TLP: GREEN

Bangladesh Cyberthreat Landscape

Jan - Dec 2020

Risk Assessment Unit | BGD e-GOV CIRT

BASED ON WORKSHOP AND ONLINE SURVERY

BGD e-GOV CIRT

1. 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.

Information classification according TLP in BGD e-GOV CIRT

TLP	Distribution principle	Mapping with the business category	Description
RED	(1-to-1, strictly limited)	Confidential information	Sensitive information disclosure of which can harm BGD e-GOV CIRT or its external parties' reputation, operations, or includes personal BGD e-GOV CIRT team members or external parties' data and information which is treated as confidential information in BGD e-GOV CIRT agreements
AMBER	(1-to-group, limited)	Internal information	Incidents information and all other information which is not treated as a public or confidential
GREEN	(1-to-many, limited)/(information security community or special interest groups)	Public information	Information which was disclosed publicly in accordance with internal BGD e-GOV CIRT procedures or related agreements with external parties
WHITE	(1-to-many, unlimited)(no restrictions, public)		

2. TABLE OF CONTENTS

3. DOCUMENT INFORMATION

Project Director:	Tarique M Barkatullah	**Document version No.:**	V. 1.0
Document status	Final	**Document version date:**	15 December 2020
Prepared by:	Tamim Ahmed	**Preparation date:**	15 December 2020
Reviewed by:	Md. Sabbir Hossain	**Review date:**	20 December 2020

4. ABBREVIATIONS

APCERT	Asia Pacific Computer Emergency Response Teams
API	Application programming interface
APT	Advanced Persistent Threat
BCC	Bangladesh Computer Council
CII	Critical Information Infrastructure
DDoS	Distributed Denial of Service
DoS	Denial of Service
ENISA	European Union Agency for Network and Information Security
LFI	Local File Inclusion
MoPTIT	Ministry of Posts, Telecommunications and Information Technology of the People's Republic of Bangladesh
OWASP	Open Web Application Security Project
Q	Quarter
SOC	Security Operation Centre
XSS	Cross-site Scripting

5. PREFACE

This report aims to define national Bangladesh cyberthreat landscape for the year 2020. The findings of this report will be used for establishing national risk context for national cybersecurity strategy review as well as feed into threat list parameter of risk assessment process.

Government, Industry & all CII may further use this report to raise awareness on national cyberthreat 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 cyberthreat 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.

6. BANGLADESH CYBERTHREAT LANDSCAPE

6.1 Introduction

Cyber threat is a growing risk that is increasing every day. New threats are showing up to the horizon as well as old threats are evolving with time and technology regularly. With availability of hacking as a service and lot of free tools to generate scripts as well as other threats automatically make this attack method wide open even for the novice. As we are living in era of globalization, these evolving threats are also affecting Bangladesh equally. Each year BGD e-GOV CIRT publishes "Bangladesh Cyber Threat Landscape" report by collecting information from Critical Information Infrastructures. This year the format is a little different. We have collected the information from Critical Information Infrastructure, Government Agencies, Law Enforcing Agencies, Industry & Academia and based on their inputs preparing this document. 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 lot of Threat Landscapes. However, each nation has its own eccentricities, and in order to 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.

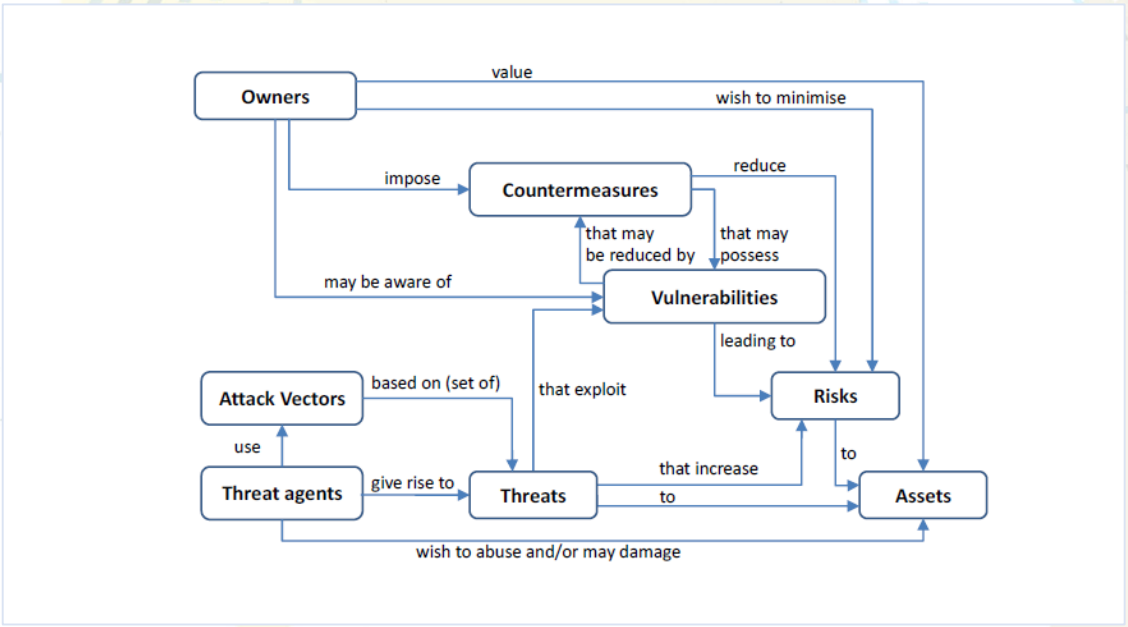


Figure 1. Cyberthreats in risk management according to ISO 15408:2005

For the development of Bangladesh cyberthreat landscape, workshop and survey was conducted. Participants of the workshop were introduced to the current trends in cyberthreat

landscape. Based on the results of an anonymous survey, Bangladesh top 15 cyberthreats have been identified and are recorded in this report.

This report will be used to raise awareness on national cyberthreat 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. Also, it is highly recommended to keep Bangladesh cyberthreat landscape up to date by reviewing and adjusting it annually by using national statistical data on cybersecurity incidents and following international cyber security landscape changes.

6.2 Overview of Bangladesh cyberthreats

This section provides an overview of Bangladesh cyberthreat landscape, comparison with ENISA cyberthreat landscape 2020 and comparison with last years' threat landscape, including how Bangladesh top threats differ from ENISA's report. Also, it visualizes involvement of threat agents in Bangladesh top cyberthreats.

Bangladesh Top Threats	
1.	Spam
2.	Ransomware
3.	Phishing
4.	Malware
5.	Information leakage
6.	Insider threat
7.	Identity theft
8.	Web based attack
9.	Data breach
10.	Denial of Service
11.	Web application attacks
12.	Botnets
13.	Cryptojacking
14.	Physical manipulation/ damage/ theft/loss
15.	Cyber espionage

Figure 2. Bangladesh Top Threats-2020

When compared with ENISA threat landscape 2020, Bangladesh cyberthreat landscape has some specificity. Due to covid19 pandemic It is noted that the role of spam and phishing in the overall Bangladesh cyberthreat landscape is significantly higher. Other threats in Bangladesh cyberthreat landscape follow international threat landscape and change in the ranking is due to spam, phishing and ransomware climbing to higher positions, Web application attacks going down and inevitably leading to change in ranking to other threats.

