Keep up with Ransomware

The Rapidly Evolving Vanhelsing Ransomware

■ Overview

In March 2025, the number of ransomware incident cases recorded a decline of approximately 28% to 773 cases, compared to 1067 cases in February. The reduction in incidents during March can be attributed to the Clop group having disclosed all victims affected by the exploitation of vulnerabilities in Cleo's file transfer solution in February. Although there was a decrease from the previous month, the figure of 773 cases remains significantly high. This is due to the emergence and activity of numerous new ransomware groups.

In March, the South Korean threat of ransomware was once again confirmed. The NightSpire group, which emerged as a new entity in March, posted 15 victims during the month alone, including a domestic video content production company. The sample data released comprised a single episode script produced by the company, and despite the scheduled release date having passed, the full data set has not been disclosed. As of April, the dark web leak site has been deactivated.

The group operating BlackLock has announced a new ransomware-as-a-service named Mamona. Initially appearing in September 2023 under the alias LostTrust, the group underwent subsequent rebrandings, adopting the name ElDorado in June 2024, and later rebranding to BlackLock in September 2024. Concurrently, they established a separate entity called Mamona RIP and commenced promotional activities on Russian hacking forums. However, due to inadequate security configurations on the Mamona servers, the Mamona dark web leak site was compromised, leading to the deactivation of the BlackLock leak site. Presently, only the BlackLock leak site remains accessible.

It has been confirmed that the RansomHub ransomware was recently distributed through a malware service framework known as SocGholish (FakeUpdates). SocGholish emerged in 2018 and operates by injecting malicious scripts into legitimate websites, subsequently hijacking user traffic. When users visit these compromised websites, they are redirected to a counterfeit page disguised as a browser update notification, where they are prompted to download a ZIP-compressed SocGholish script file. Upon execution of this script file, attackers gain the capability to exfiltrate data or execute remote commands, a method through which the distribution of RansomHub ransomware has been facilitated.

It has been confirmed that the Akira Group recently succeeded in executing a ransomware attack by exploiting webcams. The group employed their customary strategy of infiltrating systems either by utilizing exposed credentials in vulnerable remote access solutions or through brute force attacks, subsequently attempting to deploy ransomware payloads. However, their attempts to distribute ransomware were thwarted by an Endpoint Detection and Response (EDR)[1] solution. In response, they identified vulnerable webcams within the accessible systems, capitalizing on the fact that these webcams lacked EDR protection. By gaining remote shell access, they successfully deployed the ransomware.

[1] EDR: A solution for real-time detection, analysis, and response to malicious activities on endpoints (computers, mobile devices, and servers), preventing damage spread.

■ Ransomware News

RansomHub Group Distributes Ransomware via SocGholish Malware-as-a-Service

- SocGholish intercepts user traffic by injecting scripts into legitimate websites.
- Visiting a compromised site may trigger a SocGholish script disguised as a browser update.
- Executing the file allows the attacker to steal data or execute remote commands.

Akira Group Successfully Executes Ransomware Attack Webcams

- The attacker deployed the ransomware payload via network-connected webcams to evade EDR.
- The attacker exploited webcams to gain remote shell access, taking advantage of the absence of EDR solutions.

North Korean threat group Moonstone Sleet observed distributing Qilin ransomware

- The group Moonstone Sleet has a history of distributing its proprietary ransomware, FakePenny.
- The group began distributing Qilin ransomware in late February 2025.

Mamona Ransomware-as-a-service(RaaS) was hacked by the DragonForce

- Mamona is a newly unveiled RaaS operated by the group known as BlackLock.
- Insufficient security settings led to the exposure of the administrator interface and management panel.
- The darkweb leak site of Mamona was Hacked by DragonForce, rendering BlackLock's DLS inactive.
- BlackLock's DLS was recovered roughly two weeks following the hack.

