YEAR 2022

BANGLADESH CYBER THREAT LANDSCAPE

ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP : GREEN

BANGLADESH CYBER THREAT LANDSCAPE 2022

978-984-35-4011-9

PLANNING AND GUIDANCE

Tarique M Barkatullah
Director (Data Center), Director (CA & Security) and Project Director (BGD e-GOV CIRT)
Bangladesh Computer Council

EDITORIAL PANEL

Tawhidur Rahman
PCSS, EnCE, CECFE, ACE, SCCISP, CFip, CCTA, CIMP, 3CIA, 3CI, 3CE
CISO and Senior Technical Specialist (Digital Security), BGD e-GOV CIRT

Mohammad Farhad Hussain
Senior Technical Specialist (Infrastructure), BGD e-GOV CIRT

LEAD RESEARCHER

MD Samiul Islam
GIAC GSOC, WCNA, MITRE ATT&CK Defender (CTI, SOC assessment, Adversary Emulation), BelkaCE, DetegoDFE, CCNA, JNCIA, RHCE
Incident Helpdesk Associate, BGD e-GOV CIRT

Mohammad Makchudul Alam
GIAC GSOC, CEH, ISO 27001 LI, MITRE ATT&CK Defender (CTI, SOC assessment & Adversary Emulation)
Incident Handler, BGD e-GOV CIRT

CO-OPERATION

Sabrein
System & Website Administrator, BGD e-GOV CIRT

Khondker Aminul Islam
PMP, ISO 27001 ISMS LA, PRINCE2, ISO 27701 PIMS LI, Agile-SCRUM
Marketing & Business Specialist, BGD e-GOV CIRT

CONTENTS

Sharing Indicator

TLP definitions (FIRST - https://www.first.org/tlp/)

Community: Under TLP, a *community* is a group who share common goals, practices, and informal trust relationships. A community can be as broad as all cybersecurity practitioners in a country (or in a sector or region).

Organization: Under TLP, an *organization* is a group who share a common affiliation by formal membership and are bound by common policies set by the organization. An organization can be as broad as all members of an information sharing organization, but rarely broader.

Clients: Under TLP, clients are those people or entities that receive cybersecurity services from an *organization*. Clients are by default included in TLP:AMBER so that the recipients may share information further downstream in order for clients to take action to protect themselves. For teams with national responsibility this definition includes stakeholders and constituents.

a. TLP:RED = For the eyes and ears of *individual* recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

b. TLP:AMBER = Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*. Note that TLP:AMBER+STRICT restricts sharing to the *organization* only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP:AMBER+STRICT.

c. TLP:GREEN = Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

d. TLP:CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure. Sources may use TLP:CLEAR 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:CLEAR information may be shared without restriction.

Abbreviations

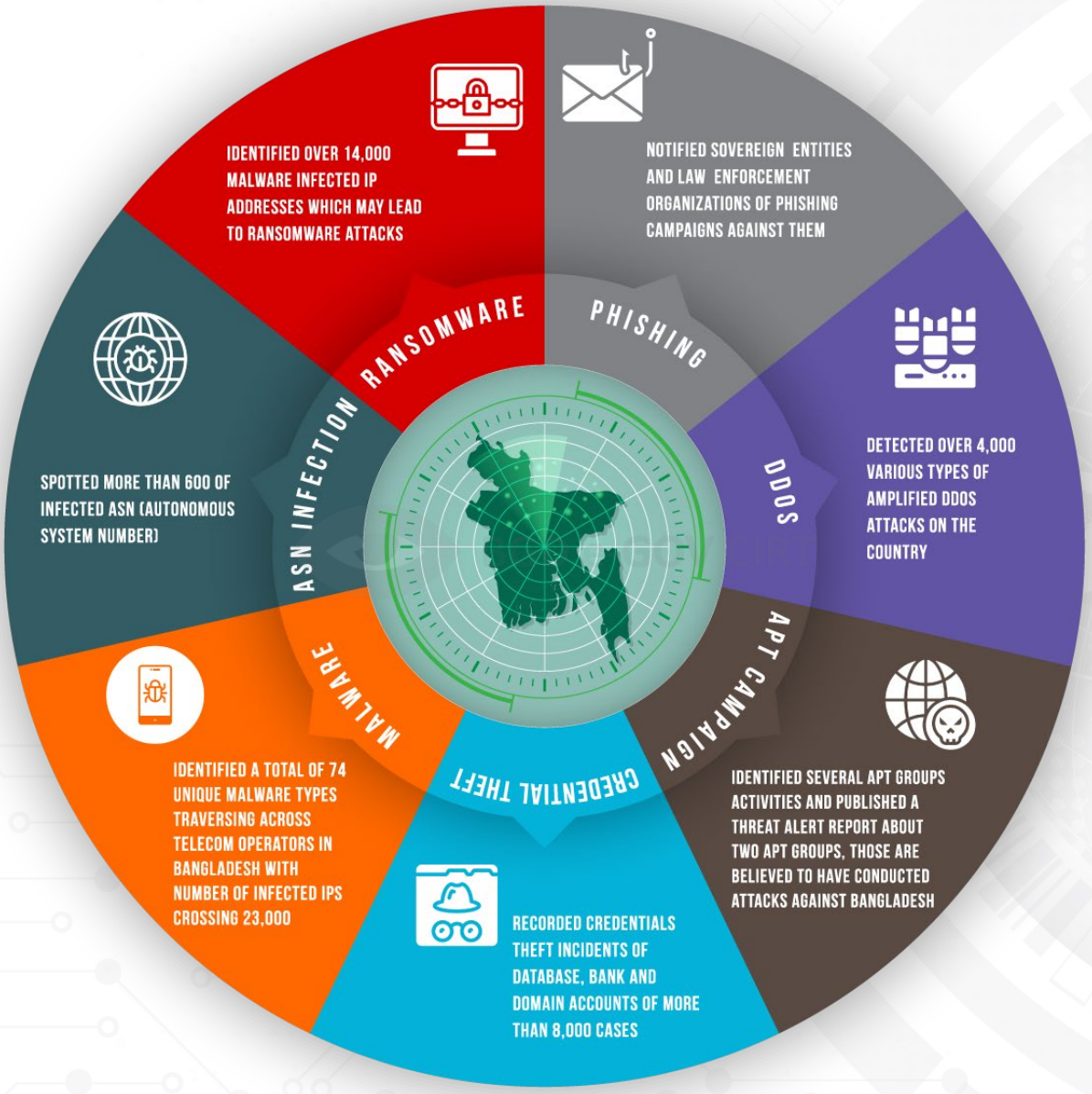
APT	Advanced Persistent Threat
APWG	Anti-Phishing Working Group
ATT&CK	Adverserial Tactics Techniques and Common Knowledege
CII	Critical Information Infrastructure
CIRT	Computer Incident Response Team
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DoS	Denial of Service
ENISA	European Union Agency for Network and Information Security
HTTP	Hypertext transfer protocol
IOC	Indicator of Compromise
Q	Quarter
RDP	Remote Desktop Protocol
RaaS	Ransomware-as-a-Service
SOC	Security Operation Centre

Introduction

Securing the cyberspace of Bangladesh is becoming more challenging as a result of the ripple effect of the ongoing geopolitical challenges. The world economy started to recover from the severe impact of the pandemic but it got embroiled again with conflicts in Europe and Middle-east. The conflicts also have spill-over effect in cyberspace. Threat actors including nation states, activists, hacker groups etc. are using destructive malwares and causing major disruptions and repercussions to global IT networks and infrastructures. Bangladesh is also experiencing the effects of global cyberwarfare and several threat alerts have been issued by BGD e-GOV CIRT for government and law enforcement agencies in 2022.

BGD e-GOV CIRT identified unique cyber attacks targeting government, financial, military, industrial, trade and commerce, healthcare, start-up and innovation, energy sectors of Bangladesh. BGD e-GOV CIRT published sectoral reports, horizon scanning reports, and organization specific reports to alert, deter and respond to possible cyber attacks.

This year's threat landscape report consists of both global and local statistics relevant to different cyber threats. Major observations for this year are as follows-



Ransomware

GLOBAL RANSOMWARE TRENDS IN 2022

In recent years, ransomware attacks have risen exponentially. Due to the insolent scope of ransomware attacks, victims suffer severe impacts. Every 11 seconds, a new ransomware attack hits businesses, healthcare providers, government entities, financial services, and individuals[1]. More criminals are being lured to the trillion-dollar cybercrime market by double extortion and ransomware as a service (RaaS).

Ransomware state of Bangladesh,2022[2] published by BGD e-GOV CIRT highlighted some global ransomware trends and statistics which are as follows-

- Every year ransomware attacks cause an estimated loss of $1 billion (equivalent to approximately one thousand crore BDT) for victim organizations and individuals.[3]
- Businesses suffer ransomware attacks every 40 seconds.[3]
- Phishing emails are the cause of two-thirds of ransomware infections.[3]
- Recovering from a ransomware attack cost businesses $1.85 million (Around 20 crore BDT) on average in 2021.[4]
- Out of all ransomware victims, 32 percent pay the ransom, but they only get 65 percent of their data back.[3]
- Only 57 percent of businesses are successful in recovering their data using a backup.[4]

High-profile ransomware incidents over the past two years, like those impacting critical infrastructure, the healthcare industry, and IT service providers, have garnered a lot of public attention.

[1] https://lookingglasscyber.com/resources/white-papers/2022-state-of-ransomware-white-paper/
[2] https://shop.cirt.gov.bd/product/ransomware-landscape-bangladesh-2022/
[3] https://www.cloudwards.net/ransomware-statistics/
[4] https://dataprot.net/statistics/ransomware-statistics/

The largest manufacturer of semiconductor chips in the world fell victim to a ransomware attack in February 2022. The company confirmed that the threat actor had started posting employee login details and confidential data online. Lapsus$, a ransomware organization, claimed responsibility for the attack and said it had access to 1TB of stolen corporate data that it planned to post online. Additionally, it requested $1 million (Around 10 crore BDT) as well as a portion of an unspecified fee from Nvidia[5].

Among many other ransomware incidents, Microsoft Digital Defense Report 2022 published the following example attacks which came to the limelight –

- In February, an attack on two companies affected the payment processing systems of hundreds of gas stations in northern Germany.[6]
- In March, an attack against Greece's postal service temporarily disrupted mail delivery and impacted the processing of financial transactions.[7]
- In late May, a ransomware attack against Costa Rican government agencies forced a national emergency to be declared after hospitals were shut down and customs and tax collection disrupted.[8]
- Also in May, an attack caused flight delays and cancellations for one of India's largest airlines, leaving hundreds of passengers stranded.[9]

SonicWall Cyber Threat report illustrates after two straight years of increase, ransomware volume peaked in Q2 2021 at 188.9 million USD (Around 200 crore BDT). This was already sufficient to raise ransomware to a new annual high when combined with Q1.

[5] https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
[6] https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
[7] https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
[8] https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
[9] https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/

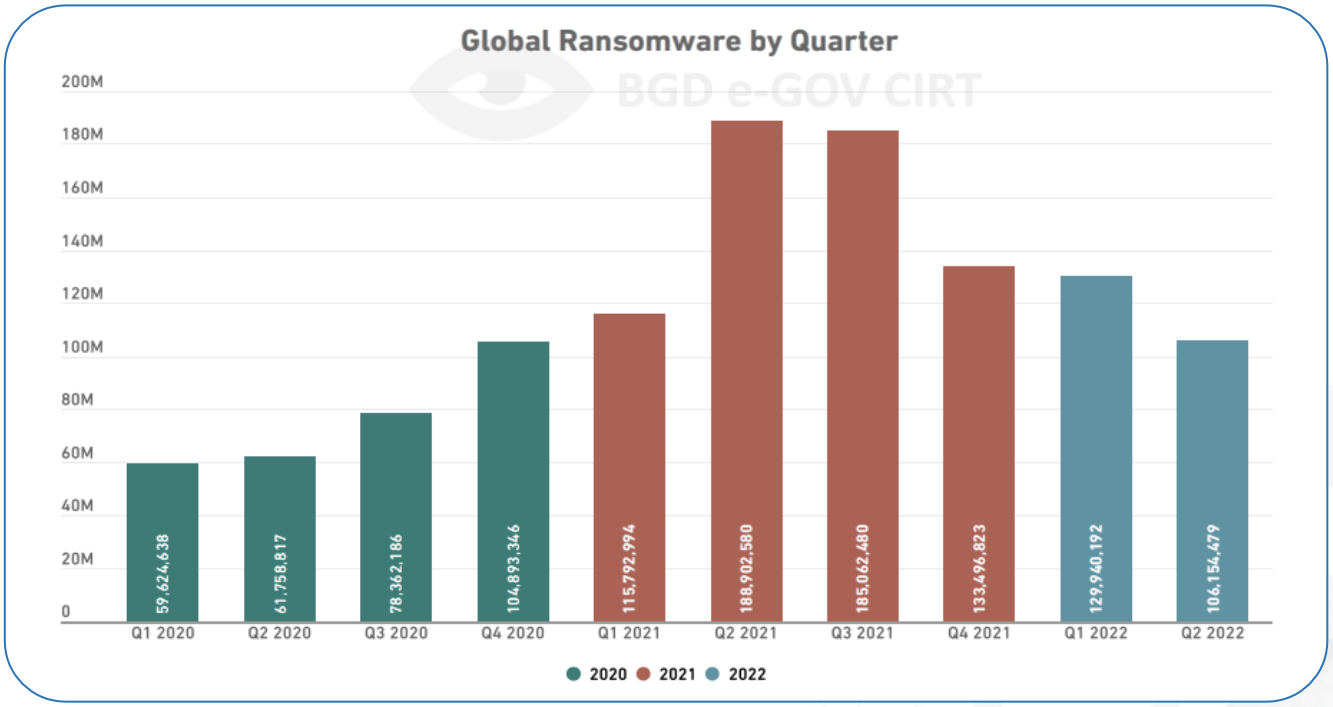


Figure 1: Global ransomware by quarter[10]

Fortunately, though, Q3 and Q4 started on a decreasing trend that has continued into this year. However, June 2022's very low ransomware total was another reason why Q2 was significant. Just 23.8 million ransomware hits were detected that month according to SonicWall analysts, which is the lowest amount in 23 months and a drop of over 45% from the already low levels observed the month before.

[10] https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf

ACTIVE RANSOMWARE STRAINS

Although there is a myriad of ransomware out there, BGD e-GOV CIRT only focused on the ones which are found to have active footprints at the time of preparation of the Ransomware state of Bangladesh,2022 report. The following diagram depicts current strains of active ransomware-

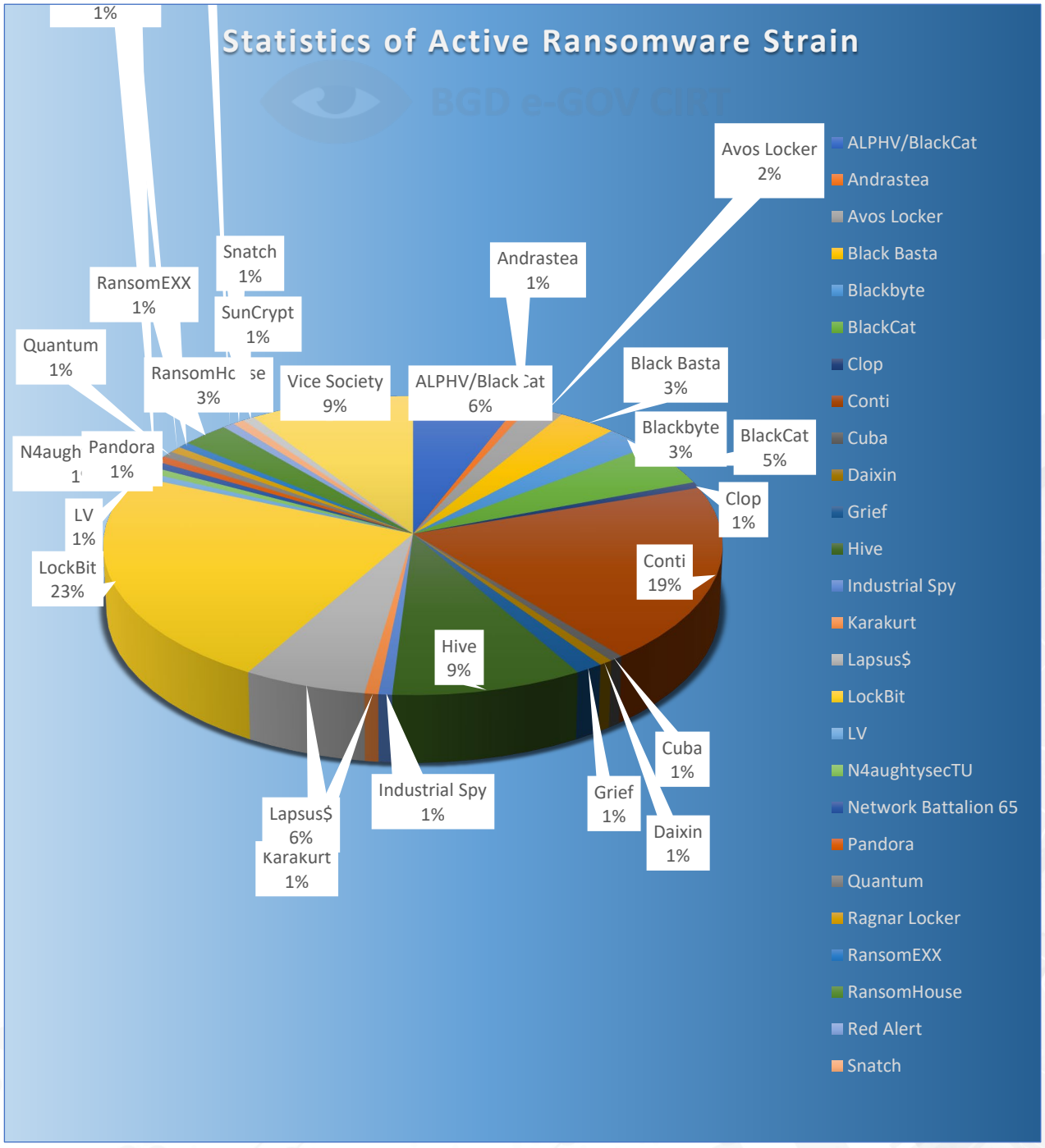
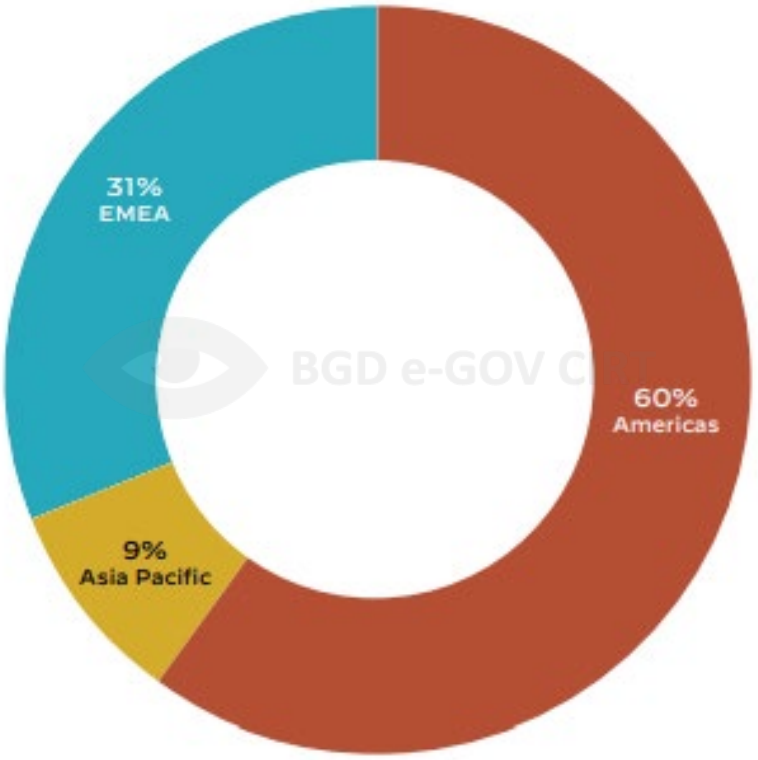