Bangladesh Top Threats 2020	Change in ranking	Top Threats 2020 by ENISA
1. Spam	↑	1. Malware
2. Ransomware	↑	2. Web based attack
3. Phishing	→	3. Phishing
4. Malware	↓	4. Web application attacks
5. Information leakage	↑	5. Spam
6. Insider threat	↑	6. Denial of Service
7. Identity theft	→	7. Identity theft
8. Web based attack	↓	8. Data breach
9. Data breach	↓	9. Insider threat
10. Denial of Service	↓	10. Botnets
11. Web application attacks	↓	11. Physical manipulation/ damage/ theft/loss
12. Botnets	↓	12. Information leakage
13. Cryptojacking	↑	13. Ransomware
14. Physical manipulation/ damage/ theft/loss	↓	14. Cyber espionage
15. Cyber espionage	↓	15. Cryptojacking

Comparison between last years' (2019) Threat Landscape with this years' (2020) landscape is give below.

Bangladesh Top Threats 2019	Change in ranking	Bangladesh Top Threats 2020
1. Malware	↓	1. Spam
2. Spam	↑	2. Ransomware
3. Phishing	→	3. Phishing
4. Web based attack	↓	4. Malware
5. Denial of Service	↓	5. Information leakage
6. Insider threat	→	6. Insider threat
7. Web application attacks	↓	7. Identity theft
8. Ransomware	↑	8. Web based attack
9. Data breach	→	9. Data breach
10. Botnets	↓	10. Denial of Service
11. Physical manipulation/ damage/ theft/loss	↓	11. Web application attacks
12. Information leakage	↑	12. Botnets
13. Cryptojacking	→	13. Cryptojacking
14. Identity theft	↑	14. Physical manipulation/ damage/ theft/loss
15. Cyber espionage	→	15. Cyber espionage

Figure 3. Comparison Bangladesh Threat Landscape 2019 and 2020

7. BANGLADESH TOP CYBERTHREATS

Bangladesh cyberthreat landscape was developed based on the results of an anonymous survey and workshop participations. A cyberthreat is assigned a rank in this report based on the number of incidents and their impact to a survey participant and weighted (weight distributed from 0 to 100%) position in ENISA's threat landscape report 2020. Format for the survey is presented at Annex 8.1.

7.1 Spam

Spam is unsolicited emails, most often send in bulk and is one of the most prevalent and persistent cyberthreats in the world. It remains the main means for malware delivery through malicious attachments and malicious URLs. Spam accounts for more than half the volume of e-mails worldwide and is mainly distributed by large spam botnets. Spam messages are most frequently used channel for cyber-criminals. Spam caused incidents are attributable to abusive content incident class.

Spam along with phishing and ransomware is the most frequently encountered and having most significant impact cyberthreat in Bangladesh.

In November 2020, the average daily spam volume globally was around 210.54 billion, which corresponds to around 84.83% of the total daily email volume[1].

In November 2020, Top 10 Spam sources by country were United States, Russian Federation, China, Brazil. **Bangladesh ranked 29th among the spam sources by country** and accounts for 7.1% of world's spam volume[2].

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.**

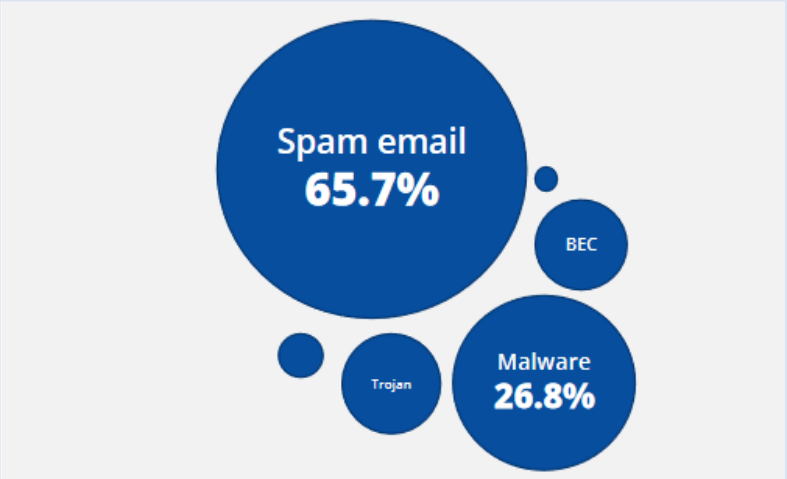


Figure: 4 Threat Leveraging from COVID-19, Source Trend Micro 1

[1] https://talosintelligence.com/reputation_center/email_rep#global-volume
[2] https://talosintelligence.com/reputation_center/email_rep#top-senders-country

7.2 Ransomware

Ransomware is a malicious software that either encrypts files or locks the home screen to demand a ransom from its victims to access the files and device. Ransomware is attributable to malicious code incident class. Ransomware cybercriminals had begun to find momentum with this new business model even before the pandemic struck. A combination of emboldened threat actors earning large sums of money enabling them to invest and improve their operations, and a general weakening of organizational security, due to, among others, mistakes made as a result of increased stress, loss of staff and income, and a larger attack surface caused by increased remote working, can only serve to make things worse for businesses in the short term.

The most common ransomware attack continues to be poorly secured Remote Desktop Protocol (RDP) access points which has been intensified by the fact that there has been a marked increase in exposed RDP endpoints due to the surge in the need for remote working. What is more, ransomware threat actors are now targeting vulnerabilities in Virtual Private Networks (VPNs) and other remote working tools and software—in particular Sodinokibi has infected victims by exploiting unpatched Pulse Secure VPN servers[3]. Egregor is a ransomware from the Sekhmet malware family that has been active since the middle of September 2020. The ransomware group hacks into companies, steals information, and finally encrypts all the data.[4]

Top 10 countries attacked by ransomware Trojans

	Country*	**%****
1	Bangladesh	2.37
2	Mozambique	1.10
3	Ethiopia	1.02
4	Afghanistan	0.87
5	Uzbekistan	0.79
6	Egypt	0.71
7	China	0.65
8	Pakistan	0.52
9	Vietnam	0.50
10	Myanmar	0.46

[3] https://www.accenture.com/_acnmedia/PDF-137/Accenture-2020-Cyber-Threatscape-Report.pdf#zoom=50
[4] https://www.cirt.gov.bd/egregor-ransomware/

Top 10 most common families of ransomware Trojans

	Name	Verdicts	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	18.77
2	(generic verdict)	Trojan-Ransom.Win32.Gen	10.37
3	(generic verdict)	Trojan-Ransom.Win32.Encoder	9.58
4	(generic verdict)	Trojan-Ransom.Win32.Generic	8.55
5	(generic verdict)	Trojan-Ransom.Win32.Phny	6.37
6	Stop	Trojan-Ransom.Win32.Stop	5.89
7	(generic verdict)	Trojan-Ransom.Win32.Crypren	4.12
8	PolyRansom/VirLock	Virus.Win32.PolyRansom	3.14
9	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	2.44
10	(generic verdict)	Trojan-Ransom.Win32.Crypmod	1.69

Figure: 5 Source: Kaspersky IT threat evolution Q3 2020 [5]

Ransomware ranks 2nd in Bangladesh top threats.

