Keep up with Ransomware

Qilin Ransomware Attack on the UK Medical Service

■ Overview

The number of ransomware damage cases in June 2024 was 346, which decreased by approximately 40% from the previous month (568 cases). This is because LockBit ransomware group displayed an active performance by posting 172 ransomware damage cases, which account for 30% of all damage cases, in May, but the number of cases posted in June decreased drastically to 12.

The Operation Cronos[1] is analyzed to be the main cause for the decreased activities of LockBit. As part of the Operation Cronos, the National Crime Agency (NCA) of the U.K. revealed the identity of, and prosecuted "LockBitSupp" who is presumed to be the LockBit administrator on May 6. Following the Operation Cronos, LockBit showed off its undiminished power by posting over 100 victims. However, its activity reduced rapidly in June.

In addition, LockBit is showing instability in its operation, such as to upload testing posts several times recently in the dark web leak site and frequently losing connections to the leak site. By these reasons, speculation is raised that LockBit has stopped its activities altogether or is preparing for rebranding.

In fact, LockBit resumed its activity by posting victims on the dark web leak site on June 22. Nevertheless, the Federal Reserve[2] data it had posted was found to be the data of Evolve Bank & Trust, a financial company. Moreover, with the dark web leak site connections being continuously unstable, the influence of LockBit is decreasing considerably.

[1] Operation Cronos: Cyber disruption operation to destroy the criminal ecosystem of LockBit, such as attack servers and dark web leak sites

[2] Federal Reserve: Central bank of the U.S. and board of directors leading each Federal Reserve Bank as an organization independent from the Federal Government

IntelBroker, which sells access privileges and stolen data on BreachForums, a hacking forum, posted the data of several famous enterprises including the U.S. semiconductor company AMD and electronics manufacturer Apple. In addition to information about AMD's new product scheduled for release as well as the company's financial statements, personal information of employees and internal source codes, the data included the source codes of three software products internally used by Apple, which are 'AppleConnect-SSO'[3], 'Apple-HWE-Confluence-advanced'[4] and 'AppleMacroPlugin'[5]. IntelBroker also caused controversy by selling the source codes of T-Mobile, a German mobile carrier, aircraft data of the U.S. Army Air Corps and the U.S. Army Strategic Missile Command, AWS[6] information of CBRE, a global U.S. real estate company, and zero-day vulnerability[7] of the issue tracking program Jira of an information and software development company, Atlassian.

Ransomware threats using the latest vulnerabilities continued in June. For the recently detected BlackBasta ransomware, a function to attempt privilege elevation through CVE-2024-26169[8], a Windows vulnerability found in March, was identified. As for the TellYouThePass ransomware, its use in an attack by uploading the web shell[9] with CVE-2024-4577 CVE-2024-4577[10] vulnerability, which occurs in Windows PHP server and was detected in June, was identified. The continued occurrence of ransomware attacks using the latest and unpatched vulnerabilities calls for particular attention.

[3] AppleConnect-SSO: SSO and authentication system dedicated to Apple that enable access to specific application programs inside the network

[4] Apple-HWE-Confluence-advanced: Software used in Apple's internal information sharing

[5] AppleMacroPlugin: A set of tools facilitating Apple's internal process

[6] AWS: Cloud computing service provided by Amazon

[7] Zero-day Vulnerability: Vulnerability for which a patch is not available

[8] CVE-2024-26169: Privilege elevation vulnerability generated in Windows error report service

[9] Web Shell: Script file to execute various commands for the respective web server on a web page

[10] CVE-2024-4577: Remote code execution vulnerability generated when PHP is run in CGI mode in Windows environment

On June 3, Synnovis, a pathological and medical service company of the U.K., was attacked by Qilin ransomware group and it caused paralysis in some of the company's services. The attack also resulted in a setback in clinical services like blood test and, consequently, patients' treatment and surgery schedules were postponed or canceled. Disrupting blood classification as well, it even led to the shortage of blood in specific blood types. Qilin posted a notification of data disclosure in the dark web leak site on June 19 and, two days later on the 21st, it disclosed medical data and patients' personal data to a scale of approximately 400GB through its Telegram channel.

Ransomware News

infosec

Qilin attacks Synnovis, causing medical service disruptions at several hospital in the UK.

- On June 3rd, pathology service provider Synnovis was hit by ransomware, disrupting medical service.
- Blood testing and typing disruptions at Synnovis led to treatment and surgery delays in the UK hospitals.
- On June 21st, Qilin release 400GB of medical and patient data via their Telegram channel.
- Qilin claims they attacked because the UK did not assist in a particular war.

LockBit claims responsibility for attacking the US Federal Reserve.

- On June 24th, LockBit Posted on DLS* claiming they stole 33TB of data from the US Federal Reserve.
- There is no sample data, criticized for saying "Fire this clinical idiot who values Americans' bank secrecy at $50K."
- The data disclosed on June 26th belongs to another bank, 'Evolve Bank & Trust', not the US Federal Reserve.

* DLS(Dedicated Leak Site): A site posting data of victims who refused to pay ransom

IntelBroker posts data from AMD, Apple, and other major companies on Hacking Forums.

- IntelBroker, affiliated with the cybercrime group CyberNigger, posted stolen data on the BreachForums.
- Includes AMD's upcoming production info, financials, employee info, and Apple's internal software source code.
- Also posted data from T-Mobile, US Army Aviation and Missile Command, CBRE, and various vulnerability sales.

Restoration of the hacking forum BreachForums.

- After being seized by the FBI and DOJ* in May, BreachForums recovered but suffered another outage on June 10th.
- "ShinyHunters" Telegram account and BF's chat channel Jacuzzi 2.0 suspended, multiple sanctions confirmed.
- On June 13th, BF restored with "ShinyHunters" transferring authority to "Anastasia" before retiring.

* DOJ(Department of Justice): The U.S. Department of Justice, the federal law enforcement agency

BlackBasta suspected of exploiting Windows zero-day vulnerability.