Figure 2: Active ransomware strain[11]

[11] https://shop.cirt.gov.bd/product/ransomware-landscape-bangladesh-2022

THE SPREAD OF GLOBAL RANSOMWARE

Impacted regions and countries (Focused in Asia Pacific Regions)



- According to leaked site data, the Americas area was the most heavily impacted by ransomware attacks in 2021, followed by EMEA and Asia Pacific.[12]
- Check Point Research (CPR) has revealed a staggering 168% year on year increase in the number of cyberattacks in Asia Pacific (APAC) when compared to May 2020. The malware types that showed the largest increase are ransomware and Remote Access Trojan (RAT), both of which increased by 26% in May 2021 compared to earlier this year.[13]

[12] https://lookingglasscyber.com/resources/white-papers/2022-state-of-ransomware-white-paper/
[13]https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/

Ransomware Trends in Bangladesh 2022

Although Asia pacific covers only 9% of the targeted countries for ransomware[14], Bangladesh could not evade the grip of such emerging threats. Victim shaming is the greatest fear factor for organizations in Bangladesh which discourage them from reporting any incident to the national incident response team. Despite efforts to raise awareness about reporting any type of incidents, especially ransomware, gathering reliable data to build a comprehensive threat landscape remains a difficult task.

"Ransomware state of Bangladesh,2022"[15] delivered some key insights-

[14] https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf
[15] https://shop.cirt.gov.bd/product/ransomware-landscape-bangladesh-2022

MALWARE INFECTIONS PERTINENT TO RANSOMWARE ATTACK

The BGD e-GOV CIRT discovered malware infection variants linked to known and likely ransomware Infection chains within the time period taken in to account for this analysis.

Since 2021, around **14,627** unique count of IP addresses originated from Bangladesh are found to be infected with malware which can be mapped to possible ransomware attack vectors.

These infections are found to be linked with potential ransomwares and some of them are part of growing botnets as well.

Malware Infection	Relevant Ransomware Threat	Total infection events
m0yv	Maze	6994
Necurs (Botnet)	Locky	5083
Trik,phorpiex (Botnet)	Avaddon	2683
wannacrypt	Wannacry	812
osiris	Locky	9
cobalstrike	Lockbit,Ryuk	4
cryptowall	Cryptowall	2
ryuk	Ryuk	2
Soidonikibi	Revil/Conti	2

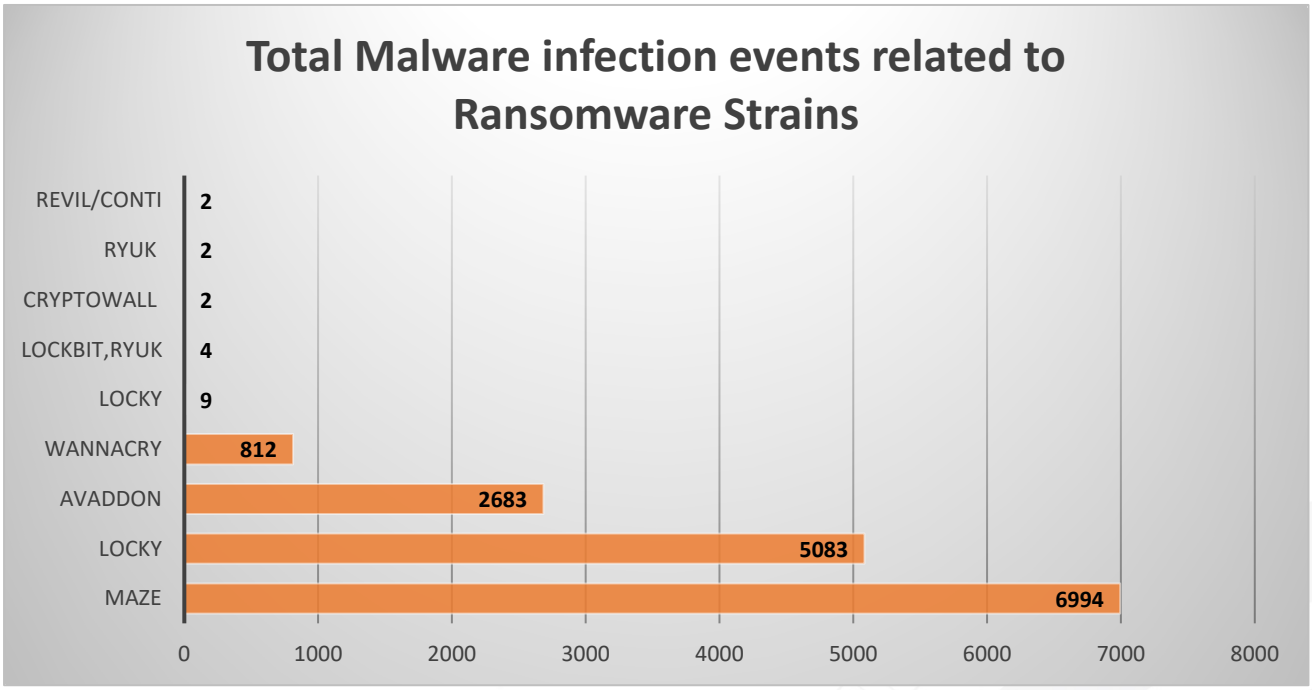


Figure 3: Relevant malware infection for a possible ransomware attack[16]

General Infection Statistics

The ten unique malwares which are identified in the previous section found to have infected **14,627** unique source IP addresses which originated from Bangladesh.

[16] https://shop.cirt.gov.bd/product/ransomware-landscape-bangladesh-2022

A significant amount of communication events were found where the destination host is a well-known IOC for **Wannacry ransomware.**

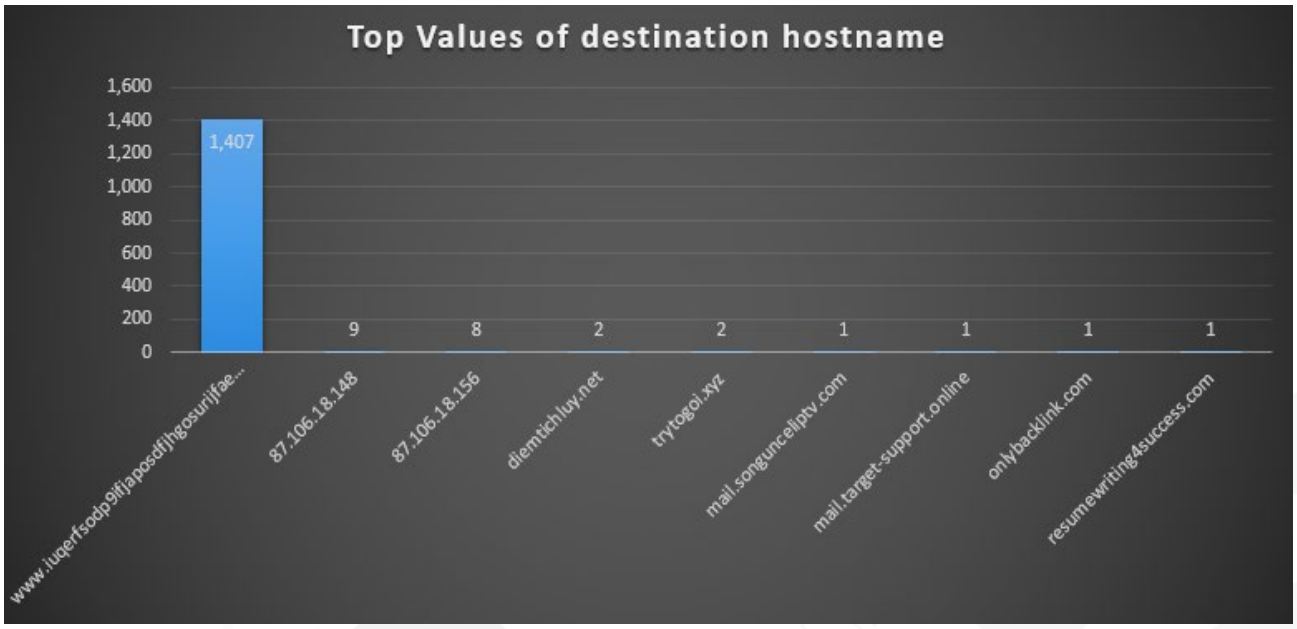


Figure 4: Top values of malicious destination hostname[17]

Phishing

Phishing remains a popular technique for attackers to conduct their malicious activities, and despite awareness-raising campaigns and exercises, users still fall for this trick[18]. Over the past year, the number of detected phishing emails has increased dramatically as a result of ongoing conflicts in Europe and Middle-east. Phishers are now more reliant on operating their phishing campaigns from legitimate infrastructures without the need to purchase or host them on their own.

Global Trends and statistics

- A new record and the worst quarter for phishing have ever been observed 1,097,811 total phishing attacks in the second quarter of 2022. [19]

[17] Threat intelligence unit of BGD e-GOV CIRT
[18] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[19] https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf

Figure 5: Global Phishing attack trends for 3Q2021- 1Q2022

- The median time it takes for an attacker to access your private data if you fall victim to a phishing email is one hour and twelve minutes, while it takes one hour and forty-two minutes for an attacker to begin moving laterally within your corporate network once a device is compromised.[20]

- Cyber attackers leveraged the Russia-Ukraine conflict in multiple phishing and cryptocurrency Spam Campaigns. Victims received emails with Russia-Ukraine conflict-themed subject lines with links leading to pages with donation requests and easy payment methods.[21]

"Phishing Activity Trends Report"[22] published by APWG narrated some key observations for 2022 which are mentioned below-

- The financial sector is the most-targeted industry sector followed by webmail/SAAS and social media. In Q2 an overall 43 percent increase in phishing was detected compared to Q1 2022.

[20] https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022
[21] https://www.phishprotection.com/blog/phishing-trends-2022/
[22] https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf

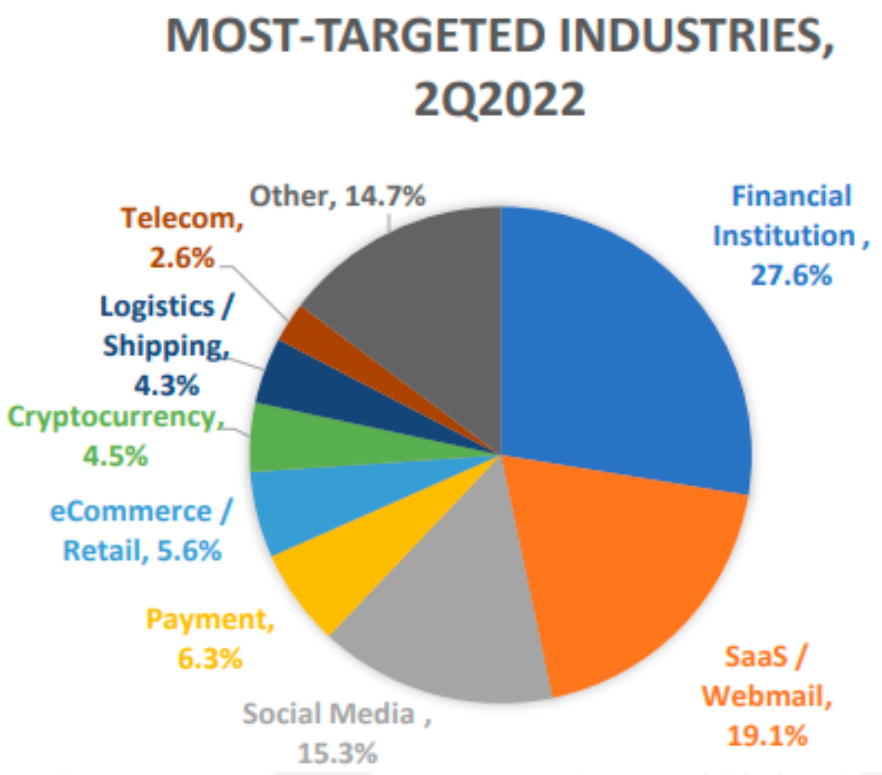


Figure 6: Targeted industries by phishing attacks in 2nd quarter of 2022

- Almost all global regions saw a net decrease in the number of phishing enabled ransomware victims identified in those regions except the APAC region, which saw a 31 percent increase in ransomware victims in the second quarter. The top industries impacted by ransomware were manufacturing, business services, retail and wholesale firms, and the healthcare sector.
- Phishing emails leveraging social media platforms through impersonation and fraud are the top two threats, accounting for three out of every four social media attacks.
- There has been an increase in mobile phone-based fraud, with smishing and vishing collectively seeing a nearly 70 percent increase in volume as compared to Q1 totals.
- Business E-mail Compromise (BEC) has caused aggregate losses in the billions of dollars, at large and small companies. BEC is a response-based spear phishing attack that involves the impersonation of a trusted party (a company executive, vendor, etc.) to trick a victim into making a financial

transaction or sending sensitive materials. 73 percent of BEC attacks in Q2 2022 were launched using a free webmail address such as Google, Microsoft Outlook, and Virgin Media.

- Back From the Dead, Emotet Returns in 2022. It re-emerged in Q4 of 2021 and started making waves with reports of massive phishing campaigns targeting Japanese businesses in February and March of 2022 and several massive new malicious phishing campaigns in April and May targeting new regions.[23]
- A huge phishing campaign nicknamed "0ktapus" has targeted over 130 companies, affecting Twilio and Signal. Login credentials belonging to nearly 10,000 individuals were stolen by attackers who imitated the popular single sign-on service Okta.[24]

Phishing trends in Bangladesh

Several phishing sites and campaigns were found to target various sectors of Bangladesh. The most targeted site was the national covid-19 vaccination site.

Phishing sites for Surokkha
https://surokkha[.]gov-bd[.]verify-online[.]quest/
https://www[.]surokkha[.]com[.]bd[.]verify-online[.]icu/
https://www[.]surokkha[.]com[.]bd[.]verify-online[.]icu
http://surokkha-gov-bd[.]quest
https://surokkha-gov-bd[.]quest
https://surokkha-gov-bd[.]quest/
https://www[.]surokkha[.]com-bd[.]foreigner-everify[.]quest/
https://www[.]surokkha[.]com-bd[.]foreigner-everify[.]quest
https://www[.]surokkha[.]gov[.]bd[.]verify-online[.]site/
https://www[.]surokkha[.]gov[.]bd[.]verify-online[.]site
https://www[.]surokkha[.]gov[.]bd[.]foreigner-everify[.]space/
https://www[.]surokkha[.]gov[.]bd[.]verify-online[.]icu/

[23] https://www.deepinstinct.com/blog/emotet-malware-returns-in-2022

[24] https://www.theverge.com/2022/8/26/23323036/phishing-scam-campaign-twilio-hack-companies

https://www[.]surokkha[.]gov[.]bd[.]verify-online[.]icu
http://surrokkha-gov-bd[.]store
https://surrokkha-gov-bd[.]store
https://app-surakkha-gov[.]bd-up[.]com
http://app-surakkha-gov[.]bd-up[.]com
https://surokkha[.]gov[.]bd-ok[.]xyz
http://surokkha[.]gov[.]bd-ok[.]xyz
http://surokkha[.]gov[.]bd[.]liont[.]site
https://surokkha[.]gov[.]bd[.]liont[.]site
https://www[.]surokkha[.]gov[.]bd[.]verify-online[.]asia/
https://www[.]surokkha[.]gov[.]bd[.]verify-online[.]asia

Table: Phishing sites targeting national COVID-19 vaccination portal of Bangladesh[25]

Figure 7: Phishing login page for https://surokkha[.]gov[.]bd-ok].]xyz[26]

[25] Threat Intelligence unit of BGD e-GOV CIRT
[26] Threat intelligence unit of BGD e-GOV CIRT

Mail service domains of all three wings of Bangladesh Armed Forces along with Law Enforcement organizations were targeted with phishing campaign.