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.

The overall trend of ransomware activity in 2020 was increased.

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

[5] https://securelist.com/it-threat-evolution-q3-2020-non-mobile-statistics/99404/

7.3 Phishing

Phishing attacks are attempts by cybercriminals to capture sensitive information by masquerading to be banks, social media platforms and other official entities otherwise known as social engineering. Phishing is an important attack vector for all types of threat agents but is most successful for data breaches and security incidents. Phishing is becoming more and more sophisticated and targeted and relates to botnets, malware, web-based attacks, exploit kits, cyber espionage, etc. Phishing is attributable to fraud incident class.

Phishing ranks 3rd in Bangladesh top threats.

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 is human element and web and browser-based attacks. APWG third quarter report of 2020 shows that most target of phishing are webmail/SAAS and second highest is Financial Institute.

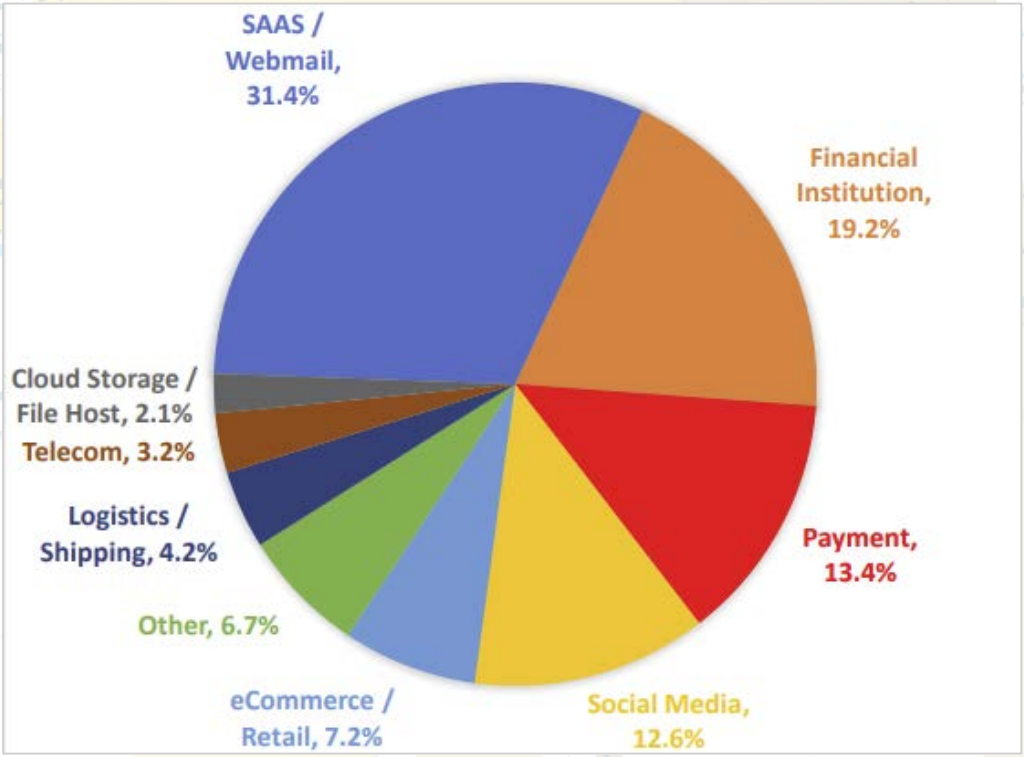


Figure: 6 Source: APWG Phishing Activity Trends Report[6]

The overall global trend of phishing in 2020 was Increasing.

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

[6] https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf

7.4 Malware

Malware is a Portmanteau term comprised of "malicious" and "software". Although frequently used interchangeably with "virus", it encompasses a much broader range of threats, including adware, keyloggers, rootkits, spyware, Trojans, viruses and warms. Malware caused incidents are attributable to malicious code incident class.

Malware is the one of the most frequently encountered and having most significant impact cyberthreat in Bangladesh

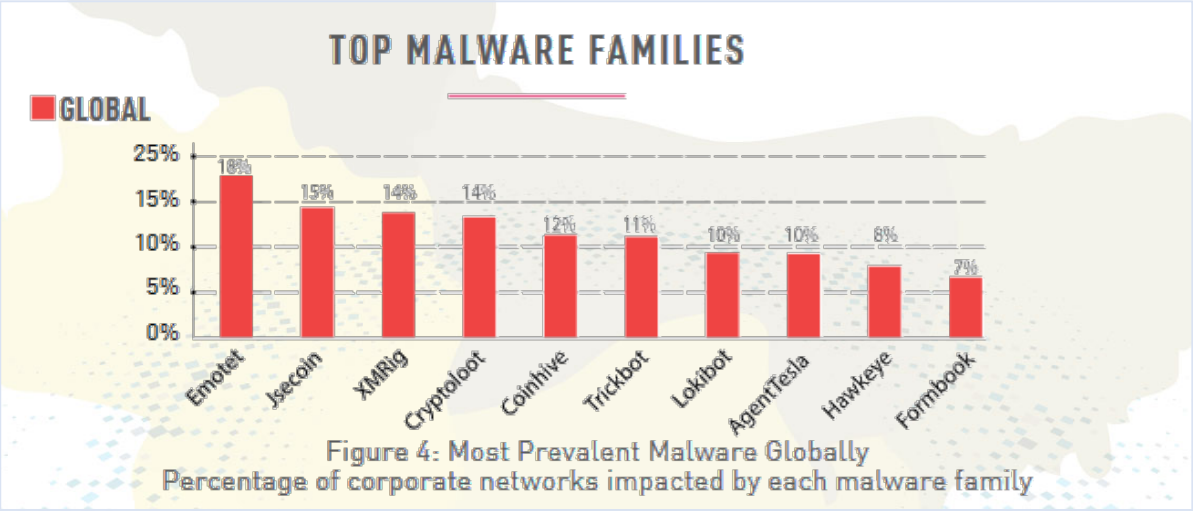


Figure:7 Source: Check Point: Cyber Security Report[7]

Top Malware family in Bangladesh (period of January,2020 to September,2020) are:

- AZORult
- KPOT Stealer
- Oski Stealer
- FormBookFormgrabber
- Loki PWS
- Nexus Stealer
- TrickBot
- Kinsing Malware
- Outlaw hacking group cryptocurrency miners

Advanced Persistent Threat (APT) threats in Bangladesh:

- Lazarus
- Silence
- OceanLotus

Figure:8 Source: Major Malware Threat Intelligence Report for Bangladesh Context[8]

The overall global trend of malware in 2020 was Same as last year the most detections from all other threats. Primary group of threat agents for malware is **cyber criminals, nation states and corporations.**

[7] https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf
8https://www.cirt.gov.bd/wp-content/uploads/2020/10/Malware-Threat-Intelligence-Report-for-Bangladesh-Context-Oct-2020-.pdf

7.5 Information leakage

Information leaks varies from personal data collected by Internet giants and online services to business data stored in companies' IT infrastructures. Human error is one of the most important factors in breaches, and trusted but unintentional insiders are to blame. Information leakage is attributable to information content security incident class.

Information leakage ranks 5th in Bangladesh top threats.

