2024 MID-YEAR CYBERSECURITY REPORT

VIETTEL THREAT INTELLIGENCE

ADDRESS

41F, Keangnam Landmark 72, Pham Hung Rd., Nam Tu Liem Dist, Ha Noi, Viet Nam

28F, A2 Block, Viettel Building, 285 Cach Mang Thang Tam Rd., Ward 12, Dist.10, HCMC, Viet Nam

CONTACT US

https://viettelcybersecurity.com/

vcs.sales@viettel.com.vn

ABOUT VCS-TI

Cyberthreats are ***growing faster than ever***, outstripping the scope of any single SecOps team.

Serious threats are hidden, and can come at any time. It's crucial to recognize these threats and take decisive action.

ABOUT VIETTEL CYBER SECURITY

Viettel Cyber Security is a branch of Viettel Group, conducting in-depth research and development of information security solutions, providing a wide range of cybersecurity services and products, in the way of protecting your digital assets.

Viettel Threat Intelligence is a solution provider offering intelligence and insights into information security threats to assist organizations and enterprises in developing prevention strategies and minimizing the risk of information security breaches.

FOREWORD

Through our **2024 Mid-year Cybersecurity Report**, we focus on analyzing and sharing information about the cybersecurity threat overview in the Philippines in the first half of 2024, including the following areas:

- Malware variants actively operating and exerting significant impact.
- Brand abuse.
- APT groups targeting large organizations and enterprises in the Philippines.
- Analysis of cybersecurity vulnerabilities that emerged in the first half of 2024.
- Data breach & Compromised credentials of individuals and organizations.

Disclaimer: *This report is exclusively intended to disseminate technical information to the cybersecurity community, organizations and enterprises, intending to enhance awareness of cybersecurity and devise precautionary measures for cybersecurity risks. Any assertions diverging from the content of this report are incongruent with our publication objectives. The report incorporates certain information collected during the provision of services to Viettel Cyber Security's clients and references data from several other sources with full citations.*

- Viettel Threat Intelligence -

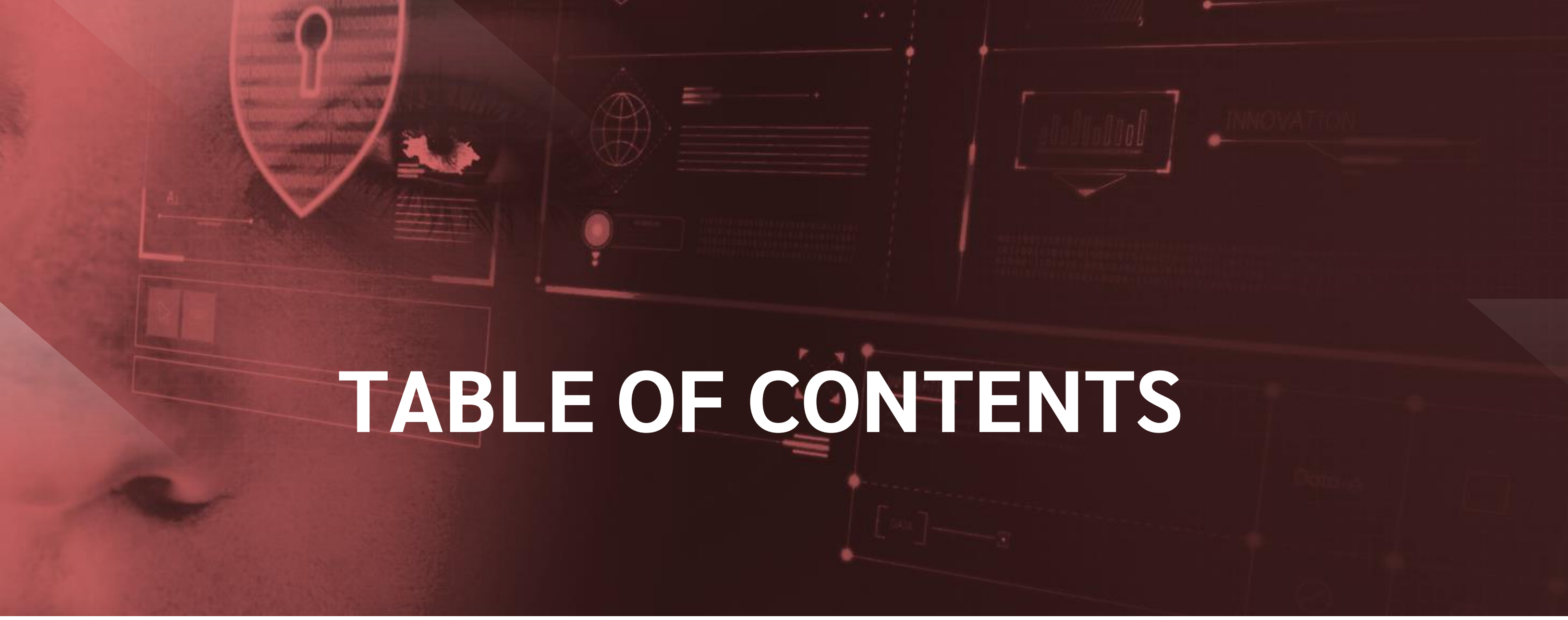


TABLE OF CONTENTS

KEY FINDINGS ON CYBERSECURITY TRENDS

For the first half of 2024, Viettel Threat Intelligence has identified several emerging cyber threats in the Philippines affecting individuals and organizations. Some prominent ones include:

Compromised Credentials & Data Breaches

Over **315,000**

Compromised credentials

47 data selling incidents:

- **660 Million** records
- **1TB** of data, **150GB** KYC data

17,456 Phishing Attacks

↑ by **27%**

in comparison with H1 2023

Top 3 targeted industries:

- **Financial–services**
- **E-commerce**
- **Government**

Vulnerabilities

17,648 **new**

vulnerabilities worldwide

↑ by **42%**

in comparison with H1 2023

- **71 new** vulnerabilities could potentially impact **Southeast Asia**.
- **Previously identified vulnerabilities** are being exploited for scanning and further attacks.

Attack Campaigns

7 APT Groups with **Significant Impact**

Most frequent Techniques: **DLL-Sideloading, CVE**

7 TERABYTES

encrypted data in **Southeast Asia**

Ransom amount: **~ $13 Million**

RECOMMENDATIONS

for Business

To ensure the operation of production and business activities for enterprises and organizations, and to minimize the risks of information security threats, Viettel Threat Intelligence offers the following recommendations:

1. Review processes, customer data management systems, internal data with data breaches and data selling incidents.
2. Implement early warning mechanisms to notify individual customers about compromised accounts using the company's services and phishing campaigns.
3. Proactively scan for indicators of compromise (IoCs), detect and respond promptly to APT groups.
4. Review, upgrade software and applications containing critical security vulnerabilities.
5. Utilize DDoS protection and mitigation services to safeguard the availability and security of organization's IT infrastructure.
6. Continuously supplement and update knowledge for security solutions from open-source or commercial sources in order to ensure information security.

In addition, to prevent the risk of increasing ransomware attacks, Viettel Threat Intelligence has the following recommendations:

1. Review data for backup: Source code, customer systems, product/service data that affects the organization's business operations.
2. Isolate networks between IT systems (business, etc.) and infrastructure management.
3. Conduct a comprehensive Information Security assessment for the organization's IT infrastructure.
4. Regularly perform proactive IoCs testing for systems.
5. Implement 24/7 continuous IT Security monitoring and response activities to detect and respond early to system attacks before severe damage occurs.
6. Implement a Threat Intelligence program to identify and respond early to cyberspace intrusion and data encryption attacks.
7. Conduct a comprehensive Information Security assessment for the organization's IT infrastructure.
8. Implement a zero trust access system to control and limit user access to resources.
9. Implement External Attack Surface Management (EASM) solutions.

H1-2024

STATISTICS & DETAILED ANALYSIS

MALWARE USECASE

Ransomware

The number of ransomware attacks is showing a significant increase, and their impact is substantial as large companies and organizations become the primary targets. Hackers often employ various methods to distribute ransomware, including phishing emails, impersonation websites, and exploiting security vulnerabilities to infiltrate target systems. The main targets of ransomware are vulnerable servers, which store valuable data and present a high potential for ransom payments.

*The data in **Ransomware** section is gathered through monitoring, incident handling, and information security management to support businesses and organizations worldwide by Viettel Cyber Security (VCS).*

Viettel Threat Intelligence issued a stark warning regarding the escalating threat of ransomware attacks targeting organizations and businesses across the Philippines. These attacks involve encrypting sensitive data and virtual infrastructure, causing severe disruptions and substantial financial losses. Attackers escalate their initial access to gain deeper system infiltration and subsequently execute data encryption through various methods such as:

- Exploiting vulnerabilities in common applications within organizations, such as email and websites, etc.
- Gaining unauthorized access through stolen credentials.
- Leveraging inadequate data partitioning and backup policies.

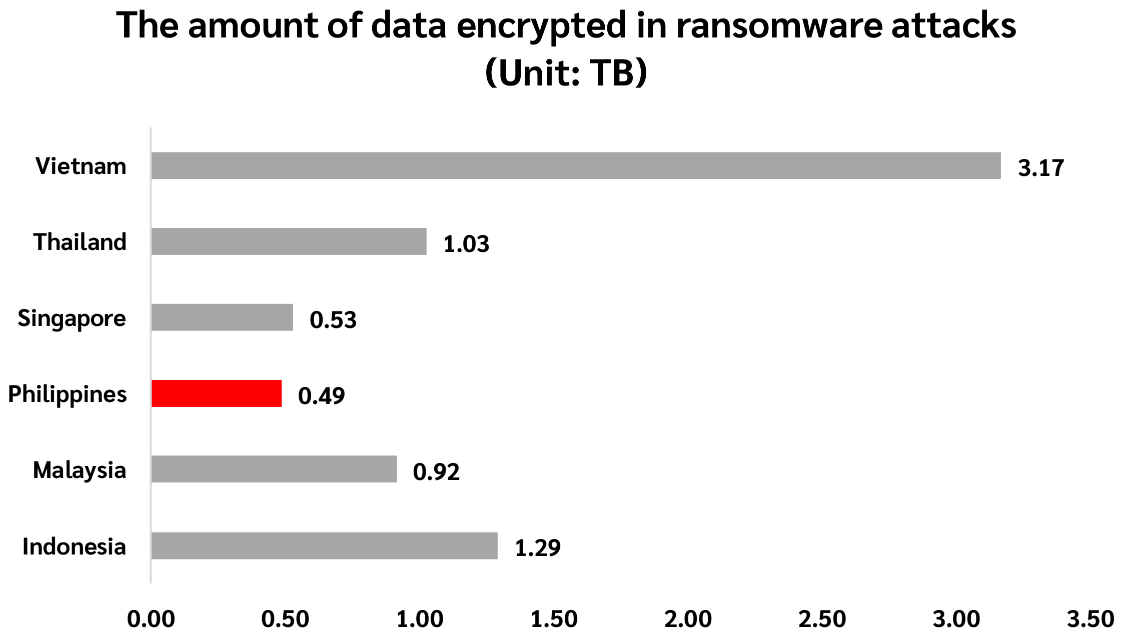


Figure 1: The amount of data encrypted in ransomware attacks across Southeast Asia (H1.2024)

In H1.2024, data encrypted in ransomware attacks across Southeast Asia reached **more than 7 Terabytes**, with the estimated total ransom amounting to **approximately 13 million USD.**

Table 1. Active ransomware groups observed by Viettel Threat Intelligence in the first half of 2024

No.	Group Name	Description	Affected targets
1	Lockbit	Operating under the Ransomware-as-a-Service (RaaS) model. According to information gathered, the group has released its latest version Lockbit 3.0.	Primarily targeting businesses and organizations.
2	Blackcat	Operating under a Ransomware-as-a-Service (RaaS) model, the group favors the Rust programming language for their ransomware variants.	Windows users.
3	APT18	An Advanced Persistent Threat operated since 2009, the group used variant of software and technique in order to gain access and control victim system such as Gh0stRat or hcdLoader.	Technology, manufacturing, government, and healthcare
4	8base	Operating under a Ransomware-as-a-Service (RaaS) model. The group use the same ransomware from Phobos group.	Primarily targeting businesses and organizations.
5	Ransomhouse	Operating under a Ransomware-as-a-Service (RaaS) model. The group recently take over affiliate and ransom data from Blackcat after the group has disband.	Primarily targeting businesses and organizations.
6	Arcus media	Operating under a Ransomware-as-a-Service (RaaS) model. The group start to emerge May this year.	Primarily targeting businesses and organizations.
7	Trinity	Operating under a Ransomware-as-a-Service (RaaS) model. The group start to emerge June this year.	Primarily targeting businesses and organizations.

Stealer Malware

In the first and second quarters of this year, there have been numerous alerts regarding various Stealer malware targeting the Philippines. Common stealer malware included Redline stealer, Raccoon stealer, Meta stealer, etc.

