Keep up with Ransomware

FOG ransomware targeting overseas educational institutions

■ Overview

A total of 415 ransomware damage cases were reported in July 2024, which increased by approximately 20% from the previous month (346 cases). LockBit, which had been slow in activity last month, posting 12 victims, increased its activity in July, posting 33 victims. They also published the contact information of the "Boss", who is believed to be the person in charge of contact, including the messenger ID and forum account, on their dark web leak site.

A recently released Wiper malware disguises itself as an update or the patch file for a technical issue in a specific security product, deleting users' data. On July 19, CrowdStrike, a cybersecurity technology company in the United States, performed an update to the Windows system sensor configuration in its next-generation endpoint security platform, Falcon, and it caused system crashes and blue screens, paralyzing the company's operations. Hacktivist[1] group Handala distributed a PDF file containing a description and instructions for the fake update, and included a download link for Wiper, disguised as an update file, to trick customers into downloading Wiper.

Brain Cipher group, which attacked Indonesia's national temporary data center, released the decryption key on their dark web leak site on July 3. After the successful attack on June 20, they reportedly negotiated with the Indonesian government and demanded a ransom of USD 8 million. According to the group, the motive for their attack was a financial, not political, penetration test, and they released the decryption keys voluntarily, not because of pressure from law enforcement agencies. They also mentioned that they will never release the decryption key without compensation in the future, and left their cryptocurrency wallet address, saying they will accept donations as a token of appreciation.

[1] Hacktivist: As a compound word of "hacker" and "activist," it refers to a hacking group that operates for political or social purposes.

The SEXi ransomware, which primarily targets VMware ESXi[2] servers, has been renamed to APT INC and continues its attacks. They were found attacking VMware ESXi environments using the leaked Babuk builder[3], and Windows environments using the LockBit 3.0 builder. In addition, several other groups are threatening the ESXi environment. Attackers were able to gain full administrator privileges by exploiting an authentication bypass vulnerability (CVE-2024-37085) in ESXi 8.0 U3, released on June 25. The ransomware groups known as Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest exploited this vulnerability to distribute Akira and BlackBasta ransomware.

IntelBroker performing in the hacking forum BreachForums has posted three articles offering to sell data from South Korean organizations. The names of the agencies were not specifically mentioned, but were listed as "Korean Policy Force," "Korean Government Agency," and "Korean Critical Government Agency". IntelBroker said the data it was selling included access to the admin portal, important documents, etc., but it declined to release the sample by reason that it would lead to the release of immediate security patches.

Avast, a Czech cybersecurity software company, has released a decryption tool that exploits a key reuse vulnerability in the DoNex ransomware. Avast began supporting victims privately in March, and released a decryption tool in July as no further activity of DoNex ransomware was detected. The DoNex Ransomware group has rebranded several times. It started out as Muse Ransomware in April 2022, used fake LockBit 3.0 in November 2022, and then renamed to DarkRace in May 2023. It was rebranded as DoNex Ransomware in March 2024, but no further activity has been observed since the five victim postings, and even the dark web leak site was deactivated in April.

[2] ESXi: This UNIX-based logical platform developed by VMware can run multiple operating systems simultaneously on a host computer.

[3] Builder: A ransomware production tool that allows you to produce ransomware with desired features through environment settings

Ransomware News

infosec

Malware distribution disguised as a CrowdStrike patch or update

- System crashes and blue screens from a July 19 CrowdStrike update
- Distributing malware disguised as an update or patch in documents
- Hacktivist Handala distributed Wiper by including a download link in a PDF file

BrainCipher released decryption keys on a dark web leak site

- Decryption keys for the Indonesia national temporary data center attacked on June 20
- Claimed the attack was not politically motivated but rather a penetration test for monetary compensation
- Claimed the decryption keys were released voluntarily this time, not due to external pressure

Posted three listings for Korean agencies data on the hacking forum BreachForums

- IntelBroker, active on BreachForums, posted three listings for Korean agencies data
- The institutions are "Korean Policy Force", "Korean Government Agency", "Korean Critical Government Agency"
- No sample data was released separately, claiming it was blocked and is no longer accessible

LockBit published their contact information on a dark web site

- Released various messenger IDs and hacking forum profiled of the contact person 'boss'
- Requesting a single, concise message to convey the key information
- Published information: Tox ID, XMPP, Briar ID, Ramp forum profile, Telegram ID, and Signal ID

Ransomware group exploiting VMware ESXi vulnerability(CVE-2024-37085)

- Authentication bypass in ESXi 8.0 U3, revealed on June 25, allows full admin access to the virtual environment
- Exploiting the vulnerability requires high privileges, but multiple groups have already done so
- Storm-0506, Storm-1755, Octo Tempest and Manatee Tempest have been used to deploy Akira/BlackBasta