Organization	Original Domain	Phishing URL/Domain
Bangladesh Armed Forces	mail.afd.gov.bd	mailafd-govbd-signin-true. *.com
Bangladesh Navy	mail.navy.mil.bd	mail-navy-mil-bd-loginhjdh. *
Bangladesh Defense Command and Staff College	mail.dscsc.mil.bd	mail-dscsc-mil-bd. *.app
Bangladesh Air Force	mail.baf.mil.bd	https://*.github.io/mail.baf.mil.bd /index.html
Rapid Action Batallion	www.rab.gov.bd	rab-gov-bd.gq

Table: Phishing campaign against military organizations of Bangladesh[27]

[27] https://mp.weixin.qq.com/s/CGHDuJAb4dav_th25yYpWA

Cyber Threat Intelligence Unit of BGD e-GOV CIRT verified and found true positives for the reported phishing links.

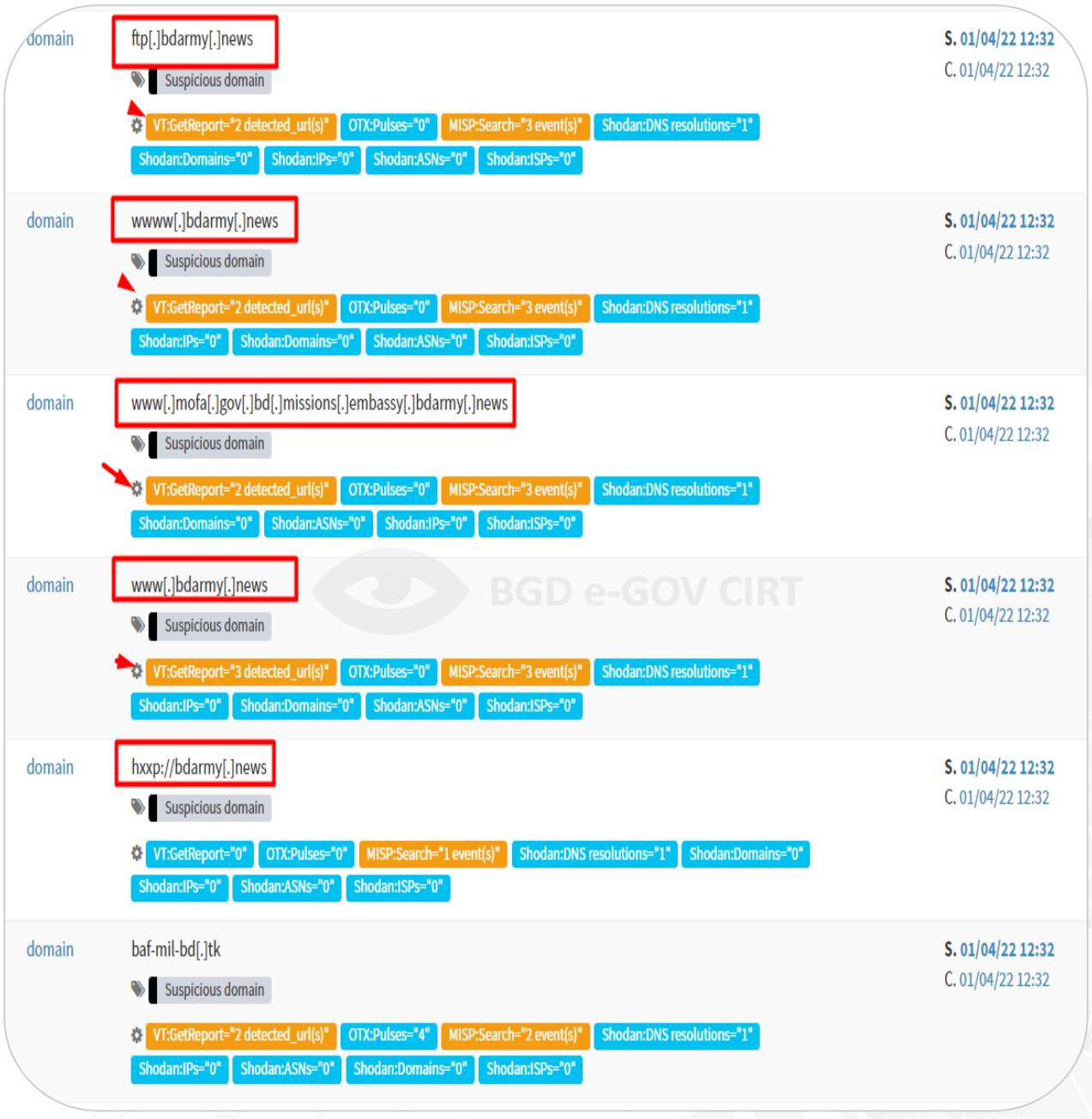


Figure 8 : IOC verification by the Threat Intelligence Unit of BGD e-GOV CIRT

Another phishing campaign was reported from a Twitter handle of the CEO, DarkTracer on March,2022

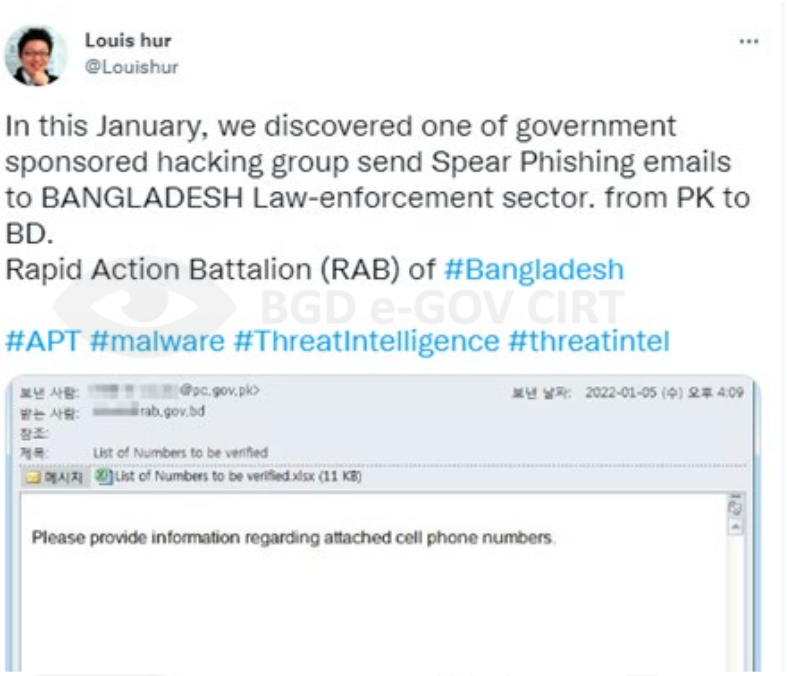


Image Source: https://twitter.com/Louishur/status/1503372969921609729

Phishstats, a real time phishing statistics and database provider reported a phishing site emulating one of the university admission portal of Bangladesh on May,2022.

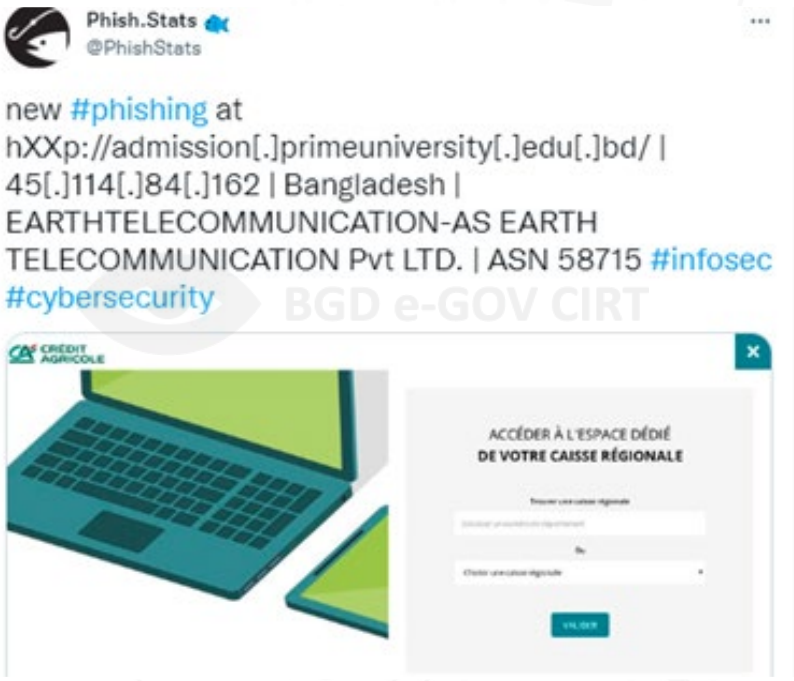
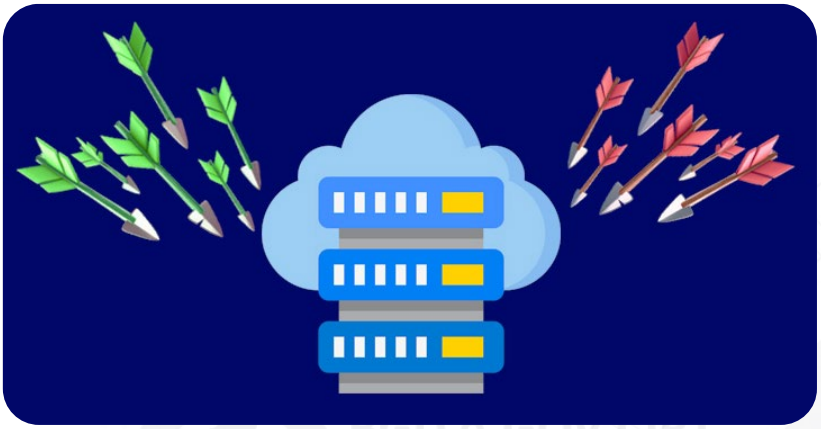


Image Source: https://twitter.com/PhishStats/status/1522325899294748673

Denial of Service (DoS)

Availability of services is always the main concern for businesses and infrastructures. This is where DDoS comes into the picture for being a major threat behind services unavailability and that makes it, though not new, have a significant persistence in the cybersecurity threat landscape.



Global Trends and statistics

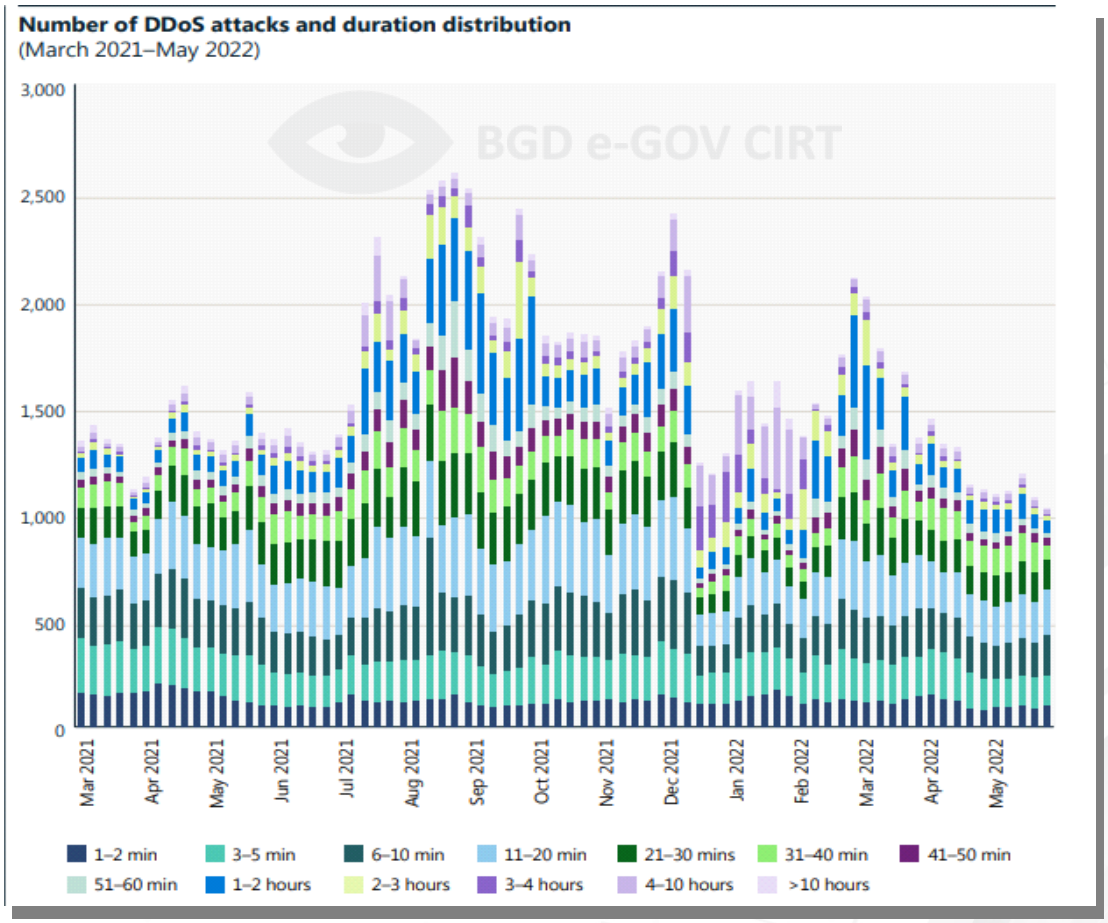
Unprecedented DDoS Attack

- In June 2022, the largest DDoS attack ever was recorded by a Google customer who was hit with a series of HTTPS DDoS attacks, peaking at 46 million requests per second. Google confirmed it has blocked the attack which is described as the largest Layer 7 DDoS reported to date — at least 76% larger than the previously reported record.[28]
- Compared to the first half of 2021, DDoS attacks have a sharp increase of 205% year over year with a 67 percent rise in the number of ransom DDoS attacks.[29]
- Attacks are becoming more complex and multi-vectored. Rather than directly attacking the victim's server, attackers paralyze one of its key functions and conduct combined attacks along different vectors.

[28] https://www.bleepingcomputer.com/news/security/google-blocks-largest-https-ddos-attack-reported-to-date/
[29] https://nsfocusglobal.com/ddos-attacks-skyrocketed-by-205-in-h1-2022/

The number of complex multi-vector attacks tripled in 2022 compared to the previous year.[30]

↳ Most attacks observed over this year were short-lived.



Approximately 28 percent of the attacks lasted less than 10 minutes, 26 percent lasted 10–30 minutes and 14 percent lasted 31–60 minutes. Thirty-two percent of the attacks were more than an hour in duration. [31]

DDoS and cyberwarfare

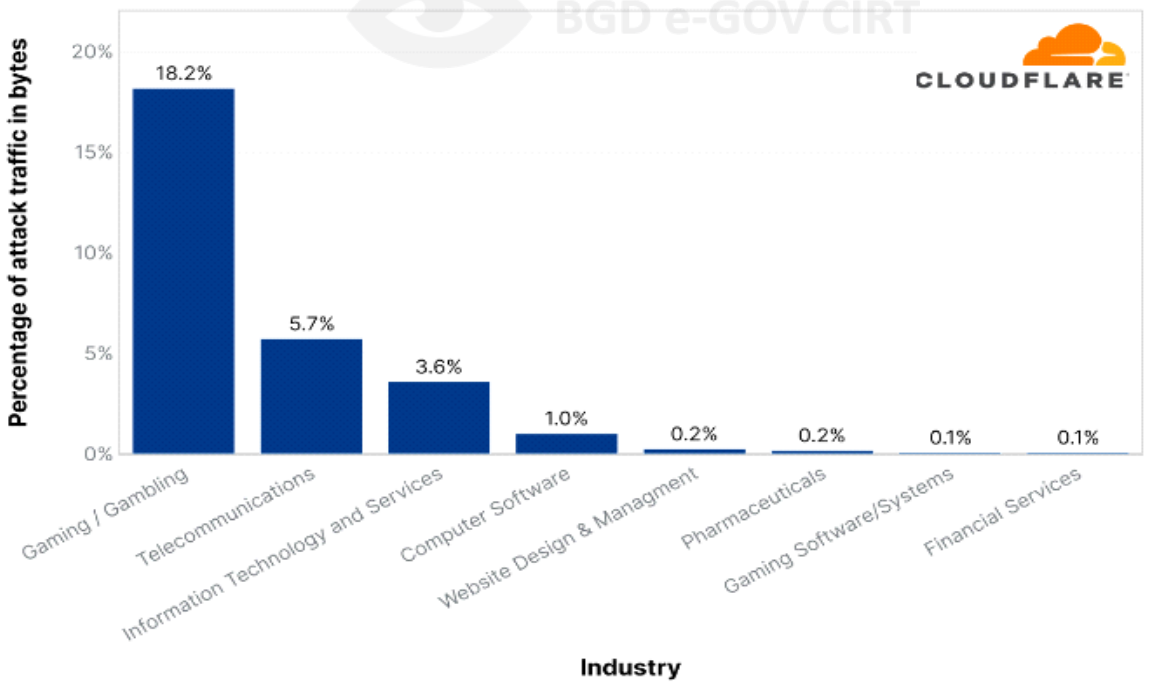
The Russia-Ukraine war has incited nation-state hackers, hacktivists and even common civilians to participate in the cyber war by conducting attacks against their opponents.