The data in ***Stealer Malware*** *section is gathered through monitoring, incident handling, and information security management to support businesses and organizations worldwide by Viettel Cyber Security (VCS).*

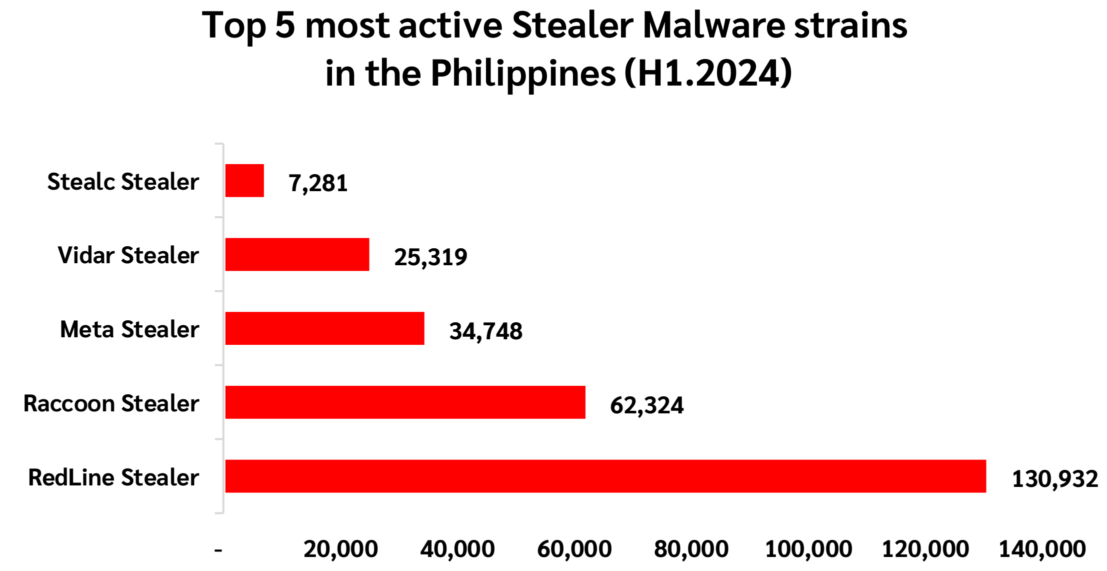


Figure 2. Top 5 most active Stealer Malware strains in the Philippines (H1.2024)

In the first half of 2024, Viettel Threat Intelligence has recorded **17,456 phishing attacks** targeting users in the Philippines. The number of attacks increased by **27%** compared to the same period in 2023, indicating that phishing attacks are still a major trend for cybercriminal groups and a serious concern for businesses, organizations, and users in the Philippines.

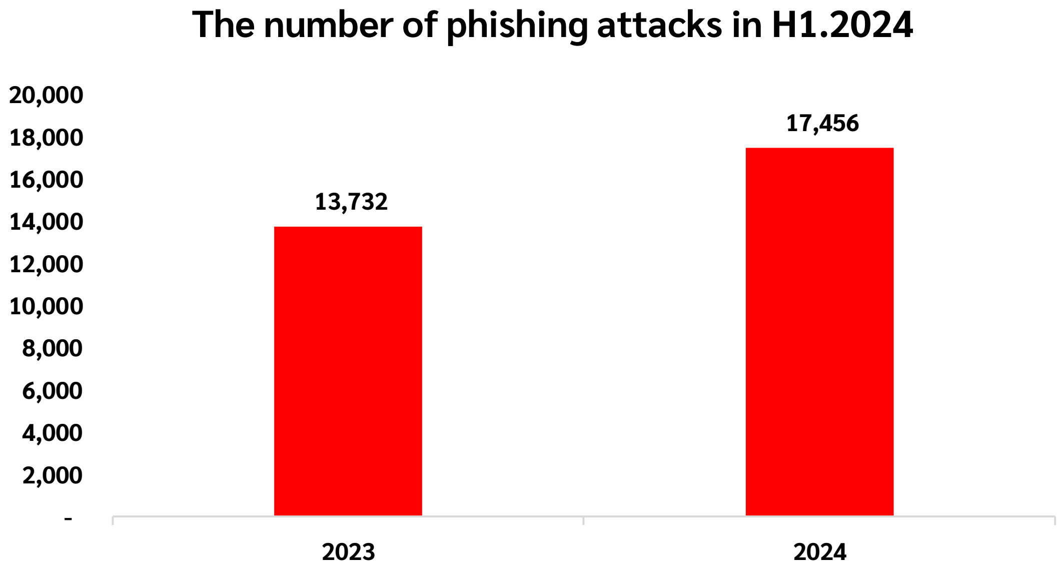


Figure 3. The number of phishing attacks in the Philippines (H1.2024)

The Financial–services sector is the top target for phishing attacks, accounting for 36% of all attacks. This is followed by the e-commerce industry with 21%.

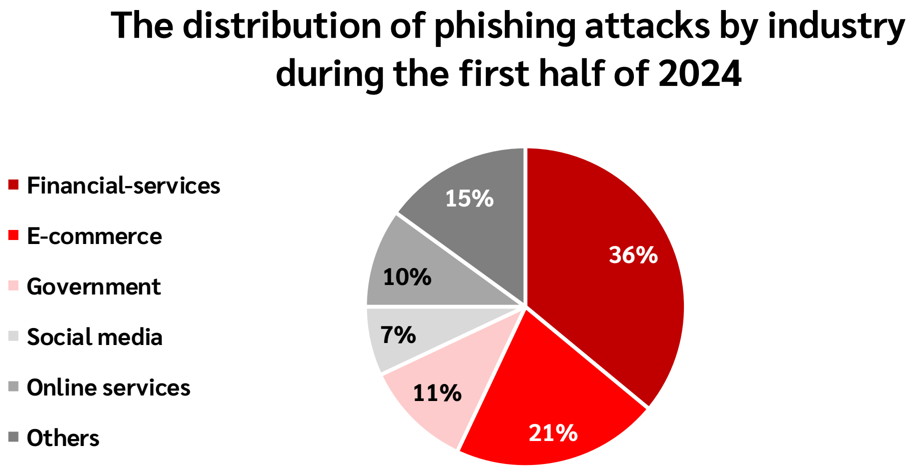


Figure 4. The distribution of phishing attacks by industry (H1.2024)

Compromised Credentials & Data Breaches

*The data in the **Compromised credentials & data breaches** section is gathered through monitoring, incident handling, and information security management to support businesses and organizations worldwide by Viettel Cyber Security (VCS).*

over 315,000 compromised credentials

Viettel Threat Intelligence has recorded **over 315,000 compromised credentials** in the Philippines in the first half of 2024. The rise of Stealer-as-a-service (SaaS) and Stealer Malware groups have contributed significantly to the increase of compromised credentials.

Numerous incidents involving the leak of privileged credentials for critical and sensitive systems, such as email systems, single sign-on (SSO) management systems, Active Directory (AD) systems, and internal access VPNs, have raised serious concerns. If this information falls into wrong hands, it could be used for malicious purposes, such as disrupting operations, stealing sensitive data, or conducting cyberattacks.

Data breaches & Selling on dark web

47 reported breaches

The first half of 2024 witnessed a surge in data breaches and selling on darkweb in the Philippines cyberspace. The amount of data breaches reached **over 660 million records**, more than **1TB** of data and nearly **150GB** of **KYC** data. These are alarming figures regarding the situation of data breaches in the Philippines.

The number of cases of data breaches and selling on dark web remained high, especially in March with 15 incidents:

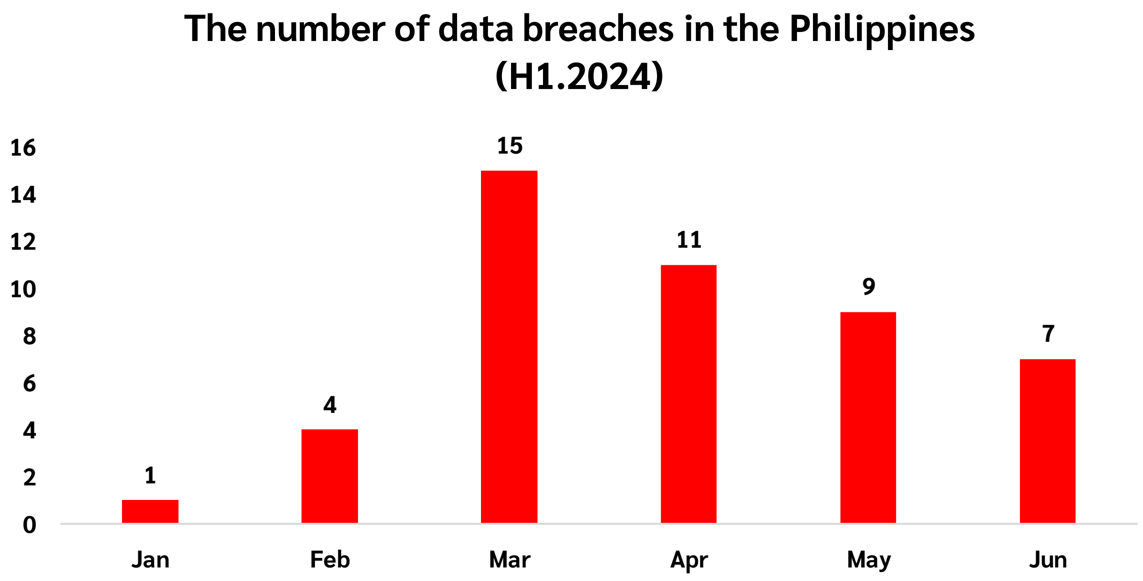


Figure 5. The number of data breaches in the Philippines (H1.2024)

The government sector experienced the highest number of data breach incidents, accounting for 26.1% of the total, followed by the education sector with 17.4%. Retail and service businesses have also become targets of attack groups, accounting for a total of 10.9%.

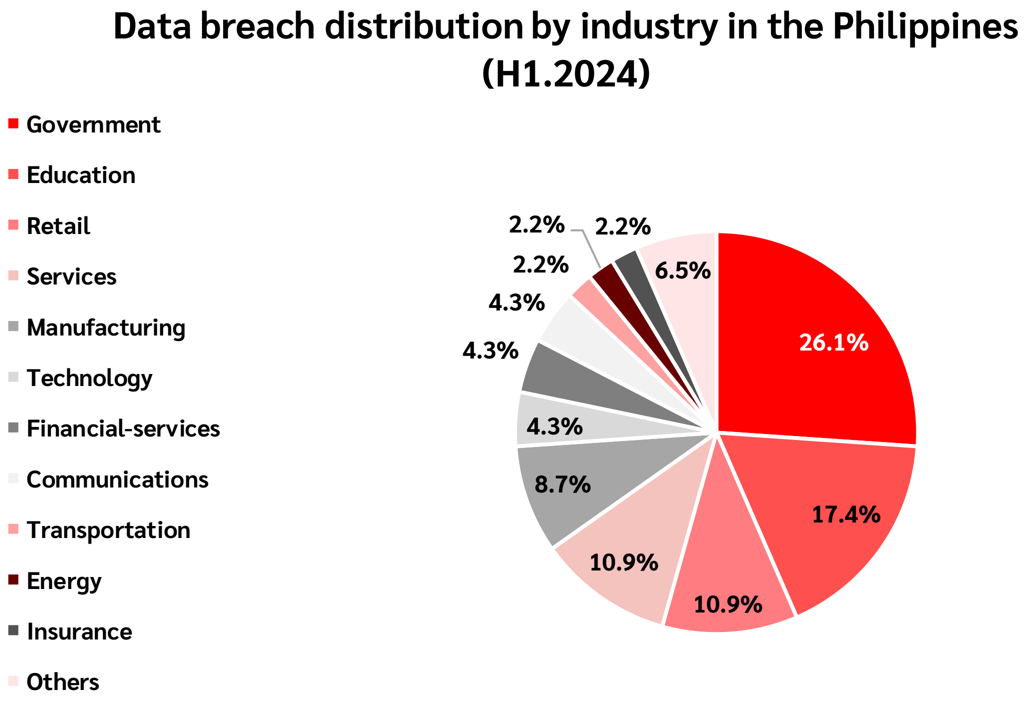


Figure 6. Data breach distribution by industry in the Philippines (H1.2024)

VULNERABLITY USECASE

*The data in the **Vulnerability Usecase** section is gathered through monitoring, incident handling, and information security management to support businesses and organizations worldwide by Viettel Cyber Security (VCS).*

In the first half of 2024, the number of vulnerabilities recorded worldwide **has increased by 42%** compared to the same period in 2023. Among them, the total number of **High** and **Critical** severity vulnerabilities (according to CVSS scores) accounts for 51% of the total vulnerabilities disclosed in cyberspace.

