ICT DIVISION
FUTURE IS HERE

DIGITAL SECURITY AGENCY

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

Bangladesh Cyber Threat Landscape

JAN - DEC 2021

TLP: WHITE

| RISK ASSESSMENT UNIT & THREAT INTELLIGENCE UNIT | BGD E-GOV CIRT |

Contents

Sharing Indicator

Traffic Light Protocol (TLP) The Traffic Light Protocol (TLP) was created to encourage greater sharing of sensitive information. It is designed to improve the flow of information between individuals, organizations or communities in a controlled and trusted way[1].

Definitions:

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction

[1] https://www.cirt.gov.bd/incident-reporting/traffic-light-protocol-tlp/

Abbreviations

APT	Advanced Persistent Threat
APWG	Anti-Phishing Working Group
BCC	Bangladesh Computer Council
CII	Critical Information Infrastructure
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DoS	Denial of Service
ENISA	European Union Agency for Network and Information Security
LFI	Local File Inclusion
OWASP	Open Web Application Security Project
Q	Quarter
RaaS	Ransomware-as-a-Service
SOC	Security Operation Centre
XSS	Cross-site Scripting

Preface

This report aims to define national Bangladesh cyber threat landscape for the year 2021. Government, Industry & all CII may further use this report to raise awareness on national cyber threat landscape among executives, risk managers, auditors and security managers in Bangladesh and encourage them to use it for managing cyber risks within their respective organization.

BGD e-GOV CIRT will keep Bangladesh cyber threat landscape up to date by reviewing and adjusting it annually by using national statistical data on cybersecurity incidents, survey data and following international cyber security landscape changes.

Bangladesh Cyberthreat Landscape

1.1 Introduction

With the advent of COVID-19 the whole world is grappling to sustain their economy. Bangladesh is no exception to tackle the challenges to keep the work force moving with the adaption of 'work from home' or 'online' education. As the internet usage grew exponentially due to intermittent 'lockdown', cyber threat landscape also evolved. Cybercriminals have shown no sign of slowing down in 2021 and, as we approach the halfway point and the gradual climb out of the COVID-19 pandemic, they are still not short of sophisticated and malicious ways to achieve their goals. Phishing attempts, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, Ransomware and access brokers, Business email compromise (BEC), Data breaches, Supply chain attacks, Crypto jacking were among the top threats reported globally[2].

BGD e-GOV CIRT publishes "Bangladesh Cyber Threat Landscape" report by collecting information from Critical Information Infrastructures, information available from open sources and BGD e-GOV CIRT's own Cyber Threat Intelligence (CTI) capabilities. It's really necessary for nationwide cybersecurity to recognise evolving developments in cyber challenges and to recognize the future of cyber-attacks and allow successful responses to cybersecurity threats. Every year international organizations like ENISA as well as Industry Service Providers publish lots of Threat Landscape reports. However, each nation has its own eccentricities, and in order to

Figure 1: (Source- Wikipedia)

[2] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/the-threat-landscape-in-2021-so-far/

develop the requisite cyber capabilities and successfully minimize cyber threats, it is important to recognize the national cyber threat landscape based on local set of data. That's where this effort comes into place. The national cyber threat landscape study of Bangladesh describes Bangladesh's top cyber threats, their interactions with threat agents, specific threat mechanisms used to initiate a particular threat and kill chain for it. Each incident category used by us is allocated to each cyberthreat.

1.2 Overview of Bangladesh cyberthreats

This section provides an overview of Bangladesh cyberthreat landscape and trend of analysis

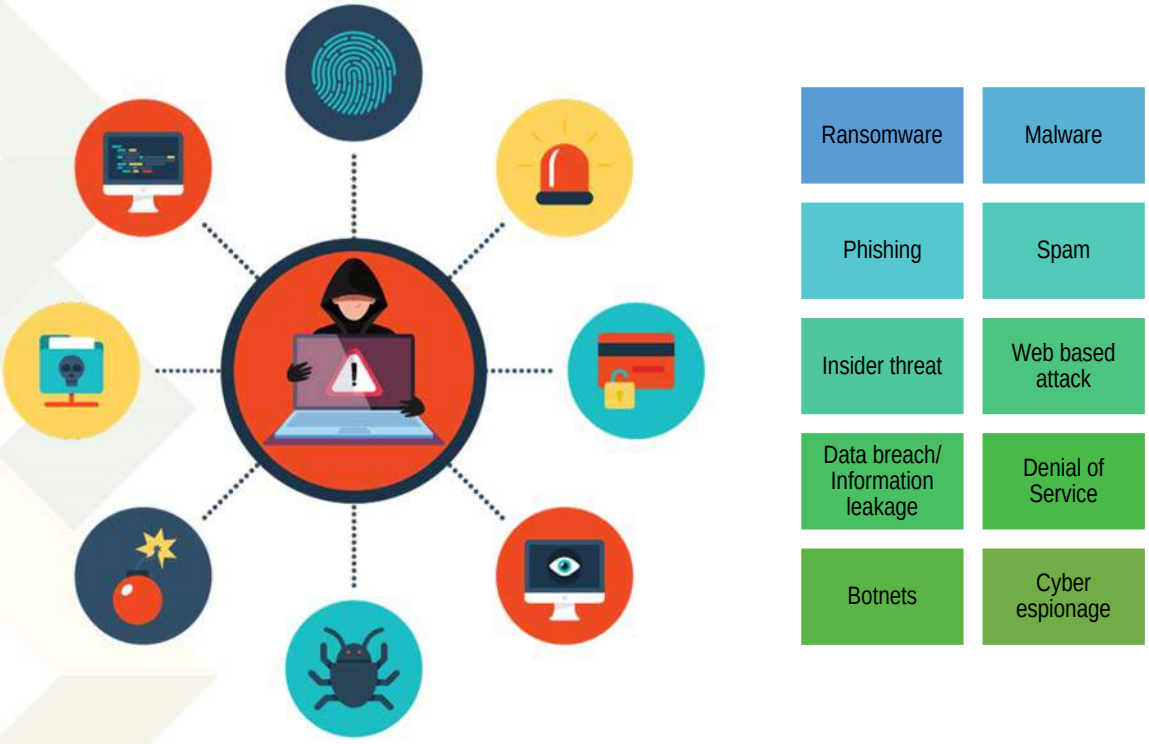


Figure 2: Bangladesh Top Threats-2021

Bangladesh Top Cyber Threats

Bangladesh cyber threat landscape is developed based on the results of an anonymous survey, BGD e-GOV CIRT's own Threat Intelligence, Open-source data, security blogs and news media articles.

2.1 Ransomware

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, attackers may also steal an organization's information and demand additional payment in return for not disclosing the information to authorities, competitors, or the public[3].

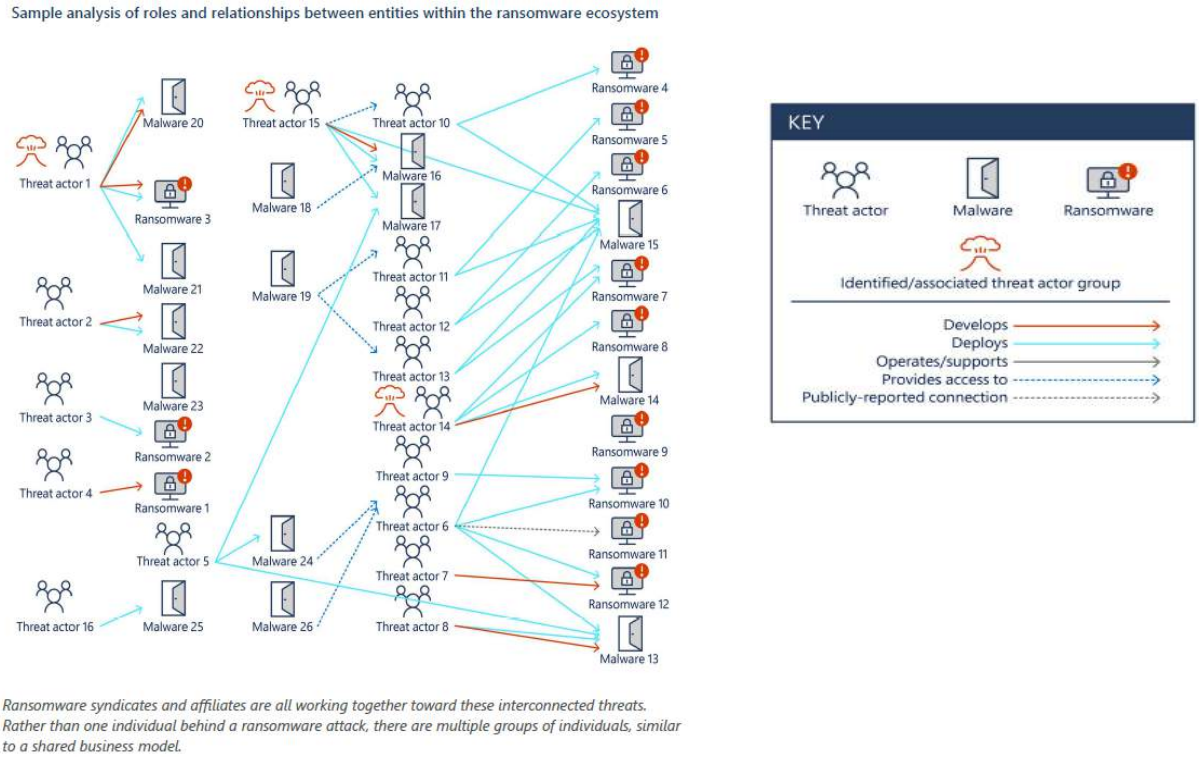


Figure 3: Sample analysis of roles and relationships between entities within the ransomware ecosystem

