BANGLADESH CYBER THREAT LANDSCAPE 2023

ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

TLP: CLEAR

BGD e-GOV CIRT

BGD e-GOV CIRT

TABLE OF CONTENTS

BGD e-GOV CIRT

CYBER THREAT LANDSCAPE 2023 BANGLADESH

PLANNING AND GUIDANCE

Engr. Fakhar Uddin Al Helal
Manager (IBM), Incharge (Data Center)
Bangladesh Computer Council

EDITORIAL PANEL

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

RESEARCHER

Mohammad Makchudul Alam
GIAC GSOC, CEH, ISO 27001 LI, MITRE ATT&CK Defender (CTI, SOC assessment & Adversary Emulation)
Information Security Specialist, BGD e-GOV CIRT
Bangladesh Computer Council

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

Md. Redowan Zaman Anik
MITRE ATT&CK Defender, CSA, CEH, RHCE, RHCSA, CCNA
Incident Handler, BGD e-GOV CIRT
Bangladesh Computer Council

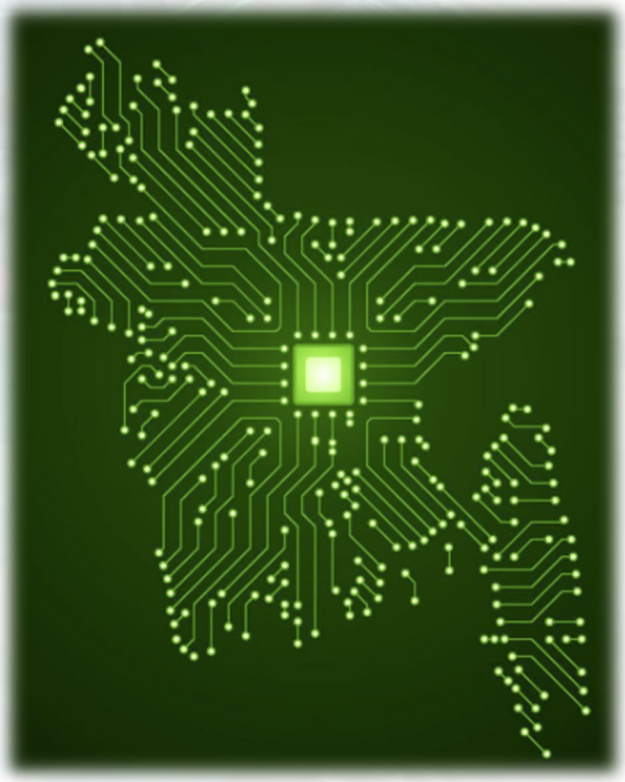
Sabrein Serag El Din El Sayed Bodour
CCNA, MCITP
CIRT System & Website Administrator, BGD e-GOV CIRT
Bangladesh Computer Council

CONTRIBUTORS

Khondker Aminul Islam
CRISC, ISO 27001 ISMS LA, ISO 27701 PIMS LI, PMP, PRINCE2
Risk Analyst, BGD e-GOV CIRT
Bangladesh Computer Council

FOREWORD

In 2023, Bangladesh has faced an intensifying cyber threat landscape, characterized by increasingly sophisticated and multifaceted attacks. The renowned APT group SideWinder has been identified executing a targeted phishing campaign, employing domains that deceptively mimic official Bangladeshi websites to compromise sensitive information from government and law enforcement entities. Concurrently, there has been a marked surge in ransomware-related incidents, with malware infections increasing by approximately 71.39%. These threats exploit critical Remote Code Execution vulnerabilities, with significant malware strains such as M0yv, Phorpiex, and Necurs being linked to various ransomware variants including Maze and Locky. Additionally, vulnerabilities within MySQL and Microsoft SQL services have been specifically targeted. Hacktivist groups, primarily from South Asia, have also intensified their activities, orchestrating numerous DDoS attacks, website defacements, and data leaks driven by ideological motives, resulting in considerable disruptions to digital operations. The escalation of phishing attacks, encompassing advanced techniques such as email phishing, spear phishing, and social media phishing, has further exacerbated the risk, inflicting substantial financial and reputational damage. Furthermore, the proliferation of info stealer malware, designed to extract and exploit sensitive data including login credentials and financial information, has compounded the cyber threat scenario. This evolving threat environment underscores the critical need for robust cybersecurity measures and heightened vigilance across all sectors in Bangladesh.



APT GROUPS TARGETING BANGLADESH

In the ever-evolving landscape of cybersecurity threats, Advanced Persistent Threats (APTs) groups stand out as a formidable group of cyber actors. They possess unparalleled sophistication, resources, and expertise, making them capable of breaching even the most fortified defenses.

APT groups pose a serious risk to organizations of all sizes and we have seen it proven after the Bangladesh bank heist in 2016 conducted by the notorious APT group 'Lazarus'. Since then, APT groups activities and footprints have been closely monitored by our cybersecurity experts. In the last quarter of 2023, Cyber Threat Intelligence Unit of BGD e-GOV CIRT has identified a malicious campaign performed by the notorious APT group named 'Siderwinder' targeting Bangladeshi entities. Through rigorous research and analysis, some phishing domains that mimic Bangladeshi official websites and domains were detected. The findings have raised the alarm of an ongoing phishing campaign conducted against entities in the country. By analyzing those malicious domains, hash files, and IP addresses, it has been discovered that they are attributed to SideWinder APT group, which targets government and law enforcement organizations in Bangladesh.

As shown in the below image, the IP address of 5.230.54[.]3 hosts malicious subdomains

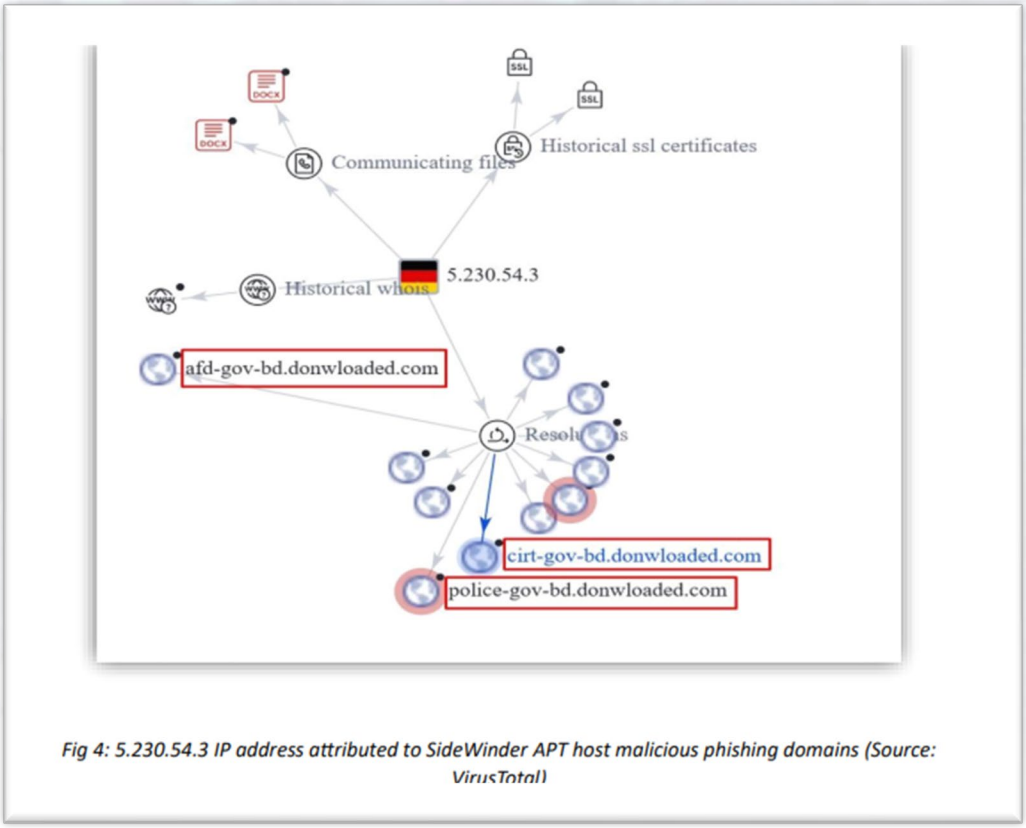


Fig 4: 5.230.54.3 IP address attributed to SideWinder APT host malicious phishing domains (Source: VirusTotal)

which mimic Bangladeshi organizations. Later found that the IP address belongs to SideWinder APT network.