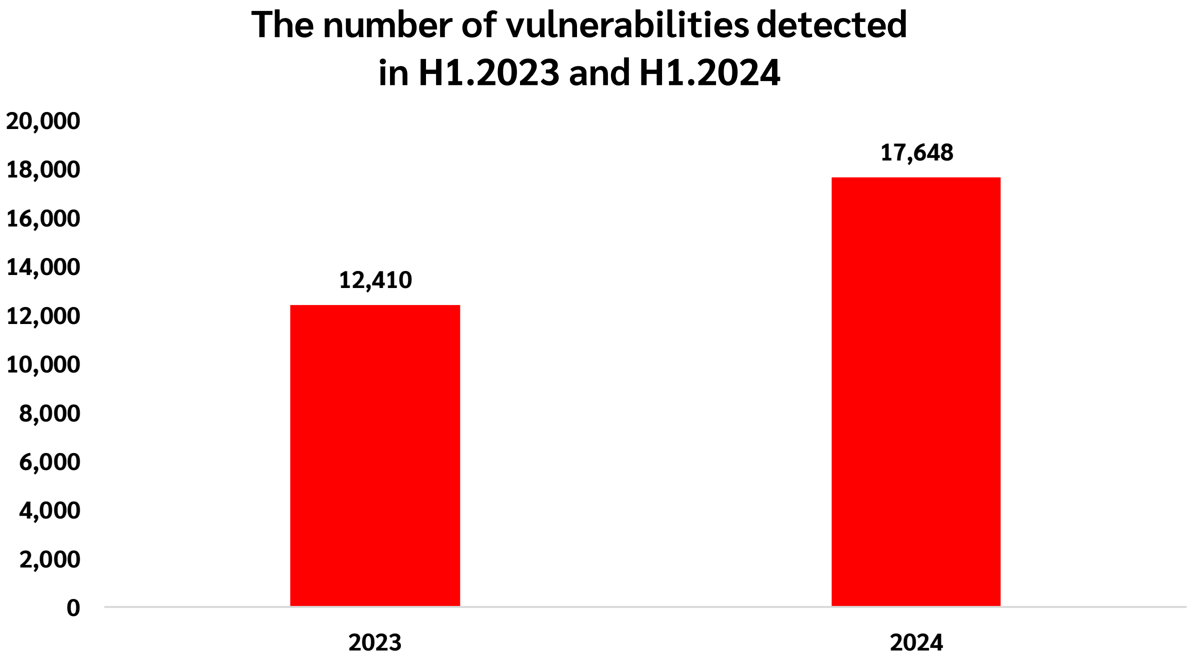


Figure 7. The number of vulnerabilities detected in H1.2023 and H1.2024

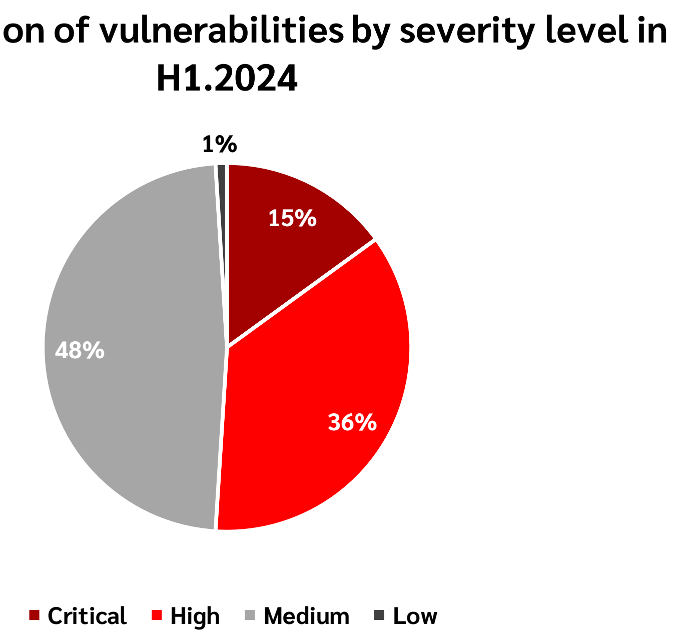


Figure 8. The proportion of vulnerabilities by severity level in H1.2024

71 alerts

related to vulnerabilities

Through the assessment and analysis of vulnerabilities, Viettel Threat Intelligence has issued **71** alerts related to vulnerabilities that significantly impact organizations and enterprises in the Philippines, specifically as follows:

Table 2. The number of vulnerabilities recorded in H1.2024 by severity level

Severity	Amount
Critical	2
High	23
Medium	45
Low	1

Below is a list of the **top 10 vulnerabilities in H1.2024** that Viettel Threat Intelligence assessed as having **significant impact** on organizations and enterprises within the Philippines due to the widespread utilization of the affected products:

Table 3. Top 10 vulnerabilities assessed as having significant impact on organizations and enterprises within the Philippines

Vulnerability name	General information	Severity level assessed by Viettel Threat Intelligence	Type
CVE-2024-21887 & CVE-2023-46805	The risk of exploiting CVE-2024-21887 vulnerability in Ivanti Connect Secure, a popular VPN solution used by many organizations. Exploiting the SSRF vulnerability combined with CVE-2024-21887 allows unauthenticated attackers to remotely execute code on the target systems.	**Critical**	RCE
CVE-2024-3400	The risk of exploiting CVE-2024-3400 vulnerability in PaloAlto Networks PAN-OS products. Attackers can exploit this vulnerability without authentication to remotely execute code on the target system. This vulnerability has been actively exploited in real-world attack campaigns.	**Critical**	RCE

Vulnerability name	General information	Severity level assessed by Viettel Threat Intelligence	Type
CVE-2024-21413	The risk of exploiting CVE-2024-21413 vulnerability in Microsoft Outlook. Successful exploitation of this vulnerability allows attackers to remotely execute code on the victim's computers. Exploitation requires interaction from the users.	**High**	RCE
CVE-2024-21762	The risk of exploiting CVE-2024-21762 vulnerability in Fortinet FortiOS and FortiProxy SSL-VPN. Exploiting the out-of-bounds write vulnerability, attackers can remotely execute code on the target system without authentication. This vulnerability has been exploited in real-world attacks by Viettel Threat Intelligence.	**High**	RCE
CVE-2023-22527	The risk of exploiting CVE-2023-22527 vulnerability in Confluence Data Center and Server products. Successful exploitation of this vulnerability allows attackers to remotely execute code on the system without authentication.	**High**	RCE

Vulnerability name	General information	Severity level assessed by Viettel Threat Intelligence	Type
CVE-2023-50164	The risk of exploiting CVE-2023-50164 vulnerability in Apache Struts 2, an open-source framework for developing web applications. Successful exploitation of this vulnerability allows attackers to upload malicious files and potentially execute code remotely on vulnerable systems.	**High**	RCE
CVE-2024-24919	The risk of exploiting CVE-2024-24919 vulnerability in CheckPoint Quantum Security Gateway. Successful exploitation of the Path Traversal vulnerability allows unauthenticated attackers to access files on the systems.	**High**	Path Traversal
CVE-2024-29849	The risk of exploiting CVE-2024-29849 vulnerability in Veeam Backup Enterprise Manager. Successful exploitation of this vulnerability allows unauthenticated attackers to bypass authentication. This means attackers can potentially log in as administrators without any credentials.	**High**	Authentication Bypass

Vulnerability name	General information	Severity level assessed by Viettel Threat Intelligence	Type
CVE-2024-4040	The risk of exploiting CVE-2024-4040 vulnerability in CrushFTP, software used for managing file transfers between computers. Successful exploitation of this vulnerability allows attackers to read arbitrary files, bypass authentication, or execute malicious code directly on the systems.	**High**	SSTI
CVE-2024-27130	Risk of exploiting CVE-2024-27130 vulnerability in QNAP QTS and QuTS hero, operating systems for QNAP NAS devices. This vulnerability, caused by a stack buffer overflow, allows unauthenticated attackers to remotely execute malicious code on the target systems.	**High**	RCE

Exploited Vulnerabilities

in real-world attack campaigns

In addition to newly disclosed vulnerabilities in the first half of 2024, threat actors have continued to actively exploit previously identified vulnerabilities for scanning and exploitation purposes. Findings from Viettel Threat Intelligence for the first semester of 2024 reveal the following vulnerabilities as the most frequently exploited in real-world attack campaigns:

Table 4. Most frequently exploited vulnerabilities in real-world attack campaigns

Vulnerability name	General information	Severity level assessed by Viettel Threat Intelligence
CVE-2022-39952	The remote code execution vulnerability exists in Fortinet FortiNAC, a NAC solution by Fortinet. Successful exploitation of CVE-2022-39952 allows unauthenticated attackers to execute arbitrary code on targeted systems.	Critical
CVE-2022-26134	The remote code execution vulnerability, identified as CVE-2022-26134, has been discovered in Atlassian Confluence, a popular collaboration tool used for document storage and management by numerous organizations. Detailed information and a patch for the vulnerability have been released by Atlassian, and the exploit code has also been publicly disclosed. Attackers can exploit this vulnerability to execute arbitrary code on systems without requiring authentication.	Critical

Vulnerability name	General information	Severity level assessed by Viettel Threat Intelligence
CVE-2021-44228	Log4Shell - A vulnerability that allows remote code execution in Apache Log4j - a popular library and framework on the Java platform. By exploiting the CVE-2021-44228 vulnerability, attackers can execute code remotely and gain control of the system. This vulnerability has emerged as one of the most severe and widely exploited in real-world cyberattacks.	Critical
CVE-2021-34473	The Pre-auth Path Confusion vulnerability leads to access control bypass on Microsoft Exchange Server. This is a vulnerability within the ProxyShell vulnerability chain. ProxyShell is a combination of three vulnerabilities: CVE-2021-34473, CVE-2021- 34523, and CVE-2021-31207. Attackers can execute arbitrary code without authentication through port 443 and gain full control of the system.	High
CVE-2019-18935	The remote code execution vulnerability was identified in Telerik UI for ASP.NET AJAX. The vulnerability occurs due to insecure deserialization of JSON-formatted objects by Telerik UI through the RadAsyncUpload component. Successful exploitation of this vulnerability allows unauthenticated attackers to execute arbitrary code on targeted systems.	High

Proportion of vulnerabilities

used in real-world attack campaigns

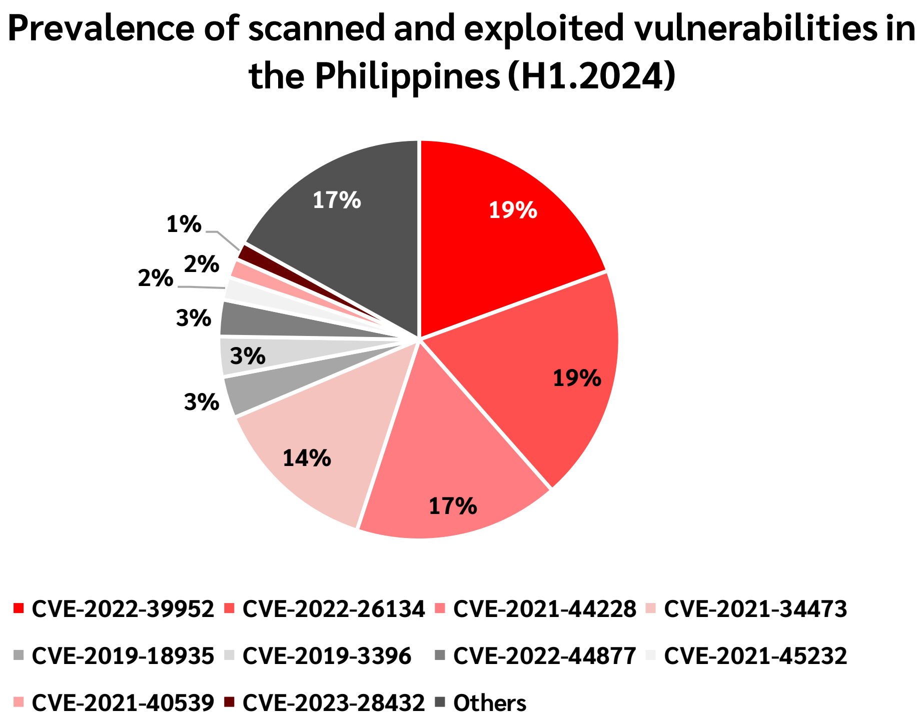


Figure 9. Prevalence of scanned and exploited vulnerabilities in the Philippines in H1.2024

The pie chart above illustrates the most commonly vulnerabilities utilized by threat actors for scanning and exploitation across organizational systems in the Philippines during the first half of 2024. These vulnerabilities include: CVE-2022-39952 (a remote code execution vulnerability in FortiNAC), CVE-2021-44228 (a remote code execution vulnerability in Apache Log4j), CVE-2022-26134 (a remote code execution vulnerability in Atlassian Confluence), CVE-2021-34473 (a remote code execution vulnerability in Microsoft Exchange Server), CVE-2019-18935 (a remote code execution vulnerability in Telerik UI), etc.