[30] https://www.bleepingcomputer.com/news/security/ddos-attack-trends-in-2022-ultrashort-powerful-multivector-attacks/
[31] https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

- Cyberattacks aimed at disabling banks and government websites was the worst in the history of Ukraine5. In Russia on the other hand, Banking Finance Services and Insurances (BFSI) companies in Russia were the most targeted [32].
- In April 2022, the pro-Russian hacking group Killnet launched DDoS attacks against Czech railroads, regional airports, and Czech's civil service server, even though Czech is not directly involved in the war.[33]

Industry sector attack spread

The Gaming / gambling industry was the most targeted by network-layer DDoS attacks, followed by Telecommunications companies, and the Information Technology and Services industry.[33]

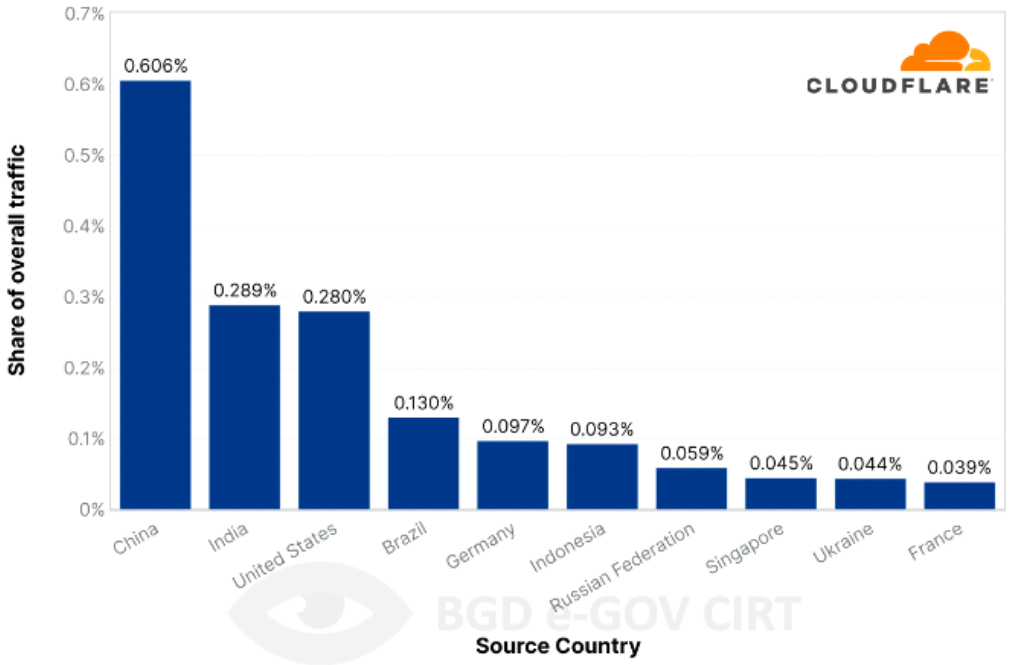


Top industries targeted by L3/4 DDoS attacks in 2022 Q3

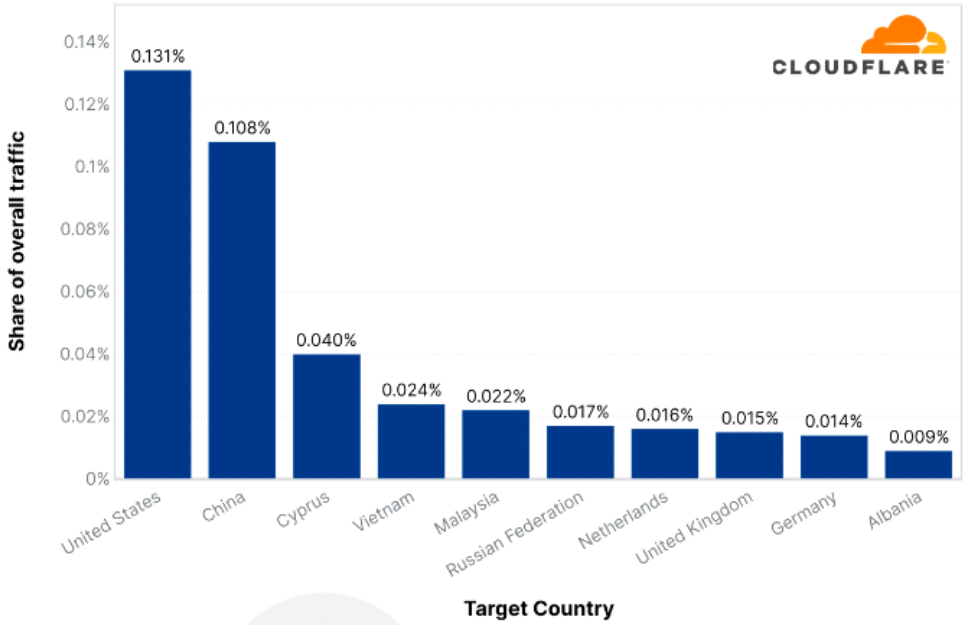
[32] https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2/
[33] https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/

Geographical Spread of DDoS Attacks

↳ The United States experienced the largest number of DDoS attacks, while china is considered to be the top source it comes from.



Top source countries of HTTP DDoS attacks in 2022 Q3



Top countries targeted by HTTP DDoS attacks in 2022 Q3

- The USA, Netherlands and Germany account for the highest distribution of botnet C&Cs, accounting for 48.49%, 9.17%, and 8.69% of botnet C&Cs respectively on average. [34]
- Bangladesh ranked sixth among the top destinations targeted by DDoS attacks in the APAC region. [35]

Ransom Denial of Service (RDoS)

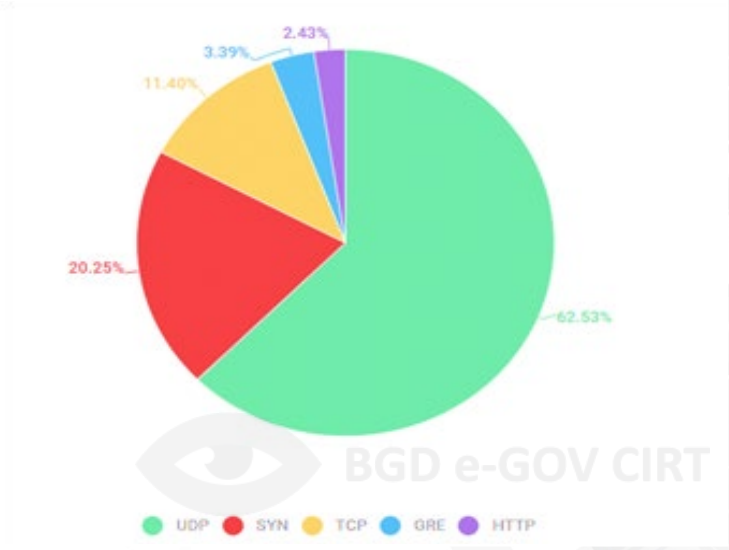
In June 2022, ransom DDoS attacks peaked at the highest of the year so far: one out of every five survey respondents who experienced a DDoS attack reported being subject to a Ransom DDoS attack or other threats.[36]

Top Ten Reflected Attack Destinations in APAC (1HY 2022)

	Percentage
South Korea	81.46%
China	14.44%
Australia	0.91%
Singapore	0.73%
Hong Kong	0.68%
Bangladesh	0.41%
Taiwan	0.38%
Vietnam	0.24%
India	0.22%
Malaysia	0.20%
Others	0.33%

The shift from UDP-based to TCP-based attacks

Although UDP is the most favored vector used in the DDoS attack, attackers are shifting to TCP-based attacks and flooding the target with traffic that is hard to be distinguished from user-intended traffic.



Distribution of DDoS attacks by type, Q2 2022

[34] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[35] https://blog.nexusguard.com/threat-report/ddos-statistical-report-for-1hy-2022
[36] https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2/

DDoS attacks are increasingly moving toward mobile networks and IoT

The little to no security of IoT devices makes them a suitable target for DDoS attacks. According to the US National Institute of Standards and Technology (NIST), 'admin' (username) and '1234' (password) was the most common combination used in attacks against IoT which makes them easily exploitable by attackers to build botnets with hundreds of thousands of IoT devices.

DDoS Attack trends in Bangladesh

Arguably, DDos is the most common cyber attack being observed in the cyberspace of Bangladesh. BGD e-GOV CIRT issued a nationwide cyber alert after observing several DDoS attacks targeting the mission-critical infrastructures of Bangladesh[37]. In the last quarter of 2022, We observed a spike in 'DDoS middle box reflection' events in recent months. APNIC published an article on 18th October 2022 titled "A new DDoS attack vector: TCP Middlebox Reflection" which states –

> *A middlebox (as per RFC 3234) is a computer networking device that transforms, inspects, filters, and manipulates traffic for purposes other than packet forwarding. Firewalls, NAT devices, load balancers, and deep packet inspection (DPI) devices are common examples of middleboxes.*

[37] https://www.thedailystar.net/tech-startup/news/govt-issues-warning-about-impending-ddos-cyber-attack-3099466

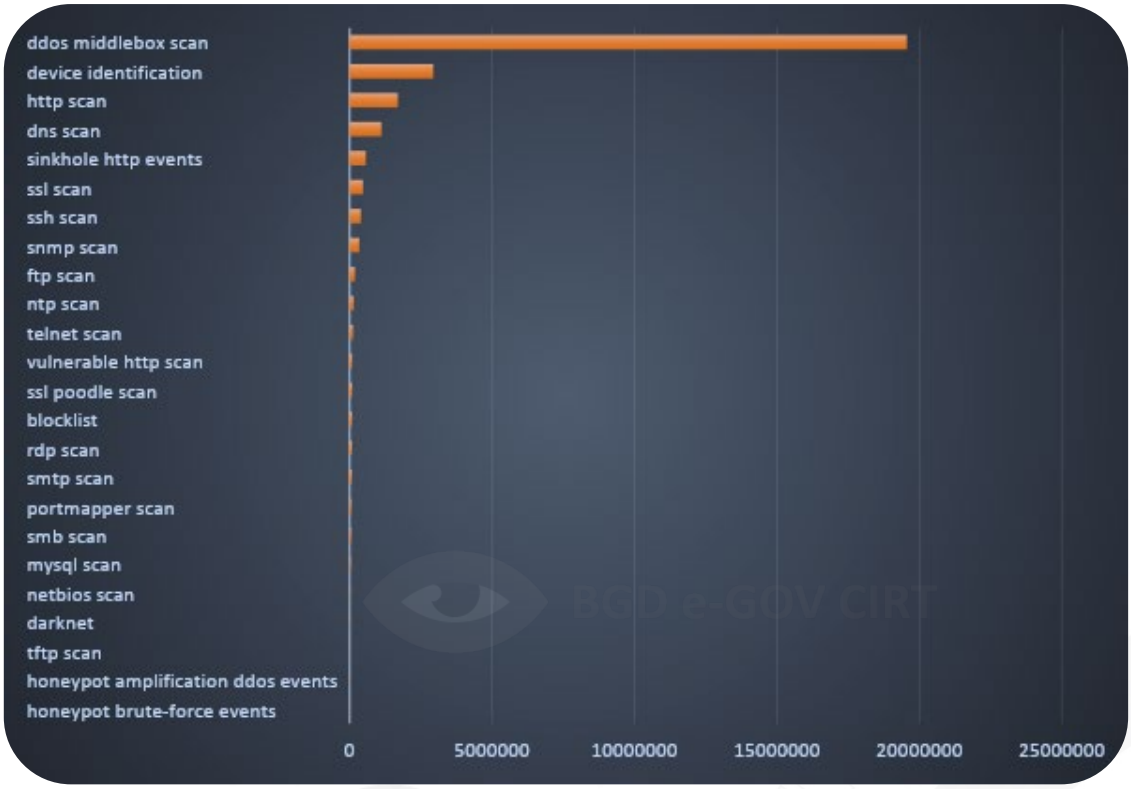
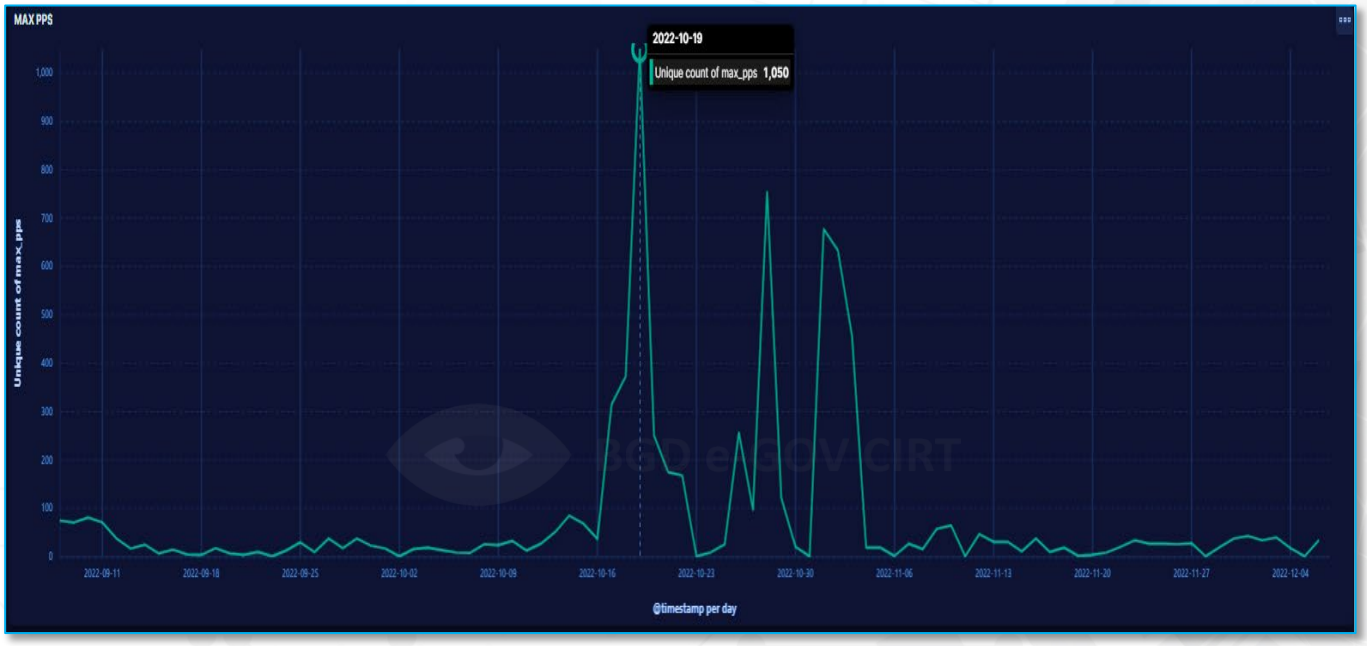


Figure 9: Surge of DDoS middlebox scan events

We have discovered DDoS amplification events soaring up to 1050 packets per second on 19th October 2022.