- Malware using CVE-2024-26169, a privilege escalation flaw in Windows Error Reporting service, found in March.
- Similar tactics, techniques, and procedures to BlackBasta, attempting ransomware payload* distribution.
- The malware was created before the vulnerability was discovered on Feb 27, 2024, and Dec 18, 2023.

* payload: Code designed to infiltrate, alter, or otherwise damage computer systems

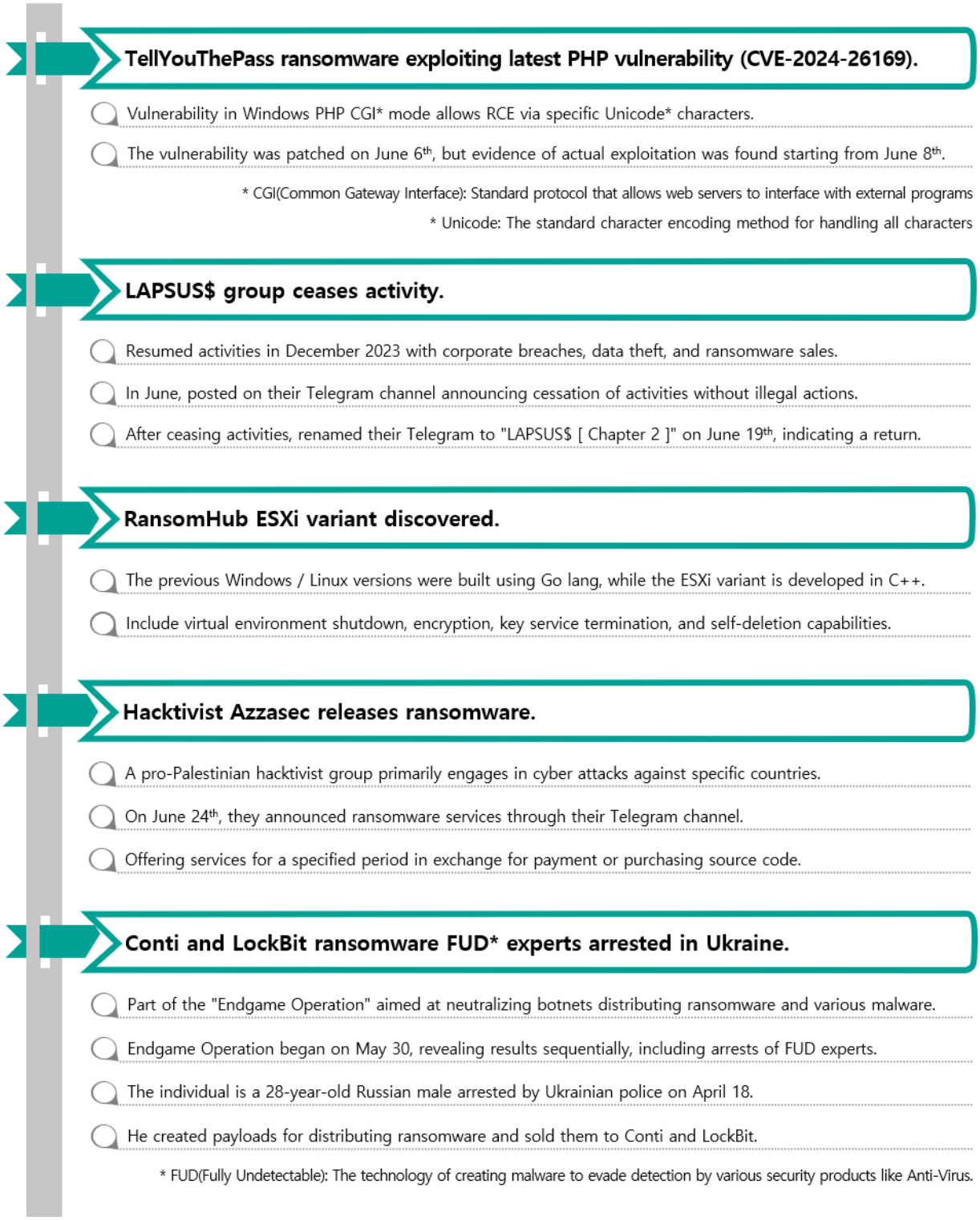


Figure 1. Ransomware Trend

Ransomware Threats

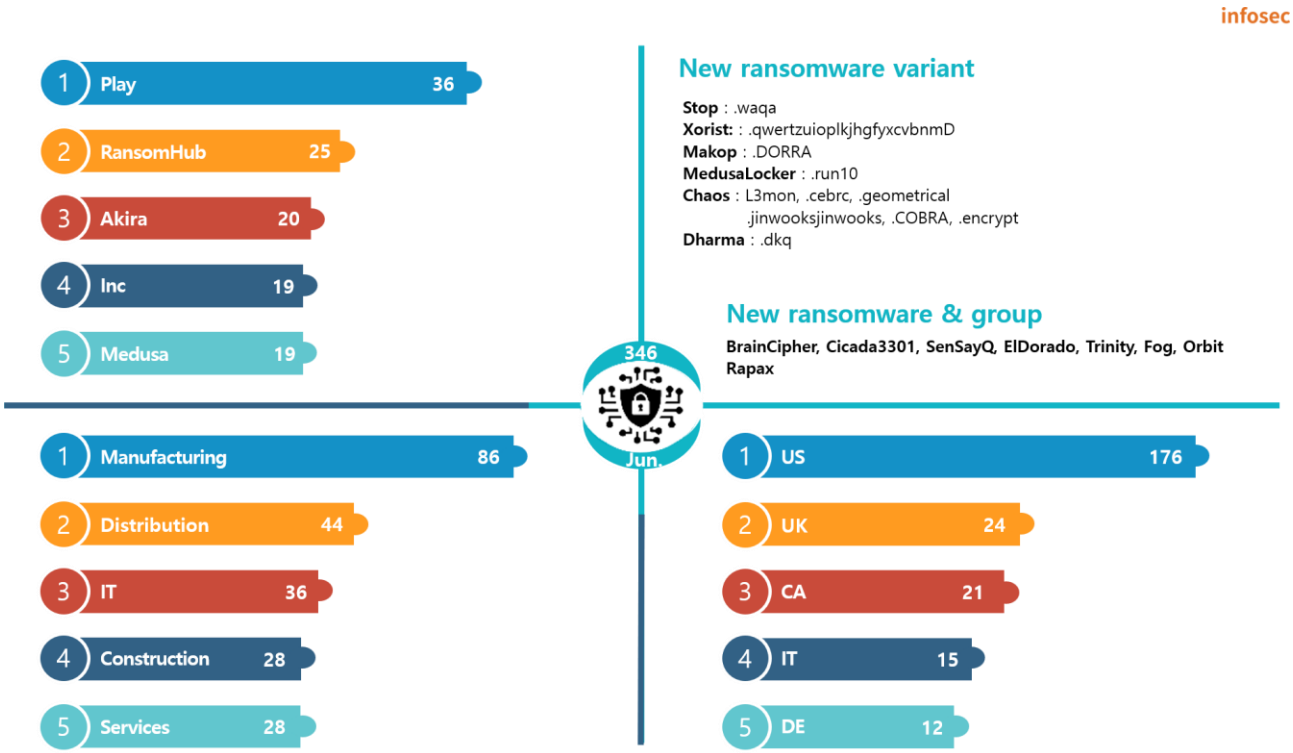


Figure 2 Ransomware Threats as of June 2024

New Threats

In June, a number of new ransomware groups appeared. A majority of them are double-threat ransomware groups that make threats by posting data on their leak sites. However, some were found to have only a chat page without the dark web leak site. A variety of other ransomware threats, such as to sell ransomware service through the dark web forum or their Telegram channels or recruit new partners, are continuously occurring.

Fog group provides a chat page address and the ID for login following a ransomware attack. When a victim logs in to the page using the given ID, it negotiates with the victim. The leak site of Fog group has not yet been identified. However, as it wrote the major data snatch in