Insiders are the primary attack vector in the leakage of information. Misconfigurations, bugs and human errors are other common attack vectors that this threat uses.

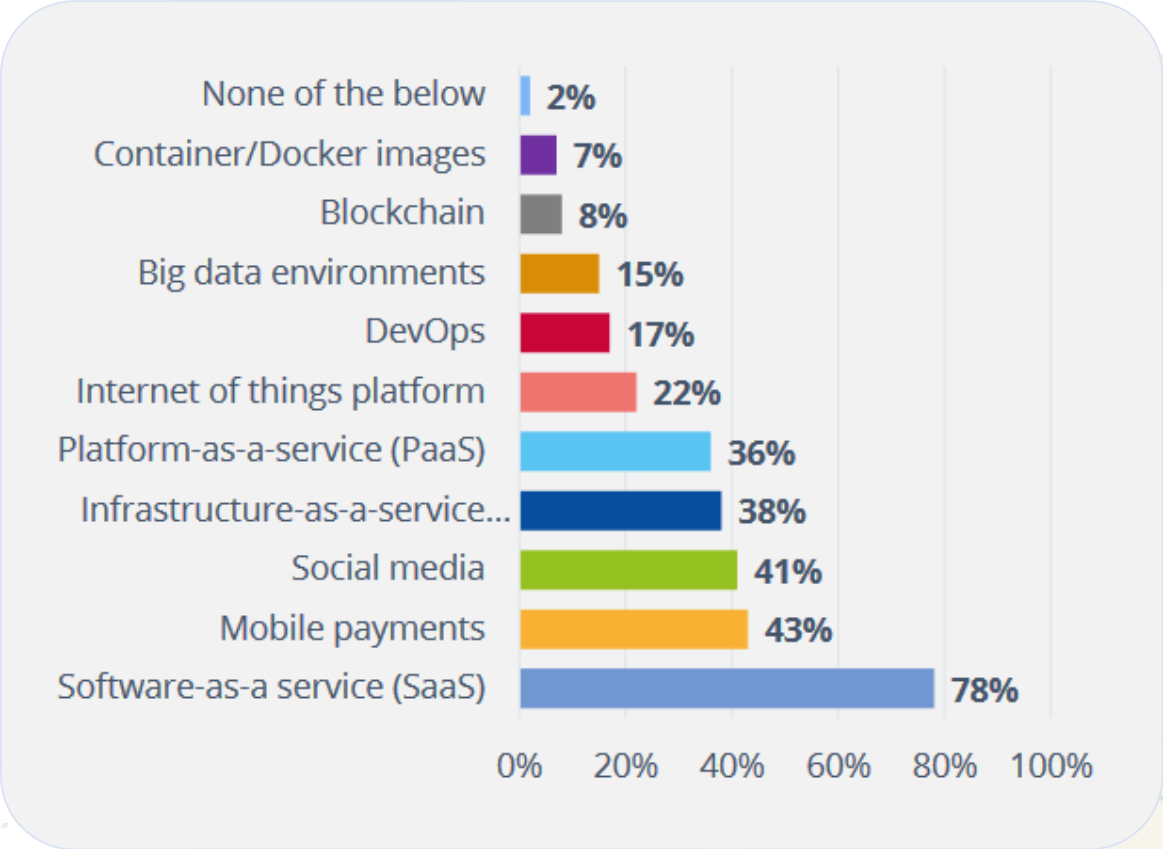


Figure 9: Types of sensitive or regulated data stored. Source: Thales [9]

The primary attack vector in information leakage is insiders. Other common attack vectors used by this threat are misconfiguration, vulnerabilities and internet exposed assets.

The overall trend of information leakage in 2020 was Increasing.

Primary group of threat agents for information leakage is **cyber criminals, nation states and corporations.**

[9] https://www.thalesesecurity.com/2020/data-threat-report

7.6 Insider threat

Insider threat refers to the threat that an insider will use his/ her legitimate access to do harm to the security of an organization. Insider incidents may be intentional or inadvertent, whereas the latter is the most frequent form of insider abuse. Detection of rouge insiders is the third of the top 3 challenges that SOCs face, preceded by detection of advanced/unknown threats and lack of security staff.[10] Insider threat is attributable to other incident class.

Insider threat ranks 6th in Bangladesh top threats.

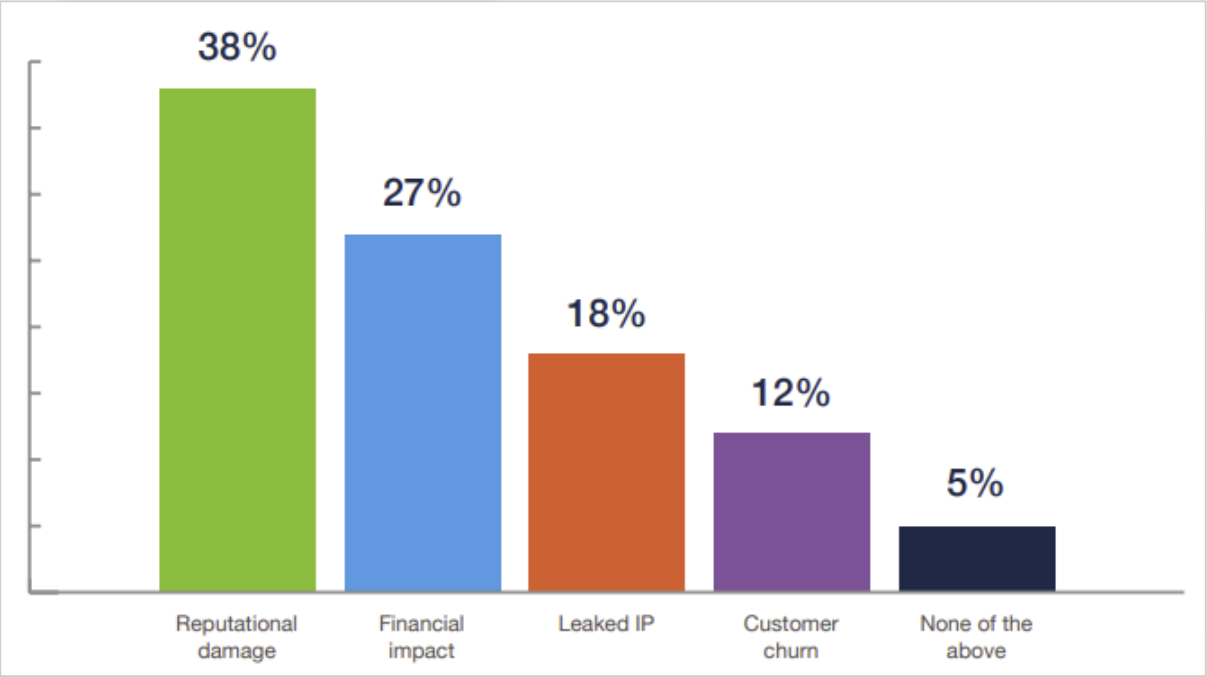


Figure 10: Impact area of insider threat incidents [11]

According to the same survey, endpoints, mobile devices, network and file servers are most commonly used to launch an insider attack.

The overall trend of insider threats in 2020 was Increasing.