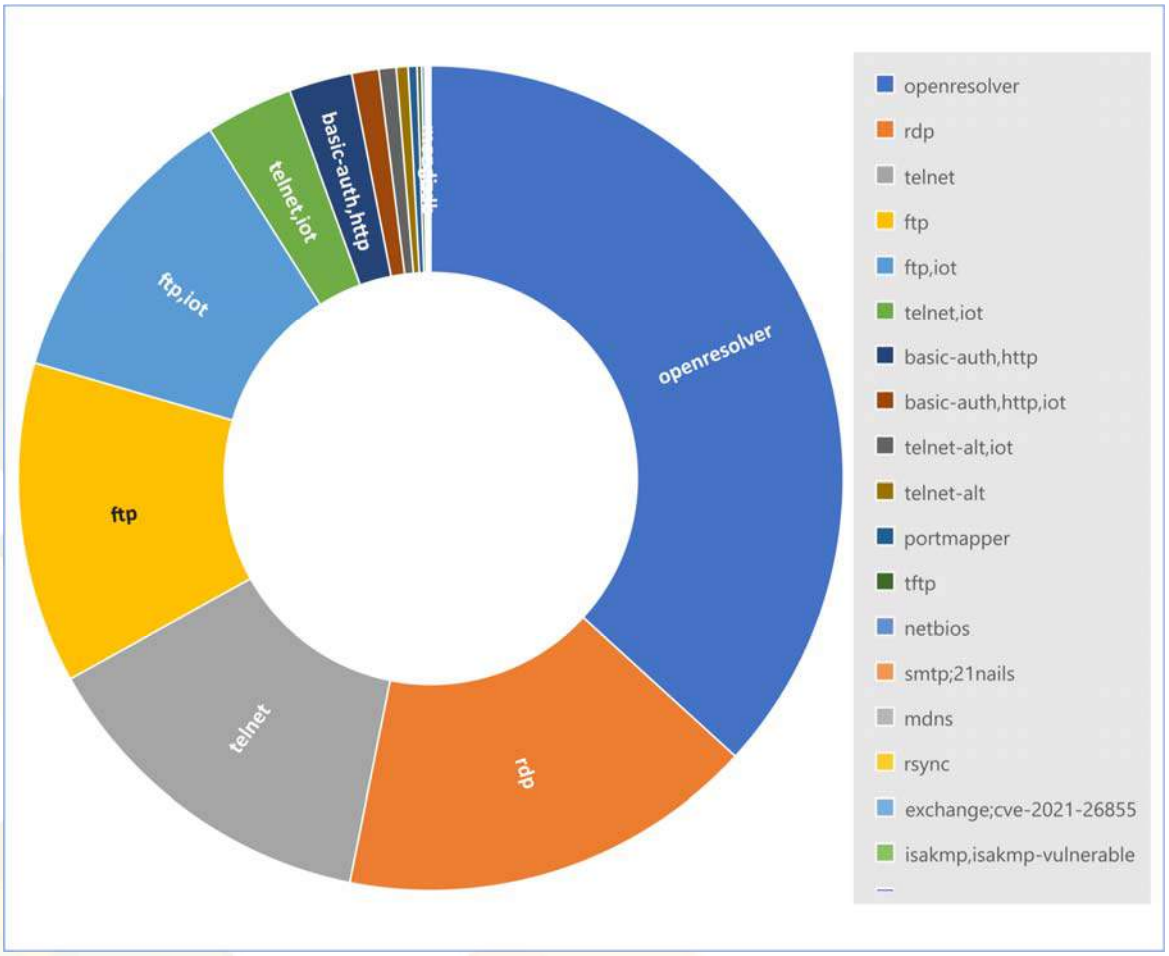
Source: (Microsoft Digital Defense Report, October 2021)[4]

[3] https://csrc.nist.gov/CSRC/media/Publications/nistir//draft/documents/NIST.IR.8374-preliminary-draft.pdf

[4] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Compromise through phishing e-mails and brute-forcing on Remote Desktop Protocol (RDP) services remain the two most common infection vectors. During the reporting period in 2021, it was being observed that the Conti and REvil threat actors dominated the ransomware market from a financial as well as from a volume of infections point of view. Both actors provide separate ransomware-as-a-service **(RaaS)** platforms through which affiliates can efficiently orchestrate their attacks. The focus on RaaS-type business models increased during 2021, making proper attribution to individual threat actors difficult.

RDP is ranked as the **second** highest detected vulnerable service in the different organizations in Bangladesh which are susceptible to exploitation.



(Source: Cyber Threat Intelligence Unit, BGD e-GOV CIRT)

Figure 4: RDP vulnerability exposure from November 2020 to November 2021 in Bangladesh

The occurrence of multiple extortion schemes also increased strongly during 2021. After initially stealing and encrypting sensitive data from organizations and threatening to release it publicly unless a payment is made, attackers also target the organizations' customers and/or partners for ransom to maximize their profits.

Cryptocurrency remains the most common pay-out method for threat actors. Attackers shifted to Monero as their cryptocurrency of choice because of its enhanced anonymity and the indistinguishability of transactions.

The average ransom amount doubled over the last year, though small amounts of ransom are still popular with threat actors. They tend to be paid more easily and result in less public exposure for the threat actor. The higher demands also increased. Over just a few months, the highest demand made in 2020 more than doubled in 2021.[5]

Top 10 countries attacked by ransomware Trojans

***Unique users attacked by ransomware Trojans as a percentage of all unique users of Kaspersky products in the country.*

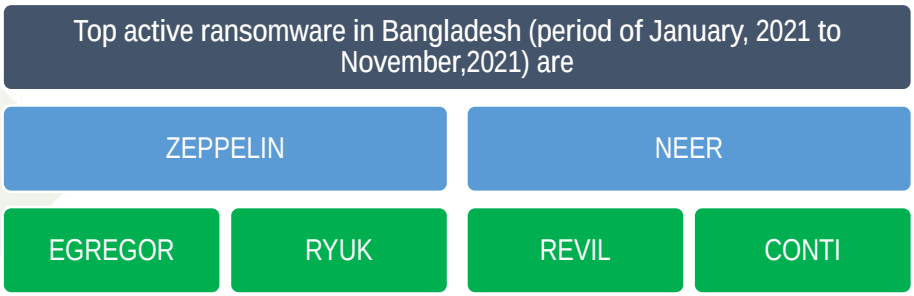
	Country*	%**
1	Bangladesh	1.85
2	Ethiopia	0.51
3	China	0.49
4	Pakistan	0.40
5	Egypt	0.38
6	Indonesia	0.36
7	Afghanistan	0.36
8	Vietnam	0.35
9	Myanmar	0.35
10	Nepal	0.33

[5] ENISA THREAT LANDSCAPE 2021

Top 10 most common families of ransomware Trojans

	Name	Verdicts	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	20.66
2	Stop	Trojan-Ransom.Win32.Stop	19.70
3	(generic verdict)	Trojan-Ransom.Win32.Gen	9.10
4	(generic verdict)	Trojan-Ransom.Win32.Crypren	6.37
5	(generic verdict)	Trojan-Ransom.Win32.Phny	6.08
6	(generic verdict)	Trojan-Ransom.Win32.Encoder	5.87
7	(generic verdict)	Trojan-Ransom.Win32.Agent	5.19
8	PolyRansom/VirLock	Virus.Win32.Polyransom / Trojan-Ransom.Win32.PolyRansom	2.39
9	(generic verdict)	Trojan-Ransom.Win32.Crypmod	1.48
10	(generic verdict)	Trojan-Ransom.MSIL.Encoder	1.26

Figure 5: Source: Kaspersky IT threat evolution Q2 2021 [6]



The attack vectors for ransomware are human element, web and browser-based attack vectors, internet exposed assets, exploitation of vulnerabilities/ misconfigurations and cryptographic/network/security protocol flaws and supply-chain attacks.

Primary group of threat agents for ransomware are cyber criminals, nation states and corporations.