These vulnerabilities affect widely used products in enterprise environments and allow attackers to execute remote code after exploitation without authentication, using simple exploitation scripts. Threat actors exploit these vulnerabilities as an initial foothold to gain access to systems and then perform subsequent malicious actions.

Proportion of exploited vulnerabilities

by Industry in Philippines (H1-2024)

The two pie charts below show the percentages of exploited vulnerabilities across industries: **Financial-services** and **Energy** sector.

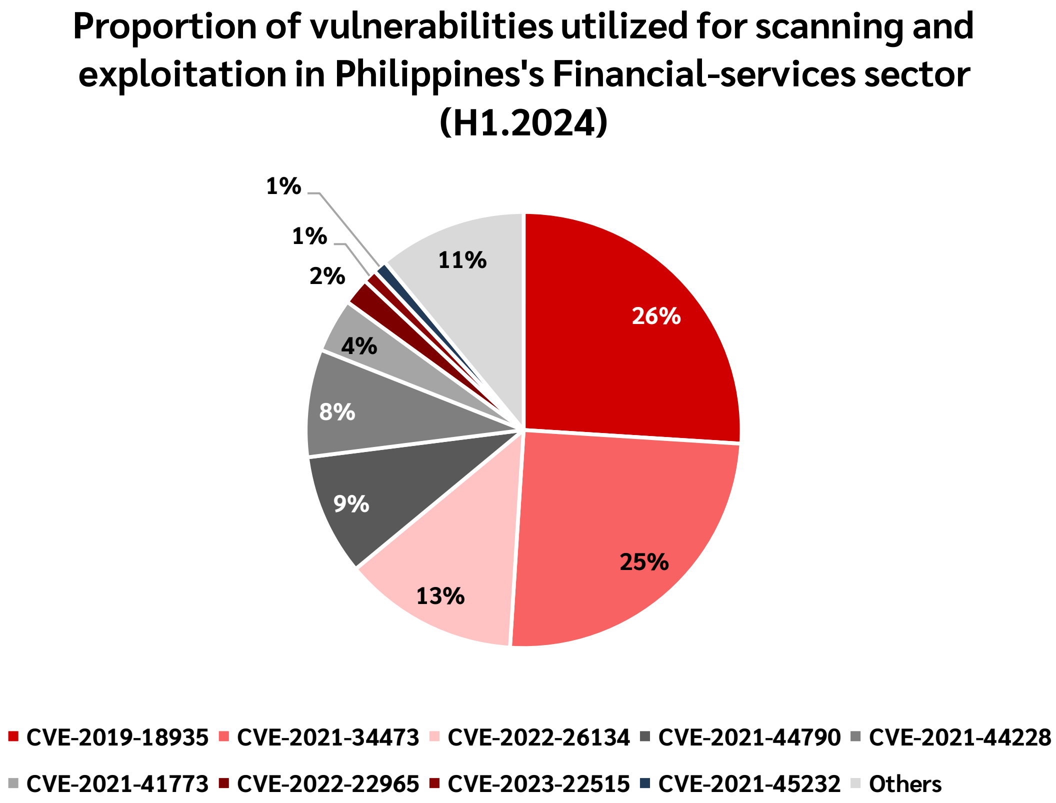


Figure 10. Vulnerabilities widely scanned and exploited in the Financial-services sector (H1.2024)

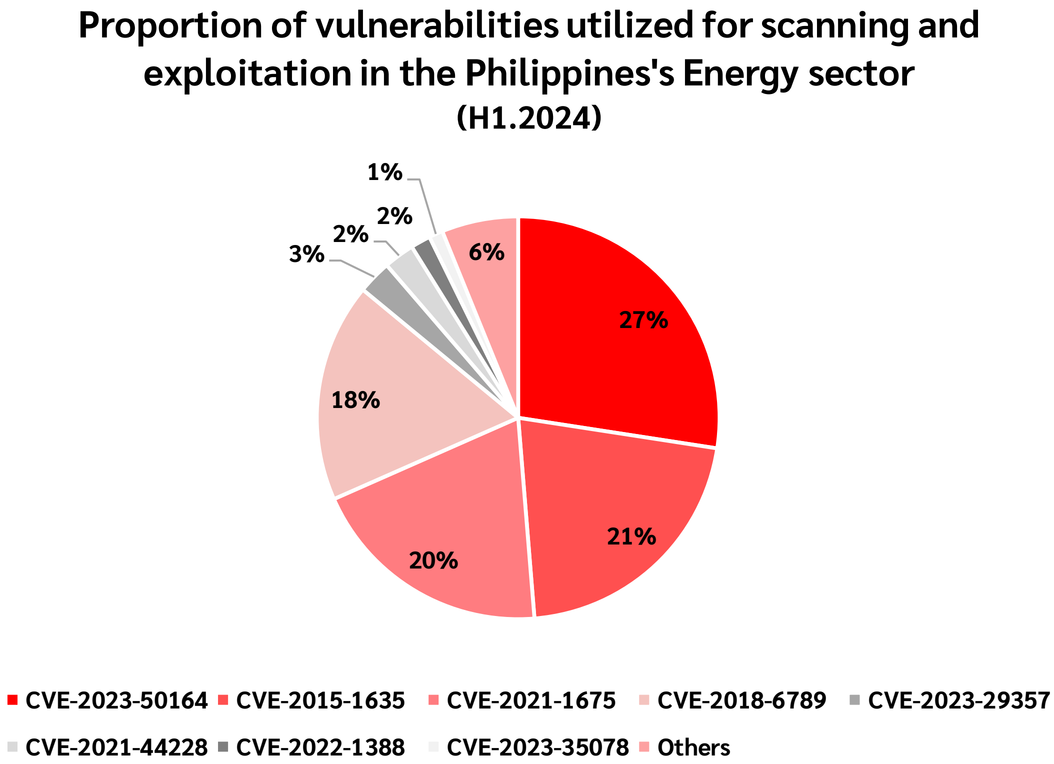


Figure 11. Vulnerabilities widely scanned and exploited in the Energy sector (H1.2024)

APT GROUPS

In H1.2024

The primary attack method employed by APT groups involved using forged documents and software to deceive users into executing malicious code.

*The data in the **APT groups** section is gathered through monitoring, incident handling, and information security management to support businesses and organizations worldwide by Viettel Cyber Security (VCS).*

Common techniques utilized by APT groups included DLL-Sideloading, exploiting clean executable files to load malicious DLLs (loaders), and leveraging CVE vulnerabilities.

In H1.2024, APT groups enhanced the tools and malware they employed in their attack campaigns. One of the most commonly used techniques by these groups was:

1. **Utilizing unfamiliar programming languages like Golang and Rust:** Malware detection relies on signatures to identify malware. Languages like Golang and Rust disrupt these signatures, making the malware harder to detect.
2. **Dynamic API Resolution, Binary Padding, Embedded Payloads:** these techniques are used to obfuscate and complicate malware analysis, effectively evading security solutions
3. **Reflective Code Loading:** this technique, often combined with Embedded Payloads, optimizes the ability to bypass security systems.
4. **Cloud Exploitation**: Exploiting cloud services like AWS, Azure to conduct attacks
5. **Command and Control (C2) over Legitimate Services:** Using legitimate services such as Dropbox, Google Drive, Twitter, Discord to establish channels for malware command and control.

6. **DLL-SideLoading:** This is the most common technique used by attack groups. They utilize this method to bypass system defenses by executing payloads through a legitimate process.

List of APT Groups with Significant Impact on Southeast Asia Businesses and Organizations in H1.2024

1

Mustang Panda

Sector: Government

In H1.2024, Viettel Threat Intelligence detected numerous malware variants associated with Mustang Panda targeting businesses, organizations, and the public services sector in Southeast Asia.

Frequently Used Techniques and Tools: Spearphishing Attachment, DLL Side Loading, Template Injection.

2

APT32

Sector: Public services

Recently, the APT32 group employed a new Rust-based malware variant to execute Cobalt Strike attacks against government agencies and organizations.

Frequently Used Techniques and Tools: Spearphishing Attachment, DLL Side Loading, ActiveMime, Cobalt Strike.

3

Kimsuky

Sector: Business

Viettel Threat Intelligence also identified Kimsuky malware targeting critical infrastructure. The group utilized the AppleSeed malware to steal sensitive information and techniques from organizations.

Frequently Used Techniques and Tools: Spearphishing Attachment, DLL Side Loading, CVE exploiting.

4

SharpPanda

Sector: Government

SharpPanda, first detected in 2018, frequently employs phishing emails in conjunction with Microsoft Office vulnerabilities.

Frequently Used Techniques and Tools: Spearphishing Attachment, DLL Side Loading, CVE exploiting.

5

Lazarus

Sector: Government, Banking - finance

This group has conducted numerous attack campaigns against Southeast Asia businesses.

Frequently Used Techniques and Tools: Spearphishing Attachment, DLL Side Loading, Template Injection, LNK.

6

APT27

Sector: Business

During cybersecurity investigation, Viettel Threat Intelligence discovered malicious code from APT27 targeting various Southeast Asia companies and organizations.

Frequently Used Techniques and Tools: Spearphishing Attachment, DLL Side Loading.

7

APT28

Sector: Business

The group often utilizes phishing emails, security vulnerabilities, or compromised accounts to spread malware.

Frequently Used Techniques and Tools: Spearphishing Attachment, DLL Side Loading.

The figure below lists APT groups with the most connected IPs in **Southeast Asia** accessing connections during H1.2024.

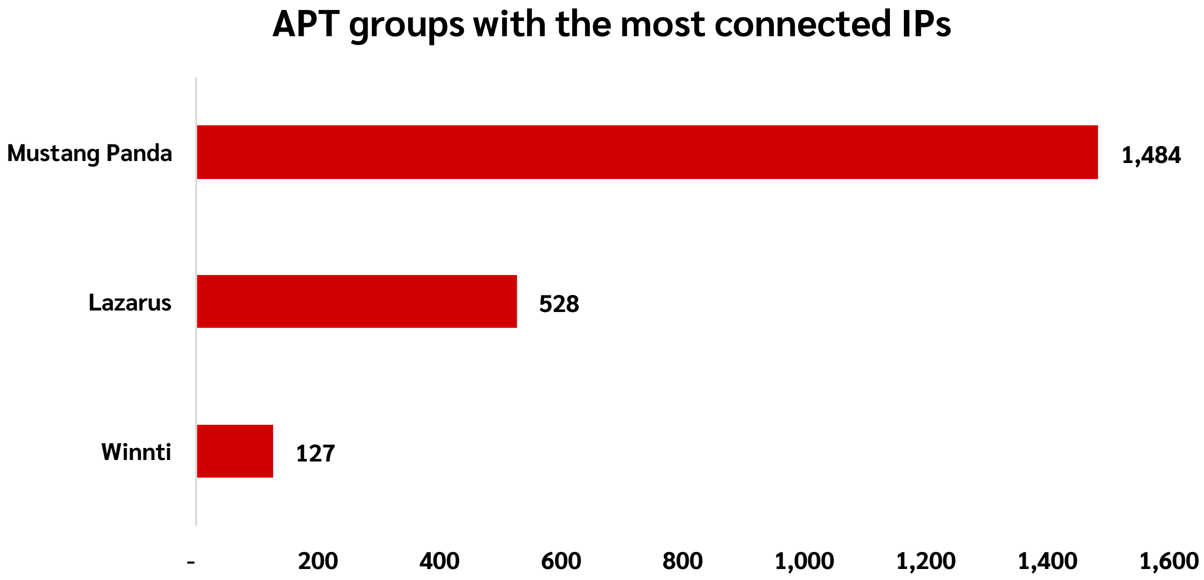


Figure 12. APT groups with the most connected IPs (H1.2024)

Table 5. List of notable APT campaigns in H1.2024

No.	APT campaign	Description	Sector	Time
1	Warning about Kimsuky APT campaign	Warning about APT attack campaign by the Kimsuky group aimed at critical infrastructure. The malware's mission is to steal important technical and organizational information. The malicious code used is AppleSeed, leveraging JavaScript to attack victim machines. During monitoring in cyberspace, Viettel Threat Intelligence has detected malicious code from the	Many sectors	Jan 2024

No.	APT campaign	Description	Sector	Time
		Goblin Panda group targeting Southeast Asia.		
2	Warning about Goblin Panda APT campaign	During network monitoring, Viettel Threat Intelligence detected malicious code from the Goblin Panda group targeting Southeast Asia.	Many sectors	Jan 2024
3	Warning about new malware from APT41	New malware from APT41 detected targeting critical national infrastructure of countries including the Philippines.	Many sectors	Jan 2024
4	Warning about APT28 campaign	Warning about attack campaigns used the Pawn Storm group (APT28) targeting organizations across Europe, Asia, and North America.	Public services	Feb 2024
5	Warning about suspicious malware identified as APT27	Viettel Threat Intelligence warns that during network reconnaissance, suspicious malware variants attributed to APT27 have been detected targeting several companies and organizations in Southeast Asia.	Companies & organizations in Southeast Asia	Feb 2024
6	The Mustang Panda group used DOPLUGS malware to launch attacks	Warning about the Mustang Panda group used the DOPLUGS malware to attack Asia, including	Public services	Feb 2024