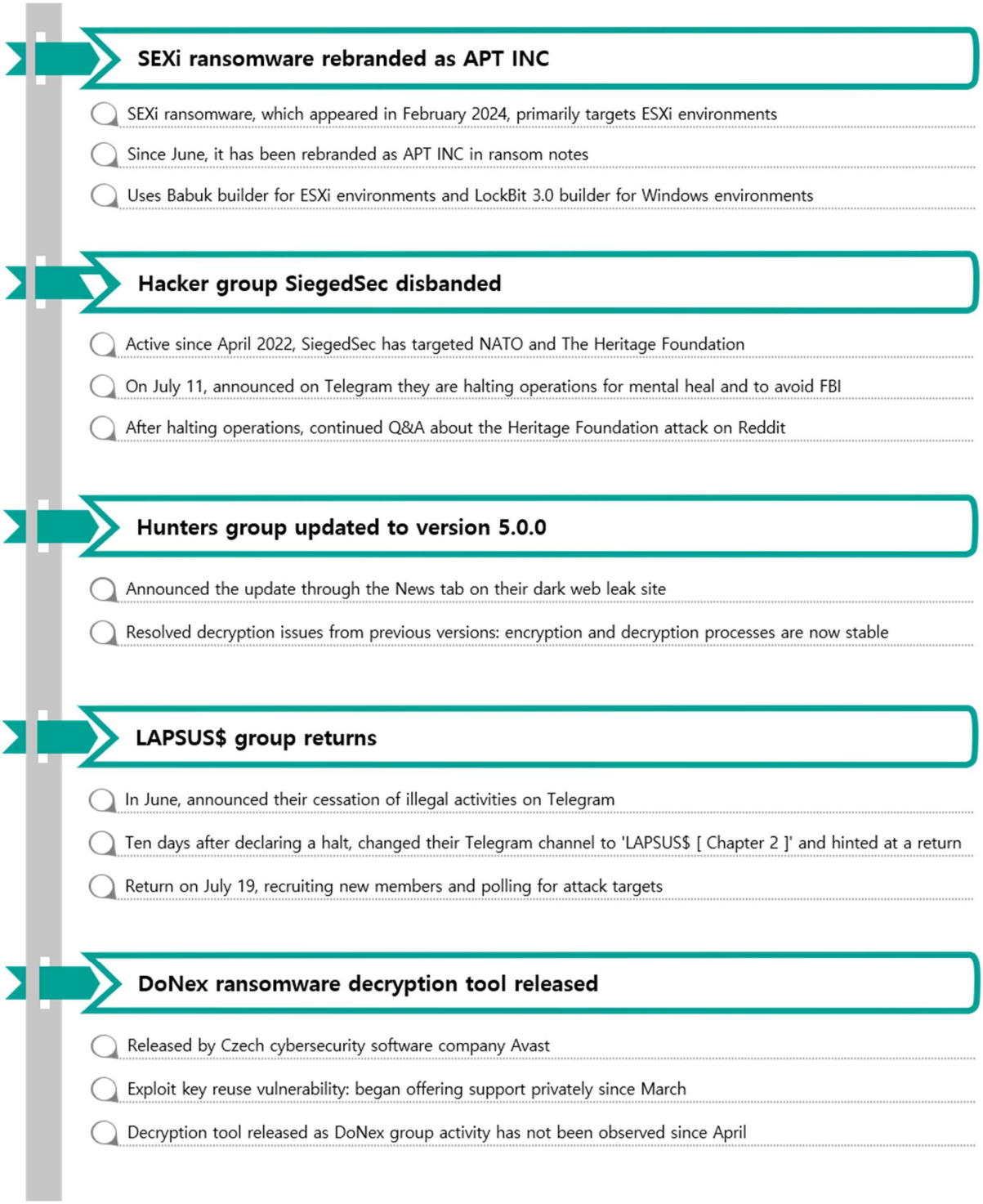


Figure 1. Ransomware Trend

■ Ransomware Threats

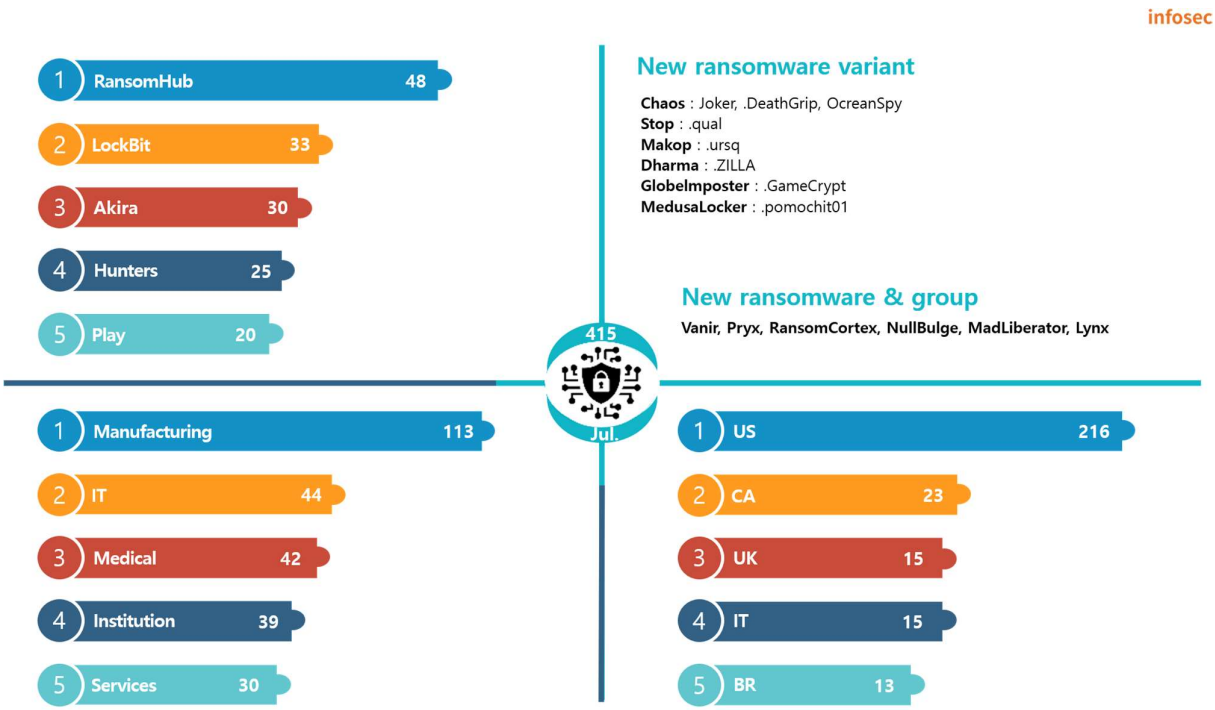


Figure 2. Ransomware Threats as of Jul. 2024

New threats

In July, several new ransomware groups emerged, and some groups resumed their activities. The LAPSUS$ group, which announced its inactivity through the Telegram channel in June, has returned after a month and is continuing its activities by recruiting new members and holding a vote on its next attack target.

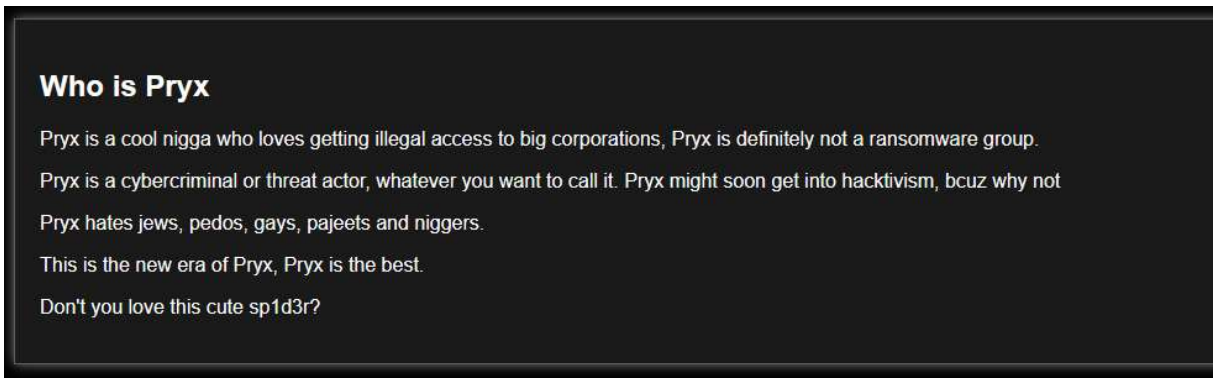


Figure 3. Introduction of Pryx group

Pryx group, which emerged in July, has posted two victims. They stated on the dark web leak site that they are not a ransomware group and could become hacktivists. They set up a page on the dark web leak site for comments, and in addition to posting about data leaks, they also made politically-motivated posts about the Arab Spring and the 2023 violent protests in France. This makes them appear to be more of a hacktivist operation with social and political objectives than ransomware as they have stated.

Figure 4. Dark web leak sites (Top: Vanir, Bottom: Akira)

Vanir ransomware uses a similar command shell design to that of the Akira ransomware group on its dark web leak site, and the way it navigates to other pages by entering commands is also very similar. So far, they have listed a total of three victims, and have also posted on dark web leak sites recruiting partners.

Madliberator Group posted eight victims in July alone. Although the number of victims was not large, the group posted victims across a wide range of industries, including manufacturing, finance, institutions, healthcare, and distribution. In addition, the new Lynx group has posted two victims, while hacktivist NullBulge has released Discord data from Indian YouTuber ChiefShifter and 1.2TB of internal collaboration tool data from American media conglomerate Disney.

Figure 5. Darkweb leak site of RansomCortex