[6] https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

Due to the rapid growth of ransomware activities, BGD e-GOV CIRT issued **"Ransomware Prevention & First Response Guideline (Version 2),"** which is available on the BGD e-GOV CIRT website.

Link: https://www.cirt.gov.bd/ransomware-prevention-first-response-guideline-version-2/

2.2 Malware

Malware has evolved to take advantage of tools that are available and, in some cases, are not inherently malicious. One prime example has been the use of **Cobalt Strike**, a commercial penetration testing tool. While Cobalt Strike is a penetration testing, it has been used more frequently in various attacks, ranging from nation state to human-operated ransomware, to perform system and network discovery actions and move laterally through a network. Cobalt Strike is specifically designed to evade traditional detection methodologies and offers the operator a range of options for performing obfuscation of their attack commands.[7]

Malware is one of the most frequently encountered and has the most significant impact among cyber threats in Bangladesh.

7 (Malware tools, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi)

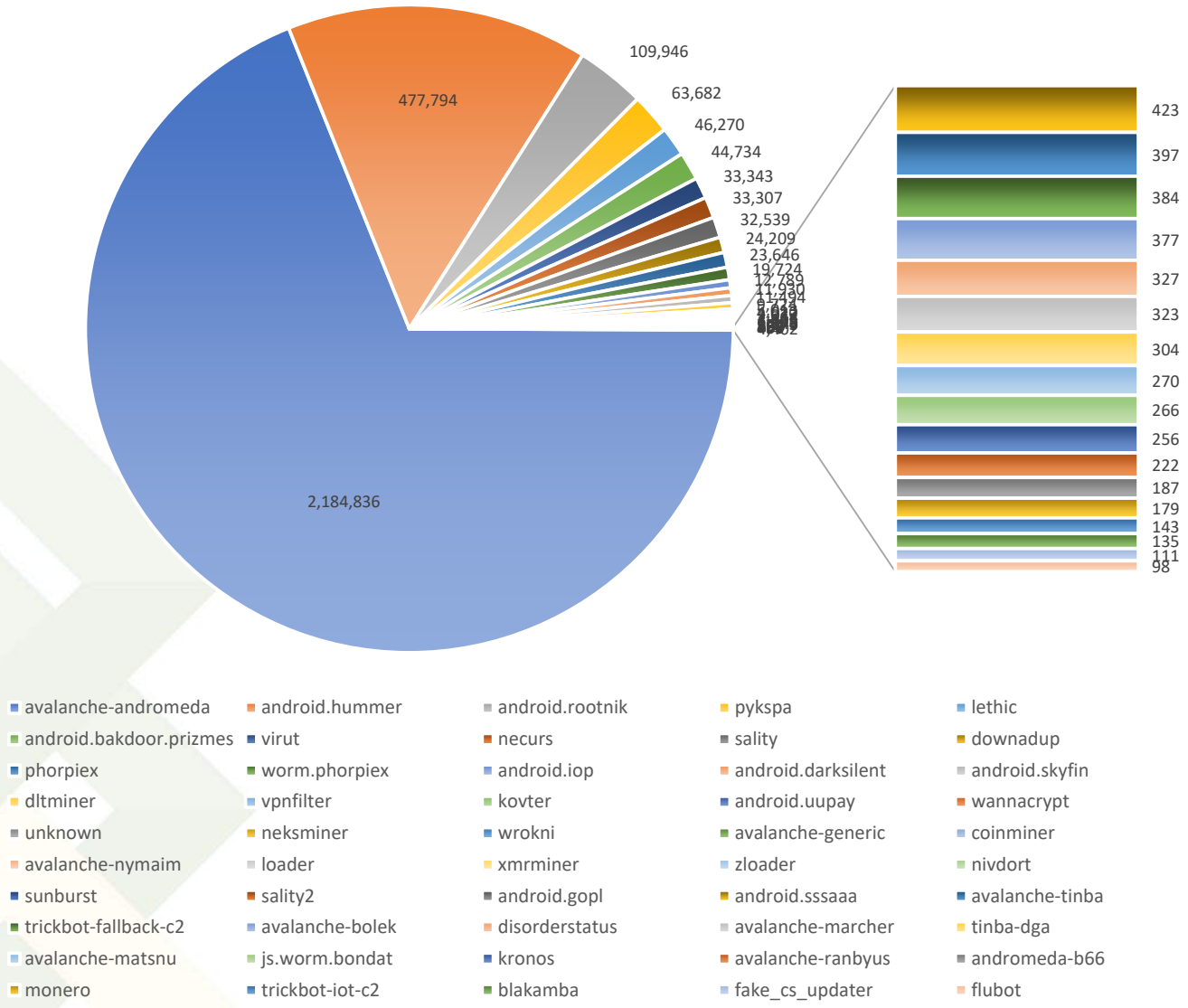


Figure 6: Top 10 malware infection for C&C communication for Bangladesh from September 2020 to September 2021
Source: BGD e-GOV CIRT Threat Intelligence Unit

Figure 7: Source: Malware Threat Intelligence Report for Bangladesh Context - Dec 2021

Web and e-mail protocols were the most often utilized primary attack vectors for malware distribution. However, several malware families were able to propagate even further inside a network by using brute force tactics or exploiting system weaknesses.

Primary group of threat agents for malware is cyber criminals, nation states and corporations.

2.3 Phishing

Phishing – the act of coercing victims into sharing personal data, credentials, or financial information online, often under the illusion that they are doing so with their bank or a trusted third party – has evolved to incorporate QR codes. This was first recorded in 2020 but has become increasingly popular in 2021. This is likely due to the rise in the use of QR codes throughout the pandemic as a simple means for civilians to check-in or receive necessary information when interacting with shops, restaurants, and other physical spaces.

Early in 2021, several phishing schemes were identified that asked victims to disclose vital data using a QR code. Doing so would allow attackers to leak data, gain access to financial information, or infect the device. This was evident in a series of communications, appearing to be from banks, that asked users to follow a QR code to receive vital COVID-19 information relating to their banking.[8]

Cyber Threat Intelligence Research unit of BGD e-GOV CIRT published a report on new variants of KASABLANKA LodaRAT targeting financial and government organizations of Bangladesh where 'Phishing' method was used as the initial infection phase.[9]

Top Phishing Objectives

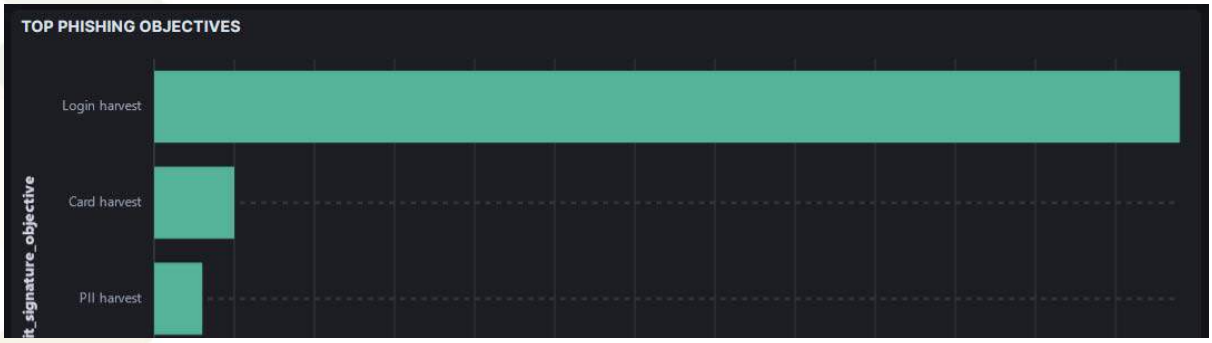


Figure: 8 Source: Cyber TIIR

[8] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/the-threat-landscape-in-2021-so-far/
[9] https://www.cirt.gov.bd/wp-content/uploads/2021/02/LodaRAT-BD-CAMPAIGN-Threat-Report-1.pdf

Phase-1.1: Initial Infection through Phishing

In this campaign attackers tried to allure the people interested for vaccination by using fake web portal (corona-bd.com/apply) like as Bangladesh Govt. official COVID-19 vaccine program associated website (corona.gov.bd)