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

[10] http://www.cybersecurity-insiders.com/wp-content/uploads/2017/02/2017-Threat-Hunting-Report.pdf
[11] https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

7.7 Identity theft

Identity theft is a cyberthreat in which the attacker aims at obtaining confidential information that is used to identify a person or even a computer system (names, addresses, contact data, credentials, financial data, health data, logs, etc.). Subsequently, this information is abused to impersonate the owner of the identity. Fraudsters acquire identity data in various ways – hacking, dark web shopping, exploiting personal information on social media, social engineering. Identity thefts are attributable to information content security incident class.

Identity theft ranks 7th in Bangladesh top threats.

Globally, most common types of identity theft are the following:

Type of data	2019	2018	2017
E-mail	70	44	32
Password	64	39	27
Name	23	37	41
Miscellaneous	18	19	15
Social security number	11	22	27
Credit card	11	16	19
Address	11	22	30
Account	10	7	4
Unknown	8	13	18
Date of birth	8	13	12
Medical	5	9	7
Financial	5	13	19

Figure 12: Most common types of identity theft [12]

TOP 5 identity theft threats come from:

- **Skimmers**. An identity theft method where fraudsters place these devices (skimmers) over card readers at checkout registers, gas stations or ATMs. Skimmers store credit and debit card information and fraudsters can then use this data to make counterfeit cards, use them for online purchases, or sell them on the black market.
- **Dumpster divers**. Fraudsters dig through trash or mailbox, looking for bank statements, copies of tax returns and other documents that have personal information.
- **Phishers**. Phishers use authentic-looking e-mails and websites to trick users to click on a link or open an attachment that will download malware onto their computers and leave confidential information vulnerable.
- **Hackers**. These threat agents install malware on computer networks, legitimate websites, and by extension to user systems, and steal personal information.

[12] https://www.lifelock.com/education/how-common-is-identity-theft

- **Telephone impersonators**. Fraudsters may contact a bank's call centre many times, each time gaining a different piece of information until they have enough information to impersonate an actual bank customer and gain account access.

The primary attack vectors for identity thefts are attacking human element and internet exposed assets. Some of the most common information that people unknowingly make available online and can be abused includes birthdates, phone numbers, credit card information, etc. [13]

The overall trend of identity theft follows the trends of data breaches and in 2020 was Increasing.

Primary group of threat agents for identity theft is **cyber criminals, insiders, nation states, corporations, hacktivists, cyber fighters and cyber terrorists.**

7.8 Web-based attacks

Web-based attacks are those attacks that make use of web-enabled systems and services (browsers and their extensions, websites and their Content Management Systems, and the IT-component of web services and web applications. Globally, web-based attacks are very popular in combination with malware campaigns.

Web-based attacks are also common in Bangladesh and rank 8th in Bangladesh top threats.

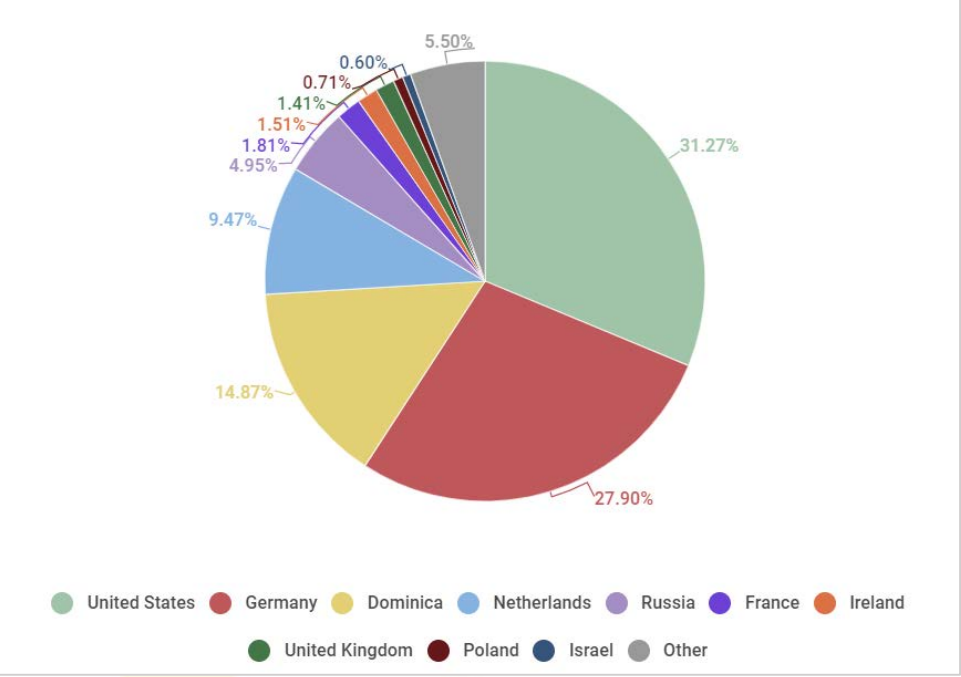


Figure: 13 Web-Based Attack distribution by source Country [14]

[13] https://www.experian.com/blogs/ask-experian/survey-findings-are-consumers-making-it-easier-for-identity-thieves
14 https://securelist.com/it-threat-evolution-q3-2020-non-mobile-statistics/99404/

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. Web browser vulnerabilities continue to represent a big threat for users. Most of the known financial malware use browser exploits (when malicious code takes advantage of a flaw or vulnerability in an operating system or piece of software to alter a user's browser settings) and man-in-the browser techniques. Number of malicious URL's is very high, and they are commonly used to spread malware. Drive-by downloads is another specific attack vector commonly used by cybercriminals to spread malware by planting a malicious script into HTTP or PHP code on the website and require no action by the victim – just simply visit the compromised website and be infected automatically if their computer is vulnerable. Water-holing malware attack method is used by attackers to infect the websites often visited by the targeted victim.

The overall trend of web-based attacks in 2020 was Same as previous year.

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

7.9 Data breach

Data breach is unauthorized movement or disclosure of sensitive information to someone that is not authorized to have or see that information. Data breach incidents are encountered ex-post – when a data breach is being assessed, the successful incident has already happened. Data breach is attributable to information content security incident class.

Data breach ranks 9th in Bangladesh top threats.

Main Attack vectors are E-Mail/Phishing, Cloud/Web Applications, Insider Threat

Data breaches by sector and organization size

Incidents	Breaches	Small	Large	Unknown
Accommodation	61	34	7	20
Administrative	17	6	6	5
Agriculture	2	2	0	0
Construction	11	7	3	1
Education	99	14	8	77
Entertainment	10	2	3	5
Finance	207	26	19	162
Healthcare	304	29	25	250
Information	155	20	18	117
Management	2	1	1	0
Manufacturing	87	10	22	55
Mining	15	2	5	8
Other services	54	6	5	43
Professional	157	34	10	113
Public	330	17	83	230
Real Estate	14	6	3	5
Retail	139	46	19	74
Trade	16	4	8	4
Transportation	36	3	9	24
Utilities	8	2	0	6
Unknown	289	0	109	180
Total	2.013	271	363	1,379

Figure 14 Source: Verizon DBIR, 2019 [15]

The overall trend of data breaches in 2020 was Same as previous year. Primary group of threat agents for data breach is **cyber criminals, insiders, nation states, corporations, hacktivists and cyber fighters.**

[15] https://enterprise.verizon.com/resources/reports/dbir/

7.10 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.