ransom note, it can always use the double-threat strategy. In May alone, Fog ransomware attacked four educational and one recreational facilities in the U.S. It was found to have distributed ransomware by penetrating networks using the damaged VPN[11] credentials.

[11] VPN (Virtual Private Network): Virtual security network used to protect personal information on the Internet and bypass regional restrictions

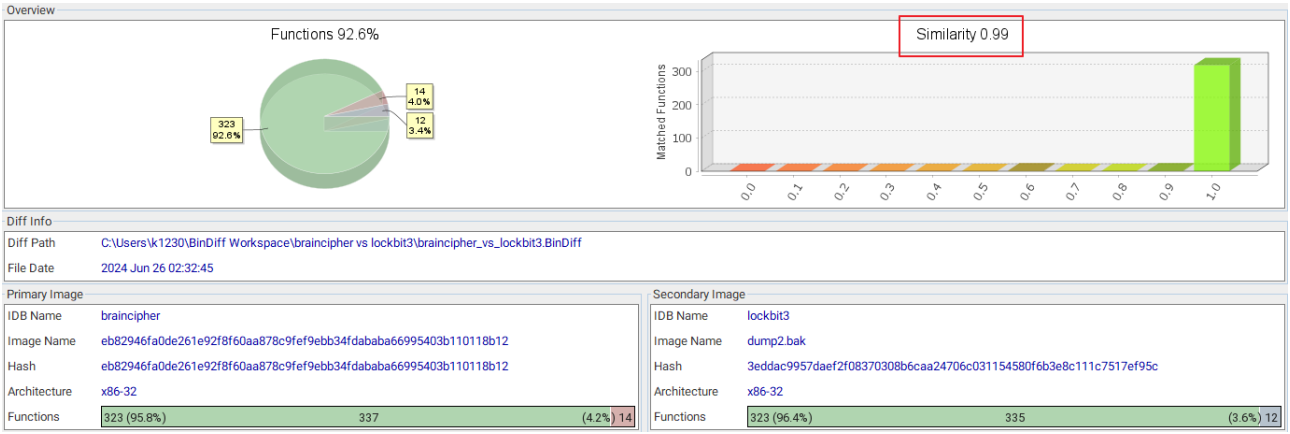


Figure 3. Similarity of BrainCipher and LockBit 3.0 Ransomware

BrainCipher group, which is a new ransomware group, has been identified to use ransomware created with the leaked LockBit 3.0 builder[12]. This group suspended public services of approximately 200 Indonesian government and local organizations, and paralyzed immigration processing at airports by attacking the country's temporary national data center (PDNS). It reportedly demanded the ransom of USD 8 million (approx. KRW 11 billion) in the process of negotiation. In the past, only a dark web page that could be accessed with an ID usded to the ransom note had been known. On June 26, however, a dark web leak site accessible without an ID was additionally found.

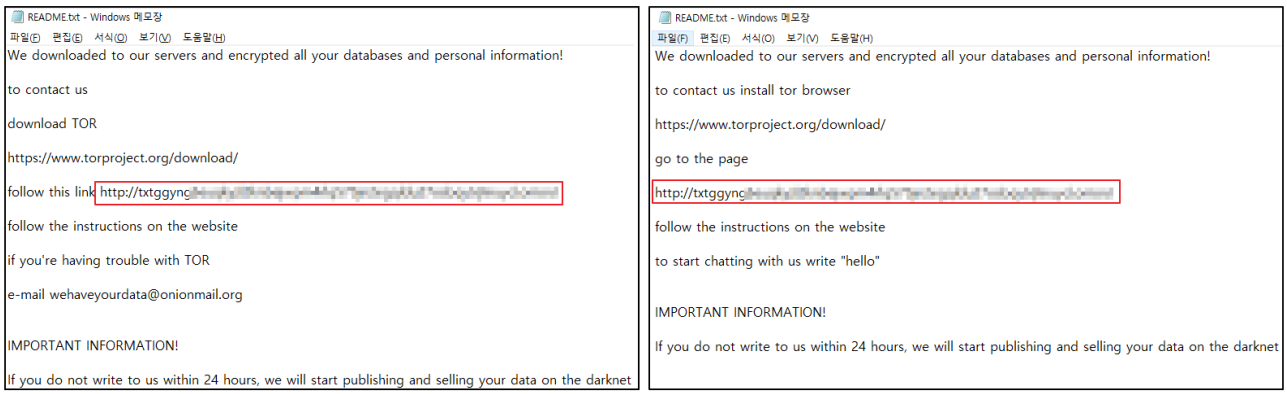


Figure 4. Comparison of Ransom Notes (Left: Trinity, Right: 2023Lock)