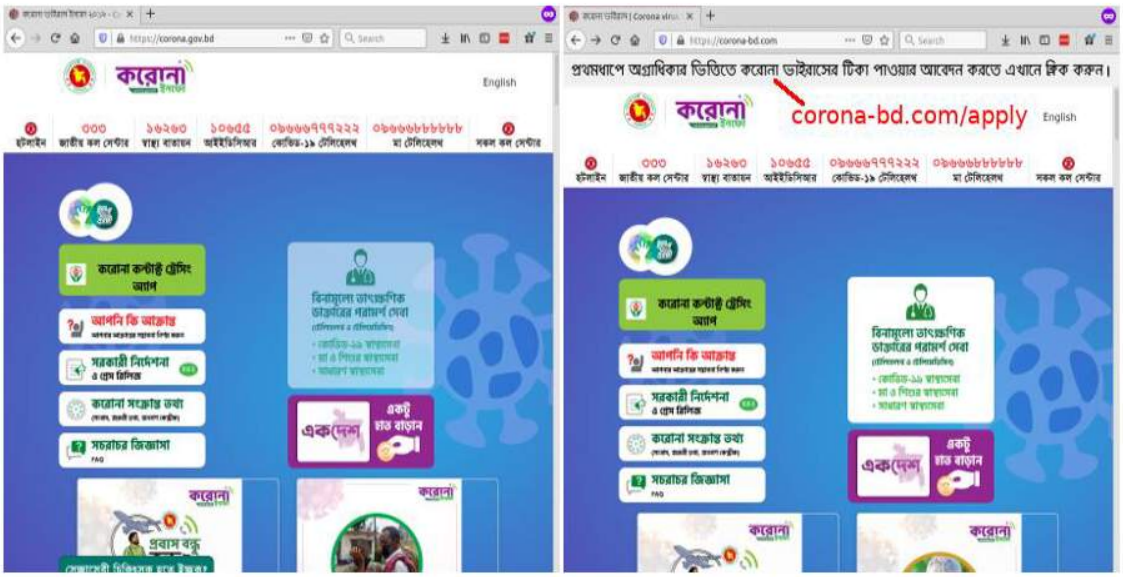


Figure 9: Phishing attack with fake covid-19 vaccine portal

Spam and phishing are two cyberthreats that go hand in hand, while botnets are usually used to deliver them. Targeted attacks usually aim to have financial gain either by delivering ransomware and asking for a ransom to decrypt valuable corporate data or delivering spyware to steal financial information, or to compromise organization's e-mail accounts and perform various types of internal phishing.

The attack vectors for phishing are human element and web and browser-based attacks.

Most targeted industries of phishing attack have a radical change according to the APWG first quarter report of 2021 in comparison with the previous year's 3rd quarter report. It shows that most target of phishing are Financial Institutions and second highest is now social media.

The trend indicates that financial institutions are being the coveted target of the phishing attacks with the increase of around 5% more phishing attack in 2021

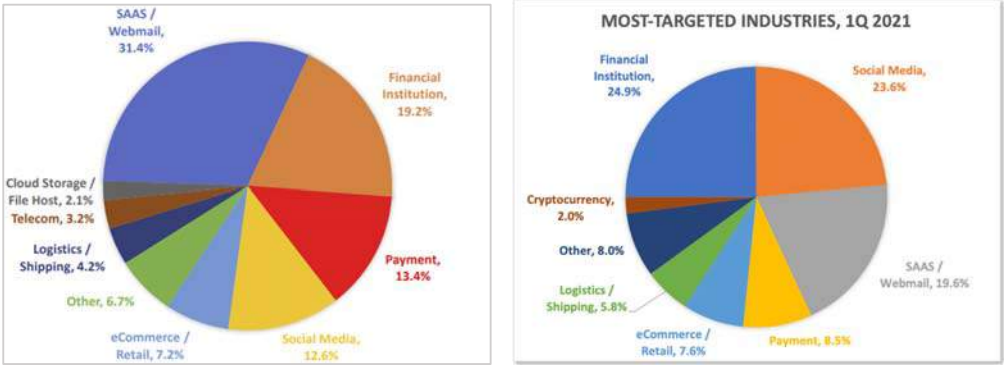


Figure 10: APWG Phishing Activity Trends Report [10]

Primary group of threat agents for phishing are **cyber criminals, insiders, nation.**

2.4 Spam

As nations were fighting their battle with COVID-19, cyber criminals devised new techniques to trick users with convincing SPAM messages. People were desperate to retain their jobs, get vaccinated from trustworthy pharmaceutical companies. This is a well-known psychological trick, because if you take a couple of moments to think about the contents of the spam message, you'll probably realize it's a fake. If the spammer triggers a fear reaction, you act before you think, and you get snared in the trap.[11]

Email flow has changed a lot over the years. There is a huge gap between the large spam runs of the past and the modern email attacks we see today. Today's sophisticated email attacks generally only account for a small

[10] https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf;
[11] https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

percentage of the total email flow within organizations, but they are highly effective – business email compromise (BEC) accounts for over 1% of all traffic but can cost an organization an average of $37,000 per attack.[12]

Cybercriminals are getting better at configuring the attack infrastructure, making it difficult to distinguish between legitimate and weaponized domains – and many attacks likely make it past most traditional email defences.

In September 2021, the average daily spam volume globally was around 88.88 billion, which corresponds to around 84.15% of the total daily email volume[13].

In November 2021, Top 10 Spam sources by country were United States, China, Russian Federation, India, Bulgaria, Brazil, Germany, France, United Kingdom, Poland. **Bangladesh ranked 18th among the spam sources by country** and accounts for 7.2% of world's spam volume.[14]

[12] https://businessinsights.bitdefender.com/defending-against-email-threats-that-dont-involve-malware
[13] https://talosintelligence.com/reputation_center/email_rep#global-volume
[14] https://talosintelligence.com/reputation_center/email_rep#global-volume

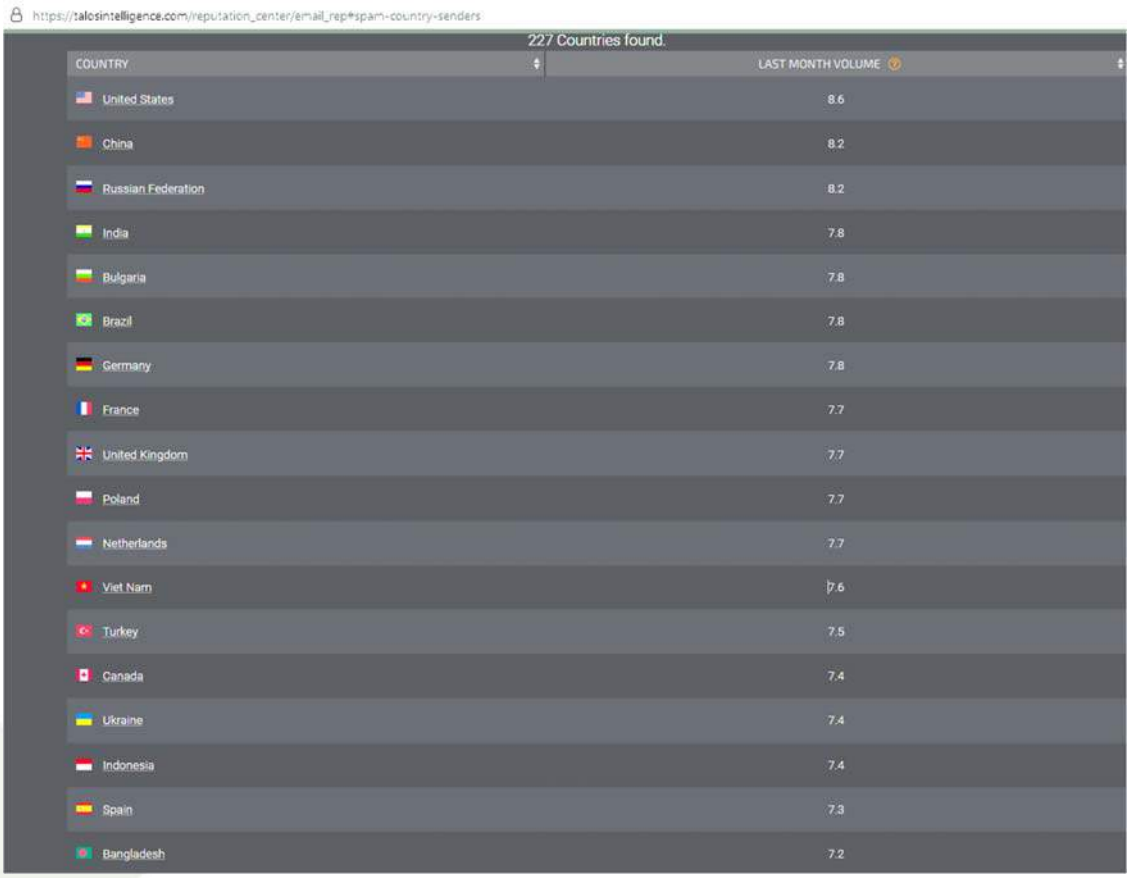


Figure 11: Talos intelligence Email & Spam Data [11]

Most emailed malware consists of simple trojans accompanied by social engineering intended to trick recipients into running them. Still, a significant minority seeks to exploit a vulnerability on the recipient's computer. In 2021, the most commonly encountered exploits in email attachments included the following, in order of prevalence[15] :

[15] https://trustwave.azureedge.net/media/17959/2021-email-threat-report.pdf?rnd=132658400790000000

Exploit	% of exploit encounters	Description
CVE-2018-0802	59.74%	Equation Editor - Microsoft Office Memory Corruption Vulnerability
CVE-2017-11882	35.56%	Equation Editor - Microsoft Office Memory Corruption Vulnerability
CVE-2014-6352	3.02%	Specially crafted Object Linking & Embedding (OLE) object allow remote code execution. Common attack in the wild were crafted Powerpoint document.
CVE-2010-3333	0.59%	Rich Test Format (RFT) Stack Buffer Overflow Vulnerability
CVE-2015-1641	0.41%	Microsoft Office Memory Corruption Vulnerability
CVE-2017-019	0.36%	Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API.
CVE-2014-4114	0.15%	Windows OLE Remote Code Execution Vulnerability
CVE-2015-5119	0.08%	Adobe ActionScript Remote Code Execution
CVE-2020-0674	0.03%	Scripting Engine Memory Corruption Vulnerability
CVE-2020-1214	0.03%	VBScript Remote Code Execution Vulnerability
Others	0.06%	

Figure 92: The most commonly encountered exploits in email attachments

Source: (Trustwave, 2021-email-threat-report) [16]

The global attack vector for spam is a human element, as spam messages target and exploit people to open malicious links or attachments.