The newly emerged Vanhelsing group begin group partners

- The advertisement for RaaS partner recruitment was posted on RAMP, a prominent Russian hacking forum.
- The scope of targeted platforms expanded within just three weeks of its initial release.
- Total of eight victims were posted over a period of about one month.

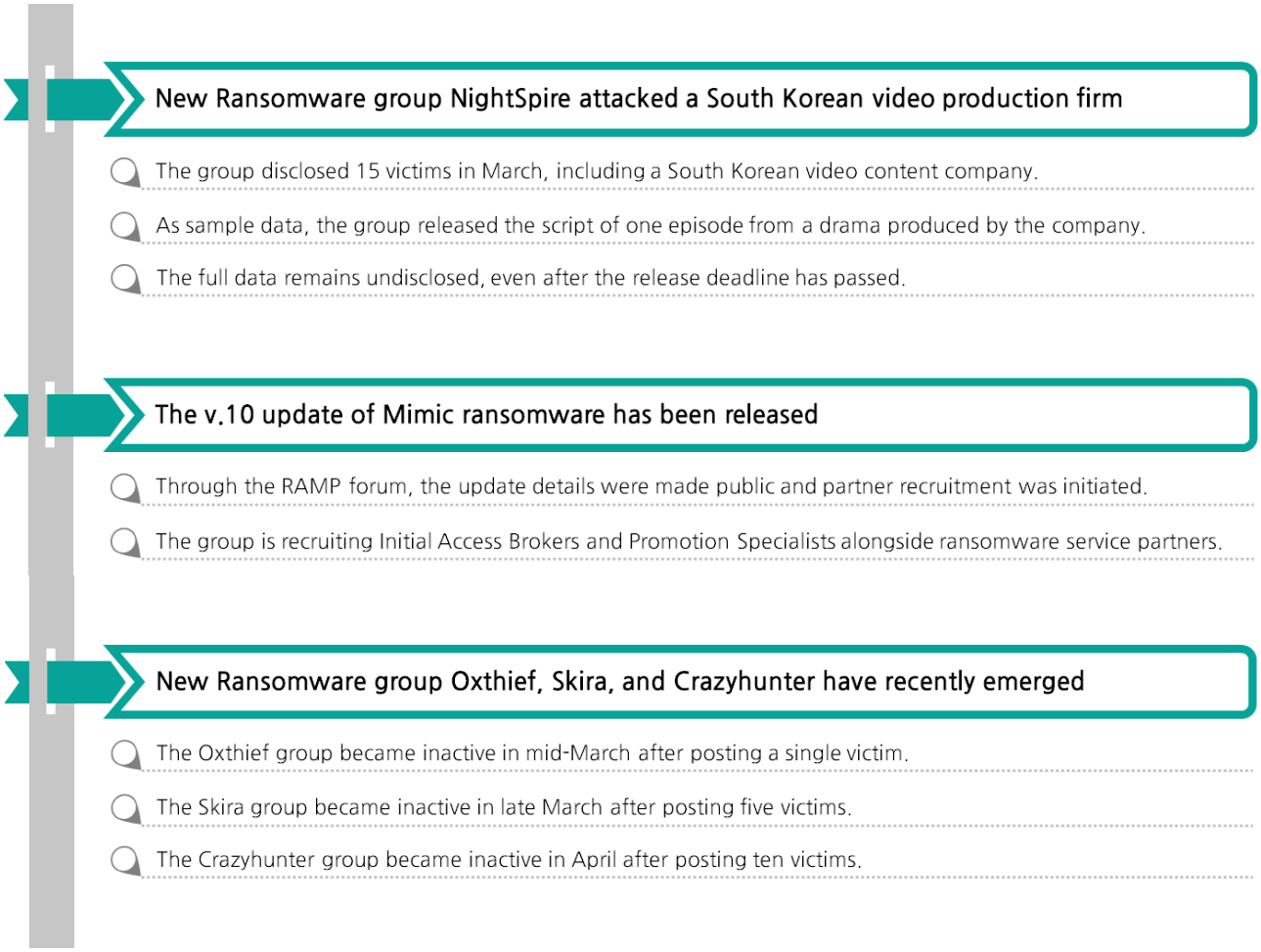


Figure 1. Trends in Ransomware

Ransomware Threats

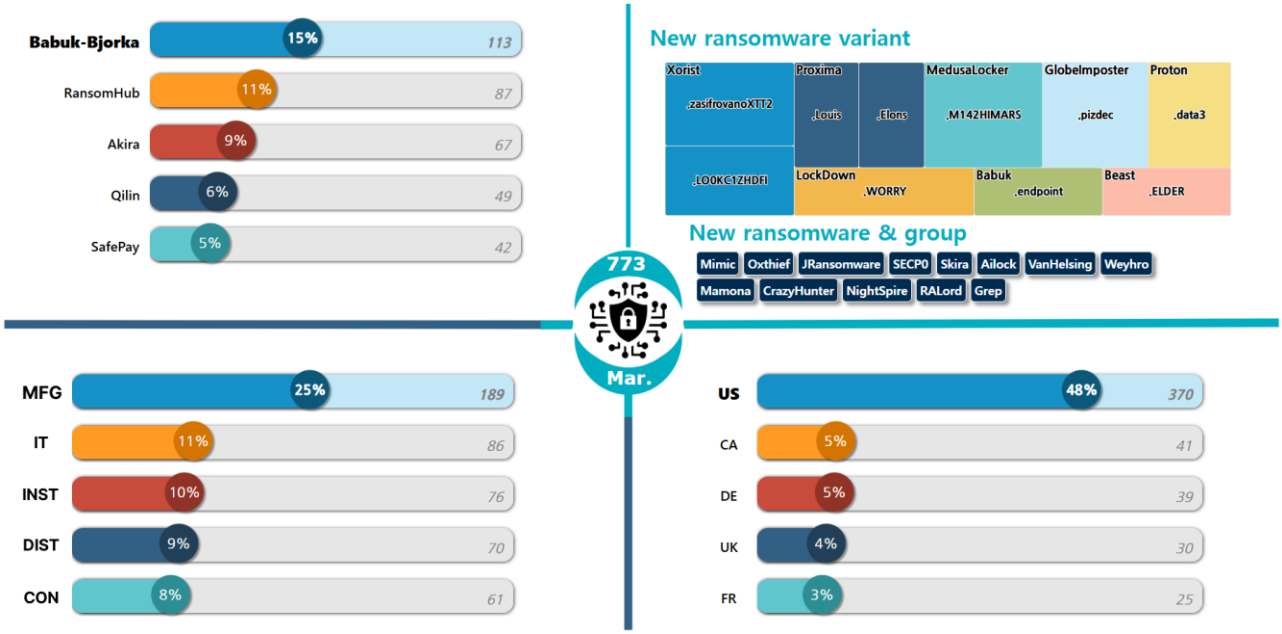


Figure 2. Ransomware Threat Landscape as of March 2025

New Threats

In March, updates concerning existing ransomware groups were observed, alongside the identification of several new ransomware collectives. A total of six new groups were detected, of which three—Oxthief, Skira, and CrazyHunter—are currently inaccessible as of April. Initially emerging in early March, the Oxthief and Skira groups uploaded one and five victims respectively; however, their dark web leak sites became inactive starting from March. Similarly, the leak site for CrazyHunter was deactivated in April.