Lastly, a new ransomware group, RansomCortex, which appeared on July 11, announced 4 victims related to the healthcare industry upon its appearance. However, as of August 1, all data were deleted from the dark web leak site, the site's title was changed to "Offline," and no additional activity was discovered.

Top 5 Ransomware

Figure 6. Major Ransomware Attacks by Industry/Country

RansomHub Group has been very active, posting 48 incidents in July alone, which accounts for 32% of the total activity. Since the BlackCat/Alphv's Exit Scam[4] in March, BlackCat (Alphv) partners have joined RansomHub, and activity has been steadily increasing since March. In June, they attacked a local architectural firm and, in July, the Florida Department of Health. In July, a new version of the ransomware was discovered with some additional features. A detailed analysis of RansomHub can be found in SK Shielders' 2024 Q2 Ransomware Trend Report, "KARA Ransomware Trend Report 2024 2Q."

[4] Exit Scam: A scam where the attacker does not pay fees to the affiliate or disappears without recovering the files after receiving payment from the ransomware victim

LockBit Ransomware group recorded a relatively low number of 12 victims last month, but increased its activity again in July, posting 33 victims. In July, however, two people involved in the LockBit Ransomware attacks pleaded guilty, and the dark web leak site remains unsettled, being intermittently inaccessible or frequently displaying test posts.

Akira Group has been active since April 2023, and in July, it was found to exploit CVE-2024-37085, a VMware ESXi authentication bypass vulnerability. This month, they attacked Canadian Federated Co-operatives Limited, causing problems in food inventory and card lockouts, which also affected operations of federated members' retail stores. They also attacked financial institution Financoop to steal around 20GB of financial information and internal data, and Heidmar, a crude oil and refined petroleum transportation services company.