Denial of service ranks 10th in Bangladesh top threats.

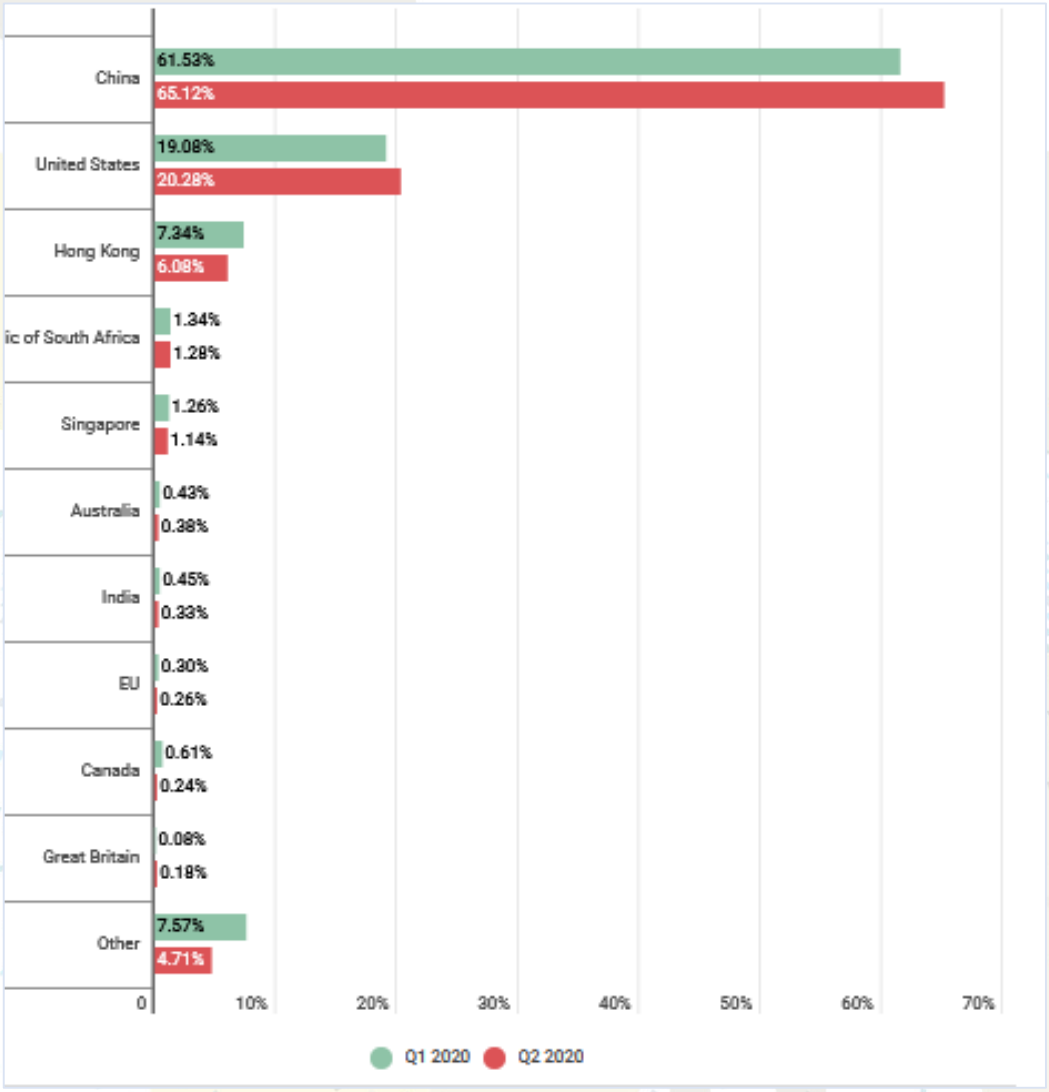


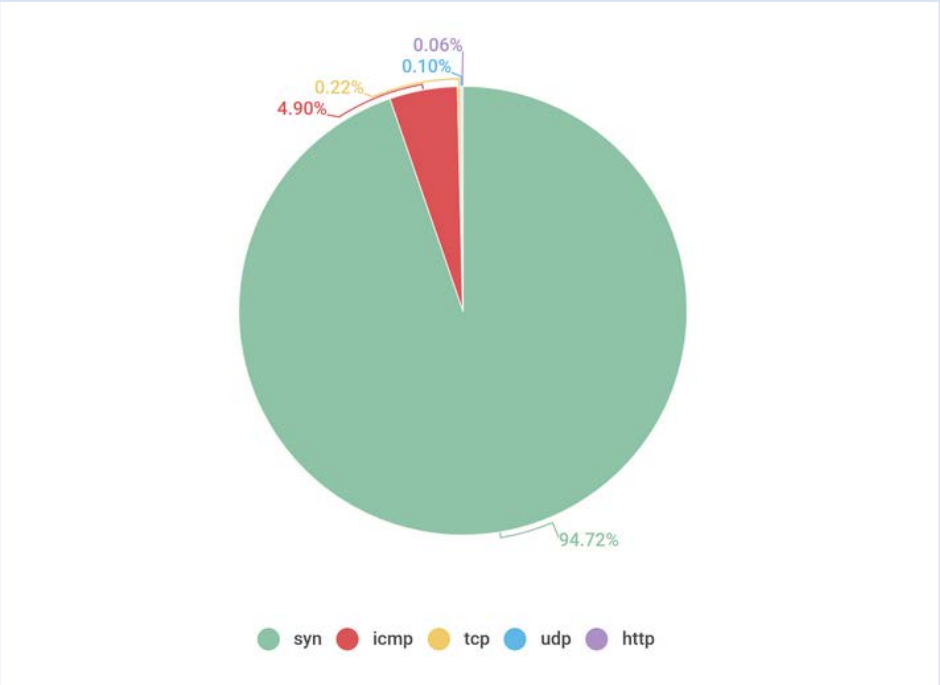
Figure 15. Distribution of DDoS attacks by country Q1 and Q2 2020 [16]

The specific attack vectors for Denial of Service attacks are SYN flooding, UDP fragments, DNS floods, NTP floods, and CHARGEN attacks.

SYN flooding in the quarter was 94.7% (up by 2.1 p.p.). For a second consecutive quarter, the leader is followed by ICMP flooding (4.9%), which is 1.3 p.p. above the previous reporting

[16] https://securelist.com/ddos-attacks-in-q2-2020/98077/

period. TCP attacks accounted for 0.2% of the total number, and UDP and HTTP attacks (0.1%) round out the list [16]



Distribution of DDoS attacks by type, Q2 2020

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 16: Top 10 Sources in APAC (Asia Pacific) region [17]

The overall trend of denial of service attacks in 2020 was Decreasing.

[17] https://blog.nexusguard.com/threat-report/ddos-threat-report-2020-q2

7.11 Web application attacks

Web application attacks are those attacks directed against available web applications, web services, and mobile applications. Web application attacks are attributable to intrusion attempts incident class. These types of attacks are very popular globally and are expected to remain. So, government and financial organizations representing tempting targets. Web application attacks are attributable to intrusion attempts incident class.

Web application attacks are common in Bangladesh and ranks 11th in Bangladesh top threats.