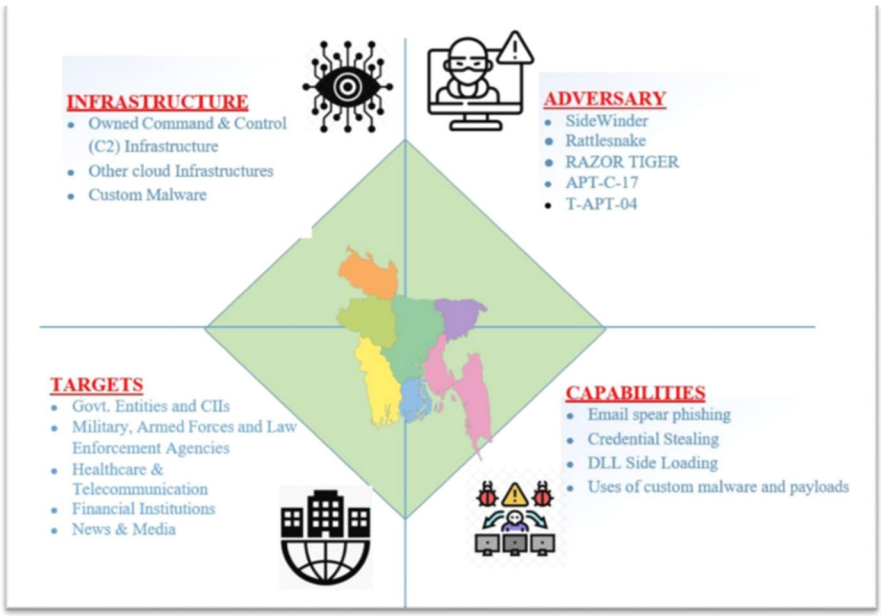


Fig 1: Threat model of SideWinder APT group

SideWinder has been using spear phishing as its primary initial attack vector against their victims. The attack is initiated by a victim receiving a phishing email containing a malicious attachment or URL. The email lures are often crafted for the target organization and include contents that the recipients would find relatable or interested in learning about. They used

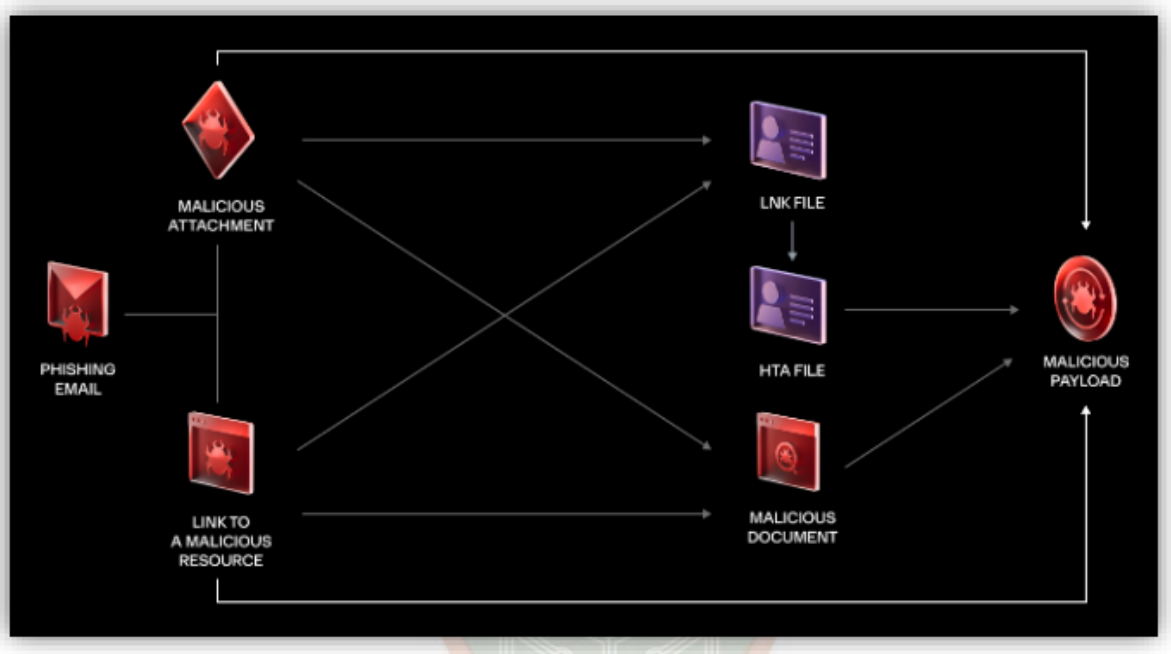


Fig 3: SideWinder's attack chain

emails pertaining to domains which look-a-like several government, military and law enforcement agencies' domains of Bangladesh (e.g. cirt-gov-bd.donwloaded[.]com)

Code execution

- When a user clicks on the malicious link/attached file (RTF, DOCX, ZIP, LNK,..etc.), a code execution is initiated to download a remote HTA file from the group's controlled server.
- The HTA file run leads to the execution of the payload malware through DLL side loading technique. (The malware can be a remote access Trojan (RAT) or an information stealer)
- The Malware starts collecting sensitive and confidential info./files and send it to the C2 server.

	Url	Domain	IPv4
2	http://bdmil.alit.live/3398/1/54346/2/0/0/0/m/files-491dc489/file.rtf	bdmil.alit.live	
3	http://navy-mil-bd.jmicc.xyz/5625/1/8145/2/0/0/0/m/files-b11074b7/file.rtf	navy-mil-bd.jmicc.xyz	
4	http://mailnavybd.govpk.net/5845/1/12/2/0/0/0/m/files-ca78574e/file.rtf	mailnavybd.govpk.net	5.255.112.194
5	https://mailnavymilbd.govpk.net/5848/1/13/2/0/0/0/m/files-57d837e4/file.rtf	mailnavymilbd.govpk.net	
6	http://mailnavymilbd.govpk.net/5848/1/13/2/0/0/0/m/files-57d837e4/file.rtf	mailnavymilbd.govpk.net	
7	http://bdmil.alit.live/3398/1/50073/2/0/0/0/m/files-ac995f17/file.rtf	bdmil.alit.live	
8		mofa-bd.org	
9	https://bangladeshmarineacademylibrary.ppinewsagency.live/5083/1/3417/2/0/0/0/m/files-76793138/file.rtf	bangladeshmarineacademylibrary.ppinewsagency.live	

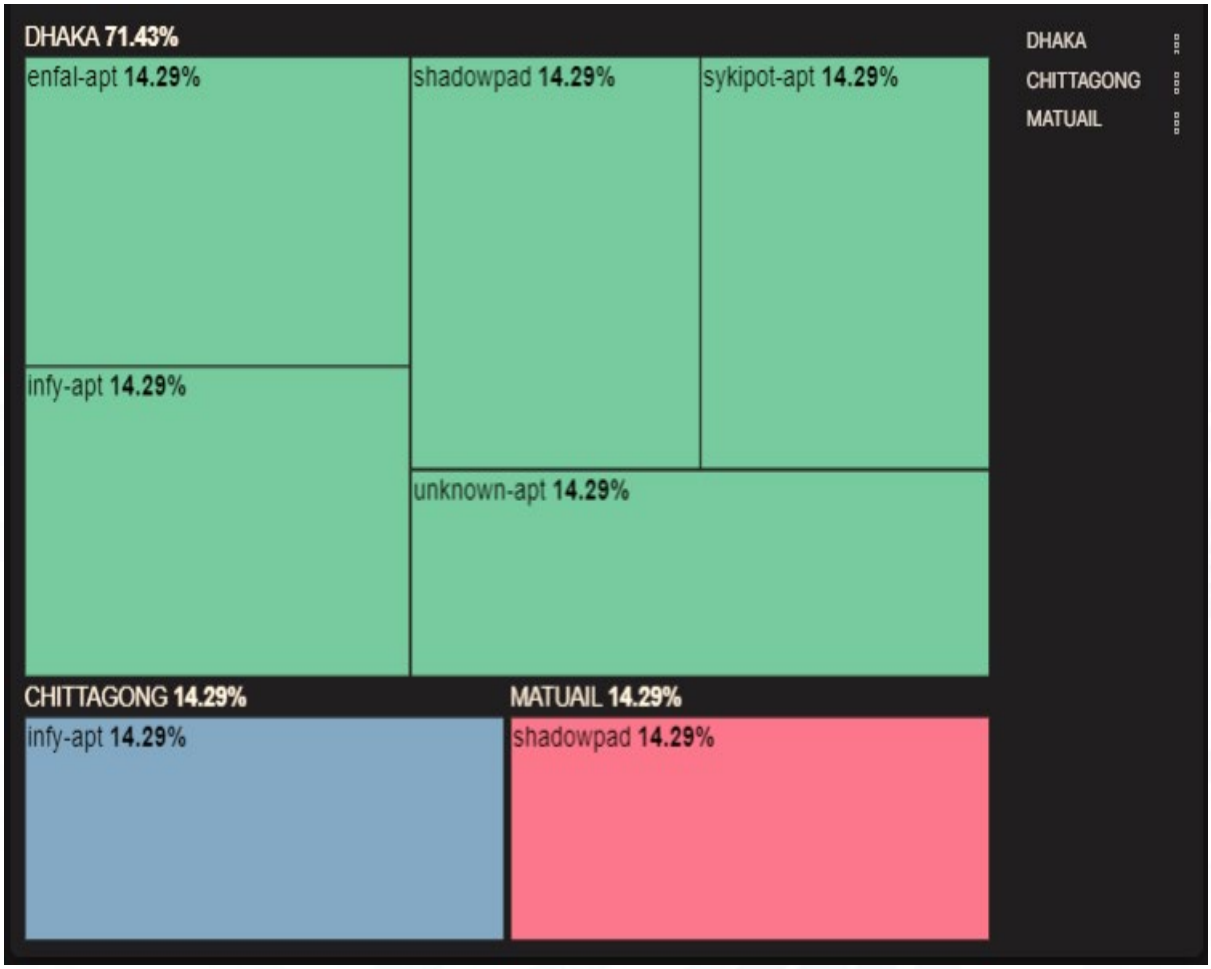
We observed that the file type mostly used by the group in its phishing attacks targeted at Bangladeshi entities is "RTF", a rich text document file. It is worth mentioning that the APT group uses Server-Side Polymorphism which is a technique used by the group in an attempt to evade detection by traditional antiviruses which are based on signatures to detect malicious files.