Four other new groups were found. In particular, Trinity ransomware, which posted three victims in the dark web leak site, displays similarity in its ransom note to that of the 2023Lock ransomware detected in February 2024. The registry values and mutex[13] values also partially matched those of Venus ransomware that has been active since 2022. Additionally, ElDorado group posted 15 victims, a large number, and Cicada 3301 and SenSayQ group posted four and two victims respectively.

[12] Builder: Ransomware building tool to create ransomware comprising the required functions through environment setting

[13] Mutex: Technique to prevent concurrently approach to a single resource by several threads

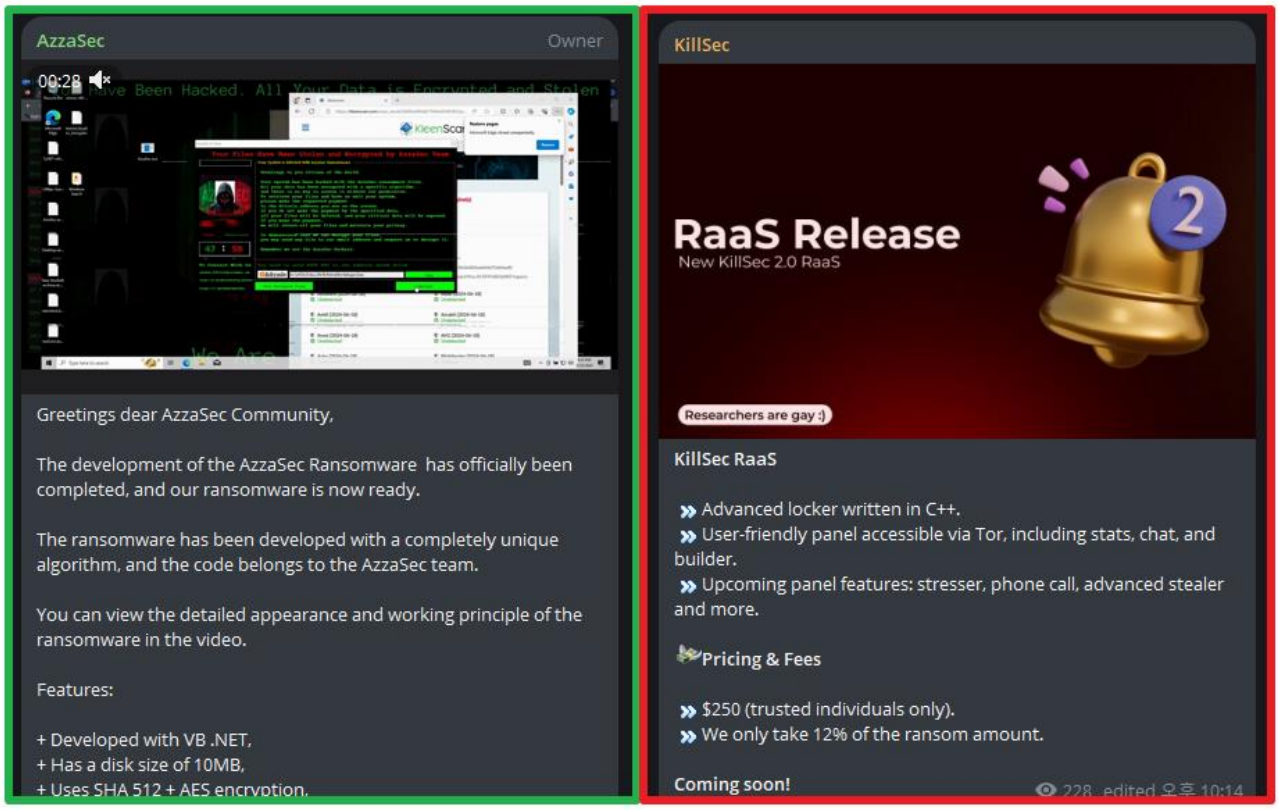


Figure 5. Ransomware Sale in Telegram Channel (Left: Azzasec, Right: KillSec)

Ransomware threats are also continuously found on Telegram and hacking forum. Azzasec, a hacktivist that has been performing since February 2024, is a pro-Palestinian group that supports Palestine and attacks the hostile countries. Recently, this group posted a message to sell ransomware service and source codes together with a demonstration video on its Telegram channel.

KillSec ransomware group, which was started in October 2023, began posting ransomware victims on the dark web leak site in March 2024. It posted a message to sell KillSec 2.0 RaaS[14], an updated version of its existing ransomware service, on the Telegram channel. As such, hacktivist groups are continuously performing ransomware activities to create and sell ransomware in addition to launching attacks for political or social purposes.

[14] RaaS (Ransomware-as-a-Service): Business model providing ransomware codes or tools necessary for attack in return for money

Top 5 Ransomware

Figure 6. Major Ransomware Attacks by Industry/Country

Play ransomware group has a characteristic to post the victims collectively on the dark web leak site. In June, it performed most actively by posting 26 and 10 victims in two separate occasions. Recently, all VMs[15] were ended in the ESXi environment and encrypted, and it was followed by the detection of an ESXi variant with a self-deletion function, which is threatening in more areas than before.