No.	APT campaign	Description	Sector	Time
	in Asia	Southeast Asia. DOPLUGS is a new downloader malware with backdoor functionality designed to download more comprehensive PlugX malware.		
7	Warning about Mustang Panda APT group	Warning about during Cyberspace monitoring detected a malicious pattern associated with the Mustang Panda group.	Many sectors	Feb 2024
8	Warning about Mustang Panda APT group	Warning about the Mustang Panda group targeted Southeast Asia with attack campaigns.	Many sectors	Mar 2024
9	Warning about Earth Krahang APT group	The APT Earth Krahang group compromised public service organizations in Southeast Asia. They exploited this access to launch spear-phishing attacks and install backdoors on victim systems.	Public services	Mar 2024
10	Warning about Sharp Panda APT group malware	Warning about during cyberspace monitoring a malicious pattern was detected in fake documents tailored to the languages of targeted countries, exploiting the CVE-2017-0199.	Many sectors	Apr 2024

No.	APT campaign	Description	Sector	Time
11	Warning about new malware variant from APT32	Warning about the APT32 group targeted the public service sector in Southeast Asia with a new malicious code written in Rust, designed to execute Cobalt Strike.	Public services	Apr 2024
12	Warning about the Lazarus group campaign	Warning about the Lazarus group launched a new attack campaign using stealer malware to target popular platforms like GitHub, GitLab, and Bitbucket in an attempt to steal information.	Many sectors	May 2024
13	Warning about a suspected APT Turla campaign	Warning about a suspected APT Turla campaign used phishing emails containing Tiny backdoor malware to infect victims' systems and steal sensitive information.	Many sectors	May 2024
14	Warning about APT Mustang Panda group targeted Southeast Asia	Warning about the APT Mustang Panda group targeted Southeast Asia using counterfeit documents tailored to the local language.	Many sectors	Jun 2024
15	The attack campaign by the DarkPeony group aimed to distribute the PlugX malware	Warning about the DarkPeony group launched an attack campaign spreading malware through MSC files to implant PlugX malware on targeted devices.	Many sectors	Jun 2024

APPENDIX

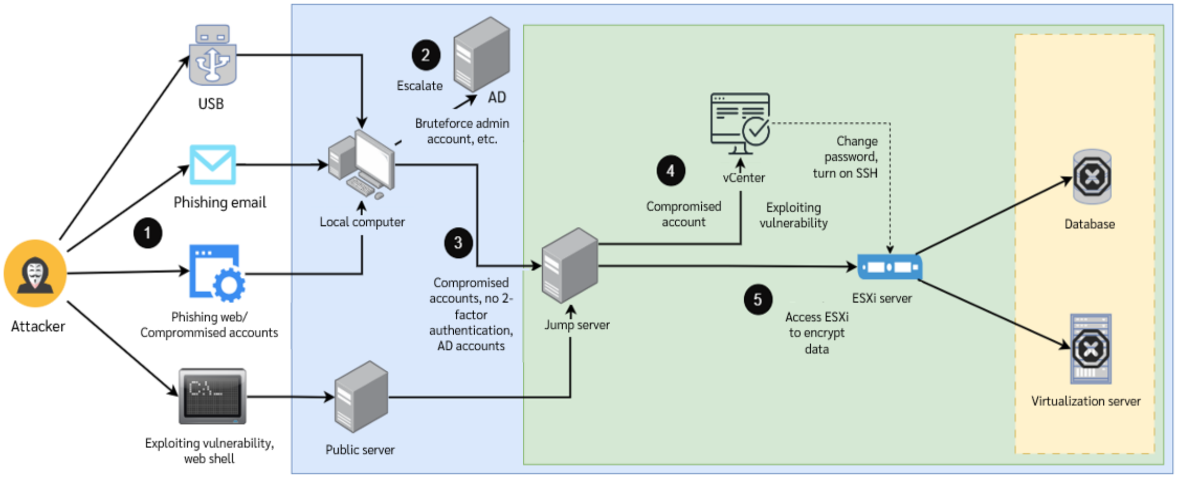
RANSOMWARE ENCRYPTING DATA AND TARGETING VIRTUALIZATION INFRASTRUCTURE OF ORGANIZATIONS AND ENTERPRISES

I. SUMMARY

Viettel Threat Intelligence warns about the risk of Ransomware encrypting data and virtual infrastructure of organizations and enterprises. The attack campaign is strongly active, purposeful, and targets businesses and organizations in Southeast Asia. Specific as follows:

- **Attack methods:** The attackers escalate privileges, embed deep within the system, and carry out encryption using methods such as:
  - Exploiting vulnerabilities in public-facing applications within the organization. Example: email, website, etc.
  - Compromising login credentials of critical systems within the organization.
  - Inadequate data partitioning policies, backup procedures, etc.
- **The impact on organizations:**
  - **Data loss:** Organization's data being encrypted and stolen may lead to leakage of sensitive and important information.
  - **Service disruption:** Encryption of the organization's virtual infrastructure leads to disruptions in production and business activities. The disruption can last for days, weeks, or may not be recoverable if there are no adequate backup policies and contingency systems.
  - **Impact on the organization's reputation:** For businesses, service disruption or experiencing cybersecurity incidents can erode trust among partners and customers, leading to doubts, suspicion, and lower assessments of the business's ability to provide products/services.

II. ATTACK SCENARIO



Step 1: Initial access

The attackers infiltrate the organization's network through the following methods:

- Malware is installed within the internal network through phishing emails, fraudulent websites, USB, etc.

*(Detailed information about the malware samples can be found in **VI. MALWARE ANALYSIS**)*

- Through brute force or obtaining compromised remote system login accounts to access the internal network.
- Through exploiting vulnerabilities in public systems, attackers install webshells and escalate privileges within the internal network.

Step 2: Escalate privilege

When the attackers gain access to a local device, they will attempt to escalate privileges to carry out further attacks. For example, they may:

- Brute-force administrator accounts.
- Seize control of Active Directory administration.
- Compromise other workstations, etc.

Step 3: Access management zone

After escalating privileges, the attackers attempt to access the network area containing virtualization management systems through various ways such as:

- Allowing workstations access to the administrative network zone.
- Using shared AD accounts for computers accessing the administrative network zone.
- Bypassing two-factor authentication when accessing the administrative network zone.

Step 4: Gain access to the vCenter hypervisor

While situated in the administrative network zone, the attackers take advantage of the following weaknesses to gain access to the VCenter administration system:

- Exploiting control takeover vulnerabilities on the VCenter administration system such as: CVE-2022-31680, CVE-2021-22005, CVE-2021-21985, CVE-2021-21972, etc.

*(Detailed information about the exploitable vulnerabilities can be found in section **V. VULNERABILITIES IN VCENTER AND EXSI**)*

- By stealing administrative accounts stored on intermediate systems.

Then, the attackers enable SSH on ESXi or change the SSH password of ESXi.

Step 5: Encrypt fully virtualized infrastructures and demand ransom

The attackers access ESXi via SSH, turn off all virtual machines and encrypt fully virtualized infrastructures.

III. RECOMMENDATIONS

Strengthen organization's cybersecurity:

- *Short-term:*
  - Review backup systems, ensuring that backup data is physically and logically separated from main systems, with the ability to restore in case of serious incidents (including servers, applications, data).
  - Review and disable direct SSH access on ESXi servers, and enhance monitoring of the enabling/disabling of this feature.
  - Review and restrict access rights to virtualization management servers (vCenter).
  - Review and restrict access rights to jump servers, control administrative connections from jump servers to critical systems.
  - Review and restrict administrative account configurations on the Active Directory system and related systems that share administrative accounts.
  - Alert or lock accounts upon detecting multiple failed login attempts or logins from unfamiliar IPs (IPs unrelated to the organization or from different countries).
  - Apply the Principle of Least Privilege to all systems and services, where users only have access rights necessary to perform their tasks.
  - Update patches for vulnerabilities in Internet-facing applications.
  - Consider implementing multi-factor authentication for critical systems and accounts.

- *Long-term:*
  - Network segregation: Separate network resources (servers, workstations, IoT devices, etc.).
  - Review and assess cybersecurity condition of the entire organization's IT infrastructure.
  - Periodically conduct proactive penetration testing and threat hunting for systems.
  - Implement 24/7 IT Security monitoring and response activities to detect and promptly handle attacks on systems before significant damage occurs.
  - Deploy Threat Intelligence service to identify and respond early to ongoing intrusion campaigns, data encryption attacks in cyberspace.
  - Implement privilege management solutions (PAM/PIM).
  - Implement zero trust access control systems to control and restrict user access to resources.
  - Implement External Attack Surface Management solutions.

IV. COMMON MISTAKES

1. Allowing the display of information about remote connection services such as VPN, RDP through default ports or displaying them on the website without device restrictions.

Threat: Attackers may scan for remote connection services, exploit vulnerabilities in these services, or leverage compromised accounts to infiltrate the system.

Recommendations:

- Change the default ports for RDP, VPN connections. Avoid sharing or displaying VPN, RDP information on the website.
- Restrict the users, devices, and IPs allowed to use RDP.

2. Allowing partners and third-party services to connect to the organization's system without proper authorization or access limitations.

Threat: Attackers may target partners, third-party services, and subsequently gain direct access to the organization's system.

Recommendations:

- Apply the Principle of Least Privilege to all parties, where third parties are granted minimal access necessary to perform their respective tasks.
- Consider implementing zero trust access control systems, which only allows access or usage when permission is granted.

3. Email credentials, VPN, or critical system accounts stored in the browser or insecure environments (saved in txt files, Excel, notes, etc.).

Threat: Attackers steal stored passwords from browsers or insecure environments to carry out attacks.

Recommendations:

- Do not store passwords in browsers.
- Utilize specialized password management software with multi-factor authentication.
- Consider implementing multi-factor authentication mechanisms for critical systems and accounts.

V. VULNERABILITIES IN VCENTER AND EXSI

Here is a list of vulnerabilities found in VCenter and ESXi that attacker groups could exploit to gain initial access to the target system in real-world scenarios:

CVE-2021-21985, CVE-2021-21974, CVE-2022-31680, CVE-2021-22005, CVE-2019-5544, CVE-2021-21972, CVE-2020-3952, etc.

1. CVE-2021-21972 | Remote Code Execution vulnerability in VMWare vCenter Server

General information:

The vulnerability allows an unauthenticated attacker to exploit via port 443 to upload arbitrary files, thereby executing unrestricted commands on the operating system of the vCenter Server.

Severity level assessed by VCS-TI: **Critical**.

Precondition:

- VMWare vCenter versions below 6.5 U3n, 6.7 U3l, or 7.0 U1c
- The attackers have a connection to portal web VMware vCenter

Signs of recognition:

The hackers' packet exhibits the following signs:

- HTTP POST request method
- URL "/ui/vropspluginui/rest/services/uploadova"

Suricata rule:

```
alert http any any -> any any (msg:"Detect CVE-2020-21972"; flow:to_server,established; content:"/ui/vropspluginui/rest/services/uploadova"; startswith; http_uri; content:"POST"; http_method; classtype:web-application-attack; sid:20212322; rev:1;)
```

2. CVE-2021-21985 | Remote Code Execution vulnerability in VMware vCenter Server

General information:

The vulnerability occurs due to the lack of input validation in the Virtual SAN Health Check plug-in, which is enabled by default. Attackers exploit this vulnerability through port 443. Upon successful exploitation, the attacker gains the ability to execute arbitrary commands on the vCenter server without authentication.

Severity level assessed by VCS-TI: **High**.

Precondition:

- The server is installed and uses one of the following versions:
  - vCenter Server 6.5
  - vCenter Server 6.7
  - vCenter Server 7.0
  - Cloud Foundation (vCenter Server) 3.x
  - Cloud Foundation (vCenter Server) 4.x
- The attackers need the ability to access vCenter Server via port 443

Signs of recognition:

The hackers' packet exhibits the following signs:

- HTTP POST request method
- Query to "/ui/h5-vsan/rest/proxy/service/&vsanProviderUtils_setVmodlHelper"
- Queries containing the string "methodInput"

Suricata rule:

```
alert http any any -> any any (msg:"CVE-2021-21985";content:"POST";http_method;content:"/ui/h5-vsan/rest/proxy/service/&vsanProviderUtils_setVmodlHelper"; startswith;http_uri;content:"methodInput";http_client_body;classtype:web-application-attack;sid:20212462;rev:1;)
```

3. CVE-2022-31680 | Remote Code Execution vulnerability in VMware vCenter Server Platform Services Controller

General information:

Java deserialization vulnerability in the Platform Services Controller feature of VMware vCenter Server. An attacker with administrator privileges can exploit this vulnerability to remotely execute code on the system.

Severity level assessed by VCS-TI: **High**.