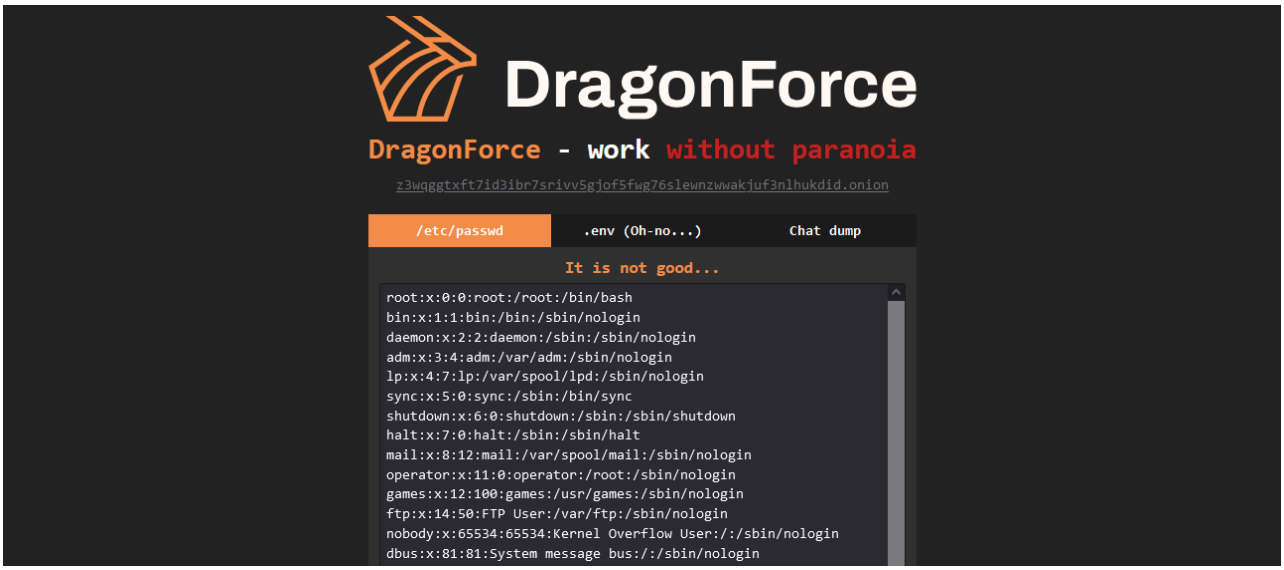


Figure 3. The Mamona dark web leak site hacked by DragonForce

The group operating BlackLock recently unveiled a new ransomware-as-a-service called Mamona, which has been compromised due to inadequate security configurations. Not only was the Mamona administrator page exposed, but also its management panel. This issue was shared on a Russian hacking forum, enabling forum users to access the service unauthorized and view data. Subsequently, BlackLock's leak site was deactivated, and the DragonForce group even tampered with Mamona's dark web leak site. Approximately two weeks later, BlackLock restored the deactivated dark web leak site; however, Mamona is no longer operational.

A new group has been identified on a Russian hacking forum promoting their ransomware services. The Vanhelsing group commenced recruitment of partners in early March to utilize their Ransomware-as-a-Service (RaaS)[2] on the Russian hacking forum, and within three weeks of launch, they expanded their target platforms. Additionally, they posted eight victims over the course of a month.