Hunters Ransomware group has announced on its dark web leak site that their encryption and decryption tool was updated to version 5.0.0. This version reportedly has solved all issues of previous versions, allowing smoother encryption and decryption processing. They attacked Northeast Rehabilitation Hospital Network, an American rehabilitation medical services provider, and stole approximately 410 GB of hospital operational data and patient information. They also attacked Kenya Urban Roads Authority, an urban road authority of Keny, stealing approximately 18GB of data including personally identifiable information, financial documents, and customer data.

Play Ransomware Group has been focusing 61% of all attacks on the US-based businesses during its active period. Especially In July, all of their attacks targeted the US businesses. A ransomware variant that encrypts VMware ESXi environments in Linux environments has been discovered recently. This variant could allow attackers to corrupt VM disks or configuration files, or encrypt virtual machine files, and could affect more platforms than before.

■ Ransomware in focus

Overview of FOG Ransomware

Source: FOG ransomware data leak site

For FOG ransomware, which has been detected since May 2024, no dark web leak site was identified in the early stages of the activity. They negotiated with victims on dark web chat pages listed in the ransomnotes. However, on July 17, a dark web leak site was discovered where seven victims were posted, and four additional victims were later posted, bringing the total of 11 victims.

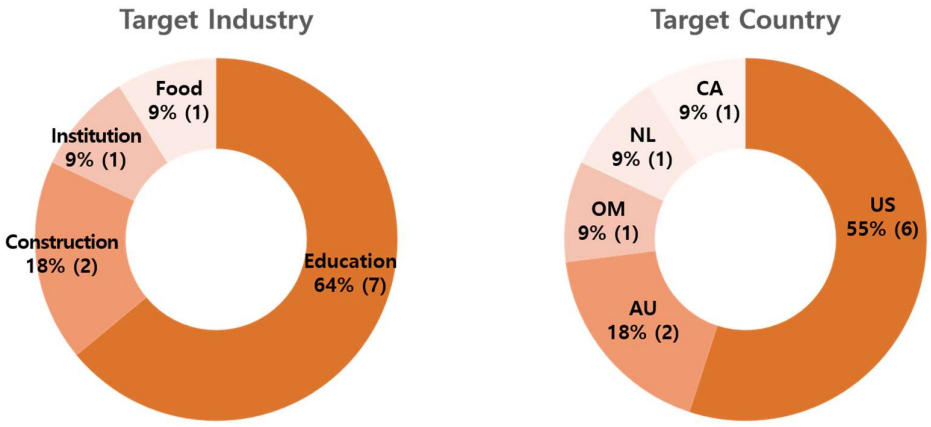


Figure 7. Statistics on FOG ransomware attacks

Most of the victims listed on the dark web leak site were educational institutions. 7 out of the 11 victims were educational institutions, including Geelong Lutheran University in Australia, German University of Technology in Oman, University of Texas at Odessa in the United States, and the Wichita State University of Applied Science and Technology Campus in the United States, as well as school districts in some areas of the United States.