Precondition:

- The server runs VMware vCenter Server version 6.5
- An attacker with administrator privileges can connect to the system

Signs of recognition:

The hackers' packet exhibits the following signs:

- HTTP GET request method
- Query to endpoint /psc/data/constraint/
- Contain base64 strings in URI

4. CVE-2021-22005 | Remote Code Execution vulnerability in VMware vCenter Server

General information:

Vulnerability occurs in the Analytics Service, where unauthenticated attackers can exploit via port 443 to upload arbitrary files. Successful exploitation allows unauthenticated attackers to remotely execute code on the server, thereby gaining system control.

Severity level assessed by VCS-TI: **Critical.**

Precondition:

- The server is installed and utilizes VMware vCenter Server versions 6.7 and 7.0.
- The attackers need the ability to access vCenter Server via port 443.

Signs of recognition:

First scenario:

The hackers' packet exhibits the following signs:

- HTTP POST request method
- Query to "/analytics/telemetry/ph/api/hyper/send"
- Contain "../" string (exploit path traversal vulnerability)

Suricata rule:

alert http any any -> any any (msg:"Detecting CVE-2021-22005 attack telemetry endpoint";content:"POST";http_method;content:"/analytics/telemetry/ph/api/hyper/send"; startswith;http_uri;content:"../";http_uri;classtype:web-application-attack;sid:202127721;rev:1;)

Second scenario:

The hackers' packet exhibits the following signs:

- HTTP POST request method
- Contain "/analytics/ph/api/dataapp/agent" string
- Contain "..;/" string (bypass proxy filter to exploit path traversal vulnerability)

Suricata rule:

alert http any any -> any any (msg:"Detecting CVE-2021-22005 attack dataapp

```
endpoint";content:"POST";http_method;content:"/analytics/ph/api/dataapp/agent";http_uri;content:"..|3b|/";http_uri;classtype:web-application-attack;sid:202127722;rev:1;)
```

5. CVE-2019-5544 | Remote Code Execution vulnerability in VMware ESXi

General information:

The OpenSLP service is running on VMware ESXi hosts to implement the Service Location Protocol (SLP). Attackers can directly access this service via port 427 or through the Horizon DaaS management appliance. Through this, attackers can overwrite the heap memory area of this service, leading to remote code execution.

Severity level assessed by VCS-TI: **High**.

Precondition:

- The system utilizes the following versions:
  - ESXi 6.7
  - ESXi 6.5
  - ESXi 6.0
  - Horizon DaaS 8.x
- Attackers must have internet connection to port 427 on VMware ESXi hosts or gain access to the Horizon DaaS management appliance.

6. CVE-2020-3952 | Information Disclosure vulnerability in VMware vCenter Server

General information:

An attacker with network access to port 389 on vmdir deployment1 can extract highly sensitive information such as administrative account authentication details. They can then use this information to compromise the vCenter Server or other services using vmdir for authentication.

Severity level assessed by VCS-TI: **High.**

Precondition:

- vCenter Server is running 6.7 version and Platform Services Controllers versions are updated from old versions of vSphere.
- The attacker must have network connection to VMware Directory Service.

RECOMMENDATIONS

- Viettel Threat Intelligence recommends administrators to update VMware vCenter and ESXi to the latest versions, and install all available patches for vulnerabilities. The download path for patches is:

    - https://customerconnect.vmware.com/group/vmware/patch
- Utilize WAF/IDS/IPS to detect and prevent exploitation attacks based on IoCs.

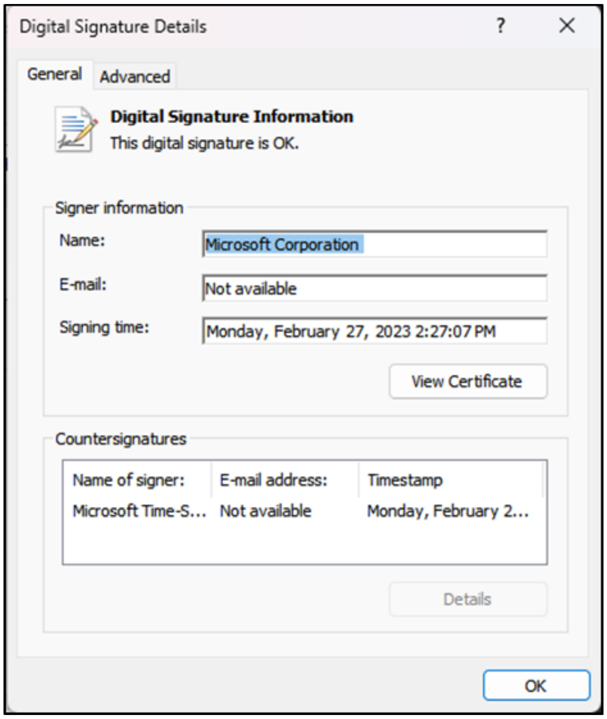
Furthermore, to ensure cybersecurity for organizations against the risk of Ransomware attacks, Viettel Threat Intelligence recommends administrators to implement the following configurations for VMware vSphere:

- Administration Connection
    - Restrict administrative connections (ports 22, 443, 5480) centrally through 2FA intermediate supporting system.
- Administrative Accounts
    - Remove unused accounts.
    - Utilize local authentication (vCenter SSO), do not use AD accounts.
    - Apply Principle of Least Privilege based on administrative tasks.
- ESXi host
    - ESXi host must be configured with lockdown mode set to at least Normal.
    - Disable SSH on all ESXi hosts.

VI. MALWARE ANALYSIS

1. Sample 1: version.dll

The malware utilizes DLL-SideLoading technique through the OneDriveStandaloneUpdater.exe program, which has a valid Microsoft signature. Upon execution, this file proceeds to execute the malicious version.dll file located in the same directory.



Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

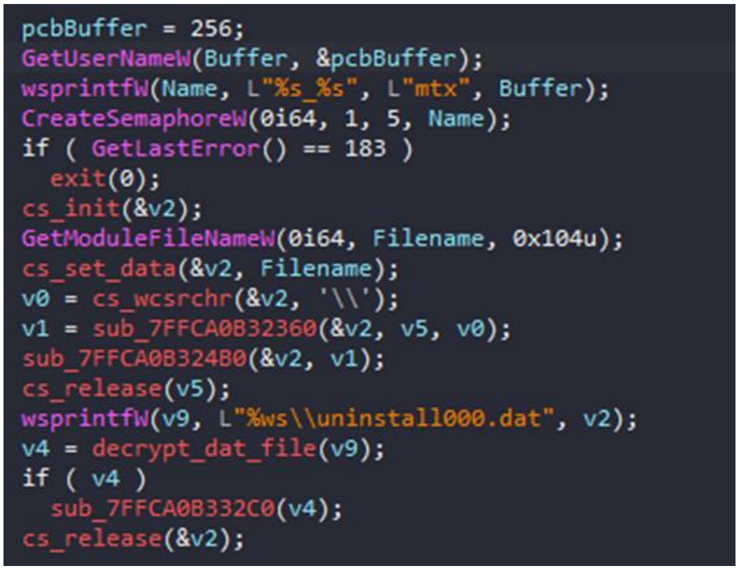
Signer information

Name: Microsoft Corporation
E-mail: Not available
Signing time: Monday, February 27, 2023 2:27:07 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Microsoft Time-S...	Not available	Monday, February 2...

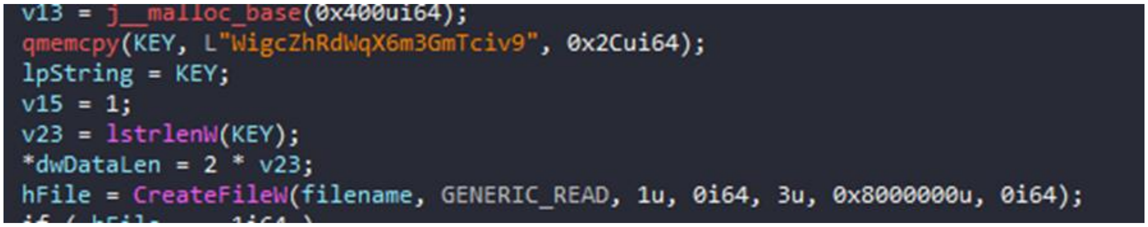
When executed, the file version.dll creates a mutex in the format mtx_<UserName>, and then proceeds to read the file uninstall000.dat in the same directory.



```
pcbBuffer = 256;
GetUserNameW(Buffer, &pcbBuffer);
wsprintfW(Name, L"%s_%s", L"mtx", Buffer);
CreateSemaphoreW(0i64, 1, 5, Name);
if ( GetLastError() == 183 )
  exit(0);
cs_init(&v2);
GetModuleFileNameW(0i64, Filename, 0x104u);
cs_set_data(&v2, Filename);
v0 = cs_wcsrchr(&v2, '\\');
v1 = sub_7FFCA0B32360(&v2, v5, v0);
sub_7FFCA0B324B0(&v2, v1);
cs_release(v5);
wsprintfW(v9, L"%ws\\uninstall000.dat", v2);
v4 = decrypt_dat_file(v9);
if ( v4 )
  sub_7FFCA0B332C0(v4);
cs_release(&v2);
```

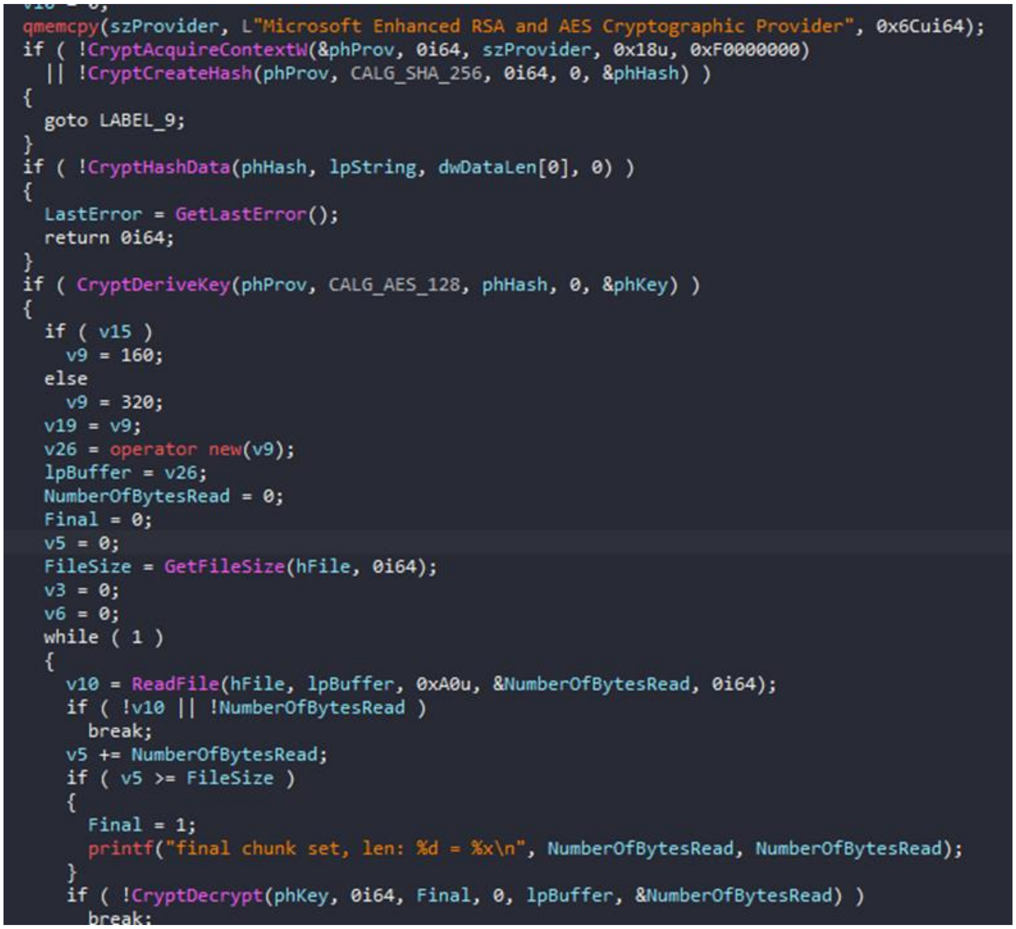
In the decrypt_dat_file command, the malware initializes the decryption key

WigcZhRdWqX6m3GmTciv9, and then opens the file uninstall000.dat.