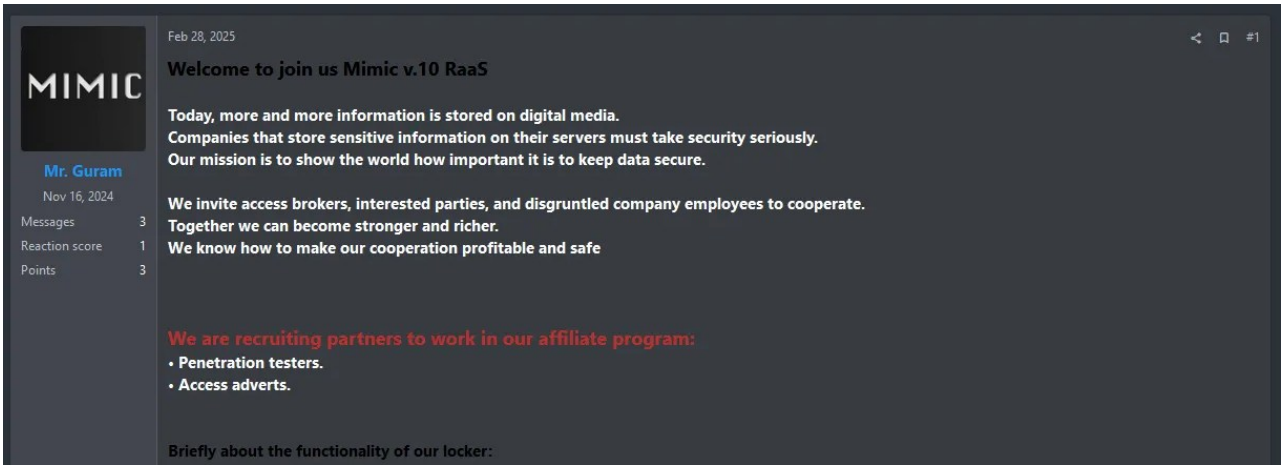


Figure 4. Promotional Material for Mimic v.10

[2] RaaS (Ransomware-as-a-Service): business model that offers ransomware as a service, enabling anyone to easily create and launch ransomware attacks.

Since June 2022, the Mimic ransomware, known for its activities, has launched v.10 and is currently recruiting initial penetration experts and access advertisement managers on Russian hacking forums. The ransomware they offer supports a diverse range of operating systems including Windows, ESXi[3] ,NAS[4] ,FreeBSD[5]. In addition to providing ransomware, they also offer services such as making extortionate calls to victims and supplying software necessary for various operations.

Two ransomware groups have been identified that, although they are ransomware operators, do not manage separate data leak sites but solely operate chat pages for ransom negotiations. These groups are JRansomware and Ailock. They provide a chat page URL and a session ID required for login in the ransom note, thereby administering a chat page individually for each victim.

[3] ESXi: UNIX-based logical platform developed by VMware that allows a host computer to run multiple operating systems concurrently.

[4] NAS: Storage solution comprising multiple storage devices that are accessible over a network.

[5] FreeBSD: Unix-inspired OS distributed as open-source software.