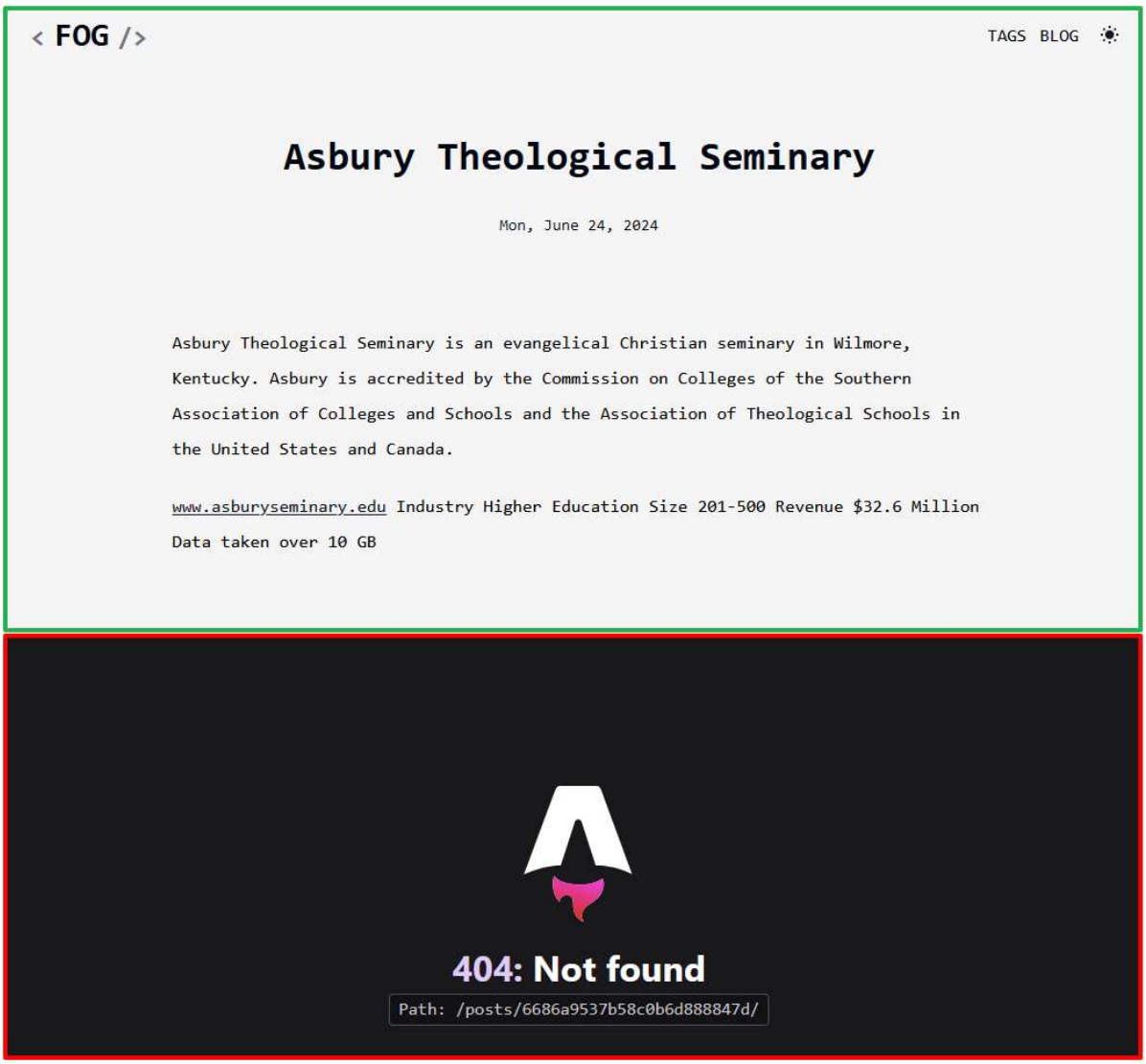


Figure 8. Posts on the FOG ransomware data leak site (Top: readable post, Bottom: unreadable post)

FOG ransomware has been consistently posting victims on dark web leak sites since July 17, but most of the posts are unreadable. As of July 30, 1 of 11 posts has been deleted, only 2 posts are readable, and the remaining 8 posts are redirected to an error page stating that the page does not exist. In addition, there are no sample data or public data in the two normally accessible posts. The fact that dark web leak sites are not operating smoothly could indicate several possibilities, including poor management or posts being edited only when negotiations on the chat page break down, and therefore requires continued monitoring.