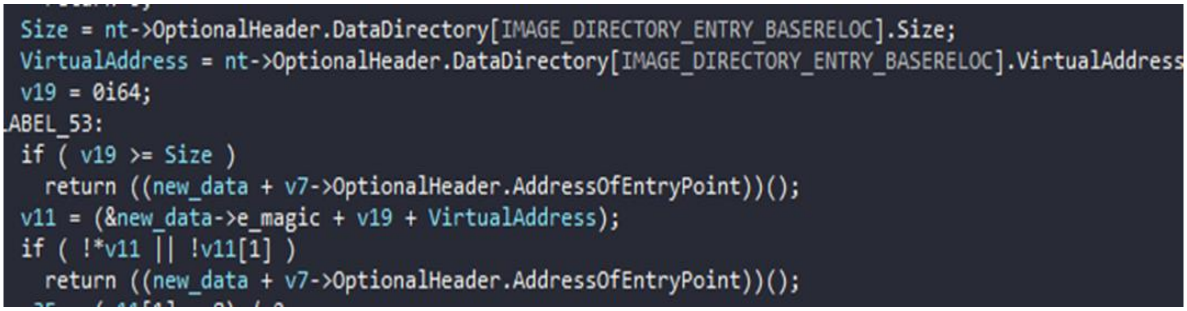
```
v13 = j__malloc_base(0x400ui64);
qmemcpy(KEY, L"WigcZhRdWqX6m3GmTciv9", 0x2Cui64);
lpString = KEY;
v15 = 1;
v23 = lstrlenW(KEY);
*dwDataLen = 2 * v23;
hFile = CreateFileW(filename, GENERIC_READ, 1u, 0i64, 3u, 0x8000000u, 0i64);
```

After initializing the decryption key, the malware hashes the key string with SHA-256 and decrypts the data in the DAT file using AES-128.



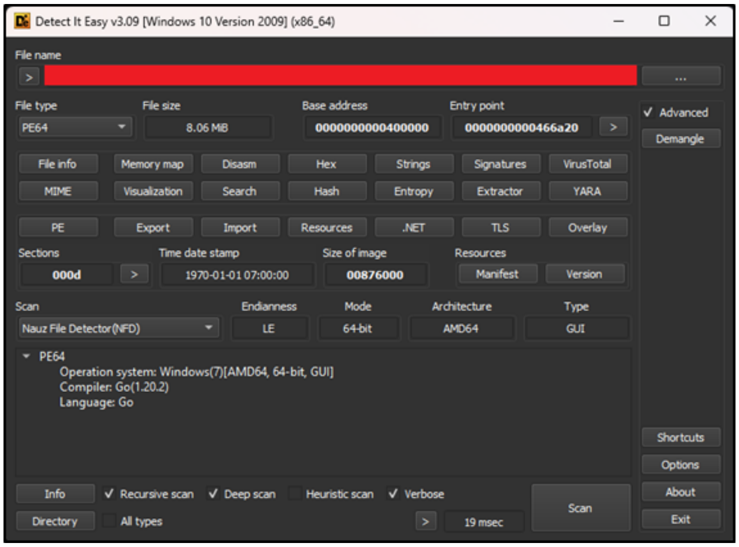
```
qmemcpy(szProvider, L"Microsoft Enhanced RSA and AES Cryptographic Provider", 0x6Cui64);
if ( !CryptAcquireContextW(&phProv, 0i64, szProvider, 0x18u, 0xF0000000)
  || !CryptCreateHash(phProv, CALG_SHA_256, 0i64, 0, &phHash) )
{
  goto LABEL_9;
}
if ( !CryptHashData(phHash, lpString, dwDataLen[0], 0) )
{
  LastError = GetLastError();
  return 0i64;
}
if ( CryptDeriveKey(phProv, CALG_AES_128, phHash, 0, &phKey) )
{
  if ( v15 )
    v9 = 160;
  else
    v9 = 320;
  v19 = v9;
  v26 = operator new(v9);
  lpBuffer = v26;
  NumberOfBytesRead = 0;
  Final = 0;
  v5 = 0;
  FileSize = GetFileSize(hFile, 0i64);
  v3 = 0;
  v6 = 0;
  while ( 1 )
  {
    v10 = ReadFile(hFile, lpBuffer, 0xA0u, &NumberOfBytesRead, 0i64);
    if ( !v10 || !NumberOfBytesRead )
      break;
    v5 += NumberOfBytesRead;
    if ( v5 >= FileSize )
    {
      Final = 1;
      printf("final chunk set, len: %d = %x\n", NumberOfBytesRead, NumberOfBytesRead);
    }
    if ( !CryptDecrypt(phKey, 0i64, Final, 0, lpBuffer, &NumberOfBytesRead) )
      break;
```

After decryption, the data is a PE file. The malware will then parse the data of this PE file and execute it in memory.



```
Size = nt->OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].Size;
VirtualAddress = nt->OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAddress
v19 = 0i64;
ABEL_53:
if ( v19 >= Size )
  return ((new_data + v7->OptionalHeader.AddressOfEntryPoint))();
v11 = (&new_data->e_magic + v19 + VirtualAddress);
if ( !*v11 || !v11[1] )
  return ((new_data + v7->OptionalHeader.AddressOfEntryPoint))();
```

The decrypted PE file is written in Golang 1.20.2 and was downloaded by the attacker from github then saved at *C:\Users\Administrator\Downloads\geacon_plus-main*. Geacon_plus is a Cobalt Strike beacon rewritten in Golang to bypass AV.



Detect It Easy v3.09 [Windows 10 Version 2009] (x86_64)

File name: [redacted]

File type: PE64 | File size: 8.06 MiB | Base address: 0000000000400000 | Entry point: 000000000466a20

☑ Advanced

Sections: 000d | Time date stamp: 1970-01-01 07:00:00 | Size of image: 00876000

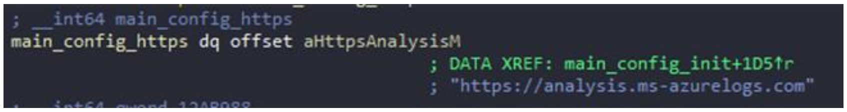
Scan: Nauz File Detector(NFD) | Endianness: LE | Mode: 64-bit | Architecture: AMD64 | Type: GUI

```
PE64
    Operation system: Windows(7)[AMD64, 64-bit, GUI]
    Compiler: Go(1.20.2)
    Language: Go
```

☑ Recursive scan ☑ Deep scan □ Heuristic scan ☑ Verbose □ All types

19 msec

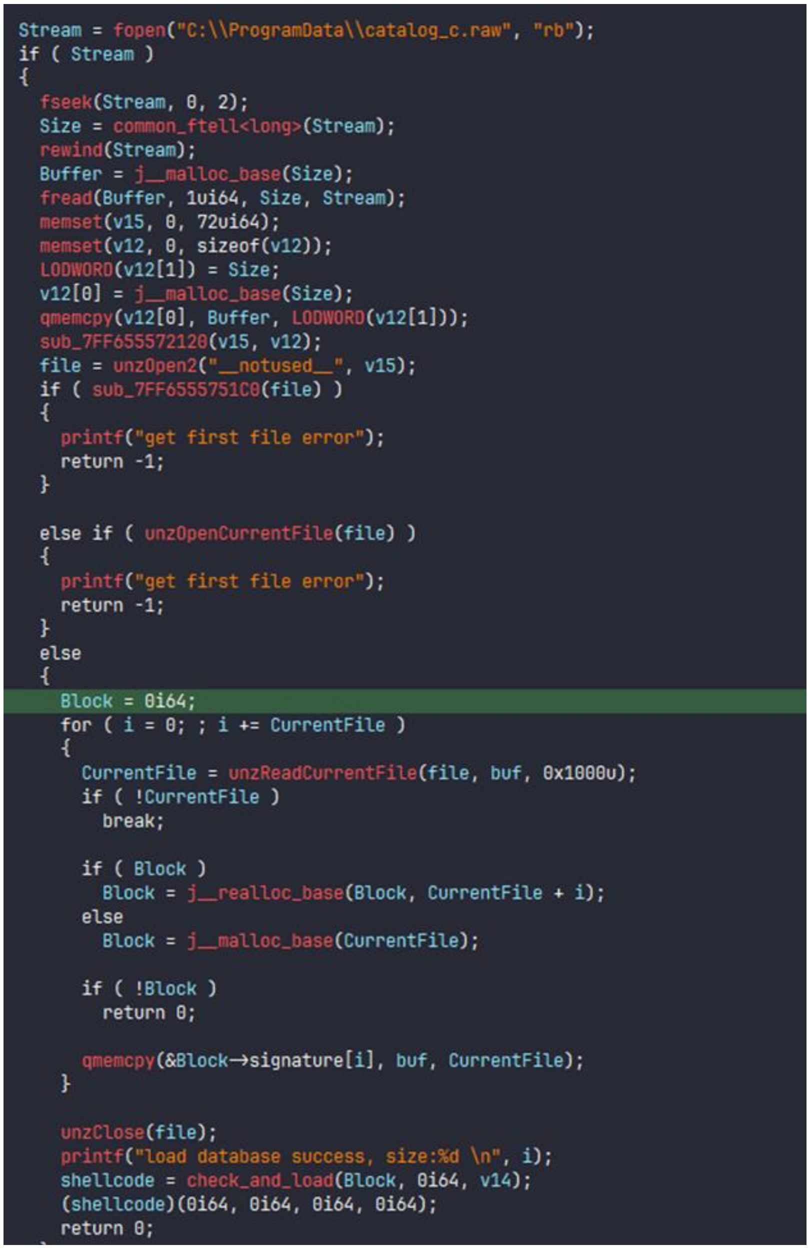
C&C of the malware is configured as shown in the image below.



```
; __int64 main_config_https
main_config_https dq offset aHttpsAnalysisM
                                        ; DATA XREF: main_config_init+1D5↑r
                                        ; "https://analysis.ms-azurelogs.com"
; __int64 qword_12AB988
```

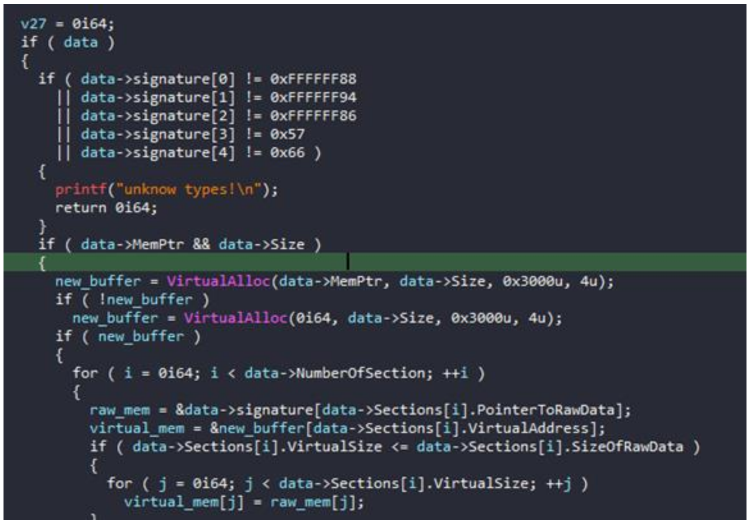
2. Sample 2: AutoUpdate.exe

When executed, the malware opens a file located at the path *C:\ProgramData\catalog_c.raw*. After opening it, the malware proceeds to read files within the catalog_c.raw using the minizip library.



