a34e72fe3b7c9308f3
ac350d37ea708570061ee9e8a33eb7f6a8379c85074798cd6053810a7e11be72
a9b92af42dfb524ba4dfb6678f07cd3d092f787883bdbcf3bec94f31fb02b731
953515d0316a6a15073bd326646e9a7ddff25c6e114c7b33ef3af9fae9457089
a395f3117130be7b870cc14ced1c4000dabcd433da4093f5806ab3d077a1a5fc
53ea1062db08f39641619e4048eb946f95fbbf75f3207e0c752f1bb80dd301e6
aace71b910db739e74ad861b6602a4bd9cefddcc76e0a7af07600e346ffa724d
d78655b0159bfc0a5092a3bdca5df9df596e540ca63817efb4fef6b3483a4367
509c2d8dcf0c88b2d45c34696163e6be002a6c8ca773fe1aa5f7c02193b890d1
4c52d85058e2c703129ac13ca622fb3698d8fc9a603f87d3a579a59f27b71c07
6fa110eff13b7c25d3268f5987ef44265b6e3a526a8f920c4dca3327522b2a69
145b2267d9f66a1dbc156880b78502244df31379d7140c46f8469e24b9b4868f
308cd9428c76be3c18ff1aa5426ef0ec3ffe4b4f11426282c0b3a7bcdb4303dc
a84fc65fef7bad1496a406bdef35ece5c0a25e9acdc2002915513f6dbb1ce20a
c2acbe1d24a03fad1eda61c3835532aba253e4ae91a5216c9af48fb2a69a60b5
b1389eb1753925a90e552d986bf4bbce9c268427cd4428f6269462fabdf81407
2c76ca7f3e8cdab5d2119b36dc14526d62a66dc68d11b6c04c69fde13db78a1e
61c18ba58e530247d084684d536ef4e7ecbbb7519edeff7c423969653469ad90

469cada3f2c849ae314f9c91e6f1fe78998662750dbe8162982b49dafe41c720
4ed51ff918c3f3545f470ca872fd4002b747d8fc5c13bdc64d36eac6afa8c13d
472c640e3aa109d6764b3344802b52689f986e80962625603d4b0f295f8e7e65
61ced32180fea11a6da94f06aecc582486b1ece953be871f243d1a1941e6f7c4
81aaaf9ba8bde779501aeeb93bd5b756f22e29ebef308695921643101d91eeb0
17a0e2e1071b55f1bfbd1dfec214302e6ea108a94d7df41eaa6514e8809ca395
b03f0d4962f95dc06f38d5f5003fbc1f10b0346ecf0f467ac17d3e97752b9732
41e010421d14c84eab91aa934eea5559af423bb7d5f190333e381f54671c0349
2d38097bc525f1c19e603c7ced9eeccf91fb226df7018acfe3245ec1c14b929b
3ec5847dd91d9f805b6a7ba2cc6019ff55f348c0ad0982762f9781666dd719aa
7886d6b3d753d93c811cfd293182baaf1fd4ddf32fdaeae60d9c04478d9788c1
313126956556d1b6046058056b87c7b58055d9337ebc7c9623403d78c0c3b21b
3038ecf1ac6efa37175fb9fed9729830fcaaf9193ccdfbe995cc91d387b52a0d
2db1ad473af09f7a4bb00f5d430b10fd37a6210b08020fda075278e006485413
0a420383658b5b055d90831a80ae43f5a4ccac20c9a1fef80934161331dfe4ff
53b4c69d7a5ae473acd58ecddc0af309dd94cd8a29ad1d6477b852449b7e3e45
e21151c2220c2d770fda86dcccc8ea195fabecfcfd66b64d70a2f3539cccdc7d
e06bd69ed77d5bd085b4cf911420bca8da4714bc5b10b856ea8e26292dcb272f
ebb63681d2a7388e6f388a257023c6e9d37656623fe844e4f71b379be77c3714
7b6c0961a875ef54fc05aad00f1ca09f53e9adbdaac076f28f24465ffbbf7efb
88787b90652c7f9eb525ff2ab46f3911f94282c5dff823996bc45cdb9f0764e1
7b0e890778c44cc94dc4c70a39b8abad3c234439c6e913c46bc31f949a508e6b
395c14850589be33d35dd30c25fe60dc9ce1dcc20d42ccfa0334de5bac785baa
ff99b44cd27f05d65e668fb4e2327cc405d3b61c3b3cebd59f552de3f1e49b10
d36b2ea6c5a147491335947249af4c124957f0efafffe7a84a8c431ea0203ccb
aaf3ac779d3142bcb38c3eaa0551f7e3bdde1731c9cdd70b19a0777803c8b7ee
27926f11036b8c53cdea3ee42a1ffe3c79dc8db8c7b42b4e36ff07f223f2a9ba
65f19226d715af259bff8de39e2241110ef2ab4c193fd8558bdc68ae073bead0
020677e7e67b3ba926e4dd133550589df7bde3f8c3769b5156fdcb893d74b8fa
0d0b260a6c35f8f7277b65eb5b04f5705a92a4992d3a6a1d642905584051820d
9327054a9d5cf509c33bc170d925c201c4b97c420a32ed6dafcfcab74ef75975
5912aa2e72ff3ce0806c4b1f9befc45ee0c30d80a6a1e69719c47a4e9fb06e46
cde2f71914ce6b4b8721d77ec5106caad4de9529599997ba0a2b26647950c01b
91c3735296b58d78827c53eea80faf0a73c5780ff04d5b4b34b5944a71d00767
a2460412575cdc187dfb69eb2847c5b43156af7f7d94b71422e7f771e8adb51e
676bb8fee61b083f6668582b40b1f3c177707cb0b6e8cfbc442714ee3ff9710a
7d0a31d3b194f5d01c6111adcab210f8b0b19948579613595044126872425a46
3e1b01e6ca8cfdb0097bd7208d55f5051eaba258626830af4ec76c1593911bdf
5deb2dab773cffc3be4ffa62d1a60a892c8fa629dba756d7ba3ad2fa20d7fce3
e215a31d89413fc3c6a25b15b215d4454db0c536bec00ba464da3ec902b35b37
0eb730dc79467ef99b95b4db977dc9c65f13063099e48def6cb327ed596bcbd1
110b8dea1ffcbec94a55f64ae2d830cdb3db7292dd468d3a151e0bf5c0fe968a
bb48dfdef6dbca5b48442903bfddf53de83b5717da3e33ecab2e1336006e5ed6

b10fc8e280b07bc6726d4fca9d8ae4d21a1793604076507a0d11c10e64167247
d612153c6799156006675a501afab1f6499d63d2e5d097c9250ef59c3cff36cf
e2eab634daaf20b36b2f38558047feb56a93dd2c6ed38612dc3fd9002a0eda31
9056fea2df4ac95a8187db15814e674a9d0136467f9d77be3ba255bca27ccdbd
b8d8fa28786ab5d130916fd74e07ff2967ab2b30f5ef56a4223bd93d29abcb4a
d259cdc6dbcb403cfde0e4cf4c96070957e65b808b384cb4d1890e674fcb764b
64da33787b54a0d179d7f77768b7af1e6ca7ee942a437dc751073879ae6d6c14
c712ec2f809f31216003f5f3bce37294d11033781c10134af2dbb9b3abd66a0e
ce0b7f8ab3c630f798c737a343ea28766c5abb33edec7fa4d0217c270b288083
5e2cb28edf82caa31d343cb8b198828dfb07a382a771005b60c3ae2b2ac45e3a
80eb918351d2b53fcfdb88f54a519c54bfe60105865858810af4556718b18b80
5d1dd61fb9f088fcbaf98a91bbd74b0892d4f71b97621292d6d37e5db1936a58
4a00adb83e61ba92cefd7fe0dd8c83d8beffeb204facd0d1fd14cbb295cf884e
2fd5559054ac351f9d7108c98bce74f555b7800d26ab6e4ec04c166f136259ee
f274e3b14a6767facd45943de518d0d4df74dabe0ef9e49bb2bbbd3cde526d6f
2e837de8a8d60a72c448952cfcac80113de69209f8a76afe30e461b2a3633a23
a89acefcf34aa84085f883e244d81568a30e30fc6141c4f921713786dfd477a1
a40cfd18ef0e03899b4dbe3817b3341260db794e1bd2b089fabf9f0f2ec650b8
cd661a71d7f7e7076bd90af46ca5b3202b5a4af1067ac9ddff8dfcb8e6987426
663165336842b628414d89bf7377a70649e8550ab3b89ef746758f3199672e1b
955784eeceb7e6c6da1d44478aca12b9a6a1e40c75f8333e4cbd6df764d7f296
7d94300325464df86d9ebb45c91f583ecf38c2e5a6ad4f06712dd6ecb21dfd4d
b297755a71dc1bd8e5e584dfe8ce076c64b7f5e0499ec097587b21240f55c57f
994e3bc490252e90591ee14388e8f53136da5fac266a1b8325cf776ed391327f
6542ee7d3366d844032f8fc03289c69db6077138620ca5061bfb220959ffe81e
7d99a7dc4f6ed8b3f32ef92ce40cfb91c3c5dc8e560117389535bf5bb27b53e6
441b643e896283ffb547252a0b394c2399180cb72984124b8640f224abe3e028
0f7a5627f37685682f095234054fcba253c3cf280414a494ed0dde8dfa63cd8b
083f81943e72b3a96d17630067166d6fd06df02a328992eb54723ee88e7df106
a0ce7ed257fcb4ec385638a869c0ce0592371e0503762a3aeddde34ff182e962
f698d8deeeaa44fe208ffb1d8f3ae57d0b6c6f43d7a0bf41ab72dae7f88a3c44
3165627e4ded9960b986def2fbed402d245966315b54c3a89b510b8eceb7c979
eff4c3243fd0bd13b0884c69aa25c4d069332f26c817ec1aa5ab98201cd9c1c5
57e00014877dd9eb85989a158c6b0fbd4de0b41fa5f7a5f1eed73119553b7143
4c082bf933c3a873bd774f6cc2450cbb4c2fd908389cb07b6a9327122bb8071b
3d64a45e56ea2472a8cbf8df930efa64ab0418c2d3f4f92b49cada87be51f054
0c010a0898f7eaea2870e86e11320be494111200d3f760f15f17728f9969029f
704f4dbb64205a566071599b02b22886a582e0a08e6b764f9a3328e84073f769
d7ac9c7b70f448f8ff48828a23d570223a759e289d4bd5b9ab0d582aad196ad7
302d605bd0e8846d8261382f9d6d3c288d95c158f62f084b1c5290c7dfa4559c
a1bb1a235a285681de8be1085cef749d2d305fa8e76bd173a86a777a72442bc1
0feadf86df99be0fdaa52ea84166bef6d3a2f5fd6b9c07341f996aba88406c8e
3b9a31f69da970aefa1d31dfd559124919ae009ce79101ed28c31b83f1a7ca68

08e2f425b0ed39b9703d2c8e5588aa85db198bd656f5baa32192015880b93547
07cec4a087d04dea5b2ddc2b179419cb8e9b52c8fe57e316d022113fd4d93f42
68cbf002d5c65bdb9fbcc633470bb541c25353316f47d9ebbd0d3a7fee23db3b
537fc80ccc99df1e4a194581fdfd4e4560c18097c865ee24f15b15279264899f
a0eddb2bc423809474d86f890fc08bcb17d1c2bd846df9172839dbad937ddb46
4952c0dc99dea75efce027e0bb6526008e6d40b7f177580ec95e6e2c4d9f2fb1
440e5c7dc8c96c287d8dab0f91925adf9301da5d63008b291a027a9a472253d2
13259542561eab0cd77576366414654992744 30cd975ea9fff96b2890c53178d
f08b3dfc9e869971be9af9b68d428e9653a1068af4658408593975a58dc51447
b77cfd1df763ef721e455d635a8a1d51b0d65b56a008b01ac0b0cb9977a3df2b
eac43784d9ba3bad1ee431ad1f3b8e84ef65103376a2622e48b1443765d8fca6
db8c137451215f911510a79c71d348ab7c426547d0b12aa2409778d724cddfef
07d0d9d0c0531228f65a6755d141ecc1a51877c67d0201a9263e78f580a3f3c4
b48cad5227ef4848f7389b64dfb0945e2d28402b7390e37bb3df7f453a3e8a01
d7e7408bd1b3c89c9fc693fc9996e262c0b07827c2accefe1177257a063a5464
3614eb0eb68bc920e9fad8440ddfa24950ce84b48f221d9df00edefdb0f3f7fc
24debefee1d7922216044279fa934bacab868f282823a078675f7783ad08355e
7216c89688c1d303f04c2561f677d58c67b11100c6626fcd657d967900da1ff3
6e8c2e9537eabe0bea96f7696622f612aa127c8d6d5a24a6b3240f468ca51b6e
77e0f6c3b03834313696a2838628076ec6ecafe96a17e54824d6387ed8f4cb73
26405516ec357afb8df799e98f0383aefaa57f94a8cf3583d764245a237a31a1
cfb3ce110a126b5dfccd67a1b2174c1dca9204cefe409e09b13cda0a0cfb0c37
7e2093c257499140e9410379ab54df6a5d4e88e4112187ae32bbd26c0dcff0ea
6f09f6e168e755073ad1ff68e50755ad375569677a5ab04719e8f9f563e1a6ff
86700e4c17e80106c323805845adfb67edaf6815c50e3e5dad48823267bf1522
d31d43bc57661a4e25732120b3404825dbf1691809591ac519d6a6b0e1b9bd5e
dfbf403841dc37f0638770531b1e76bd41311be38aecc1ff195279cb01f98d71
d231e6600f0dee9655d46c40dc7d233039df2eb406c9bccf29c1d864389bab61
a917ced37b5bfdbe06e2f8a965febdf1f15d21ec3dba906c7326a5f38c16c37b
58b77b133e1060a8599bdbdb94a99fb7ed37b27c776475296af423eebad39f72
e05253e3889ab93cdda3fe3cf0696e98d4ff9ff4fce19abace52d472bc334361
423a5da767d83872fd49cdb23a2679e16c11eade5c6736724f234d6a7c5d3521
abbb17da964e7027eca8e904320abb93408f86fc37c17354413366b30f67c51e
fff4c3b4cacad968d34f765dbba45f4057574bfa52b6c0c6b65af83b3b5c2fae
5a06029e50bd3da5ec4cc19b8a9ea24f0d9b5b823cb13b5d3bc8d18e76144243
6295c16dbcc9850f855c61e2bb44d1cb5bf67c3a628524d3e9aab6000539bce3
69ad89659790720721d5826a7634958d6beb388c69afef8c99f99d6d64b6dcaa
45683ebf238580f114c582c18b536683137aa1c5b09badaf3e1d5d5dcdb3ba41
0373abd3ee03748c46b5fc10b8ec8034c2e15231e00ffbbe694507aa90da895d
fae6f30b8e5be75809b66853ee9dbf4bdd02450cd0c7aac6369e1df85a361993
e27ec9637798763779eee891d3485598ff35b06f3c2d3a5021256f5939439cd6
a153a8b40f3c9f673bf35f2fc606c967624c2345c24277635ea751725892bd74
df2edc9c52a0e5cde0222f6cbbbf39433ce02ce3653aaff58418b6d04141fd03

df1f612baba98746f588d0700192f29dab74e7cd914d87d5f44628aa815caeea
b84260370d04651f71e7a2b4e12ccc9c02d090aa43e8577533345f3b8f3ead27
71f94df2d34a936eb66827a723bb3bdd5284f889d8f86fa4589765bba8be252a
9257f780796c9d86631e7b33649a6396cb4b52cfca0bb5039e0c202e665cd68e
1c5e676ff71240ec699f8a2fd74f239044fbf9d1aa99095ba8397d478ebf5cb6
784cfb1bfdd7080c658fad08b1f679bbb0c94e6e468a3605ea47cdce533df815
e9de591d624def658c4c07c61d40652236997ce9cf769cc5c48b814da12251f6
3163ae82ffd8d34f0522958478b05baf31c6410c453944a7e0e84cda52f2a4b6
59f08d110f595281cc40f76ea270e9a6dbbd25dd44c16a83db7f45a5985454d5
a758ba816688b35e3647b95377eb8a6dc60d7ac6d66fc232c7ecc85d0991f7bb
dadfb1f20177cff50637dcc71704d8754eb39d5992334f9dbbedb74b7f2eac48
3293bfb473da4f4db7a78e554ac89502945678731d18c8f6f9ccd72bccdcef94
0bcf34306868b7f06d0d1fe4dc31ffea7d07512401d1a0df4eb82d75a1b9a893
e31e0984af4b94776c8fa9819ce31c10b25dd80592c39f57a5bc698ee622d5d7
47453cc59f3ba057219a7395e1716f5fe3e7883c657906320f1ca23895e220f5
ffb28229e4745f8114436d09a7db5bf015e12c52fff6dbe495c64786be8a61a3
7652ee3f8c2e706b1030b1d51c60cb6b78f8cbd2f874a24fc9b8a4fd75fd887a
760dc8f2955a07f3cdcbab4c22ec78b8598b7a0b1e4ac44c3c32c6ac105be386
82984519dba71071cbc2199e5249f112b687ccb1ecd9c2d25677a1e2b74cd4ba
5acc1165317ca9670e5adc26076582b29627dc11c9f430b878fed776b3a7fbbb
1a7ccf279b337593fd8a4f5f521752da9634a21c02603721c0f767dbba774d85
19d620c33ed4f6c05735d35b7c619035100bfbd642773c4b30f52c5efb9fcef8
26b1e6f07bdcc8e4f4840d559d57cc981987bb15dbc061664c12750741d78098
022fcf806761f6de9ccf4a125614720ac263b720069eb8e2ace150ef8f1de477
bd77d7f8af8329dfb0bcc0624d6d824d427fbaf859ab2dedd8629aa2f3b7ae0d
01de97b656ddc26ce4ed0513f3e7b07e01c6c9e9331c80ad9f1ad3c141c36db1
4ff387c61707a912059f9278dd445853df023aa4a994d94e5b21c8cb6d11a38b
3c0bcece2ee9c2f6cf5d82e122b9c05fa330a615848f7e867ef788e7d832f5ae
a8493fa13a055830673d09c8ba904c6f072d89a57ef780a0393a9d785d45e79e
641450a92f4c8d2d9e909f17ce75831f7fe91455992baff70a280d76b6959ce1
359a1b3ad44dee6069f97171188588bf78d989f7ebb08fb6107698d1dece5436
ff12b3b1c623c201a1dfe9daf1eed1065c7e3714bd031cf1b5b75b0047112219
6c619fb910363db175f646270b0f8334a2799ca9290c649931dc8844ff45c390
25219603929735d21187aa9de49af4dd3b4b969db681e0d4c2948c804a9b437d
6ae7f44a94f1e6263b7332318b595cc564c92d90580b6cda4fea7a2b28a53857
983ab49cde9ab3df7b0c8712b130deea11d84cc6f3d5cb0b545a4473db29b175
45cf0d99a7b96fbf079fd53871048e1eab8ae2633986cf7bbad0991c08155c86
f0838363d58cb764e2622d1517d7563ca2d0e5041b48494c28f31bfc04d6bcce
9d03e61a18fcdde0b207ac6cc284fdd77d73f47fab2e3076b538b9b1bcfbbbd6
6dbbf8bdac861df3846fa7d72fbf3518f7027373f4e95bede3238f02355a72db
5f0bb927d3f25cc5b5a43182c1a6cd01ba8fa7003b504687559b695703d80dcf
0ff90ea7ebd843020136822c8c5cec26e123e64b9f386e7c1f0a3ae2f2f95135
f3e6deaa85308b49627320b79d7f7835dc8aef30549fa9865ea471a6c7dca269

2e542316657433d3c11982666e6408b789c08a07ad5dd1385b0f1d2eedbd8e01
c30574268d0f662ec46f86a5d7f656c498bf7ae8150ef9bc29e38ae4b8a4e0a9
7d2acfa0c977d95e9c99aaf72323b39ade768bffc817b486656b4799515dd437
4a332cd110153e96e3fb02c37e926c6921f4a55a1ef2072ec83dad22931f2e95
282ad9c31caa70a4bf53ff88c00884d8918da023a7b8809b43bd564ed8e73314
8bbb63d18bd4b4d08f7441075670f8a73749ae550b59de034a6615ed6b449362
b6ee7bef5e4f0912eddfacffbdf4af86d3e83f60c363024bdf26af40d22c9854
7b31266399754180206aaccded3035620432c1422d32604079ae84114e575dc8
ea25e56cc3a69afc4b922a3b24f016f36615c950db5d8ebdef7e143a3fc46991
fea6f12ad72ecfdd3b5c08e69d677818cefcb6f3ba1b5526bb27dd18650e12a3
336a009ff29438fdf563ec4fce80493b848fd6d9adf3250774799d27a04c93f0
59f5df8728c0a0abb25711df99c6f984aaab611a7c0349a3d41c842d1f6b7198
4bb77c62a8dfec838a0f0ec9b4a72e47e3ae996ad9967b35c6a6fb3b33724066
26331930d17f414a8171e5e30ac538d2c956a9306fe54562b778441f1b74f239
004c55c21410ee75e493c39eafb12829cb3cbc187de545cb20356c7b0113bed4
704ec12f15737d689fb770dae90fa72952b9a0d1094309b72415e099944e36c6
1efe4183147800d221e2cfbbbe76b3bb0bf9591913ba03df424dfa3b3ccd6f2c
04f2c899db134f36a17aaf6a4c7e3d153ec1147ab48536b87aaacf2009f8f12f
910537b76b0d975d16f05346c913f4f941bc364f491234adf2926d6f2d187f91
11b2576aff9dcd7c37310ccf832047995598e6f06712a0a7908e2935a7582922
74d5df4ae64eaf5a72c9f240492c9ea03e8e25e1880ef29ca97cadb7cd55322b
cedd4fdf7aeba9a15387fb0e84e33a7b19485cbb5ee10a32865af2f5e7cf09e9
6b277ad52b76eb97d38cb89f013d3aa7a5908e2255f8b4319c2baa81fe9a47b1
5cc2fcad196355bb6021d2c9fd25e7c97458c08f83aa4b0c620151871b99cf12
45a3a1346df52370efa678e43c97430dd0d6377124a6a95659ec478a46c61a0b
32c04e45d0752dea622318075c819fb4db2d69690a5eb96124c0ef692ebecd76
632cfe00176024de8833d9054b049c4657e84f99efa22ce2a2b162a875e8298e
7e26d20871c595f2a077263358b0a1c80417ba487dae9cc27fc2fef4c8a69a9f
d06f6b6a1ca7f3f2453d6f91026b9089362db2e676fbd3a02d04662f6c449084
f02401f5636f618c48e15d9519ccdb5a994ac666c531316e8f7561d4cdc847a7
1b150b17e5ddb4c8de2f55164190828c300c06dea8b59bfec31517c67c2ad4c1
03b402a2346c44d85a3c2f1108ade5606198203677acdf633ffc21eb2a01f7cc
dddd2fa6c8a17d4361ef56ca7abd213a935e3cf880dddfff4291c2c7fbdf1ad9
e49d9931fe0a6d655b3134168ea12e8f5f4534a68fe8ea8979ddb07e10c2b081
c03dc46fb6f01e9a1bcee445378b62b49f008c88cc531e41f2fd095ddac42816
4426431bb5020c9ca12fd8fc8577ee6b96b308e4ea548f510103926854d01776
871b7c708c5a7e207f5f4420f4ce9d76602ad0ea578d84457057a69946b5c062
c07f389ff3ae830ae41294a376f362f08364deb9890bdaf634971a4e0c68a5a3
3d5cd1e9504023e45dad522fa08978657a4a0f04e464b7e9dc2747acbe8ea274
081f5a2dedd7737ee516397e376e6f625b76dba37e07a4bd3b13e2247838cad4
3052326e492167f29e638211dd0bf50f14261668773aa77517e6ba77b23afc96
c6a5c171e35b3c6c1b24ea57395d08acfcdf8b8691d0394819a49718ee8f74ca
69f59fea7516eca5602e8a4559c0d9664864fe21a259b70b56cd6e1c67db3901

7d40397520e001422a19ace058d74e3b8063177f3acf828aaab1f36986b6cec0
fc94d0a3c27b020cb70ec7f34c4b82f09a0684b42242bdd9390ce9ab446d18b2
1b730ac88405b8995caa1681b7ba068ac37df98cb37a1c92936e5d3b12dad936
e5a80c1e010b0dcdf64acaae4783fee7afe5ea2d4be575f54ab5b82706a91e26
7c12fb544ee4df411491573636029ba40149baea37094b6fd7c73ed31b537df1
f6319fd0e1d3b9d3694c46f80208e70b389e7dcc6aaad2508b80575c604c5dba
97543bd8b63f1b27c04cf6f5aeaf8aec9dcfd082b5de88af6f0d017b7405f699
d98290c7291caa674222a0659f446f63b92148084b86fc290cb2980ae52e1ae2
a4557b1c6e262aca89994a39dea510f17a88fa68f9c281d4a0147bf96496bd2e
5953b48cd90f0364b3c06fbb2a136d20c6ded520940b26a26ad1a72569f2cbba
98108921f0b98d2d25b9eba896982ed51c4c4d776a6d03e5a25818edf02f58f2
a4aac44fdc878c952313ff039b00e06a02ac8ee65c01eeedec7a2cddeacd5b07
c2c6eebb322a52b09e1dff22df103ee8caf0a438f0102eb78daa4d24e2510fa0
37abec061f2d7c0f080995d99aa1f6d43e67e4c33642446fe2305aa1d04c9ca7
5f9cd0f9ab982eb6197097f00dae8684726797ba3dd589ad30df3f9f24e312fd
fe460ecb4c52f21cfd390b29eb89d9c019c04cf6ce0e39fed390998c43e60017
08c2544b6a9f85b9d82e9dee5c089161008e3b89a4ca58bf4cfbd17457503aee
a22937e4ecfc71024007fab78a46e1879f07be79b8c4d75b3a3cdb8178238a0e
12e0985175c6f3850a884617152a9f2ff683adba0b3d6303354317bfc7c3e169
5d1f5a384a756a8a5659b78cbb1fc815b75be9063fa34b9ae938825fc34ad0fb
e179f03dd608b090bec933fa62d3714b6deda6c1629eec6bf82f2df55aa22307
6142f9c4ac27a3f5676c625d685e4ad500eaed2d936564b84fe5c0251e581701
e5eadf6e20c3c941717e6da78da8c77a3bf55dc1195c6cec3262d2110ab403c4
33da331fabda5a63ab9f51aad3d5548c1bc602860923913aaf6b5b12fbde112e
a68c6cec889147f1e40d586e716d13223e3f6e204e5d95b2856c2a386c3af5fa
cc81f28c91202a16456d7b17e0f96f6a387254d6eea3391421db8bf825326231
946cb06baea952cceb16ebaee6aeadc683d6daff735587e9ce0431286dcd2338
37d6877342c37ad2853927ab760ec9d154d898fd813041b0aa3e815783d3dceb
ca29928d42f9f800935c5b3a9f6d9d53576441620072974e5b54aefb85b0a0d6
b2fef273176494e16c108bec2ef17224b646ac006fe5dbc1ec9b454e352a9487
add014ff8b1388f70685fc032e84b8c1f83344e071312c4a4ad824c977d9053c
654665dd6cee61fc1039686e50b8cbf0db565a83f7c4b01a548fbeb2ed20fd87
ea4ae096096375b1961c304a841575c69b747cf89ec169db4e63117054e4ccb9
c306bab7e295f12600c410b6d843bffb74987e156a5d826e88521e4d52b0891a
a79dc2fcdb532da97c84693ccecc171de176b49ae652b172f151d55bfeac88d6
3a66ceb8117115bf1f9997ff375be2de3eab918de31f053289554fbba8084b7d
c7d63a172279023b6d29b26f36acf8186190cfd8b0b9427672ce6253bbdcc48a
2eba41e4c16f0b8ce4e3670c7f6f8264519979f3838b6bf213c3074398eed7c7
3dc7348f5d897b8ab8b4aa24d1dbb7ee38afb2b7d33923c18468320bbb557b1b
15db4847cc9cdc45dbdae8c8914c8abcc428ae2fc06f09c6ba98badaaa9bcb62
5224daf0439550238a17fdc4ef254f369dc0c0a3f67cfc0a92fd32807d6d90d7
30c4891e16adcddf9e1b1feb5f234d3768ece1e305cfd118c282d2716b5077ea
9b14c6c62e1d51dfb0d1788aa4b9d15378de28404b1714170f516fa3520d5920

860eca4febbe7add62a39cf83e323bf96aea427afb4f072be2f4c0de6290c5dc
305969c977eba1dc0d805419f778ebaf5b794dfe7138e06514e017c3192a8215
7e661cc6b6dc8925c3b26644d7e02a722548c17e8319c8de8a4ea34eb9e1942f
a1d6cf31e038b97ca712a3f9b27448f1df424c0ae2255c274950b8fb3fee1461
06d7db54b1284059a416ef43ce2dd7f15317f51aa327fefd8a183875d3845d16
839ddaba04d5aceff23685da7500c37e4f3b9acc456d5f8b46bab50a055d04b4
13d01e4b3c73136d412661e71dfa90a21ca5f6f2b39b15f724800ec4966f54dc
d8db45d397082c5a89bc054a69ce211213ebf8cedc726e9870bbb754a1a2b9e7
5f34bc5fee8030623a0e65fe3fcf8b3897f6cd757e3abed9ac3b3e05cac4eb71
ee7e63794795257d86c882bde532c26b4afa8d1f45fd398dfe2fd15d814b9eb0
9e3fdb30de85f9b5ab7856e082cf7410e17e9602d647f5ad7ddaec3d7b5bc0ab
e799afa7f161102e5c9fc11c0bddfe91efcba43ff3c3303cc6f99e146a6f7b13
38dfff46d7e186ee9e6be2d0fb1c4c85ad1d16cfbd5ecfd5709a12095ae22f49
c435e3f3667d0e5a6c42f9b33fac9bb41a3a1d37f983be9cdfe9059306b43c91
158b1af70462e5dd0e696c8bc8572811787fa091025fee85c64a9d2f32d47d44
bb847cd1c68ed0c404a0f596e4aca753cdbc1254c78e8b11d45f66345bf5d5ca
ed158a0eb0a7c1451abfd7ea2e96ddcc93fb3908f86965e8ce4c339d0dc1556c
f31189f18786bdff80a207acef9bb78b8738fa1ed27bab20f031137a4713eec5
41455ac55f1e1b6e3b47e59e6880189d0cc2b9bff9b8999f0f10ef1ddac66cf3
bcdb37f98e4c58cc9bf39060e3d70e93621c0d1ccca9d68e1c7393f5433070e2
5217984452cdd182b3d0184bd19514a5fe77ae39648f4cf1fed2bc273d1a842a
8d53d15740e89db21250aae47d9000a47cc247f38931196b5646ec9309ed17a1
2e23bd838023c6a8262ba38cb6fe114fc391d4f0347fde890fa998b05a2ac7c3
3140c7defd7885a562b21bf0a6dbb82f387734810af69c15378ddb5b3c6f8430
2bcb13bda98243165223239ae3869c2be267682d331022054bc180f9c8b260fe
f7c40acc2a25f09a2e4bc6e6258ac25dce15e9af5a78d09dabb3f5dd68666a89
e8ea146c04be7c0d31108266289a1e63d90c04e7d0870ef6b17a2976b8b89401
235df8f9dab95b9f7304bf2762d7a58044e2a4196a22aaaf859fe6d3764337e6
389fb48d3eb2d7a10384a46732ddd0ec8d213e6b8278cd6f46f5698f4f7c9caa
8425b3df9c6844f6f5315b69973257aeadd5375a8533edd2ce823c2f920857be
584c6fbf524f4c69d41d87c6c44e0466d847c00914bfd383aec66c80635cde2f
bf67f3dc5bc7e5fbfc040cdec410b76c486fbacfe433df3018a6a4ae7ef6bd87
800245f5affc8db1f045087eadb3298a1dccc059659c1e91d3917e6fc0fd83f0
9a88eeb3d2f284fb81049b55acbed030f9b89288fcac90a67969f36b5534b466
8ff4bcbaf1a47f8ceeb96c45648748e438c161b0dfa9f5b8cb1ae14ccc86b442
2a4926fe9f0c51add1d8910f78d5f02a748ba84f77afc2c92ca6c65d8cbf8eb0
b46be792d330c0bf88f9bc635dbbe5e4023f4111d80b5aabb675142c25d8d094
ac16c7c990127a986c4b34461c55eb3a46f85b5f66481572fdd3fa74aa391bd2
bac0ca7327bbbdb2088e9370b119b4a8906467e74d3840dc059f21ade24e4a0c
f7bd457cae8e2a379110b2add566d127e554607fa852139735a9e0edac22c3f6
866eb8c39446809e9da5d51708d5efcb61dd96359d219cd5ef030234b8af3a28
9be0d0552a149b533d17645b46fb0e81190a1f6b9f397ba6832beddc345518c7
4281684ab4f6738784137775bc6860385a386984790a92feaca839e1ed99ffb1

b702642bb7fee3b9e58d77ec6938eb5982db244694927c7682816cb2f884e8af
84c48ed92fba303dd7f9625b13f87abbed7557a429b85a96e7c9dec30c42ee03
0ea51f379174773a410e00b9677c9c4e80315707c4e3a119e458c3435876476e
73189cfe3ad4bfbef32cb62eba91effca866ab2adb3d2b3716f64501b2a2975e
53e5067dc5af9c4ced155873ce1d6e3125769f271bc69deb48b3856e4405a7c2
938979ccc2da9ee2a57ff6961a52ef83277af7f1d94d783f3eb81f41aea4f8e6
af0a44d8fe436f61efb8652e00446cbef66952dec560e130e6b591c6b2c680ff
e9a6249b407f0e9648f7d6b73f643b10f7c528b575494b352c86acb32bb20927
bf0e826c6b992a555d04bd0907fe202d740b56342700b36a9f396215afce7fa4
9d2c2b69162af1f910792a87e79f7e6321782bfd7b9efacf07cb878b7c5b2da5
b75cfd7a700027a28223f596c28275060dbf757bff43a0839a1d4025433304fd
57dfd2bfd43a30d8010edf816ca4fcef4b6cc11996f27818f201774f127e8051
f0d2246a388bc7375af5a3c933469479925a21e61074323ffcb73a99e3e41171
d88b4ee9235d7f0dd347e4c39f3d55afc431c6fff4ad0af8fafb42c311a9a3be
d959a1c63cfc92d288225a5962317056cf77689927870b04778248ad5b46fd26
ff526d716bd934baa568421b9c3f0326406788d0614e796255f73fec688d97d4
439b642ff1d22fcbe2c50ba3585a32986939192fcc5f72b8fa60caaeb19f9e19
a72a055bab77986d670d54b0f1197d54053c5fd185178667ad9ab542955b8ab4
cad53655a5dd4c476194b7ad54a2205d62f8d16275aefe8cc9ff9242e619a918
64339985b0beb95a1c80276921581d55a19ab931e1fcbedcb6cc93a46f9d5207
50272ee6c6e3727ff2f00c59ce3c162add3d4152511665a3e82173510e1fc7fc
0741a7e7bde5ec56834e66a9bea3d985e8b67f75c5bc86792c78b194869c91cd
f41c688cfa0df503f9e3b491baa3baa8078a2afb9d27bb4fc7448163388c7902
6ad56d64444fa76e1ad43a8c260c493b9086d4116eb18af630e65d3fd39bf6d6
8ad05a5987855feb2a8ed308a6b76bc085c819919b1c4c1e337c29e4f0fa6c52
ac4528ead85350280ece4311ae4f280550b84e77d7b14c7c352c028772f886fe
fa31f427a6bc98d50e2c75fb3a5e398b8905d2cc959226ea079e00ade124fa47
7b47c391649590bc310e527373fc3a1ca4dd50921a4c05ff4c1a3fc6a4d12c61
459c160698a3da83180d6e72dc884715e21857ea46de4e924015c72081099311
42c9d7642006ed99f9c3392b269e9b9defc1e91ac8404707ee4aabbf25557426
9fffb082e84d20815e2db6f458329e7dde9f819e542af23019a602629518da19
0d858ed0665dc54bbeb1e7dd17b0d7af09aa2fd5244277a67e8aea7ff3ff027d
06a95a621f8cf99fa703768fb16c1b48aadf9a95c1aa6e53422b1736d193c806
34248cf2a36bf90042cf6bdd1115b1c4be3d2140cc3ca2c1259faa3da23f36d5
47c3ded60e6979a26869aa8879bc59477dbe1fb87040d49228803a59dbdaeb64
d9cd20ba6a161a41a12de9f94e4d57f28445b34b37653887c1941094451dc7c9
57f038e207b777d275d1266f7043e1691462475716c621935ced2111e5e0060c
d1a262e469e7c2cc9b54dfd22c60db534f9cf4d950d266b593fca71b81504345
190d87bceaf710c226d50840d2a4e0282a8e53999736990a980816ed999098b6
b2143696b373f65c3b9b2949d7b3c56a62bd714ba1be741adee85e26f87f783b
14ae412a657f789117a51c56b3581dfb16082d3884933b4e600ad7ccde6d6a4c
84aab1614c01ba0f2a1d4207fece0a740a561e0324ca9ae934d9a169cfb28a7d
e165ea0eda2af4731e680a97a51dcd2cbb382569e8afa179f2eaeb86074486e9