[38] https://www.microsoft.com/en-us/security/blog/2022/05/23/anatomy-of-ddos-amplification-attacks/

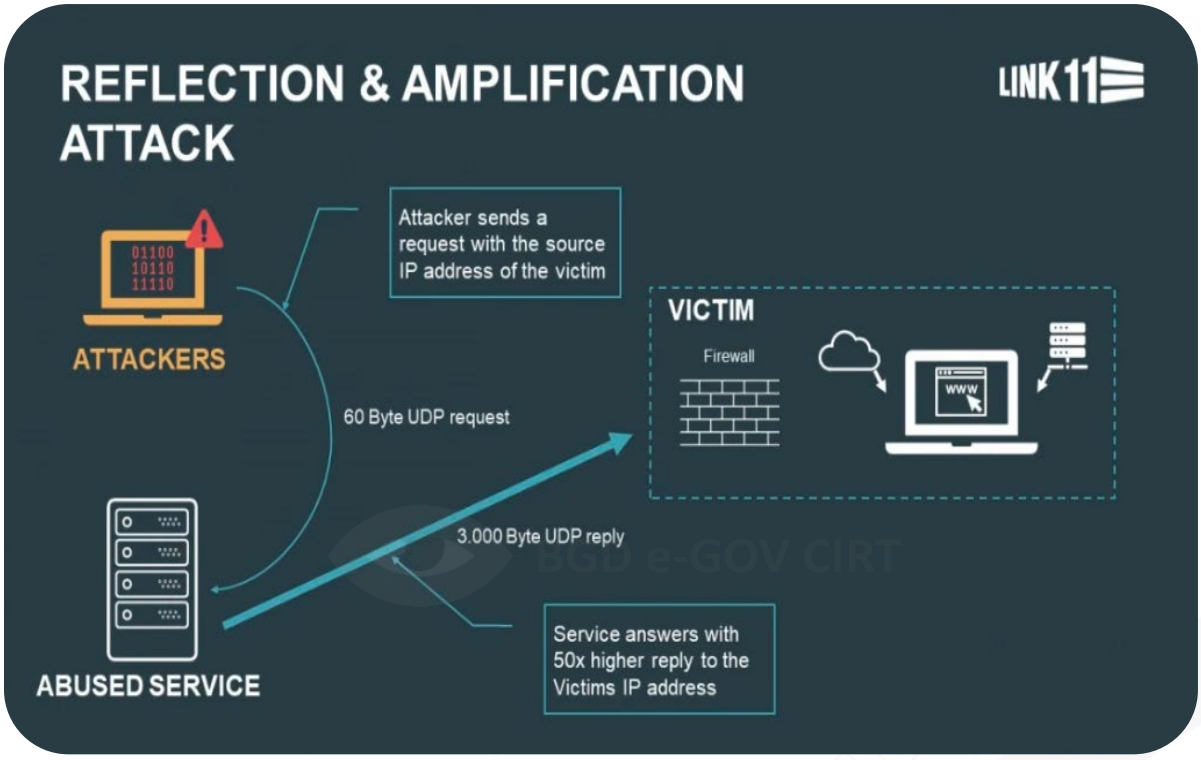


Figure 10: illustration of reflection and amplification attack[39] (image courtesy: Link 11)

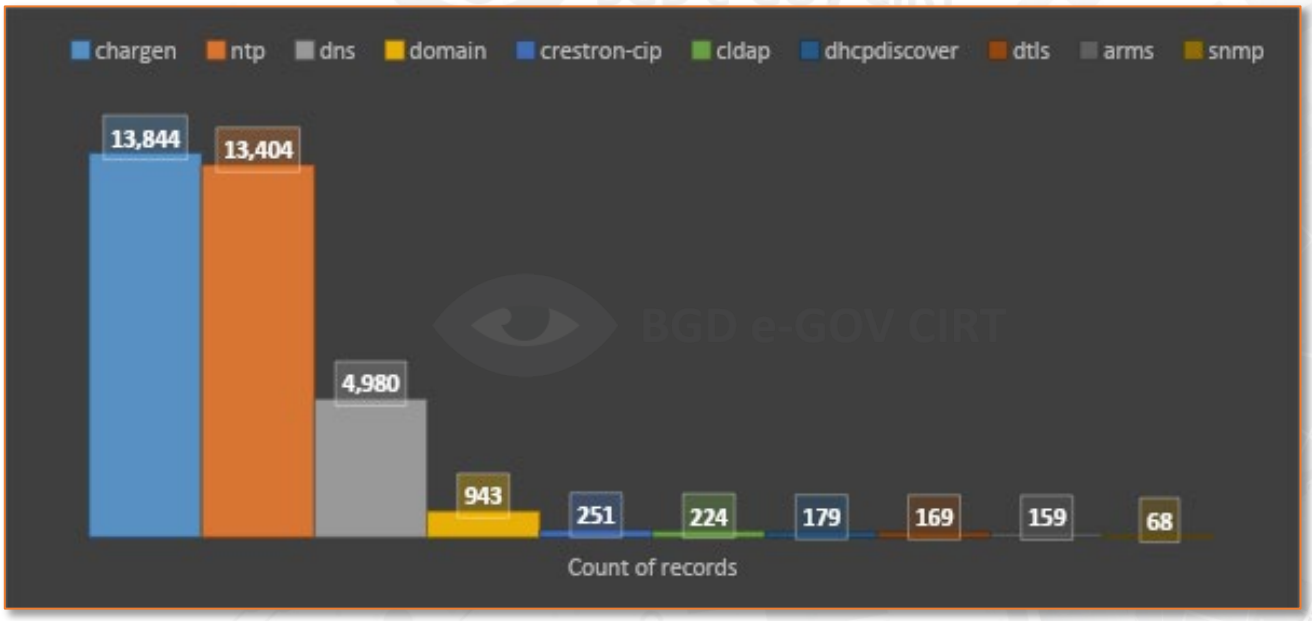


Figure 11: Amplification attacks observed from September 2022 to December 2022 [40]

(Note: Event records depict approximate counts)

[39] https://www.link11.com/en/security-wiki/
[40] Threat Intelligence unit of BGD e-GOV CIRT

The following table lists the top attack source host names and their corresponding cities found to be used for this type of amplification attack.

Top values of src city	Top values of src_hostname
DHAKA	caching[.]sambd[.]net
DHAKA	visit[.]keznews[.]com
DHAKA	103[.]85[.]156[.]1[.]race[.]net[.]bd
DHAKA	ip226[.]ip-198-50-247[.]net
DHAKA	ip234[.]ip-198-50-233[.]net
CHITTAGONG	144[.]48[.]116[.]1[.]race[.]net[.]bd
CHITTAGONG	103[.]85[.]158[.]1[.]race[.]net[.]bd
CHITTAGONG	103[.]141[.]65-0[.]iq-tel[.]net
CHITTAGONG	103[.]186[.]219-0[.]iq-tel[.]net
CHITTAGONG	103[.]85[.]158[.]13[.]race[.]net[.]bd
NARAYANGANJ SADAR	167[.]130[.]cetus[.]link3[.]net
NARAYANGANJ SADAR	167[.]179[.]cetus[.]link3[.]net
NARAYANGANJ SADAR	167[.]195[.]cetus[.]link3[.]net
NARAYANGANJ SADAR	167[.]197[.]cetus[.]link3[.]net
NARAYANGANJ SADAR	167[.]204[.]cetus[.]link3[.]net
FENI SADAR	dhknat-27[.]147[.]200[.]146[.]link3[.]net
FENI SADAR	dhknat-27[.]147[.]200[.]149[.]link3[.]net
FENI SADAR	dhknat-27[.]147[.]200[.]157[.]link3[.]net
FENI SADAR	dhknat-27[.]147[.]200[.]158[.]link3[.]net
KHULNA	visit[.]keznews[.]com
KHULNA	103[.]54[.]39[.]1[.]race[.]net[.]bd
KHULNA	103[.]200[.]37-232[.]skyviewonlineltd[.]com
KHULNA	103[.]200[.]37-235[.]skyviewonlineltd[.]com
KHULNA	103[.]54[.]38[.]196[.]race[.]net[.]bd

Malware traversal in mobile telecom operators

According to the statistics published on the BTRC website, which was last updated on November 28, 2022, Bangladesh has approximately 181.67 million mobile phone subscribers.[41] The threat intelligence unit of BGD e-GOV CIRT identified a substantial number of footprints for malware infections through mobile telecom operators. It **DOES NOT** necessarily mean that the telecom service provider infrastructures are infected, rather it is an alarming indicator of huge number of mobile data users who might have been infected with malwares. The following treemap shows the infection rate of the most prominent malware traversing across all four telecom operators.

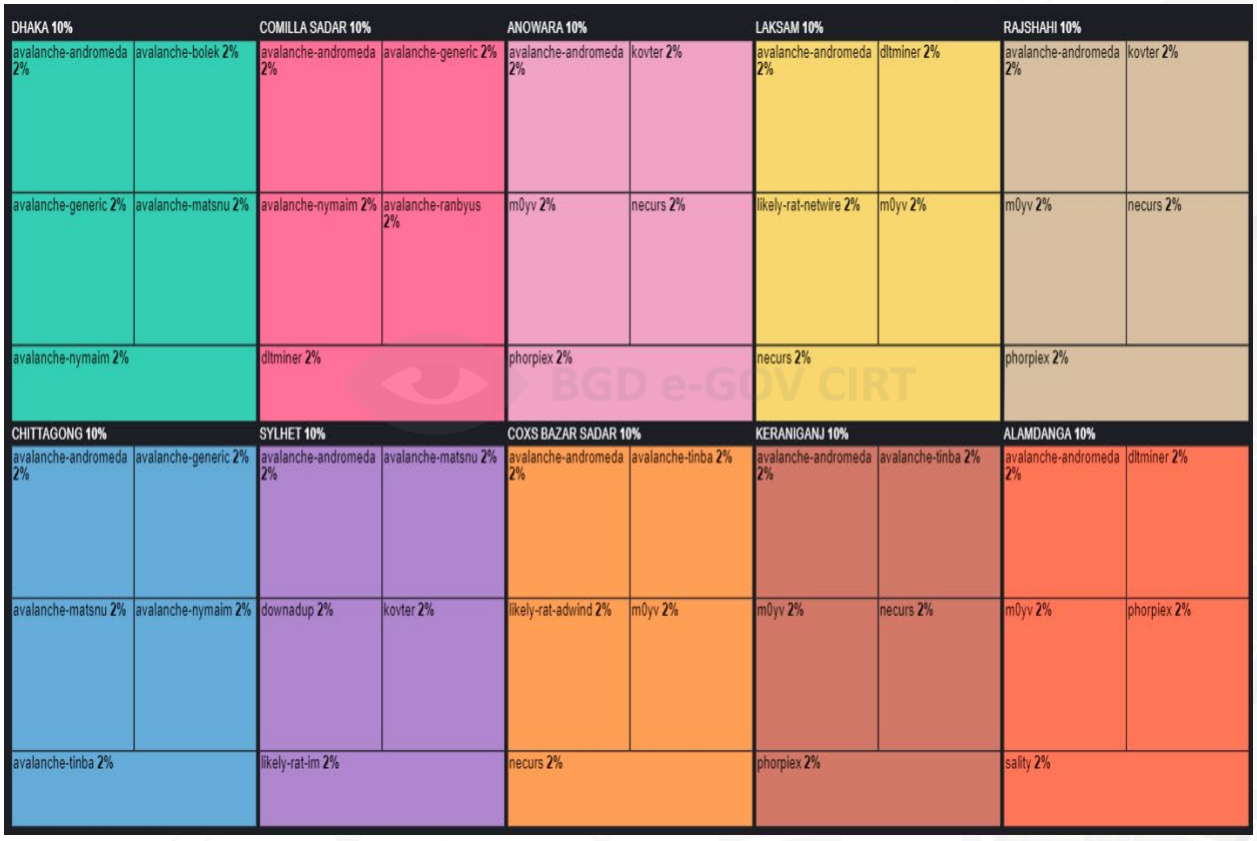
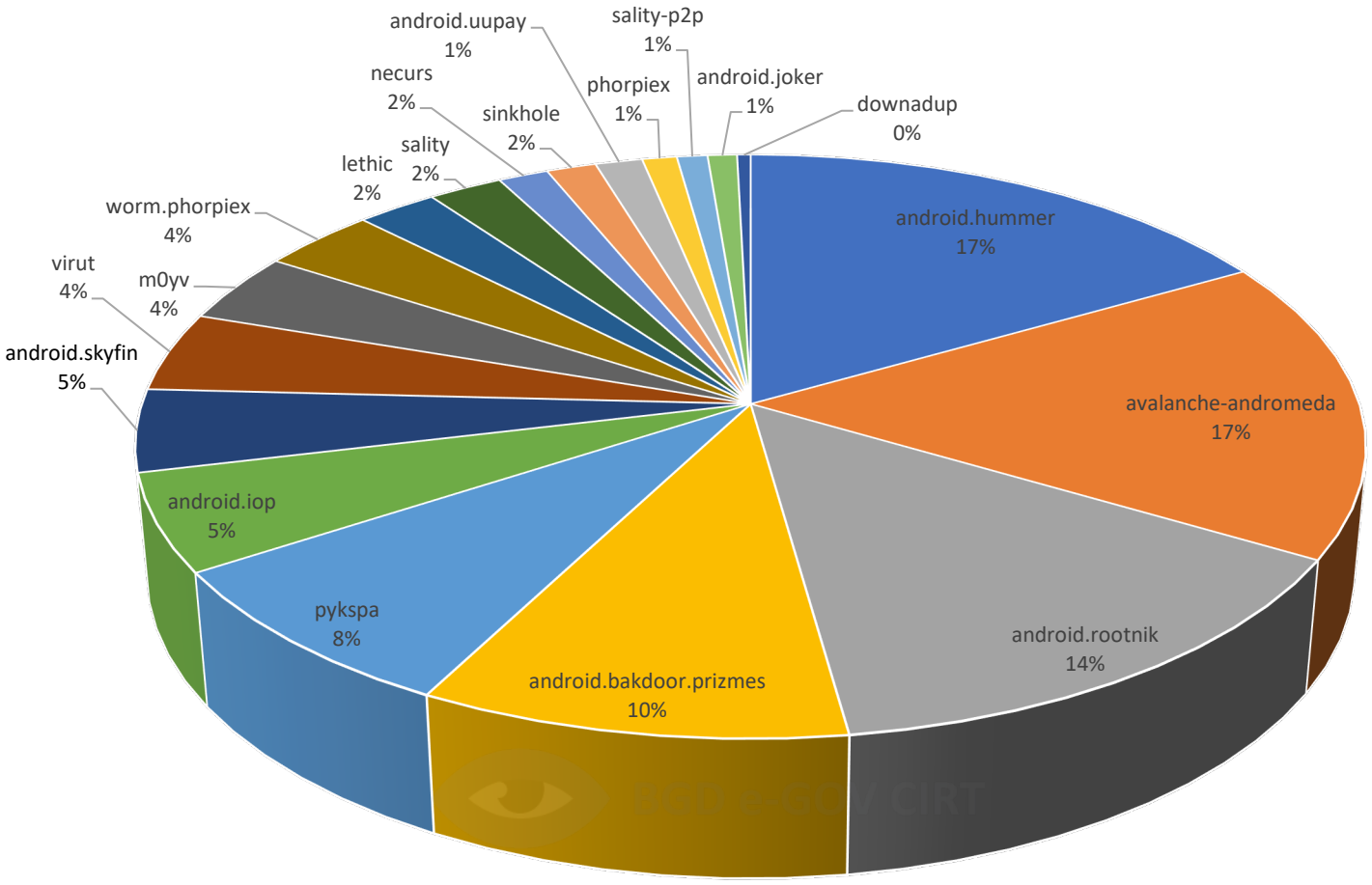


Figure 12: Regional heatmap of malware traversal by telecom operators in Bangladesh[42]

After reviewing the statistical data for the year 2022 it is observed that android.hummer, avalanche-andromeda, android.rootnik are the top three

[41] http://btrc.gov.bd/
[42] Threat Intelligence unit of BGD e-GOV CIRT

android based malware that had a communication footprint over the mobile telecom operators of Bangladesh.



[43] Threat intelligence unit of BGD e-GOV CIRT

A total of **74** unique malware infections are found to be communicating across the four telecom operators in Bangladesh.

List of Malware traversing mobile telecom operators in 2022					
1	android.bakdoor.prizmes	26	dresscode	51	nivdort
2	android.gopl	27	esfury	52	phorpiex
3	android.hummer	28	expiro	53	pykspa
4	android.iop	29	fake_cs_updater	54	qrypter.rat
5	android.joker	30	flubot	55	ramdo
6	android.rootnik	31	gozi	56	sality
7	android.skyfin	32	jdk-update-apt	57	sality-p2p
8	android.sssaaa	33	js.worm.bondat	58	shiz
9	android.uupay	34	kasidet	59	sinkhole
10	andromeda-b66	35	kovter	60	softpulse
11	avalanche-andromeda	36	lethic	61	sunburst
12	avalanche-bolek	37	likely-rat-adwind	62	tinba
13	avalanche-generic	38	likely-rat-at	63	tinba-dga
14	avalanche-marcher	39	likely-rat-firebird	64	Top values of infection
15	avalanche-matsnu	40	likely-rat-im	65	trojan.click3
16	avalanche-nymaim	41	likely-rat-netwire	66	tsifiri
17	avalanche-pandabanker	42	likely-rat-orcus	67	unknown
18	avalanche-ranbyus	43	likely-rat-remcos	68	verst
19	avalanche-tinba	44	likely-rat-warzone	69	virut
20	blakamba	45	likely-rat-wsh	70	win.neurevt
21	coinminer	46	loader	71	worm.phorpiex
22	disorderstatus	47	m0yv	72	wrokni
23	dltminer	48	monero	73	xmrminer
24	downadup	49	necurs	74	zloader
25	downloader.bitcoinminer	50	neurevt		

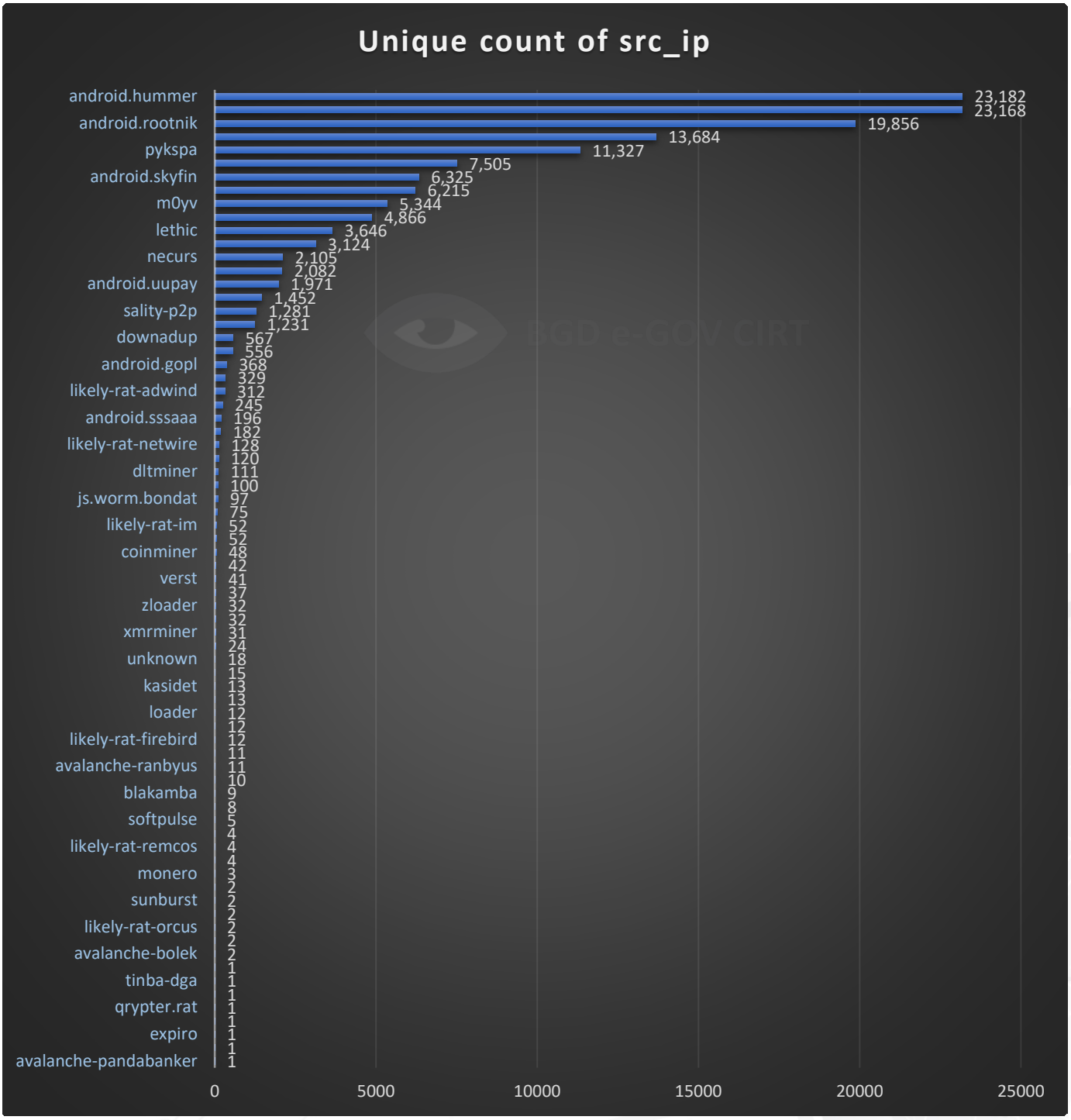


Figure 13: Malware infection with the unique count of source IP address[44]

[44] Threat intelligence unit of BGD e-GOV CIRT

APT group activities in global landscape

In 2022 the world started to experience the heated geopolitical situation in Europe, Middle-east and Far-East, which not only racketed the geographic boundaries but also the cyberspace. Threat actors with affiliations to nation states continued their APT activity in 2022. APT groups including the infamous Sandworm as well as Gamaredon, InvisiMole, Callisto, and Turla continued to operate with special focus in Europe.