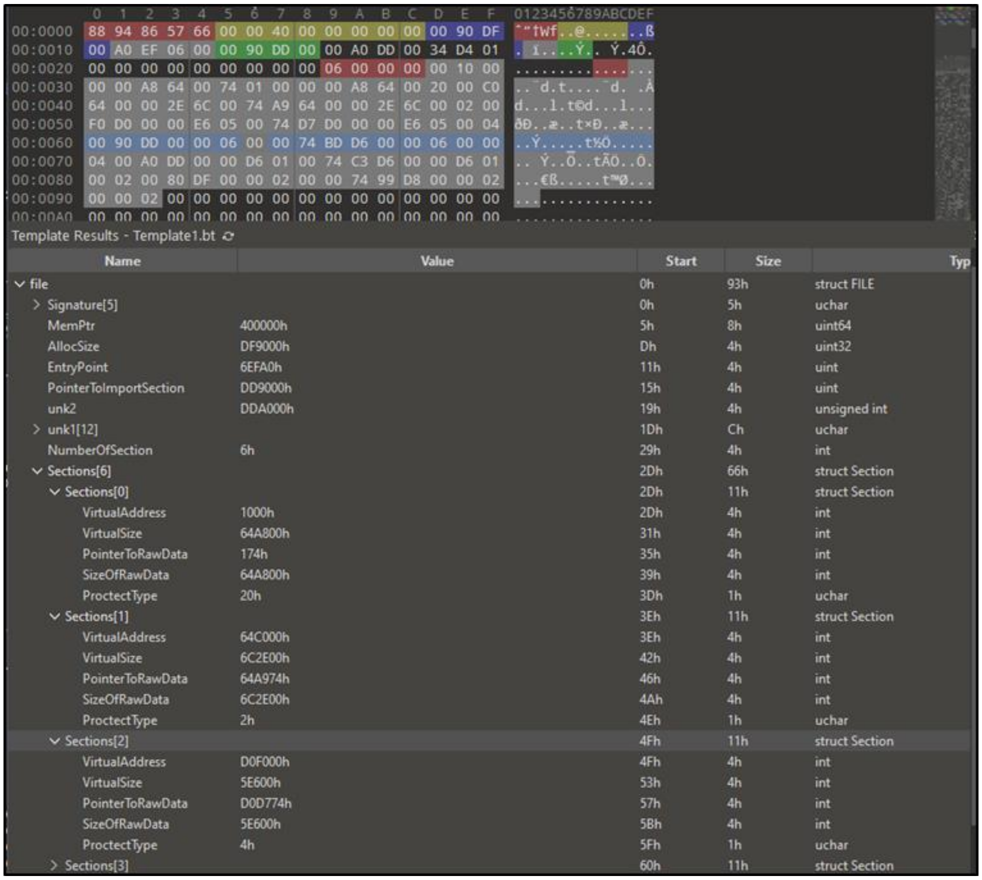
```
Stream = fopen("C:\\ProgramData\\catalog_c.raw", "rb");
if ( Stream )
{
  fseek(Stream, 0, 2);
  Size = common_ftell<long>(Stream);
  rewind(Stream);
  Buffer = j__malloc_base(Size);
  fread(Buffer, 1ui64, Size, Stream);
  memset(v15, 0, 72ui64);
  memset(v12, 0, sizeof(v12));
  LODWORD(v12[1]) = Size;
  v12[0] = j__malloc_base(Size);
  qmemcpy(v12[0], Buffer, LODWORD(v12[1]));
  sub_7FF655572120(v15, v12);
  file = unzOpen2("__notused__", v15);
  if ( sub_7FF6555751C0(file) )
  {
    printf("get first file error");
    return -1;
  }

  else if ( unzOpenCurrentFile(file) )
  {
    printf("get first file error");
    return -1;
  }
  else
  {
    Block = 0i64;
    for ( i = 0; ; i += CurrentFile )
    {
      CurrentFile = unzReadCurrentFile(file, buf, 0x1000u);
      if ( !CurrentFile )
        break;

      if ( Block )
        Block = j__realloc_base(Block, CurrentFile + i);
      else
        Block = j__malloc_base(CurrentFile);

      if ( !Block )
        return 0;

      qmemcpy(&Block->signature[i], buf, CurrentFile);
    }

    unzClose(file);
    printf("load database success, size:%d \n", i);
    shellcode = check_and_load(Block, 0i64, v14);
    (shellcode)(0i64, 0i64, 0i64, 0i64);
    return 0;
```

The malware reads the child files and examines the characteristics of each file. The child files are deleted PE files with a custom header. If the file starts with the byte string [0x88, 0x94, 0x86, 0x57, 0x66], the malware will then parse its new PE structure.



```
v27 = 0i64;
if ( data )
{
  if ( data->signature[0] != 0xFFFFFF88
    || data->signature[1] != 0xFFFFFF94
    || data->signature[2] != 0xFFFFFF86
    || data->signature[3] != 0x57
    || data->signature[4] != 0x66 )
  {
    printf("unknow types!\n");
    return 0i64;
  }
  if ( data->MemPtr && data->Size )
  {
    new_buffer = VirtualAlloc(data->MemPtr, data->Size, 0x3000u, 4u);
    if ( !new_buffer )
      new_buffer = VirtualAlloc(0i64, data->Size, 0x3000u, 4u);
    if ( new_buffer )
    {
      for ( i = 0i64; i < data->NumberOfSection; ++i )
      {
        raw_mem = &data->signature[data->Sections[i].PointerToRawData];
        virtual_mem = &new_buffer[data->Sections[i].VirtualAddress];
        if ( data->Sections[i].VirtualSize <= data->Sections[i].SizeOfRawData )
        {
          for ( j = 0i64; j < data->Sections[i].VirtualSize; ++j )
            virtual_mem[j] = raw_mem[j];
```

PE files with custom header are defined as below:

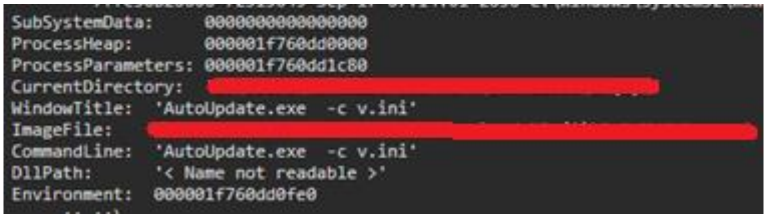


```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00:0000  88 94 86 57 66 00 00 40 00 00 00 00 00 00 90 DF  ˆ”†Wf..@.......ß
00:0010  00 A0 EF 06 00 00 90 DD 00 00 A0 DD 00 34 D4 01  . ï....Ý.. Ý.4Ô.
00:0020  00 00 00 00 00 00 00 00 00 06 00 00 00 00 10 00  ................
00:0030  00 00 A8 64 00 74 01 00 00 00 A8 64 00 20 00 C0  ..¨d.t....¨d. .À
00:0040  64 00 00 2E 6C 00 74 A9 64 00 00 2E 6C 00 02 00  d...l.t©d...l...
00:0050  F0 D0 00 00 E6 05 00 74 D7 D0 00 00 E6 05 00 04  ðÐ..æ..t×Ð..æ...
00:0060  00 90 DD 00 00 06 00 00 74 BD D6 00 00 06 00 00  ..Ý.....t½Ö.....
00:0070  04 00 A0 DD 00 00 D6 01 00 74 C3 D6 00 00 D6 01  .. Ý..Ö..tÃÖ..Ö.
00:0080  00 02 00 80 DF 00 00 02 00 00 74 99 D8 00 00 02  ...€ß.....t™Ø...
00:0090  00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00:00A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Template Results - Template1.bt

Name	Value	Start	Size	Typ
file		0h	93h	struct FILE
Signature[5]		0h	5h	uchar
MemPtr	400000h	5h	8h	uint64
AllocSize	DF9000h	Dh	4h	uint32
EntryPoint	6EFA0h	11h	4h	uint
PointerToImportSection	DD9000h	15h	4h	uint
unk2	DDA000h	19h	4h	unsigned int
unk1[12]		1Dh	Ch	uchar
NumberOfSection	6h	29h	4h	int
Sections[6]		2Dh	66h	struct Section
Sections[0]		2Dh	11h	struct Section
VirtualAddress	1000h	2Dh	4h	int
VirtualSize	64A800h	31h	4h	int
PointerToRawData	174h	35h	4h	int
SizeOfRawData	64A800h	39h	4h	int
ProctectType	20h	3Dh	1h	uchar
Sections[1]		3Eh	11h	struct Section
VirtualAddress	64C000h	3Eh	4h	int
VirtualSize	6C2E00h	42h	4h	int
PointerToRawData	64A974h	46h	4h	int
SizeOfRawData	6C2E00h	4Ah	4h	int
ProctectType	2h	4Eh	1h	uchar
Sections[2]		4Fh	11h	struct Section
VirtualAddress	D0F000h	4Fh	4h	int
VirtualSize	5E600h	53h	4h	int
PointerToRawData	D0D774h	57h	4h	int
SizeOfRawData	5E600h	5Bh	4h	int
ProctectType	4h	5Fh	1h	uchar
Sections[3]		60h	11h	struct Section

Based on the file’s characteristics, it can be observed that this PE file is the frp version v0.53.2 tool used for tunneling into the victim’s device. Upon inspecting dump file, the malware runs -c v.ini command to load its configuration.



```
SubSystemData:     0000000000000000
ProcessHeap:       000001f760dd0000
ProcessParameters: 000001f760dd1c80
CurrentDirectory:  [redacted]
WindowTitle:  'AutoUpdate.exe  -c v.ini'
ImageFile:    [redacted]
CommandLine:  'AutoUpdate.exe  -c v.ini'
DllPath:      '< Name not readable >'
Environment:  000001f760dd0fe0
```

3. Signs of recognition / Malware infrastructure

- AutoUpdate.exe

  - MD5: 07F85171FFA199899EC0B7136F164986

  - SHA1: D1E74FCE59CBA9B6C17858BF55C38FF0CFE4F5DD

  - SHA256:

  FC9A2144BB00FD79BBC820880EE0DFC6EB5C10D6BB2F86310AD9D3300144F1F5

- catalog_c.raw

  - MD5: C3DBEEB5B9339E62FA9300F4E3BBC89D

  - SHA1: A49F088E92BE96FAB3FAF0C47F51340700DC5DB2

  - SH256:

  36A2AEEE2E2544D8536CD425350EE49409E1C791C38001C45BF263FEB336CAC5

- version.dll:

  - MD5: AE9601C8A66D41828795A3F6CCE31B19

  - SHA1: 59FD6C36F7F1DF95E0E68B48351F947998C67C68

  - SHA256:

  B82A546F752766A78655A1BD80106EF8C701802B64CFC466D5053CBA51021943

- uninstall000.dat

  - MD5: DE33F0E9EDF04726396E802CBED71702

  - SHA1: CF0A88140A67C1986DCF485E965C933106419039

  - SHA256:

  7C3894E32774C8B61B8CC6A5DEDFF3B62B3DD1EF2544E10DCA2B17334398ECD0

Network IOCs:

• 54.180.143[.]194

• analysis.ms-azurelogs[.]com

4. Administrators can check for the following signs of abnormality

- **Unusual enabling or disabling of SSH on ESXi** *(Note: SSH is disabled by default)*

Check within the **shell.log file**:

```
norm_id="VmwareESX" label="Enable" label="SSH"
| chart count() by log_host,message
```

- **The hackers conduct Brute-force attack or SSH password-spraying on ESXi:**

Check within the “**/var/log/vobd.log” file**:

```
[label="SSH" label="Login" label="Fail"
| chart distinct_count(user) as user_count by log_host, source_address
| search user_count > 5] as s1 followed by
[label="Session" label="Open" label="SSH"] as s2 on
s1.source_address=s2.source_address
```

- **The hackers conduct web interface brute-force or ESXi unusual accounts.**

Check within the “**/var/log/hostd.log**” file if there are multiple unsuccessful login attempts followed by a successful login.

```
[10 label="Authentication" label="Fail" action="Rejected" having same source_address]
as s1 followed by
[label="Authentication" label="Successful" action="Accepted" ]
as s2 on s1.source_address=s2.source_address
```

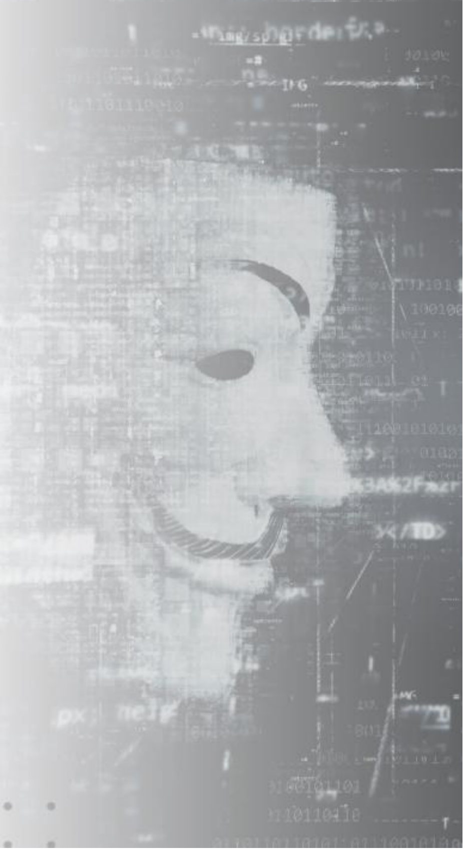
Additionally, administrators can also inspect the **"/var/log/auth.log"** file to check for suspicious login information (for example, multiple unsuccessful login attempts from the same IP address).

5. Malware response / Handling

Based on the IoCs, VCS-TI recommends our clients to perform the following tasks:

- Conduct a thorough review of malware within the organization.

- Update IoCs into your organization’s security solutions (SIEM, IPS/IDS, etc.).



Illuminate the Hidden Dangers

Shine a light on the darkest corners of the cyber world!

- **Proactive Identification:** Spot potential threats before they strike.
- **Comprehensive Scanning:** Leave no stone unturned with our extensive security scans.
- **Actionable Insights:** Equip yourself with the knowledge to fortify your defenses.

We commit to excellence

Best Cyber Security Company - Asia.

in 2022, 2023

(100-499 employees)

1. AI-driven Threat Intelligence Platform

By integrating with more than 50 appliances, our solutions optimize threat intelligence data under a single platform to match information with MITRE ATT&CK and IoCs, thereby proactively hunt early and relevant attack. We leverage Machine Learning and AI technology to priority threat aligned to organization’s security solutions (SIEM, SOAR, EDR) and gain deep insights of tactics, techniques and procedure.

2. Exclusive threat data

Collect **exclusive** data sources from Viettel - the 1st telecom operators of SEA and FIRST, APWG, Vietnam National Cyber Security Center, Vietnam Computer Emergency Response Team.

3. High accuracy and dedicated service

Strongly focused on actionable threat insights and value-added services. We commit MTTD, MTTR and 24/7 customer support to ensure our clients stay ahead of cyber threat.

viettel
security

VIETTEL THREAT INTELLIGENCE