RansomHub group, which was started in February 2024, is performing actively while displaying a fast growth rate. It recruited partners in a method for its affiliates to make profits first and pay a part of their profits as service charges to RansomHub. It started recording a fast growth rate after notchy[16], which had performed as an affiliate of BlackCat/ALPHV, and Scattered Spider[17] participated in its

[15] VM (Virtual Machine): Computing resource to execute programs or operating systems by implementing a physical computing environment with software

[16] Notchy: An affiliate for which RansomHub posted a message claiming for not receiving service charges from BlackCat (ALPHV) on RAMP, a Russian hacking forum

[17] Scattered Spider: A group that became known following an attack launched on MGM, a large-scale U.S. resort and accommodation service group, in September 2023

activities. In June, it disclosed information of approximately two million customers stolen by attacking Frontier Communications, a large-scale U.S. common carrier, in April.

In addition to the Windows and Linux version created with Go language[18], RansomHub started using the ESXi[19] variant, which is based on C++. RansomHub's ESXi variant offers a function to end and encrypt the virtual environment, interrupt logging by deactivating key services such as the log generation and control tool, syslog in UNIX environment, and independently delete malicious codes to avoid detection and analysis. Attention is needed because ransomware groups aim for an ESXi environment in which several virtual servers can be infected through a single attack.

Akira group, which made its appearance in April 2023, intensively attacked the manufacturing field in June. Approximately 40% or more of its attacks in June targeted the manufacturing field. In particular, it stole internal data including project details and confidential contracts by attacking Panasonic Australia, a company manufacturing and selling cameras and sound equipment, and sensitive information such as personal data, confidential contracts and confidentiality agreements to a scale of approximately 40GB by attacking TETRA, a U.S. petroleum and gas service company.

On June 24, 2024, Inc group, which appeared in August 2023, penetrated the Cambridge University Press and its assessment system, and posted the sample data. It is found to have subsequently demanded ransom of approximately USD 5.6 million for prevention of data disclosure. In May, it created and relocated to a new dark web leak site, and posted a message to sell ransomware source code in XSS, a Russian hacking forum. There are various reasons for a ransomware group to sell source code. However, according to an analysis, the main reason to separate or rebrand a group, or for several groups to use the same ransomware (or a derived variant) with a goal to cause confusion in the investigation.

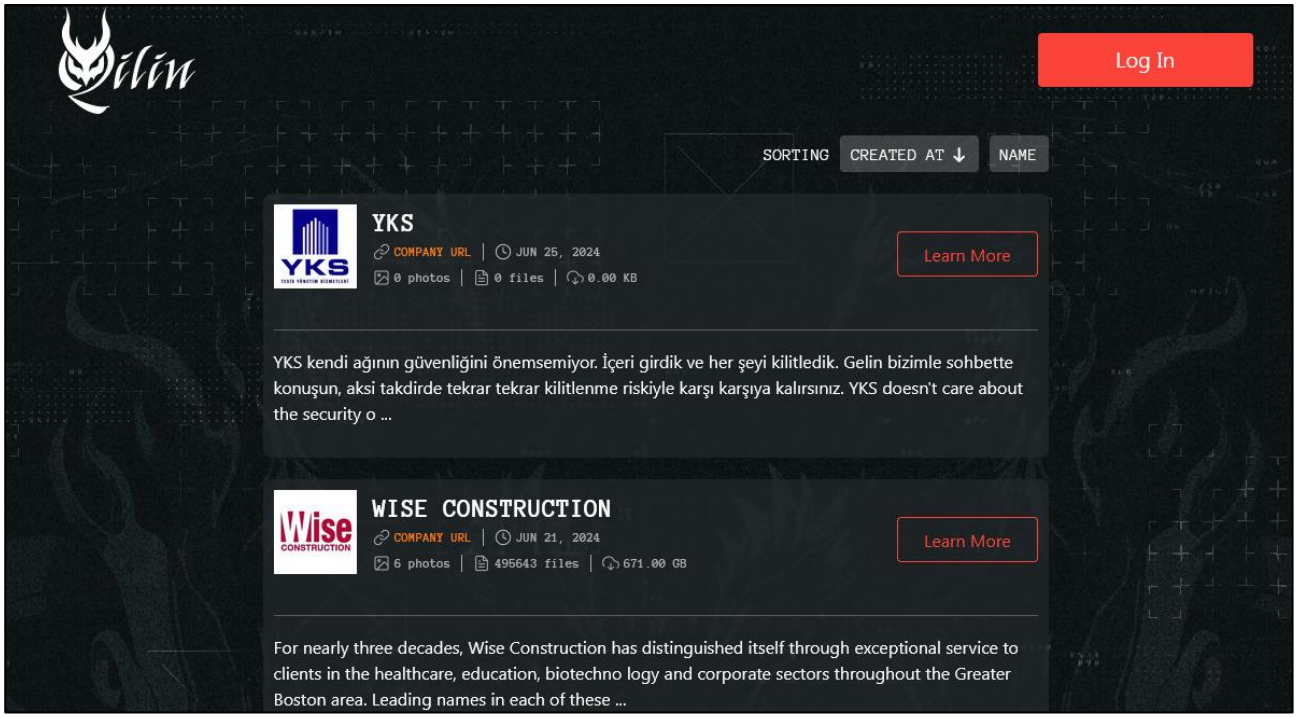
Medusa ransomware group displayed a difference from other groups that it intensively attacked organizations and associations. In June, it launched a ransomware attack against St. Helena City Hall in California, U.S., and paralyzed the city hall's computer system and municipal library. It stole data by 120GB and demanded USD 200,000 in ransom. It also demanded ransom by attacking the U.S. Women's Sports Association, which is a nonprofit organization, and Tri-City College Prep, a U.S. public middle and high school.

[18] Go Language: Opensource programming language developed by Google to improve productivity

[19] ESXi: UNIX-based logical platform developed by VMware that can concurrently execute multiple operating systems in a computer

■ Ransomware in focus

Overview of Qilin Ransomware



Source: Qilin Ransomware Group Data Leak Site / Dark Web

Qilin ransomware group, which first appeared in July 2022, has posted 128 victims so far on the dark web data leak site. In November 2023, especially, it posted a Korean semiconductor component maker. Recently, it attacked Synnovis, a U.K. pathological service provider, based on a political motivation and this resulted in the paralysis of the company's blood test and information sharing system, causing an enormous damage of some hospitals having to cancel patient treatment and surgeries.