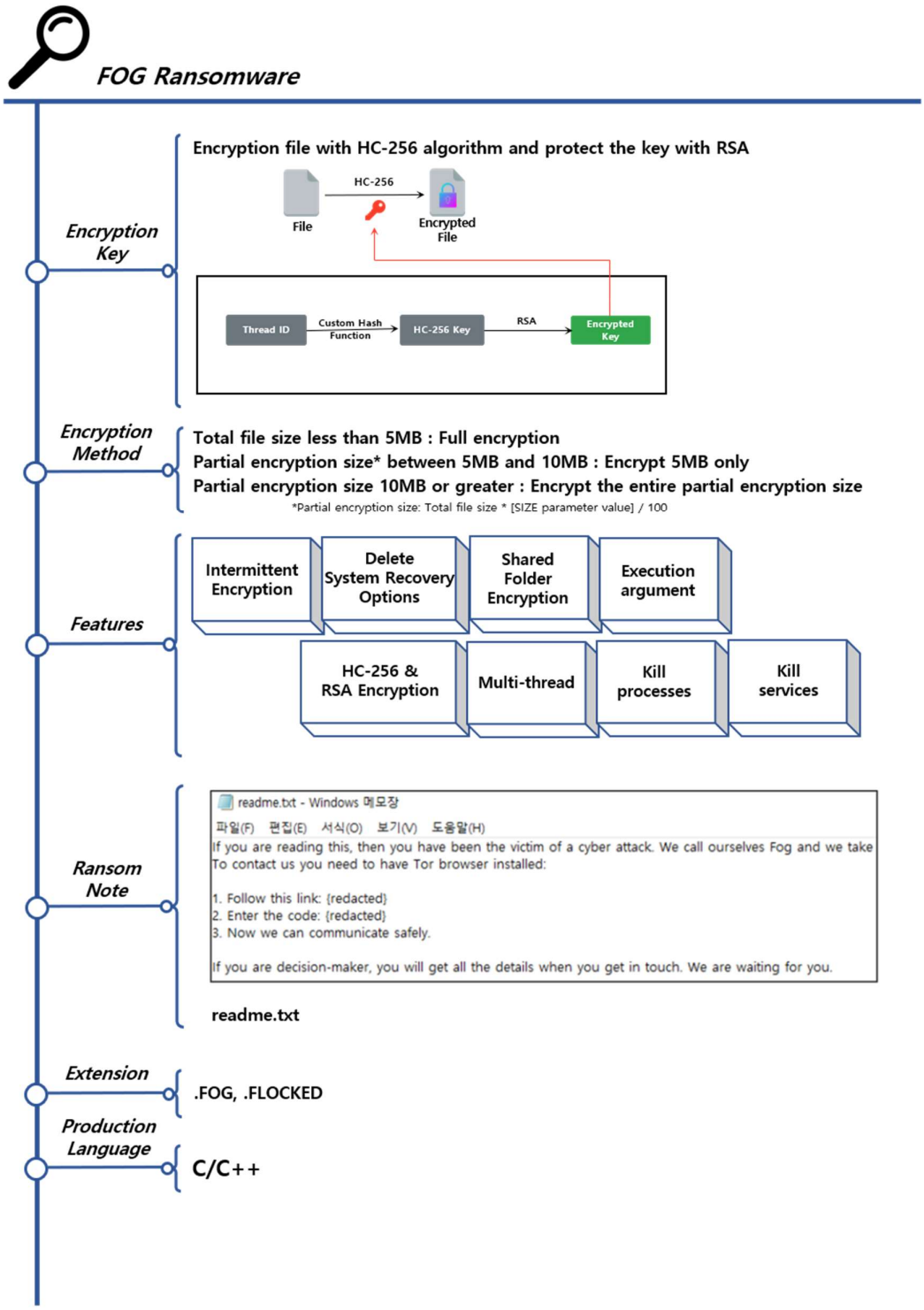


Figure 9. Overview of FOG ransomware

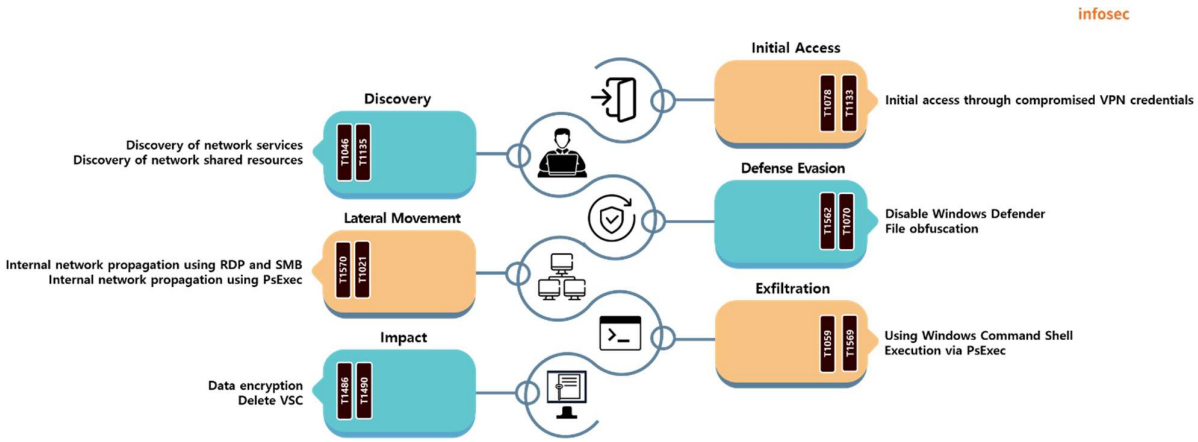


Figure 10. Attack strategies of FOG ransomware

FOG ransomware exploits compromised VPN[5] credentials to infiltrate victims' networks. After initial penetration, they scan the target system for network services and disable Windows Defender to prevent further malicious activity from being detected. They then use RDP[6] and SMB[7] in an attempt for internal spreading across the identified internal networks, and use PsExec[8] to distribute and execute payloads[9]. The deployed payload includes a PowerShell script that, in the Hyper-V[10] environments, encrypts VMDK[11] files and deletes Veeam[12] storage backups, as well as ransomware payloads that encrypt local system and network shared resources.

FOG ransomware can be executed by receiving multiple execution arguments. It works normally when the key value to decrypt the settings required for ransomware execution, such as the RSA public key, encryption exception targets and the list of processes and services for termination, is delivered as the "-ID" argument. In addition, execution arguments that can activate or deactivate various functions are shown in the table below.

[5] VPN(Virtual Private Network): A virtual secure network used to protect personal information and bypass regional restrictions on the Internet

[6] RDP(Remote Desktop Protocol): A protocol that allows you to control other computers remotely

[7] SMB(Server Message Block): A message format used to share files, directories, and peripherals in a Windows environment

[8] PsExec: A command-line tool that allows you to run processes remotely without installing specific software on other systems

[9] Payload: Code designed to penetrate, modify, or otherwise damage computer systems

[10] Hyper-V: A virtualization tool that allows you to run multiple operating systems in a Windows environment

[11] VMDK(Virtual Machine Disk): Virtual hard disk drives used in virtual environments

[12] Veeam: Backup app that can be used in Microsoft Hyper-V virtual environments, a virtualization tool for Windows operating system

Argument	Description
-NOMUTEX	Deactivate mutex[13] creation function
-LOG	Save ransomware startup log in C:₩ProgramData₩lock_log.txt
-TARGET {PATH}	Encrypt files in the specified path only
-ID {KEY}	Key required to decrypt various settings used by ransomware
-CONSOLE	Create a console window that outputs file encryption logs
-PROCOFF	Deactivate process termination function
-UNCOFF	Deactivate network shared resource encryption function
-SIZE {INT}	Percentage of the files to be encrypted ({int}%, default: 15)

Table 1. FOG ransomware execution arguments

FOG ransomware creates log files for debugging[14] purposes. Depending on the execution arguments, it can create two additional logs. When executed the ransomware saves logs used for debugging purposes, such as start and end messages for each function, execution results, and error messages, in the "C:₩ProgramData₩DbgLog.sys" path. In addition, the "-LOG" argument saves a log file containing the ransomware start time in the path "C:₩ProgramData₩lock_log.txt," and the "-CONSOLE" argument, when entered, outputs the names of the files being encrypted in a separate console window during the file encryption process, enabling to check which files are currently being encrypted.

```
2024-07-26 오전 10:28:11 [+] Defined mutex name: jBgB4ZHxUhNdJL9mz61WFXxI0GUXPAxw
2024-07-26 오전 10:28:11 [=] Decrypting json config
2024-07-26 오전 10:28:11 [=] Checking mutex...
2024-07-26 오전 10:28:11 [!] Skip mutex check by -nomutex param.
2024-07-26 오전 10:28:24 [+] JSON config loaded successfully
2024-07-26 오전 10:28:24 [=] Init prgn data...
2024-07-26 오전 10:28:25 Found disk # 1 (C:\), type: 1
2024-07-26 오전 10:28:25 Uknonwn DrvType (5) of root: D:\, skipped
2024-07-26 오전 10:28:25 [=] thread 14168 created
2024-07-26 오전 10:28:25 [=] thread 9100 created
2024-07-26 오전 10:28:25 [=] thread 5324 created
```