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	Timeline
sykipot-apt *(aka: getkys, Wkysol)*	The Sykipot attack group is known in part for creating the Sykipot APT malware family. This custom malware family leveraged flaws in Adobe Acrobat and Adobe Reader and used spear phishing attacks to effectuate zero-day exploits upon its victims. [1] Actor(s): **Samurai Panda**	chosunkor[.]com	January
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. [2]	updateserver1[.]com	January-March
enfal-apt	ENFAL is a backdoor that is specifically used for downloading other malware. It is used in several targeted attacks. It has been used by APT15 and APT24 groups. [3]	Macosservice[.]com ipad-admin[.]net	March
Shadowpad *(aka: POISONPLUG.SHADOW, XShellGhost)*	The ShadowPad advanced modular remote access trojan (RAT) has been deployed by the Chinese government-sponsored **BRONZE ATLAS** threat group since at least 2017. A growing list of other Chinese threat groups have deployed it globally since 2019 in attacks against organizations in various industry verticals. ShadowPad extracts information about the host, executes commands, interacts with the file system and registry, and deploys new modules to extend functionality. [4] Actor(s): **APT23, APT41, APT17, DAGGER PANDA, Earth Lusca, Tonto Team, WET PANDA**	mssysinfo[.]xyz	July-November

[1] https://www.infosecinstitute.com/resources/malware-analysis/malware-spotlight-what-is-apt/
[2] https://malpedia.caad.fkie.fraunhofer.de/actor/infy
[3] https://www.mandiant.com/resources/insights/apt-groups
[4] https://www.secureworks.com/research/shadowpad-malware-analysis

C2 DESTINATIONS FOR APT GROUPS FOOTPRINT IN BANGLADESH



THE STATE OF RANSOMWARE IN BANGLADESH

In an era marked by the rapid growth of internet users and widespread adoption of digital technologies, ensuring cybersecurity has become an ongoing challenge. BGD e-GOV CIRT remains dedicated to safeguarding Bangladesh's cyberspace. As part of our commitment to fostering digital resilience, we have conducted an extensive study on ransomware within Bangladesh. Despite the rise in ransomware incidents, malware infections, and exploitable vulnerabilities in 2023, a notable shift has occurred. Organizations are increasingly proactive in reporting incidents and seeking assistance, marking a significant change in cybersecurity practices.

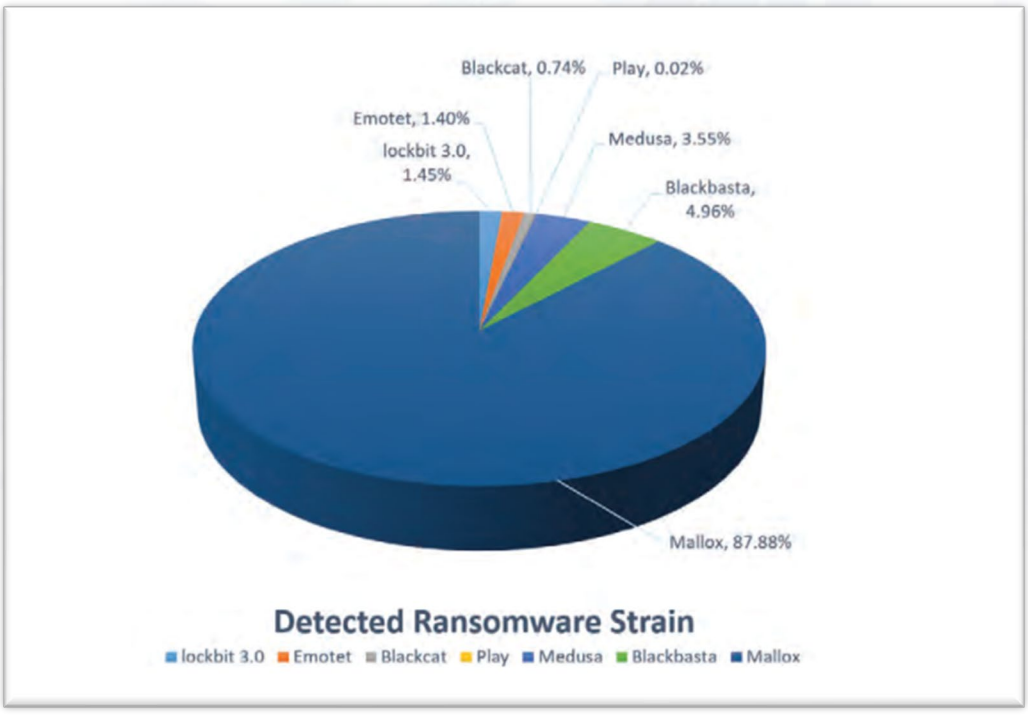
This section represents the culmination of our year-long efforts, drawing from a wealth of data from reported incidents and rigorous local and global threat intelligence research focused on ransomware. Our main goal is to offer organizations and individuals essential insights and

information crucial for strengthening defenses against ransomware threats. Within these pages, readers will explore valuable perspectives derived from our thorough analysis, covering malware trends, vulnerabilities, active ransomware variants, and key findings from comprehensive investigations. As the digital landscape evolves, our aim is to equip readers with the knowledge needed to enhance preparedness and resilience in the face of evolving ransomware threats.

Ransomware Trends

In our analysis of ransomware threats in Bangladesh, we've uncovered an increase in ransomware-related risks, critical vulnerabilities, and specific malwares with the potential to initiate disastrous attacks.

1. There has been a significant increase of approximately **71.39%** in malware infection events related to potential ransomware threats.
2. Common Vulnerabilities and Exposures (CVEs) associated with Remote Code Execution Vulnerabilities were identified that could be exploited to lead ransomware attacks in Bangladesh.
3. Among the identified malware infections with potential to lead ransomware threats, three significant malware strains have been pinpointed: M0yv, Phorpiex, and Necurs. Each of these possesses the capability to trigger ransomware attacks, with each one being associated with a distinct strain, including Maze, Avaddon, Grandcab, and Locky.
4. Furthermore, our analysis has brought to light a significant number of attempts linked to Indicators of Compromise (IOCs) associated with Mallox Ransomware. These attempts were predominantly concentrated on exploiting vulnerabilities with Mysql or Microsoft SQL services.



Global statistics show that Bangladesh was hit the most by ransomware Trojans than any other country.

TOP 10 countries and territories attacked by ransomware Trojans

	Countries and territories*	%**
1	Bangladesh	3.34
2	Yemen	2.07
3	South Korea	1.89
4	Mozambique	1.61
5	Sudan	1.56
6	Palestine	1.45
7	Taiwan	1.40
8	Afghanistan	1.09
9	China	0.99
10	Syria	0.97

Figure : Geography of Most Attacked Countries by Ransomware Trojans [5]

[5] https://securelist.com/ksb-2022-statistics/108129/

Sectorial Impact of Ransomware

Ransomware attacks in Bangladesh have notably risen, affecting multiple industries. Cybersecurity experts suggest that these attacks often stem from inadequate cybersecurity measures rather than highly sophisticated methods. Nonetheless, the repercussions for affected industries remain profound.

BGD e-GOV CIRT has played a pivotal role in promoting the adoption of enhanced cybersecurity practices. The organization consistently urges entities across Bangladesh to promptly report any incidents or suspicious activities detected within their networks. Encouragingly, in 2022, there was a notable increase in the number of organizations affected by ransomware attacks that chose to proactively report such incidents to BGD e-GOV CIRT.

This willingness to report ransomware incidents to BGD e-GOV CIRT marks a significant advancement in the ongoing fight against ransomware. It enables BGD e-GOV CIRT to provide immediate technical incident response guidance and support. Additionally, the organization can closely monitor the recovery process and, in some cases, offer on-site technical expertise to assist organizations in mitigating the impact of ransomware attacks.

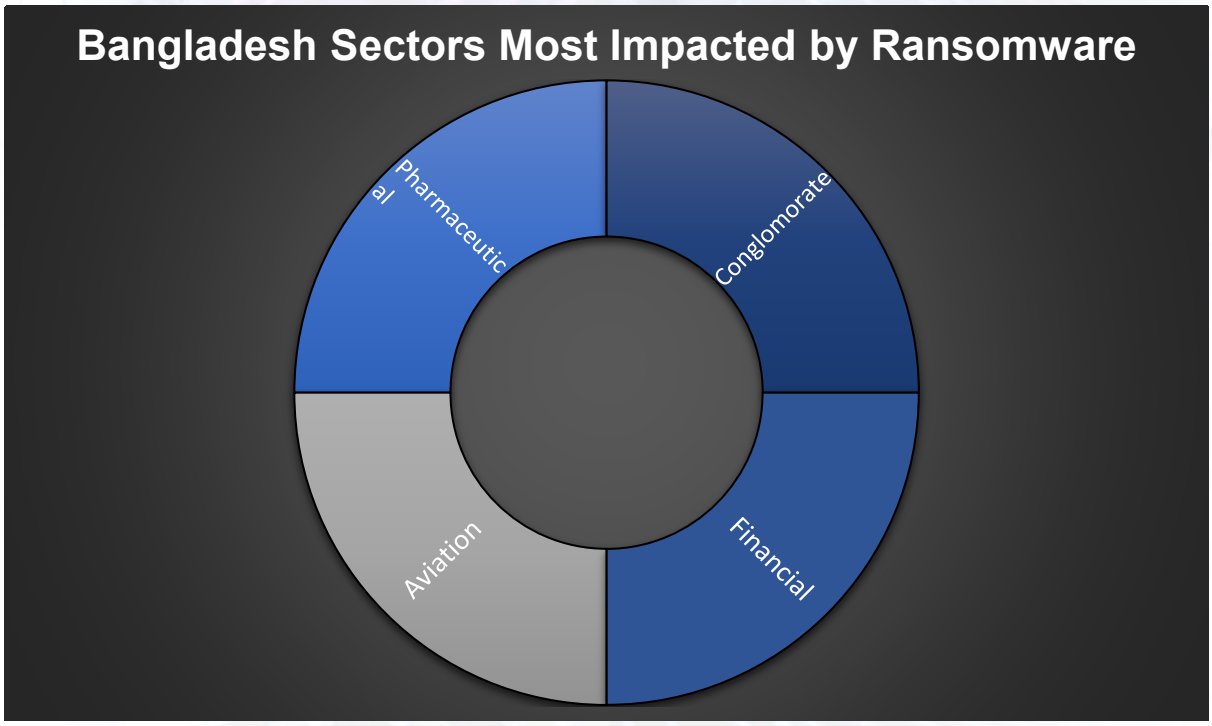


Figure : Bangladesh Sectors Most Impacted by Ransomware Within Last Year

Ransomware Incidents in 2023

LOCKBIT 3.0

Incident in December 2022

Target: Leading Pharmaceutical company in Bangladesh

Data Breach: 750GB of data, including personal folders, infrastructure, and accounting data