8893db5e27f952dd00e34a128f877bfb4ffc92eef7a8ad4c62dd0def470e96c2
bc565bc871a26f1aaa6f9171f416649186872a7dda093bc3010f5ae2c5f9f028
89b80267f9c7fc291474e5751c2e42838fdab7a5cbd50a322ed8f8efc3d2ce83
4e66ba3e35fc5665cebf66a94c6ba833e391024c4270ef8cd56b374cc6f1cfbc
8d49f2821af6ff22dc0bcf71867a400eae95f6cfef036473319e0dcb9f599171
527ef4c44bd35b6763c6b3f46acb887198f1232d15aa1cd83d7d9c6e790d3d6c
8e6364356dc908615f29f625d124ebc8c22082d2d4f979275c513c4f64a612eb
0eb0a20ad325e3671a249e989d1249e2dc686ccf30e10a6743a219fdbc4fb85b
c230eadd0755738a83561ae1042c27c981f6ee83bc434a107abd5f0d1a328f57
5bd692159fba5402a1ec58449e4b8c651d8341e1b8c93e7a080b66a99fa78c41
037cd208f7b7060813159aab0a76efb90d76164fc9917dbf87e2d2d5157533ab
23342c65ef4ecb58c81b37653db1ef0cdea208a3d9f34559c905524d902a8c85
b8495877c87b7bab07738c134033182df2ac258ee34c2f5f667076500e07031f
a7c87a1755493b9c4a91d680f45496b41a86263688cb1231276b43f2a3a376d3
7900546939d88b26a3baa3cc1281ec8519c78b9ff5a582f68260f2f50055030c
6ca39f44f7815ae3651e60e91db21b0195b41b1053a68fc519f2e056b7cf92b4
38dd63e1ef9952bb89d0fa9af86f9c2f37573b16f2f17ddfc5e3ec19bb462fb6
8e879c05ee3c6129c413078e7bde2eb127fe07f6fe7e698a94e2ef0ce262a3e8
e6dd8c69f132c74cab4c52de9564a719a316232d1881d93e7afcf5fdbc37d4d7
09cd1819f542d4bfbdf80c5624cc39be22103a18c52c305ab4baf5e7f32c0f46
25292c05d589e36d711c1a9195d0618c335a778cfe9d497882d064821e57a166
745bbef2ef887e64fc4dd9a8307ce451b3a2aee39021de2c917f6b461b2a217a
228ec161435b8f8a450ffe179219ca8c4df2d1ed3b351112be366d6efa38f559
b03bc92eba05d7b30aff6f73dec99055b414a15a790af597a3b0788e832bf762
2b96cec301fc7513ca361d4f5ba36812502947def2c0f00fd3cbc5c03cba874e
40799737a777300dec8d7c497683478dce5b24ed23b010aab87aaa256e3d36a4
0951b535828ebf6b436e687d2893bbce368667acf47c4659018a37a8f6857d8e
4062565aae249adcf08624ca187e6eaa528d291a53d2be08f8a7b270a8c5977f
5a100cdc3cd6f827d1ed82fc00a5796c7d3ca84c5f60f56fbbfd53260a009386
4492379bb1524f175e2c4a520da9ac7dfdc620ed7199048adf76f573692228d8
7d4f7e9484176c6bf18e2c9c223259a098dd1608c90aa51b34f2f5b9a02b3740
8a15b07429c7c9d89e8abb6d8d270952a88b325ec58a10ce761f36ac4acfb2a3
d6601a6a0409223f722000674185650ebee561fdf11af539b93dfe269559b7f9
4f6c7e44a4e12ab7b2b7e211a3df2a1548dfcfc4033135c5021949908c5f5294
61f14f13d217e1f90d924ec5c5aff08fc7ddbb32c38d185c195ad00a7b649520
afae0cbf313683e13515f3da25c71e5df88fb3fb0514f843677b51ebb021b7f3
26c4c04d763f0d1eba408821412ec805560fcce7436347af4ef2d6709f05a63d
808f8532904fe2103078ba6f2c62447bae0aeabc68f107c84d3a0ad30cf568f4
baea4f7e32474f368b4600e269e8578a49dcefaa2b6d414f7315ffe0ee3d4298
493d581411427eb0f62e554a9d040a92482d9ab35946b31ee8b26c0ce0489cea
2b6d4869a41e5f0219b5144b7b3556764cd75d9296fe8b576b34d0d5b1832d15
b018945db9b23221469871386b7cfe8b738a26be06b488fbe6f3e37be3216279
41bdace4fecd354b3665220106534afe2d1e463214f8c59fd94ca188686d8af9

21eb671a2919b78dbe37d8f0d15164aa41ff4562ca4fec48c5583ce3782581cf
8329388f80c4c1c051e96f148195cb92c1ff5a065c551d2671e47a97f47b2660
c727ad0000c6f40c707c08dd5b66162875e761873910a83e04db7705d95f401d
27a8a0cf5f1078c5fc3ecf3b4c9c5baa302c32039fbdb2fd03aa38c3aa908df3
c6fe24596db03add9a9bede203e2e9596dbeaab8acdbfec03552297800354828
a127b88865376e77f498a9758de097bb8785aabf2918f27b4b88520e586794b3
ff22e63b561a42d4eb86780e9c87fdd3377d10aa0299b371ff4747d8f51fa50a
3f4e884bd33032b6e0daab91d50a96c3e8f88938971accf7948e1da76a45704d
2557b0e1d100dbf92e01dc07537a49353539f3e78df85753ed651142637c0872
5f96bf657af29be82cdafd71aeee4fdc68805ada749c085c4ab26c8f822337e7
e2e4dfbed9aeaea61eff41981f4924b725fce01765581f94f9948448e874215f
266466827857f3bb680a601e96780fcc7d4b3323addc39af39349c88f7ee1955
472ea4929c5e0fb4e29597311ed90a14c57bc67fbf26f81a3aac042aa3dccb55
6c009275d952cc6ec5d9d41fc9d7a47a31813483b768291c5c01e54a83787ca9
4c6f74a274ea7255a178650a656c1d84c6d717043301917ffbf31285059bbd87
889cfc8b07dd2b1adacd08d5c2e25bcb43e1fffea1d8af0f7886ce4e6385cd13
f2d649046d1a8811426a257d70e9bdc371d27931d2b76b391b0a630c84172c4b
e48d7b9e764032ca07c2335a16b19b6ba9243f993cc36af88a633c3ca428cedf
4eec3329ff385d89e1c31dc7e58ec48abf87947ab122e68fbdc95df96fd298b7
4ae6313a056ef5762e96c0a8f2527bc686a39a317e07484da9229dd265e7d345
2e539d0600466f5987994eef6ddaca883ee3ccb2d46ff756c37ea6c0bedefe6e
da2ffe73cefd2ebbe0efa415da6eab91dacdc87dd46110d6aa0871f75a45bd2a
793be04c163f7a9e026105dd78b88b378cb35188604cf99d8af1fc470d8db4c7
6322383a5cedc8e5de5f689c0fc4df7f96fc0e1ccf1d508e836a3e5842d05a73
fe59b0e9352931157563a19c33ef0f259dab19e1fec88bd94b7eab6e8c7b2b5f
f1a54dca2fdfe59ec3f537148460364fb5d046c9b4e7db5fc819a9732ae0e063
a652f35cb877145e83ab813733083bb25c7fc717522abf10377de1f7a8fc4b43
bb75c9ba7cc5163c39daa2ad35ce32001416654e76ed77896a793c4c0c34e619
38489de0d8cdc5b208ead2ba87eb221e010e8b78099c8704281d2a7755815349
febd5232fe500962f382de753e2659d42e0e934229b1259bc28c6e857094b299
35d9012da0b1264657ef54518b638ff664713478d419d3f72e655c49a2b9209f
449d3145218e6146310f82bef55401a2d882cf41a1771dfcb8bff50bb815dda3
1b00b0c4aa3b442c1e0358a0067fcbcb2081370330388ebb88a0225d2a6be4de
aa9c7c350b62986883d43ee63bb4c3592eb7cd35e9d392cbbd2502e092eea86b
97c6dc02eaa6b8ce8d46460d5d94f57ceb4f355626d1cd3ddaf6dccea81d75e2
65dec7020899647195bce984ec8dfb20503119fc2888f7c83b3d2493fd57aea9
b2c0878ae97dc48c413065626b05235c86d8dd7897bcdb741e68ca88c2a0ecc0
1c67a8264da6b531239a5f310568f35254c04ace57409a644ff7b2754bbe1b35
3a69780947319168210a7656851ee5af73d7a417231c5d29da2c2281da2b0ece
caaee9e7039d9a775f78f563a76c33d3d643cc604f33247d92b36fb583768843
341bb8dcbfe656bae3d11079be116dbc25cd4ef5554d0462d3eb62ed6d78c0d3
782cc8a4347d607a1fab534181a318181e11724f7cef7f68cc63a39ba8ab1509
cef50adae5e53a904246b688d8164535aff9062e3b446ac140cf42afd63ad0eb

d4f74d05e1932b218d2da600f68a4c969e770e249240eea5a3020c0f8adf15e2
f4d458a49c4b490f0033d48466716ded8221f261eae2f1c38ef78f550f42064d
70200426178917e2c4737a0e53b30b706a481a47bfaed460b48e4b17611421c4
c871410689004c712b6428a5f2b9bc7e49e6c84b740c7453e4eee835e13f1eba
d439e32be9f8dbeda8d23e73d64bb92fcb795fbe9668aa9bcd028daddeccca2b
8dd2c218c9ef809ffa27ce117007b2439c5df4d6f69f948381e5c75fe17aa1d1
3803e67be2e686647bfda324dde1b00ecad0c01f8c192626565f32a03726e6ed
6acd92d0dfe3e298d73b78a3dcc6d52ff4f85a70a9f2d0dcfe7ae4af2dd685cc
07062d9ecb16bd3a4ea00d434f469fe63d5c1c95d1b4903705de31353e9c92ce
8b6eb727d5091e587319ee88ec5e72555e6d63d7b0389a12dd76618edc5222c1
270c68177450f00cd7eabd444ec5c4b10e6b2f0799b73a3a25b4caed2da17ec7
172d54f2ed2c422ab063c57d00c8ed44fcb2f18aa068a289308a1207d79de42d
9949956a4ca9604f7c6b71a57157f61e2129c5397fec0f29b8fd6690f31a0ff7
9a5e110e3ab973a52e9bba5bf5cbe110f12fede20e3395588d1d4e57acbdfb31
2eade1bebc1927c3da61d590cbc6dc9ed9aae9ec0ab7836d6fcaf8eb653da6c0
95efb091998fee13cae08c1ae70a8edf4372362e8270d37614bc51b17cde9bbe
21f5514d6256a20dcf9af315ee742d6d2a5b07009b200b447c45b2e8f057361d
119ae4ad1797b6e1a46404264de95c1e5e0bb95920926ed9740676864ebb6411
5881d307ad1b7ac72daf7ab5dd3f72a278ae4bda0a61e25f86940540250c3dce
2d4a460a5f165e33c695791f2803dfaf348b0cc5cd9938119856986745db0bbd
939ac722791058d6cdf165624d7cc3a47e3c815a7bb62eb2493755ae1b3c514f
47edd2fc695f04623ec883416dbf166a495ded54cc4af7e41ceadd1cd4449608
5518c1bad3dc9b63c3b34a57d96a6dad11b0c30f6ad08ce7064e65d6eeec315d
2d981e468deac0ad5b47f7c55d05ea5812ddd4d539f9939cc6825ea261750533
061c155e87eaf790cc8bfa6c59ab7c1e5184df77dee4bd1c59506c9a91785b9a
60d522f415c0b2bfffb2a25650e6ac975ca8976750129ac769d257bf173dcec2
81dd46a4cc1138ff7a7f12747af501b51f0ad35c5a247cb44e2296cc8fa4c886
c057b3a6bb9082b6be0b57d1c07ae30bc97a97ea9740a1781a23ea7e20686a6b
b4e6724be4764ca14060262a9b3dee20f1a72be9f5ae7f15294ffa3cd037b78b
679eec0b8f3a9bb2d85ef1f9e0220b98bb7ffb9f9a7e1a3e7c2fb45af37b4f68
7e0e7deb55fb6024127273620466148fc70cea5bea43457cddd38fa650b0665c
ce0e152ef2cb8f1e74580d632a17451b8e007719433074a614d0468bad11a8dc
236a245ae5b6333336a38a0c347664386866e70c043d57c85b37d15b7ecd050a
c2f7e50e753322249a98e2e906b3cb6e328fcb09a4cca341304fd25a742c6e37
c481440ea7bf78e552c402afb0cdb8d1e7ecc73b4b9db14257479dec03669a12
eeaa075f3e53737471e8da2f7e932e67776f2387ddef73c4208aebded98eea2b
72b3636718456d99a3d12267baa7b94d2e58a996036c2d39505e3e02ad38d94f
cf0999f84bfcefbb789fca7bc22f2ee9cb870d9e794d177efd1acb6647e01862
885ca96b477e09edbb20e979a422597b56d72ce1435551a43d30aa9024d9e2ec
795ae4097aa3bd5932be4110f6bd992f46d605d4c9e3afced314454d35395a59
4c704849972882b81e398f14357c35546f513928aafb687f0e36f18438077055
141c92659d1b126d85383ee099cbc56e3bc9832c952446bd8969bf900d4ccf4c
110568a2c505b72ef3957f1d2ce42ab1fb9264180ef94704ce2b9f1f0d5beffd

1eb22abc743122ce749f3d5263bf9285d2dccbc2b520b62a1b280783e87c671b
e1c837fc2399ffc3b211b422f67b4af02041f79b4eadfa8e4f1b79d8c133d714
5359a7bb5e7b68e61ecce8c1ca6167c88a685a1085b6005cecd5ef9c7a838af5
1ce65c338471814b69ab2779a24a3e80d1e09ab37f3f064bf9d9065541f18df1
8204a9061f124dd83745c01bb328063712615dfc6e4179a9886ae3eba3f53633
bb7f7096787f9e4974baca7b8faece258464d426ce1ff749d9870f24671358b9
ab3ebbda6147230b70c9807047ab5bbb4481f7bb8c71955e579047d91226b5aa
c4e3f4d812a95fd7c49e98143a5dcb8b13542e3d8a72054b3d6f844c242d8084
9cb4b0f1330478d7748fc1f92e3150dfcb7cf958dce302e9224c235d4b6f19ed
e97deb1869b219dc1b93820b360c79d9d535685926ce4a46f567bc27c352ac72
4ae1677f511ddc57784c330b1c9c6091e136ada2123ebb1ddaae7666cd075872
c11e2306a7926e55f4b2fcbbe7307690059572f1857724bd4aaa7974be6a4b56
5b76985f26c17df4897fff102a7ca66c39e8b58dc06dd367ff6aacc0616a664b
a53a13a6f3aed8523710ff38a8d38f5aa9ebd9b44a25cc4967130f238f9990a3
d909945e0188839c5b52043c1ade5951a8481d53eb5bb9564366e73f6928c907
de83af838038998474a7f3cf1ba3a146af5a5b6d1b53ac59966978ae9703fa19
1e2b962a1a850808c9d071324e642d2891ea2c0b8cd48f471b1af16fa38ae399
301bd83352dde7113cc7769d918da2953a6dcfe7935a7e945ac251378873264f
d971842441c83c1bba05742d124620f5741bb5d5da9ffb31f06efa4bbdcf04ee
ff73e549a1d761c8e323e60d96aa31c0733aa4933243064c668c11eba3143f77
d2676976c12581ea3954804e7831a8a11019cddfb2a6e91dcac3d3299600aa15
e425b6bbf5d74f3f4b442a8b9b083629a89a616645eb3507e59292afabf181d2
5c2dd8fadf9f0bb60513f693b188a704583bb68da5572442d6c742ba0c8989c0
ffe9b86bbc2298ba003796bd18283fb4fba78962ae5aefd213a78b3494fd5708
b8bc0be5b8778f1813fc20c8984cc8d902d41df3f1a67f4e33a73ec577ad20cb
32425dc129d5b4cf6483e267907365ba5ad87c082d536e190f1d46f6a70b3ec8
cea94b50159f940df6ef1b7a1dd0fffd1ea45ce6aa86696f1441826029980984
2d1ae38f918293599bee7df30185084e767a447c0f89ac42ca79dbaa828ce1b1
ccb03e6b26ba9039f0a098231495072dd5fcca587d2f3aa7d51f84419b349c91
b2a3b46498abdec68e82b85f01fc8d96ada56bb9a9a9d294eab8441e17484a79
84312d3b0760540ead06151d0d9dec9ed674afca615ee4caa47155abf51b93a0
7747440bc9aa779ef0b7e925f029ebf1a4b0d8f40baf01b21606c891b61d10da
3fad24c3a572e93764ca528cc025b19928682e8ed05f4fec4adac5dadb9c7127
72895802000d4eb9b9c850b8360f8489e14e120cc3ecc25aae6a86c46469d79d
29844b8125bb408f2c95754303f8b201ba754950111151bb3405740ebb5dae30
e95c6ebc4737d2dc3fa3a29df456322fc19bd4e85373008b580cfc042037b9bf
780e56adc4a71c46892fe30b269a8d879a8fad0f885ac90dd1605d2510c5172a
7be2628f1cfba974979208cace745561e0403c639df8e87238938c8afae30788
b56be15f2d31a64e3fdff5461a2c72eb7f18743cd3711e2574b85e5d71fb64f3
627c2b722ea28fdd9558dd62e0938908bded7aa16a7649af87f88f1fef0fc44f
467c587ccff90bf8b4fff77aa88392640fcca75656cfb8bb9fb4c0e935edb525
03265294358b7edb7a8b689474e9791d30a4d6fc47f9caadbc0fc064abc447ae
4d369817cc80d25f0f483b9d66633cbb33de6fe8c3e248a3abc9548f30d97b0f

cb8fa89b2664155e4fb60bf33024bc6d4b1d658abbec250a2a13b3d2e337ad86
147a44b7d1011aa553cbc4fec0aa13c051c6a6f882318cebbe52acc65a1af011
6d3e9d218cec36df5822a600c059cc06c6f0fb059cd0a1d9ec9899227d9a9ace

List of CVE commonly exploited by PATCHWORK:

CVE-2012-1856

The TabStrip ActiveX control in the Common Controls in MSCOMCTL.OCX in Microsoft Office 2003 SP3, Office 2003 Web Components SP3, Office 2007 SP2 and SP3, Office 2010 SP1, SQL Server 2000 SP4, SQL Server 2005 SP4, SQL Server 2008 SP2, SP3, R2, R2 SP1, and R2 SP2, Commerce Server 2002 SP4, Commerce Server 2007 SP2, Commerce Server 2009 Gold and R2, Host Integration Server 2004 SP1, Visual FoxPro 8.0 SP1, Visual FoxPro 9.0 SP2, and Visual Basic 6.0 Runtime allows remote attackers to execute arbitrary code via a crafted (1) document or (2) web page that triggers system-state corruption, aka "MSCOMCTL.OCX RCE Vulnerability."

CVE-2014-4114

Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a "Sandworm" attack in June through October 2014, aka "Windows OLE Remote Code Execution Vulnerability."

CVE-2017-0199

Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."

CVE-2015-1641

Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, and Office Web Apps Server 2010 SP2 and 2013 SP1 allow remote attackers to execute arbitrary code via a crafted RTF document, aka "Microsoft Office Memory Corruption Vulnerability."

CVE-2017-8570

Microsoft Office allows a remote code execution vulnerability due to the way that it handles objects in memory, aka "Microsoft Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-0243.

CVE-2012-0158

The (1) ListView, (2) ListView2, (3) TreeView, and (4) TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Controls in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0 Runtime allow remote attackers to execute arbitrary code via a crafted (a) web site, (b) Office document, or (c) .rtf file that triggers "system state" corruption, as exploited in the wild in April 2012, aka "MSCOMCTL.OCX RCE Vulnerability."

CVE-2017-0261

Microsoft Office 2010 SP2, Office 2013 SP1, and Office 2016 allow a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-0262 and CVE-2017-0281.

CVE-2017-11882

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

CVE-2015-2545

Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2013 RT SP1 allows remote attackers to execute arbitrary code via a crafted EPS image, aka "Microsoft Office Malformed EPS File Vulnerability."

CVE-2015-2546

The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 allows local users to gain privileges via a crafted application, aka "Win32k Memory Corruption Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2511, CVE-2015-2517, and CVE-2015-2518.

CVE-2014-6352

Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object, as exploited in the wild in October 2014 with a crafted PowerPoint document.

Advanced Persistent Threat (APT): RedDelta

RedDelta threat actor known since 2020. They attacked entities related to the Catholic Church in various country. In addition, researchers discovered attacks against law enforcement and government entities in asia.

Releted Tools:

modified PlugX
Poison Ivy
Cobalt Strike

Indicators of Compromise (IOCs)

CnC:

systeminfor[.]comsoftwarelabs[.]com
cabsecnow[.]com
lameers[.]com
http://103[.]85[.]24[.]190/qum[.]dat
http://167[.]88[.]180[.]198/dis[.]dat
http://167[.]88[.]180[.]198/hk[.]dat
167[.]88[.]180[.]5
167[.]88[.]180[.]32
103[.]85[.]24[.]136
167[.]88[.]177[.]224
103[.]85[.]24[.]190
103[.]85[.]24[.]149
167[.]88[.]180[.]198
85[.]209[.]43[.]21
lib[.]jsquerys[.]net
lib[.]hostareas[.]com
154[.]213[.]21[.]70
154[.]213[.]21[.]27
154[.]213[.]21[.]73
sbicabsec[.]com
cab-sec[.]com
forexdualsystem[.]com
lionforcesystems[.]com
apple-net[.]com
wbemsystem[.]com

MD5:

e5a23e8a2c0f98850b1a43b595c08e63

SHA-256:

4cef5835072bb0290a05f9c5281d4a614733f480ba7f1904ae91325a10a15a04
f6e5a3a32fb3aaf3f2c56ee482998b09a6ced0a60c38088e7153f3ca247ab1cc
7d85ebd460df8710d0f60278014654009be39945a820755e1fbd59030c14f4c7
bc6c2fda18f8ee36930b469f6500e28096eb6795e5fd17c44273c67bc9fa6a6d
4c8405e1c6531bcb95e863d0165a589ea31f1e623c00bcfd02fbf4f434c2da79
01c1fd0e5b8b7bbed62bc8a6f7c9ceff1725d4ff6ee86fa813bf6e70b079812f
8a07c265a20279d4b60da2cc26f2bb041730c90c6d3eca64a8dd9f4a032d85d3
86590f80b4e1608d0367a7943468304f7eb665c9195c24996281b1a958bc1512
fb7e8a99cf8cb30f829db0794042232acfe7324722cbea89ba8b77ce2dcf1caa
282eef984c20cc334f926725cc36ab610b00d05b5990c7f55c324791ab156d92
b6cb4f1c94cb2165a654e6655e099fa53c9e42d78847faf44bdbe2aadd128129
2bc7ed201c7af3e57a20eec4099e242631734fa37b50fa4bce194751f497f7c8
9bac74c592a36ee249d6e0b086bfab395a37537ec87c2095f999c00b946ae81d
7824eb5f173c43574593bd3afab41a60e0e2ffae80201a9b884721b451e6d935
76d0a85c8a8e21f59d858efafe9badf7315793ce4d4725574c06a653ba0bdb86
59aaa2b8116ba01c1b37937db37213ff1f4a8552a7211ab21f73ffac2c0c13ce
da95da58ea9669401ab40e398baaced000d1ef0f96328edbaee6aae664dca235
79ca5e8079c8fa2196c74e70d9cebc07e07cca54f8b19596b780b15aaa69b6eb
38629fb94f89d2504e1582679f82960bf343143c624a148b923d9cf4aa4db0b7
c21e3c27397549c712cdadd2ffab52f1f52ae6855931eee95c2d6533e8a4adb2
d30916f20a9352d5a4ddee5a961428baa34a0a17d4a7ad40c96f4857567f5f34

Advanced Persistent Threat (APT): SYSTEMBC TA

SYSTEMBC TA related to four campaign. It registered 2 domains for each campaign - one in .com zone and another - in .xyz. The Threat Actor used 'Hosting Concepts B.V. d/b/a' (openprovider[.]com, registrar[.]eu) for registration and all domain were delegated to Cloudflare's NS.

Indicators of Compromise (IOCs)

CnC:

dump17alertos[.]com
dump17alertos[.]xyz
dec15coma[.]com
dec15coma[.]xyz
alanpo09[.]xyz
alanpo09[.]com
209[.]151[.]144[.]238
95[.]142[.]45[.]61
109[.]234[.]39[.]211

Advanced Persistent Threat (APT): Basilisk

Indicators of Compromise (IOCs)

CnC:

www[.]3hourprofits[.]com
liftboost[.]co
snipemy[.]info
ali[.]kz[.]mail[.]ru
www[.]page
lamerhaberdotcom[.]files[.]wordpress[.]com
youhack[.]vip
198[.]200[.]94[.]190
190[.]204[.]88[.]61
60[.]51[.]212[.]61
74[.]110[.]58[.]102
129[.]128[.]146[.]149
69[.]244[.]100[.]198
75[.]190[.]200[.]181

Advanced Persistent Threat (APT): Lazarus

The cybercrime group Lazarus (also known as Dark Seoul Gang/HIDDEN COBRA/Guardians of Peace), is behind the so many major attacks.

Originally a criminal group, the group has now been designated as an advanced persistent threat due to intended nature, threat, and wide array of methods used when conducting an operation.

Related Tools

- AdFind
- SMBmap
- Plink
- Responder
- wget
- tcpdump
- XenArmor
- WinRAR
- ProcDump
- Mimikatz
- AppleJeus
- AuditCred
- BADCALL
- Bankshot
- BLINDINGCAN
- Cryptoistic
- Dacls
- Dtrack
- ECCENTRICBANDWAGON
- FALLCHILL
- HARDRAIN
- HOPLIGHT
- HotCroissant
- KEYMARBLE
- RATANKBA
- netsh
- Proxysvc
- RawDisk
- TAINTEDSCRIBE

TYPEFRAME
Volgmer
WannaCry

Malware List of Lazarus APT:

a. Manuscrypt

Manuscrypt is a RAT-type Trojan that can receive commands sent by the actors responsible from the C&C server to the victim's computer via double proxies. Usually, a Trojan hits the victim's computer using other Lazarus malware or after the user visits a compromised website.

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Other Name: FALLCHILL

General information

The Trojan collects basic system information and sends it to C&C:

- Operating system version
- Processor information
- System name
- Local IP address information
- Unique generated ID
- MAC address

Manuscrypt has the following built-in features for remote operations, providing different capabilities on the victim's system:

- retrieve information about all installed drives, including drive type and free disk space;
- create, run and terminate a new process and its main thread;
- search, read, write, move and execute files;
- get and change the timestamps of files or directories;
- change the current directory for the process or file; and
- remove the Trojan and artefacts associated with malware from the infected system

Indicators of Compromise (IOCs)

CnC:

62[.]243[.]45[.]227
59[.]90[.]93[.]138
5[.]79[.]99[.]169
82[.]223[.]73[.]81
91[.]116[.]139[.]195

71[.]125[.]1[.]132
71[.]125[.]1[.]133
96[.]65[.]90[.]58
98[.]159[.]16[.]132
41[.]92[.]208[.]194
122[.]114[.]89[.]131
221[.]235[.]53[.]229
66[.]242[.]128[.]12
66[.]242[.]128[.]173
66[.]242[.]128[.]186
181[.]119[.]19[.]118
181[.]119[.]19[.]54
98[.]101[.]211[.]162
59[.]90[.]93[.]97
175[.]100[.]189[.]174
http://www[.]028xmz[.]com/include/common[.]php
www[.]028xmz[.]com
45[.]34[.]66[.]30
http://168wangpi[.]com/include/charset[.]php
168wangpi[.]com
http://10vs[.]net/include/left[.]php
10vs[.]net
http://www[.]qdbazaar[.]com/include/footer[.]php
www[.]qdbazaar[.]com
104[.]31[.]74[.]89
https://www[.]anlway[.]com/include/arc[.]search[.]class[.]php
www[.]anlway[.]com
107[.]165[.]165[.]35
http://www[.]paulkaren[.]com/synthpop/main[.]asp
www[.]paulkaren[.]com
108[.]61[.]91[.]60
222[.]239[.]223[.]156
117[.]232[.]100[.]154
27[.]123[.]221[.]66
191[.]233[.]33[.]177
200[.]57[.]90[.]108
82[.]223[.]213[.]115
173[.]0[.]129[.]65
199[.]167[.]100[.]46
111[.]207[.]78[.]204
184[.]107[.]209[.]2
98[.]101[.]211[.]251
98[.]113[.]84[.]130
66[.]242[.]128[.]164
66[.]242[.]128[.]179
75[.]103[.]110[.]134
208[.]78[.]33[.]82

122[.]114[.]94[.]26
62[.]215[.]99[.]90
210[.]202[.]40[.]35
181[.]119[.]19[.]5
181[.]119[.]19[.]50
http://www[.]530hr[.]com/data/common[.]php
www[.]530hr[.]com
23[.]107[.]38[.]5
http://0756rz[.]com/include/left[.]php
0756rz[.]com
https://www[.]naviilibs[.]com/video/battle32[.]avi
www[.]naviilibs[.]com 198[.]54[.]116[.]51
https://www[.]naviilibs[.]com/video/battle64[.]avi
221[.]208[.]194[.]72
196[.]25[.]89[.]30
208[.]180[.]64[.]10
41[.]92[.]208[.]196
41[.]92[.]208[.]197
190[.]82[.]86[.]164
http://www[.]marmarademo[.]com/include/extend[.]php
www[.]marmarademo[.]com
http://www[.]97nb[.]net/include/arc[.]sglistview[.]php
www[.]97nb[.]net
103[.]238[.]227[.]72
66[.]242[.]128[.]185
98[.]101[.]211[.]140
64[.]29[.]144[.]201
66[.]175[.]41[.]191
66[.]242[.]128[.]13
66[.]242[.]128[.]158
181[.]119[.]19[.]56
81[.]0[.]213[.]173
222[.]122[.]31[.]115
http://www[.]pakteb[.]com/include/left[.]php
www[.]pakteb[.]com
104[.]221[.]134[.]28
https://www[.]apshenyihl[.]com/include/arc[.]speclist[.]class[.]php
www[.]apshenyihl[.]com
http://ansetech[.]co[.]kr/smarteditor/common[.]asp
ansetech[.]co[.]kr 106[.]10[.]79[.]34
http://mileage[.]krb[.]co[.]kr/common/db_conf[.]asp
mileage[.]krb[.]co[.]kr
211[.]48[.]76[.]36
http://www[.]51up[.]com/ace/main[.]asp
www[.]51up[.]com
112[.]126[.]67[.]80
190[.]82[.]74[.]66

77[.]78[.]100[.]101
125[.]160[.]213[.]239
36[.]71[.]90[.]4
181[.]119[.]19[.]141
181[.]119[.]19[.]196
182[.]56[.]5[.]227
210[.]61[.]8[.]12
195[.]74[.]38[.]115
173[.]0[.]129[.]83
208[.]78[.]33[.]70
216[.]163[.]20[.]178
50[.]62[.]168[.]157
66[.]242[.]128[.]170
66[.]242[.]128[.]223
197[.]211[.]212[.]14
104[.]192[.]193[.]149
http://51xz8[.]com/include/top[.]php
51xz8[.]com
23[.]244[.]213[.]174
http://1996hengyou[.]com/include/dialog/left[.]php
1996hengyou[.]com
160[.]124[.]191[.]80
http://www[.]nuokejs[.]com/contactus/about[.]php
www[.]nuokejs[.]com
104[.]195[.]1[.]39
smtp01[.]ansetech[.]co[.]kr
210[.]101[.]60[.]1
https://www[.]ap8898[.]com/include/arc[.]search[.]class[.]php
www[.]ap8898[.]com
104[.]222[.]238[.]212
http://www[.]shieldonline[.]co[.]za/sitemap[.]asp
www[.]shieldonline[.]co[.]za
196[.]38[.]160[.]213
http://www[.]33cow[.]com/include/control[.]php
www[.]33cow[.]com
falcancoin[.]io
203[.]160[.]191[.]116
191[.]234[.]40[.]112
66[.]232[.]121[.]65
209[.]183[.]21[.]222
119[.]10[.]74[.]66
139[.]217[.]27[.]203
181[.]119[.]19[.]58
181[.]119[.]19[.]74
190[.]105[.]225[.]232
125[.]212[.]132[.]222
http://168va[.]com/include/data/left[.]php

168va[.]com
71[.]125[.]1[.]130
71[.]125[.]1[.]138
72[.]167[.]53[.]183
98[.]101[.]211[.]170
66[.]242[.]128[.]11
80[.]91[.]118[.]45
66[.]242[.]128[.]134
66[.]242[.]128[.]140
66[.]242[.]128[.]162
66[.]242[.]128[.]163
66[.]242[.]128[.]181
66[.]99[.]86[.]8
112[.]217[.]108[.]138
211[.]192[.]239[.]232
https://www[.]elite4print[.]com/admin/order/batchPdfs[.]asp
https://tpddata[.]com/flash/gcoin2[.]swf
tpddata[.]com
104[.]243[.]41[.]186
https://tpddata[.]com/flash/gcoin4[.]swf
www[.]nuokejs[.]com
https://sfacor[.]com/upload/profile_2[.]dmg
sfacor[.]com
78[.]128[.]92[.]133
https://sfacor[.]com/upload/profile_4[.]dmg
https://wifispeedcheck[.]net/upload/conf3[.]dat
wifispeedcheck[.]net
192[.]99[.]34[.]204
https://wifispeedcheck[.]net/upload/conf6[.]dat
https://tpddata[.]com/skins/skin-8[.]thm
https://tpddata[.]com/skins/skin-6[.]thm
https://www[.]ap8898[.]com/include/arc[.]search[.]class[.]php
http://www[.]shieldonline[.]co[.]za/sitemap[.]asp
http://www[.]33cow[.]com/include/control[.]php
www[.]ap8898[.]com
www[.]shieldonline[.]co[.]za
ansetech[.]co[.]kr
106[.]10[.]79[.]34
https://itaddnet[.]com/res/prof3[.]db
https://www[.]daslibs[.]com/res/prof3[.]db
itaddnet[.]com
www[.]daslibs[.]com
https://itaddnet[.]com/res/prof6[.]db
https://www[.]daslibs[.]com/res/prof6[.]db
http://www[.]yich[.]co[.]kr/jbcgi/edit/tmp/notice_20112030837572332[.]png
www[.]yich[.]co[.]kr
222[.]231[.]2[.]43

http://www[.]jscw[.]co[.]kr/jbcgi/edit/tmp/notice_201002191504537620[.]gif
www[.]jscw[.]co[.]kr
222[.]231[.]2[.]179
http://hypnosmd[.]com/include/top[.]php
hypnosmd[.]com
64[.]90[.]49[.]224
http://168va[.]com/include/data/left[.]php
www[.]naviilibs[.]com
198[.]54[.]116[.]51

MD5:

9578c2be6437dcc8517e78a5de1fa975
bf474b8acd55380b1169bb949d60e9e4
d17b96b56d5eed6e918d89f0ba120d7e
47e7b297f020d53f7de7dc0f450e262d
1ca31319721740ecb79f4b9ee74cd9b0
633BD738AE63B6CE9C2A48CBDDD15406
34c2ac6daa44116713f882694b6b41e8
24906e88a757cb535eb17e6c190f371f
3005f1308e4519477ac25d7bbf054899
68fa29a40f64c9594cc3dbe8649f9ebc
d2de01858417fa3b580b3a95857847d5
86685ec8c3c717aa2a9702e2c9dec379
361c2c5be75439dda958daa6032cab49
3d0355ff78dcc979b3f83a679b6ba794
233ad743dd26c959fa735ffbaa456c05
cea52553aed83e408702ad7c03f287c7
e1ed584a672cab33af29114576ad6cce
d8484469587756ce0d10a09027044808
86d3c1b354ce696e454c42d8dc6df1b7
5182e7a2037717f2f9bbf6ba298c48fb
278833c6f56ce1f82c368e623bf8ae96
1f04ca0504ba5e5d721eed5575bc19ef
425dfb5944dab3b3adbffe5128f4cf29

SHA-256:

4d3c9ea93c299c397ec4af094a57acc597e6a9eaa1005eabe59c1f6617abd3b9
58a97c2c731cdf045f26ccc7cba370bd2dfee277a9c43c0421c53593e493f7bc
dced1acbbe11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156
546dbd370a40c8e46f9b599a414f25000eec5ae6b3e046a035fe6e6cd5d874e1
c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777
8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8
089e49de61701004a5eff6de65476ed9c7632b6020c2c0f38bb5761bca897359
5e54bccbd4d93447e79cda0558b0b308a186c2be571c739e5460a3cb6ef665c0
f8b329fc1f4d50f5509a72c1f630155538f4d2c6e49b80ce4841fada6547c4bd
3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395
380b76590d3e878d73bc7964fe225a2721218dcda7ed9c571b433af07a8b1107

6ebcc34020c85459dc62b745c7783d4a7e41f2c5d4f051e8817934ed7c5d0d9b
4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324
3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92
f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff
bbf09724de5e0e039846d191e44460aa4071fefad22a4e8161a2628a99bad024
d060123c21869b765b22b712a8ca47266a33464095411e2b7bdf7e327d23ed07
d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3
a606716355035d4a1ea0b15f3bee30aad41a2c32df28c2d468eafd18361d60d6
2a000d4d6f1dec6dfd230bb793b7fdd91db1194f0a1ea2e184ca18214e350a74
c10363059c57c52501c01f85e3bb43533ccc639f0ea57f43bae5736a8e7a9bc8
feb884409fb5dd2a45e5461481706cf04b877b648b39879ee5e55a1e61b87856
ec84802bb2bb33c52c1f02e7a7b74c6ea6247611c410bf386a95dc1eb45e2347
ec0aa9678fb5eb631b9ec94de63d8eb923728faf5b0672ba6eed43971a2ad1d0
e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2
1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7
1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc
7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882
9d9dda39af17a37d92b429b68f4a8fc0a76e93ff1bd03f06258c51b73eb40efa
5d134f42ce7616882df6a9156bca882097b549d1c9269a5849608114f381b9b7
bdff852398f174e9eef1db1c2d3fefdda25fe0ea90a40a2e06e51b5c0ebd69eb
0a118eb23399000d148186b9079fa59caf4c3faa7e7a8f91533e467ac9b6ff41
e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292
d30cb50641ff79fa059fbf1950047d2e34eb3e9ee7b5ff5cced0912160d3edb9
201c7cd10a2bd50dde0948d14c3c7a0732955c908a3392aee3d08b94470c9d33
20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64
4bd7d801d7ce3fe9c2928dbc834b296e934473f5bbcc9a1fd18af5ebd43192cd
40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116
a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6
e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef
675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1
e69d6c2d3e9c4beebee7f3a4a3892e5fdc601beda7c3ec735f0dfba2b29418a7
eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c
c68bfd97f5eff77d2cb44840a7ee3e19fecc304a5a3206068bd69a288bc9802e

b. CuriousLoadert

Loader used by hackers from Lazarus. Discovered as part of the attack in October 2019, however, the first sample dates back to December 2018.