Figure11. DbgLog.sys log

The FOG ransomware has the setting values for execution encrypted. It uses a custom hash algorithm to create a 512-bit key from the value passed with the execution argument "-ID", and then decrypts the setting value using the HC-256 algorithm. The decrypted setting values are stored in the heap memory field, and the ransomware is executed without being terminated only if it is decrypted normally. The role of each setting value used by the FOG ransomware is shown in the table below.

[13] Mutex: A technique to prevents multiple threads from accessing a single resource simultaneously in multi-threads

[14] Debugging: The process of finding and correcting system errors that occur during development of the program

Setting values	Description
PathStopList	Encryption exception directory
FileMaskStopList	Encryption exception file extension
ShutdownProcesses	List of targets of process shutdown
ShutdownServices	List of targets for service shutdown
RSAPubKey	RSA public key used to protect file encryption keys
LockedExt	Encryption file change extension
NoteFileName	Ransomnote file name
NoteFileContents	Contents of ransomnote

Table 2. Setting values of FOG ransomware

Before file encryption, all processes and services are shut down. The targets of shutdown are on the "ShutdownProcesses" and "ShutdownServices" lists among the decrypted setting values. When the "-PROCOFF" argument is entered, file encryption begins immediately, skipping process and service shutdown before encryption. File encryption basically scans both local drives and network shared resources, and encrypts all files except those in encryption exception directories and with exception extensions. When running the ransomware, network shared resources can be kept not encrypted by using the "-UNCOFF" argument. Also, using the "-Target" argument, only the paths entered with the argument, not the entire drive, are encrypted.

File encryption determines whether to partially encrypt a file based on the file size and the "-SIZE" argument value. It calculates the entered "-SIZE" value as a percentage (%) of the total file size, and uses it as the partial encryption size. For example, when "-SIZE 20" is entered, 20% of the total file size is used as the partial encryption size. If the file is less than 5MB, the entire file is encrypted and, otherwise, partial encryption is applied. The method of partial encryption also differs according to size. If the previously calculated partial encryption size is 5 MB or more but less than 10 MB, only 5 MB of the file is encrypted. If it is 10 MB or more, encryption is performed for the calculated partial encryption size. File encryption is performed using the HC-256 algorithm, and the key used for encryption is protected using the RSA public key stored in the settings value.

In addition, Windows commands are used to delete both disk backup copies and the recycle bin data to prevent arbitrary recovery by users.

Measures against FOG ransomware

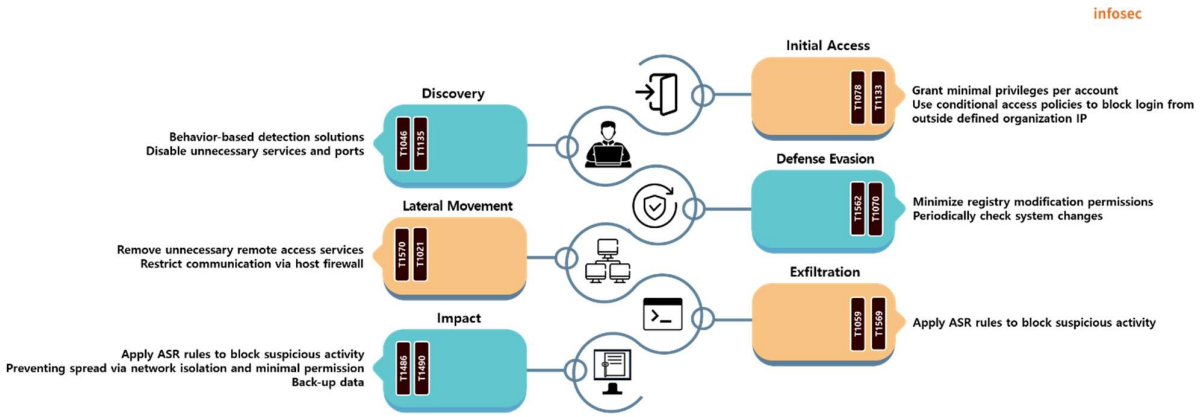


Figure 12. Measures against FOG ransomware

FOG ransomware uses compromised VPN credentials for initial infiltration. To prevent this, only the minimal privileges must be granted to each account or a deactivation conditional access policy to restrict logging in from non-compliant devices or external IPs must be used. Management activities, such as deactivating or blocking unnecessary services among remotely available services, periodically checking and auditing accounts, and deactivating or restricting unnecessary accounts, must also be performed