Ransomware Type: LOCKBIT 3.0

Alias: LockBit Black

Model: Ransomware-as-a-Service (RaaS)

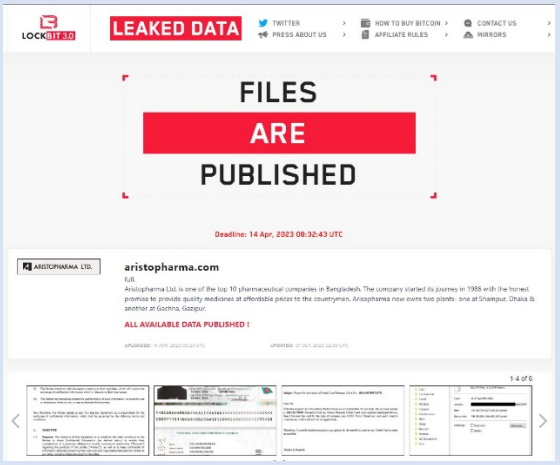
Evolution: LockBit 2.0 > LockBit 3.0

- Since January 2020, functioned as an affiliate-based ransomware variant
- First observed in September 2019
- Most active ransomware group in 2022 and as of Q1 2023

In December 2022, the notorious ransomware gang LOCKBIT 3.0 claimed responsibility for a ransomware attack on one of the leading Pharmaceutical companies in Bangladesh. According to a post by the group, the hackers successfully breached the company's network and infiltrated 750GB of data that contains personal folders of key employees, all infrastructure and accounting data.

LockBit 3.0, also known as "LockBit Black," function as a Ransomware-as-a-Service (RaaS) model and is a continuation of previous versions of the ransomware, LockBit 2.0, and LockBit. Since January 2020, LockBit has functioned as an affiliate-based ransomware variant. [6] The group was first observed in September 2019, it became the most active ransomware group of 2022 with the shutdown of Conti, and as of the first quarter of 2023, it still stand out as the most active ransomware group.[7]

8



[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
[7] https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/
[8] https://cyware.com/news/lockbit-30-ransomware-group-expands-targets-multiple-sectors-worldwide-4dbb1d22

MONEY MESSAGE

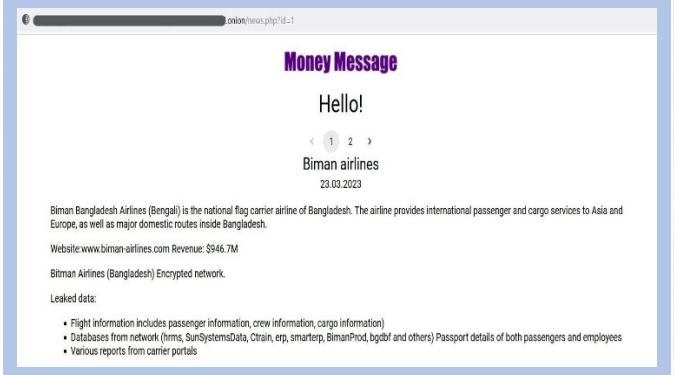
Incident in March 2023

Target: Leading transportation organization in Bangladesh

Notable: Newcomer to the ransomware landscape

Impact: Critical server and computer systems affected, operations disruption

- Threatened to disclose 100GB of personal and confidential information



A few months later, specifically in March 2023, a significant ransomware attack struck a leading transportation organization in Bangladesh. The incident is the year's most cybersecurity-related hot topic for cybersecurity professionals in the country and for the public until today. In this incident, the threat actor was a newcomer to the ransomware criminal activity landscape. Later known as 'Money Message'.

It started when one of the company's critical servers along with some computers came under a ransomware attack conducted by Money Message, causing operations disruption.
Threat actors demanded a huge ransom for restoring access to the server and threatened to disclose 100GB of personal and confidential information, which they managed to infiltrate.

ALPHV/BlackCat

Incident in June 2023

Target: Financial organization in Bangladesh

Initial Access Method: Stolen credentials obtained through initial access brokers

Data Breach: 170 GB of sensitive data, including SQL backups, financial data, employee information

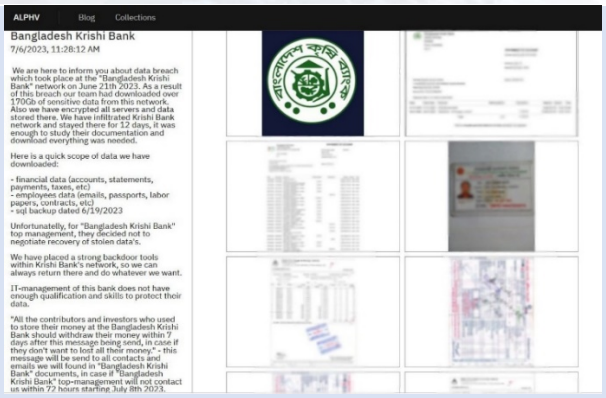
Notable: Ransomware family written in Rust

Model: Ransomware as a service (RaaS)

- Operates a public data leak site to pressure victims to pay ransom demands
- Placed a potent backdoor to ensure persistent access to the network

Last June, the prolific group ALPHV/BlackCat has claimed responsibility for the data breach of a financial organization in Bangladesh. As a result of this breach, the hackers were able to infiltrate 170 GB of sensitive data from the network. The data contained: SQL backup, financial data (accounts, statements, payments, etc), employees' data (emails, passports, contracts, etc). Threat actors claimed to have placed a potent backdoor to ensure persistent access to the network.

BlackCat, also known as ALPHV is a ransomware family written in Rust that made its first appearance in November 2021. BlackCat operates on ransomware as a service (RaaS) model, with developers offering the malware for use by affiliates and taking a percentage of ransom payments. For initial access, the ransomware relies essentially on stolen credentials obtained through initial access brokers. The group operates a public data leak site to pressure victims to pay ransom demands.[9]



[9] https://en.wikipedia.org/wiki/BlackCat_(cyber_gang)

AKIRA RANSOMWARE GROUP

Incident in June 2023

Target: Conglomerate company in Bangladesh

Initial Access Method: Infiltration through compromised VPN services and exploiting unsecured credentials

Notable: Emerging group, first discovered in March 2023

Total Victims: Compromised more than 63 victims

Target Profile: Actively targeting small and medium-sized businesses worldwide

Actions: Attempts to delete backup folders, encrypts files with a specific extension, and adds ".akira" to each encrypted file.

On June another attack struck a conglomerate company in Bangladesh. Later, Akira ransomware group declared its responsibility for the attack and listed the company on its website victim list. According to the post made by the group, the company's leadership didn't show willingness to negotiate the ransom amount, hence their leaked data was published on the group dark website.

Akira ransomware group is an emerging group first discovered in March 2023 and has since compromised more than 63 victims. The group is actively targeting small and medium-sized businesses around the world. Akira commonly infiltrates targeted Windows and Linux systems through VPN services, especially where users have not enabled multi-factor authentication. To gain access to victims' devices, attackers use compromised credentials, which they most likely acquire on the dark web. Once a system is infected with Akira, the malware attempts to delete backup folders that could be used to restore lost data. Then, the ransomware encrypts files with certain extensions and adds the ".akira" extension to each of them.[10]