Platform: N/A

Threat level: Middle

Category: Loader

General information

Indicators of Compromise (IOCs)

MD5:

84b8af33a6181ac13fa5529d08500fc7
11fdc0be9d85b4ff1faf5ca33cc272ed
5e60ff179d6e4af28f91f70f45b72038
2b02465b65024336a9e15d7f34c1f5d9
f6d6f3580160cd29b285edf7d0c647ce
14d79cd918b4f610c1a6d43cadeeff7b
c0a8483b836efdbae190cc069129d5c3

c. SvcRAT

Platform: N/A

Threat level: High

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

23[.]95[.]229[.]119
107[.]175[.]59[.]21
192[.]3[.]31[.]12
66[.]154[.]103[.]104
107[.]174[.]25[.]127
172[.]245[.]156[.]203
https://151[.]106[.]27[.]234:443
151[.]106[.]27[.]234
162[.]255[.]119[.]153
162[.]255[.]119[.]34

MD5:

08b6891f3320c653d69dfd5d0694c69a
947fa11d132caea04e6c13e6150d48e0
932a845b27d5fb9ec78638a839ba5fb1
7f6263ccd71f05e5d3a7ca694ae513ad
8bd120acee67839d73ff6b1fea81b37a
7a372a2f85e9d2b6a3aebb63d8884080
c744a0435bce2fdcc6b05737321f8559
293b4729b8a619a2a2d2a2529e494925
6bd3ff14323c72bccbee75908cbaa899
04c640a5ff10f139738981372cbeb676
51b4527a31e5f4d89d0fed1c18b3199d
79e6d1e84be8742131b95cb94b94b4f5

d. RATv3.ps

RATv3.ps - is a PowerShell remote access tool (RAT) or backdoor having the functionality to run commands, manipulate files, upload/download files from a C2 server, manipulate running processes, collect system information and manipulate the Windows registry.

Platform: N/A

Threat level: N/A

Category: Backdoor, remote-access-trojan

Other Name: PowerBrace

General information

- It communicates over TLS with a custom protocol using XOR encoding. Minor obfuscation occurs throughout the script, which makes it slightly more difficult to analyse. The script uses several light forms of obfuscation. Function names and variable names are replaced with non-descriptive names, and strings are stored as base64 encoded Unicode.
- This malware collects various operating system information and sends it to the C2 server. The collected data includes:

  - Internal IP address
  - Computer name
  - Username
  - OS version
  - OS architecture
  - Proxy status
  - Proxy server
  - Script path
  - Last boot time
  - OS caption
  - OS language
  - OS country code
  - Primary C2 address and port
  - Secondary C2 address and port
  - 32/64 bit system

Indicators of Compromise (IOCs)

SHA256:

6ed6ac7b499f7fa613949c412b4245dd21c684192afd3de5614575c37cf35e1f
51f4660f6a3ecda7324fe163b23ce3c66b9bcff638fbb008d231c312bb1e5dec
fd7c2afabbfc3b20ec73d5719eba04195c59b4a70b2de266995438032e1e80ef

cb47b8e49881c8aed31e5b0c354e7eb14532c3ff6da69705142370bdaa289ebb
113b65ed938f8f3199bf28f0fe932dc80560d70f0fc1c5918c99783df00a978f
56102f70df2e481a91d3be1e33facd7e220e2b685405ddf873f3ab079e99873e
8a0e6c50a6483f2f01a458cd0cb4e485605778c42c9708b07b820968132efb76
29f1322ce49386c7cc916e0e63d706cbcaa0132ea56c55ec57c0c14c3dac8993
98d46a54383eedccd3d80cf0bf6712ab4a7acdbd69f7893fb98b4ee4a020d55d
52eb8f654d33f1d5c34b5bae0d83360158d8eccc32ddcbb555d7b1b7c943842c

e. Linux.Dacls

Linux.Dacls is a malicious remote-control software for OC Linux used by the Lazarus group.

Platform: Linux

Threat level: High

Category: remote-access-trojan

General information

- Its functions are modular, the C2 protocol uses two-layer TLS and RC4 encryption, the configuration file uses AES encryption and supports the dynamic update of C2 instructions. Linux.Dacls is compiled directly in the Bot program. It was found that Linux has 6 plugins: execution commands, file management, process management, test network access, C2 connection agent, network scan.
- The main functions of Linux.Dacls Bot include: execute commands, file management, process management, test network access, C2 connection agent, network scanning module

Indicators of Compromise (IOCs)

CnC:

162[.]241[.]217[.]135
www[.]areac-agr[.]com
http://www[.]areac-agr[.]com/cms/wp-content/uploads/2015/12/ldata[.]dat

MD5:

80c0efb9e129f7f9b05a783df6959812
859e7e9a11b37d355955f85b9a305fec

f. MAC.Dacls

MAC.Dacls is a malicious remote-control software for macOS used by the Lazarus group.

Platform: macOS

Threat level: Middle

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

67[.]43[.]239[.]146
185[.]62[.]58[.]207

MD5:

81f8f0526740b55fe484c42126cd8396
f05437d510287448325bac98a1378de1
b19984c67baee3b9274fe7d9a9073fa2
024e28cb5e42eb0fe813ac9892eb7cbe

g. Win32.Dacls

Win32.Dacls is malicious remote-control software for Windows which was used by Lazarus.

Platform: Windows

Threat level: High

Category: remote-access-trojan

General information

Its functions are modular, the C2 Protocol uses two-layer TLS and RC4 encryption, the configuration file uses AES encryption and supports dynamic updating of C2 instructions. Plug-in module Win32.Dacls is dynamically loaded via a remote URL.

Indicators of Compromise (IOCs)

CnC:

162[.]241[.]217[.]135
www[.]areac-agr[.]com
http://www[.]areac-agr[.]com/cms/wp-content/uploads/2015/12/rdata[.]dat
68[.]168[.]123[.]86
172[.]93[.]184[.]62
104[.]232[.]71[.]7
23[.]227[.]199[.]69

MD5:

22a968beda8a033eb31ae175b7e0a937

SHA256:

3095f9326c66c9a035cb12bf50e2115c3aa6f7860dab9a8b8f82a223f366283a
45ab66dbcb78158b2c2448207717646655d804bdc4f975c47fafbe21a0213fbc
82d33a67c68f7c476a9ac1e960abc6a911f797446a2c24f0e13b92af1eb385b8
d2f1cccfe688c074c3d58ae8f7be7b10dbea5d7ae53320c3f7b6e48cd4f62955

cdf74f48c9ea905682155441cf03f4207dbeb2a2f09c4605a5cf4a9a367286e8
cdac934dbd8831b962718fdbaf050ebaa8b89be6c98c8cd7479a9d91939c63c6
40249bc29030349a85d18677483acb97aca028df8a55fda93728f253f72f2e0a

Network Signatures

TROJAN Possible DACLS RAT CnC (Log Server Reporting)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Possible DACLS RAT CnC (Log Server Reporting)"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"log=save&session_id="; http_client_body; depth:20; fast_pattern; content:"&value="; distance:0; http_client_body; pcre:"/^log=save&session_id=[^&]+&value=[^&]+$/P"; reference:url,blog.netlab.360.com/dacls-the-dual-platform-rat-en/; classtype:trojan-activity; sid:2029879; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2020_04_10, deployment Perimeter, former_category MALWARE, signature_severity Major, updated_at 2020_04_10, severity 3, ti_malware_id c75434dd3df9e41547cf58adb15fe91008f60740, ti_malware_name Win32.Dacls, malware_family Win32.Dacls, rule_origin etpro;)

h. VHD Ransomware

This crypto ransomware encrypts user data with AES-256 ECB + RSA-2048 and then demands a BTC ransom to get the files back.

Platform: N/A

Threat level: Low

Category: Ransomware

Other Names: N/A

General information

- The activity of this crypto-ransomware occurred in the second half of March 2020. Date stamp: March 19, 2020. It is aimed at English-speaking users, which does not prevent its distribution around the world.
- The ransom note is called: **HowToDecrypt.txt**
- Email addresses used:
  - johndoe2020@meet-me.live
  - johndoe2020@airmailhub.com
  - miclejaps@msgden[.]net
  - stevenjoker@msgden.net
- An extension is added to encrypted files: .vhd

- Experts note 2 features of this program:
  - The ransomware uses Mersenne Twister as a source of randomness, but unfortunately for the victims the RNG is reseeded every time new data is consumed.
  - VHD implements a mechanism to resume operations if the encryption process is interrupted. For files larger than 16MB, the ransomware stores the current cryptographic materials on the hard drive, in clear text. This information is not deleted securely afterwards, which implies there may be a chance to recover some of the files.

Indicators of Compromise (IOCs)

MD5:

EFD4A87E7C5DCBB64B7313A13B4B1012
DD00A8610BB84B54E99AE8099DB1FC20
CCC6026ACF7EADADA9ADACCAB70CA4D6
6D12547772B57A6DA2B25D2188451983
D0806C9D8BCEA0BD47D80FA004744D7D

i. PowerRatankba

PowerRatankba is a powerShell-based malware variant of «Ratankba», which used as a first stage reconnaissance tool and for the deployment of further stage implants on targets that are deemed interesting by the actor.

Platform: Windows

Threat level: High

Category: atm-malware

Other Names: Recon.PS

Indicators of Compromise (IOCs)

CnC:

http://51[.]255[.]219[.]82/files/download/falconcoin[.]zip
http://51[.]255[.]219[.]82/files/download/falconcoin[.]pdf
http://51[.]255[.]219[.]82/theme[.]gif
https://dreamlabs[.]net/index[.]php?act=getps1
https://bodyshoppechiropractic[.]com/tbl_add[.]php
http://dreamlabs[.]net/logos[.]gif
http://dreamlabs[.]net/dreamlabs[.]net
bepis[.]space
juchniewicz[.]club
lawrencemedia[.]website
cabdinc[.]top

crossfr[.]site
canellas[.]cloud
gochuonpire[.]us
calvinm[.]io
ofiteksol[.]pw
terry[.]network
cwt[.]host
cmii[.]space
jetnetflow[.]online
millerrdserver[.]host
cmplex[.]host
mikeshomeserver[.]win
finishline[.]cc
sdroy[.]pw
derzh[.]club
thupa[.]info
trade[.]publicvm[.]com
bodyshoppechiropractic[.]com
eselevseuhdeste[.]site
utiwteehamecagsoin[.]site
ppepos-test[.]xyz
itidsegcaerunetrexe[.]site
alertas[.]club
kalicki[.]club
pavlovs[.]site
retaildealmanagerqa[.]cafe
soundboard[.]site
carlet[.]fun
liangz[.]xyz
arsenique[.]link
ecombox[.]store
spektra[.]app
yoann[.]host
brookju[.]us
dnas[.]cloud
wiemer[.]network
jhonizzle[.]us
sandwichan[.]fun
coachbot[.]win
middletownchiropractic[.]rocks
sharedrive[.]space
skemper[.]us
kalicki[.]fun

autoif[.]online
www[.]businesshop[.]net
reig[.]world
avia-tickets[.]services
betonghosp[.]us
ccheng[.]pw
shudaizi[.]app
jcnetworks[.]tech
werpo[.]win
azeroth[.]network
vilenpro[.]men
zcs[.]space
vtadrones[.]network
thesaleemfam[.]photos
sucio[.]supply
wkw2[.]us
scrfamous[.]club
sam1b[.]us
usersec[.]online
woolf[.]network
workspace1[.]app
geoenterprise[.]site
encorereg[.]us
caprica[.]link
youreinvitedtomy[.]club
gateserve[.]xyz
monkkx[.]info
firelightarchival[.]info
socowsareorteocsin[.]site
chateaude[.]chat
minglen[.]club
cgitool[.]online
morella[.]online
zkre[.]xyz
mdkder3[.]pro
ktn[.]services
kbh118[.]xyz
jtek[.]solutions
fwsod[.]info
polyant[.]mobi
oca1[.]pw
roguemedia[.]site
srv65[.]xyz

ecombox[.]online
thegordon[.]club
gdlaw[.]space
donovanclan[.]website
rilla[.]xyz
apps[.]got-game[.]org
vietcasino[.]linkpc[.]net
alexandroskokkinos[.]site
usasport[.]news
jayoung[.]xyz
dividebyzero[.]us
mcpcore[.]host
hopechannel[.]io
bukatiket[.]fun
vpnforthe[.]win
flashwitz[.]xyz
legalize[.]fun
freshlife[.]cloud
luckydog[.]network
dubovsky[.]site
dedoviq[.]website
dochelp[.]space
ronandlaura[.]rocks
vanhassel[.]zone
201[.]139[.]226[.]67
23[.]227[.]196[.]117
166[.]62[.]112[.]193
144[.]217[.]51[.]246
158[.]69[.]57[.]135
198[.]100[.]157[.]239
127[.]0[.]0[.]1
51[.]255[.]219[.]82
92[.]222[.]106[.]229
180[.]235[.]133[.]121
https://ecombox[.]store/tbl_add[.]php
104[.]227[.]146[.]249
https://ecombox[.]store/tbl_add[.]php?action=bgetpsc
https://ecombox[.]store/tbl_add[.]php?action=cgetpsa

MD5:

c9ed87e9f99c631cda368f6f329ee27e
911de8d67af652a87415f8c0a30688b2
1f7897b041a812f96f1925138ea38c46

1507e7a741367745425e0530e23768e6
79d09d46fd66085587afca579557bc89
17f0f148f53968effcb42230518aeb67
563db5fc71da5f3bfc216aa3ec52f074
ec264b9c938355f1a7d1dc97c73fa9a6
cb52c013f7af0219d45953bae663c9a2
34404a3fb9804977c6ab86cb991fb130
18a451d70f96a1335623b385f0993bcc
5d06ff8f43f631cd2a71a565dd10b7a5
eb30a58da33f1caca3a01e1467d6661c
3c2f5ff382b0ec132101e92f72256490
2025d91c1cdd33db576b2c90ef4067c7
9cee042ba1e447baf13eaeb9305f7280
5ad8143d954ebd5de6be0a40e0f65732
f34b72471a205c4eee5221ab9a349c55
df934e2d23507a7f413580eae11bb7dc
50ca734bfba54ed33af469537b5e22c1
cb29db3900204071323a940c2a9434b8
cba175498af45dca6970aeee83a6d9f4
ed2cace34381b6bbeb98af31e73e7904
6c360e9a6f933bf172591a81881ca79b
9216b29114fb6713ef228370cbfe4045
a8b14ca96830d3b1d4d2f70b92d2d186
636f8bd214d092ae3feb547599b4935e
8b51170fc6ecbea6b8496c8a8a8e4f1a

SHA-256:

20d94f7d8ee2c4367443a930370d5685789762b1d11794810dc0ac6c626ad78e
3cd0689b2bae5109caedeb2cf9dd4b3a975ab277fadbbb26065e489565470a5c
b265a5d984c4654ac0b25ddcf8048d0aabc28e36d3e2439d1c08468842857f46
99ad06cca4910c62e8d6b68801c6122137cf8458083bb58cbc767eebc220180d
20f7e342a5f3224cab8f0439e2ba02bb051cd3e1afcd603142a60ac8af9699ba
41f155f039448edb42c3a566e7b8e150829b97d83109c0c394d199cdcfd20f9b
db8163d054a35522d0dec35743cfd2c9872e0eb446467b573a79f84d61761471
1768f2e9cea5f8c97007c6f822531c1c9043c151187c54ebfb289980ff63d666
f7f2dd674532056c0d67ef1fb7c8ae8dd0484768604b551ee9b6c4405008fe6b
d844777dcafcde8622b9472b6cd442c50c3747579868a53a505ef2f5a4f0e26a

j. PowerTask

Backdoor of Lazarus group which was uploaded to VirusTotal on 29/03/2019.

Platform: Windows

Threat level: High

Category: Backdoor

Other Names: N/A

General information

- Researched file "stage.ps1" was uploaded to VirusTotal on 29.03.2019 from Nigeria. This file is a PowerShell script. It has following functions:
  - Checks presence of connection with specified network node
  - Updates configuration parameters
  - Executes commands in Windows CLI
  - Creates new processes
  - Launches PowerShell commands
  - Deletes itself
- File doesn't contain C&C address. Executed commands are read by the script from the file. The name of the file is transmitted during the launch of the script. Based on these facts we may assume that other tool is used for communication with C&C. On the moment we didn't detect it.

Indicators of Compromise (IOCs)

MD5:

ee664c219e8cf9a3ef6f9b7eb56f3c18
ae4e5917e3b4cf2e7c2457f411b66343
e186e60ab803d23d1cdf39c313cb34a4
c9b3b6bdc0cbb09f1ca5d4caab8bea9f

k. HOPLIGHT

On infected systems, the malware collects information about the target's device and sends the data to a remote server. It can also receive commands from its command and control (C&C) server and execute various operations on infected hosts.

Platform: N/A

Threat level: Middle

Category: Backdoor

Other Names: N/A

General information

- HOPLIGHT can:
  - Read, write, and move files
  - Enumerate system drives
  - Create and terminate processes
  - Inject code into running processes

- Create, start, and stop services
- Modify registry settings
- Connect to a remote host
- Upload and download files

- The malware also uses a built-in proxy application to mask its communications with the remote command-and-control (C&C) server.
- The proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connections with remote malicious actors.

Indicators of Compromise (IOCs)

CnC:

117[.]239[.]241[.]2
217[.]117[.]4[.]110
195[.]158[.]234[.]60
210[.]137[.]6[.]37
119[.]18[.]230[.]253
221[.]138[.]17[.]152

SHA256:

b05aae59b3c1d024b19c88448811debef1eada2f51761a5c41e70da3db7615a9
084b21bc32ee19af98f85aee8204a148032ce7eabef668481b919195dd62b319
c66ef8652e15b579b409170658c95d35cfd6231c7ce030b172692f911e7dcff8
05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461
ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09
2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818
b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101

I. BISTROMATH

It is a full-featured Remote Access Trojan (RAT).

Platform: N/A

Threat level: Middle

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

159[.]100[.]250[.]231

SHA256:

43193c4efa8689ff6de3fb18e30607bb941b43abb21e8cee0cfd664c6f4ad97c
133820ebac6e005737d5bb97a5db549490a9f210f4e95098bc9b0a7748f52d1f

m. SLICKSHOES

It is a dropper that decodes and drops the embedded file.

Platform: N/A

Threat level: Middle

Category: Dropper

Indicators of Compromise (IOCs)

CnC:

188[.]165[.]37[.]168

MD5:

cca9fbb11c194fc53015185b741887a8

n. CROWDEDFLOUNDER

Malware, which is designed to unpack and execute a Remote Access Trojan (RAT) binary in memory

Platform: Windows

Threat level: Middle

Category: Trojan, remote-access-trojan

General information

- This sample (MD5: f2b9d1cb2c4b1cd11a8682755bcc52fa) a Themida packed 32-bit Windows executable, which is designed to unpack and execute a Remote Access Trojan (RAT) binary in memory. This application is designed to accept arguments during execution or can be installed as a service with command line arguments. It is designed to listen as a proxy for incoming connections containing commands or can connect to a remote server to receive commands.

- When executed, the application is designed to open the Windows Firewall on the victim's machine to allow for incoming and outgoing connections from the victim system. The firewall is modified using a (netsh firewall add portopening) command.
- The following command line arguments are utilized to control the RAT functionality:
  -p: You can use the -p command line argument to force the malware to listen on a specific port. Example: malware.exe -p 8888
  -h: You can use the -h CLI to force the malware to connect to a remote host and port. Example: malware.exe -h <url_string>:8888

- The RAT uses a rotating exclusive or (XOR) cryptographic algorithm to secure its data transfers and command-and-control (C2) sessions. The malware is designed to accept instructions from the remote server to perform the following functions:

  - Download and upload files
  - Execute secondary payloads
  - Execute shell commands
  - Terminate running processes
  - Delete files
  - Search files
  - Set file attributes
  - Collect device information from installed storage devices (disk free space and their type)
  - List running processes information
  - Collect and send information about the victim's system
  - Securely download malicious DLLs and inject them into remote processes

Indicators of Compromise (IOCs)

MD5:

f2b9d1cb2c4b1cd11a8682755bcc52fa

o. HOTCROISSANT

This is the full-featured implant for reconnaissance, uploading/dowloading files and executing commands

Platform: N/A

Threat level: Middle

Category: Trojan

General information

- Sample (MD5: 062e9cd9cdcabc928fc6186c3921e945), detected by experts, is a full-featured beaconing implant. his sample performs a custom XOR network encoding and is capable of many features including conducting system surveys, file upload/download, process and command execution, and performing screen captures.
- The sample performs dynamic DLL importing and API lookups using LoadLibrary and GetProcAddress on obfuscated strings in an attempt to hide it's usage of network functions. However, only a small number of API calls are obfuscated this way, and their selection is not consistent through the sample.
- The sample obfuscates strings used for API lookups as well as the strings used during the network handshake using a simple Byte xor with 0x0f.

- The sample attempts to connect to a hardcoded C2 IP and then immediately sends it's Victim Info. It then listens for commands from the C2 and returns the results. Network communications are first zipped and then encoded with a custom xor algorithm.

Indicators of Compromise (IOCs)

CnC:

94[.]177[.]123[.]138

MD5:

062e9cd9cdcabc928fc6186c3921e945

p. ARTFULPIE

An implant that performs downloading and in-memory loading and execution of a DLL from a hardcoded URL

Platform: N/A

Threat level: Middle

Category: Loader

General information

- An implant (MD5: 2d92116440edef4190279a043af6794b) that performs downloading and in-memory loading and execution of a DLL from a hardcoded URL.
- Downloads the hardcoded URL hxxp[:]//193[.]56[.]28[.]103:88/xampp/thinkmeter[.]dll into memory using the user-agent string: "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)".
- Loads the .dll into its own address space manually (fully in memory).
- Calls the .dll's entry-point.

Indicators of Compromise (IOCs)

CnC:

193[.]56[.]28[.]103

MD5:

2d92116440edef4190279a043af6794b

q. BUFFETLINE

A tool, which is used for uploading/downloading, deleting and executing files, accessing the Windows command-line interface, creating and process completion

Platform: Windows

Threat level: Middle

Category: Trojan

General information

- A sample (MD5: 11cb4f1cdd9370162d67945059f70d0d) is a full-featured beaconing implant. This sample uses PolarSSL for session authentication, but then utilizes a FakeTLS scheme for network encoding using a modified RC4 algorithm. It has the capability to download, upload, delete, and execute files; enable Windows CLI access; create and terminate processes; and perform target system enumeration.
- The sample performs dynamic DLL importing and API lookups using LoadLibrary and GetProcAddress on obfuscated strings in an attempt to hide it's usage of network functions.
- The sample obfuscates strings used for API lookups as well as the strings used during the network handshake using a modified RC4 algorithm. A Python 3 script to decrypt the obfuscated strings is given below. Note: The hardcoded command and control (C2) IP's are not obfuscated, but appear in plaintext within the executable.
- The sample attempts to perform a PolarSSL handshake to initiate a connection to each of these hardcoded C2 IPs using TLS version 1.1. It uses the PolarSSL server_name extension with the Server Name set to «!Q@W#E$R%T^Y&U*I(O)P».
- After the TLS authentication is completed this particular sample does NOT use the session key that is generated via TLS. Instead, it uses a FakeTLS scheme, where a 'fake' TLS packet header is prepended to the packet data which is encrypted with custom xor encryption scheme
- After the TLS authentication, the sample performs a handshake with the C&C, where hardcoded 32 Byte strings are exchanged, as well as a Victim ID and the Victim Internal IP. After this exchange, the implant sends it's Victim Information, and then waits for tasking from the C&C.

Indicators of Compromise (IOCs)

CnC:

107[.]6[.]12[.]135
210[.]202[.]40[.]35

MD5:

11cb4f1cdd9370162d67945059f70d0d

r. KEYMARBLE

Trojan such as Remote Access Trojan (RAT), which is used to attack hackers from the group Lazarus

Platform: Windows

Threat level: Middle

Category: Trojan

General information

- This RAT uses a customized XOR cryptographic algorithm to secure its data transfers and command-and-control (C2) sessions. It is designed to accept instructions from the remote server to perform the following functions:
  - Download and upload files
  - Execute secondary payloads
  - Execute shell commands
  - Terminate running processes
  - Delete files
  - Search files
  - Set file attributes
  - Create registry entries for storing data:(HKEY_CURRENT_USER\SOFTWARE\Microsoft\WABE\DataPath)
  - Collect device information from installed storage devices (disk free space and their type)
  - List running processes information
  - Capture screenshots
  - Collect and send information about the victim's system (operating system, CPU, MAC address, computer name, language settings, list of disk devices and their type, time elapsed since the system was started, and unique identifier of the victim's system)

Indicators of Compromise (IOCs)

CnC:

222[.]143[.]21[.]13
194[.]45[.]8[.]41
212[.]143[.]21[.]43
100[.]43[.]153[.]60
104[.]194[.]160[.]59
104[.]194[.]160[.]69
http://37[.]238[.]135[.]70/img/anan[.]jpg
37[.]238[.]135[.]70

MD5:

3e925fb44f6d408e9f0f52cc8f0be2b4
b1091ee2a5af5e9f9aa0b9e57ab4cc41
1ce252b7bf2bca58266ae89d79c19144
cf6fb91589af0951f34bad0785bec4c1
6526e4b8c5dd407382300497f974be37
704d491c155aad996f16377a35732cb4
50bc6970fd8a8594bad6c64dd8b80a01
d8e51f1b9f78785ed7449145b705b2e4
dc3fff0873c3e8e853f6c5e01aa94fcf

SHA-1:

7C55572E8573D08F3A69FB15B7FEF10DF1A8CB33
E7FDEAB60AA4203EA0FF24506B3FC666FBFF759F
18EA298684308E50E3AE6BB66D7321A5CE664C8E
8826D4EDBB00F0A45C23567B16BEED2CE18B1B6A

s. Dtrack

This spyware was created by the Lazarus group and is being used to upload and download files to victims' systems, record key strokes and conduct other actions typical of a malicious remote administration tool (RAT).

Platform: N/A

Threat level: High

Category: Backdoor, remote-access-trojan

General information

A list of features is provided in the table below.

- upload a file to the victim's computer
- make target file persistent with auto execution on the victim's host start
- download a file from the victim's computer
- dump all disk volume data and upload it to a host controlled by criminals
- dump a chosen disk volume and upload it to a host controlled by criminals
- dump a chosen folder and upload it to a host controlled by criminals
- set a new interval timeout value between new command checks
- exit and remove the persistence and the binary itself
- default execute a process on the victim's host

Indicators of Compromise (IOCs)

CnC:

http://www[.]totalmateria[.]net/wp/profile2[.]php
www[.]totalmateria[.]net
http://www[.]materialindia[.]in/wp/wp-main/gallery/profile2[.]php
www[.]materialindia[.]in
http://10[.]0[.]3[.]254/software[.]php
10[.]0[.]3[.]254
http://katawaku[.]jp/bbs/data/theme/profile2[.]php
http://10[.]44[.]0[.]2/openldap/scripts/profile[.]php
10[.]44[.]0[.]2
http://gamestoyshop[.]us/ocart2/catalog/demo/provision[.]php

gamestoyshop[.]us
51[.]91[.]7[.]156
http://newshoesfasion[.]com/oscom/private/identity[.]php
newshoesfasion[.]com
158[.]69[.]114[.]83
http://heromessi[.]com/wp-public/career/car_add[.]php
heromessi[.]com
http://hawai-tour[.]com/wp/wp-imgs/luxury/scenes/view[.]php
hawai-tour[.]com
http://www[.]trendshow[.]xyz/wp/wp-admin/control/
www[.]trendshow[.]xyz
http://eshopt[.]freeoda[.]com/phpBB3/phpbb/php/config/
eshopt[.]freeoda[.]com
10[.]6[.]139[.]114
http://www[.]trendshow[.]xyz/wp/wp-template/

MD5:

7b9f11c1f7e227b615600d92a1c2893e
79843ad2896ab0dd81e07f4b4a62b970
4c357078e539beca24f290ff532f5cfe

SHA256:

fe51590db6f835a3a210eba178d78d5eeafe8a47bf4ca44b3a6b3dfb599f1702
4f71c62df0163d301cbc96e70771ebec2d4410679240c1d94183f5e10879c2f1
93a01fbbdd63943c151679d037d32b1d82a55d66c6cb93c40ff63f2b770e5ca9
4de28886265c1c8dae529f8158bdc6fa88dc2f5a595f44f677ab56641a7d618f
394356a5fad986dc59bbbb13f51912d4651edeec25411a35ec7d11255dc7a85e
e68b35f526826971d7a8f3b3d622b9f3eec395512aa537336f6cef883488ea60
17507e78a9f2449394a55a9fa5cbf2f08a1d2b1fdeac01324b5257230d4dd202
fe51590db6f835a3a210eba178d78d5eeafe8a47bf4ca44b3a6b3dfb599f1702
58fef66f346fe3ed320e22640ab997055e54c8704fc272392d71e367e2d1c2bb
94c57c2f40e699e08c1a880e9d1a34f295d5fc3534d1401dfed608bf4f04bb9b
36f43755e5e5988d112f28fbc1dcd9bdee4a31fb7004b52db26dacdbfe7cb72f
9f8d0568db4442962d4cd876448437997fc546403d8842ccb78b377541a7be33
541ebc44761cace61b2939a73e6b40d2ed0b8805e52746260978e451e9944fa1
3c9e6b520acc5b2eb16a5d06b3c37418e7260c45b1aafa2c53c84950b19b727f
9d9571b93218f9a635cfeb67b3b31e211be062fd0593c0756eb06a1f58e187fd
e505da2176c80a99fb3659bdecc3e0d3622179e8d7db2b120ead5abd598aeabd
bf8e3f0430a2a53608432cca208ac7d932e84a557defcfcdcb468b68cfacd7f8

t. Dtrack.Stealer

The application code is based on the source code of Dtrack.Backdoor. The "1007" command of the Trojan Dtrack.Backdoor dumps all disk volume data to a file and uploads it to a host controlled by criminals. The stealer performs the similar actions.

Platform: N/A

Threat level: Middle

Category: Infostealer

Indicators of Compromise (IOCs)

CnC:

172[.]22[.]22[.]156
10[.]2[.]114[.]1
172[.]22[.]22[.]5
10[.]2[.]4[.]1
10[.]2[.]114[.]9
http://10[.]2[.]114[.]9/cgibin/lib/dbc/func[.]php

MD5:

4f8091a5513659b2980cb53578d3f798
a1d103ae93c8b7cba0ea5b03d0bd2d9d

u. BADCALL

BADCALL is composed of three separate files, the first two are Windows executables designed to disable the firewall (by modifying a registry key) and transform infected systems into proxy servers. They, too, disguise malicious C2 communications as encrypted HTTPS traffic, but in actuality they encrypt their activity using a rudimentary cipher (XOR/ADD and SUB/XOR, respectively). The third file is an Android Package Kit (APK) file designed to run on Android platforms as a fully functioning Remote Access Tool (RAT).