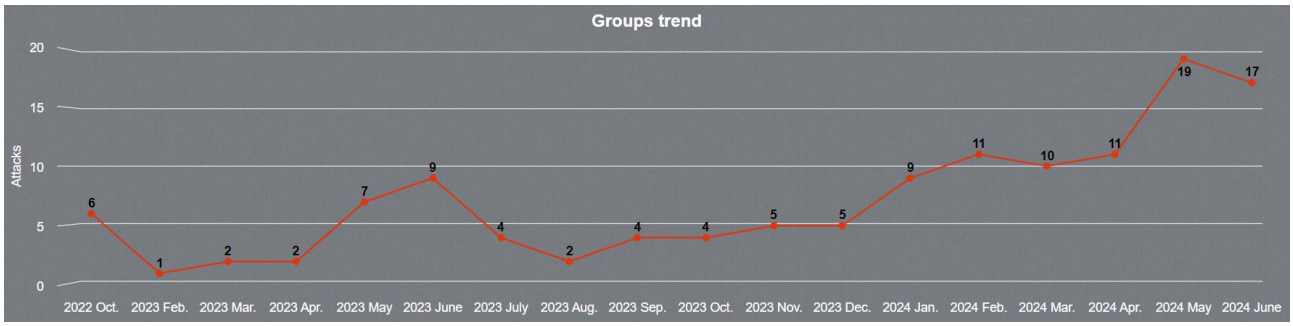
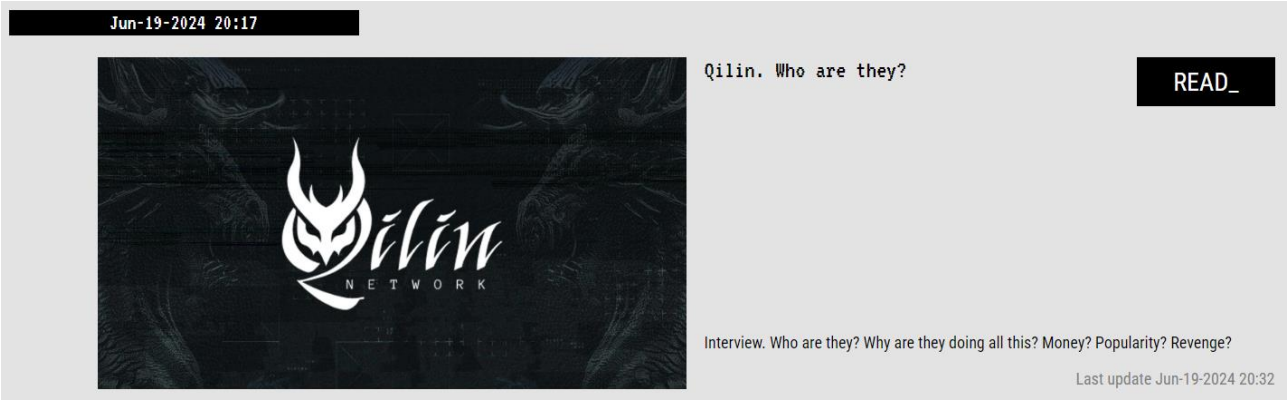


Figure 7. Statistics of Qilin Ransomware Group Attacks

Qilin ransomware group began its activity under the name "Agenda." During the initial phase, it attempted attacks targeting medical and educational institutes in Africa and Asia. It generated a dark web leak site and posted six victims in October 2022, but no additional activity was detected until January 2023. Then, in February 2023, the group announced the resumption of its activity by

uploading an RaaS promotion post to the hacking forum and started performing full scale by posting victims in the dark web data leak site.

Currently, Qilin's dark web leak site contains the links and QR codes connected to WikiLeaksV2. WikiLeaksV2 is an information disclosure site created in February 2024 by an organization that follows and supports WikiLeaks, a nonprofit organization that had collected and shared confidential documents and media clips about Kenya's corruption, Yemen's drone attack and the air raid in Bagdad, and its founder Julian Assange. Operated with separate donations like WikiLeaks, this organization posts information obtained from informants. It has a range of categories from international economy, international relations, governments, war and army to medical institutes and associations. So far, only the data on government, war, army, medical institutes and associations have been posted. With an exception of the government data, all data had been previously leaked by Qilin. Partial data of the recently attacked Synnovis are also posted.



Source: WikiLeaksV2

Figure 8. Qilin Interview Posted on WikiLeaksV2

WikiLeaksV2 also contains the recently posted interview with Qilin group. According to this interview, the group claims that it is performing activities to raise fund for the nation's freedom and, having lost the comrades in battlefields, it is attacking only the targets that are politically related to the global support for countries at war. Considering the time of Qilin group's appearance, its interview with WikiLeaksV2, and the interview with BBC, a public broadcasting company of the U.K., in relation to the recent attack of Synnovis, this group is predicted to have a close relevance to the Russo-Ukrainian War.

During the initial phase, Qilin used Agenda ransomware created using Go language, and showed meticulousness to use ransomware customized to each victim. The Go language-based Agenda ransomware was distributed targeting medical and educational institutes in Asia and Africa, and verified to infect the Windows system. This ransomware operates successfully only when a password is delivered as a factor concurrently with its execution. It has also been found to have the functions to delete the backup copies, randomly change the victim's Windows account password, and execute safe mode booting. In case of file encryption, it was carried out targeting the network shared folder, not disk drive. After a file encryption using AES-256 algorithm, the encryption key was protected with RSA-2048 algorithm.

In September 2022, two months into the group's activity, a Qilin variant created on the basis of Rust was detected. It has been verified that the group is still using the Rust variant. The newly discovered Rust variant uses ChaCha20 or AES algorithm in file encryption, and offers the additional functions to spread ransomware to a virtual environment such as VMWare vCenter[20] and ESXi, and directly spread it to a designated host using PsExec[21]. As the scope of threat is expanding because it aims for ransomware spreading not only in the Windows, but also ESXi, the Rust-based Qilin ransomware will be examined in detail, and a response plan in preparation for Qilin group's strategy will be proposed in this issue.