[10] https://therecord.media/akira-ransomware-early-victims-conti-links

Malware Variants Related to Ransomware

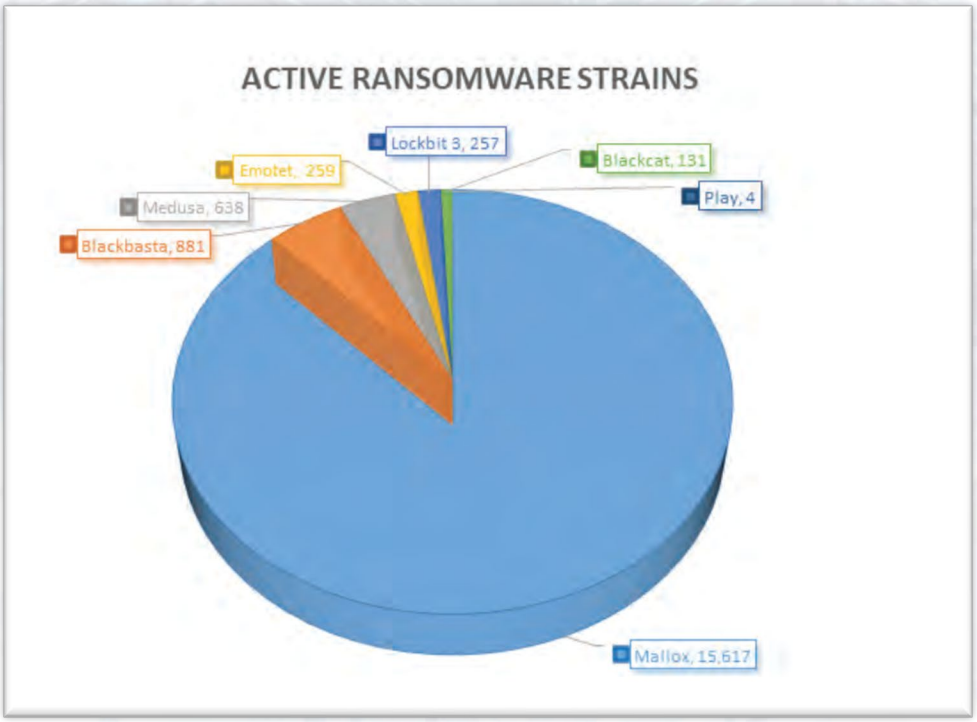
CTI Unit of BGD e-GOV CIRT has identified various infection variants linked to well-known ransomware threats. Over the past year, our team detected a total of 25,038 unique instances of IP addresses originating from Bangladesh that were affected by the malware infections mentioned below,

Serial	Malware Name	Possible Ransomware Threat	Total infection events
1	M0yv	Maze	269,018
2	Worm.Phorpiex	Avaddon and Gandcrab	16,865
3	Necurs	Locky	12,382
4	Phorpiex	Avaddon and Gandcrab	3,817
5	Kovter	Kovter	1,129
6	Nymaim	Nymaim	406
7	Zeus	Cryptolocker	98
8	Cobaltstrike	Lockbit,Ryuk	36
9	Zeus Gameover	CryptoLocker	21
10	Sphinx	Blackcat	17
11	Emotet	Trickbot, Ryuk	14
12	Osiris	Locky	4
13	Ryuk	Ryuk	1

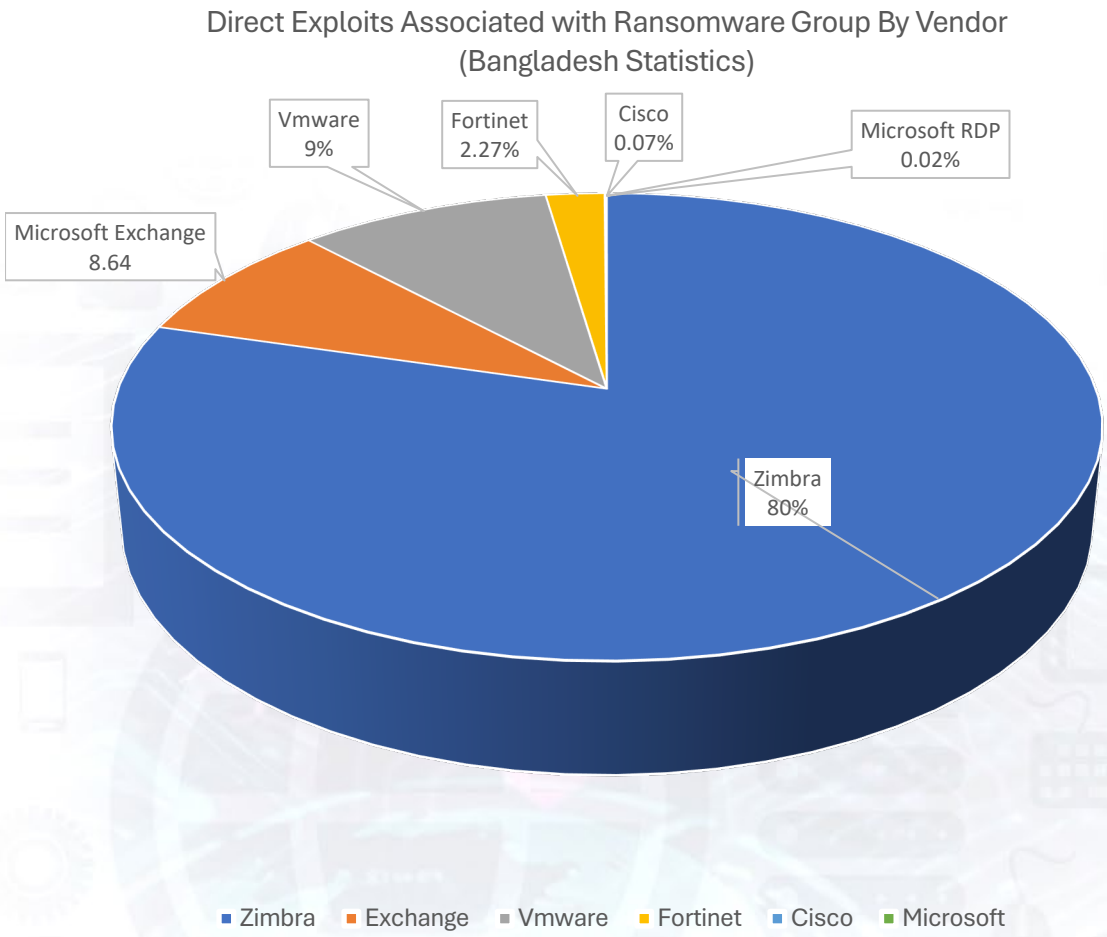
Figure : Top Recorded Ransomware-related Malware Infections in Bangladesh Cyberspace

Active Ransomware Strains

At BGD e-GOV CIRT, our vigilant oversight efforts have centered on detecting potential exploitation activities conducted by ransomware threat actors. Our main objective is to deliver actionable intelligence aimed at safeguarding critical information infrastructures and other organizations. In 2023, our Cyber Threat Intelligence (CTI) unit identified traces of activity linked to seven distinct ransomware threats. It is noteworthy that despite these findings, none of these threats successfully infiltrated or compromised any infrastructure elements. However, we did observe active attempts of exploitation originating from these entities associated with ransomware threat actors. The visual representation below illustrates these active attempts by ransomware threat entities.

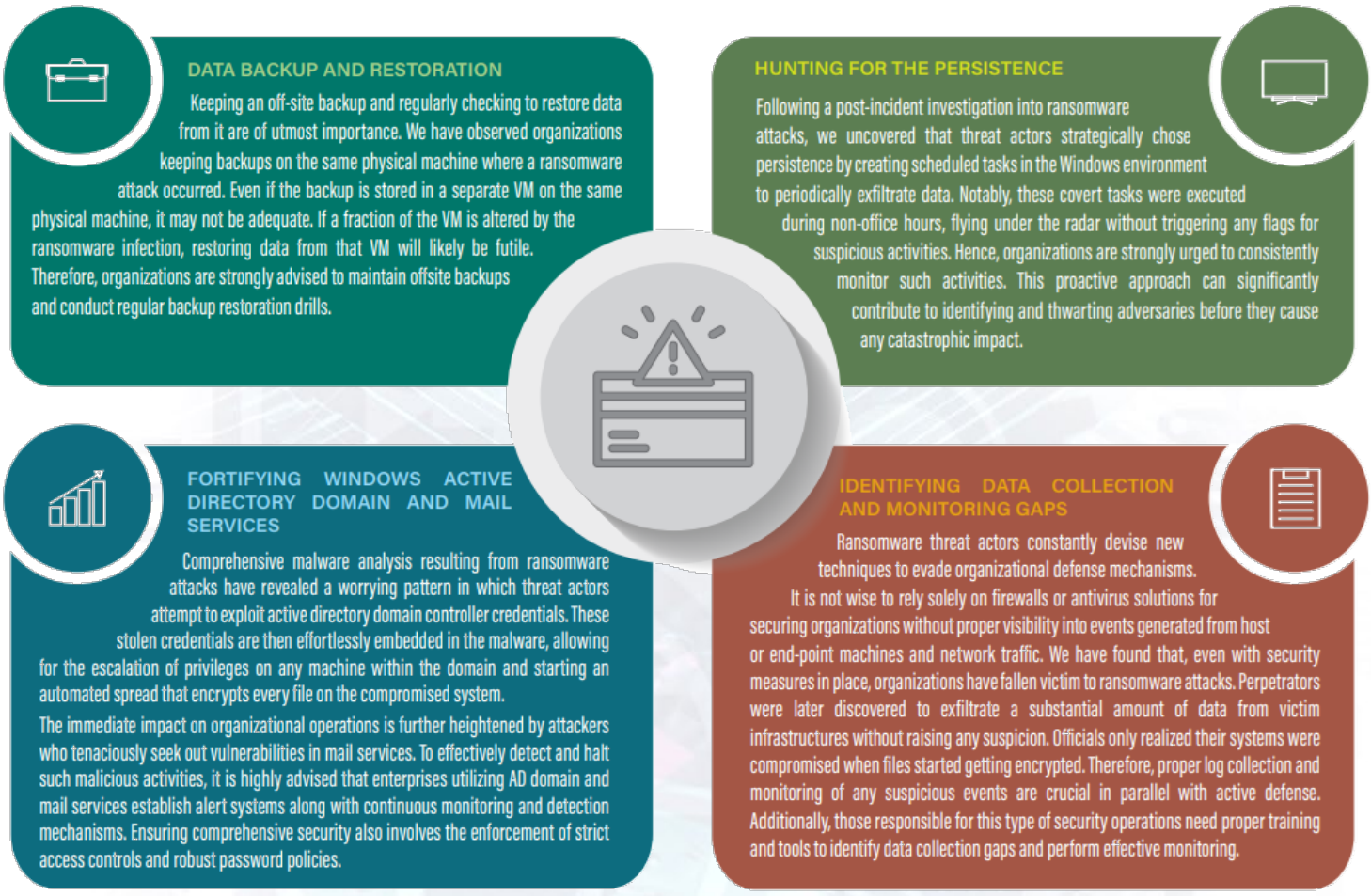


Our analysis of the gathered data emphasizes the presence of Remote Code Execution (RCE) vulnerabilities in products from different vendors. Notably, Zimbra stands out with the highest share of received vulnerability notifications, totaling 80%. Following closely is VMware at 9%. Additionally, critical vulnerabilities, classified as such by the National Vulnerability Database (NVD), also impact Microsoft Exchange, Microsoft RDP, Cisco, and Fortinet, collectively comprising 10% of vulnerability notifications.