Platform: Android

Threat level: Middle

Category: remote-access-trojan

General information

The Trojan has the following functions of a backdoor:

- Record the microphone
- Capture from the camera
- Upload, execute, and manipulate local files
- Download remote files
- Record GPS information

- Read contact information
- Observe SMS or MMS messages
- Record web browsing history and bookmarks
- Scan and capture WiFi information

Indicators of Compromise (IOCs)

MD5:

12cc14bbbc421275c3c6145bfa186dff
150cc194e43a661288a43a422212dc3e
3ad421c887aee54527b22844baeabbfe
763f0e57113d5855bafafc03c15f5b8f
d93b6a5c04d392fc8ed30375be17beb4

SHA256:

edd2aff8fad0c76021adc74fe3cb3cb1a02913a839ad0f2cf31fdea8b5aa8195
a984a5ac41446db9592345e547afe7fb0a3d85fcbbbdc46e16be1336f7a54041
06cadaac0710ed1ef262e79c5cf12d8cd463b226d45d0014b2085432cdabb4f3
4607082448dd745af3261ebed97013060e58c1d3241d21ea050dcdf7794df416
4694895d6cc30a336d125d20065de25246cc273ba8f55b5e56746fddaadb4d8a

v. Electricfish

Electricfish is a malware variant that targets Windows systems and is used by the advanced persistent threat Lazarus Group. The malware contained a custom protocol that permits traffic to be funneled between source IP and destination IP addresses, allowing traffic to travel through proxies to outside a victim network, bypassing authentication requirements. This can be used by attackers to covertly exfiltrate data and stay hidden in the network.

Platform: Windows

Threat level: N/A

Category: tunneling-tool

Indicators of Compromise (IOCs)

MD5:

df934e2d23507a7f413580eae11bb7dc
41030182de3899cded5531fb0dad5a78
f9ced93b94c8c8a8c0de20028300e11d
8d9123cd2648020292b5c35edc9ae22e
fa51d3b55296436ad91099bc6fb13c9f
63440d2ba41916c5cb9f0f91f4c82b5a
ee54ae8df7b969c4fd6ffda465eeddd4
0ba6bb2ad05d86207b5303657e3f6874

22082079ab45ccc256e73b3a7fd54791

Network Signatures

TROJAN Win32/ElectricFish Authentication Packet Observed

alert tcp $HOME_NET any -> any any (msg:"TROJAN Win32/ElectricFish Authentication Packet Observed"; target:src_ip; flow:established,to_server; content:"aaaabbbbccccdddd|00 00 00 00 00 00 00 00|"; depth:24; fast_pattern; content:"|00 00 04 00 00 00|"; distance:2; within:6; reference:url,www.us-cert.gov/ncas/analysis-reports/AR19-129A; classtype:trojan-activity; sid:2027340; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, created_at 2019_05_09, deployment Perimeter, deployment Internal, former_category TROJAN, performance_impact Low, signature_severity Major, tag APT, tag T1090, tag connection_proxy, updated_at 2019_05_09, severity 3, ti_malware_id b44769790886c8833ba893d8927ff6c79108a51c, ti_malware_name Electricfish, malware_family Electricfish, rule_origin etpro;)

w. RATv3.ps

RATv3.ps - is a PowerShell remote access tool (RAT) or backdoor having the functionality to run commands, manipulate files, upload/download files from a C2 server, manipulate running processes, collect system information and manipulate the Windows registry.

Platform: Windows

Threat level: High

Category: Backdoor, remote-access-trojan

General information

It communicates over TLS with a custom protocol using XOR encoding. Minor obfuscation occurs throughout the script, which makes it slightly more difficult to analyse. The script uses several light forms of obfuscation. Function names and variable names are replaced with non-descriptive names, and strings are stored as base64 encoded Unicode.

This malware collects various operating system information and sends it to the C2 server. The collected data includes:

- Internal IP address
- Computer name
- Username
- OS version
- OS architecture
- Proxy status
- Proxy server

- Script path
- Last boot time
- OS caption
- OS language
- OS country code
- Primary C2 address and port
- Secondary C2 address and port
- 32/64 bit system

Indicators of Compromise (IOCs)

MD5:

b12325a1e6379b213d35def383da2986
aff88674d2869f79f9c6d5ecf5fc2d63
1e2795f69e07e430d9e5641d3c07f41e
3be75036010f1f2102b6ce09a9299bca
b88d4d72fdabfc040ac7fb768bf72dcd
7c651d115109fd8f35fddfc44fd24518
25376ea6ae0903084c45bf9c57bd6e4f
8a41520c89dce75a345ab20ee352fef0

x. Rising Sun

this is a full-featured modular backdoor that conducts reconnaissance on the victim's network.

Platform: N/A

Threat level: High

Category: Backdoor

General information

It was found that Rising Sun is based on the Duuzer Trojan family, which also belongs to cybercriminals from the Lazarus group.

The Rising Sun has 14 backdoor options:

- Execute commands
- Get disk information
- Disc type
- Total bytes on disk
- Total free bytes on disk
- Name of the specified volume
- Run a process from a binary Windows
- Get information about processes
- End the process

- Get file time
- Read file
- Clear process memory
- Burn file to disk
- Delete file
- Getting more information about files in a directory
- Connect to IP address
- Change file attributes

Indicators of Compromise (IOCs)

CnC:

87[.]101[.]243[.]252

MD5:

f3bd9e1c01f2145eb475a98c87f94a25
51b3e2c7a8ad29f296365972c8452621
f940a21971820a2fcf8433c28be1e967
71cdcc903f94f56c758121d0b442690f
bb6cbebd4ffd642d437afc605c32eca0

SHA256:

47181c973a8a69740b710a420ea8f6bf82ce8a613134a8b080b64ce26bb5db93
6b71465e59eb1e266d47efeaecc256a186d3e08f570bffcfd5ac55e635c67c2a
c7024cf43d285ec9671e8dc1eae87281a6ee6f28e92d69d94474efc2521f03ed
d57d772eefa6086b5c249efff01189cf4869c2b73007af63affc353474eaafcb
5b28c86d7e581e52328942b35ece0d0875585fbb4e29378666d1af5be7f56b46
fb6d81f4165b41febc739358aeba0fe15048e1d445296e8df9104875be30f9a7
d589043a6f460855445e35154c5a0ff9dbc8ee9e159ae880e38ca00ea2b9a94f
a01bd92c02c9ef7c4785d8bf61ecff734e990b255bba8e22d4513f35f370fd14
c327de2239034b6f6978884b33582ce97761bcc224239c955f62feebd01e5946
37f652e2060066a1c2c317195573a334416f5a9b9933cfb1ece55bea8048d80f
4cf3a7e17dc4628725dd34b8e98238ed0a2df2dc83189db98d85a38f73706fa5
fd5a7e54cfdd3b3f32b44d8fdd845e62d6b86c0ddb550c544d659588d06ceaee
4efeea9eeae3d668897206eeccb1444d542ea537ca5c2787f13dd5dadd0e6aaa
4a6aba1c182dd8304bac91cc9e1fc39291d78044995f559c1d3bce05afd19982
90d8643e7e52f095ed59ed739167421e45958984c4c9186c4a025e2fd2be668b
66df7660ddae300b1fcf1098b698868dd6f52db5fcf679fc37a396d28613e66b
89b25f9a454240a3f52de9bf6f9a829d2b4af04a7d9e9f4136f920f7e372909b
5a69bce8196b048f8b98f48c8f4950c8b059c43577e35d4af5f26c624140377c
477ca3e7353938f75032d04e232eb2c298f06f95328bca1a34fce1d8c9d12023
88a5287b6e9879e79240660408e2e868d9d332e3c37c753a05a40b87f1549646

y. KillDisk

KillDisk is a hard drive eraser software for secure formatting of hard drives without any possibility of following data recovery.

Platform: N/A

Threat level: N/A

Category: Trojan, wiper

Indicators of Compromise (IOCs)

SHA256:

edbc90c217eebabb7a9b618163716f430098202e904ddc16ce9db994c6509310
1a09b182c63207aa6988b064ec0ee811c173724c33cf6dfe36437427a5c23446
11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80
0dc82b9f257a3c03d51c4792fd6fc11a29814008651bbf40ae9cdd5f16455743
c4a07bfc37a44dc85df2c63f369abb530dc2193ab1be506fc5dd45d56a44ca76
91dfd9ef7d61ef1c1c20bf0dd29fd0e1862f02d94758d454cd7265d2171b8c88
5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6
368d5c536832b843c6de2513baf7b11bcafea1647c65df7b6f2648840fa50f75
c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d
8a04f8481f1ef57f66b974802919e936c59a32d1cd9ef83186e6911b9ae773b0
a6a167e214acd34b4084237ba7f6476d2e999849281aa5b1b3f92138c7d91c7a
8a81a1d0fae933862b51f63064069aa5af3854763f5edc29c997964de5e284e5
f9f3374d89baf1878854f1700c8d5a2e5cf40de36071d97c6b9ff6b55d837fca

z. PowerSpritz

PowerSpritz is a Windows executable that hides both its valid payload and malicious PowerShell command using a custom implementation of the now rarely used Spritz encryption algorithm.

Platform: N/A

Threat level: N/A

Category: dropper

General information

Indicators of Compromise (IOCs)

CnC:

http://skype[.]2[.]vu/1
https://doc-00-64-docs[.]googleusercontent[.]com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/

39cbphg8k5qve4q5rr6nonee1bueiu8o/1499428800000/13030420262846080952/*/0B63J1WTZC49hX1JnZUo4Y1pnRG8?e=download
http://122[.]248[.]34[.]23/Index[.]php?t=SkypeSetup&r=mail_new
http://201[.]211[.]183[.]215:8080/update[.]php?t=Skype&r=update
http://122[.]248[.]34[.]23/Index[.]php?t=Telegram&r=1[.]1[.]9
http://macintosh[.]linkpc[.]net:8080/mainls[.]cs
http://telegramupdate[.]2[.]vu/5
http://dogecoin[.]deaftone[.]com:8080/mainls[.]cs
http://skype[.]2[.]vu/k
http://skypeupdate[.]2[.]vu/1
https://drive[.]google[.]com/uc?export=download&id=0B63J1WTZC49hdDR0clR3cFplTVE
skype[.]2[.]vu
macintosh[.]linkpc[.]net
telegramupdate[.]2[.]vu
dogecoin[.]deaftone[.]com
skypeupdate[.]2[.]vu
104[.]236[.]48[.]227

MD5:

26466867557f84dd4784845280da1f27
ad99fd5711dbec2520f62385a595ee3b
b82f3e54bb97d4f92dc7c777f2e765ab
0518ca7a8bd6d93bbafc6022669d5459

SHA-256:

cbebafb2f4d77967ffb1a74aac09633b5af616046f31dddf899019ba78a55411
9ca3e56dcb2d1b92e88a0d09d8cab2207ee6d1f55bada744ef81e8b8cf155453
5a162898a38601e41d538f067eaf81d6a038268bc52a86cf13c2e43ca2487c07

aa. Joanap

Joanap is a fully functional RAT that can receive multiple commands that can be set remotely from a management server. Joanap usually infects the system as a file downloaded by other malware that users unknowingly downloaded either when visiting sites compromised by hackers or when opening malicious email attachments. Joanap gives cybercriminals the ability to expand data, load and run additional payloads, initialize proxy connections on a compromised Windows device, manage files and processes, create and delete directories, and manage nodes.

Platform: N/A

Threat level: N/A

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

110[.]164[.]115[.]177
118[.]102[.]187[.]188
118[.]70[.]143[.]38
119[.]15[.]245[.]179
122[.]55[.]13[.]34
168[.]144[.]197[.]98
189[.]114[.]147[.]186
196[.]44[.]250[.]231
201[.]222[.]66[.]25
60[.]251[.]197[.]122
62[.]135[.]122[.]53
62[.]150[.]4[.]42
62[.]87[.]153[.]243
63[.]131[.]248[.]197
63[.]149[.]164[.]98
64[.]71[.]162[.]61
66[.]210[.]47[.]247
69[.]15[.]198[.]186
72[.]156[.]127[.]210
75[.]145[.]139[.]249
78[.]38[.]221[.]4
80[.]191[.]114[.]136
81[.]130[.]210[.]66
81[.]83[.]10[.]138
83[.]211[.]229[.]42
92[.]253[.]102[.]217
92[.]47[.]141[.]99
93[.]62[.]0[.]22
94[.]28[.]57[.]110
96[.]39[.]78[.]157

MD5:

298775B04A166FF4B8FBD3609E716945
4613f51087f01715bf9132c704aea2c2
fd59af723b7a4044ab41f1b2a33350d6
074dc6c0fa12cadbc016b8b5b5b7b7c5
27a3498690d6e86f45229acd2ebc0510
7a83c6cd46984a84c40d77e9acff28bc
1d8f0e2375f6bc1e045fa2f25cd4f7e0
304cea78b53d8baaa2748c7b0bce5dd0
a1ad82988af5d5b2c4003c42a81dda17

SHA-256:

29b8c57226b70fc7e095bb8bed4611d923f0bcefc661ebae5182168613b497f8
66d44e2bc7495662d068051c5a687d17c7e95c8f04acb0f06248b34cd255cd25
fae77c173815b561ad02d8994d0e789337a04d9966dd27a372fd9055f1ac58b1
c1c56c7eb2f6b406df908ae822a6ea936f9cc63010ee3c206186f356f2d1aa94
4c5b8c3e0369eb738686c8a111dfe460e26eb3700837c941ea2e9afd3255981e
113d705d7736c707e06fb37ac328080b3976838d0a7b021fd5fb299896c22c7c
1a6c3e5643d7e22554ac0a543c87a2897ea4ea5a07bc080943a310a391e20713
0b860af58a9d2d7607f09022aa69508b0966a1cc8d953d3995a5fe07f8fabcac
5d73d14525ced5bdf16181f70f4d931b9c942c1ae16e318517d1cd53f4cd6ea9
c34ad273d836b2f058bbd73ea9958d272bd63f4119dacacc310bf38646ff567b
500c713aa82a11c4c33e9617cad4241fcef85661930e4986c205233759a55ae8
5f5acf76a991c1ca33855a96ec0ac77092f2909e0344657fe3acf0b2419d1eea
c6d96be46ce3d616e0cb36d53c4fade7e954e74bfd2e34f9f15c4df58fc732d2
d558bb63ed9f613d51badd8fea7e8ea5921a9e31925cd163ec0412e0d999df58
006e0cc29697db70b2d4319f320aa0e52f78bf876646f687aa313e8ba04e6992
2d9edf45988614f002b71899740d724008e9a808efad00fa79760b31e0a08073
3d2a7ea04d2247b49e2dcad63a179ae6a47237eddbfd354082f1417a63e9696e
ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781
f4113e30d50e0afc4fa610a3181169bb03f6766aea633ed8c0c0d1639dfc5b29
08203b4ddc9571418b2631ebbc50bea57a00eadf4d4c28bd882ee8e831577a19
a3992ed9a4273de53950fc55e5b56cc5b1327ffee59b1cea9e45679adc84d008
575028bbfd1c3aaff27967c9971176ae7038902f1a67d70def55ae8456e6166d
428cf6ec1a4c947b51ec099a656f575ce42f67737ee53f3afc3068a25adb4c0d
f53e3e0b3c524471b1f064aabd0f782802abb4e29534a1b61a6b25ad8ec30e79

bb. Brambul

Brambul is a malicious SMB worm for 32-bit Windows that functions as a dynamic library service file or portable executable file that is frequently downloaded and installed on the victim's network by droppers. When executed, the malware attempts to contact victim systems and IP addresses on the local subnets of the victims. If successful, the application tries to gain unauthorized access via the SMB protocol (ports 139 and 445) by launching a brute force attack using a list of available passwords. In addition, the malware generates random IP addresses for further attacks.

Platform: N/A

Threat level: N/A

Category: remote-access-trojan

Indicators of Compromise (IOCs)

MD5:

e86c2f4fc88918246bf697b6a404c3ea
1c532fad2c60636654d4c778cfe10408
1db2dced6dfa04ed75b246ff2784046a
3844ec6ec70347913bd1156f8cd159b8
40878869de3fc5f23e14bc3f76541263
95a5f91931723a65dcd4a3937546da34
99d9f156c73bd69d5df1a1fe1b08c544
a1ad82988af5d5b2c4003c42a81dda17
ca4c2009bf7ff17d556cc095a4ce06dd
f273d1283364625f986050bdf7dec8bb

cc. BrowserPasswordDump

Browser Password Dump is the free command-line (cmd.exe) version of Browser Password Decryptor. This shady tool serves the purpose of recovering passwords from popular web browsers through cmd.exe.

Platform: Windows

Threat level: N/A

Category: N/A

Indicators of Compromise (IOCs)

MD5:

e74047ca6798423e47096c77efb0ca1d

dd. HARDRAIN

HARDRAIN is composed three malicious executable files. The first two are 32-bit, Windows-based dynamic link library (DLL) executables, which configure the Windows Firewall to allow incoming connections, thus allowing machines to function as proxies. Illicit communications are masked as HTTPS sessions by leveraging public certificates sourced from legitimate Internet services. In reality, however, the traffic is actually encrypted using an unidentified algorithm. Accompanying these two DLL files is an Android-based Executable Linkable Format (ELF) file that connects to hard-coded Internet Protocol (IP) addresses and acts as a RAT program.

Platform: Android

Threat level: Middle

Category: remote-access-trojan

Indicators of Compromise (IOCs)

MD5:

9ce9a0b3876aacbf0e8023c97fd0a21d
8b98bdf2c6a299e1fde217889af54845
24f61120946ddac5e1d15cd64c48b7e6

ee. Gh0st

Gh0st is a well-known Chinese RAT used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth. Gh0st presumably was made by. C.Rufus Security Team, source code is publicly available since 2011.

Platform: Windows

Threat level: High

Category: RAT

Other Name: Ghost, Gh0st RAT

General information

Gh0st is a well-known Chinese RAT used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth. Gh0st presumably was made by. C.Rufus Security Team, source code is publicly available since 2011.

Indicators of Compromise (IOCs)

CnC:

http://180[.]235[.]133[.]235/img[.]gif
http://phpvlan[.]com:8080
http://180[.]235[.]133[.]121/images/img[.]gif
phpvlan[.]com
Pi[.]mai1[.]info
162[.]251[.]120[.]179

MD5:

858eaa588a5e30cd5156b27f72caa0fe
a173106fa27ac9861054dbf881ba568a
f7b106acc281a9aa395fb944c858c0c0
bbf9822a903ef7b9f33544bc36197594
b47223ab622282cb5ae934cea8353a5b

SHA256:

0b1217bd95678ca4e6f81952226a0cfd639ce4b2f7e7fce94ab177d42c5abf62
afbcd0dd46988f3151a08da87740fb77d285fc4c6b20b4ae4456b7773050e960
3eb72d696525b2968a528bc66414c11f31babe7c19f815cba19b131ed35ffdb2
3a856d8c835232fe81711680dc098ed2b21a4feda7761ed39405d453b4e949f6

Network Signatures

Win32.Trojan.PCRat/Gh0st Beacon

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan.PCRat/Gh0st Beacon"; target:src_ip; flow:established,to_server; content:"greater!"; depth:8; threshold:type limit, track by_src, seconds 360, count 1; classtype:backdoor; reference:md5,44e65266280b6ab1832dc1bc24ea5a40; sid:1002066; rev:1; metadata:severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin gib;)

TROJAN [CrowdStrike] ANCHOR PANDA - Adobe Gh0st Beacon

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN [CrowdStrike] ANCHOR PANDA - Adobe Gh0st Beacon"; target:src_ip; flow:established, to_server; content:"Adobe"; depth:5; content:"|e0 00 00 00 78 9c|"; distance:4; within:15; reference:url,blog.crowdstrike.com/whois-anchor-panda/index.html; classtype:backdoor; sid:2016656; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2013_03_22, deployment Perimeter, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, malware_family Panda, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 23

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 23"; target:src_ip; flow:to_server,established; dsize:>11; content:"|78 9c|"; offset:8; byte_jump:4,-18,relative,little,from_beginning, post_offset 1; isdataat:!2,relative; pcre:"/^.{8}[\x20-\x7e]+?.{2}\x78\x9c/s"; reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; reference:md5,db1c4342f617798bcb2ba5655d32bf67; classtype:backdoor; sid:2018075; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2014_02_05, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Gh0st_Apple Checkin

alert http $HOME_NET any -> $EXTERNAL_NET 110 (msg:"TROJAN Gh0st_Apple Checkin"; target:src_ip; flow:to_server,established; content:"GET"; http_method; content:".gif?pid"; fast_pattern; content:"&v="; content:"Mozilla/4.0("; http_user_agent; reference:url,contagiodump.blogspot.com.br/2013/09/sandbox-

miming-cve-2012-0158-in-mhtml.html;
reference:md5,82644661f6639c9fcb021ad197b565f7; classtype:backdoor;
sid:2017412; rev:8; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2013_09_03, deployment Perimeter, former_category MALWARE,
signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01,
severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c,
ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Gh0st Trojan CnC 2

alert tcp $HOME_NET any -> $EXTERNAL_NET !25 (msg:"TROJAN Gh0st Trojan CnC
2"; target:src_ip; flow:established,to_server; dsize:<250; content:"Gh0st"; offset:8;
depth:5; classtype:backdoor; sid:2017505; rev:3; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2013_09_20, deployment Perimeter, former_category MALWARE,
signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01,
severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c,
ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 12 SET

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family
PCRat/Gh0st CnC traffic (OUTBOUND) 12 SET"; target:src_ip;
flow:to_server,established; dsize:8; content:"|00 00|"; offset:2; depth:2; content:"|00
00|"; distance:2; within:2; flowbits:set,ET.gh0stFmly; flowbits:noalert;
reference:url,www.securelist.com/en/descriptions/10155706/Trojan-
GameThief.Win32.Magania.eogz;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Na
me=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231;
reference:md5,3b1abb60bafbab204aeddf8acdf58ac9; classtype:backdoor;
sid:2017935; rev:3; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint,
created_at 2014_01_06, deployment Perimeter, former_category MALWARE,
signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01,
severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c,
ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 15

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family
PCRat/Gh0st CnC traffic (OUTBOUND) 15"; target:src_ip; flow:to_server,established;
dsize:>11; content:"FWKJGH"; offset:8; depth:6;
byte_jump:4,0,little,from_beginning,post_offset 5; isdataat:!2,relative;
reference:url,www.securelist.com/en/descriptions/10155706/Trojan-
GameThief.Win32.Magania.eogz;
reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Na
me=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231;

reference:md5,edd8c8009fc1ce2991eef6069ae6bf82; classtype:backdoor; sid:2017974; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2014_01_16, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 17

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 17"; target:src_ip; flow:to_server,established; dsize:>11; content:"AngeL"; depth:5; byte_jump:4,0,relative,little,from_beginning,post_offset -1; isdataat:!2,relative; reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; classtype:backdoor; sid:2018007; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2014_01_23, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;

TROJAN Gh0st Remote Access Trojan Encrypted Session To CnC Server

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Gh0st Remote Access Trojan Encrypted Session To CnC Server"; target:src_ip; flow:established,to_server; dsize:100<>300; content:"Gh0st"; depth:5; reference:url,www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; reference:url,www.symantec.com/connect/blogs/inside-back-door-attack; classtype:backdoor; sid:2013214; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2011_07_06, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2016_07_01, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 5

alert tcp $HOME_NET any -> $EXTERNAL_NET [!5800] (msg:"TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 5"; target:src_ip; flow:to_server,established; dsize:>11; content:"|78 9c|"; fast_pattern; byte_jump:4,0,little,post_offset 1; isdataat:!2,relative; byte_extract:4,0,compressed_size,little; byte_test:4,>,compressed_size,4,little; pcre:"/^.{8}[\x20-\x7e]+?[\x00]*?\x78\x9c/s";

reference:url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eogz; reference:url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FPcClient.ZR&ThreatID=-2147325231; classtype:backdoor; sid:2017876; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2013_12_17, deployment Perimeter, former_category MALWARE, signature_severity Critical, tag PCRAT, tag Gh0st, tag RAT, updated_at 2019_10_07, severity 5, ti_malware_id a4ed8587dd24232c3d4faf06f0be64b7ac0b2e6c, ti_malware_name Gh0st, malware_family Gh0st, rule_origin etpro;)

ff. WannaCry

WannaCry, originally named as WanaCrypt, having aliases of Wana Crypt0r and Wana Decrypt0r, is a ransomware wormon Microsoft Windows (can be run on Linux via WINE) that uses two NSA-leaked tools that has wreaked havoc in airports, banks, universities, hospitals and many other facilities. It has spread to some 150 countries worldwide.

Platform: Windows

Threat level: High

Category: Ransomware

General information

On 12/05/2017, 2017 widespread use of ransomware WannaCry Cryptor that affects Microsoft Windows systems was observed. This ransomware has the behaviour of a worm and was spreader using exploit ETERNALBLUE. It scanned network and infected each vulnerable machine. Thus, great number of systems were infected in 11 countries during two hours. Big corporations and companies were affected. The threat actor is asking for $ 300 in Bitcoins to restore access to the files.

Security researches @MalwareTechBlog and Darien Huss (Proofpoint) established that the switch was hardcoded into the malware in case the creator wanted to stop it spreading. This involved a very long nonsensical domain name that the malware makes a request to – just as if it was looking up any website – and if the request comes back and shows that the domain is live, the kill switch takes effect and the malware stops spreading. This domain was unregistered, so researcher registered it in himself and stop spreading.

In addition, on 12/05/2017 Microsoft released patch for unsupported systems to fix this vulnerability.

Indicators of Compromise (IOCs)

CnC:

85[.]248[.]227[.]164
194[.]109[.]206[.]212
217[.]79[.]190[.]25
204[.]11[.]50[.]131
95[.]183[.]48[.]12
171[.]25[.]193[.]9
195[.]154[.]164[.]243
131[.]188[.]40[.]189
5[.]9[.]159[.]14
199[.]254[.]238[.]52
178[.]16[.]208[.]57
128[.]31[.]0[.]39
163[.]172[.]35[.]247
154[.]35[.]175[.]225
iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
104[.]17[.]37[.]137
104[.]17[.]38[.]137
104[.]17[.]39[.]137
104[.]17[.]40[.]137
104[.]17[.]41[.]137
212[.]51[.]134[.]123
5[.]199[.]142[.]236
197[.]231[.]221[.]221
149[.]202[.]160[.]69
46[.]101[.]166[.]19
91[.]121[.]65[.]179
2[.]3[.]69[.]209
146[.]0[.]32[.]144
50[.]7[.]161[.]218
87[.]101[.]243[.]252
184[.]74[.]243[.]67
203[.]69[.]210[.]247

MD5:

6f0338af379659a5155b3d2a4f1a1e92
3bc855bfadfea71a445080ba72b26c1c
f27cf59b00dacdd266ad7894a1df0894

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 1"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:ransomware; sid:2024298; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2019_10_07, severity 5, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 3"; target:src_ip; flow:established,to_server; content:"ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf"; http_header; fast_pattern; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:ransomware; sid:2024300; rev:5; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2019_10_07, severity 5, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 2"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis;

reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:trojan-activity; sid:2024299; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2017_05_18, severity 3, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 4

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 4"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:trojan-activity; sid:2024301; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2017_05_18, severity 3, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 5

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN W32/WannaCry.Ransomware Killswitch Domain HTTP Request 5"; target:src_ip; flow:established,to_server; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; http_header; fast_pattern:only; content:"Host|3a 20|"; http_header; pcre:"/^[^\s]*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea\.[a-z]{2,5}\x0d\x0a/HRi"; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:trojan-activity; sid:2024302; rev:3; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_16, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Critical, tag Ransomware, updated_at 2017_05_18, severity 3, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

TROJAN Possible WannaCry DNS Lookup 1

alert dns $HOME_NET any -> any any (msg:"TROJAN Possible WannaCry DNS Lookup 1"; target:src_ip; dns_query; content:"iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea"; depth:41; nocase; reference:cve,2017-0144; reference:url,www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis; reference:url,www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; classtype:ransomware; sid:2024291; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_05_12, deployment Perimeter, former_category TROJAN, signature_severity Critical, tag Ransomware, updated_at 2020_08_20, severity 5, ti_malware_id 209b7f4c6f832f3d645dbf8ba8f6697ac649d3de, ti_malware_name WannaCry, malware_family WannaCry, rule_origin etpro;)

gg. DoublePulsar

DoublePulsar is a backdoor developed by Equation Group (Presumably, this group is part of ANB) that was leaked by The Shadow Brokers in early 2017. DoublePulsar can be classified as a "stager" - an implant that first gets on the infected device and serves to install other implants.

Platform: N/A

Threat level: High

Category: Backdoor

Indicators of Compromise (IOCs)

Network Signatures

EXPLOIT Possible DOUBLEPULSAR Beacon Response

alert smb $HOME_NET any -> any any (msg:"EXPLOIT Possible DOUBLEPULSAR Beacon Response"; target:src_ip; flow:from_server,established; content:"|00 00 00 23 ff|SMB2|02 00 00 c0 98 07 c0 00 00|"; depth:18; content:"|00 00 00 08 ff fe 00 08|"; distance:8; within:8; fast_pattern; pcre:"/^[\x50-\x59]/R"; content:"|00 00 00|"; distance:1; within:3; isdataat:!1,relative; classtype:ek-activity; sid:2024216; rev:1; metadata:attack_target SMB_Server, created_at 2017_04_17, deployment Internal, former_category EXPLOIT, signature_severity Critical, updated_at 2019_09_28, severity 3, ti_malware_id c7c12af404eff6f639799e6b103044f1aa0d7357, ti_malware_name DoublePulsar, malware_family DoublePulsar, rule_origin etpro;)

EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication

alert tcp any any -> $HOME_NET 445 (msg:"EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication"; target:src_ip; flow:to_server, established;

content:"|FF|SMB2|00 00 00 00|"; depth:9; offset:4;
byte_test:2,!=,0x0000,52,relative,little;
pcre:"/^.{52}(?:\x04|\x09|\x0A|\x0B|\x0C|\x0E|\x11)\x00/R";
reference:url,github.com/ptresearch/AttackDetection; classtype:attempted-admin;
sid:2024766; rev:2; metadata:affected_product
Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target SMB_Server, created_at
2017_09_25, deployment Internet, former_category EXPLOIT, performance_impact
Low, signature_severity Major, updated_at 2017_09_28, severity 1, ti_malware_id
c7c12af404eff6f639799e6b103044f1aa0d7357, ti_malware_name DoublePulsar,
malware_family DoublePulsar, rule_origin etpro;)

hh. Volgmer

Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. Since at least 2013, Lazarus Group (aka Hidden Cobra) actors have been observed using Volgmer malware in the wild to target the government, financial, automotive, and media industries. It is a Destover-related backdoor and has several capabilities including: gathering system information, updating service registry keys, downloading and uploading files, executing commands, terminating processes, and listing directories. Also, a botnet controller functionality was discovered in one of the known samples. The malware communicates with its C&C server either through a custom binary protocol via TCP port 8080 or 8088 or by implementing Secure Socket Layer (SSL) encryption.

Platform: Windows

Threat level: High

Category: Backdoor

General information

Gather system information
Update service registry keys
Download and upload files
Execute commands
Terminate processes
List directories
Control botnets

Successful network intrusion could result in the following impacts:

Temporary or permanent loss of sensitive or proprietary information,
Disruption to regular operations,
Financial losses incurred to restore systems and files, and
Potential harm to an organization’s reputation.

Indicators of Compromise (IOCs)

CnC:

12[.]217[.]8[.]82
200[.]42[.]69[.]13
206[.]123[.]66[.]136
213[.]207[.]142[.]82
195[.]28[.]91[.]232
195[.]97[.]97[.]148
83[.]231[.]204[.]157
84[.]232[.]224[.]218
114[.]79[.]141[.]59
89[.]165[.]119[.]105
91[.]106[.]77[.]7
94[.]183[.]177[.]90
95[.]38[.]16[.]188
185[.]115[.]164[.]86
78[.]39[.]125[.]67
85[.]185[.]30[.]195
61[.]153[.]146[.]207
203[.]196[.]136[.]60
43[.]249[.]216[.]6
117[.]240[.]190[.]226
14[.]102[.]46[.]3
182[.]77[.]61[.]231
116[.]90[.]226[.]67
203[.]118[.]42[.]155
222[.]236[.]46[.]5
182[.]73[.]165[.]58
183[.]82[.]199[.]174
183[.]82[.]33[.]102
203[.]110[.]91[.]252
113[.]203[.]238[.]98
186[.]149[.]198[.]172
103[.]27[.]164[.]42
115[.]178[.]96[.]66
117[.]218[.]84[.]197
14[.]139[.]125[.]214
180[.]211[.]97[.]186
82[.]129[.]240[.]148
82[.]201[.]131[.]124
203[.]88[.]138[.]79
178[.]248[.]41[.]117

103[.]241[.]106[.]15
58[.]185[.]197[.]210
185[.]134[.]98[.]141
213[.]207[.]209[.]36
37[.]235[.]21[.]166
91[.]98[.]126[.]92
123[.]176[.]38[.]17
190[.]210[.]39[.]16
206[.]163[.]230[.]170
220[.]128[.]131[.]251
24[.]242[.]176[.]130
64[.]3[.]218[.]243
78[.]93[.]190[.]70
200[.]87[.]126[.]116
91[.]98[.]36[.]66
123[.]231[.]112[.]147
110[.]77[.]137[.]38
118[.]175[.]22[.]10
116[.]48[.]145[.]179
186[.]116[.]9[.]20
199[.]15[.]234[.]120
115[.]115[.]174[.]67
115[.]249[.]29[.]78
117[.]211[.]164[.]245
37[.]216[.]67[.]155
85[.]132[.]123[.]50
88[.]201[.]64[.]185
45[.]124[.]169[.]36
222[.]44[.]80[.]138
117[.]239[.]102[.]132
117[.]239[.]144[.]203
117[.]247[.]8[.]239
14[.]141[.]129[.]116
182[.]156[.]76[.]122
41[.]131[.]164[.]156
128[.]65[.]184[.]131
78[.]38[.]114[.]15
117[.]239[.]214[.]162
123[.]176[.]38[.]175
212[.]33[.]200[.]86
41[.]21[.]201[.]101
89[.]122[.]121[.]230
194[.]224[.]95[.]20

121[.]170[.]194[.]185
45[.]118[.]34[.]215
139[.]255[.]62[.]10
128[.]65[.]187[.]94
185[.]46[.]218[.]77
222[.]165[.]146[.]86
122[.]146[.]157[.]141
203[.]147[.]10[.]65
217[.]218[.]90[.]124
78[.]38[.]182[.]242
85[.]9[.]74[.]159
80[.]95[.]219[.]72
203[.]131[.]222[.]99
210[.]187[.]87[.]181
182[.]74[.]42[.]194
182[.]176[.]121[.]244
125[.]18[.]9[.]228
182[.]72[.]113[.]90
103[.]16[.]223[.]35
134[.]121[.]41[.]45
58[.]82[.]155[.]98
217[.]219[.]193[.]158
217[.]219[.]202[.]199
37[.]98[.]114[.]90
80[.]191[.]171[.]32
91[.]98[.]112[.]196
182[.]73[.]245[.]46
115[.]186[.]133[.]195
182[.]187[.]139[.]132
84[.]235[.]85[.]86
61[.]91[.]47[.]142
89[.]190[.]188[.]42
109[.]68[.]120[.]179
103[.]10[.]55[.]35
31[.]146[.]82[.]22
103[.]27[.]164[.]10
185[.]113[.]149[.]239
27[.]114[.]187[.]37
140[.]136[.]205[.]209
125[.]25[.]206[.]15
117[.]247[.]63[.]127
118[.]67[.]237[.]124
125[.]17[.]79[.]35

200[.]42[.]69[.]133
112[.]133[.]214[.]38
199[.]68[.]196[.]125
113[.]28[.]244[.]194

MD5:

2D2B88AE9F7E5B49B728AD7A1D220E84
9A5FA5C5F3915B2297A1C379BE9979F0
BA8C717088A00999F08984408D0C5288
1B8AD5872662A03F4EC08F6750C89ABC
E034BA76BEB43B04D2CA6785AA76F007
EB9DB98914207815D763E2E5CFBE96B9
143cb4f16dcfc16a02812718acd32c8f
1ecd83ee7e4cfc8fed7ceb998e75b996
35f9cfe5110471a82e330d904c97466a
5dd1ccc8fb2a5615bf5656721339efed
81180bf9c7b282c6b8411f8f315bc422
e3d03829cbec1a8cca56c6ae730ba9a8
82777a88d6f2ffd53f8c5ae5a6b6565b
b13ad0e8ffca0572b6ac9a5ee1d03f21
f9e6c35dbb62101498ec755152a8a67b
a545f548b09fdf61405f5cc07e4a7fa1
a976c54b849939b35a1b8dbc930c029d
aefcd8e98a231bccbc9b2c6d578fc8f3
8dc5877956229c5139670b1f75fb0953
53098c29b748e881e4d62720d7190ac5
af1f7d8ec11ce9bb4609a1088dea0e85
3a6b48871abbf2a1ce4c89b08bc0b7d8

Network Signatures

Possible Volgmer User-Agent

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Possible Volgmer User-Agent"; target:src_ip; flow:established,to_server; content:"Mozillar/"; http_user_agent; depth:9; classtype:backdoor; reference:url,https://www.us-cert.gov/ncas/alerts/TA17-318B; sid:1002080; rev:1; metadata:severity 5, ti_malware_id faece0aa10e65d5804c138704c65c4ed54e144df, ti_malware_name Volgmer, malware_family Volgmer, rule_origin gib;)

ii. FASTCash

This malware in turn intercepts fraudulent Lazarus cash withdrawal requests and sends fake approval responses, allowing the attackers to steal cash from ATMs.