Top 5 Ransomware

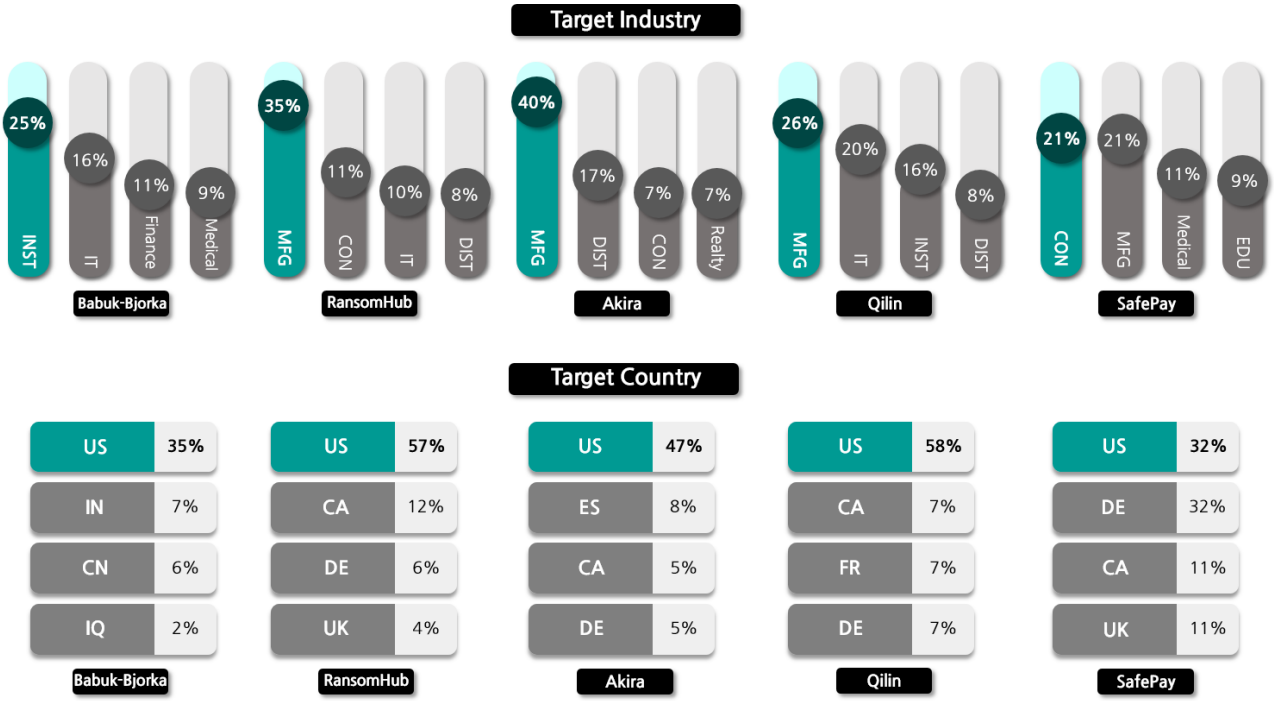


Figure 5. Current Status of Major Ransomware Attacks by Industry/Nation

The group known as Babuk-Bjorka, which claims to be Babuk2, commenced their operations in January. They exhibited their most prolific activity in March by posting 113 victims, many of whom had previously been compromised by other groups such as RansomHub, Meow, Everest, Babuk, Funksec, and LockBit, with their data already made public. Consequently, it is imperative to ascertain whether these incidents represent genuine attacks where data was exfiltrated by the group itself, or whether they merely recycled previously disclosed data to extort ransom.

The RansomHub group orchestrated an attack on the Malaysian engineering services corporation, HexcoSys Group, resulting in the exfiltration of 336GB of data, which included contracts, blueprints, source codes, and product development data. Additionally, they targeted Japan Rebuilt, a Japanese automotive parts manufacturer, from which they leaked 200GB of data encompassing production data, financial information, payment details, and customer records.

In March, the Akira Group launched an attack on CS Plastics, a Belgian industrial machinery manufacturer, resulting in the leakage of sensitive data, including audit reports, financial statements, and personal information of employees and customers. Additionally, recent observations have confirmed that they are employing novel attack strategies, such as using webcams to circumvent the detection capabilities of EDR (Endpoint Detection and Response) solutions. Detailed information on Akira Group's specific attack strategies and countermeasures can be found in the SK Shields KARA Ransomware Trend Report for the fourth quarter of 2024.

It has been recently revealed that the Qilin group is associated with the North Korean threat group known as Moonstone Sleet. Moonstone Sleet, a threat group with a history of distributing its self-developed FakePenny ransomware, has been identified as deploying the Qilin ransomware payload since the end of February 2025.

On March 30th alone, the SafePay Group disclosed a batch of 31 victims. Among these, Sir William Ramsay School, a secondary school located in High Wycombe, UK, suffered a data breach involving the leakage of 183GB of data. Similarly, Brighton Australia, a construction contracting firm in Australia, experienced the exfiltration of 160GB of data, which included financial statements, accounting records, personnel files, and customer documents.