Countries, regions and verticals affected by the APT groups described in the APT activity report 2022 published by internet security firm ESET included:

Targeted countries and regions	Targeted business verticals
• Argentina • Germany • Hong Kong • Iran • Israel • Japan • Kyrgyzstan • Netherlands • Poland • South Africa • Ukraine • United States • Uzbekistan • Asia • Europe	• Aerospace • Blockchain technology companies • Branding and marketing • Communications industry • Cybersecurity • Defense • Diamond industry • Education • Embassies • Engineering • Financial services • Information technology • Law • Manufacturing • Media • National and local governments • Political entities • Retail • Social services • Telecommunication

The Global Research and Analysis Team (GReAT) from Kaspersky, a leading security solution provider, released an article that outlines important APT trends in the last quarter of 2022[45]. The researchers state that in order to launch increasingly complex attacks, APT actors constantly modify their tactics, improve their toolkits, and adopt new tools and methodologies.

[45] https://securelist.com/apt-trends-report-q3-2022/107787/

Threat Actor Origin	APT group	Targeted Continent/Countries
China-based	APT41 (a.k.a Wicked Panda)	Asia
	DiceyF	Hong Kong, the Philippines, China, and Vietnam
	APT10 (a.k.a menupass)	Japan
	APT29	North America, Europe, Asia, and the Middle East
Middle-east based	FramedGolf	Middle-east region
	Defttorero(a.k.a Volatile cedar)	UAE, Saudi Arabia, Egypt, Kuwait, Lebanon, Jordan and Turkey[46]
Southeast Asia and Korean Peninsula based	Tropic Trooper	East and Southeast Asia (Taiwan, the Philippines, and Hong Kong)47
	Lazarus group	South Korea The United States Japan India Russia Bangladesh Poland Turkey Brazil
	Kimsuky	United States, Russia, Europe, and the UN48

Table: Globally prevalent APT groups in 2022[49]

[46] https://www.bizbahrain.com/kaspersky-uncovers-new-tactics-used-by-the-middle-eastern-apt-group-defttorero/
[47] https://attack.mitre.org/groups/G0081/
[48] https://attack.mitre.org/groups/G0094/
[49] https://cyware.com/news/a-quick-peek-into-the-global-apt-game-q3-2022-trends-56b48de8

APT Groups activities targeting Bangladesh

Advanced Persistent Threat Groups or APT groups pose a significant risk for a targeted nation as they are often executed by state-sponsored attackers. At the advent of 2022, the threat intelligence unit of BGD e-GOV CIRT published a threat alert report about the suspicious activities of **DoNotTeam (also known as APT-C-35 or Bellyworm) and Patchwork (APT-C-09)**. The report states,

> *"DoNotTeam (also known as APT-C-35 or Bellyworm) is an APT organization suspected of having a South Asian background. It mainly conducts cyberattacks against the governments and military of neighboring countries including Pakistan, Bangladesh, Nepal, and Sri Lanka, usually to steal sensitive information. The organization can attack both Windows and Android platforms. A recent suspected attack on Bangladesh by this APT group was found to use **"Bangladesh University of Professionals 2021 Electronic Engineering Presentation"** as the subject and sent the PPT decoy file to the victim via phishing email. After the victim opens the decoy file and executes the macro, it will upload basic computer and user information to the remote server, and download the subsequent attack module for local execution."* [50]

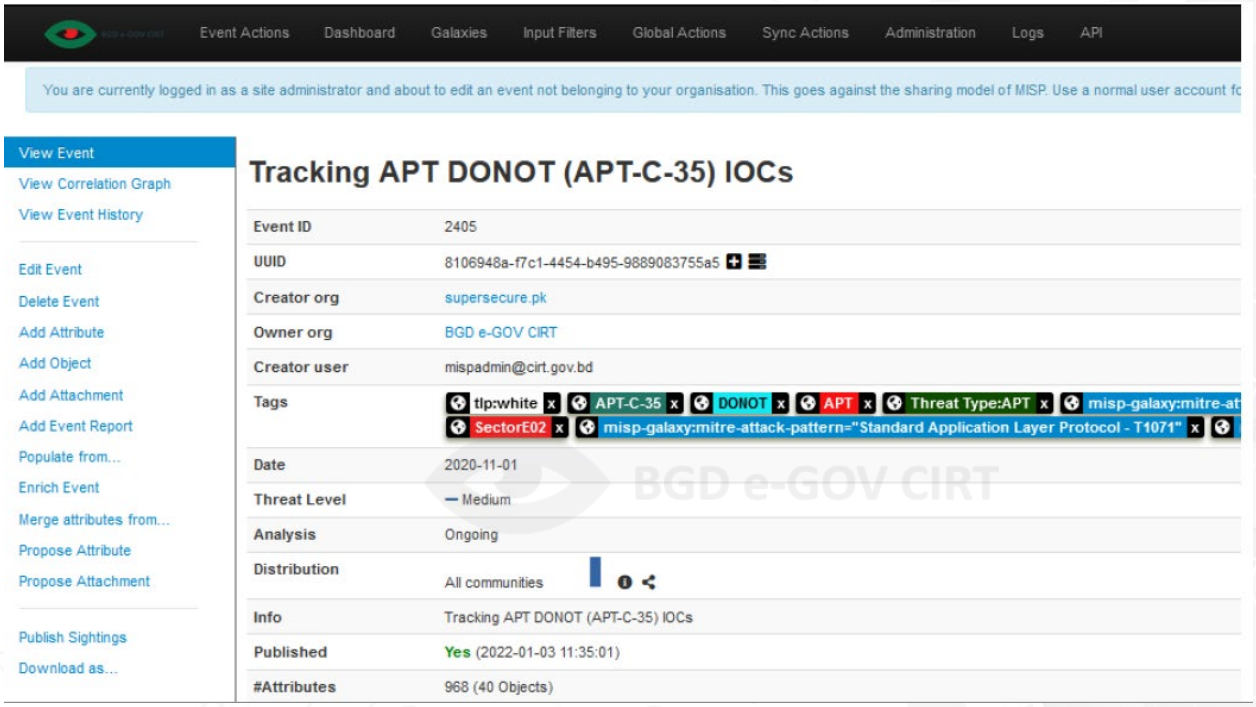


Figure 14 : Suspicious activities detection of APT group DONOT (APT-C-35)[51]

[50] https://mp.weixin.qq.com/s/gsUN6lXMz17_jkR8xIrZNA
[51] Threat intelligence unit of BGD e-GOV CIRT

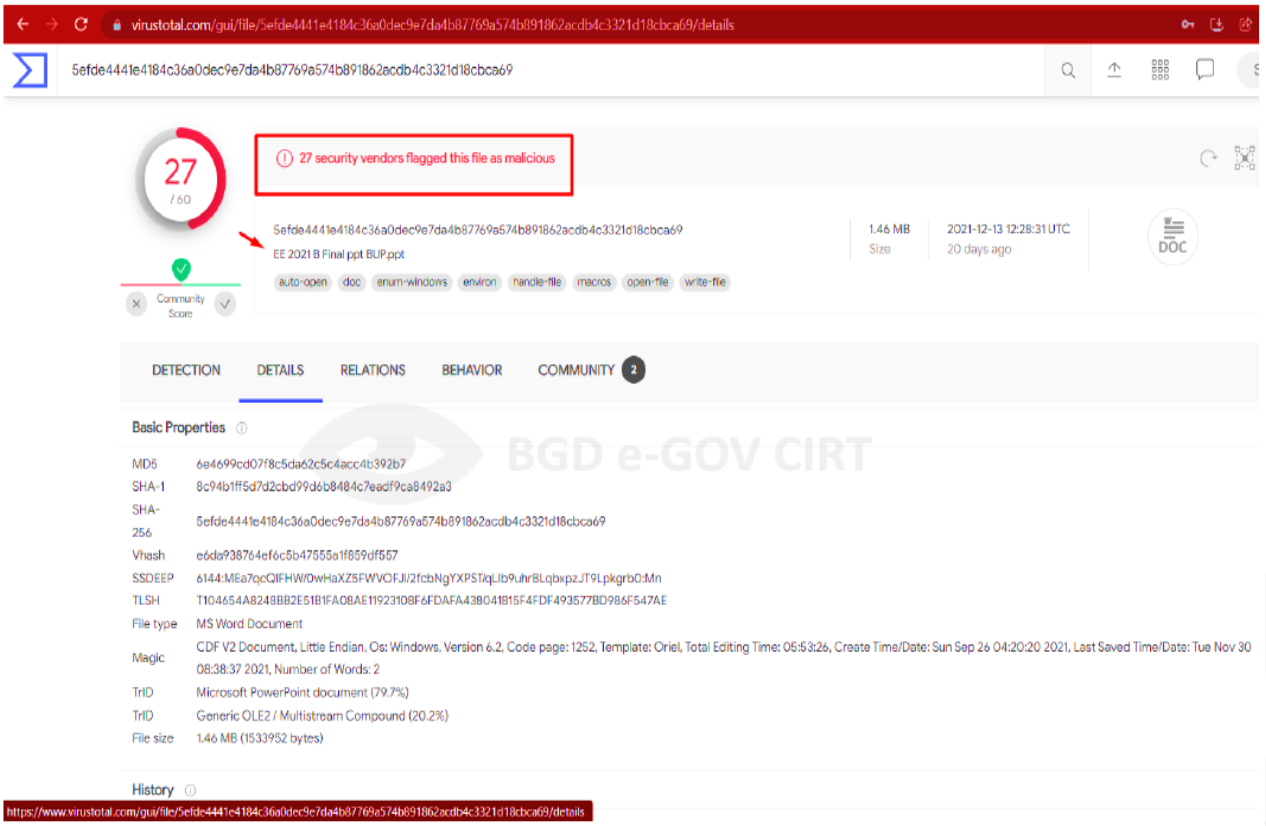


Figure 15 : Malicious File Hash Detection with the file name 'EE 2021 B Final ppt BUP.ppt'[52]

The report also mentions about APT group Patchwork (APT-C-09)-

> *"Patchwork is a cyberespionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. Patchwork has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. Patchwork was also seen operating spear phishing campaigns targeting U.S. think tank groups in March and April of 2018"*[53]

[52] https://www.virustotal.com/gui/file/5efde4441e4184c36a0dec9e7da4b87769a574b891862acdb4c3321d18cbca69/details

[53] https://attack.mitre.org/groups/G0040/

Threat intelligence unit of BGD e-GOV CIRT also identified several other footprints of different APT groups listed below in last year-

APT GROUP	Description	Observed IOC in Bangladesh
Infy-apt (aka: Operation Mermaid, Prince of Persia, Foudre)	Infy is a group of suspected **Iranian** origin which became one of the most frequently observed agents for attempted malware attacks against Iranian civil society beginning in late 2014, growing in use up to the February 2016 parliamentary election in Iran. After the conclusion of the parliamentary election, the rate of attempted intrusions and new compromises through the Infy agent slowed, but did not end. The trends witnessed in reports from recipients are reinforced through telemetry provided by design failures in more recent versions of the Infy malware. [54]	youripinfo[.]com updateserver1[.]com updatebox4[.]com updateserver3[.]com lost[.]updateserver1[.]com
Emissary-panda (aka: IronPanda, Lucky Mouse, LuckyMouse, Iron Panda, APT 27, Emissary Panda, Iron Tiger, ZipToken, Group 35, TEMP.Hippo, TG 3390, Bronze Union, Threat Group 3390)	Emissary Panda is a threat group believed to be operating out of **China** and responsible for conducting cyber espionage campaigns against a variety of targets, including government agencies, defense contractors, and media companies. The group has been active since at least 2007 and has been linked to a number of high-profile attacks, including the 2014 breach of the U.S. Office of Personnel Management (OPM) in which the personal data of millions of federal employees was compromised. Emissary Panda is known for using a wide range of tactics and tools to compromise its targets, including phishing campaigns, custom malware, and exploit kits. The group is also known for its use of infrastructure and tactics that are similar to those used by other Chinese APT groups, suggesting that it may have some level of support from the Chinese government.[55]	redhatupdater[.]com yofeopxuuehixwmj[.]redhatupdater[.]com
Tick (a.k.a. "BRONZE BUTLER" or "REDBALDKNIGHT"))	TICK (is a cyberespionage group known for its supply chain attacks and use of different malware families to attack organizations across different sectors such as defense, aerospace, satellite communications, and retail industries, as well as industrial chemical companies. Trend Micro has been observing this group's operations from as early as 2008, including	komdsecko[.]net

[54] https://malpedia.caad.fkie.fraunhofer.de/actor/infy
[55] https://www.anomali.com/blog/weekly-threat-briefing-emissary-panda-attacks-middle-east-government-sharepoint-servers

APT GROUP	Description	Observed IOC in Bangladesh
	its use of social engineering attacks commonly written in fluent Japanese following their usual target victims' affiliations.[56]	
Machete-apt	Machete is a suspected Spanish-speaking cyber espionage group that has been active since at least 2010. It has primarily focused its operations within Latin America, with a particular emphasis on Venezuela, but also in the US, Europe, Russia, and parts of Asia. Machete generally targets high-profile organizations such as government institutions, intelligence services, and military units, as well as telecommunications and power companies.[57]	koliast[.]com tobabean[.]expert artyomt[.]com mail[.]tobabean[.]expert
Pittytiger	PittyTiger is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.[58]	iphone4-office[.]org iphone4-office[.]net googlemailsystem[.]net ipad-admin[.]net ipad-admin[.]com googlemailsystem[.]net[.] googlemailsystem[.]org googlemailsystem[.]com iphone4-office[.]com macosservice[.]com ipad-admin[.]org
Threatneedle	ThreatNeedle is a backdoor that has been used by Lazarus Group since at least 2019 to target cryptocurrency, defense, and mobile gaming organizations. It is considered to be an advanced cluster of Lazarus Group's Manuscrypt (a.k.a. NukeSped) malware family.[59]	codevexillium[.]org
Muddywater	MuddyWater is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). Since at least 2017, MuddyWater has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.[60]	208[.]100[.]26[.]245

[56] https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf
[57] https://attack.mitre.org/groups/G0095/
[58] https://attack.mitre.org/groups/G0011/
[59] https://attack.mitre.org/software/S0665/
[60] https://attack.mitre.org/groups/G0069/

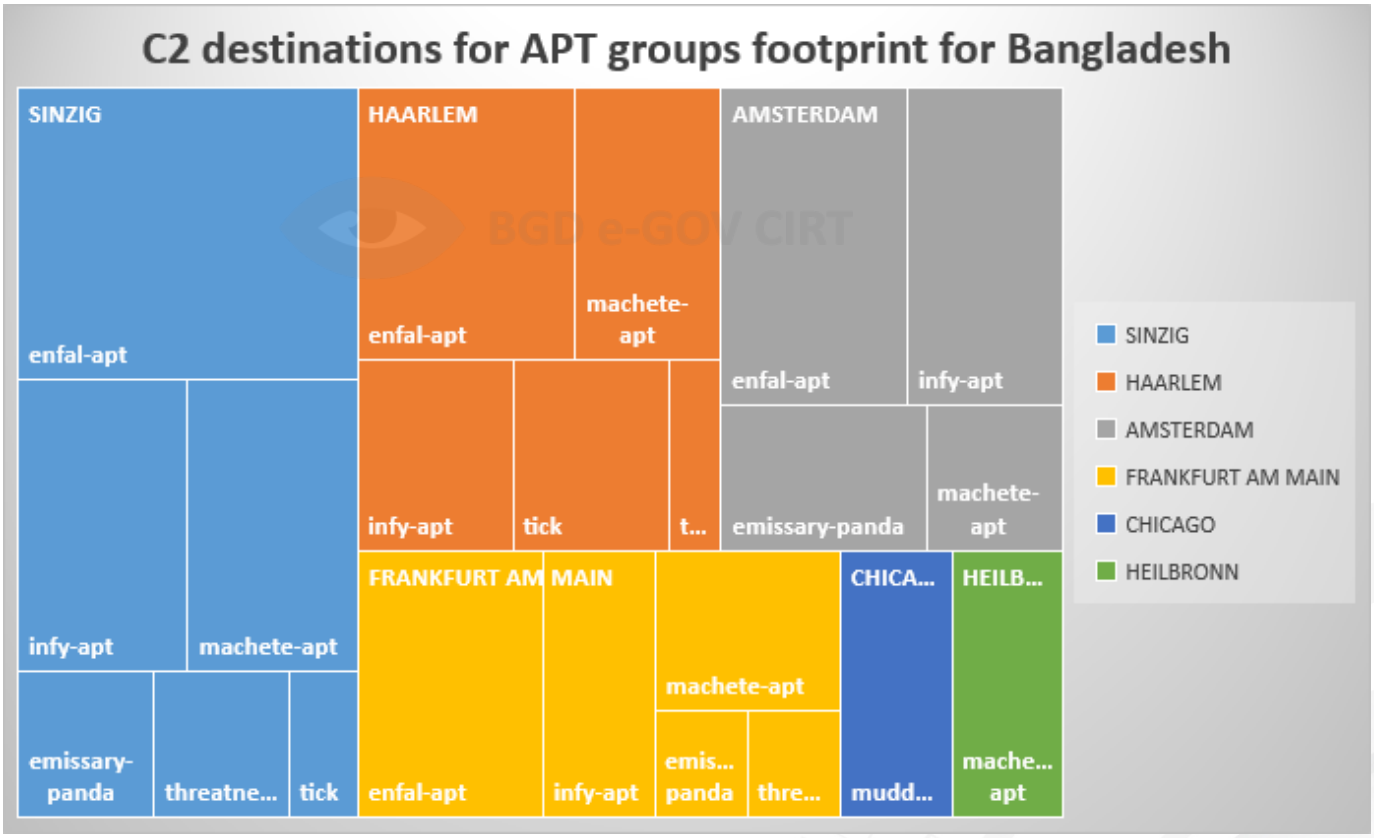


Figure 16: C2 destinations for APT groups footprints in Bangladesh[61]

[61] Threat intelligence unit of BGD e-GOV CIRT

Credential theft , dark web trading and online fraud

Credential theft is a type of cyber attack in which an attacker attempts to obtain login credentials (such as a username and password) for a system or service. The attacker may use a variety of tactics to obtain the credentials, including phishing attacks, malware, keyloggers, and social engineering.