Platform: ATM, Windows

Threat level: High

Category: atm-malware

Indicators of Compromise (IOCs)

MD5:

b3efec620885e6cf5b60f72e66d908a9
b66be2f7c046205b01453951c161e6cc
46b318bbb72ee68c9d9183d78e79fb5a
d790997dd950bb39229dc5bd3c2047ff
a2b1a45a242cee03fab0bedb2e460587

jj. Duuzer

Duuzer is a backdoor Trojan. After installing Duuzer, cybercriminals have the following capabilities:

- Gathering information about the system and disks
- Create, number and end processes
- Access, download, modify and delete files
- Change temporary file attributes
- Execute commands.

Platform: N/A

Threat level: N/A

Category: Backdoor

Indicators of Compromise (IOCs)

MD5:

1205c4bd5d02782cc4e66dfa3fef749c
92d618db54690c6ae193f07a31d92098
3e6be312a28b2633c8849d3e95e487b5
41a6d7c944bd84329bd31bb07f83150a
7343f81a0e42ebf283415da7b3da253f
73471f41319468ab207b8d5b33b0b4be
84a3f8941bb4bf15ba28090f8bc0faec
b04fabf3a7a710aafe5bc2d899c0fc2b
e04792e8e0959e66499bfacb2a76802b
3a963e1de08c9920c1dfe923bd4594ff
51b3e2c7a8ad29f296365972c8452621

5f05a8f1e545457dbd42fe1329f79452
91e5a64826f75f74a5ae123abdf7cef5
9749a4b538022e2602945523192964ad
9ca7ec51a98c2b16fd7d9a985877a4ba
bb6cbebd4ffd642d437afc605c32eca0
fb4caaaf1ac1df378d05111d810a833e
4b2d221deb0c8042780376cb565532f8
cd7a72be9c16c2ece1140bc461d6226d
f032712aa20da98a1bbad7ae5d998767
f940a21971820a2fcf8433c28be1e967
71cdcc903f94f56c758121d0b442690f
0f844300318446a70c022f9487475490

kk. Destover

Destover is a trojan that has dropper, backdoor and wiper functions. Destover's destructive payload is produced using igfxtrayex.exe.

- Delete all files on stationary and remote drives
- Change the partition table
- Install additional modules
- Connect to multiple IP addresses on ports 8080 and 8000.

Platform: N/A

Threat level: N/A

Category: Backdoor

Indicators of Compromise (IOCs)

CnC:

124[.]47[.]73[.]194
165[.]138[.]120[.]35
187[.]176[.]34[.]40
203[.]131[.]222[.]102
177[.]19[.]132[.]216
185[.]30[.]198[.]1
202[.]39[.]254[.]231
203[.]113[.]122[.]163
140[.]134[.]23[.]140
203[.]131[.]210[.]247
114[.]143[.]184[.]19
211[.]76[.]87[.]252
59[.]125[.]119[.]135
65[.]117[.]146[.]5
93[.]157[.]14[.]154

62[.]0[.]79[.]45
59[.]90[.]208[.]171
206[.]248[.]59[.]124
87[.]101[.]243[.]252
187[.]111[.]14[.]62
209[.]237[.]95[.]19
71[.]40[.]211[.]3
85[.]112[.]29[.]106
201[.]25[.]189[.]114
208[.]87[.]77[.]153
201[.]216[.]206[.]49
69[.]54[.]32[.]30
223[.]255[.]129[.]230
37[.]148[.]208[.]67
200[.]87[.]126[.]117
94[.]199[.]145[.]55
185[.]20[.]218[.]28
177[.]52[.]193[.]198
201[.]22[.]95[.]127
1[.]202[.]129[.]201
113[.]10[.]158[.]4
124[.]81[.]92[.]85
196[.]36[.]64[.]50
103[.]233[.]121[.]22
200[.]202[.]169[.]103
202[.]152[.]17[.]116
37[.]34[.]176[.]14
202[.]182[.]50[.]211
208[.]105[.]226[.]235
213[.]42[.]82[.]243
31[.]210[.]53[.]11
59[.]125[.]62[.]35
91[.]183[.]41[.]5
148[.]238[.]251[.]30
175[.]111[.]4[.]4
185[.]81[.]99[.]17
201[.]163[.]208[.]37
203[.]115[.]13[.]105
210[.]211[.]124[.]229
67[.]229[.]173[.]226
91[.]183[.]71[.]18
208[.]69[.]30[.]151
161[.]139[.]39[.]234

31[.]210[.]54[.]14
5[.]22[.]140[.]93
87[.]101[.]243[.]246
90[.]80[.]152[.]49
110[.]77[.]140[.]155
161[.]246[.]14[.]35
186[.]167[.]17[.]115
175[.]45[.]4[.]158
61[.]91[.]100[.]211
62[.]141[.]29[.]175
184[.]20[.]197[.]204
110[.]78[.]165[.]32
202[.]9[.]100[.]206
41[.]21[.]201[.]107
184[.]173[.]254[.]54
101[.]76[.]99[.]183
199[.]83[.]230[.]236
187[.]54[.]39[.]210
37[.]58[.]148[.]34
112[.]206[.]230[.]54
177[.]189[.]204[.]214
203[.]170[.]66[.]206
41[.]76[.]46[.]182
78[.]38[.]114[.]213
203[.]132[.]205[.]250
113[.]160[.]112[.]125
177[.]0[.]154[.]88
194[.]165[.]149[.]51
196[.]202[.]33[.]106
88[.]53[.]215[.]64
217[.]96[.]33[.]164

MD5:

d1c27ee7ce18675974edf42d4eea25c6
760c35a80d758f032d02cf4db12d3e55
e1864a55d5ccb76af4bf7a0ae16279ba
b80aa583591eaf758fd95ab4ea7afe39
2618dd3e5c59ca851f03df12c0cab3b8

SHA-256:

201a9c5fe6a8ae0d1c4312d07ef2066e5991b1462b68f102154bb9cb25bf59f9
f6cb8343444771c3d03cc90e3ac5f76ff9a4cb9cd41e65c3b7f52b38b20c0c27
0753f8a7ae38fdb830484d0d737f975884499b9335e70b7d22b7d4ab149c01b5
4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9

e0066ddc9e6f62e687994a05027e3eaa02f6f3ad6d71d16986b757413f2fb71c
9ec83d39d160bf3ea4d829fa8d771d37b4f20bec3a68452dfc9283d72cee24f8
10d3ab45077f01675a814b189d0ac8a157be5d9f1805caa2c707eecbb2cbf9ac
33207f4969529ad367909e72e0f9d0a63c4d1db412e41b05a93a7184ec212af1
389ee412499fd90ef136e84d5b34ce516bda9295fa418019921356f35eb2d037
e0ce1f4b9ca61747467cee56307f9ea15dd6935f399837806f775e9b4f40e9ca
54ab7e41e64eb769b02b855504c656eaaff08b3f46d241cb369346504a372b4f
47830371f6f3d90d6a9fbe39e7f8d43a2e126090457448d0542fcbec4982afd6
83e507104ead804855d07bc836af4990542d1eac5ac2a8ce86f985d082199f6f
d94ceade521452864ae8daae9d6b202a79d4761f755c7c769ec4e103c7c3127d
bebf6266e765f7a0eefcde7c51507cc9f6e3b5d5b82a001660454e4e84f6e032
4166f6637b3b11f69cccbeb775f9ee6987a5a30475c54db189b837ee3fbbf0d1
eeb146ebbc3f144f5a6156d07322a696eead9c4895a9a6f94212d24056acd41c
6959af7786a58dd1f06d5463d5ba472396214d9005fce8559d534533712a9121
68006e20a2f37609ffd0b244af30397e18df07483001150bcc685a9861e43d44
d8fedef123b3d386f0917f11db9fae0956ffe5b16a9aaad8805f72309437d066
2368ee0e0001599b7789d8199c7b19f362a87925118ae054309d85f960d982ec
6e3db4da27f12eaba005217eba7cd9133bc258c97fe44605d12e20a556775009
98abfcc9a0213156933ccd9cb0b85dc51f50e498dbfdec62f6a66dc0660d4d92
d36f79df9a289d01cbb89852b2612fd22273d65b3579410df8b5259b49808a39
696ff9dda1ce759e8ff6dd96b04c75d232e10fe03809ba8abac7317f477f7cf5
7501c95647cef0c56e20c6d6a55de3d23f428e8878a05a603a0b37ea987a74e2
3c3d2ab255daa9482fd64f89c06cdbfff3b2931e5e8e66004f93509b72cf1cc7
7d9631a62ae275c58e7ad2a3e5e4c4eac22cff46c077410ad628be6c38dd5e08
ca4b4a3011947735a614a3dc43b67000d3a8deefb3fffa95b48f1d13032f2aea
31a76629115688e2675188d6f671beacfe930794d41cf73438426cc3e01cebae
7cea18dce8eb565264cc37bfa4dea03e87660b5cea725e36b472bafdcfe05ab1
757cd920d844fdcb04582a89b55f62b9a3e9bf73804abf94c9a9e15d06030b93
8a4f000049ad2a6c4eeac823c087b1c6e68c58b241c70341821cceccdf0f2d17
0654d112c17793c7a0026688cee569e780b989a9eb509585a977efd326dc2873
453d8bd3e2069bc50703eb4c5d278aad02304d4dc5d804ad2ec00b2343feb7a4
1f689996439db60970f4185f9cfc09f59bfe92650ba09bda38c7b1074c3e497b
029f93b7b7012777ee9fb2878d9c03b7fc68afad0b52cdc89b28a7ea501a0365
5831e614d79f3259fd48cfd5cd3c7e8e2c00491107d2c7d327970945afcb577d
6b70aa88c3610528730e5fb877415bc06a16f15373c131284d5649214cd2e96b
9b4c90ca8906e9fea63c9ea7a725db5fc66e1ca6c2a20bec2e8c1749b0000af5
b0cfaab0140f3ea9802dc6ed25bf208a2720fb590733966b7a3e9264a93a4e66
b3c0b7e355bee34cdb73d0bbdb1ba1b61797c035db31f0c82b19f9aa6a7abcc7
36844e66e5f4d802595909e2cbe90a96ad27da6b254af143b6611ab9ee85a13e
4efeea9eeae3d668897206eeccb1444d542ea537ca5c2787f13dd5dadd0e6aaa
5b28c86d7e581e52328942b35ece0d0875585fbb4e29378666d1af5be7f56b46
66df7660ddae300b1fcf1098b698868dd6f52db5fcf679fc37a396d28613e66b
72008e5f6aab8d58e4c8041cde20ee8a4d208c81e2b3770dbae247b86eb98afe
822a7be0e520bb490386ad456db01f26c0f69711b4ac61ba2cb892d5780fe38f
899ff9489dde2c5f49d6835625353bfe5ea8ca3195ca01362987a9d4bdac162d
8b50d7d93565aab87c21e42af04230a63cd076d19f8b83b063ef0f61d510adc7
90d8643e7e52f095ed59ed739167421e45958984c4c9186c4a025e2fd2be668b

ac27cfa2f2a0d3d66fea709d7ebb54a3a85bf5134d1b20c49e07a21b6df6255a
c5be570095471bef850282c5aaf9772f5baa23c633fe8612df41f6d1ebe4b565
ce0e43c2b9cb130cd36f1bc5897db2960d310c6e3382e81abfa9a3f2e3b781d7
facb32efc05bc8c4f3cb3baa6824db0f7effc56c02dbc52c33bafe242a1def77
763d1cb589146dd44e082060053ffbf5040830c79be004f848a9593d6be124ac
02d1d4e7acd9d3ec22588d89aed31c9a9d55547ef74fa3749659b610893f5405
47181c973a8a69740b710a420ea8f6bf82ce8a613134a8b080b64ce26bb5db93
e187811826b2c33b8b06bd2392be94a49d068da7f703ae060ee4faffde22c2fe
2811fdceb8a8aa03bbf59c0b01a43bd1f2aee675a8f20d38194258046987e5fa
39e53ba6984782a06188dc5797571897f336a58b8d36020e380aa6cd8f1c40a2
530a0f370f6f3b78c853d1e1a6e7105f6a0f814746d8a165c4c694a40c7ad09a
7a2a740d60bd082c1b50ab915ef86cc689ba3a25c35ac12b24e21aa118593959
eaea45f8bfb3d8ea39833d9dcdb77222365e601264575e66546910efe97cba99
ee49322ed9fb43a9a743b54cc6f0da22da1d6bc58e87be07fd2efe5e26c3ef8a
ef07d6a3eb4a0047248c845be3da3282c208ede9508a48dbb8128eacc0550edf
477ca3e7353938f75032d04e232eb2c298f06f95328bca1a34fce1d8c9d12023
5a69bce8196b048f8b98f48c8f4950c8b059c43577e35d4af5f26c624140377c
89b25f9a454240a3f52de9bf6f9a829d2b4af04a7d9e9f4136f920f7e372909b
a01bd92c02c9ef7c4785d8bf61ecff734e990b255bba8e22d4513f35f370fd14
b93793e3f9e0919641df0759d64d760aa3fdea9c7f6d15c47b13ecd87d48e6a9
d589043a6f460855445e35154c5a0ff9dbc8ee9e159ae880e38ca00ea2b9a94f
92cc25e9a87765586e05a8246f7edb43df1695d2350ed921df403bdec12ad889
f2a14c5ef6669d1eb08fababb47a4b13f68ec8847511d4c90cdca507b42a5cf3
520778a12e34808bd5cf7b3bdf7ce491781654b240d315a3a4d7eff50341fb18
e55fff05de6f2d5d714d4c0fa90e37ef59a5ec4d90fdf2d24d1cb55e8509b065
e506987c5936380e7fe0eb1625efe48b431b942f61f5d8cf59655dc6a9afc212
2477f5e6620461b9146b32a9b49def593755ac9788fc4beeee81bf248aa2e92a
f69747d654acc33299324e1da7d58a0c8a4bd2de464ec817ad201452a9fa4b54
44884565800eebf41185861133710b4a42a99d80b6a74436bf788c0e210b9f50
2f629c3c65c286c7f55929e3d0148722c768c730a7d172802afe4496c0abd683
b5e1740312b734fb70a011b6fe52c5504c526a4cccb55e154177abe21b1441c9
0e162a2f07454d65eaed0c69e6c91dd10d29bdb27e0b3b181211057661683812
a53e33c77ecb6c650ee022a1311e7d642d902d07dd519758f899476dbaae3e49
c95eaedaafd8041bb0fea414b4ebc0f893f54cdec0f52978be13f7835737de2a
da255866246689572474d13d3408c954b17d4cc969c45d6f45827799e97ed116
8465138c0638244adc514b2722fcb60b2a26a8756aa7d97f150e9bdc77e337cc
77a32726af6205d27999b9a564dd7b020dc0a8f697a81a8f597b971140e28976
794b5e8e98e3f0c436515d37212621486f23b57a2c945c189594c5bf88821228
c248da81ba83d9e6947c4bff3921b1830abda35fed3847effe6387deb5b8ddbb
fba0b8bdc1be44d100ac31b864830fcc9d056f1f5ab5486384e09bd088256dd0
c3f5e30b10733c2dfab2fd143ca55344345cc25e42fbb27e2c582ba086fe3326

II. Koredos

Trojan.Koredos / DDoS-KSig / DeltaAlfa Trojan.Koredos is a Trojan horse that attempts to carry out DDoS attacks and encrypts data files found on the infected computer.

Platform: N/A

Threat level: N/A

Category: DDoS

Other Name: Trojan.Koredos, DDoS-KSig, DeltaAlfa

Indicators of Compromise (IOCs)

SHA256:

a256459a3efa052aa924775d79a9ca28d0e304a45819ab49fef56cca9bf83d16
f09dae150921aa57673a0f1737f9c384399dcf1987eb735cef0111ea1ba3c895
57477b0ca0214ab4c73030aa652dd26131315e0350bfa5d7738236357a0fc93a

mm. KorDllBot

It is a family of small/medium size trojans that usually are configured to be installed as services.

Platform: N/A

Threat level: N/A

Category: Backdoor

Other Name: Redobot

General information

KorDllbot is a family of small/medium size trojans that usually are configured to be installed as services. Samples can vary a great deal in functionality - from just listening on a port and accepting commands, to harvesting data, to actively spreading over SMB. This functionality seems almost modular, using different encryption and encoding methods and different C&C command words.

Common capability seen in the KorDllbot family is:

- Get bot status
- List logical drives
- List directory
- Change directory
- Get process list
- Kill process
- Execute file
- Delete file
- Change file time
- Execute shell command
- Download file
- Upload file
- Get volume serial number

- Get file attributes

Indicators of Compromise (IOCs)

SHA-256:

2d9edf45988614f002b71899740d724008e9a808efad00fa79760b31e0a08073
6e8a2329567cdbbba68460ccb97209867d7508983cb638662b33bfe90d0134d4
e0cd4eb8108dab716f3c2e94e6c0079051bfe9c7c2ed4fcbfdd16b4dd1c18d4d
9d9889585f1a4048a3955d3a9cead2f426a509afaeacad27540382cc3266f0fa
9bc8fe605a4ad852894801271efd771da688d707b9fbe208106917a0796bbfdc
0a27acaaebc7db0878239b40ab9d2feff13888839c05a03348fc09b78de6ced5
f98c67c4cf9b02acaabb555664a0d9d648a1e43f681f9bf234af066d5451be8d
1226d3635c1a216be9316c9dfa97f103c79ed4c44397e5e675d3b1e37786bf31
e97a8909349a072ed945899fbe276fc27e9c5847bc578b0abccf017da3fd680c
82169a2d8f15680c93e1436687538afa01d6a2ecfe7a7cb613817c64a1a82342
162d6223c1c1219ca81a77e60e6b776058517272fe7cac828a3f64dcacd87811
c16a66c1d8e681e962f03728411230fe7c618b7294c143422005785d3a724ec4
87e68055959328d857b287e797896d9a96695b69ed300a843eee73319427b3b3
7b171a160cb2a17f87ca6a4a1c62b4cd9e718f987b7278d3effe0614b5b51be4
dda136bc51670e57a4b2f091f83ab7b44291a9323d5483abd9e91b78221e027f
69300a42e055f68a8057192077fbbef3be5b66514ea9ca258b077c5c7e9417a9
96c35225dc4cac65cc43a6cc6cdcce3d13b3bda286c8c65cad5f2879f696ad2a
29355f6d4341089b36834b4a941ef96b3bf758a4fe35fbb401cc4e74b9b1c90f
82fe3a8f2248643505e8de1977b734f97eb38225e6d3df6ea8f906430514b4f5
3acaea01fd79484d5a72c72e1b9c2fbf391145fb1533c17a8a83e897d8777f82
6059cb08489170aea77caf0940131e5765b153a593e76d93a0f244e89ddb9e90
c4852ddba88e5c53a8711c4c7540b7ac98dac6b9e31d10dd999a81a4f0e117c3
888844c040be9d0fc3dab00dd004aa9e8619f939aff2eba21e4f48ca20e13784
d7044a35e76543a03cd343d71652c7bbd9a28e246d7f3a43f4a2e75cd0ef7366
c5baece9978649659220af2681a3a43b83f8ae47afdd3862185d1fec7735a7d2
218ee208323dc38ebc7f63dba73fac5541b53d7ce1858131fa3bfd434003091d
7a538c3eed1f01b62a19226750c1369e4e9210b1331d5829ca91fe2b69087f06
57b4c2e71f46fe3e7811a80d19200700c15dd358bdf9d9fdf61f1c9a669f7b4b
006e0cc29697db70b2d4319f320aa0e52f78bf876646f687aa313e8ba04e6992
f4a06dd6ebfd0805d445f45ce33d7bba4a33c561111c39a347024069a78169e9
cd8c729da299b29618819afeef8b2a79451e6c3d35dea3769ef638c649c69001
6d5d706f5356e087f5961ba2ed808c51876d15c2e09eb081618767b36b1d012f
50974c15a546e961fbee8653e5725960a77b79e0f7c8eadf3b6d35ba3a46dd57
bfb5fa2a09ac60efcc0e9f05e781bd22cae0b8f6ba356d7819285f073845a0eb
56e0b1794a588e330e32a10813cdc9904e472c55f17dd6c8de341aeaf837d077
ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781
87bae4517ff40d9a8800ba4d2fa8d2f9df3c2e224e97c4b3c162688f2b0d832e
fd95e095658314c9815df6a97558897cb344255bd54d03c965fa4cbd16d7bafd
a4b982d4e7137d7d3687f3127e6d5c2a8b2be1f53daeebce9175461c7e6a53cd

81067f057d523fdcddf7df1da39a7c3614c45f6bff6bd387274c049244efda3b
9e226a5eb4de19fcb3f7ecc3abcf52ea22a1f1a42a08dd104f5f7a00164e074e
08203b4ddc9571418b2631ebbc50bea57a00eadf4d4c28bd882ee8e831577a19
8e3c3398353931c513c32330c07f65b6ee6f62fc7a56edac7cbe4edb1bf4c74e
bb4204dd059849848e9492523ce32520bf37cb80974320c0ca71f3b79e83f462
2f8c448bb05ed1218e638c61bb56ebb953b962ed5e065b08fa03cfcf6f6a1c68
73edc54abb3d6b8df6bd1e4a77c373314cbe99a660c8c6eea770673063f55503
3ebb3d8292a1aa5dc81b028beeefdec0f0448516d6225b336ee37d550ab8c3ab
792b484ac94f0baefc7e016895373ba92c2927e3463f62adb701ddbe4c90604c
163571bd56001963c4dcb0650bb17fa23ba23a5237c21f2401f4e894dfe4f50d
3d2a7ea04d2247b49e2dcad63a179ae6a47237eddbfd354082f1417a63e9696e
af7b53ce584b83085488e1190e1458948eaf767631f766e446354d0d5523e9d0
041605e498bb41b07d2d43003152cc2a992e7e2ade7a47ee9aef2570bdb16d94
9bcecd6afa54eb4f343b7eb82a86ceee189cc10bc91fa83f8cdc98cc5aaef117
b7f2595dd62d1174ce6e5ddf43bf2b42f7001c7a4ec3c4cbe3359e30c674ed83
b039383a19e3da74a5a631dfe4e505020a5c5799578187e4ccc016c22872b246
94e14a85a2046b40842f6c898c5f6c3200de3d89c178a9a9f9a639c1d3de9ee9

nn. DYEPACK

DYEPACK is a tool, which is used to work with SWIFT, consists of SWIFT Alliance software Hook Files and SWIFT transactions Information Harvester. It allows attackers to initiate transactions, steal money, and hide any evidence of the fraudulent transactions from the victimized bank.

Indicators of Compromise (IOCs)

Yara Rules

```
rule win_dyepack_auto {

   meta:
      author = "Felix Bilstein - yara-signator at cocacoding dot com"
      date = "2021-10-07"
      version = "1"
      description = "Detects win.dyepack."
      info = "autogenerated rule brought to you by yara-signator"
      tool = "yara-signator v0.6.0"
      signator_config = "callsandjumps;datarefs;binvalue"
      malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.dyepack"
      malpedia_rule_date = "20211007"
      malpedia_hash = "e5b790e0f888f252d49063a1251ca60ec2832535"
      malpedia_version = "20211008"
      malpedia_license = "CC BY-SA 4.0"
      malpedia_sharing = "TLP:WHITE"

   /* DISCLAIMER
    * The strings used in this rule have been automatically selected from the
    * disassembly of memory dumps and unpacked files, using YARA-Signator.
```

```
    * The code and documentation is published here:
    * https://github.com/fxb-cocacoding/yara-signator
    * As Malpedia is used as data source, please note that for a given
    * number of families, only single samples are documented.
    * This likely impacts the degree of generalization these rules will offer.
    * Take the described generation method also into consideration when you
    * apply the rules in your use cases and assign them confidence levels.
    */

    strings:
        $sequence_0 = { 8d542418 53 52 8d44242c 51 }
            // n = 5, score = 300
            //   8d542418           | lea             edx, dword ptr [esp + 0x18]
            //   53                 | push            ebx
            //   52                 | push            edx
            //   8d44242c           | lea             eax, dword ptr [esp + 0x2c]
            //   51                 | push            ecx

        $sequence_1 = { 56 ff15???????? 85c0 741e 8b442418 3bc3 }
            // n = 6, score = 300
            //   56                 | push            esi
            //   ff15????????       |
            //   85c0               | test            eax, eax
            //   741e               | je              0x20
            //   8b442418           | mov             eax, dword ptr [esp + 0x18]
            //   3bc3               | cmp             eax, ebx

        $sequence_2 = { 8b4c2410 33ed 33ff 3bc3 7c60 }
            // n = 5, score = 300
            //   8b4c2410           | mov             ecx, dword ptr [esp + 0x10]
            //   33ed               | xor             ebp, ebp
            //   33ff               | xor             edi, edi
            //   3bc3               | cmp             eax, ebx
            //   7c60               | jl              0x62

        $sequence_3 = { 3be9 72ac 56 ff15???????? 56 ff15???????? 8b8c2428100000 }
            // n = 7, score = 300
            //   3be9               | cmp             ebp, ecx
            //   72ac               | jb              0xffffffae
            //   56                 | push            esi
            //   ff15????????       |
            //   56                 | push            esi
            //   ff15????????       |
            //   8b8c2428100000     | mov             ecx, dword ptr [esp + 0x1028]

        $sequence_4 = { 81f900100000 760b b900100000 895c2420 eb04 89442420 }
            // n = 6, score = 300
            //   81f900100000       | cmp             ecx, 0x1000
            //   760b               | jbe             0xd
            //   b900100000         | mov             ecx, 0x1000
            //   895c2420           | mov             dword ptr [esp + 0x20], ebx
```

```
        // eb04             | jmp             6
        // 89442420         | mov             dword ptr [esp + 0x20], eax

    $sequence_5 = { ff15???????? 8d442410 895c2410 50 56 }
        // n = 5, score = 300
        // ff15????????     |
        // 8d442410         | lea             eax, dword ptr [esp + 0x10]
        // 895c2410         | mov             dword ptr [esp + 0x10], ebx
        // 50               | push            eax
        // 56               | push            esi

    $sequence_6 = { eb04 89442420 8d542418 53 52 8d44242c 51 }
        // n = 7, score = 300
        // eb04             | jmp             6
        // 89442420         | mov             dword ptr [esp + 0x20], eax
        // 8d542418         | lea             edx, dword ptr [esp + 0x18]
        // 53               | push            ebx
        // 52               | push            edx
        // 8d44242c         | lea             eax, dword ptr [esp + 0x2c]
        // 51               | push            ecx

    $sequence_7 = { ff15???????? 8b8c2428100000 53 51 e8???????? 83c408 }
        // n = 6, score = 300
        // ff15????????     |
        // 8b8c2428100000   | mov             ecx, dword ptr [esp + 0x1028]
        // 53               | push            ebx
        // 51               | push            ecx
        // e8????????       |
        // 83c408           | add             esp, 8

    $sequence_8 = { ffd7 8d4c2418 53 51 8d54242c }
        // n = 5, score = 300
        // ffd7             | call            edi
        // 8d4c2418         | lea             ecx, dword ptr [esp + 0x18]
        // 53               | push            ebx
        // 51               | push            ecx
        // 8d54242c         | lea             edx, dword ptr [esp + 0x2c]

    $sequence_9 = { 55 6a02 53 6aff 56 ffd7 8d4c2418 }
        // n = 7, score = 300
        // 55               | push            ebp
        // 6a02             | push            2
        // 53               | push            ebx
        // 6aff             | push            -1
        // 56               | push            esi
        // ffd7             | call            edi
        // 8d4c2418         | lea             ecx, dword ptr [esp + 0x18]

    condition:
        7 of them and filesize < 212992
}
```

Reference URL:

https://malpedia.caad.fkie.fraunhofer.de/details/win.dyepack

Related malware analysis video URL:

https://media.ccc.de/v/froscon2021-2670-der_cyber-bankraub_von_bangladesch

oo. Client_RAT

The Client_RAT program provides full control over the target system: it allows you to analyze the system, download and execute files, transfer data from the infected computer to the C&C server. Communications with the C&C server are performed over an encrypted SSL channel. For this purpose, Client_RAT uses statically linked libcurl libraries, version 7.47.1 (FEB 2016).

Threat level: High

Category: remote-access-trojan

Indicators of Compromise (IOCs)

MD5:

9216b29114fb6713ef228370cbfe4045
8e32fccd70cec634d13795bcb1da85ff

SHA256:

6c1d8c4afbc7f85f05fb2e4d17e5553255b0195a0b56ba5309e362e2156debfc

pp. Server_RAT

The Client_RAT program provides full control over the target system: it allows you to analyze the system, download and execute files, transfer data from the infected computer to the C&C server. Communications with the C&C server are performed over an encrypted SSL channel. For this purpose, Client_RAT uses statically linked libcurl libraries, version 7.47.1 (FEB 2016).

Category: remote-access-trojan

Indicators of Compromise (IOCs)

MD5:

570e6ea21cdce694a4a74876ca87534a
e4fb05a8c2da92ec5b19bdb59814464a
f38f6d976e6d66abc86f9992e808670a

qq. Server_TrafficForwarder

Server_TrafficForwarder redirects traffic from one external server to another. The file is a resident application that, once launched, waits for incoming connections on a specific port to provide further control of the PC to the attacker. Server_TrafficForwarder uses the wolfSSL staticly linked library to implement asymmetric encryption of traffic between the client and the server.

Threat level: High

Category: Backdoor

Indicators of Compromise (IOCs)

CnC:

104[.]168[.]202[.]24
186[.]177[.]30[.]152
192[.]119[.]81[.]132
103[.]48[.]194[.]106
103[.]248[.]72[.]78
142[.]11[.]229[.]152
182[.]176[.]147[.]86
103[.]5[.]124[.]222
205[.]252[.]217[.]18
70[.]164[.]255[.]184
8[.]9[.]30[.]59
83[.]101[.]154[.]203
185[.]227[.]109[.]38
113[.]161[.]212[.]29
187[.]248[.]42[.]21
86[.]98[.]75[.]98
200[.]38[.]60[.]135
220[.]163[.]251[.]43
209[.]208[.]109[.]38
82[.]65[.]132[.]156
185[.]144[.]83[.]73
46[.]21[.]147[.]26
104[.]168[.]211[.]86
186[.]74[.]136[.]91
202[.]182[.]102[.]14
83[.]101[.]154[.]197
104[.]168[.]218[.]6
23[.]30[.]140[.]235
176[.]9[.]157[.]50
46[.]44[.]248[.]134

MD5:

d032aeb54cf1229e011c070ecd64c33e

SHA256:

dd45954237cad570b93bcf1a55dac4600e5ee6f5cb830b0279933a4de489df88
11ca273353d44a6c81747f0cd54c4a84ff020aa2a6f3d4b45436660a1d673ff1

rr. Client_TrafficForwarder

Client_TrafficForwarder - Forwards operator's commands from external network into corporate network. This module was installed on one of the PCs in the internal network of the attacked organization. It proxies traffic from C&C server to PCs in the local network of the attacked organization.

Threat level: High

Category: Backdoor

Indicators of Compromise (IOCs)

SHA256:

70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38
9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852

ss. WannaCry

WannaCry, originally named as WanaCrypt, having aliases of Wana Crypt0r and Wana Decrypt0r, is a ransomware wormon Microsoft Windows (can be run on Linux via WINE) that uses two NSA-leaked tools that has wreaked havoc in airports, banks, universities, hospitals and many other facilities. It has spread to some 150 countries worldwide

Threat level: High

Platfrom: Windows

Category: Ransomware

Indicators of Compromise (IOCs)

CnC:

57g7spgrzlojinas[.]onion
cwwnhwhlz52maqm7[.]onion
Xxlvbrloxvriy2c5[.]onion
iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
gx7ekbenv2riucmf[.]onion
sqjolphimrr7jqw6[.]onion
5[.]199[.]142[.]236

87[.]101[.]243[.]252
104[.]41[.]151[.]54
212[.]51[.]134[.]123
149[.]202[.]160[.]69
128[.]31[.]0[.]39
154[.]35[.]175[.]225
194[.]109[.]206[.]212
204[.]11[.]50[.]131
146[.]0[.]32[.]144
50[.]7[.]161[.]218
217[.]79[.]190[.]25
131[.]188[.]40[.]189
5[.]9[.]159[.]14
104[.]17[.]37[.]137"
2[.]3[.]69[.]209
178[.]16[.]208[.]57
171[.]25[.]193[.]9
197[.]231[.]221[.]221
184[.]74[.]243[.]67
203[.]69[.]210[.]247
85[.]248[.]227[.]164
199[.]254[.]238[.]52
163[.]172[.]35[.]247
95[.]183[.]48[.]12
195[.]154[.]164[.]243
46[.]101[.]166[.]19
91[.]121[.]65[.]179

SHA256:

92b0f4517fb22535d262a7f17d19f7c21820a011bfe1f72a2ec9fbffbdc7e3e0
77a250e81fdaf9a075b1244a9434c30bf449012c9b647b265fa81a7b0db2513f
51432d3196d9b78bdc9867a77d601caffd4adaa66dcac944a5ba0b3112bbea3b
f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
96ac1e4330e092a05bc8bada12dd6f442d5afb2d5e75271a90dcaf697e662fca
f01b7f52e3cb64f01ddc248eb6ae871775ef7cb4297eba5d230d0345af9a5077
58be53d5012b3f45c1ca6f4897bece4773efbe1ccbf0be460061c183ee14ca19
2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
c916b96aaa85bf2e6e985f38e2a2e78f80ad94c573838cdbe4aabc8d0b429115
1a7123fbb6f27b920acde8571945c2e11297e91b7168afad58e9ee06232a40ef
043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2
ca8dc152dc93ec526e505cf2a173a635562ffbf55507e3980f7dc6d508f0f258
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
5cd126b4f8c77bdf0c5c980761a9c84411586951122131f13b0640db83f792d8
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2
35f05cb83c79ee76b126d6b0bdffffc4b6f1a7067621699fcdfa7110db47cd5b
6c77e67da7e0ad457e104eb15ad1e3cfe0243fb9458abaaa36ad62907c2f13e8
4a25d98c121bb3bd5b54e0b6a5348f7b09966bffeec30776e5a731813f05d49e
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
aa958261eca99fa5389087bdb41ab20cba658bde504ca99726e43f7a4a2830a3
68c779f97a570513eb2c6ef04a0d3852d5077b2c226b77891686efb82efaace8

tt. EternalBlue

EternalBlue is an exploit that uses a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. It is developed by the U.S. National Security Agency (NSA) according to testimony by former NSA employees. It was leaked by the Shadow Brokers hacker group on April 14, 2017, one month after Microsoft released patches for the vulnerability. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.