Insights From the Investigated Incidents

Organizations affected by ransomware attacks must swiftly prioritize restoring normal operations. When faced with encrypted data and ransom notes, immediate actions are crucial. In Bangladesh, BGD e-GOV CIRT investigated several ransomware attacks against various organizations in 2023. While these organizations promptly sought assistance, our role as incident responders encountered challenges. We faced complexities in meticulously identifying the root causes of ransomware attacks, minimizing their impact, and facilitating the restoration of backup data. In this section, we share valuable insights gained from thorough examinations of reported incidents, highlighting lessons learned throughout the process.

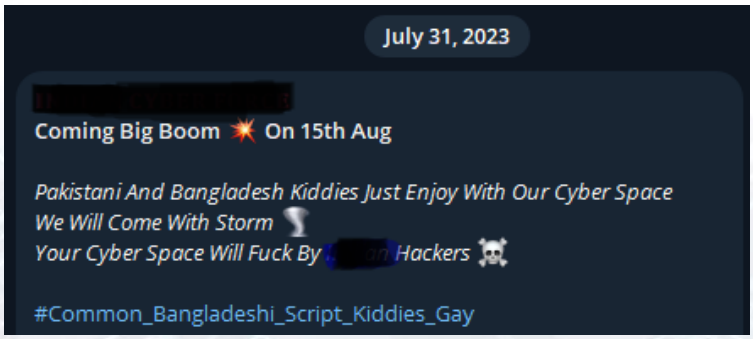


Growing Hacktivist Threats to Bangladesh's Cybersecurity

Throughout 2023, Bangladesh experienced a significant increase in cyberattacks carried out by hacktivist groups. These groups, identified as originating from South Asia, have launched numerous denial-of-service (DDoS) attacks, website defacements, and data leaks targeting various organizations in Bangladesh, particularly within the government and banking sectors. Supposedly these attackers are driven by religious and ideological motives, aiming to disrupt the digital operations of Bangladeshi organizations through small to medium-scale cyber-attacks.

Our cybersecurity experts observed a substantial increase in attacks in August, following a cyber-attack announcement by hacktivists in late July. The peak attacks took place on 15th August, where attackers flooded Bangladeshi organizations with DDoS, website defacements, and data leak attacks. While the attack was going on, BGD e-GOV CIRT has taken preventive steps by issuing a nation-wide alert to warn critical information infrastructures (CII), banks and financial institutions, health care and all sorts of government and private organizations of the possible conducted cyber-attacks by the groups that may disrupt IT operations and businesses.

During the attacks, our experts closely monitored hackers' activities in Bangladesh cyberspace, maintaining active communication with affected organizations and providing immediate technical and operational advice to mitigate the attacks consequences. Our analysis and threat-hunting procedures revealed a significant shift in cybercriminal tactics, with threat actors now exploiting cloud infrastructure virtual machines to launch DDoS attacks.



Phishing

Phishing, a form of cybercrime, involves tricking individuals into providing sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in electronic communications. In recent years, Bangladesh has faced several significant phishing attacks, with two particularly noteworthy incidents. One attack was caused by an API form vulnerability, and the other was orchestrated by an Advanced Persistent Threat (APT) group.

In 2024, Bangladesh continues to face a growing threat from increasingly sophisticated phishing attacks, including advanced email phishing, personalized spear phishing, smishing, vishing, and social media phishing. These attacks result in significant financial losses, identity theft, and emotional distress for individuals, while businesses suffer from financial damage, data breaches, and reputational harm. The government and organizations are responding with enhanced cybersecurity initiatives, public awareness campaigns, stronger legislation, and international collaboration. To combat phishing, it is crucial for individuals and businesses to stay informed, verify the authenticity of communications, use robust security measures, and promptly report phishing attempts to authorities.

1. A sophisticated phishing campaign was targeting Zimbra email users in government entities worldwide, including in Bangladesh. The campaign used API-based phishing attacks to compromise sensitive personal, financial, and health information. Hackers sent phishing emails with '.htm' attachments that mimic legitimate Zimbra login pages. When users enter their credentials on these fake pages, the information is sent to the attackers via an embedded API-based form. This form uses hidden fields and a CSRF token for security, and the data is transmitted using the HTTP POST method to specific API endpoints. The attackers tailor unique forms for different government domains, making detection more difficult. Investigations revealed that the stolen credentials are sent as XML payloads, which include user session, account, and security token information, and are used to check user permissions for actions like "sending on behalf of" others. This campaign highlights the need for heightened vigilance and enhanced security measures to protect against such sophisticated phishing attacks.

   For example, we observed the following links are used to target government domains.

   a) https://api[.]formcake.com/api/form/f409c6db-23f4-4fdf-b031-0747811b4c47/submission
   b) https://api[.]formcake.com/api/form/9a0b8e3f-aef1-4375-b9e9-906804fc045c/submission

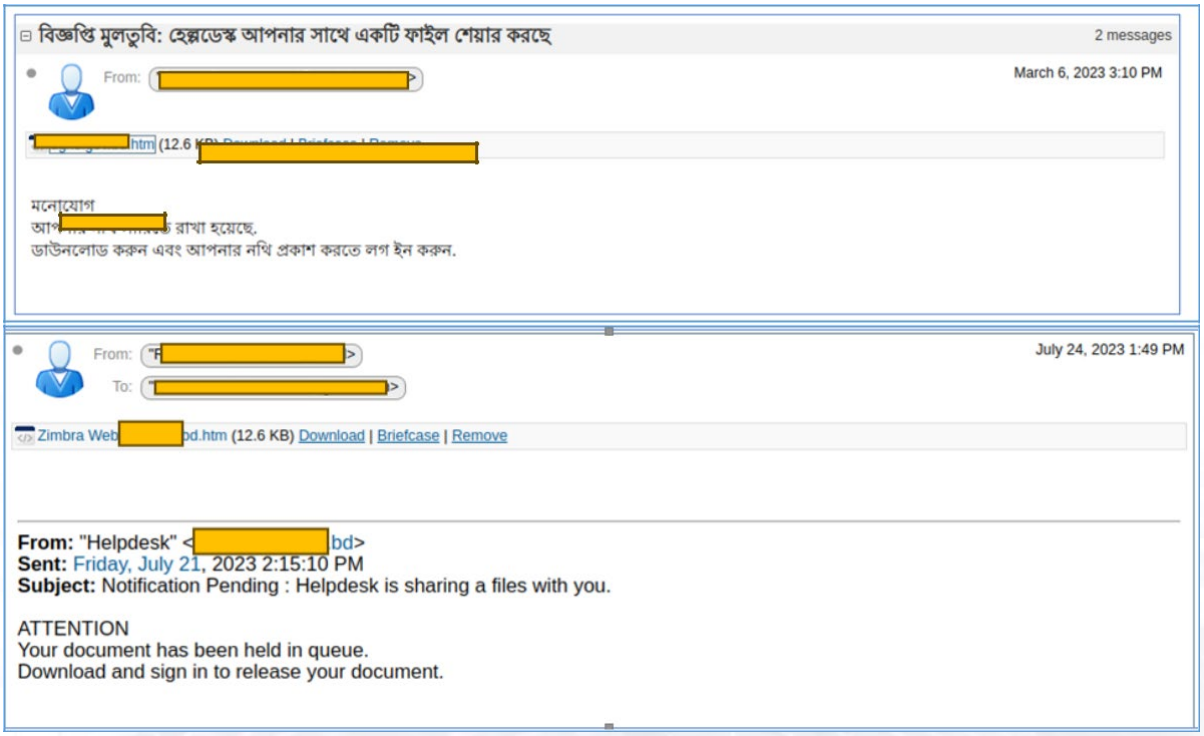


Fig: **Sample phishing mail targeting government domain**

Fig: **Phishing login page for e-mail accounts**

2. SideWinder APT group, primarily targets government and law enforcement organizations in Bangladesh. The phishing campaign involves domains that mimic official Bangladeshi websites and uses RTF (Rich Text Format) files in its attacks. A notable technique employed by the group is Server-Side Polymorphism, which allows them to evade detection by traditional antivirus software that relies on signature-based methods. This discovery highlights the ongoing cyber threats faced by Bangladeshi entities and underscores the need for advanced security measures to counter such sophisticated attacks.