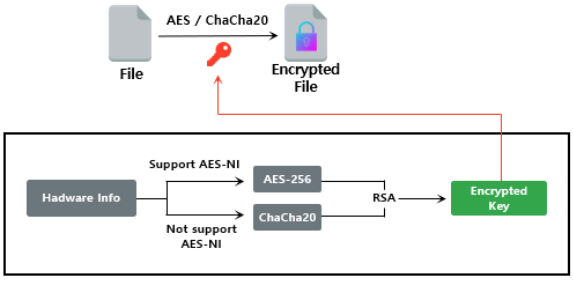
[20] VMWare vCenter: Platform on which multiple ESXi and virtual systems can be monitored through centralized control

[21] PsExec: Command string tool enabling remote execution of a process without the need to install software in another system

Qilin Ransomware

Encryption Key

Encrypt files with AES-256(CTR) or ChaCha20 algorithm and protect the key with RSA-4096



Encryption Method

fast [n] : Encrypts from the beginning of the file for n * 32 MB
skip-step [n] [p] : Encrypts n Bytes every p Bytes
percent [n] [p] : Encrypts n * 32 MB every p(%) of the entire file

Features

- Intermittent Encryption
- Delete System Recovery Options
- Shared Folder Encryption
- Propagation of vCenter and ESXi
- Self-Destruct
- AES/ChaCha20 & RSA Encryption
- Safe Mode boot
- Delete Windows Event log
- Anti-VM & Anti-Sandbox

Ransom Note

```
-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreement, your data will be published.
Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

-- Warning
```

README-RECOVER-[a-zA-Z0-9_-]{10}.txt

Extension

.[a-zA-Z0-9_-]{10}

Production Language

Rust

Figure 9. Overview of Qilin Ransomware

Qilin Ransomware Strategy

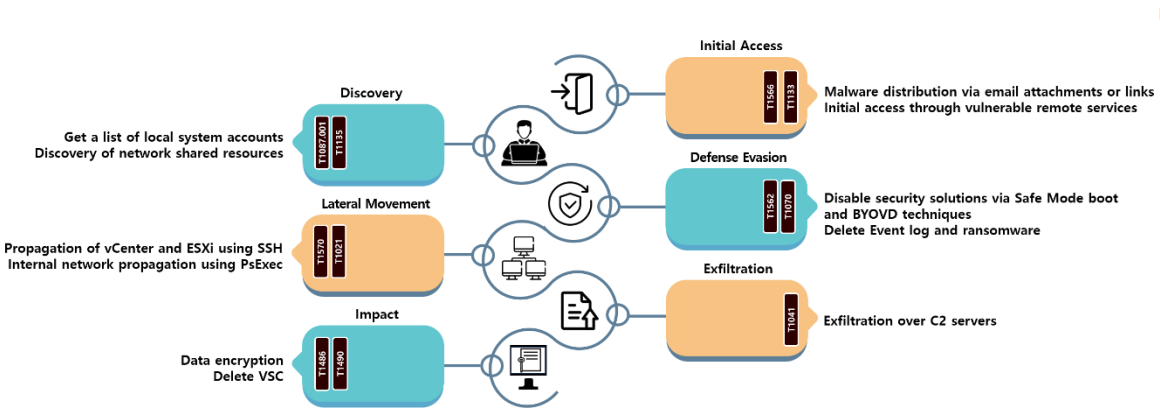


Figure 10. Qilin Ransomware Attack Strategies

Qilin ransomware group distributes the payload for ransomware execution in several ways. It uses a method to send an attached file or a separate download link via email and encourage the target of attack to download it, or a method to directly distribute the payload after penetrating a vulnerable remote access environment. Also, the ransomware can be successfully executed only when a password separately set by the attacker is delivered together with the "--password" factor.

Qilin ransomware uses a number of strategies to avoid detection by security solutions and interrupt the victims' system access. In many cases, security solutions do not work in safe mode. Therefore, to avoid detection, it provides a function to be executed following rebooting in safe mode. After safe mode rebooting, it uses a unique strategy to reset the system account password as a random character string. In addition to the safe mode booting, Qilin ransomware uses BYOVD[22] to end security solutions like Anti-Virus and EDR[23] with the driver privilege.

If a separate factor is delivered for the ransomware execution, the ransomware can be spread to the internal network. For this, the "--spread-vcenter" and "--spread" factors are used. When "--spread-vcenter" is entered at the ransomware execution, spread to VMWare vCenter or ESXi is attempted using the PowerShell script built in the ransomware. However, to attempt ransomware spread using this function, separate vCenter or ESXi administrator credentials are required. Once the attacker enters the credentials, the administrator password is changed the same as the Qilin ransomware password following a connection to the designated host. Then, SSH[24] is activated to

[22] BYOVD(Bring Your Own Vulnerable Driver): Attack method through vulnerable driver module for which system privilege can be used

[23] EDR(Endpoint Detection and Response): Solution to prevent damage spreading by detecting, analyzing and responding to malicious actions occurring in computers, mobile devices, servers, etc. real time

[24] SSH (Secure Shell): A security protocol used to access other remote hosts

spread the ransomware. Through the activated SSH session, the ransomware is uploaded and executed. Using the "--spread" factor, PsExec is saved in a temporary folder and spread to another host in the internal network. Then, the ransomware is executed using the "--spread" option to infect all networks.

After the initial penetration or internal spreading, Qilin ransomware deletes a backup copy in the internal system to make it difficult for users to recover it and encrypts the file. The encryption targets include not only files saved in drive, but also the network shared folders. Prior to encryption, the ransomware checks hardware information, and decides a file encryption algorithm to be used on the system. It uses AES-CTR(256) algorithm for hardware that supports AES-NI, which is a set of commands to improve AES encryption and decryption performance. If AES-NI is not supported, it uses ChaCha20 algorithm. Encryption is carried out using the keys randomly created by file, and the keys used in encryption are protected with RSA-4096 public key that is built in the ransomware.