Threat level: High

Platfrom: Windows

Category: Exploit

Indicators of Compromise (IOCs)

SHA256:

42d57d7f0f65e78f3e4e5fb63828703d083395500c3b0aa0c603c221782c7af0

uu. RatankbaPOS

Malicious software for stealing bank card data from PoS terminals (point-of-sale). It can target an encrypted form of track data. From the confirmed data - RatankbaPOS is focused on a software application, framework or device associated with "SoftCamp POS".

Category: Trojan

Indicators of Compromise (IOCs)

CnC:

http://www[.]energydonate[.]com/images/character[.]gif
www[.]energydonate[.]com
81[.]95[.]5[.]179
http://www[.]webkingston[.]com/top[.]gif

www[.]webkingston[.]com
89[.]33[.]246[.]102
http://www[.]webkingston[.]com/update[.]jsp?action=need_update
www[.]webkingston[.]com
http://www[.]energydonate[.]com/files/download/bithumb[.]zip
http://www[.]energydonate[.]com/files/download/bithumb[.]pdf
www[.]energydonate[.]com
http://online-help[.]serveftp[.]com/list[.]jsp?action=up
online-help[.]serveftp[.]com

SHA256:

42d57d7f0f65e78f3e4e5fb63828703d083395500c3b0aa0c603c221782c7af0
2b05a692518a6102c540e209cb4eb1391b28944fdb270aef7ea47e1ddeff5ae2
d334c40b42d2e6286f0553ae9e6e73e7e7aaec04a85df070b790738d66fd14fb
b66624ab8591c2b10730b7138cbf44703abec62bfc7774d626191468869bf21c
79a4b6329e35e23c3974960b2cecc68ee30ce803619158ef3fefcec5d4671c98

vv. Mydoom

Mydoom is a computer worm affecting Microsoft Windows and Windows NT. It was first sighted on January 26, 2004. Mydoom sread primarily via e-mail and through the file-sharing network Kazaa. The worm's media file is about 29 kilobytes in size and contains the text string "sync-1.01; andy; I'm just doing my job, nothing personal, sorry." When infecting a computer, Mydoom modifies the operating system by blocking access to the websites of many antivirus companies, news feeds and various sections of the Microsoft website, blocks almost all antivirus activities and downloads additional virus programs from the network.

Threat Level: Low

Platform: Windows

Category: Trojan

Indicators of Compromise (IOCs)

SHA256:

a263ab215d67350bc4a05c88accecfd5414ebe375c34a50f808f949dbf47d146
57b76adc01c5712971c1d2d13c4bdc0527f6f4396131f3b362d3b329dcda3c86
685f3b0222fd7f4459a7a8f7e6591dbb6e158d4910de739abc3417856861bbd9
101fd3c73b1470f26d7d0c869c96187baade91bb20ab1c85f0e5ef8535d48028
ebfe51f8ec057e6c6c681a9a4781cf76ca81496ba849ed1c22cabc41cdb23d8b
e6e82910f9e78cdf0179338f5eaddcd8ca0419820261680a3ecf99a78d75645e
7b02f15dd2027abf3fda4fad30de74c4cc0229ae0edcea14029987796625b128
62d56a0c9d90b04b04c872c244c925700815357cebf2aedeed8aaa62e9835518
174a783e5eda640ed895e8fe7e955a35b291669b6b15e6c00bdc4f0e6f29a825
51b00941b52a07ef36fc5e02c27fa5c4409eeebc057c77d85c036dc66cc5357d

cae7f30dfa33b2be8e701440c32baf5f09eb9eb48133c7ccba3ea9c036dcb0f7
61c76a5b2d5cb64d15129ccaa8e6d1eb1a3fff70f355a1dc345b4c3adf47a1d0
8d4e971b1e8006cc692f435cb96d250d921ce3281946fa398e5a331c8135fd40
8439c80486f8dc7904f0bca895abbe982d192762f257cd6ca9b08ea95475d99e
38deb039a4e241d776c827775c05a04df748c7d61af12fff2b190d6a256f915d
a11730284b54e9cca469937c9e3a44bc4d44d50bc874b465936a13bc5840ed21
2eef31f51097013e3e4d0a5106bb4994acbf98f702f3523976beac7e1385c558
6e9ff7030954e6b1f07958fff37f3acfab011343d2f699ddfee03197f4256e66
3a7ac3c767bdefbf18d87a73ba5fd12d635f3ccb5e0dde1efa7114267fe17fa6
5a8cba64e930e2462ebf1a6a5dfa5ddf5ffe4077e1fefeb72cc40f703ae5815b
1ee9f95e80bf97b81bafebcdec1202c584ae9dd0370a1dc9daa28f705d0d0fd3
eafe61e75111b6ea41ffb4bed94d52d662855078c30fb2f71d37e8e81bcb4eb6
04c652b646cd966ffda5b2f42e39e637c810164f4cfa5d8eee6be697176dac40
051faffea3caee82ca0d9b921f14dca9947ddbdda77eb68b402b44eec89852e3
b33d24b0616e3da7e76d82dc3be03780f77d889952e80b6cc17b799540ce4a0c
5b03e17fe3f4e10186f3cdd199407cad1b2433774aa4809df67d216beee49952
1c51d5cf8ac5a0a0715ba67100597afb49c43643c2513dbc58b1bb512a96b0c9
5474960e814a9af0a3034fbdc8438338e43d59c7ee1d68d19a3cd01218027696
b83403362a379a049467e60834af4bba94dd50d042c947603ca906363fc7ef3a
1bd033d864637781497595dc8cbe0bd793782c9df3f0108a3d90a5f76bbb1b7c
c739492981608953fba2e52f4e52d0876490c32403dbd1fb54c2cd6dbd260f4f
a2cc01f4f3b8061f8ce50ea65f73f98ad8afe166018480b96c3081ba814941aa
1581d461f355a6ff3a756b7d656b1be1f28b4d0d04cef21983a978ed64dc68f0
7845924de55e750a25de391e4ef81268827dcf2c85b25d26fe7088a04f7d5a07
60d3ceae1d00a20c67677627ec15d087f380bbdb2280448486c0d8eedd43eb94
f9013facbdb0956a640e3a9db203e3b8a0ea541acb8a21e2ff0f2b331e47e916
284f4278f91074b319805b34136a5d8b4845b51303892d79f31ca95b3eb7f1ff
f4312e5237156c6395bb6d929561e1ad8738e52f2b9bb3b7f10f502ed2aae98f
2dc3762482c8befeef44b35bcd58c1c2ac5f5925be022ffa72904fb8ed30e57e
b7b421994ef322c083bb76591bcb01b1457a7fd9f2064661d056d53fa2107764
5a775d570b8db4fccb1e32a3e7046908218eb6c2300486a47af2e8c691ae2ad4
207e599a962706c20a044ea47e3e7442d8c4233cc8442317632189c2d4063101
09a5d3bf4131fa23b3384dc5fb4d193228f335c206c19613de47e86acfe8a024
3b7b9a86668c2ac021e64b5beafd6c9c87b5cea2ea8d228a2efdde6743f37dd0
e34401e88b11c6b52536b65a8252631aa0f904fba1a3e81470373ad2d7c8fba3
e12fac13c4cd2cc2f619a3dde8a05edb9b802ed96108daac7eea9b15e1cd37f0
febc4382a5bd6a8cc9f799a572c61a4016489bd5247f5aa5b08bb33010bf7520
3e6231e6c6fbaa75b98d1d4d3f8f592c78fb6302a79855ddca5a824ca95120a5
0b2fb6107a77df4a12deb8e4cc678e1d59cf7e0cd4f50c3793afb4ba76479336
ccd9f6afe4f8fcd616e610115cd5068511f53c1c0f9622bf3d4f481c7278253f
60ddc8bd836bd2c8b94645602a8139df46df5dcc779beaf594cbf768db7620f6
418627fc27f55d94874817ad02ce3600080e6603be2ad028a58e6b7dcb2e7151
0ce8fc3f53ee2513a0fbb958a43cafff1bdd468b754c507f11886b403e44169f

4b73928ddf05aa43d40c0a8325160a6508178284b54be70e5acea7e6f0bb67cc
7e076c42efa21d9078a373ef0052242a16c6ee523242cd6a9e99f923ae3b2723
bce3e83592bd3365904f0edd711721d8ee19b6ea6c901a059fc59bdbc536bd07
972f18a532ee833e868a5eec6f6598548a96b66e86ed2b15de0c6bd3f0d9d95e
375f8c7b65cc064e2a4b250a7685b94ceaea93b9addc801b31429ff437354df9
15d8e36411b8fc03f2b643d98e7ceb602b6019c1bf924dcd56cb26f67ec5e30f
b5b62df0458a90d61212588283c66634bc1e9899bf65308fa0286b36c91c43c7
f43b0fb0a276e13ee5319bc3723a1e4c842f5e8976b81f97b097009ef6312810
2027f6d667606b578a87352a5b71ccc169efdf1bd6d13e6509697605a2fa1a7b
74da9dab37a3e4b47e3341e5ee6526209400b16d089ab84beaf59b49d41aca3f
55f3e0cda8e89ba4045079657b798b5f0cc03e05e870d8fae47729caf2cdd38e
03c0bf5f19ad1ad923eef1b732aa4647f7c464aaf02cf0bf5603eaa88c64d27f
b1f71f677c974c688644c24aa1d82b561b2e670e21e6ee5782fdefbac0dd278d
48e331573bf0423ec07ba56f9df259717719fc7b99d9169996f2137cde95dc04
f603933b6eb456840b02c8e6a51eb38698270ae2d9406012c9ac36845a3a8852
db29b262eebae8f6632501a6770e7625587e7ee1474b1b3166c56e127237ad53
ea2f035ad26e35bcb1569e53ba3d22df10e757d9a61d00169466f1d7d3605776
15d50bcf232bc58c0da3ba683982720e0e7e5fd278ca2546cebffac8b7d2e3f7
27c8390835c7c5fa7437a35fc615a877819717edf90237816b314a355d9cfef9
d6ec2623029d98b800966fa737047a421559d66e550d16e038024303f9ce4a4b
71f343780289370fbbd84fb71165111b7dc5fcca496d8a7a43b5a42e496a2009
a4eb4c59254fdd541bb4eb6298a76d29388b60abcac036e8223b7a51ee7672df
c2bf169dbfd2d91df168d85a99acc99dcde6565f8e81588765e51e90ed94a5a8
bc450d2e1b979a16182c5abce17e2d48a93089f6a172dbc63dc923be310cff89
10da255e4ccf4a5fd21472cd113874d5a60ceda730dc37ee3ed0b5f4a4ac0884
60c83ced44d68aab4de54a799649100bceef8ac4b3958d948fb94933c7aded99
e455363ac22b3812d4b5acf7b0e3e6b514938e7603a724d85552a41f49be98d2
1a37b51440b26371a8da0be3edbe32aebebf2ed28642d3b6e24fc0ab5db1e17f
421ba61e106ee1bf151612b7907f46f5a9d9a8df9b14b21d86b1d9cf5baccf94
2a6f7123e394266264f1dd34e692d27d264d968d52dbdbe2fda91c5831540389
4c8b9ca17ac2bb7dd10bfc67d45b0be99ec794f57a1b243208fdae32755d4ff5
c1d4b540165fc6447cbead223eef5575b07d5b24c749eabc4d74dd657ba76c23
10042317bffa0de85f95fad52586af6584e3578eca844d46f1948884f24de55a
9551662334f772d22af97522905d12f9d976be9535cca556c01abba223bd3bf1
58801744ee6378b952356744ea237f6487d5bfe150716007c8f840f19fc17438
9e4a7d13499f2b382863281bb87b8518413d07183bcb0c8a50f15d5a3a160052
345e23a545fe7c2a354545ba22912baf9a87558049acac992f48562064d677f9

ww. EagleXP

EagleXP is closely related to NSTAR and HTTP Troy based on reused components. EagleXP used this compile path: D:\VMware\eaglexp(Backup)\eaglexp\vmshare\ Work\BsDll-up\Release\BsDll.pdb

Category: Spyware

Indicators of Compromise (IOCs)

Network Signature:

DNS Lookup (byonshop.com) related to Lazarus

alert dns $HOME_NET any -> any any (msg:"DNS Lookup (byonshop.com) related to Lazarus"; flow:from_client; dns_query; content:"byonshop.com"; nocase; pcre:"/(^|\.|\s)byonshop\.com($|\s)/U"; target:src_ip; classtype:apt-trojan; threshold:type limit, track by_src, seconds 60, count 1; sid:1551768; rev:1; metadata:malware_family Lazarus, rule_origin ti_cnc, severity 5, ti_threatactor_id 5e9f20fdcf5876b5772b3d09b432f4080711ac5f, ti_threatactor_name Lazarus, ti_malware_id 2473696fea0df21c871914d7e3866b81225f602e, ti_malware_name EagleXP, ti_malware_id e92e84ab91a20a1789b833bf903c91b7fdaf48af, ti_malware_name NSTAR;)

Domain request in SNI (byonshop.com) related to Lazarus

alert tls $HOME_NET any -> any any (msg:"Domain request in SNI (byonshop.com) related to Lazarus"; flow:established,to_server; tls_sni; content:"byonshop.com"; pcre:"/(^|\.|\s)byonshop\.com($|\s)/U"; target:src_ip; classtype:apt-trojan; threshold:type limit, track by_src, seconds 60, count 1; sid:1551767; rev:1; metadata:malware_family Lazarus, rule_origin ti_cnc, severity 5, ti_threatactor_id 5e9f20fdcf5876b5772b3d09b432f4080711ac5f, ti_threatactor_name Lazarus, ti_malware_id 2473696fea0df21c871914d7e3866b81225f602e, ti_malware_name EagleXP, ti_malware_id e92e84ab91a20a1789b833bf903c91b7fdaf48af, ti_malware_name NSTAR;)

Http request (byonshop.com) related to Lazarus

alert http $HOME_NET any -> any any (msg:"Http request (byonshop.com) related to Lazarus"; flow:established,to_server; content:"byonshop.com"; pcre:"/(^|\.|\s)byonshop\.com($|\s)/W"; http_host; target:src_ip; classtype:apt-trojan; threshold:type limit, track by_src, seconds 60, count 1; sid:1551766; rev:1; metadata:malware_family Lazarus, rule_origin ti_cnc, severity 5, ti_threatactor_id 5e9f20fdcf5876b5772b3d09b432f4080711ac5f, ti_threatactor_name Lazarus, ti_malware_id 2473696fea0df21c871914d7e3866b81225f602e, ti_malware_name EagleXP, ti_malware_id e92e84ab91a20a1789b833bf903c91b7fdaf48af, ti_malware_name NSTAR;)

xx. Jokra

It is a Trojan whose main task is to erase the hard drive of a compromised computer.

Category: wiper

Indicators of Compromise (IOCs)

SHA256:

239ed753232d3cc0e75323d16d359150937934d30da022628e575997c8dd60a2
d7a71f83d576fdf75e7978539bac04ad8b6605207b29379b89c24c0d0f31da61
929dc09a8bd8491b77f050a2736d39c30597ec7090d8f081eeb6179b6f8ab033

422c767682bee719d85298554af5c59cf7e48cf57daaf1c5bdd87c5d1aab40cc

yy. Dozer

Trojan.Dozer acts as a backdoor and connects to IP addresses through specific ports. The Trojan can start an HTTP session using GET or POST, UDP, ICMP, TCP ACK or TCP SYN to perform DDoS attacks.

Category: Backdoor

Indicators of Compromise (IOCs)

IoC:

216[.]199[.]83[.]203
213[.]33[.]116[.]41
213[.]23[.]243[.]210

zz. NSTAR

NSTAR appears to be the first production version of the Troy family. This Trojan is based upon malware created for a military espionage campaign that first emerged in 2009.The malware establishes an internet relay chat (IRC) channel to receive real-time commands in the same manner as the military espionage malware.

Platform: Windows

Category: Spyware

Indicators of Compromise (IOCs)

IoC:

byonshop.com

Advanced Persistent Threat (APT): Silence

Silence APT, a cybercriminal group, known for targeting financial organizations primarily in former Soviet states and neighboring countries is now aggressively targeting banks in more than 30 countries across America, Europe, Africa, and Asia including: Bangladesh.

Silence uses phishing as their infection vector. The threat actor's emails usually contain a picture or a link without a malicious payload and are sent out to a huge recipient database of up to 85,000 users.

Silence has made a number of changes to their toolset with one goal: to complicate detection by security tools. In particular, they changed their encryption alphabets, string encryption, and commands for the bot and the main module. In addition, the actor has completely rewritten TrueBot loader, the first-stage module, on which the success of the group's entire attack depends. The hackers also started using Ivoke, a fileless loader, and EDA agent, both written in PowerShell. Silence has also made a move to including fileless modules in their arsenal, albeit much later than other APT groups, suggesting that the group is still playing catch-up compared to other cybercriminal groups.

Related Tools

EmpireDNSAgent
Radmin
Mimikatz
Nmap

Malware List of Silence APT:

a. Silence Backdoor

Platform: Windows

Threat level: High

Category: Backdoor

Other Name: Silence.MainModule

Indicators of Compromise (IOCs)

CnC:

195[.]123[.]246[.]126
37[.]120[.]145[.]253
185[.]29[.]10[.]13
185[.]236[.]76[.]216
167[.]99[.]43[.]101
185[.]70[.]184[.]32
counterstat[.]pw

counterstat[.]club
185[.]161[.]208[.]9
151[.]248[.]115[.]41
193[.]124[.]18[.]72
185[.]154[.]52[.]83
185[.]154[.]52[.]142
185[.]29[.]9[.]41
zaometallniva[.]ru
1mliked[.]ru
185[.]20[.]187[.]89
http://185[.]161[.]208[.]61/index[.]php?xy=1
http://185[.]29[.]10[.]117/index[.]php

MD5:

363df0b3c8b7b390573d3a9f09953feb
800060b75675493f2df6d9e0f81474fd
E81CD10C838F5A268944AAF50B1BB3B5
0512D025AD198A94E16D03EF31F790EF
ff411742f5e8b970d27bef660349b559
fd133e977471a76de8a22ccb0d9815b2
8b437da524c25d03ab33d7d78d2d6a77
afdfe8c799aa76420622d370416a72be
39537145ce7f01aa8b8c27f9fd40eaa2
7EAF9BBD855C6A124E2EE962BF2DB735
c4f18d40b17e506f42f72b8ff111a614
F1954B7034582DA44D3F6A160F0A9322

b. Silence.ProxyBot

The program is designed to access isolated segments of the network via an intermediate node

Platform: N/A

Threat level: N/A

Category: Bot

Indicators of Compromise (IOCs)

CnC:

91[.]92[.]136[.]193
79[.]141[.]168[.]114
45[.]84[.]0[.]201
185[.]29[.]10[.]13
167[.]99[.]43[.]101
185[.]70[.]184[.]32

counterstat[.]pw
counterstat[.]club
185[.]20[.]187[.]89
84[.]38[.]134[.]103
http://185[.]161[.]208[.]61/run[.]exe
46[.]183[.]221[.]89

MD5:

ce04972114bbd5844aa2f63d83cdd333
3f5372c2776e5cc8aec8a7107f49cf8a
f1f73008183d1b161f25b62a76cd2513
043b383e895a26848bef90abb8da2216
1136c47332daa275d2ecc179a0bf4c0c
BEBB2DE1C051B4E847EE6501D118D522
2fe01a04d6beef14555b2cf9a717615c
b33cd8d369a7167351c69fe57bae0bb1
50565c4b80f41d2e7eb989cd24082aab
88cb1babb591381054001a7a588f7a28

c. APT.Silence.EDA.ps1

Platform: N/A

Threat level: High

Category: remote-access-trojan

General information

This program is intended for remote management of compromised system via DNS protocol and processes following modules: changing the address of the management server, downloading the file from the network, sending a local file to the management server, executing commands in the cmd.exe, collecting system information, rebooting and turning off the system, traffic tunneling.

Indicators of Compromise (IOCs)

CnC:

91[.]92[.]136[.]193
79[.]141[.]168[.]114
45[.]84[.]0[.]201
167[.]99[.]43[.]101
counterstat[.]pw
counterstat[.]club

MD5:

ce04972114bbd5844aa2f63d83cdd333

3f5372c2776e5cc8aec8a7107f49cf8a
f1f73008183d1b161f25b62a76cd2513
043b383e895a26848bef90abb8da2216
1136c47332daa275d2ecc179a0bf4c0c
9812a3436f917af18a7f93a2c71dc846
dcba65555652431c8d3cd773bf873118

d. Truebot (Silence's loader)

Loader for backdoor of Silence group, was first detected end of 2017.

Platform: Windows

Threat level: High

Category: Loader

Other Name: N/A

Indicators of Compromise (IOCs)

CnC:

185[.]70[.]186[.]149
151[.]248[.]115[.]41
193[.]124[.]18[.]72
185[.]154[.]52[.]83
185[.]154[.]52[.]142
185[.]29[.]9[.]41
zaometallniva[.]ru
1mliked[.]ru
84[.]38[.]133[.]22
itablex[.]com
213[.]183[.]63[.]227
185[.]70[.]187[.]188
http://185[.]70[.]187[.]188/inf/getsi[.]php
http://185[.]70[.]187[.]188/inf/logs/logpc[.]php
217[.]160[.]233[.]141
185[.]244[.]131[.]68
http://basch[.]eu/administrator/components/com_admin/sql/updates/mysql/exe[.]exe
http://185[.]244[.]131[.]68/z/get[.]php
185[.]175[.]58[.]136
http://185[.]175[.]58[.]136/gif/gifupload[.]php
http://146[.]0[.]77[.]112/a/logs/logpc[.]php
146[.]0[.]77[.]112
http://146[.]0[.]77[.]112/a/getsi[.]php
http://146[.]0[.]72[.]139/flk

146[.]0[.]72[.]139
http://5[.]39[.]218[.]204/ks
5[.]39[.]218[.]204
http://5[.]8[.]88[.]254/HUYfhwuiGYUR/opensource[.]php/name=?
fpbank[.]ru
http://91[.]243[.]80[.]200/yre
91[.]243[.]80[.]200
5[.]8[.]88[.]254
http://144[.]217[.]14[.]173/file[.]exe
http://137[.]74[.]224[.]142/z/get[.]php

MD5:

7441cca252b7a2da481ddf2c70eed727
b2ad4409323147b63e370745e5209996
8cc6d41f5be9144093a2ff8a5c3b32a3
65f673a77c93c4a2c9db34b3704279e2
edf59a111cce8ea1d09a2b4e8febdfdf
e2e1035f382c397d64303e345876a9db
5127fff71a4251e3c62c420a4de57010
f1a4e74e72390ef98c23f19589d3c7cd
81f3e843b26d254ae58c44d778c7ee5b
13cc98fcb654ac83cda6d3ec9946fa9b
C2A00949DDACFED9ED2EF83A8CB44780
97599e2edc7e7025d5c2a7d7a81dac47
C2F1AF367576FFA39182864044769E42
404d69c8b74d375522b9afe90072a1f4
43eda1810677afe6791dd7a33eb3d83c
7d3614df9409da3933637f09587af28c
15d097a50718f2e7251433ea65401588
a58a830dce460e91217328bdefb25cbe
9b037ead562c789620a167af85d32f72
c6c84da4f27103db4ff593f4d4f45d95

Network Signatures

Win32.Trojan_YU Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan_YU Checkin"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:".php?name="; http_uri; fast_pattern; pcre:"/\.php\?name=[0-9a-f]+ HTTP\/1\.1\x0d\x0aHost\: ([0-9]{1,3}\.){3}[0-9]{1,3}\x0d\x0a\x0d\x0a$/"; threshold:type limit, track by_src, count 1, seconds 360; classtype:apt-trojan; reference:md5,9b037ead562c789620a167af85d32f72; sid:1001404; rev:1; metadata:severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648,

ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin gib;)

TrueBot (Silence APT) CnC activity 1

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TrueBot (Silence APT) CnC activity 1"; flow:established,to_server; content:".php?xy=1"; http_uri; isdataat:!1,relative; fast_pattern; content:"User-Agent|3a 20 0d 0a 0d 0a|"; target:src_ip; classtype:apt-trojan; reference:md5,c4f18d40b17e506f42f72b8ff111a614; sid:1002195; rev:1; metadata:severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin gib;)

TROJAN TrueBot/Silence.Downloader CnC Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN TrueBot/Silence.Downloader CnC Checkin"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; isdataat:!1,relative; content:"Content-Disposition|3a 20|form-data|3b 20|name=|22|file|22 3b 20|filename=|22|C|3a 5c|"; http_client_body; content:".DAT|22 3b 0d 0a|"; http_client_body; distance:0; content:"|0d 0a|Host Name|3a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20|"; http_client_body; distance:0; content:"|0d 0a|OS Name|3a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20|"; http_client_body; distance:0; content:"|0d 0a|OS Version|3a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20|"; http_client_body; distance:0; http_header_names; content:!"Referer"; content:!"User-Agent"; content:!"Accept"; reference:md5,c2a00949ddacfed9ed2ef83a8cb44780; classtype:apt-trojan; sid:2026559; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_10_29, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_09_16, severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin etpro;)

TROJAN TrueBot/Silence.Downloader Keep-Alive

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN TrueBot/Silence.Downloader Keep-Alive"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:".php?dns="; http_uri; fast_pattern; pcre:"/^[a-f0-9]{8}$/RUs"; http_header_names; content:"|0d 0a|Host|0d 0a 0d 0a|"; depth:10; isdataat:!1,relative; reference:md5,c2a00949ddacfed9ed2ef83a8cb44780; classtype:apt-trojan; sid:2026560; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2018_10_29, deployment Perimeter, former_category TROJAN, performance_impact Moderate, signature_severity Major, updated_at 2020_09_16, severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin etpro;)

TrueBot (Silence APT) CnC activity 2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TrueBot (Silence APT) CnC activity 2"; flow:established,to_server; content:".php?xy=2&axy="; http_uri; target:src_ip; classtype:apt-trojan; reference:md5,c4f18d40b17e506f42f72b8ff111a614; sid:1002196; rev:1; metadata:severity 5, ti_malware_id 8ad76d853cdeb0644cda053bb7f0d50275847648, ti_malware_name Truebot (Silence's loader), malware_family Truebot (Silence's loader), rule_origin gib;)

e. FlawedAmmyy

It is malicious program for remote control, based on leaked source codes of legitimate utility Ammyy Admin. After infection, it allows full access to threat actors: opportunity to remote entering to the system, to restart it, process commands and upload any files. In addition, it has function of remote desktop. It was discovered in 2016. In August 2018 there were malicious email sendings with this malware to banks.

Platform: Windows

Threat level: High

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

http://n57u[[.]]com/inform
195[.]123[.]224[.]99
http://g78k[.]com/set
51[.]254[.]167[.]115
http://g50e[[.]]com/security
http://g50e[[.]]com/benat[.]exe
31[.]202[.]132[.]13
http://r48t[[.]]com/input
54[.]36[.]91[.]25
http://f67i[[.]]com/con
81[.]4[.]101[.]187
185[.]99[.]132[.]12

MD5:

b2f2ce77063476ef9c8ebb3c63fad402
a471555caf8dbb9d30fac3014172515f
73964f92d3e5e142047574afa78726e3
627ae12b487dfacad66d4ff3bf8a5134
0906ab6a9ed0fa8f173d6800f8957f4a
919c8bd911850741522fedf362effca3
92feb5c5358835e80dd1f62ef6ebc475

aa0a5f274d4c612b6fdfb91f66aef94f
65713d26cf111eb64de1aa524bbecb2b
5fdeaa5e62fabc9933352efe016f1565
bacd1120ad0918b81d98de9b9acb69ce
85e1828d863004ff681f2908297c7fee
1094ec2f32abc7780f0856928cb0c261

Network Signatures

RAT.FlawedAmmyy CnC communication

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"RAT.FlawedAmmyy CnC communication"; flow:established,to_server; content:"id="; content:"&os="; distance:0; content:"&priv="; distance:0; content:"&cred="; distance:0; content:"&pcname="; distance:0; content:"&avname="; distance:0; content:"&build_time="; distance:0; content:"&card="; distance:0; target:src_ip; classtype:backdoor; reference:md5,b2f2ce77063476ef9c8ebb3c63fad402; sid:1002344; rev:1; metadata:severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin gib;)

TROJAN Win32/FlawedAmmyy RAT Reporting System Details

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/FlawedAmmyy RAT Reporting System Details"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|2e|php"; http_uri; isdataat:!1,relative; content:"Host|20|Name|3a 20 20 20 20 20|"; http_client_body; depth:17; fast_pattern; content:"OS|20|Name|3a 20 20 20 20|"; http_client_body; distance:0; content:"OS|20|Version|3a 20 20 20 20|"; http_client_body; distance:0; reference:md5,d334c877fb1adc37fd68bf2b40275d7e; reference:md5,cf1e4eb6325ed0d9969bddac56eeda58; classtype:backdoor; sid:2837164; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_07_01, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, tag RAT, updated_at 2019_09_28, severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin etpro;)

TROJAN Win32/FlawedAmmyy RAT Reporting Loader Results

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/FlawedAmmyy RAT Reporting Loader Results"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|2e|php"; http_uri; isdataat:!1,relative; content:"running loader|0d 0a|"; http_client_body; depth:16; fast_pattern; content:"exiting loader"; http_client_body; distance:0; reference:md5,d334c877fb1adc37fd68bf2b40275d7e;

reference:md5,cf1e4eb6325ed0d9969bddac56eeda58; classtype:backdoor; sid:2837165; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_07_01, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, tag RAT, updated_at 2019_09_28, severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin etpro;)

TROJAN Win32/FlawedAmmyy RAT Reporting Installed Software

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Win32/FlawedAmmyy RAT Reporting Installed Software"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|2e|php"; http_uri; isdataat:!1,relative; content:"|ff fe 4e 00 61 00 6d 00 65 00 20 00 20 00 20 00|"; http_client_body; depth:16; fast_pattern; content:"|56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 20 00 20 00 20|"; http_client_body; distance:0; reference:md5,d334c877fb1adc37fd68bf2b40275d7e; reference:md5,cf1e4eb6325ed0d9969bddac56eeda58; classtype:backdoor; sid:2837166; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2019_07_01, deployment Perimeter, former_category TROJAN, performance_impact Low, signature_severity Major, tag RAT, updated_at 2019_09_28, severity 5, ti_malware_id 34c0a6e49e3384309ce0f552beb14ca6c14060f8, ti_malware_name FlawedAmmyy, malware_family FlawedAmmyy, rule_origin etpro;)

f. Ammyy Admin

Ammyy Admin - is a free remote desktop sharing and PC remote control software that can be used for remote administration, remote office arrangement, remote support or distant education purposes.

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Indicators of Compromise (IOCs)

CnC:

http://31[.]207[.]45[.]85/d[.]dat
31[.]207[.]45[.]85
http://185[.]179[.]188[.]185/ldr[.]exe
185[.]179[.]188[.]185

MD5:

7af426e0952b13ef158a4220e25df1ae

e71819cf79b1d5627acd9ac9aec6a4bc

Network Signatures

POLICY RemoteAdmin Win32.Ammyy.z Checkin

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"POLICY RemoteAdmin Win32.Ammyy.z Checkin"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:!"User-Agent|3a| "; http_header; content:"v="; depth:2; http_client_body; content:"&d="; distance:3; within:3; http_client_body; pcre:"/^v=\d\.\d&d=[a-zA-Z0-9-/]+?$/P"; reference:md5,da83a04e05d95f8b68b4bd2198de2097; classtype:trojan-activity; sid:2806289; rev:10; metadata:created_at 2013_04_23, updated_at 2020_06_09, severity 3, ti_malware_id 6ddc5de6cfaf12b1adb729a4f26e0358efe648a0, ti_malware_name Ammyy Admin, malware_family Ammyy Admin, rule_origin etpro;)

g. Atmosphere

Atmosphere is a software created by Silence group for controlling the ATM dispenser. It was first discovered in October 2017. It allows to get information on the content of ATM cassettes and to issue cash. Another version of Atmosphere discovered in April 2018. There were minor differences compared to the previous versions, but it was clear that the developer went a long way to debug the program and that he eventually got rid of the unnecessary functions and enhanced the program's sustainability. For example, this version didn't process commands from the PIN pad.

Platform: ATM

Threat level: High

Category: atm-malware

Indicators of Compromise (IOCs)

MD5:

44f15f1657a64423cb49ea317ce0c631

h. Smoke Bot

Smoke bot is malware with functions of loader and form grabber. This malware is known since 2011.