Once the credentials have been obtained, the attacker can use them to gain unauthorized access to the system or service, potentially stealing sensitive data, interfering with operations, or carrying out other nefarious deeds.

The threat intelligence unit of BGD e-GOV CIRT actively monitors popular social media channels and the dark web market to discover security breaches in critical information infrastructures (CIIs), domain accounts, banks and databases.

In 2022, the highest number of login credentials are supposedly stolen for database access which amounted around 3,838. Bank account credentials followed with around 1,967 (masked bank cards) and 1,672 (bank cards) leaks. Miscellaneous domain accounts (CIIs, government, academia, and private organizations) login credentials compromises were counted to around 891.

"Sectorial Threat Intelligence Report for Banking Industries", published in September 2022, states that –

> *"On the dark web, a substantial number of Bangladeshi bank card credentials were found to be leaked. Although it might be caused by the negligence of individual subscribers, the relevant banking authorities should be aware of which card credentials are available on the dark web and take the necessary precautions, and spread awareness.* [62]
> "

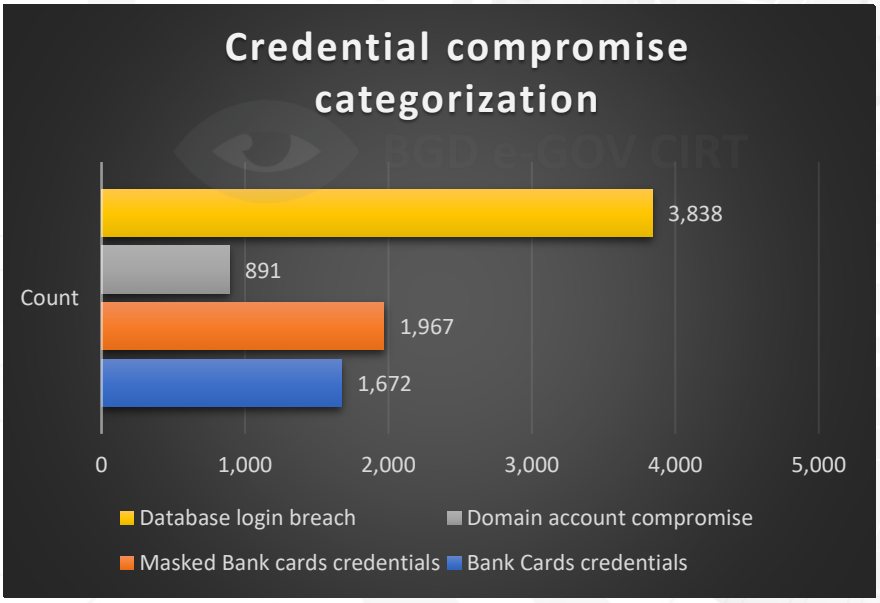


Figure 17: credential compromise statistics[62]

[62] https://shop.cirt.gov.bd/product/sectorial-threat-intelligence-for-banks-july-2022/

Around **20 stealer-type malware** was identified which was used for credential theft. Among them, Redline Stealer and AZORult were the most prominent.

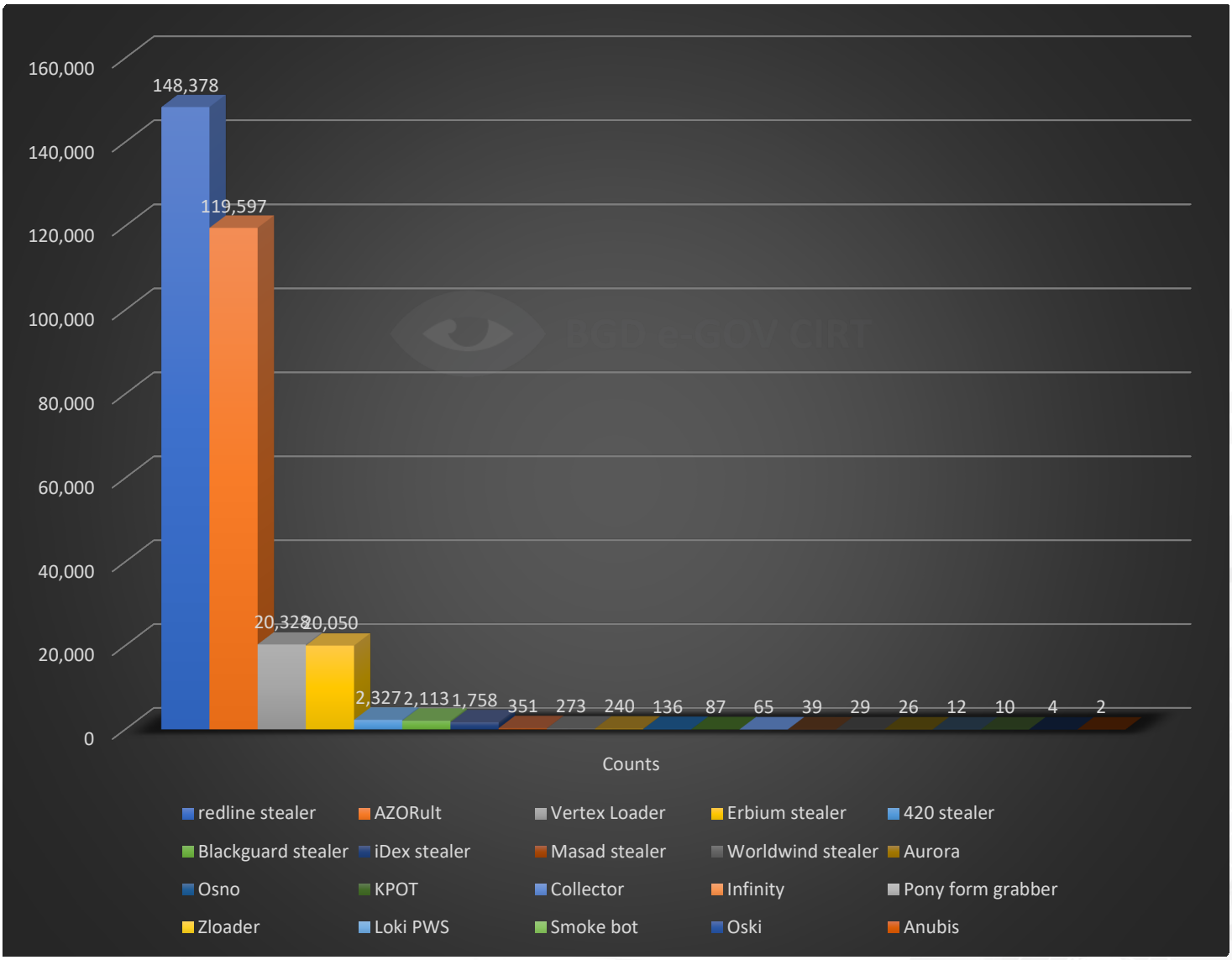


Figure 18: Stealer Malware statistics[63]

[63] Threat Intelligence Unit of BGD e-GOV CIRT

Financial Implications of Cybercrime in Bangladesh

The rising incidents of cyber frauds in the financial sector have become a cause of worry in Bangladesh. In 2014, the state-owned Sonali Bank lost $250,000 (Tk 2 crore) to cyber criminals, who allegedly hacked into the bank's security system and transferred the money to an account in Turkey.[64]

In February 2016, cyber criminals intruded into Bangladesh Bank's SWIFT network to illegally transfer close to US$1 billion from the Federal Reserve Bank of New York account. Five of the thirty-five fraudulent instructions were successful in transferring US$101 million, with US$20 million traced to Sri Lanka and US$81 million to the Philippines. All the money transferred to Sri Lanka has since been recovered. However, as of 2018 only around US$18 million of the US$81 million transferred to the Philippines has been recovered.[65]

In 2019 three local private banks in Bangladesh suffered major cyber attacks where hackers stole up to USD 3 million from cash machines in Cyprus, Russia and Ukraine using cloned credit cards.[66]

BGD e-GOV CIRT discovered 3,639 bank cards on the dark web issued by different Bangladeshi Banks. Besides, BGD e-GOV CIRT also identified vulnerabilities in the banking infrastructures that can be exploited by threat actors.

These bank cards on dark web may expose financial institutions to the risk of losing maximum of 3639 X $12000 = $4,36,68,000 plus other available credit amount in Bangladesh Taka. This risk is associated to both the financial organizations and individual account holders.

As per the Guideline on ICT Security For Banks and Non-Bank Financial Institutions (Clause 4.2.6, Version 3.0, May 2015) all banks and financial institutions shall inform Bangladesh Bank as soon as possible in the event that a critical system has failed over to its disaster recovery system. But unfortunately due to possible reputational damage banks seldom report such incidents. BGD e-GOV CIRT during it's regular surveillance have found core banking systems and internet banking gateways accessible through internet. This exposes the total deposit of these financial institutions. BGD e-GOV CIRT has been assisting the central bank of Bangladesh and also other financial institutions to alert about any potential cyber attack and vulnerability exposure to take necessary precautions in order to protect their infrastructures, assets and deposits.

[64] https://www.thedailystar.net/hackers-active-12573
[65] https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery
[66] https://www.regulationasia.com/bangladesh-three-private-banks-hit-by-cyber-attacks/

Year	Threat Alert and Intelligence Report Provided to the Central Bank of Bangladesh and other Financial institutions
2021	31
2022	46

Bangladesh Financial Intelligence Unit illustrated the trend of e-commerce transaction using card in Bangladesh in the annual report 2021-2022

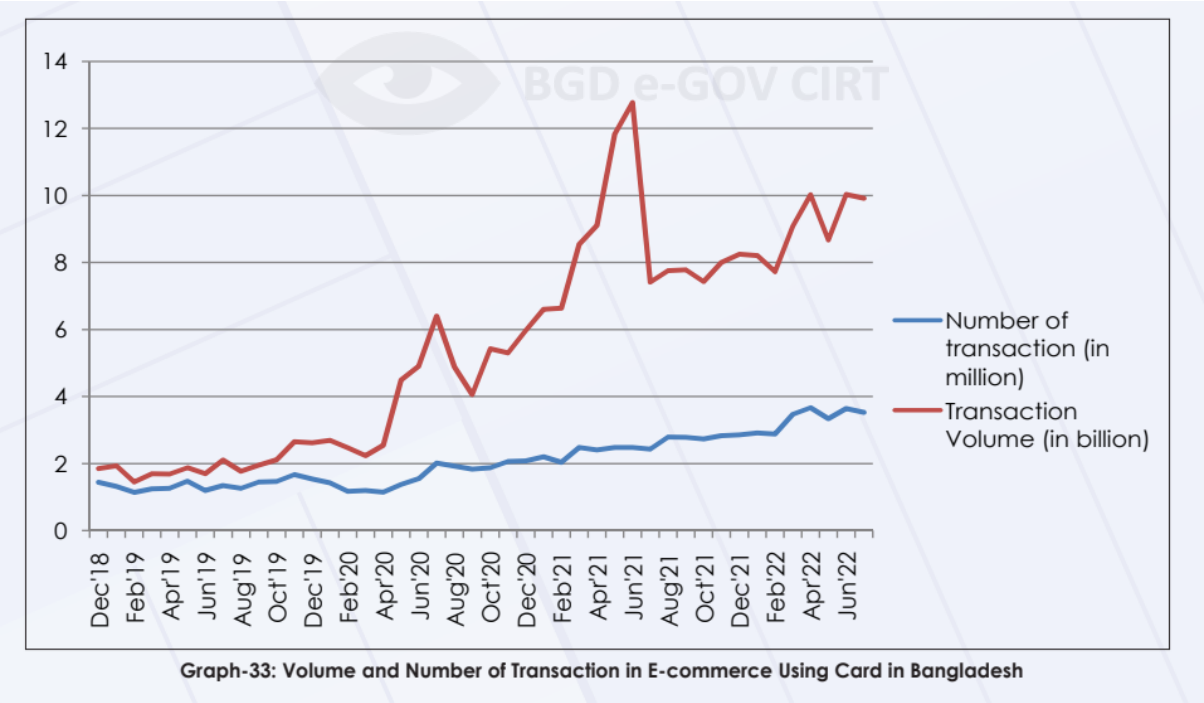


Figure 17: Trend of e-commerce transaction using Card in Bangladesh[67]

These new e-commerce and e-transaction platforms have created new opportunities for digital lifestyle but has also attracted cyber crime using phishing sites or fake business identities. For instance, advance payment of Tk339 crore from customers and merchants taken by Evaly till March 14 could not be traced, which authorities think have been embezzled or laundered.[68] Similar cases of online fraud are also reported for different e-commerce marketplace like E-Orange[69], Priyoshop, Dhamaka etc.

[67] https://www.bfiu.org.bd/pdf/pub/annual/2021-2022.pdf
[68] https://archive.dhakatribune.com/business/2021/07/25/it-is-not-possible-to-return-investments-just-by-closing-down-evaly#:~:text=A%20recent%20report%20by%20the,and%20Tk190%20crore%20from%20merchants.
[69] https://www.thedailystar.net/business/economy/e-commerce/news/e-orange-owners-staff-sued-embezzling-tk-1100-crore-customers-2154316

Vulnerable Service Exposure

Threat actors and cybercriminals are always sneaking in for vulnerable services which can be exploited to gain initial access to a targeted infrastructure. Later on, this exposure may lead to 'privilege escalation'[70] and 'lateral movement'[71] to facilitate the intruder to setup command and control[72] (C2) communication, steal data or execute ransomware attack by encrypting data.

Threat intelligence unit of BGD e-GOV CIRT states that the organizations, including CIIs, government and private sector, are being exposed with numerous vulnerable services which are lucrative for cyber criminals.