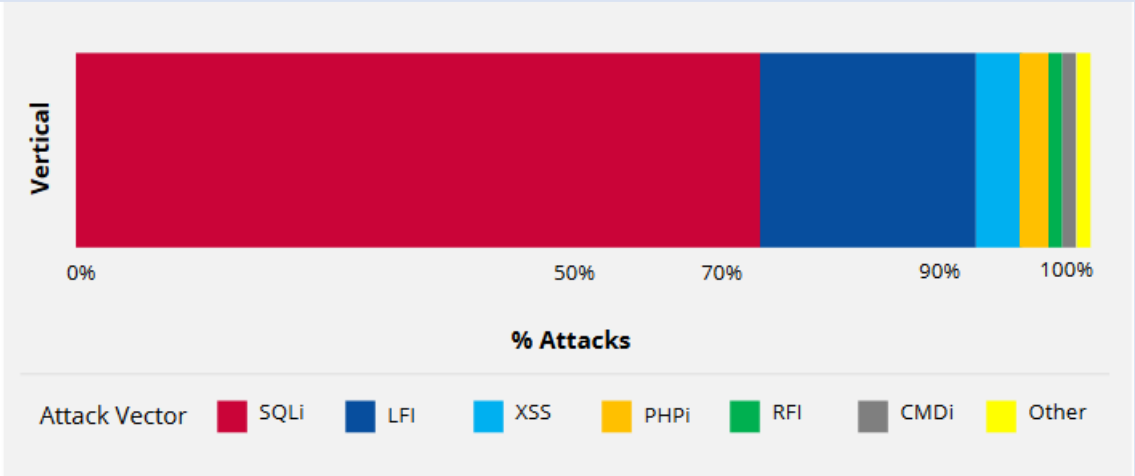


Figure 17 SQLi continues to dominate when looking at all verticals 18

The attack vectors for web application attacks are web and browser attacks, internet exposed assets, exploitation of vulnerabilities/ misconfigurations and cryptographic/ network/security protocol flaws and supply chain attacks. The most prevalent web application attacks are SQL Injection attacks, Local File Inclusion, Cross-site Scripting (XSS), Remote File Inclusion and PHP injections or PHP Object Injection.

The overall trend of web application attacks in 2020 was Same as previous year.

Primary group of threat agents for web application attacks is **cyber criminals, nation states, corporations, hacktivists and cyber fighters.**

Primary group of threat agents for denial of service is **cyber criminals, hacktivists, cyber fighters and script kiddies.**

18 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

7.12 Botnets

Botnets are a connected network of computers, usually controlled by a command and control centre, that communicate together in order to accomplish certain tasks.

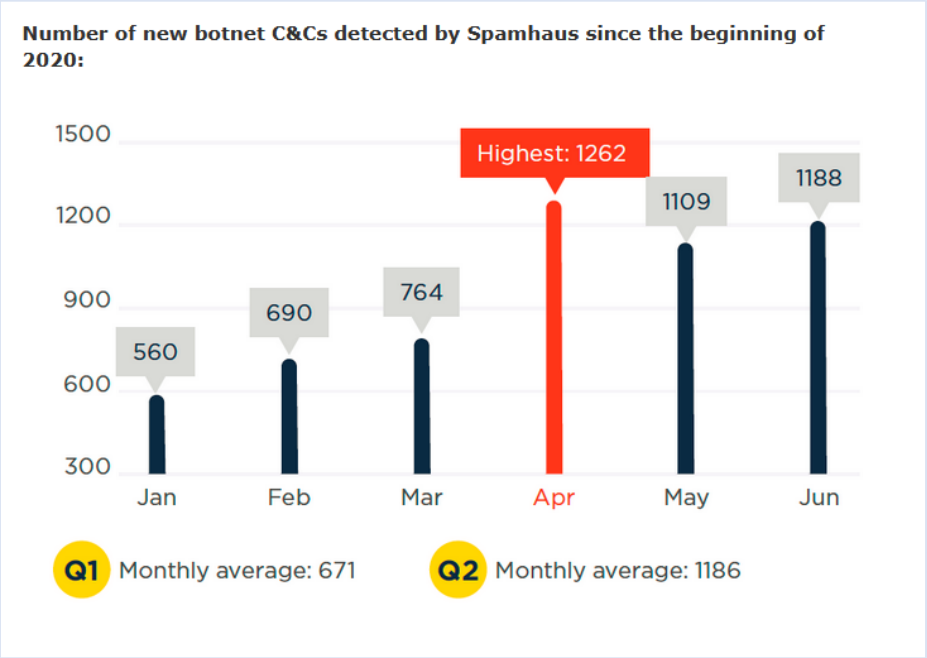


Figure 18 Source: Spamhaus Botnet Threat Update: Q2-2020 [19]

Botnets rank 12th in Bangladesh top threats survey.

Top 20 locations of botnet C&Cs

Rank	Country	Q2 2020	% Change Q on Q	Rank	Country	Q2 2020	% Change Q on Q
#1	United States	896	7%	#11	Sweden	59	136%
#2	Russia	812	32%	#12	Canada	53	56%
#3	Netherlands	337	61%	#13	Ukraine	50	92%
#4	Germany	185	7%	#14	Estonia	46	New Entry
#5	Singapore	131	157%	#15	Moldova	45	105%
#6	France	108	35%	#16	Turkey	44	100%
#7	Great Britain	89	37%	#17	Romania	39	63%
#8	China	74	-15%	#18	India	37	New entry
#9	Bulgaria	72	38%	#19	Vietnam	29	45%
#10	Hungary	70	New Entry	#20	Lithuania	29	New entry

Figure 19 Source: Spamhaus Botnet Threat Update: Q2-2020 [20]

Most of the botnets are used to perform DDoS attacks.

[19] https://www.spamhaus.org/news/article/800/spamhaus-botnet-threat-update-q2-2020
[20] 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. Besides, botnets have specific attack vectors – the attackers are using common compromising/ infection techniques in order to create the zombie networks and subsequently using them to conduct various other attack types, such as malware infection, phishing, spam attacks and performing DDoS attacks.

The overall trend of botnet population activity in 2020 was Decreasing.

7.13 Cryptojacking

Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads **cryptomining** code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser.

Cryptojacking rank 13th in Bangladesh top threats.

Cryptocurrency mining continues to rise as one can observe from the figure below

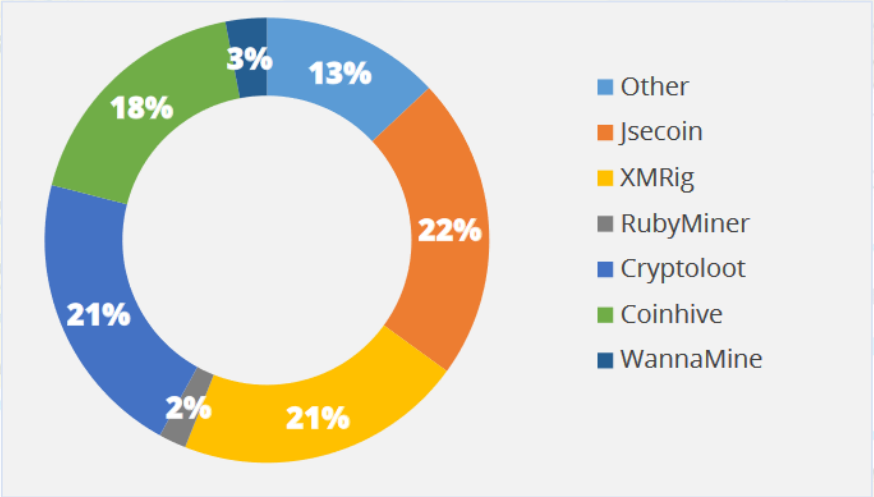


Figure 20: Top crypto mining malware globally [21]

The primary attack vector for Cryptojacking is incorporating cryptojacking capabilities in existing malware and botnets. The majority of the devices targeted by cyber criminals are endpoint devices (laptops/desktops), enterprise servers and cloud infrastructure, IoT devices, websites, mobile devices and ICS systems

The overall trend of Cryptojacking in 2020 was Decreasing.