Platform: ATM

Threat level: High

Category: atm-malware

Other Names: Sharik, Dofoil, Smoke Loader

Indicators of Compromise (IOCs)

MD5:

44f15f1657a64423cb49ea317ce0c631

Network Signatures

TROJAN Smokeloader getgrab Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getgrab Command"; target:src_ip; flow:established,to_server; content:"cmd=getgrab"; http_uri; classtype:backdoor; sid:2014009; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smokeloader getproxy Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getproxy Command"; target:src_ip; flow:established,to_server; content:"cmd=getproxy&login="; http_uri; classtype:backdoor; sid:2014010; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smokeloader getsock Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getsock Command"; target:src_ip; flow:established,to_server; content:"cmd=getsocks&login="; http_uri; classtype:backdoor; sid:2014011; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smokeloader getload Command

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smokeloader getload Command"; target:src_ip; flow:established,to_server; content:"cmd=getload&login="; http_uri; reference:url,sophosnews.files.wordpress.com/2013/07/sophosszappanosplugxrevisitedintroducingsmoaler-rev1.pdf; reference:url,symantec.com/security_response/writeup.jsp?docid=2011-100515-1838-99&tabid=2; classtype:backdoor; sid:2014012; rev:3; metadata:created_at 2011_12_08, updated_at 2020_04_20, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smoke Loader Checkin r=gate

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Smoke Loader Checkin r=gate"; target:src_ip; flow:established,to_server; content:".php?r=gate&"; http_uri; content:"&group="; http_uri; distance:0; content:"&debug="; http_uri; distance:0; content:"5.0 (Windows|3b| U|3b| MSIE 9"; http_header; reference:md5,7ef1e61d9b394a972516cc453bf0ec06; classtype:trojan-activity; sid:2014728; rev:6; metadata:created_at 2012_05_09, former_category MALWARE, updated_at 2020_05_13, severity 3, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Smoke Loader C2 Response

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Smoke Loader C2 Response"; target:dest_ip; flow:established,from_server; content:"Content-Length|3a| 4|0d 0a|"; http_header; file_data; content:"Smk"; depth:3; fast_pattern; pcre:"/^\d+[\r\n]*?$/Rs"; classtype:trojan-activity; sid:2015835; rev:7; metadata:created_at 2012_10_22, former_category MALWARE, updated_at 2012_10_22, severity 3, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN SmokeBot grab data plaintext

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN SmokeBot grab data plaintext"; target:src_ip; flow:established,to_server; content:"cmd=grab&data="; fast_pattern; http_client_body; content:"&login="; http_client_body; classtype:trojan-activity; sid:2016011; rev:5; metadata:created_at 2012_12_07, updated_at 2020_09_17, severity 3, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

Smoke Loader domain +uri

alert http any any -> any any (msg:"Smoke Loader domain +uri"; target:src_ip; flow:from_client; content:"GET"; http_method; pcre:"/\.php\?act\=([^&]*)\&file\=/I"; nocase; content:!"www.tumcivil.com"; classtype:backdoor; http_host; sid:1000429; rev:2; metadata:severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin gib;)

TROJAN SmokeLoader - Init 0x

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN SmokeLoader - Init 0x"; target:dest_ip; flow:established,to_client; content:"Init|3a| 0x"; http_header; classtype:backdoor; sid:2016088; rev:2; metadata:created_at 2012_12_21, updated_at 2020_04_22, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

SMOKE LOADER

alert http any any -> any any (msg:"SMOKE LOADER"; target:src_ip; flow:from_client; content:"index.php?cmd=getgrab"; classtype:general-suspicious; http_uri; sid:1000412; rev:1; metadata:severity 2, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin gib;)

TROJAN Sharik/Smoke CnC Beacon 2

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Sharik/Smoke CnC Beacon 2"; target:src_ip; flow:established,to_server; urilen:1; content:"POST"; http_method; content:!"Accept"; http_header; content:!"Referer|3a|"; http_header; content:"Cache-Control|3a 20|no-cache|0d 0a|Pragma|3a 20|no-cache|0d 0a|Content-Type|3a 20|application/x-www-form-urlencoded|0d 0a|User-Agent|3a 20|"; depth:104; http_header; fast_pattern:76,20; content:"Connection|3a 20|Keep-Alive|0d 0a|Content-Length|3a 20|"; distance:0; http_header; pcre:"/^[\x20-\x7e\r\n]{0,20}[^\x20-\x7e\r\n]/P"; pcre:"/User-Agent\x3a[^\r\n]+(?:MSIE|rv\x3a)[^\r\n]+\r\nConnection\x3a\x20Keep-Alive\r\nContent-Length\x3a\x20\d+\r\nHost\x3a[^\r\n]+\r\n(?:\r\n)?$/Hm"; reference:md5,789ee114125a6e1db363b505a643c03d; classtype:backdoor; sid:2021631; rev:2; metadata:created_at 2015_08_14, former_category MALWARE, updated_at 2020_05_29, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;)

TROJAN Sharik/Smoke Loader Receiving Payload

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"TROJAN Sharik/Smoke Loader Receiving Payload"; target:dest_ip; flow:established,from_server; content:"404"; http_stat_code; file_data; content:"|00|"; distance:1; within:1; content:"|00|MZ"; distance:1; within:3; content:"This program must be run under Win32"; distance:0; fast_pattern; reference:md5,65c7426b056482fcda962a7a14e86601; classtype:backdoor; sid:2023567; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2016_11_30, deployment Perimeter, performance_impact Low, signature_severity Major, updated_at 2020_08_03, severity 5, ti_malware_id 5b5cd1f6f7dc81a094c5ae3d166841e709e57622, ti_malware_name Smoke Bot, malware_family Smoke Bot, rule_origin etpro;

i. Silence's ATM malware

Malware for ATM cashing out used by Silence group

Platform: Windows

Threat level: High

Category: atm-malware

Other Names: ATMRod

Indicators of Compromise (IOCs)

CnC:

http://149[.]56[.]131[.]140:443/microsoft
http://149[.]56[.]131[.]140:443/win

MD5:

B3ABB10CC8F4CBB454992B95064A9006
14863087695D0F4B40F480FD18D061A4
79E61313FEBE5C67D168CFC3C88CD743
4107F2756EDB33AF1F79B1DCE3D2FD77
86EA1F46DF745A30577F02FC24E266FF
6743F474E3A6A02BC1CCC5373E5EBBFA
DDB276DBFBCE7A9E19FEECC2C453733D

j. Silence.SurveillanceModule

A module for spying on users. It used for secretly taking screenshots and proceeded to investigate the operator's work via a pseudo-video stream

Platform: Windows

Threat level: High

Category: Spyware

Other Names: N/A

General information

- Silence.SurveillanceModule a module for secretly taking screenshots and proceeded to investigate the operator's work via a pseudo-video stream.

Indicators of Compromise (IOCs)

MD5:

242b471bae5ef9b4de8019781e553b85
d7491ed06a7f19a2983774fd50d65fb2

k. Perl IRC DDoS bot

This bot is a Perl script designed to run on Linux OS. Its functionality includes retrieving information about the infected machine, executing shell commands (cmd), sending emails, downloading files, scanning ports and carrying out DDoS attacks.

Platform: Linux

Threat level: Middle

Category: DDoS

Other Names: N/A

Indicators of Compromise (IOCs)

CnC:

http://92[.]222[.]68[.]32/bot[.]pl
http://92[.]222[.]68[.]32/wolf/

MD5:

081ee959cbe6bc7dde7a6d13168e4fb4
ee650c800d2eedd471ed59aa9435e55f
aa9c31883b3d8e493efad2f983908be3

l. Kikothac

Kikothac is a Trojan horse that opens a back door on the compromised computer and downloads potentially malicious files.

Platform: Windows

Threat level: Middle

Category: Backdoor

Indicators of Compromise (IOCs)

CnC:

46[.]183[.]221[.]89
193[.]169[.]245[.]89
185[.]29[.]9[.]45

MD5:

9628d7ce2dd26c188e04378d10fb8ef3
0074d8c3183e2b62b85a2b9f71d4ccd8
440b21958ad0e51795796d3c1a72f7b3

Advanced Persistent Threat (APT): OceanLotus

Group OceanLotus began active operations in late 2009. Among the objects of the attacks noted: government agencies, organizations for the protection of human rights, media, companies in the oil industry, research institutes, enterprises of marine industry, retail, hospitality, banking, it companies, companies involved in information security, individuals and activists. Various researchers noted the long-term nature of the group's campaigns, the active phase is preceded by a long period of preparation. OceanLotus is interested in cyber espionage, intelligence, and intellectual property theft. Along with phishing mailings disseminated by e-mail addresses of potential victims, OceanLotus also conduct a spa attack, an attack supported compromise of a large range of legitimate sites. alternative aliases: APT32, APT-C-00, SeaLotus, cobalt Kitty. throughout its activities, the criminal group used the subsequent vulnerabilities:

During its activities, the criminal group used the following vulnerabilities:

• CVE-2016-7255

• CVE-2017-11882

• CVE-2017-8759

• CVE-2017-0199

Related Tools

NBTScan
Matomo
fingerprintjs2
Cobalt Strike
Mimikatz
GetPassword_x64
OceanLotus.Custom Outlook Credential Dumper
HookPasswordChange
OceanLotus.Custom Windows Credential Dumper
NetCat
PSUnlock
OceanLotus.IPCheckTool

Malware List of OceanLotus APT:

a. Cobalt Strike

"Cobalt Strike" is a framework that offers a range of methods for conducting attacks, including delivery and control of malware on the victim's computer. Connection with the "Cobalt Strike" server is conducted through creation of hidden channels via DNS, HTTP, HTTPS protocols to avoid detection.

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Other Name: Framwork

General information

"Cobalt Strike" is a framework that offers a range of methods for conducting attacks, including delivery and control of malware on the victim's computer. Connection with the "Cobalt Strike" server is conducted through creation of hidden channels via DNS, HTTP, HTTPS protocols to avoid detection. The payload can carry out the following commands:

- Receive system information (OS, hardware, list of processes, computer name, etc.)
- Receive information on the network
- Execute commands in shell
- Download and launch .exe files
- Launch programs for copying of logins and passwords from Windows memory using the exploit in the lsass.exe process (using "mimikatz")
- Bypass Windows (UAC) user account management
- Make copies of hash passwords for Windows
- Gain remote access via VNC protocols with the ability to intervene in current Windows processes
- Provide access to file system
- Scan ports
- Take print screens
- Log keystrokes from specific processes
- Launch a SOCKS proxy server on a specified port, which allows tunnelling of traffic to other applications using DNS, HTTP, HTTPS protocols to avoid detection.
- Provide VPN server functionality
- Provide access to infected computer using «psexec»;
- Change file timestamp attributes

Indicators of Compromise (IOCs)

CnC:

cdn[.]redirectme[.]net
137[.]74[.]181[.]105
http://www[.]hkbytes[.]info/resource/image[.]jpg
www[.]hkbytes[.]info
http://27[.]102[.]102[.]139/lcpd/index[.]jpg
27[.]102[.]102[.]139
https://27[.]102[.]102[.]139/oEcE
http://www[.]hkbytes[.]info/logo[.]gif

MD5:

DFBF9CC304E36C0B67DB02AAA062297B
AD43D67ED35472D4D6541D9C555F05DB
8ADFD63DE516FCB142EA443FD5AB3B95

045451fa238a75305cc26ac982472367

Network Signatures

Cobalt Strike http related X-Malware EICAR header

alert http any any -> any any (msg:"Cobalt Strike http related X-Malware EICAR header"; target:dest_ip; content:"X-Malware"; http_header; content:"EICAR-STANDARD-ANTIVIRUS-TEST-FILE"; http_header; within:64; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1000829; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Strike reported domain name (host4.marketshigh.com)

alert http any any -> any any (msg:"Cobalt Strike reported domain name (host4.marketshigh.com)"; target:src_ip; flow:established,to_server; content:"host4.marketshigh.com"; http_host; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1001420; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt-related DNS Lookup (host4.marketshigh.com)

alert udp any any -> any 53 (msg:"Cobalt-related DNS Lookup (host4.marketshigh.com)"; target:src_ip; flow:from_client; content:"|05|host4|0b|marketshigh|03|com|00|"; nocase; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1001421; rev:1; metadata:severity 5, ti_threatactor_id c509eac2111b5bd8b67314feb259572255c6f6cc, ti_threatactor_name Cobalt, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (wecloud.biz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (wecloud.biz)"; target:src_ip; flow:from_client; content:"|07|wecloud|03|biz|00|"; classtype:apt-trojan; nocase; sid:1001650; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (mail.maincdn.biz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (mail.maincdn.biz)"; target:src_ip; flow:from_client; content:"|04|mail|07|maincdn|03|biz|00|"; classtype:apt-trojan; nocase; sid:1001651;

rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (document.com.kz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (document.com.kz)"; target:src_ip; flow:from_client; content:"|08|document|03|com|02|kz|00|"; classtype:apt-trojan; nocase; sid:1001652; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Strike reported IP address

alert tcp $HOME_NET any -> [92.63.111.201,192.52.167.228,89.33.64.134,45.32.165.110,37.1.207.202,176.9.99.134,46.21.147.63,86.105.1.116] !445 (msg:"Cobalt Strike reported IP address"; target:src_ip; threshold:type limit, track by_src, seconds 30, count 1; classtype:apt-trojan; reference:url,http://bytesdarkly.com/2014/11/cobalt-strike-review/; sid:1001419; rev:2; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Win32.Trojan.Dropper Downloading Cobalt Strike Beacon

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Win32.Trojan.Dropper Downloading Cobalt Strike Beacon"; target:src_ip; flow:established,to_server; content:"GET"; http_method; content:!"Referer|3a|"; nocase; http_header; content:!"Accept-Language|3a|"; nocase; http_header; content:"%20?id="; http_raw_uri; fast_pattern; pcre:"/\/%20\?id=\d*&act=\d*$/I"; classtype:apt-trojan; reference:md5,7edca868c6c52a9f7b24892dc361e444; sid:1001493; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS DNS Lookup (address-in.kz)

alert udp $HOME_NET any -> any 53 (msg:"Cobalt Backdoor JS DNS Lookup (address-in.kz)"; target:src_ip; flow:from_client; content:"|0a|address-in|02|kz|00|"; classtype:apt-trojan; nocase; sid:1001790; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

Cobalt Backdoor JS Response with payload

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"Cobalt Backdoor JS Response with payload"; target:dest_ip; flow:established,to_client;

flowbits:isset,GIB.cobalt.backdoor.js.payload; file_data; content:"<package"; depth:8; content:"<component id="; distance:0; content:"<registration"; distance:0; content:"progid="; distance:0; content:"classid="; distance:0; content:"<script language=|22|JScript|22|"; distance:0; classtype:apt-trojan; reference:md5,bd07b04e008093a40f60e48b903c59cf; sid:1001728; rev:1; metadata:severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin gib;)

TROJAN Cobalt Strike Exfiltration

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"TROJAN Cobalt Strike Exfiltration"; target:src_ip; flow:established,to_server; content:"POST"; http_method; content:"|43 6f 62 61 6c 74 20 53 74 72 69 6b 65 20 42 65 61 63 6f 6e 29|"; fast_pattern; http_user_agent; isdataat:!1,relative; http_header_names; content:!"Referer"; classtype:apt-trojan; sid:2025636; rev:1; metadata:affected_product Web_Browsers, attack_target Client_Endpoint, created_at 2018_07_03, deployment Perimeter, former_category TROJAN, signature_severity Major, updated_at 2020_09_16, severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin etpro;)

TROJAN CopyKittens Cobalt Strike DNS Lookup (cloudflare-analyse . com)

alert dns $HOME_NET any -> any any (msg:"TROJAN CopyKittens Cobalt Strike DNS Lookup (cloudflare-analyse . com)"; target:src_ip; dns_query; content:"cloudflare.analyse.com"; depth:22; nocase; isdataat:!1,relative; fast_pattern; threshold:type limit, track by_src, count 1, seconds 60; reference:url,www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf; reference:md5,752240cddda5acb5e8d026cef82e2b54; classtype:apt-trojan; sid:2024497; rev:4; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2017_07_25, deployment Perimeter, former_category MALWARE, performance_impact Moderate, signature_severity Major, updated_at 2020_09_17, severity 5, ti_malware_id b69fc9d439d2fd41e98a7e3c60b9a55340012eb6, ti_malware_name Cobalt Strike, malware_family Cobalt Strike, rule_origin etpro;)

b. METALJACK

Platform: Windows

Threat level: Middle

Category: remote-access-trojan

Other Name: Framwork

Indicators of Compromise (IOCs)

CnC:

vitlescaux[.]com
141[.]98[.]212[.]23

MD5:

a4808a329b071a1a37b8d03b1305b0cb

c. KerrDown

The loader used by the OceanLotus group since March 2018.

Platform: N/A

Threat level: N/A

Category: N/A

Other Name: downloader

Indicators of Compromise (IOCs)

CnC:

vitlescaux[.]com
141[.]98[.]212[.]23
account[.]dvrdns[.]org
https://outlook[.]updateoffices[.]net/vean32[.]png
88[.]150[.]138[.]114
https://cortanasyn[.]com/kirr64[.]png
cortanasyn[.]com
https://syn[.]servebbs[.]com/kuss32[.]gif
syn[.]servebbs[.]com

MD5:

6875F307D95790CA25C1DA542EA736A8
8D42D9FD3A4D32BC0474D07052CE8984
05b5707d79ca0aee269eb1b02db75b19
8ac2841fbb960a36739a958783ad1694
0a5e5a9a77e64d4fdd987ef7ae66fbe3
d279e98e77d895dc5a981bb8312a5918
3b36fb3a8cf15b0c5a288329e357e916
8ccfd46a24d3bcbee934af91dda8483d
a91e0c32ea93465b80d1bab41193ea4f
d568d10f3e66b89159abf402b31a37b8
f198ab61bc0bf8e5ae8c237d93c7b95d
cab262b84dbd319f3df84f221e5c451f
9bcd0b2590c53e4c0ed5614b127c6ba7
ac5f18f1c20901472d4708bd06a2d191
85dc4f704ee017844e84b42d4b17a1c3

50c6e221e5cd4f41973f3d6779ae1c4c
f5ad93917cd5b119f82b52a0d62f4a93
d6955b482cb67558e2152f6cdd0a2c91
77390c852addc3581d14acf06991982e
4973d4d95b17150153fddc07bbdb6575
49e969a9312ee2ae639002716276073f
6aa22d6c51ea5abe9a9af3a3fb51721b
b75bf1c32bcbe5dfd9261dd558b63277
611f35b485bf2b79db911842bb9d4e8f
c9093362a83b0e7672a161fd9ef9498a
305d992821740a9cbbda9b3a2b50a67c
c28abdfe45590af0ef5c4e7a96d4b979
bf040c081ad1b051fdf3e8ba458d3a9c
751c735585fdff7cb1bf2ae2f281393c
6c2a8612c6511df2876bdb124c33d3e1
1211dea7b68129d48513662e546c6e21
a406626173132c8bd6fe52672deacbe7
e04594ba7e2c63d4f48d92cc99246cce
43c03994e843164625794f4ac727811e
7338852de96796d7f733123f04dd1ae9
6b8fc8c9fe4f4ef90b2fcbcc0d24cfc9
4bdada3dea9b6bb14418e584c1b6af08
2f1f8142d479a1daf3cbd404c7c22f9f
c3bb2b1eabfb34181a9a052e4f06397c
7a6ba3e26c86f3366f544f4553c9d00a
4e7e56be0fdea72564ba761916897895
7df61bc3a146fcf56fe1bbd3c26ea8c0
d40b4277e0d417e2e0cff47458ddd62d
b1990e19efaf88206f7bffe9df0d9419
3c04352c5230b8cbaa12f262dc01d335
d65287550672dac1a89b804c90e7accf
9a10292157ac3748212fb77769873f6c
2756b2f6ba5bcf811c8baced5e98b79f
f3551be56b9f72374787442453bf0428
a530410bca453c93b65d0de465c428e4
c78fd680494b505525d706c285d5ebce
f42611ac0ea2c66d9f27ae14706c1b00
518f52aabd9a059d181bfe864097091e
3a869e8a7b7022082d5a8661ed2fb602
865a7e3cd87b5bc5feec9d61313f2944
760024b35e51a06dcde2128843b1bfdb
ce0afd0b440e25267a96e181d3d9ec5a
546bb6ef89bebfb053999777f6930d7e
38f9655c72474b6c97dc9db9b3609677
9972111cc944d20c9b315fd56eb3a177
0f877ad5464fcbb12e1c019adf7065cc

SHA-256:

5cda7d8294a8804d09108359dd2d96cdf4fdcf22ec9c00f0182d005afff76743

d. OceanLotus.Denis

Denis is a simple backdoor developed by the OceanLotus Group, well observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.

Platform: Windows

Threat level: Middle

Category: Backdoor

Other Name: N/A

Indicators of Compromise (IOCs)

CnC:

udt[.]sophiahoule[.]com
ourkekwiciver[.]com
dieordaunt[.]com
straliaenollma[.]xyz
andreagahuvrauvin[.]com
byronorenstein[.]com
stienollmache[.]xyz
Andreagbridge[.]Com
illagedrivestralia[.]Xyz
http://dload01[.]s3[.]amazonaws[.]com/b89fdbf4-9f80-11e7-abc4-2209cec278b6b50a/FirefoxInstaller[.]exe
nasahlaes[.]com
jeffreyue[.]com
rackerasr[.]com
urnage[.]com
maerferd[.]com
harinarach[.]com
eoneorbin[.]com
74[.]119[.]239[.]234
tsworthoa[.]com
orinneamoure[.]com
lbertussbau[.]com
arinaurna[.]com
icmannaws[.]com
avidsontre[.]com
aulolloy[.]com

MD5:

a8ff3e6abe26c4ce72267154ca604ce3
c7931fa4c144c1c4dc19ad4c41c1e17f
56b5a96b8582b32ad50d6b6d9e980ce7
DD8B36F8F967A26314820C35632FA0D0

F3551BE56B9F72374787442453BF0428
655C536462944D0F3C9FCF4EC19D2015
6AA3115FA1F3ADB8F0539E93D2CF21CA
DDD161A6BB63CA46E8CB0663587920FE
74731674920C51668C36CC3C16F30553
b612735909c41fb7a47e9c12fd1b6cfc
b123f9151c5e7057f061f3e03c1e8416
9453f31cdb02533d509948cc4fd0c44f
4282c6633122dce395de35c05159282d
eb2b52ed27346962c4b7b26df51ebafa
62944e26b36b1dcace429ae26ba66164
fcd7227891271a65b729a27de962c0cb
58d2907361f6414742dcc5071ca20980
1fa011e6a692ee95452c626e61b5263a
627e3ff5659b9a0ab9dc4b283c3288dd
d592b06f9d112c8650091166c19ea05a
88152846c45924d5706a11523942c82b
05bc07fc6265e6affa8478118c02942a

e. OceanLotus.masOS.Backdoor

It was discovered in November 2014. The Trojan was disguised as an Adobe Flash update and was used to attack macOS users by the OceanLotus APT group. The Trojan allows an attacker to manipulate the file system: transfer commands for execution via the command line; download files at a specific URL; modify files (as well as delete, move, copy); terminate processes. The components of the Trojan itself are encrypted, which complicates its analysis; in addition, the malware makes changes to the security settings of the Internet browser, thereby allowing attackers to download arbitrary files without the user's knowledge. The malware also checks for a running virtual environment and reads the OS version.

Platform: Mac

Threat level: N/A

Category: Backdoor

Other Name: N/A

Indicators of Compromise (IOCs)

CnC:

web[.]dalalepredaa[.]com
rio[.]imbandaad[.]com
web[.]dalalepredaa[.]com
5[.]135[.]199[.]9

MD5:

06334cb14c1512bf2794af8dae5ab357
a76be0181705809898d5d7d9aed86ee8

da71b64e77ad45bab56cf71ecd4f55d4
306d3ed0a7c899b5ef9d0e3c91f05193
9831a7bfcf595351206a2ea5679fa65e

f. WINDSHIELD

A malicious program used by the group since 2014. Features WINDSHIELD communication via TCP; 4 C2 servers and 6 configured ports - a pair is chosen at random; manipulation of the registry / file system; collecting information about the values of the registry, username and computer; termination of processes; loading additional modules.

Platform: N/A

Threat level: N/A

Category: Backdoor

Other Name: N/A

Indicators of Compromise (IOCs)

MD5:

7a81a6fdaee15162a3a231751bdd0259
189a078150b12baff608fc18af4bb837
5bcf16810c7ef5bce3023d0bbefb4391
79D06DD20768FD8CD4A043833C1F2D4B

g. Denes

A dropper used by the OceanLotus group to install other malicious components and programs.

Platform: N/A

Threat level: N/A

Category: dropper

Other Name: N/A

Indicators of Compromise (IOCs)

MD5:

49a2e438309e219fa4d9c51dfb7ffcb1
96b971c9ac868c8d9ae98618b9a9bddc
88152846c45924d5706a11523942c82b
d592b06f9d112c8650091166c19ea05a

h. OceanLotus.SteganoLoader

Loader used since September 2018 by the OceanLotus group. The downloader combines steganography and Dll Side-loading techniques, which allows you to download malware using legitimate software along with .png images.

Platform: N/A

Threat level: N/A

Category: Loader, APT

Other Name: N/A

Indicators of Compromise (IOCs)

MD5:

c55f1145ecc9ea52b2872a99a3f04eb4
bbeba6edfea62c34ab92a60e86fd7ce7
ec52a11625bdb4aad3740ff8cc6d8c0f
1675afb65f32c7b148f5d8acbeed2acc
43b57414a07f69aa87ad3ec85fb06b6d
f6c672a15b2c5101279a6420f8d4ecc7
71f512da26deeeceb7e41fbb6a5e3267
08c984ac6b0e0a291f16d0c249310a14

SHA-256:

a2719f203c3e8dcdcc714dd3c1b60a4cbb5f7d7296dbb88b2a756d85bf0e9c1e

i. Downloader

A program that can install malicious components and programs. The dropper can be either another malicious program or legitimate software infected with malicious code.

Platform: N/A

Threat level: N/A

Category: Trojan

Other Name: N/A

Indicators of Compromise (IOCs)

CnC:

ourkekwiciver[.]com
dieordaunt[.]com
straliaenollma[.]xyz
andreagahuvrauvin[.]com
byronorenstein[.]com
stienollmache[.]xyz
Andreagbridge[.]Com
illagedrivestralia[.]Xyz
164[.]132[.]45[.]67
192[.]34[.]109[.]173
http://defprocindia[.]com/register[.]doc

defprocindia[.]com
162[.]255[.]119[.]117
http://www[.]oxfam[.]org/en/invitation<https://drive/google/com/file/s/0B7fMhZc0wl0OeTJpZmViQXU4YVE/edit?usp=sharing
www[.]oxfam[.]org
151[.]236[.]216[.]85
tripadvisor[.]dyndns[.]info
62[.]75[.]204[.]91
neuro[.]dyndns-at-home[.]com
foursquare[.]dyndns[.]tv
wowwiki[.]dynalias[.]net
yelp[.]webhop[.]org
179[.]43[.]134[.]61

MD5:

b123f9151c5e7057f061f3e03c1e8416
9453f31cdb02533d509948cc4fd0c44f
4282c6633122dce395de35c05159282d
3dfc49add45ad35a7c6e21054a53a351
a3d09d969df1742a7cc9511f07e9b44b
6ecb19b51d50af36179c870f3504c623
109cd896f8e13f925584dbbad400b338
A08b9a984b28e520cbde839d83db2d14
877ecaa43243f6b57745f72278965467
87d108b2763ce08d3f611f7d240597ec
5f69999d8f1fa69b57b6e14ab4730edd
75a00fcede0b91793a19295a8b9a7060
cd74dd88322431441fb1088ac7dd6715
e3e99f6d1333ca76a80ba2899a4e2587
02AE075DA4FB2A6D38CE06F8F40E397E
B10F93CDBCDF43D4C5C5770872E239F4
fd4e2b72bbd5f0f27eb5788cc6a7dedd
da71b64e77ad45bab56cf71ecd4f55d4
9831a7bfcf595351206a2ea5679fa65e
d1233d34fcbd643b8c03c026dc4b2e7e
af170750a8228c9e5f21bfc35fc67721
6e667d6c9e527ada1a3284aa333d954d
616d32151c907fdd4e718bde2163cc40
1a60715c51da0caa8a5ebff6fdc9d472

SHA-256:

2fa7ad4736e2bb1d50cbaec625c776cdb6fce0b8eb66035df32764d5a2a18013

j. OceanLotus.Backdoor

The backdoor that the OceanLotus group has been using since May 2017. Backdoor features: system fingerprint; setting the session identifier; creating a process and getting the result of execution; getting information from a file or registry key and calculating MD5; creating /

deleting / moving directories / files; creating an entry in the registry or a stream in memory; file system search; creating a list of logical drives; install and run the program; switch to HTTP; reboot; setting / retrieving environment variables; running shellcode in a new thread.

Platform: N/A

Threat level: N/A

Category: Trojan

Other Name: N/A

Indicators of Compromise (IOCs)

CnC:

tephens[.]com
traveroyce[.]com

MD5:

B10F93CDBCDF43D4C5C5770872E239F4
72A5AD375401F33A5079CAEE18884C9D
79D06DD20768FD8CD4A043833C1F2D4B
EC505565E4CB5A22BFD3F63E4AD83FF3
93da064e3fc4422c63fecca93ee1b157
a7f98d3b7b7e2a7d1c194c2f26045618
96b971c9ac868c8d9ae98618b9a9bddc

k. PhantomLance

PhantomLance is a malicious program for the Android operating system. This malware able to collect confidential information from the victim's device. To do this, the malware can obtain root rights on the device, and thus gain the ability to transmit geolocation data, a call log, SMS messages, a list of installed applications, and full information about the infected device to its operators. At the same time, its functionality can be expanded at any time by loading additional modules from the C&C server.

Platform: N/A

Threat level: N/A

Category: Backdoor

Other Name: N/A

Indicators of Compromise (IOCs)

MD5:

2e06bbc26611305b28b40349a600f95c
b1990e19efaf88206f7bffe9df0d9419
7048d56d923e049ca7f3d97fb5ba9812
e648a2cc826707aec33208408b882e31

3285ae59877c6241200f784b62531694
8d5c64fdaae76bb74831c0543a7865c3
6bf9b834d841b13348851f2dc033773e
0d5c03da348dce513bf575545493f3e3
0e7c2adda3bc65242a365ef72b91f3a8
a795f662d10040728e916e1fd7570c1d
d23472f47833049034011cad68958b46
8b35b3956078fc28e5709c5439e4dcb0
af44bb0dd464680395230ade0d6414cd
65d399e6a77acf7e63ba771877f96f8e
79f06cb9281177a51278b2a33090c867
b107c35b4ca3e549bdf102de918749ba
83cd59e3ed1ba15f7a8cadfe9183e156
c399d93146f3d12feb32da23b75304ba
83c423c36ecda310375e8a1f4348a35e
94a3ca93f1500b5bd7fd020569e46589
54777021c34b0aed226145fde8424991
872a3dd2cd5e01633b57fa5b9ac4648d
243e2c6433815f2ecc204ada4821e7d6
a330456d7ca25c88060dc158049f3298
a097b8d49386c8aab0bb38bbfdf315b2
7285f44fa75c3c7a27bbb4870fc0cdca
b4706f171cf98742413d642b6ae728dc
8008bedaaebc1284b1b834c5fd9a7a71
0e7b59b601a1c7ecd6f2f54b5cd8416a

I. OceanLotus.Encryptor

OceanLotus Encryptor - First discovered in February 2014. The Trojan is an executable file masquerading as JPG or Word files. To bypass security systems, the program, by filling with random characters, increases the file size, which leads to the fact that the file becomes too large for uploading to cloud systems for their subsequent analysis. The Trojan is also capable of detecting the virtual environment and, in case of a positive result, stops further execution.

Platform: N/A

Threat level: N/A

Category: Trojan

Other Name: N/A

Indicators of Compromise (IOCs)

CnC:

active[.]soariz[.]com
193[.]169[.]244[.]73

MD5:

0529b1d393f405bc2b2b33709dd57153
d39edc7922054a0f14a5b000a28e3329
d1233d34fcbd643b8c03c026dc4b2e7e
41bced8c65c5822d43cadad7d1dc49fd

Log4Shell-CVE-2021-44228: Critical Apache Log4j Vulnerability

Apache Log4j is a Java-based logging utility it is part of the Apache Logging Services, a project of the Apache Software Foundation. Log4j is one of several Java logging frameworks.

A critical remote code execution vulnerability in the popular Apache Foundation Log4j library has been disclosed. Log4Shell (CVE-2021-44228) is a zero-day vulnerability in Log4j, the popular Java logging framework, involving arbitrary code execution. CVE-2021-44228/ Log4Shell received a CVSS severity score of a maximum 10[1]. It has been characterized by Tenable as "the single biggest, most critical vulnerability of the last decade"[2].

1. https://nvd.nist.gov/vuln/detail/CVE-2021-44228
2. https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell

Indicators of Compromise (IOCs)

CnC:

1[.]116[.]59[.]211
1[.]14[.]17[.]89
1[.]179[.]247[.]182
1[.]209[.]249[.]188
1[.]209[.]47[.]241
101[.]204[.]24[.]28
101[.]206[.]168[.]120
101[.]35[.]154[.]34
101[.]35[.]199[.]152
101[.]43[.]40[.]206
101[.]71[.]37[.]219
101[.]71[.]37[.]47
101[.]71[.]38[.]179
101[.]71[.]38[.]231
101[.]89[.]19[.]197
101[.]93[.]86[.]68
103[.]103[.]0[.]141
103[.]103[.]0[.]142
103[.]107[.]198[.]108
103[.]107[.]198[.]109
103[.]112[.]31[.]26
103[.]13[.]220[.]57
103[.]130[.]166[.]234
103[.]145[.]22[.]103
103[.]149[.]162[.]116
103[.]149[.]248[.]27
103[.]194[.]184[.]98

103[.]200[.]38[.]236
103[.]214[.]5[.]13
103[.]232[.]136[.]12
103[.]232[.]137[.]187
103[.]244[.]80[.]194
103[.]4[.]30[.]79
103[.]47[.]48[.]65
103[.]90[.]239[.]209
104[.]200[.]138[.]39
104[.]244[.]72[.]115
104[.]244[.]72[.]129
104[.]244[.]72[.]136
104[.]244[.]72[.]7
104[.]244[.]73[.]126
104[.]244[.]73[.]43
104[.]244[.]73[.]85
104[.]244[.]73[.]93
104[.]244[.]74[.]121
104[.]244[.]74[.]211
104[.]244[.]74[.]55
104[.]244[.]74[.]57
104[.]244[.]75[.]225
104[.]244[.]75[.]74
104[.]244[.]76[.]13
104[.]244[.]76[.]170
104[.]244[.]76[.]173
104[.]244[.]76[.]44
104[.]244[.]77[.]139
104[.]244[.]77[.]235
104[.]244[.]78[.]213
104[.]244[.]79[.]234
104[.]244[.]79[.]6
104[.]248[.]144[.]120
106[.]92[.]114[.]249
107[.]172[.]214[.]23
107[.]189[.]1[.]160
107[.]189[.]1[.]178
107[.]189[.]10[.]137
107[.]189[.]10[.]143
107[.]189[.]11[.]153
107[.]189[.]11[.]228
107[.]189[.]12[.]135
107[.]189[.]13[.]143
107[.]189[.]14[.]182
107[.]189[.]14[.]27
107[.]189[.]14[.]76
107[.]189[.]14[.]98

107[.]189[.]28[.]100
107[.]189[.]28[.]241
107[.]189[.]29[.]107
107[.]189[.]29[.]41
107[.]189[.]3[.]244
107[.]189[.]31[.]195
107[.]189[.]31[.]241
107[.]189[.]7[.]88
107[.]189[.]8[.]65
108[.]61[.]148[.]110
109[.]201[.]133[.]100
109[.]237[.]96[.]124
109[.]70[.]100[.]19
109[.]70[.]100[.]22
109[.]70[.]100[.]23
109[.]70[.]100[.]25
109[.]70[.]100[.]26
109[.]70[.]100[.]27
109[.]70[.]100[.]28
109[.]70[.]100[.]31
109[.]70[.]100[.]34
109[.]70[.]100[.]36
109[.]70[.]150[.]139
109[.]73[.]65[.]32
110[.]191[.]179[.]149
110[.]42[.]200[.]96
111[.]127[.]128[.]136
111[.]193[.]180[.]158
111[.]205[.]62[.]212
111[.]28[.]189[.]51
111[.]59[.]85[.]209
112[.]10[.]117[.]77
112[.]103[.]102[.]184
112[.]215[.]172[.]64
112[.]27[.]199[.]180
112[.]74[.]185[.]158
112[.]74[.]34[.]48
112[.]74[.]52[.]90
113[.]141[.]64[.]14
113[.]17[.]41[.]134
113[.]207[.]68[.]47
113[.]68[.]61[.]30
113[.]98[.]224[.]68
114[.]112[.]161[.]155
114[.]132[.]231[.]19
114[.]24[.]19[.]243
114[.]246[.]35[.]153

114[.]254[.]20[.]186
114[.]32[.]82[.]82
115[.]151[.]228[.]146
115[.]151[.]228[.]18
115[.]151[.]228[.]235
115[.]151[.]228[.]4
115[.]151[.]228[.]64
115[.]151[.]228[.]83
115[.]151[.]228[.]92
115[.]151[.]228[.]95
115[.]151[.]229[.]14
115[.]151[.]229[.]16
115[.]151[.]229[.]27
115[.]151[.]229[.]39
115[.]60[.]103[.]185
116[.]206[.]103[.]246
116[.]206[.]231[.]53
116[.]24[.]67[.]213
116[.]246[.]0[.]93
116[.]62[.]20[.]122
116[.]89[.]189[.]19
116[.]89[.]189[.]30
117[.]139[.]38[.]130
117[.]192[.]11[.]154
117[.]36[.]0[.]131
117[.]89[.]128[.]117
118[.]112[.]74[.]135
118[.]112[.]74[.]218
118[.]27[.]36[.]56
119[.]160[.]234[.]68
119[.]84[.]170[.]84
120[.]195[.]30[.]152
120[.]211[.]140[.]116
120[.]228[.]88[.]232
120[.]239[.]67[.]147
120[.]24[.]23[.]84
121[.]229[.]219[.]55
121[.]24[.]8[.]114
121[.]31[.]247[.]58
121[.]36[.]213[.]142
121[.]4[.]56[.]143
121[.]5[.]113[.]11
121[.]5[.]219[.]20
122[.]117[.]91[.]144
122[.]155[.]174[.]180
122[.]161[.]48[.]150
122[.]161[.]50[.]23