Factor	Description
fast [Number of Blocks]	Encryption by as much as [number of blocks] * 32MB from the beginning of file
skip-step [Encryption Size] [Interval]	Encryption by as much as [encryption size] bytes in each [interval]
percent [Number of Blocks] [Ratio]	Encryption by as much as [number of blocks] * 32MB according to [ratio] of all files (%)

Table 1. Execution Factors according to Encryption Mode

As for file encryption, the entire file is encrypted by default. Depending on the execution factors, however, three partial encryption modes are additionally supported. With fast factor, the first part of a file can be encrypted according to the integer entered. With skip-step and percent factors, the file is encrypted in each of the intervals set.

Several functions making ransomware analysis difficult are also included. Using Anti-VM and Anti-Sandbox, which disable operation in a virtual environment by checking whether the current execution environment is VM or Sandbox[25], the ransomware file analysis is interrupted. There is also a self-deletion function to execute deletion just before the encryption process is completed so as to disable the securing of the ransomware itself. In addition, all event logs are deleted to make analysis difficult.

[25] Sandbox: A system operating system, an isolated environment that does not affect or is not affected by external factors such as installation program

How to respond to the Qilin ransomware

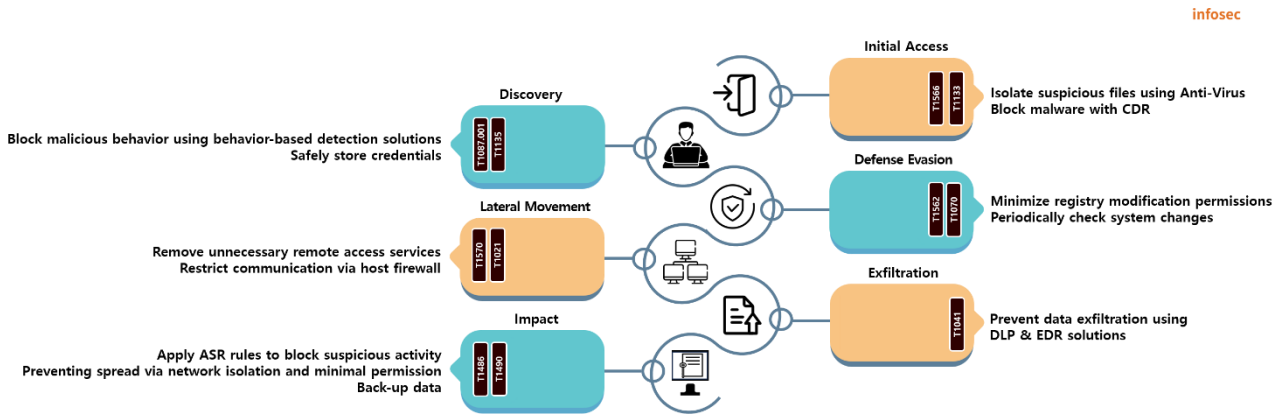


Figure 11. Qilin Ransomware Response Plan

Qilin spreads ransomware through an email attached file or a link, or directly distributes it by penetrating a vulnerable remote access program. Therefore, caution is required to not open suspicious emails or emails and attached files from unidentified senders. It is necessary to improve security awareness by holding separate training sessions on a regular basis. For more active response, Email Thread Response & Detection, a solution to detect and block email risks in Sandbox environment, can be used. In addition, when using a remote access program, it is necessary to securely store credentials necessary for access and keep the program in a version without vulnerability through continuous updates. When not using the remote access function, it is recommended to deactivate it.

Qilin ransomware uses a method of safe mode booting to bypass security solutions. To prevent this, only the minimum necessary administrator privilege for safe mode booting must be given, and a security solution that can be used in safe mode must be applied to detect and block malicious actions.

As ransomware spreading to the internal network is attempted using the credentials secured, the credentials must be stored safely. Also, it is necessary to use an additional authentication process. In some cases, SSH is used in the ransomware spreading. Therefore, when not in use, deactivate SSH as a preemptive measure. Another method is to use the host firewall to limit communication through such tools as PsExec.

Lastly, as Qilin ransomware encrypts the network shared files, it must be blocked from approaching external resources by minimizing or deactivating the network shared resource access privilege. In addition, as a response to the function to delete backup copies and prevent the file recovery by users, data must be divided, and backed up in separate networks or repositories.

Indicator Of Compromise

Qilin : SHA256

6316417fcd979c39a4da672ba3521f62081ff4dfebb868ef65a1f2dff9a738ea
27f7a332ba10bae9dbc527ea25c787cb1850f0b34295cd49118f040f08f4fe56
27a91c2e53e9e7bd6a1ccb8b0bed1f954f3011973248e710598a5e7d6c6ed668
55e070a86b3ef2488d0e58f945f432aca494bfe65c9c4363d739649225efbbd1

File Name

STL.exe
forigpatch.exe
file.exe

■ Reference Websites

• Imperva official website (https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware/)

• SC Media official website (https://www.scmagazine.com/brief/vmware-esxi-subjected-to-attacks-with-ransomhub-for-linux)

• Synnovis official website (https://www.synnovis.co.uk/news-and-press/cyberattack-update-24-june-2024)

• The Guardian (https://www.theguardian.com/society/article/2024/jun/21/uk-national-crime-agency-russian-ransomware-hackers-qilin-nhs-patient-records)

• U.K. National Health Service (https://digital.nhs.uk/news/synnovis-cyber-incident)

• BleepingComputer official website (https://www.bleepingcomputer.com/news/security/major-london-hospitals-disrupted-by-synnovis-ransomware-attack/)

• BBC (https://www.bbc.com/news/articles/c2eeg9gygyno)

• BBC (https://www.bbc.com/news/articles/ceddqglk7qgo)

• Symantec corporate blog (https://symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day)

• Trend Micro official website (https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html)