Primary group of threat agents for spam is insiders.

2.5 Insider threat

An insider threat is a malicious activity against an organization that comes from users with legitimate access to an organization's network, applications or databases. These users can be current employees, former employees, or third parties like partners, contractors, or temporary workers with access to the organization's physical or digital assets. While the term is most commonly used to describe illicit or malicious activity, it can also refer to users who unintentionally cause harm to the business.[17]

[16] https://trustwave.azureedge.net/media/17959/2021-email-threat-report.pdf?rnd=132658400790000000
[17] https://www.exabeam.com/ueba/insider-threats/

Insiders can carry out their plans via abuse of access rights. The attacker may try what is known as privilege escalation, which is taking advantage of system or application flaws to gain access to resources they do not have permission to access.[18]

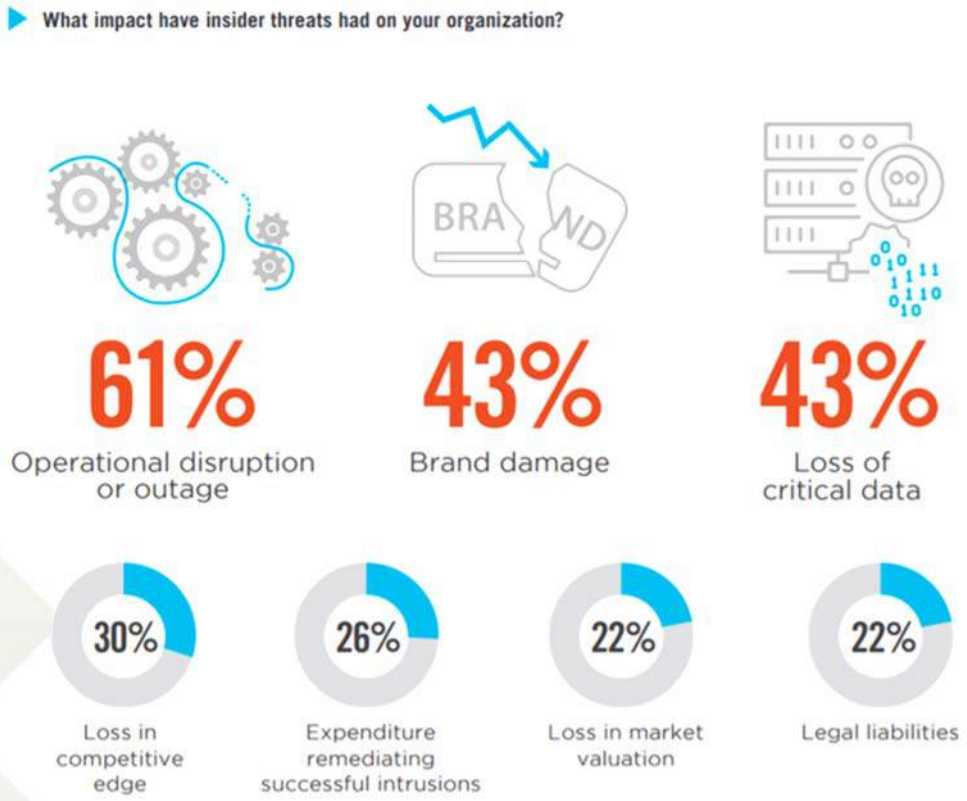


Figure 103: Impact of insider threat in an organization [19]

Primary group of threat agents for insider threat is cyber criminals and corporations.

2.6 Web-based attacks

Cybersecurity attacks have continued to increase in 2021 and their impact was more alarming when all the nations over the world had to struggle with COVID-19 pandemic. Web-based attacks took a spike where availability and

[18] https://www.exabeam.com/ueba/insider-threats/
[19] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

integrity were the target of a plethora of threats and attacks, among which the families of Denial of Service (DoS) and Web Attacks stood out.

Threat intelligence unit of BGD e-GOV CIRT shared the following statistics of top targeted systems of cyber-attacks from November 2020 to November 2021.

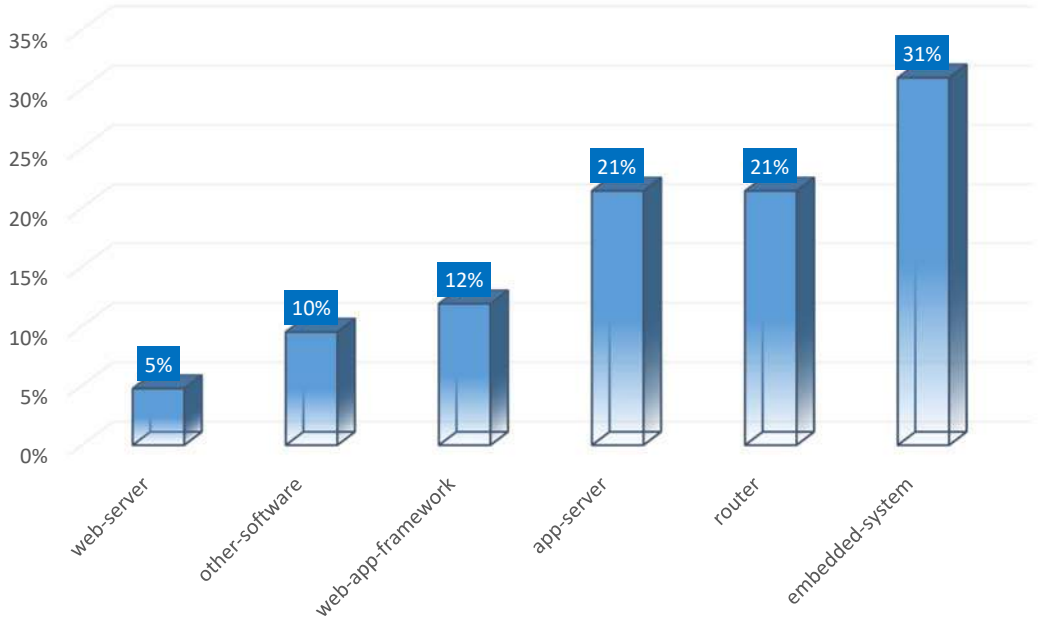


Figure 114: Top targeted system in Bangladesh (Source: BGD e-GOV CIRT)

The statistics clearly shows in total 38% (web-server, web-app-framework, app server) of the attacks was targeted to web-based systems.

It was also being observed that among top 10 attack types http-scan, telnet-brute-force, ssh-brute-force attack types were the most prominent web attacks.

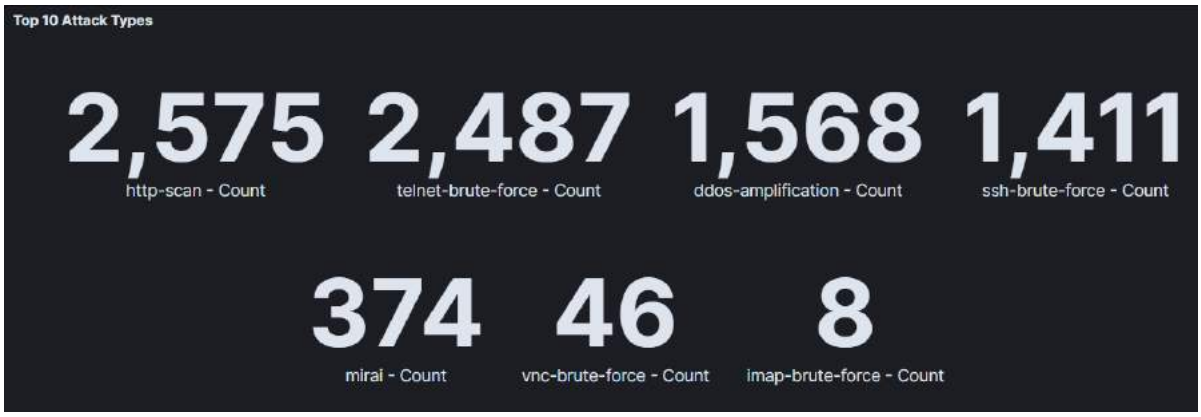


Figure 15: Top 10 attack types in Bangladesh (Source : BGD e-GOV CIRT)

The attack vectors for web-based attacks are internet exposed assets, exploitation of vulnerabilities/ mis-configurations and cryptographic/ network/security protocol flaws and supply chain attacks.