Some of those identified phishing domains are listed below:

Phishing domain	
police-gov-bd.fia-gov[.]net	bangladesh.tni-mil[.]com
police-circular-gov-bd.fia-gov[.]net	afd-gov-bd.donwloaded[.]com
mofa-gov-bd.fia-gov[.]net	cirt-gov-bd.donwloaded[.]com
police-gov-bd.donwloaded[.]com	

Malware Propagation and Vulnerability Exposure via Mobile Data Networks

Bangladesh mobile internet users have soared to 127.84 million, according to the BTRC statistics provided in May 2024, which represents an increase of approximately 10.62% over the past year. This impressive growth is also bringing additional challenges for a secure cyberspace. The Cyber Threat Intelligence Unit (CTI) of BGD e-GOV CIRT has found a substantial amount of malware infection among these mobile internet users, exposed and vulnerable services related to mobile data operators, and credential compromises affecting mobile internet users.

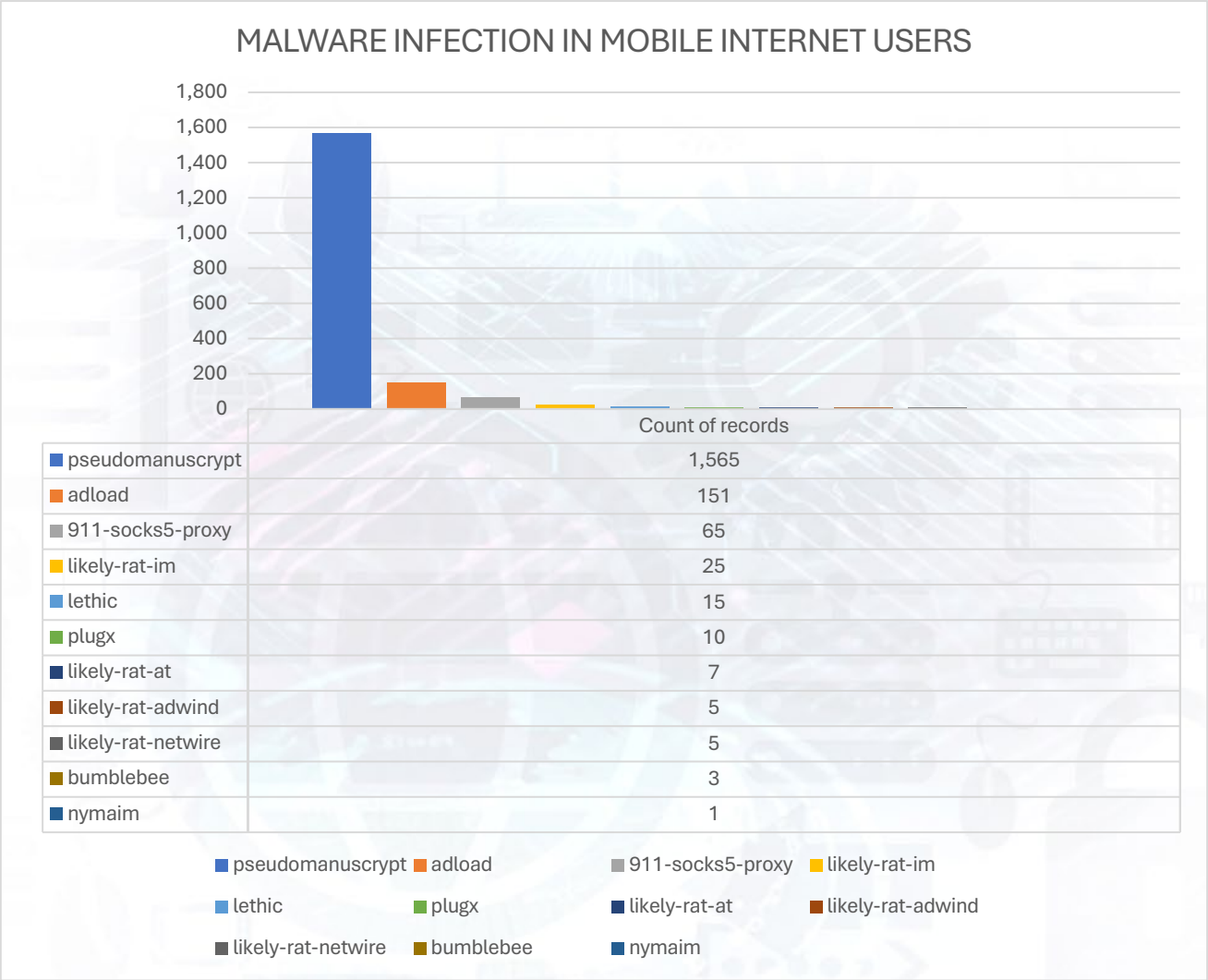
A brief overview of the last six months' findings is given below:

1. Malware infections in mobile internet users

- Total number of malware-infected IP addresses → 1,854
  Grameenphone : 862
  Banglalink: 307
  Robi: 276
  Teletalk: 46

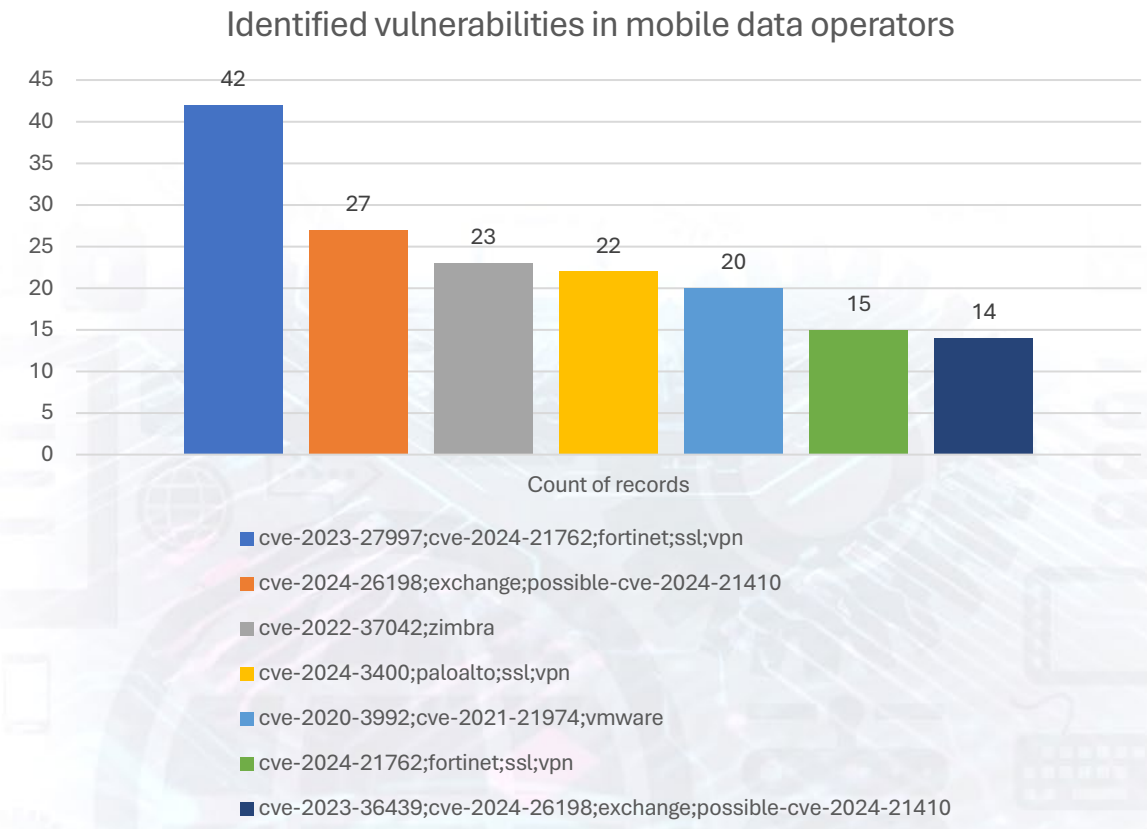
- Total number of unique malware identified → 11
  Grameenphone : 8
  Banglalink: 4
  Robi: 9
  Teletalk: 4

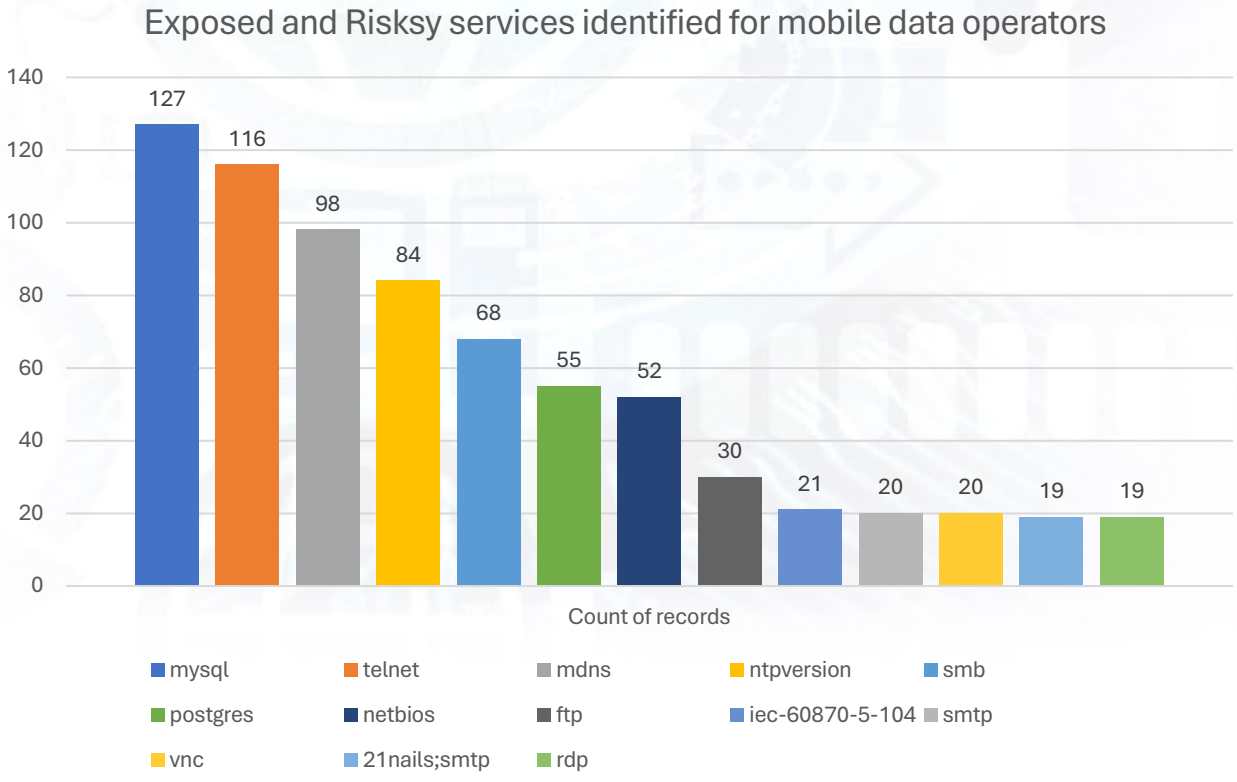
- Most prominent malware is 'pseudomanuscrypt' affecting 1,322 unique ip address