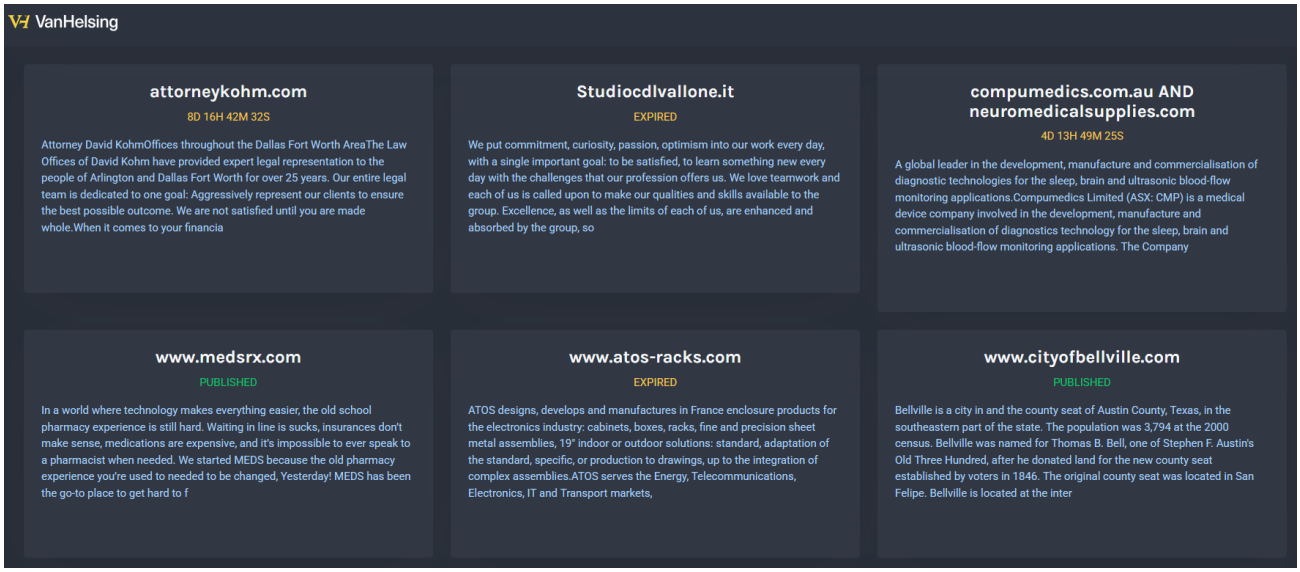


Figure 6. Vanhesling Dark Web Leak Site

The Vanhelsing group, which emerged on March 7, is a ransomware collective that began recruiting affiliates on the Russian hacking forum RAMP. They do not require a membership fee from individuals with a certain level of reputation; others, however, must pay a deposit equivalent to 5,000 USD to join. According to promotional posts on the forum, the group prohibits attacks against CIS countries and demands only a 20% commission from the ransom obtained.