From January 1, 2021, to November 30, 2021, the BGD e-GOV CIRT registered more than 100 web defacement cases. Majority of this Injection attack occurred due to lack of secure coding. BGD e-GOV encourages developers to follow the OWASP Top 10 for secure coding.

Primary group of threat agents for web-based attacks is cyber criminals, nation states, corporations, hacktivists, cyber fighters and cyber terrorists.

2.7 Denial of Services

Denial of service is an attack that prevents or impairs the authorized use of information system resources or services. These types of attacks, especially DDoS, remain an important threat for almost all kind of businesses with an online presence.

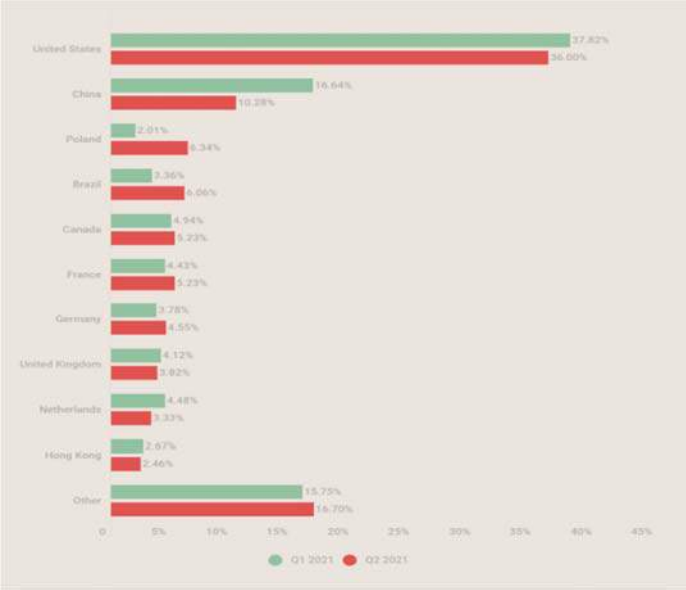


Figure 16: Distribution of DDoS attacks by country Q1 and Q2 2021[20]

The specific attack vectors for Denial of Service attacks are: Portmap/Remote Procedure Call (RPC), Multicast Domain Name System (mDNS), Memcached, SYN flooding, UDP fragments, DNS floods, NTP floods, and CHARGEN attacks.

Looking at the distribution by type of attack, we see that UDP flooding in Q2 significantly increased its slice (60% vs 42% in Q1). SYN flooding (23.67%), which until 2021 was the most common type of DDoS, is fighting to regain lost territory: this quarter it swapped places with TCP flooding (13.42%) to claim second place.[18]

[20] https://securelist.com/ddos-attacks-in-q2-2021/103424/

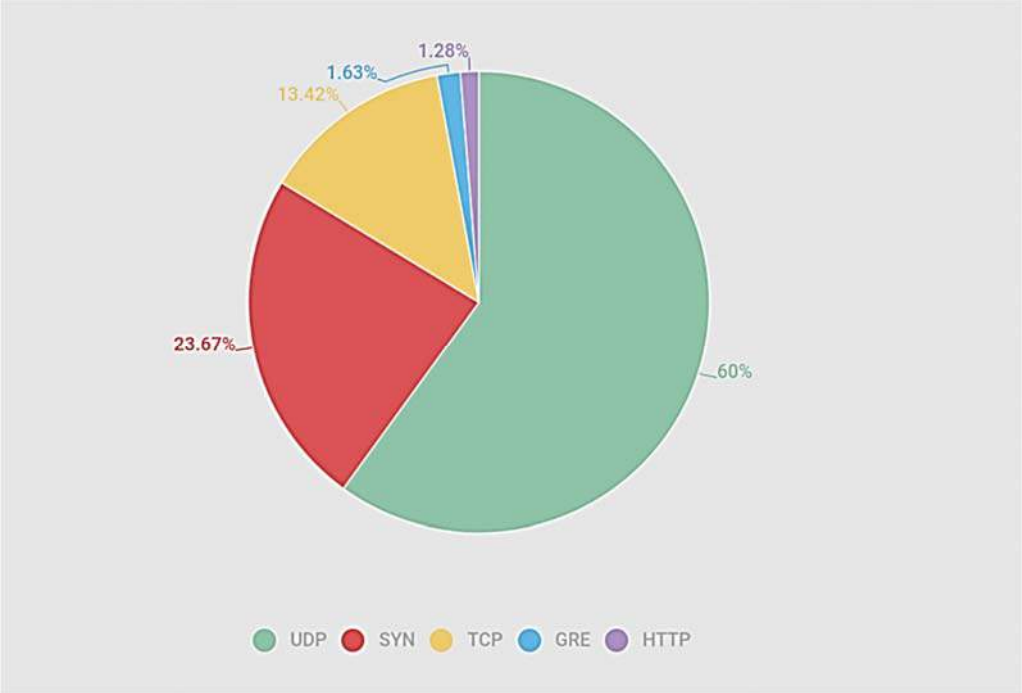


Figure 17: Distribution of DDoS attacks by type, Q2 2021

APAC	%
China	85.96%
Indonesia	3.48%
Thailand	2.72%
Taiwan	2.15%
Malaysia	1.10%
India	0.81%
Vietnam	0.65%
Pakistan	0.60%
Philippines	0.57%
Bangladesh	0.48%
Others (6 Regions)	1.48%

Figure 18: Top 10 Sources in APAC (Asia Pacific) region [21]

[21] https://blog.nexusguard.com/threat-report/ddos-threat-report-2021-q2

2.8 Data breach

Bangladesh may not be seen as an enticing target for influential data breaches in global perspective but the netizens of this country are equally susceptible to all sorts of credential theft, compromise and leak.

Cyber threat intelligence unit of BGD e-GOV CIRT is vigilant to monitor any suspicious dark web activities where user credentials, bank account credentials, login name and passwords which are leaked or being sold.

Besides, on April 4, 2021 a report published by one of the leading newspaper 'Dhaka Tribune' inform that Facebook user data of more than 533 million users from over 100 countries around the world, including Bangladesh, had been leaked online. Out of the total data leaked, 3.8 million users were Bangladeshi.[22]

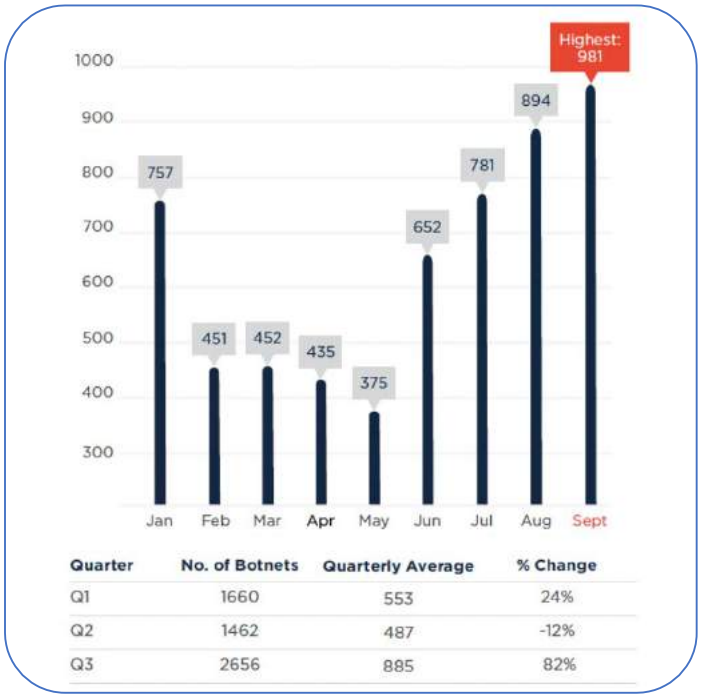
Primary group of threat agents for data breach is cyber criminals, insiders, nation states, corporations, hacktivists and cyber fighters.

2.9 Botnets

Estimates show that by the end of 2021, there will be ten times as many devices as there are people using the Internet. Many of these devices are very limited in resources and often have lots of vulnerabilities that make them easy targets.[23] Botnets are used extensively for Command and Control attacks also called as 'C2' to initiate DDOS attacks and implantation of malware to steal credentials. An increasing number of IoT devices are also exposing the risk of the expansion of botnets.