Primary group of threat agents for exploit kits is **cyber criminals, nation states and corporations.**

[21] https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

7.14 Physical manipulation/ damage/ theft/ loss

Physical loss of assets and theft remain one of the major causes of data breaches.[22] Physical attacks also pose a high risk for critical infrastructures, which are very often attacked by physical means. Physical manipulation/ damage/theft/ loss is attributable to information content security incident class. 20%_of cybersecurity incidents started or ended with a physical action[23].

Physical manipulation/ damage/ theft/ loss ranks 14th in Bangladesh top threats.

According to Verizon, physical actions were present in 11% of breaches, and it marks an increasing trend. Most physical actions related to data breaches were theft and skimmer actions, when skimming device is physically implanted on an asset that reads magnetic stripe data from a payment card. The top two assets in physical theft and loss breaches were paper documents and laptops at the victim's work area or from employee-owned vehicles.

Average person now loses 1.24 items a year and less than half of those are recovered.[24]

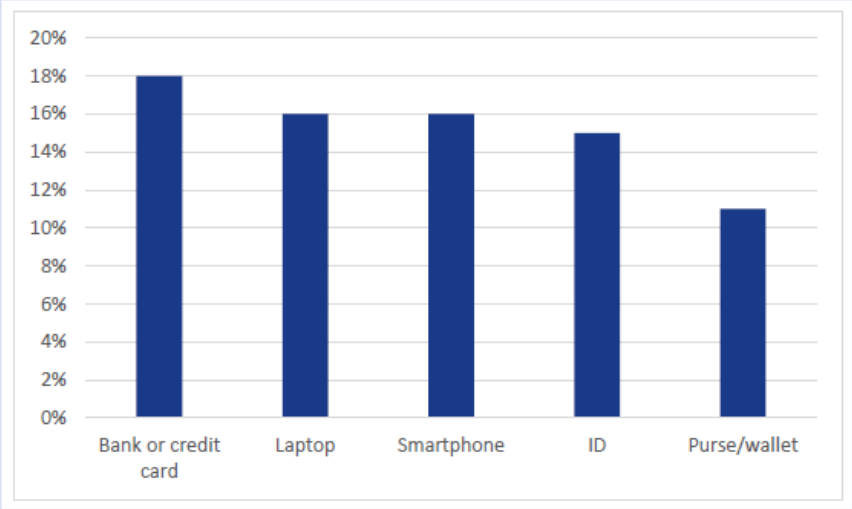


Figure 21. Items lost by people [25]

The attack vector for physical manipulation/damage/theft/loss is exploitation of vulnerabilities/ misconfigurations and cryptographic/network/security protocol flaws and supply-chain attacks.

The overall trend of physical manipulation/damage/theft/loss in 2020 was Same as previous year.

Primary group of threat agents for physical manipulation/damage/theft/loss is **cyber criminals, insiders, nation states and corporations.**

[23] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf
[24] https://enterprise.verizon.com/resources/reports/2018/dbir.pdf
[25] https://web.cs.wpi.edu/~emmanuel/courses/cs528/F18/projects/final_project/proposal/solman_xu_zhou_islam_bashir_proposal.pdf

7.15 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.

Cyber espionage ranks 15th in Bangladesh top threats.

The primary attack vectors for cyber espionage are exploitation of vulnerabilities/ misconfigurations and cryptographic/networks/security protocol flaws and supply-chain attacks. Threat agents often use complex pieces of malware.

The overall trend of cyber espionage in 2020 was Decreasing.

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

8. ANNEXES

8.1 Survey format for Bangladesh cyberthreat landscape

Aim of the survey is to identify most relevant cyber threats in Bangladesh and prepare Bangladesh cyberthreat landscape report to be used by executives, risk managers, auditors and security managers.

Therefore, we kindly ask you to answer survey questions from your organization's point of view by ticking appropriate boxes.

When providing answers on the impact of the incident to your organization, please observe following definitions of incident impact:

- **Severe –** incident that was likely to result in a significant impact to availability, confidentiality and integrity of organization's information or likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, civil liberties or public confidence
- **Medium –** incident might have affected availability, confidentiality and integrity of organization's information or might have affected public health or safety, national security, economic security, foreign relations, civil liberties or public confidence
- **Low –** incident was unlikely to affect availability, confidentiality and integrity of organization's information or public health or safety, national security, economic security, foreign relations, civil liberties or public confidence

No individual organization's information will be publicized as you provide anonymized information and your answers will be dealt as statistical figures.

No	Cyberthreat	Number of incidents your organization	Impact of the incident to your organization
1.	**Malware** software that is intentionally included or inserted in a system for a harmful purpose and usually requires user interaction to activate the code. Malware includes viruses, worms, trojans, spyware, dialler and rootkits	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
2.	**Web-based attacks** web browser exploits, web browser extensions, web servers and services exploits, drive-by	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High

No	Cyberthreat	Number of incidents your organization	Impact of the incident to your organization
	attacks, water-holing, redirection and man-in-the browser-attacks		
3.	**Web application attacks** attacks directed against web applications, web services and mobile applications through the abuse of APIs	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
4.	**Phishing** masquerading as another entity in order to persuade the user to reveal a private credential	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
5.	**Denial of Service** attack that the perpetrator seeks to make a machine or network resource unavailable to its intended users.	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
6.	**Spam** unsolicited bulk e-mail	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
7.	**Botnets, including fake social media accounts** a number of Internet-connected devices, each of which is running one or more bots and perform different malicious activities.	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
8.	**Data breach** loss of data caused by a successful launch of another cyber threat	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
9.	**Insider threat** when a person is using his/her authorized access, wittingly or unwittingly, to do harm to the security of an organization	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High

No	Cyberthreat	Number of incidents your organization	Impact of the incident to your organization
10.	**Physical manipulation/ damage/theft/loss**	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
11.	**Information leakage**	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
12.	**Identity theft** when an attacker aims at obtaining confidential information that is used to identify a person or a computer system	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
13.	**Cryptojacking** threat that hides on a computer or mobile device and uses the machine's resources to "mine" forms of online money known as cryptocurrencies	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
14.	**Ransomware** malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High
15.	**Cyber-Espionage** attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity APTs included	1 ☐ From 0-2 2 ☐ From 3-5 3 ☐ More than 5	1 ☐ Low 2 ☐ Medium 3 ☐ High