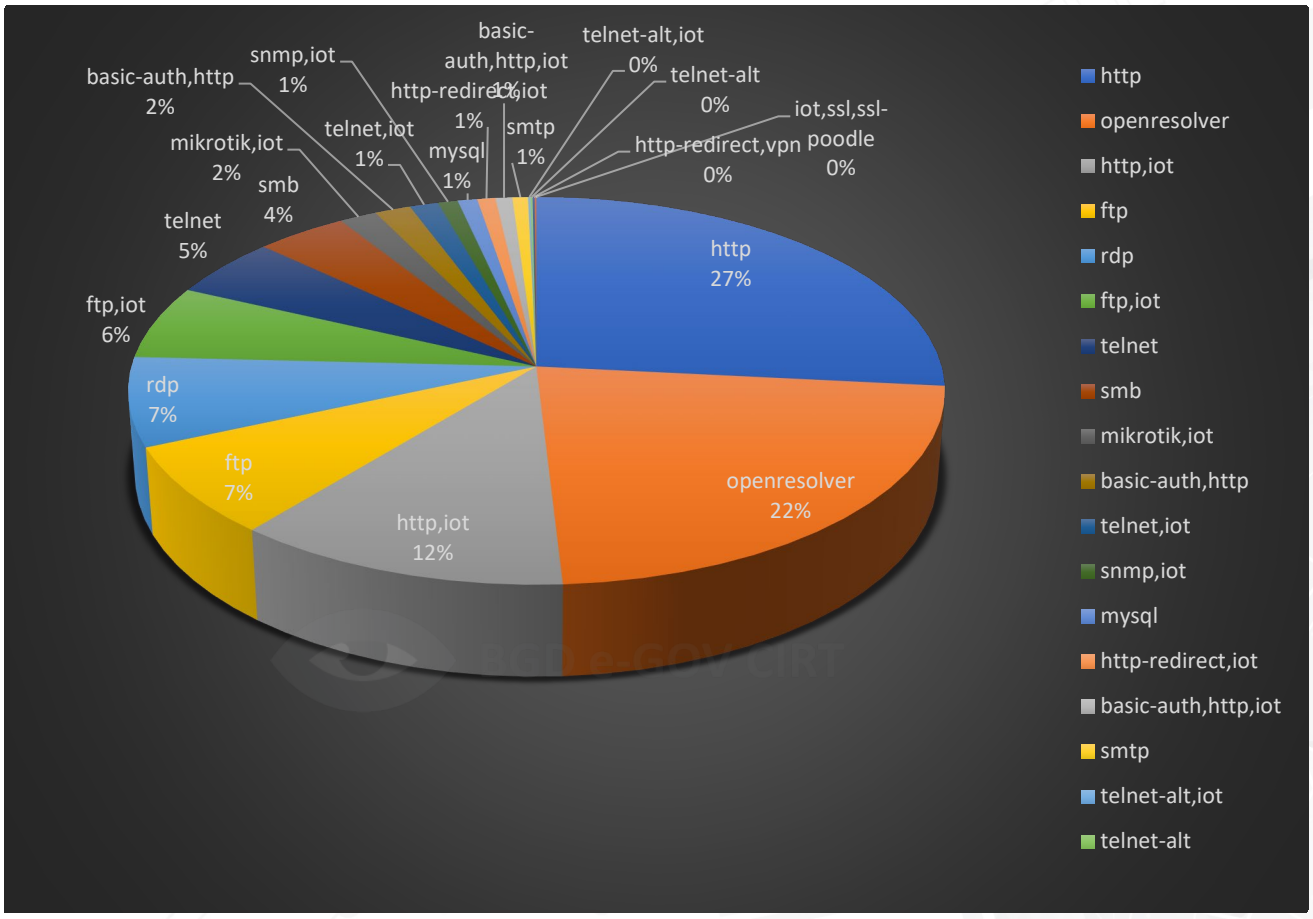


Figure 19: Identification of Vulnerable service exposure (Note: 0% means less than 1%)

Following section illustrates some of the common vulnerable service statistics considering the cyberspace of Bangladesh which requires attention –

[70] https://attack.mitre.org/tactics/TA0004/

[71] https://attack.mitre.org/tactics/TA0008/

[72] https://attack.mitre.org/tactics/TA0011/

HTTP based basic authentication

With Basic Authentication the user credentials are sent as clear text and because HTTPS is not used, they are vulnerable to packet sniffing. The Basic Authentication mechanism provides no confidentiality protection for the transmitted credentials. They are merely encoded with Base64 in transit, but not encrypted or hashed in any way. HTTPS is, therefore, typically preferred used in conjunction with Basic Authentication. Around **8,787** unique IP addresses are discovered with this sort of weak authentication.

Open DNS resolver

An "open DNS resolver" is a DNS server that resolves recursive DNS lookups for anyone on the internet. A simple lack of authentication allows malicious actors to propagate DNS amplification attacks and flood victim sites with fake DNS lookup requests, making them inaccessible. We have identified around **98,818** unique count of vulnerable IP addresses which are acting as open DNS resolver.

Telnet

Using telnet for remote login is absolutely discouraged as the credentials are transmitted in clear text which can be intercepted by bad actors. Around **14,454** unique IP addresses are identified to be using Telnet for remote access.

RDP

In recent years, there have been a number of security vulnerabilities discovered in RDP that can be exploited by attackers to gain unauthorized access to systems. One of the most well-known vulnerabilities is known as BlueKeep, and it was discovered in May 2019. BlueKeep is a vulnerability in the RDP implementation in Windows 7 and Windows Server 2008 R2 that can be used to execute arbitrary code on a remote system. **295** IP addresses are identified as susceptible to Bluekeep vulnerability.

SMB

SMB, or Server Message Block, is a network protocol that is used for file and printer sharing on Windows systems. The SMB protocol has been around for many years, and over time, several vulnerabilities have been discovered in various implementations of the protocol.

One of the most well-known SMB vulnerabilities is known as "EternalBlue." This vulnerability was discovered in 2017 and affects the SMB protocol implementation

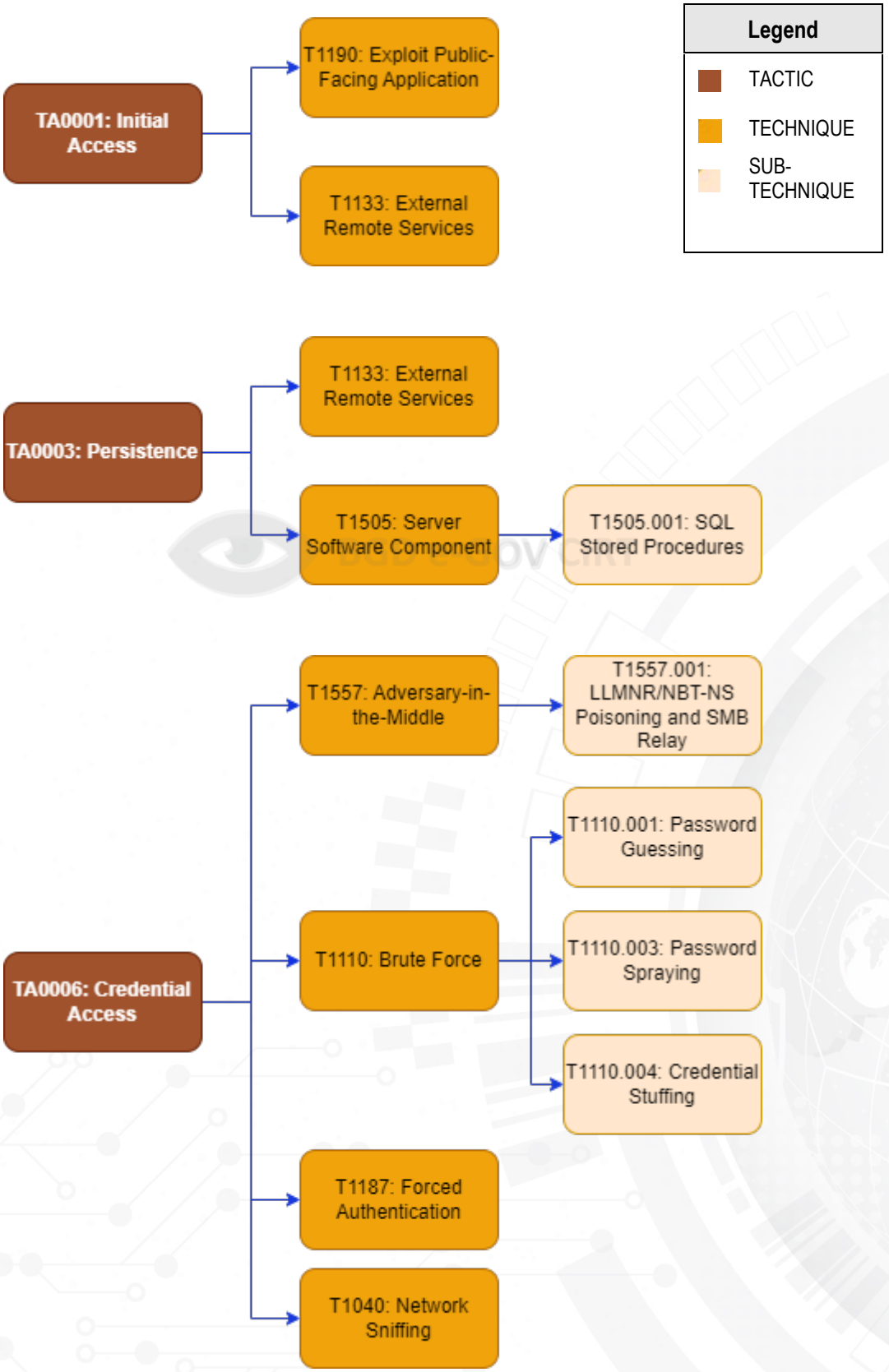
in Windows 7 and Windows Server 2008 R2. It allows an attacker to execute arbitrary code on a remote system by sending a specially crafted packet to the target system's SMB service. This vulnerability was used in the global WannaCry ransomware attack. Around **295** IP addresses are identified to be using **SMB V1.0** which is extremely vulnerable to allow remote code execution on target machine.

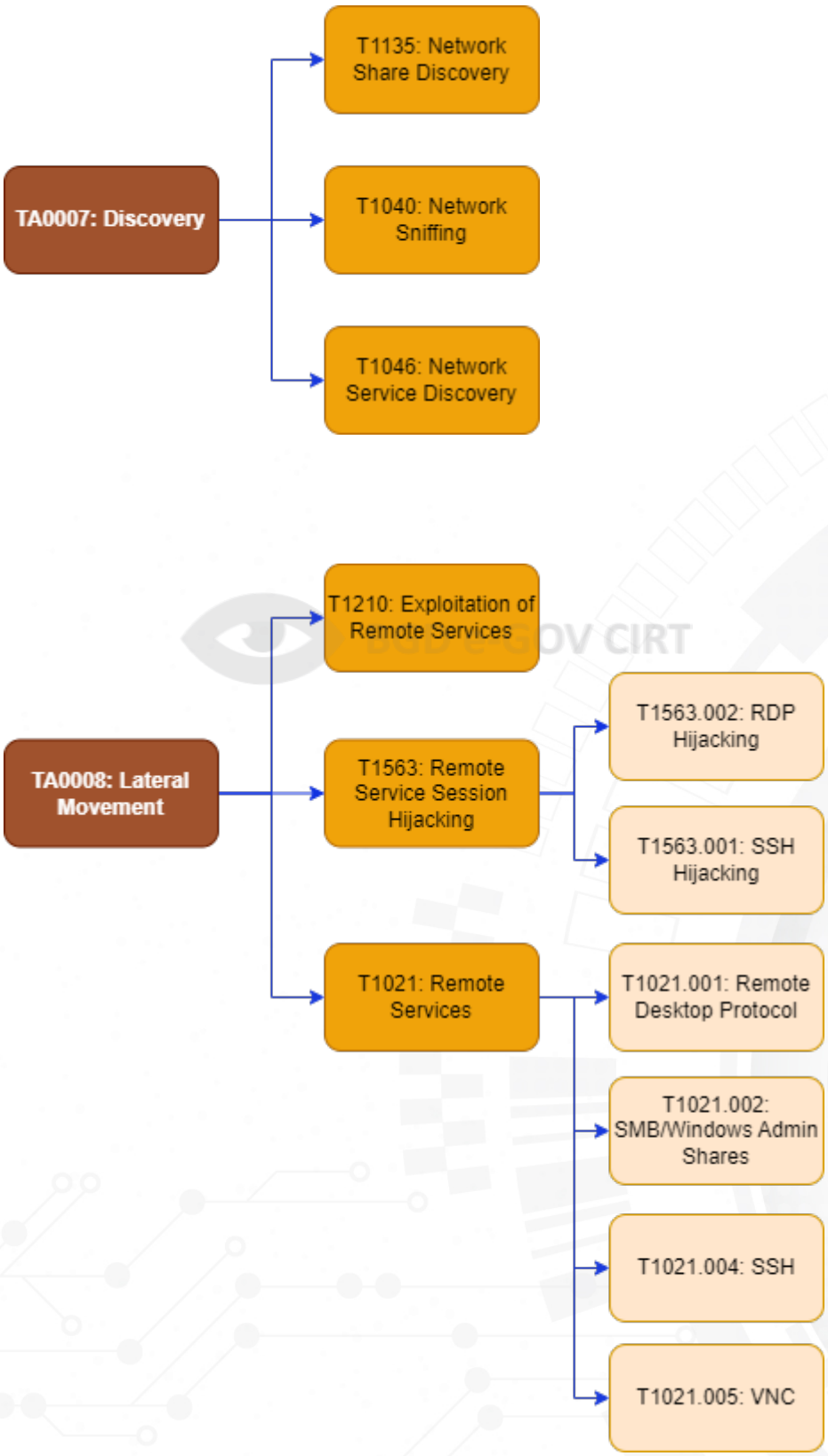
According to MITRE ATT&CK framework, exposure of such services can aid adversaries to accomplish several TACTICS (Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access[73])

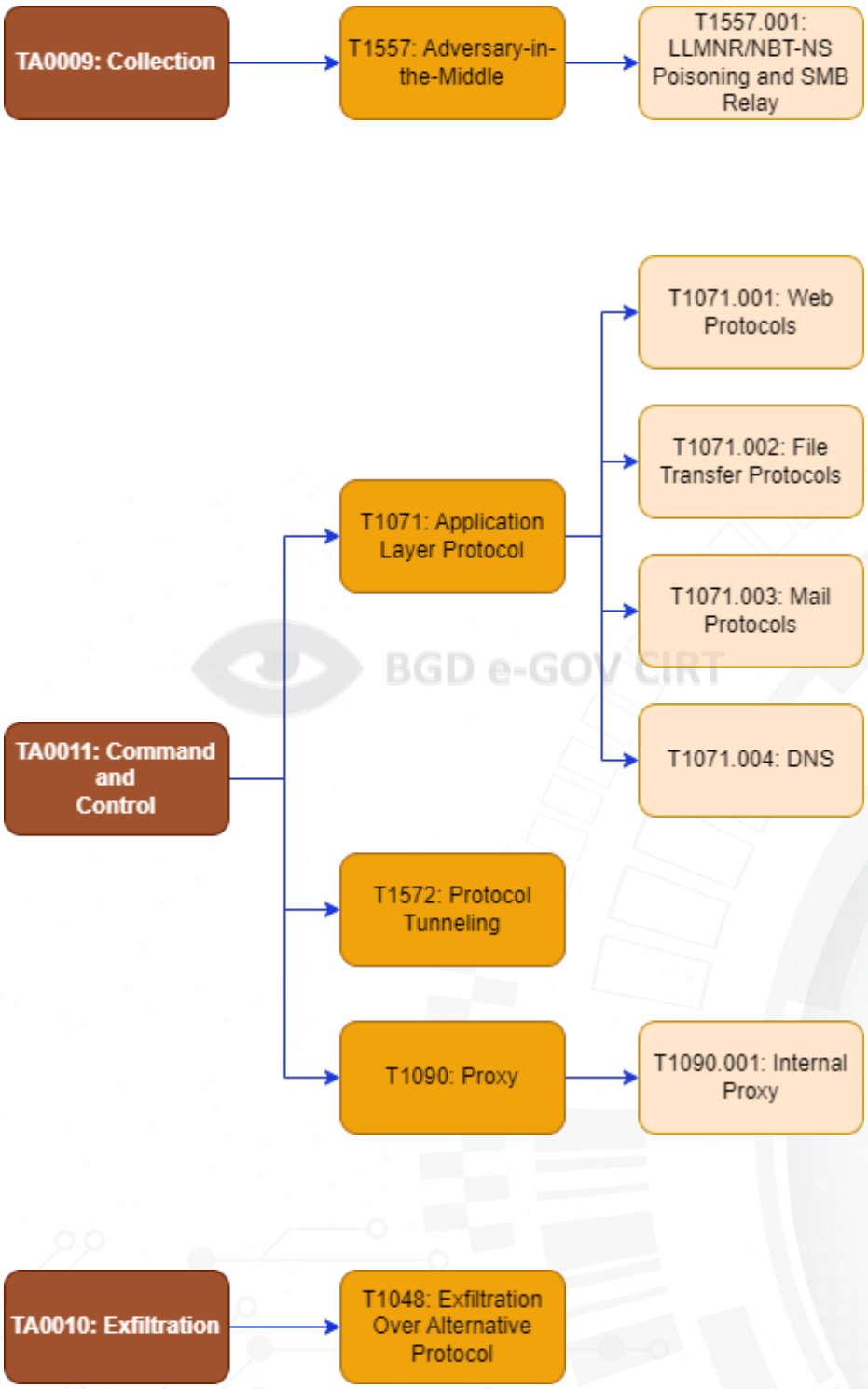
Exposure of these services may lead to accomplish TACTICS as Initial Access, Persistence, Credential Access, Discovery, Lateral Movement, Collection, Command & Control and Exfiltration by the threat actors. Following ATT&CK mapping shows the relevant Tactic, Technique and Sub-technique which adversaries may utilize by attacking these exposed services.

[73] https://attack.mitre.org/tactics/enterprise/

MITRE ATT&CK® Mapping for Vulnerable Services Exposure in Bangladesh




TA0007: Discovery
T1135: Network Share Discovery
T1040: Network Sniffing
T1046: Network Service Discovery
TA0008: Lateral Movement
T1210: Exploitation of Remote Services
T1563: Remote Service Session Hijacking
T1563.002: RDP Hijacking
T1563.001: SSH Hijacking
T1021: Remote Services
T1021.001: Remote Desktop Protocol
T1021.002: SMB/Windows Admin Shares
T1021.004: SSH
T1021.005: VNC


TA0009: Collection
T1557: Adversary-in-the-Middle
T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay
TA0011: Command and Control
T1071: Application Layer Protocol
T1071.001: Web Protocols
T1071.002: File Transfer Protocols
T1071.003: Mail Protocols
T1071.004: DNS
T1572: Protocol Tunneling
T1090: Proxy
T1090.001: Internal Proxy
TA0010: Exfiltration
T1048: Exfiltration Over Alternative Protocol

BANGLADESH CYBER THREAT LANDSCAPE

YEAR 2022

Powered by

CYBER TIIR [Threat Intelligence & Incident Research]

A product of BGD e-GOV CIRT

978-984-35-4011-9