22 https://www.dhakatribune.com/world/2021/04/04/3-8m-bangladeshi-facebook-users-data-leaked-online

23 https://www.extremenetworks.com/extreme-networks-blog/understanding-the-basic-functions-of-botnets/



Quarter	No. of Botnets	Quarterly Average	% Change
Q1	1660	553	24%
Q2	1462	487	-12%
Q3	2656	885	82%

Figure 19 Source: Spamhaus Botnet Threat Update: Q3-202124

Rank	Country	Q2 2021	Q3 2021	% Change Q on Q
#1	Russia	233	381	64%
#2	United States	281	301	7%
#3	Netherlands	168	273	63%
#4	Mexico	-	182	New Entry
#5	Germany	117	170	45%
#6	France	92	123	34%
#7	Saudi Arabia	-	117	New Entry
#8	Dominican Rep	-	96	New Entry
#9	Brazil	12	86	617%
#10	Korea	-	68	New Entry

Rank	Country	Q2 2021	Q3 2021	% Change Q on Q
#11	Uruguay	-	63	New Entry
#12	Latvia	84	58	-31%
#13	Switzerland	41	55	34%
#14	Argentina	-	50	New Entry
#15	Moldova	29	49	69%
#16	Czech Republic	31	40	29%
#17	United Kingdom	57	39	-32%
#18	Sweden	-	38	New Entry
#19	Vietnam	13	34	162%
#20	Romania	-	33	New Entry

Figure 20 Source: Spamhaus Botnet Threat Update: Q3-2021 [25]

Command and control (C&C) servers like Dridex Malware, TrickBot Malware, Emotet Malware found in Bangladesh.

24 https://www.spamhaus.org/news/article/800/spamhaus-botnet-threat-update-q2-2020

25 https://www.spamhaus.org/news/article/800/spamhaus-botnet-threat-update-q2-2020

The attack vectors for botnets are internet exposed assets and exploitation of vulnerabilities/ misconfigurations and cryptographic/network/security protocol flaws.

2.10 Cyber espionage

Cyber espionage activities are expected to grow due to geopolitical triggers, economic sanctions and strategic national goals. Organized crime syndicates and nations states are creating new techniques and tools to steal intellectual property and secrets and fall within a category of APTs. APTs represent a collection of processes, tools and resources used by certain groups in order to covertly infiltrate specific networks and remain there over a long period of time in order to exfiltrate data or perform other destructive actions. Cyber espionage is attributable to information content security incident class.

Threat actors motivated by financial, political, or ideological gain will increasingly focus attacks on supplier networks with weak cybersecurity programs. Cyber espionage adversaries have slowly shifted their attack patterns to exploiting third-and fourth-party supply chain partners.

Rise of APT groups with ingenious methods and tools have made Bangladesh prone to cyber espionage. Threat intelligence unit of BGD e-GOV CIRT found more attack vectors and new APT groups targeting different critical sectors this year. In February, **LodaRAT** a variation of familiar AutoIT malware LODA (win.loda) got in the radar which was a well-known campaign conducted by threat actor **KASABLANKA.** The attackers appeared to have a specific interest in Bangladesh-based organizations, including banks and carrier-grade voice-over-IP (VoIP) software vendors. This variant has the ability to access and record the microphone and web camera of the targeted device. Furthermore, this specific malware will ‘unpack’ itself quietly to the AppData’directory, which is a deep system folder. Though previously, LodaRAT was able to infect

windows-based system by exploiting remote access functionality, but in this campaign it evolved with capabilities of compromising android devices along with windows machines.

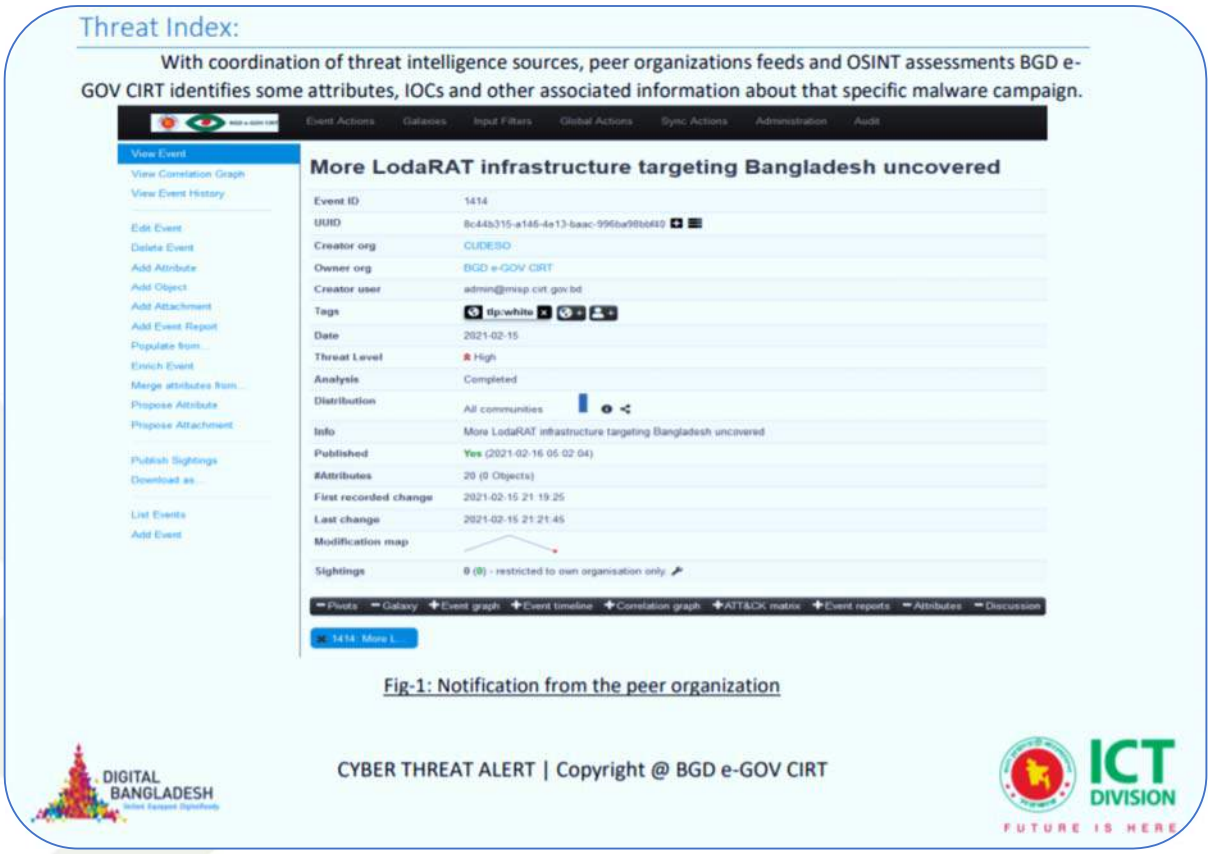


Fig 21: Detection of LodaRat [26]

Last quarter of the year was action-packed as the activities of **APT-C-61** was published. This group was found to use harpoon emails and social engineering methods to infiltrate, spread malicious programs to target devices, secretly control the target devices, and continue to steal sensitive files on the devices.

[26] https://www.cirt.gov.bd/wp-content/uploads/2021/02/LodaRAT-BD-CAMPAIGN-Threat-Report_v2.pdf