122[.]161[.]53[.]44
122[.]225[.]220[.]134
123[.]122[.]133[.]12
123[.]60[.]215[.]208
124[.]224[.]87[.]11
124[.]224[.]87[.]29
125[.]33[.]172[.]90
128[.]14[.]102[.]187
128[.]199[.]15[.]215
128[.]199[.]222[.]221
128[.]199[.]24[.]9
128[.]199[.]48[.]147
128[.]31[.]0[.]13
13[.]213[.]127[.]204
13[.]231[.]10[.]223
131[.]100[.]148[.]7
132[.]226[.]170[.]154
133[.]130[.]120[.]176
133[.]18[.]201[.]195
134[.]122[.]33[.]6
134[.]122[.]34[.]28
134[.]209[.]153[.]239
134[.]209[.]163[.]248
134[.]209[.]24[.]42
134[.]209[.]26[.]39
134[.]209[.]82[.]14
134[.]56[.]204[.]191
135[.]148[.]43[.]32
137[.]184[.]102[.]82
137[.]184[.]104[.]73
137[.]184[.]105[.]192
137[.]184[.]106[.]119
137[.]184[.]109[.]130
137[.]184[.]111[.]180
137[.]184[.]137[.]242
137[.]184[.]138[.]79
137[.]184[.]28[.]58
137[.]184[.]61[.]190
137[.]184[.]96[.]216
137[.]184[.]98[.]160
137[.]184[.]98[.]176
137[.]184[.]99[.]8
138[.]197[.]106[.]234
138[.]197[.]108[.]154
138[.]197[.]167[.]229
138[.]197[.]193[.]220
138[.]197[.]216[.]230

138[.]197[.]72[.]76
138[.]197[.]9[.]239
138[.]199[.]21[.]10
138[.]199[.]21[.]199
138[.]199[.]21[.]63
138[.]199[.]21[.]9
138[.]68[.]155[.]222
138[.]68[.]167[.]19
138[.]68[.]250[.]214
139[.]196[.]238[.]131
139[.]28[.]218[.]132
139[.]28[.]218[.]133
139[.]28[.]218[.]134
139[.]28[.]219[.]109
139[.]59[.]101[.]242
139[.]59[.]103[.]254
139[.]59[.]108[.]31
139[.]59[.]163[.]74
139[.]59[.]182[.]104
139[.]59[.]188[.]119
139[.]59[.]224[.]7
139[.]59[.]4[.]192
139[.]59[.]8[.]39
139[.]59[.]96[.]42
139[.]59[.]97[.]205
139[.]59[.]99[.]80
14[.]177[.]141[.]126
140[.]246[.]171[.]141
141[.]98[.]83[.]139
142[.]93[.]151[.]166
142[.]93[.]157[.]150
142[.]93[.]34[.]250
142[.]93[.]36[.]237
143[.]110[.]221[.]204
143[.]110[.]221[.]219
143[.]110[.]229[.]254
143[.]198[.]180[.]150
143[.]198[.]183[.]66
143[.]198[.]237[.]19
143[.]198[.]32[.]72
143[.]198[.]45[.]117
143[.]244[.]184[.]81
144[.]217[.]86[.]109
144[.]48[.]37[.]78
145[.]220[.]24[.]19
146[.]56[.]131[.]161
146[.]56[.]148[.]181

146[.]59[.]45[.]142
146[.]70[.]38[.]48
146[.]70[.]75[.]21
146[.]70[.]75[.]53
146[.]70[.]75[.]54
147[.]135[.]6[.]221
147[.]182[.]131[.]229
147[.]182[.]150[.]124
147[.]182[.]154[.]100
147[.]182[.]167[.]165
147[.]182[.]169[.]254
147[.]182[.]179[.]141
147[.]182[.]187[.]229
147[.]182[.]188[.]183
147[.]182[.]195[.]250
147[.]182[.]198[.]103
147[.]182[.]199[.]94
147[.]182[.]213[.]12
147[.]182[.]215[.]36
147[.]182[.]216[.]21
147[.]182[.]219[.]9
147[.]182[.]242[.]144
147[.]182[.]242[.]241
15[.]165[.]232[.]131
150[.]158[.]189[.]96
151[.]115[.]60[.]113
151[.]80[.]148[.]159
152[.]70[.]110[.]78
152[.]89[.]239[.]12
154[.]39[.]255[.]195
154[.]65[.]28[.]250
154[.]94[.]7[.]88
155[.]94[.]151[.]218
156[.]146[.]35[.]73
156[.]146[.]57[.]41
156[.]253[.]5[.]199
157[.]122[.]61[.]12
157[.]230[.]32[.]67
157[.]245[.]102[.]218
157[.]245[.]105[.]213
157[.]245[.]107[.]6
157[.]245[.]108[.]125
157[.]245[.]108[.]40
157[.]245[.]109[.]75
157[.]245[.]111[.]173
157[.]245[.]129[.]50
157[.]245[.]96[.]165

158[.]69[.]204[.]95
159[.]203[.]187[.]141
159[.]203[.]45[.]181
159[.]203[.]58[.]73
159[.]203[.]8[.]145
159[.]223[.]42[.]182
159[.]223[.]61[.]102
159[.]223[.]75[.]133
159[.]223[.]9[.]17
159[.]48[.]55[.]216
159[.]65[.]146[.]60
159[.]65[.]155[.]208
159[.]65[.]175[.]123
159[.]65[.]194[.]103
159[.]65[.]3[.]102
159[.]65[.]43[.]94
159[.]65[.]58[.]66
159[.]65[.]59[.]77
159[.]65[.]60[.]100
159[.]89[.]113[.]255
159[.]89[.]115[.]238
159[.]89[.]122[.]19
159[.]89[.]133[.]216
159[.]89[.]146[.]147
159[.]89[.]150[.]150
159[.]89[.]154[.]102
159[.]89[.]154[.]185
159[.]89[.]154[.]64
159[.]89[.]154[.]77
159[.]89[.]180[.]119
159[.]89[.]48[.]173
159[.]89[.]85[.]91
159[.]89[.]94[.]219
16[.]162[.]192[.]45
160[.]238[.]38[.]196
160[.]238[.]38[.]207
160[.]238[.]38[.]212
161[.]35[.]119[.]60
161[.]35[.]155[.]230
161[.]35[.]156[.]13
162[.]142[.]125[.]193
162[.]142[.]125[.]194
162[.]142[.]125[.]195
162[.]142[.]125[.]196
162[.]142[.]125[.]42
162[.]142[.]125[.]43
162[.]142[.]125[.]44

162[.]142[.]125[.]58
162[.]142[.]125[.]59
162[.]142[.]125[.]60
162[.]247[.]74[.]201
162[.]247[.]74[.]202
162[.]247[.]74[.]206
162[.]247[.]74[.]27
162[.]247[.]74[.]7
162[.]253[.]71[.]51
162[.]255[.]202[.]246
162[.]255[.]202[.]246
162[.]33[.]177[.]73
163[.]172[.]157[.]143
163[.]172[.]213[.]212
164[.]52[.]53[.]163
164[.]90[.]159[.]39
164[.]90[.]196[.]7
164[.]90[.]199[.]206
164[.]90[.]199[.]212
164[.]90[.]199[.]216
164[.]90[.]200[.]6
164[.]92[.]254[.]33
165[.]22[.]201[.]45
165[.]22[.]210[.]174
165[.]22[.]213[.]147
165[.]22[.]213[.]246
165[.]22[.]222[.]120
165[.]227[.]239[.]108
165[.]227[.]32[.]109
165[.]227[.]37[.]189
165[.]227[.]93[.]231
165[.]232[.]80[.]166
165[.]232[.]80[.]22
165[.]232[.]84[.]226
165[.]232[.]84[.]228
166[.]70[.]207[.]2
167[.]172[.]44[.]255
167[.]172[.]65[.]15
167[.]172[.]69[.]175
167[.]172[.]69[.]97
167[.]172[.]71[.]96
167[.]172[.]85[.]73
167[.]172[.]94[.]250
167[.]248[.]133[.]113
167[.]248[.]133[.]114
167[.]248[.]133[.]115
167[.]248[.]133[.]116

167[.]248[.]133[.]41
167[.]248[.]133[.]42
167[.]248[.]133[.]43
167[.]248[.]133[.]44
167[.]248[.]133[.]57
167[.]248[.]133[.]58
167[.]248[.]133[.]59
167[.]248[.]133[.]60
167[.]71[.]1[.]144
167[.]71[.]13[.]196
167[.]71[.]14[.]192
167[.]71[.]218[.]228
167[.]71[.]4[.]81
167[.]71[.]67[.]189
167[.]86[.]114[.]20
167[.]86[.]70[.]252
167[.]94[.]138[.]113
167[.]94[.]138[.]114
167[.]94[.]138[.]115
167[.]94[.]138[.]116
167[.]94[.]138[.]41
167[.]94[.]138[.]42
167[.]94[.]138[.]43
167[.]94[.]138[.]44
167[.]94[.]138[.]57
167[.]94[.]138[.]58
167[.]94[.]138[.]59
167[.]94[.]138[.]60
167[.]94[.]145[.]60
167[.]99[.]164[.]160
167[.]99[.]164[.]183
167[.]99[.]164[.]201
167[.]99[.]172[.]111
167[.]99[.]172[.]213
167[.]99[.]172[.]58
167[.]99[.]172[.]99
167[.]99[.]186[.]227
167[.]99[.]188[.]167
167[.]99[.]204[.]151
167[.]99[.]216[.]68
167[.]99[.]219[.]41
167[.]99[.]221[.]217
167[.]99[.]221[.]249
167[.]99[.]251[.]87
167[.]99[.]36[.]245
167[.]99[.]44[.]32
167[.]99[.]88[.]151

170[.]210[.]45[.]163
171[.]218[.]53[.]30
171[.]221[.]235[.]43
171[.]25[.]193[.]20
171[.]25[.]193[.]25
171[.]25[.]193[.]77
171[.]25[.]193[.]78
172[.]105[.]194[.]173
172[.]105[.]194[.]253
172[.]105[.]57[.]210
172[.]105[.]59[.]246
172[.]105[.]88[.]234
172[.]105[.]97[.]149
172[.]106[.]16[.]74
172[.]106[.]17[.]218
172[.]107[.]194[.]186
172[.]111[.]48[.]30
172[.]241[.]167[.]37
172[.]83[.]40[.]103
172[.]83[.]40[.]124
172[.]98[.]66[.]221
173[.]44[.]55[.]155
174[.]138[.]6[.]128
174[.]138[.]9[.]117
175[.]6[.]210[.]66
176[.]10[.]104[.]240
176[.]10[.]99[.]200
177[.]131[.]174[.]12
177[.]185[.]117[.]129
178[.]128[.]226[.]212
178[.]128[.]232[.]114
178[.]159[.]3[.]167
178[.]17[.]170[.]135
178[.]17[.]170[.]23
178[.]17[.]171[.]102
178[.]17[.]171[.]150
178[.]17[.]174[.]14
178[.]176[.]202[.]121
178[.]176[.]203[.]190
178[.]20[.]55[.]16
178[.]239[.]167[.]180
178[.]239[.]173[.]228
178[.]62[.]222[.]131
178[.]62[.]23[.]146
178[.]62[.]32[.]211
178[.]62[.]61[.]47
178[.]62[.]79[.]49

179[.]178[.]111[.]2
179[.]43[.]187[.]138
18[.]116[.]198[.]193
18[.]177[.]59[.]255
18[.]204[.]199[.]0
18[.]27[.]197[.]252
180[.]102[.]206[.]209
180[.]136[.]188[.]219
180[.]140[.]163[.]156
180[.]149[.]125[.]139
180[.]149[.]231[.]196
180[.]149[.]231[.]197
180[.]149[.]231[.]245
181[.]214[.]39[.]2
182[.]118[.]237[.]234
182[.]118[.]237[.]42
182[.]253[.]160[.]196
182[.]99[.]234[.]208
182[.]99[.]246[.]106
182[.]99[.]246[.]138
182[.]99[.]246[.]141
182[.]99[.]246[.]166
182[.]99[.]246[.]172
182[.]99[.]246[.]179
182[.]99[.]246[.]183
182[.]99[.]246[.]187
182[.]99[.]246[.]190
182[.]99[.]246[.]192
182[.]99[.]246[.]199
182[.]99[.]247[.]122
182[.]99[.]247[.]145
182[.]99[.]247[.]181
182[.]99[.]247[.]188
182[.]99[.]247[.]253
182[.]99[.]247[.]67
182[.]99[.]247[.]75
183[.]13[.]106[.]232
183[.]134[.]110[.]75
183[.]160[.]4[.]88
185[.]10[.]68[.]168
185[.]100[.]86[.]128
185[.]100[.]87[.]139
185[.]100[.]87[.]174
185[.]100[.]87[.]202
185[.]100[.]87[.]41
185[.]107[.]47[.]171
185[.]107[.]47[.]215

185[.]107[.]70[.]56
185[.]113[.]128[.]30
185[.]129[.]61[.]1
185[.]129[.]61[.]4
185[.]129[.]61[.]5
185[.]130[.]44[.]108
185[.]135[.]81[.]158
185[.]14[.]47[.]20
185[.]14[.]97[.]147
185[.]162[.]251[.]208
185[.]165[.]168[.]77
185[.]165[.]169[.]18
185[.]170[.]114[.]25
185[.]175[.]25[.]50
185[.]193[.]125[.]249
185[.]199[.]100[.]233
185[.]202[.]220[.]109
185[.]202[.]220[.]27
185[.]202[.]220[.]29
185[.]202[.]220[.]75
185[.]207[.]249[.]87
185[.]213[.]155[.]168
185[.]216[.]74[.]114
185[.]218[.]127[.]47
185[.]220[.]100[.]240
185[.]220[.]100[.]241
185[.]220[.]100[.]242
185[.]220[.]100[.]243
185[.]220[.]100[.]244
185[.]220[.]100[.]245
185[.]220[.]100[.]246
185[.]220[.]100[.]247
185[.]220[.]100[.]248
185[.]220[.]100[.]249
185[.]220[.]100[.]250
185[.]220[.]100[.]251
185[.]220[.]100[.]252
185[.]220[.]100[.]253
185[.]220[.]100[.]254
185[.]220[.]100[.]255
185[.]220[.]101[.]1
185[.]220[.]101[.]10
185[.]220[.]101[.]128
185[.]220[.]101[.]129
185[.]220[.]101[.]13
185[.]220[.]101[.]130
185[.]220[.]101[.]131

185[.]220[.]101[.]132
185[.]220[.]101[.]133
185[.]220[.]101[.]134
185[.]220[.]101[.]135
185[.]220[.]101[.]136
185[.]220[.]101[.]137
185[.]220[.]101[.]138
185[.]220[.]101[.]139
185[.]220[.]101[.]14
185[.]220[.]101[.]140
185[.]220[.]101[.]141
185[.]220[.]101[.]142
185[.]220[.]101[.]143
185[.]220[.]101[.]144
185[.]220[.]101[.]145
185[.]220[.]101[.]146
185[.]220[.]101[.]147
185[.]220[.]101[.]148
185[.]220[.]101[.]149
185[.]220[.]101[.]150
185[.]220[.]101[.]151
185[.]220[.]101[.]152
185[.]220[.]101[.]153
185[.]220[.]101[.]154
185[.]220[.]101[.]155
185[.]220[.]101[.]156
185[.]220[.]101[.]157
185[.]220[.]101[.]158
185[.]220[.]101[.]159
185[.]220[.]101[.]16
185[.]220[.]101[.]160
185[.]220[.]101[.]161
185[.]220[.]101[.]162
185[.]220[.]101[.]163
185[.]220[.]101[.]164
185[.]220[.]101[.]165
185[.]220[.]101[.]166
185[.]220[.]101[.]167
185[.]220[.]101[.]168
185[.]220[.]101[.]169
185[.]220[.]101[.]170
185[.]220[.]101[.]171
185[.]220[.]101[.]172
185[.]220[.]101[.]173
185[.]220[.]101[.]174
185[.]220[.]101[.]175
185[.]220[.]101[.]176

185[.]220[.]101[.]177
185[.]220[.]101[.]178
185[.]220[.]101[.]179
185[.]220[.]101[.]180
185[.]220[.]101[.]181
185[.]220[.]101[.]182
185[.]220[.]101[.]183
185[.]220[.]101[.]184
185[.]220[.]101[.]185
185[.]220[.]101[.]186
185[.]220[.]101[.]187
185[.]220[.]101[.]188
185[.]220[.]101[.]189
185[.]220[.]101[.]19
185[.]220[.]101[.]190
185[.]220[.]101[.]191
185[.]220[.]101[.]2
185[.]220[.]101[.]21
185[.]220[.]101[.]3
185[.]220[.]101[.]32
185[.]220[.]101[.]33
185[.]220[.]101[.]34
185[.]220[.]101[.]35
185[.]220[.]101[.]36
185[.]220[.]101[.]37
185[.]220[.]101[.]38
185[.]220[.]101[.]39
185[.]220[.]101[.]40
185[.]220[.]101[.]41
185[.]220[.]101[.]42
185[.]220[.]101[.]43
185[.]220[.]101[.]44
185[.]220[.]101[.]45
185[.]220[.]101[.]46
185[.]220[.]101[.]47
185[.]220[.]101[.]48
185[.]220[.]101[.]49
185[.]220[.]101[.]50
185[.]220[.]101[.]51
185[.]220[.]101[.]52
185[.]220[.]101[.]53
185[.]220[.]101[.]54
185[.]220[.]101[.]55
185[.]220[.]101[.]56
185[.]220[.]101[.]57
185[.]220[.]101[.]58
185[.]220[.]101[.]59

185[.]220[.]101[.]60
185[.]220[.]101[.]61
185[.]220[.]101[.]62
185[.]220[.]101[.]63
185[.]220[.]101[.]7
185[.]220[.]101[.]9
185[.]220[.]102[.]241
185[.]220[.]102[.]242
185[.]220[.]102[.]243
185[.]220[.]102[.]244
185[.]220[.]102[.]245
185[.]220[.]102[.]246
185[.]220[.]102[.]247
185[.]220[.]102[.]248
185[.]220[.]102[.]249
185[.]220[.]102[.]250
185[.]220[.]102[.]251
185[.]220[.]102[.]252
185[.]220[.]102[.]253
185[.]220[.]102[.]254
185[.]220[.]102[.]4
185[.]220[.]102[.]6
185[.]220[.]102[.]7
185[.]220[.]102[.]8
185[.]220[.]103[.]116
185[.]220[.]103[.]117
185[.]220[.]103[.]119
185[.]220[.]103[.]120
185[.]220[.]103[.]4
185[.]220[.]103[.]5
185[.]220[.]103[.]7
185[.]220[.]103[.]8
185[.]232[.]23[.]46
185[.]233[.]100[.]23
185[.]236[.]200[.]116
185[.]236[.]200[.]117
185[.]236[.]200[.]118
185[.]243[.]41[.]202
185[.]245[.]86[.]84
185[.]245[.]86[.]85
185[.]245[.]86[.]86
185[.]245[.]87[.]245
185[.]245[.]87[.]246
185[.]250[.]148[.]157
185[.]255[.]79[.]72
185[.]38[.]175[.]130
185[.]38[.]175[.]131

185[.]38[.]175[.]132
185[.]4[.]132[.]135
185[.]4[.]132[.]183
185[.]51[.]76[.]187
185[.]56[.]80[.]65
185[.]65[.]205[.]10
185[.]7[.]33[.]36
185[.]83[.]214[.]69
188[.]120[.]246[.]215
188[.]166[.]102[.]47
188[.]166[.]105[.]150
188[.]166[.]122[.]43
188[.]166[.]170[.]135
188[.]166[.]223[.]38
188[.]166[.]225[.]104
188[.]166[.]26[.]105
188[.]166[.]45[.]93
188[.]166[.]48[.]55
188[.]166[.]7[.]245
188[.]166[.]74[.]97
188[.]166[.]76[.]204
188[.]166[.]86[.]206
188[.]166[.]92[.]228
188[.]241[.]156[.]207
188[.]241[.]156[.]221
191[.]101[.]132[.]152
191[.]232[.]38[.]25
192[.]144[.]236[.]164
192[.]145[.]118[.]111
192[.]145[.]118[.]127
192[.]145[.]118[.]177
192[.]150[.]9[.]201
192[.]160[.]102[.]169
192[.]40[.]57[.]54
192[.]42[.]116[.]16
192[.]42[.]116[.]19
192[.]81[.]130[.]207
192[.]99[.]152[.]200
193[.]110[.]95[.]34
193[.]122[.]108[.]228
193[.]189[.]100[.]195
193[.]189[.]100[.]196
193[.]189[.]100[.]201
193[.]189[.]100[.]202
193[.]189[.]100[.]203
193[.]218[.]118[.]183
193[.]218[.]118[.]231

193[.]239[.]232[.]101
193[.]239[.]232[.]102
193[.]29[.]60[.]202
193[.]31[.]24[.]154
193[.]32[.]210[.]125
193[.]32[.]210[.]182
194[.]110[.]84[.]182
194[.]110[.]84[.]243
194[.]110[.]84[.]39
194[.]110[.]84[.]93
194[.]135[.]33[.]152
194[.]151[.]29[.]154
194[.]163[.]133[.]36
194[.]163[.]163[.]20
194[.]163[.]45[.]31
194[.]195[.]112[.]76
194[.]195[.]118[.]221
194[.]233[.]71[.]145
194[.]48[.]199[.]78
194[.]87[.]236[.]154
195[.]123[.]247[.]209
195[.]144[.]21[.]219
195[.]176[.]3[.]19
195[.]176[.]3[.]24
195[.]19[.]192[.]26
195[.]201[.]175[.]217
195[.]206[.]105[.]217
195[.]251[.]41[.]139
195[.]254[.]135[.]76
195[.]54[.]160[.]149
196[.]240[.]57[.]190
197[.]246[.]171[.]111
197[.]246[.]171[.]83
198[.]144[.]121[.]43
198[.]54[.]128[.]94
198[.]96[.]155[.]3
198[.]98[.]51[.]189
198[.]98[.]57[.]191
198[.]98[.]57[.]207
198[.]98[.]59[.]65
198[.]98[.]60[.]19
198[.]98[.]62[.]150
199[.]195[.]248[.]29
199[.]195[.]250[.]77
199[.]195[.]252[.]18
199[.]195[.]253[.]162
199[.]217[.]117[.]92

199[.]249[.]230[.]110
199[.]249[.]230[.]119
199[.]249[.]230[.]158
199[.]249[.]230[.]163
199[.]249[.]230[.]84
2[.]56[.]57[.]208
20[.]205[.]104[.]227
20[.]71[.]156[.]146
20[.]73[.]161[.]16
203[.]175[.]13[.]14
203[.]218[.]252[.]81
203[.]27[.]106[.]141
203[.]27[.]106[.]142
203[.]27[.]106[.]165
204[.]8[.]156[.]142
205[.]185[.]115[.]217
205[.]185[.]115[.]45
205[.]185[.]117[.]149
205[.]185[.]125[.]45
205[.]185[.]126[.]167
205[.]185[.]127[.]35
206[.]188[.]196[.]219
206[.]189[.]20[.]141
206[.]189[.]29[.]232
207[.]246[.]101[.]221
209[.]127[.]17[.]234
209[.]127[.]17[.]242
209[.]141[.]34[.]232
209[.]141[.]36[.]206
209[.]141[.]41[.]103
209[.]141[.]45[.]189
209[.]141[.]45[.]227
209[.]141[.]46[.]203
209[.]141[.]49[.]232
209[.]141[.]54[.]195
209[.]141[.]58[.]146
209[.]141[.]59[.]180
209[.]58[.]146[.]134
209[.]58[.]146[.]160
209[.]97[.]133[.]112
210[.]217[.]18[.]76
211[.]138[.]191[.]69
211[.]148[.]73[.]182
211[.]154[.]194[.]21
211[.]218[.]126[.]140
212[.]102[.]40[.]36
212[.]102[.]50[.]103

212[.]102[.]50[.]87
212[.]102[.]50[.]89
212[.]109[.]197[.]1
212[.]192[.]216[.]30
212[.]192[.]246[.]95
212[.]193[.]30[.]142
212[.]193[.]57[.]225
212[.]47[.]237[.]67
213[.]152[.]188[.]4
213[.]156[.]18[.]247
213[.]164[.]204[.]146
213[.]173[.]34[.]93
213[.]202[.]216[.]189
213[.]203[.]177[.]219
213[.]61[.]215[.]54
213[.]95[.]149[.]22
216[.]218[.]134[.]12
216[.]24[.]191[.]27
217[.]112[.]83[.]246
217[.]138[.]200[.]150
217[.]138[.]208[.]92
217[.]138[.]208[.]94
217[.]146[.]83[.]136
217[.]146[.]83[.]229
217[.]68[.]181[.]100
217[.]79[.]189[.]13
218[.]28[.]128[.]14
218[.]29[.]217[.]234
218[.]89[.]222[.]71
219[.]100[.]36[.]177
219[.]159[.]77[.]109
220[.]189[.]250[.]86
221[.]199[.]187[.]100
221[.]222[.]155[.]240
221[.]226[.]159[.]22
221[.]228[.]87[.]37
222[.]128[.]62[.]127
222[.]211[.]205[.]179
223[.]104[.]67[.]7
223[.]89[.]64[.]12
23[.]105[.]194[.]3
23[.]108[.]92[.]140
23[.]120[.]182[.]121
23[.]128[.]248[.]13
23[.]129[.]64[.]130
23[.]129[.]64[.]131
23[.]129[.]64[.]132

23[.]129[.]64[.]133
23[.]129[.]64[.]134
23[.]129[.]64[.]135
23[.]129[.]64[.]136
23[.]129[.]64[.]137
23[.]129[.]64[.]138
23[.]129[.]64[.]139
23[.]129[.]64[.]140
23[.]129[.]64[.]141
23[.]129[.]64[.]142
23[.]129[.]64[.]143
23[.]129[.]64[.]144
23[.]129[.]64[.]145
23[.]129[.]64[.]146
23[.]129[.]64[.]148
23[.]129[.]64[.]149
23[.]154[.]177[.]2
23[.]154[.]177[.]4
23[.]154[.]177[.]6
23[.]154[.]177[.]7
23[.]160[.]193[.]176
23[.]183[.]83[.]71
23[.]184[.]48[.]209
23[.]234[.]200[.]135
23[.]82[.]194[.]113
23[.]82[.]194[.]114
23[.]82[.]194[.]166
23[.]82[.]194[.]167
23[.]82[.]194[.]168
3[.]139[.]218[.]90
3[.]94[.]114[.]30
31[.]171[.]154[.]132
31[.]191[.]84[.]199
31[.]42[.]184[.]34
31[.]42[.]186[.]101
31[.]6[.]19[.]41
34[.]125[.]76[.]237
34[.]247[.]50[.]189
35[.]170[.]71[.]122
35[.]193[.]211[.]95
35[.]232[.]163[.]113
35[.]76[.]31[.]198
36[.]155[.]14[.]163
36[.]227[.]164[.]189
36[.]4[.]92[.]53
37[.]120[.]158[.]20
37[.]120[.]158[.]22

37[.]120[.]189[.]247
37[.]120[.]199[.]196
37[.]120[.]203[.]182
37[.]120[.]204[.]142
37[.]120[.]232[.]51
37[.]123[.]163[.]58
37[.]187[.]122[.]82
37[.]187[.]96[.]183
37[.]19[.]212[.]103
37[.]19[.]212[.]104
37[.]19[.]212[.]88
37[.]19[.]213[.]10
37[.]19[.]213[.]148
37[.]19[.]213[.]149
37[.]19[.]213[.]150
37[.]19[.]213[.]168
37[.]19[.]213[.]170
37[.]19[.]213[.]198
37[.]19[.]213[.]199
37[.]19[.]213[.]200
37[.]221[.]66[.]128
37[.]228[.]129[.]109
38[.]143[.]9[.]76
39[.]102[.]236[.]51
41[.]203[.]140[.]114
42[.]159[.]91[.]12
42[.]192[.]11[.]41
42[.]192[.]17[.]155
42[.]192[.]69[.]45
42[.]193[.]8[.]97
42[.]98[.]70[.]127
45[.]12[.]134[.]108
45[.]129[.]56[.]200
45[.]13[.]104[.]179
45[.]130[.]229[.]168
45[.]133[.]194[.]118
45[.]137[.]184[.]31
45[.]137[.]21[.]9
45[.]140[.]168[.]37
45[.]146[.]164[.]160
45[.]15[.]16[.]70
45[.]153[.]160[.]130
45[.]153[.]160[.]131
45[.]153[.]160[.]133
45[.]153[.]160[.]134
45[.]153[.]160[.]135
45[.]153[.]160[.]136

45[.]153[.]160[.]138
45[.]153[.]160[.]139
45[.]153[.]160[.]140
45[.]153[.]160[.]2
45[.]154[.]255[.]147
45[.]155[.]205[.]233
45[.]248[.]77[.]142
45[.]33[.]120[.]240
45[.]33[.]47[.]240
45[.]61[.]184[.]239
45[.]61[.]185[.]54
45[.]61[.]186[.]225
45[.]64[.]75[.]134
45[.]76[.]176[.]24
45[.]76[.]191[.]147
45[.]76[.]99[.]222
45[.]83[.]193[.]150
45[.]83[.]64[.]108
45[.]83[.]64[.]129
45[.]83[.]64[.]148
45[.]83[.]64[.]153
45[.]83[.]64[.]164
45[.]83[.]64[.]165
45[.]83[.]64[.]181
45[.]83[.]64[.]223
45[.]83[.]64[.]235
45[.]83[.]64[.]38
45[.]83[.]64[.]43
45[.]83[.]64[.]45
45[.]83[.]65[.]141
45[.]83[.]65[.]148
45[.]83[.]65[.]151
45[.]83[.]65[.]215
45[.]83[.]65[.]40
45[.]83[.]65[.]61
45[.]83[.]65[.]76
45[.]83[.]65[.]82
45[.]83[.]65[.]93
45[.]83[.]65[.]94
45[.]83[.]66[.]100
45[.]83[.]66[.]130
45[.]83[.]66[.]134
45[.]83[.]66[.]175
45[.]83[.]66[.]183
45[.]83[.]66[.]228
45[.]83[.]66[.]29
45[.]83[.]66[.]36

45[.]83[.]66[.]65
45[.]83[.]66[.]86
45[.]83[.]67[.]0
45[.]83[.]67[.]134
45[.]83[.]67[.]180
45[.]83[.]67[.]183
45[.]83[.]67[.]190
45[.]83[.]67[.]203
45[.]83[.]67[.]22
45[.]83[.]67[.]234
45[.]83[.]67[.]33
45[.]83[.]67[.]38
45[.]83[.]67[.]48
45[.]83[.]67[.]58
45[.]83[.]67[.]64
45[.]83[.]67[.]75
45[.]83[.]67[.]77
45[.]86[.]201[.]20
46[.]101[.]223[.]115
46[.]105[.]95[.]220
46[.]166[.]139[.]111
46[.]173[.]218[.]146
46[.]182[.]21[.]248
46[.]194[.]138[.]182
46[.]224[.]86[.]191
46[.]4[.]51[.]212
46[.]58[.]195[.]62
47[.]102[.]199[.]233
47[.]102[.]205[.]237
47[.]254[.]127[.]78
49[.]118[.]75[.]38
49[.]233[.]62[.]251
49[.]234[.]43[.]244
49[.]234[.]81[.]169
49[.]36[.]231[.]105
49[.]7[.]224[.]217
49[.]74[.]65[.]69
49[.]93[.]83[.]226
5[.]101[.]145[.]41
5[.]101[.]145[.]43
5[.]135[.]141[.]139
5[.]157[.]38[.]50
5[.]181[.]235[.]44
5[.]181[.]235[.]45
5[.]182[.]210[.]216
5[.]183[.]209[.]217
5[.]199[.]143[.]202

5[.]2[.]69[.]50
5[.]2[.]70[.]140
5[.]2[.]72[.]73
5[.]22[.]208[.]77
5[.]254[.]101[.]167
5[.]254[.]101[.]169
5[.]254[.]43[.]59
51[.]105[.]55[.]17
51[.]15[.]180[.]36
51[.]15[.]244[.]188
51[.]15[.]43[.]205
51[.]15[.]59[.]15
51[.]15[.]76[.]60
51[.]255[.]106[.]85
51[.]68[.]190[.]9
51[.]75[.]161[.]78
51[.]77[.]52[.]216
52[.]140[.]215[.]233
52[.]175[.]18[.]172
52[.]231[.]93[.]116
54[.]144[.]8[.]103
54[.]146[.]233[.]218
54[.]173[.]99[.]121
54[.]199[.]27[.]97
54[.]254[.]58[.]27
58[.]100[.]164[.]147
58[.]241[.]61[.]242
58[.]247[.]209[.]203
60[.]31[.]180[.]149
61[.]175[.]202[.]154
61[.]178[.]32[.]114
61[.]19[.]25[.]207
62[.]102[.]148[.]68
62[.]102[.]148[.]69
62[.]171[.]142[.]3
62[.]210[.]130[.]250
62[.]76[.]41[.]46
64[.]113[.]32[.]29
64[.]188[.]16[.]142
64[.]227[.]67[.]110
66[.]112[.]213[.]87
66[.]220[.]242[.]222
67[.]205[.]170[.]85
67[.]205[.]191[.]102
67[.]207[.]93[.]79
68[.]183[.]192[.]239
68[.]183[.]198[.]247

68[.]183[.]198[.]36
68[.]183[.]2[.]123
68[.]183[.]207[.]73
68[.]183[.]33[.]144
68[.]183[.]35[.]171
68[.]183[.]36[.]244
68[.]183[.]37[.]10
68[.]183[.]41[.]150
68[.]183[.]44[.]143
68[.]183[.]44[.]164
68[.]79[.]17[.]59
72[.]223[.]168[.]73
77[.]199[.]38[.]33
78[.]110[.]164[.]45
78[.]31[.]71[.]247
78[.]31[.]71[.]248
79[.]146[.]170[.]248
79[.]172[.]214[.]11
8[.]209[.]212[.]37
80[.]57[.]9[.]110
80[.]67[.]172[.]162
80[.]71[.]158[.]44
81[.]17[.]18[.]59
81[.]17[.]18[.]60
81[.]17[.]18[.]61
81[.]17[.]18[.]62
81[.]30[.]157[.]43
82[.]102[.]25[.]253
82[.]102[.]31[.]170
82[.]118[.]18[.]201
82[.]221[.]131[.]71
83[.]97[.]20[.]151
84[.]17[.]39[.]201
84[.]17[.]42[.]118
84[.]53[.]225[.]118
85[.]93[.]218[.]204
86[.]106[.]103[.]29
86[.]109[.]208[.]194
87[.]118[.]110[.]27
88[.]80[.]20[.]86
89[.]163[.]154[.]91
89[.]163[.]249[.]192
89[.]163[.]252[.]230
89[.]163[.]252[.]30
89[.]187[.]161[.]35
89[.]238[.]178[.]213
89[.]249[.]63[.]3

89[.]35[.]30[.]236
89[.]38[.]69[.]136
89[.]38[.]69[.]99
89[.]40[.]183[.]205
91[.]198[.]77[.]208
91[.]203[.]5[.]146
91[.]207[.]173[.]119
91[.]207[.]173[.]123
91[.]207[.]174[.]157
91[.]219[.]237[.]21
91[.]221[.]57[.]179
91[.]243[.]81[.]71
91[.]245[.]81[.]65
91[.]250[.]242[.]12
92[.]223[.]89[.]187
92[.]242[.]40[.]21
92[.]38[.]178[.]27
94[.]142[.]241[.]194
94[.]230[.]208[.]147
94[.]230[.]208[.]148
95[.]141[.]35[.]15
95[.]214[.]54[.]97
143[.]198[.]163[.]225
46[.]101[.]26[.]182
64[.]227[.]8[.]178
137[.]184[.]156[.]166
138[.]68[.]13[.]60
138[.]68[.]57[.]60
138[.]68[.]246[.]18
143[.]110[.]208[.]87
159[.]65[.]97[.]137
159[.]65[.]110[.]107
165[.]22[.]232[.]67
165[.]227[.]0[.]252
165[.]227[.]4[.]86
103[.]93[.]199[.]4
128[.]90[.]152[.]68