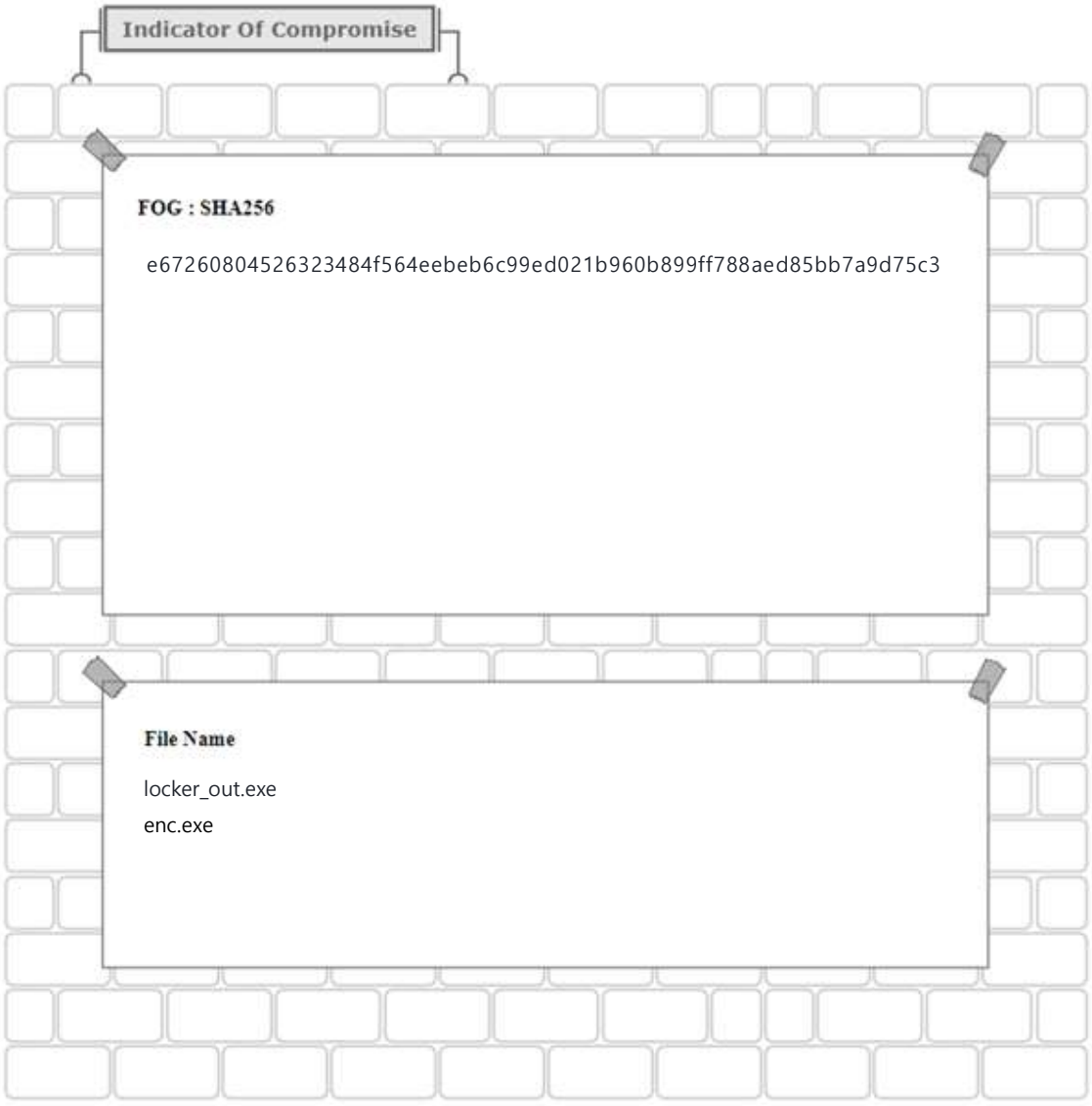
After initial penetration using VPN, FOG will search for shared resources or various network services to further spread into the internal network. To limit the users who can enumerate network shared resources, the Windows Group Policy needs to be modified. In addition, unnecessary services or ports can be deactivated in advance to prevent them from being discovered. Also, since attackers use SMB, RDP, PsExec, etc. for internal propagation, a host firewall can be used to limit abnormal communications.

FOG deploys PowerShell scripts and ransomware payloads to compromise VM environments into the internal network it infiltrates. This can be prevented by activating the ASR[15] rules or using an EDR[16] solution to block malicious activity.

FOG ransomware encrypts not only local disks but also network shared files. Therefore, the access to the network shared resources must be kept to a minimum or disabled to prevent access to external resources. Additionally, ransomware has the ability to delete backup copies to prevent users from recovering them, so the data must be backed up in a separate network or storage.

[15] ASR (Attack Surface Reduction): Protection against processes that are being used or executable by attackers

[16] EDR (Endpoint Detection and Response): A solution that detects, analyzes, and responds to malicious activities occurring on computers, mobile devices or servers in real time to prevent it from spreading damage


Indicator Of Compromise
FOG : SHA256
e672608045263234 84f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3
File Name
locker_out.exe
enc.exe

■ Reference sites

• TrendMicro's official website (https://www.trendmicro.com/en_us/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html

• Trellix's official website (https://www.trellix.com/blogs/research/akira-ransomware/)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/fake-crowdstrike-fixes-target-companies-with-malware-data-wipers/)

• Avast's official blog (https://decoded.avast.io/threatresearch/decrypted-donex-ransomware-and-its-predecessors/)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/meet-brain-cipher-the-new-ransomware-behind-indonesia-data-center-attack/)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/new-fog-ransomware-targets-us-education-sector-via-breached-vpns/)

• Microsoft's official website (https://www.microsoft.com/en-us/security/blog/2024/07/29

/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/sexi-ransomware-rebrands-to-apt-inc-continues-vmware-esxi-attacks/)

• CrowdStrike's official website (https://www.crowdstrike.com/statement-on-falcon-content-update-for-windows-hosts-kr/)