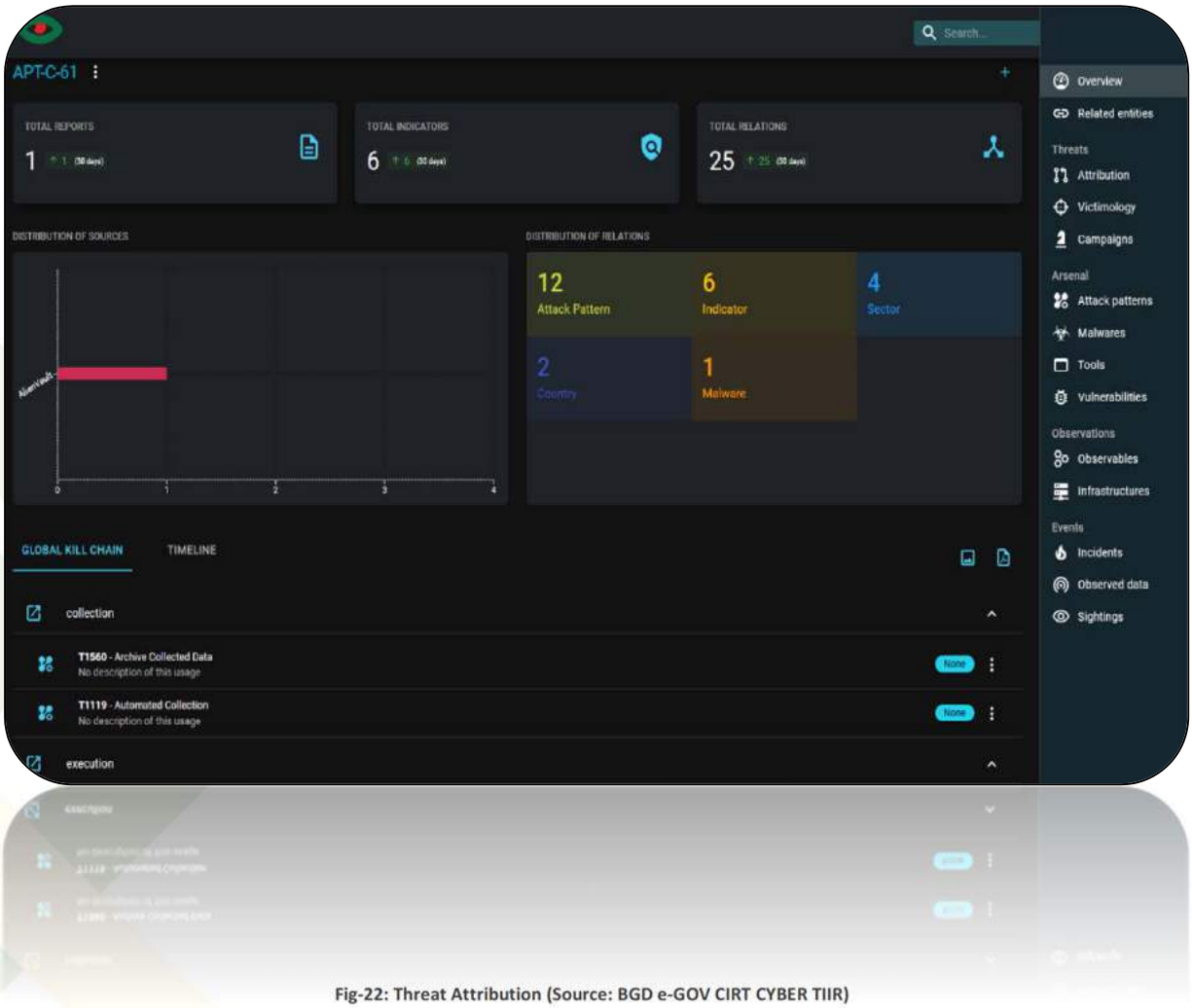


Fig-22: Threat Attribution (Source: BGD e-GOV CIRT CYBER TIIR)

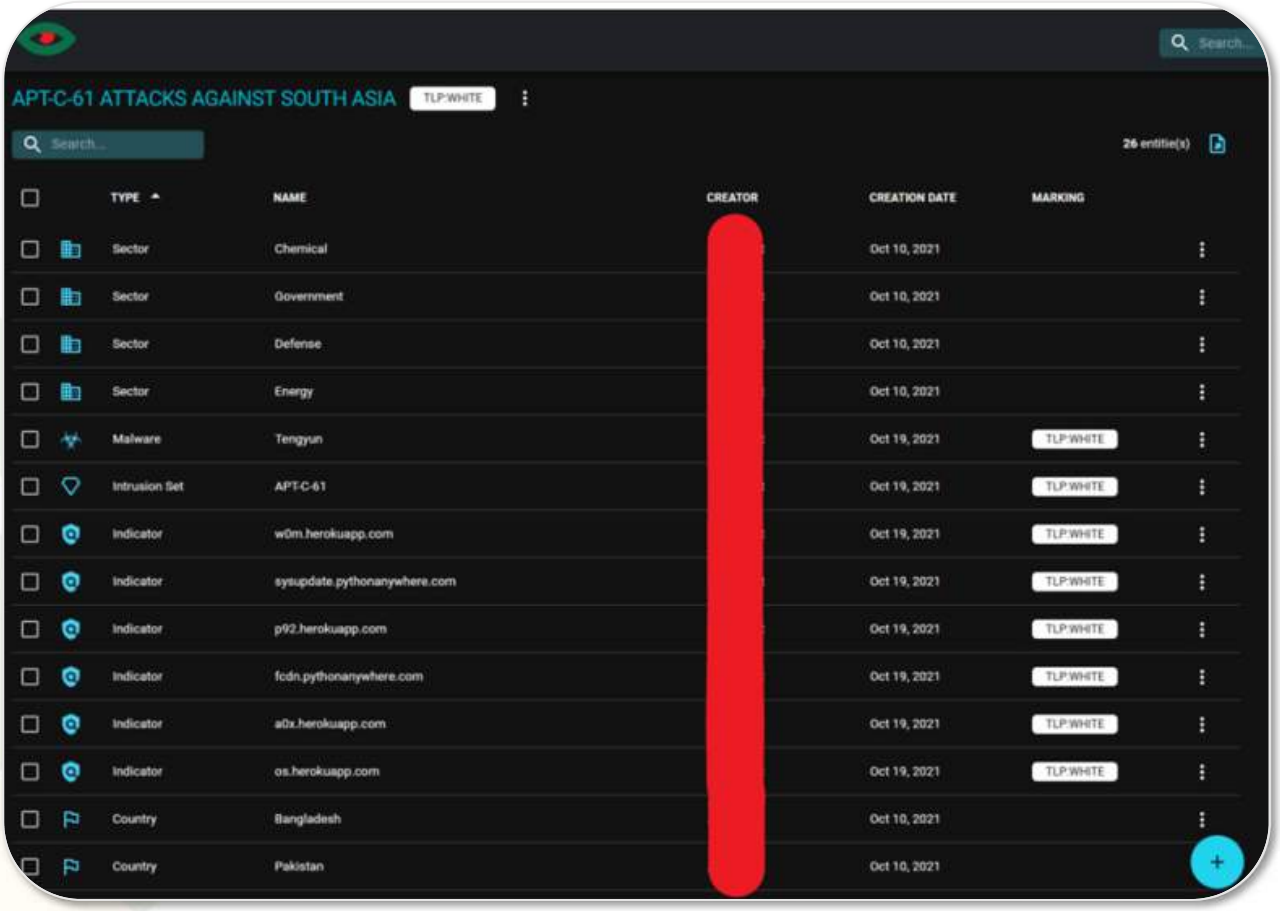


Fig-23: Threat Attribution (Source: BGD e-GOV CIRT CYBER TIIR)

Primary group of threat agents for cyber espionage is **nations states and corporations.**

Known Top Exploited Vulnerabilities in Bangladesh Perspective:

CVE-2021-44228: Critical Apache Log4j Vulnerability

A critical remote code execution vulnerability in the popular Apache Foundation Log4j library has been disclosed. Apache Log4j2 <=2.14.1 JNDI features used in the configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints.

It could allow an attacker to completely take control of an affected server.

It can be leveraged in default configurations by an unauthenticated remote attacker to target applications that make use of the Log4j library. This vulnerability, tracked as CVE-2021-44228, received a CVSS severity score of a maximum 10.0, and is widely believed to be easy to exploit.

Microsoft Exchange Server Remote Code Execution Vulnerability

CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange which allowed the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.

CVE-2021-26857 is an insecure deserialization vulnerability in the Unified Messaging service.

CVE-2021-26858 is a post-authentication arbitrary file write vulnerability in Exchange.

CVE-2021-27065 is a post-authentication arbitrary file write vulnerability in Exchange.

Windows Print Spooler Remote Code Execution Vulnerability

CVE 2021-1675: A vulnerability that allows an attacker with low access privileges to use a malicious DLL file to escalate privilege. Threat actors can only take advantage of the vulnerability if they have direct access to the vulnerable system, so Microsoft categorized it as low-risk. The June 2021 Security Updates included a successful patch for CVE 2021-1675.

CVE 2021-34527: A remote code execution (RCE) vulnerability that allows threat actors to remotely inject DLLs. Microsoft rated CVE 2021-34527 as 8.8 out of 10 on the Common Vulnerability Scoring System Scale.

Microsoft Office Memory Corruption Vulnerability

CVE-2017-11882: A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory.

An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user.

Blue Keep Vulnerability

CVE-2019-0708: A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

MS15-034 Remote Code Execution Vulnerability

The MS15-034 vulnerability could allow remote code execution if an attacker sends a specially crafted HTTP request to an affected Windows system.

Microsoft Windows SMB Server (MS17-010) Vulnerability

Microsoft Windows SMB Server is prone to a remote code-execution vulnerability. Successful exploits will allow an attacker to execute arbitrary code on the target system. Failed attacks will cause denial of service conditions.

Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability

CVE-2020-0796: A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

Fortinet Path Traversal Vulnerability

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.

IPMI Vulnerability

CVE-2013-4786: The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the HMAC from a RAKP message 2 response from a BMC.

Outdated router OS usage in network:

During various Cyber audit engagement BGD e-GOV CIRT also detect outdated router OS version in network device for various vendor equipment, which also introduce vulnerabilities into the network.

BANGLADESH CYBER THREAT LANDSCAPE

Powered by

CYBER TIIR [Threat Intelligence & Incident Research]
A unit of BGD e-GOV CIRT