	Count of records
pseudomanuscrypt	1,565
adload	151
911-socks5-proxy	65
likely-rat-im	25
lethic	15
plugx	10
likely-rat-at	7
likely-rat-adwind	5
likely-rat-netwire	5
bumblebee	3
nymaim	1

2. Vulnerable and exposed service detection for mobile data operators
▪ Total number of unique vulnerabilities identified → 7
▪ Total number of exposed and risky services → 13
▪ Most prominent vulnerability → cve-2023-27997;cve-2024-21762
▪ Most prominent exposed services → Mysql


Identified vulnerabilities in mobile data operators
45
40
35
30
25
20
15
10
5
0
42
27
23
22
20
15
14
Count of records
cve-2023-27997;cve-2024-21762;fortinet;ssl;vpn
cve-2024-26198;exchange;possible-cve-2024-21410
cve-2022-37042;zimbra
cve-2024-3400;paloalto;ssl;vpn
cve-2020-3992;cve-2021-21974;vmware
cve-2024-21762;fortinet;ssl;vpn
cve-2023-36439;cve-2024-26198;exchange;possible-cve-2024-21410


Exposed and Risksy services identified for mobile data operators
140
120
100
80
60
40
20
0
127
116
98
84
68
55
52
30
21
20
20
19
19
Count of records
mysql
telnet
mdns
ntpversion
smb
postgres
netbios
ftp
iec-60870-5-104
smtp
vnc
21nails;smtp
rdp

Potential Impact: The detection of malware infections, vulnerabilities, and compromised credentials among mobile data operators underscores significant security risks. These threats can lead to unauthorized access to sensitive data, disruptions in service availability, and potential exploitation of system weaknesses.

Recommendation: Addressing these issues promptly with robust security protocols, timely patches, and heightened monitoring is essential to mitigate risks, protect user information, and ensure the integrity of operational services. Taking proactive measures will help safeguard against potential breaches and maintain trust in the security of mobile data operations.

The Rise of Info Stealer Malware

An information stealer, also known as an info stealer, operates as a Trojan designed with the explicit purpose of extracting valuable information from a targeted system. The primary focus of these malicious entities is the gathering of login credentials, such as usernames and passwords, which are subsequently transmitted to another system over the network. Keyloggers, a common subtype of information stealers, are specifically crafted to record user keystrokes, potentially exposing sensitive information in the process.[11] The sophistication of information stealers extends to the extraction of a broad spectrum of data, including account passwords, cookies, credit card details, and cryptocurrency wallet information. These pilfered details are meticulously organized into archives, commonly referred to as 'logs,' which are then uploaded back to the threat actors. These logs serve as a repository of stolen data, fueling subsequent cyberattacks or being traded on online marketplaces, with prices ranging from $1 to $150 depending on the victim.[12] This intricate process highlights the multifaceted nature of info stealers, posing a significant threat to the security of sensitive information in the digital landscape.

Stealer Malware works with several stages which are outlined below-

Stage	Description
Infection	Stealer malware enters systems via phishing emails, malicious websites, or software vulnerabilities, staying hidden to avoid detection.
Data Collection	Stealer malware's primary function is gathering sensitive data, including login credentials, stored passwords, and information from forms and documents.
Transmission	The collected data is stealthily transmitted to a remote server controlled by the attacker to evade security software detection.
Exploitation	Cybercriminals exploit the stolen information for unauthorized account access, financial fraud, or selling data on the dark web.
Persistence	Stealer malware seeks prolonged impact by establishing persistence on the infected system through backdoors, system settings modification, or other evasion techniques.

[11] https://www.trendmicro.com/vinfo/us/security/definition/Info-stealer

[12] https://www.bleepingcomputer.com/news/security/the-new-info-stealing-malware-operations-to-watch-out-for/

Info Stealer Malware in Bangladesh

In recent times, a concerning trend has emerged, impacting a multitude of individuals within different type of organization. Notably, there has been a surge in the compromise of both official and personal credentials, presenting a substantial threat to both affected individuals and the organizations they represent. The pervasiveness of these data theft incidents raises significant alarms for Bangladesh, elevating the susceptibility to ransomware attacks. In response to this growing threat, concerted efforts have been initiated to pinpoint the most prevalent malware stealers operating in Bangladesh, aiming to address the root causes of these security breaches and fortify the nation's cybersecurity posture.

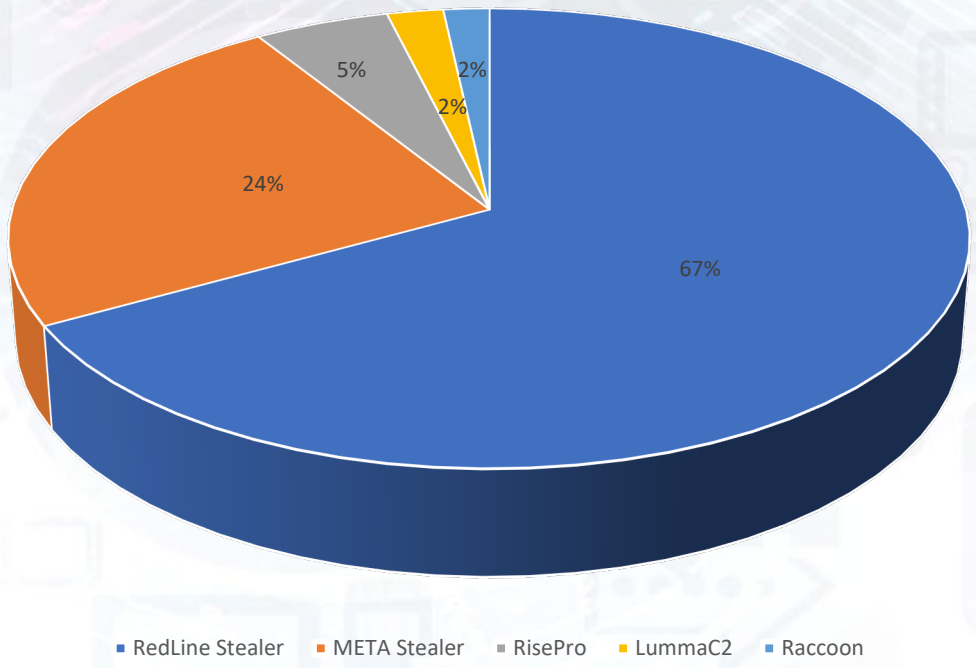


Fig: Stealer Malware records count (Percentage) in Bangladesh (recent time)

Malware	Key Characteristics	Methods	Targeted Data	Impact/Consequences	Count of Records
RedLine Stealer	Cost-efficient info-stealer; aids ransomware; customizable; surfaced in 2020.	Phishing emails, deceptive downloads	Login credentials, crypto wallets	Data theft, unauthorized access	**4,367**
MetaStealer	Advanced variant of RedLine Stealer; surfaced recently; distributed via malspam campaigns.	Malspam campaigns, malicious ads	Sensitive information, similar to RedLine	Increased scrutiny, data theft	**1,568**
RisePro	Similar to Vidar; sold on Telegram; spread via PrivateLoader.	Downloaders like win.privateloader	Credit card info, passwords, personal data	Misuse of stolen data, identity theft	**333**
Lumma Stealer	New malware; affects Windows 7-11; no clear symptoms; distributed via email, ads, social engineering.	Infected email attachments, malicious ads	Passwords, banking info, identity theft	Severe privacy risks, financial losses	**139**
Raccoon	Basic info stealer; surfaced in 2019; lacks antivirus protection; spread via browsers, exploit kits.	Browsers, exploit kits, social engineering	Browser data, system information	Data theft, service-based distribution ($200/month)	**114**

SUMMARY

In 2023, Bangladesh's cyber threat landscape has proven increasingly hazardous, with advanced threats from APT groups, a marked rise in ransomware attacks, and heightened hacktivist activities. The surge in phishing and info stealer malware adds complexity to the security environment, underscoring the critical need for comprehensive and adaptive cybersecurity strategies. Notably, a positive development has been the increased responsiveness and collaboration from organizations, particularly financial institutions, which are now providing valuable feedback on reports and engaging more actively with incident response teams. This shift towards greater cooperation is a significant step forward in enhancing the collective defense against sophisticated cyber adversaries.