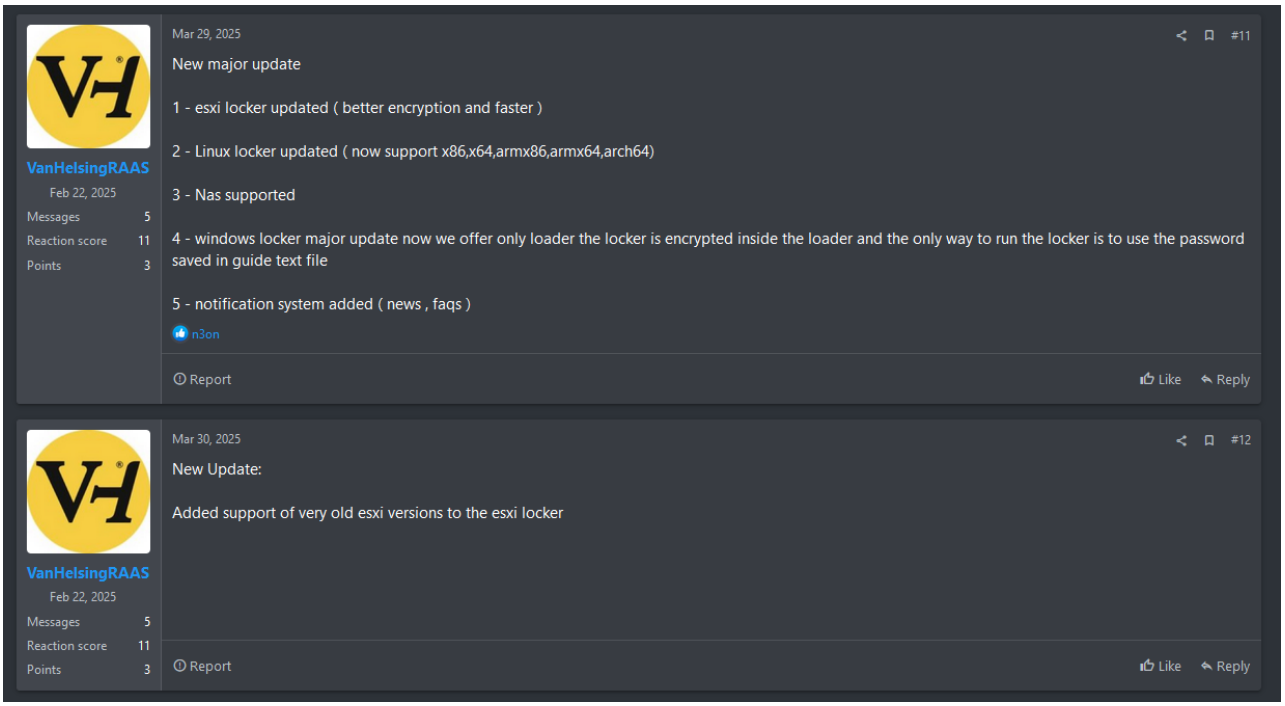


Figure 7. Vanhelsing Feature Update

From the outset, the developers have introduced encryption support targeting a diverse array of platforms including Windows, Linux, BSD[6] , ARM[7] and ESXi. According to the update history posted by the operator at the end of March, the capability to attack a broader spectrum of versions and architectures has been enhanced for Linux and ESXi, and Network Attached Storage (NAS) has also been added to the list of supported targets for attacks.

To date, only versions of Windows ransomware utilizing the encryption extensions 'vanhelsing' and 'vanlocker' have been identified. These two versions of ransomware were developed approximately five days apart, with the latest iteration featuring a newly added capability for propagating across internal networks—a feature absent in earlier versions. Additionally, although not yet implemented, parameters related to the propagation through vCenter[8] have also been detected. The rapid pace of updates to the ransomware's functionalities is not only evident but, according to promotional materials for the ransomware, it appears likely that future versions will be capable of targeting a broader array of platforms. Consequently, it is imperative to prioritize the examination of the contents pertaining to the Windows version of the ransomware in preparation for the impending threats.

[6] BSD: suite of Unix-inspired operating systems originally developed at the UC Berkeley.

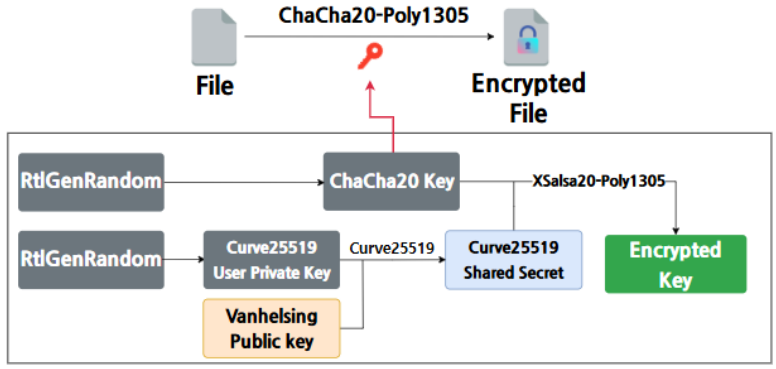
[7] ARM: low-power, high-performance processor architecture widely adopted in smartphones, tablets, and IoT devices.

[8] vCenter: unified management solution from VMware for administering clusters of ESXi hosts along with associated infrastructure.

Vanhelsing Ransomware

Encryption Key

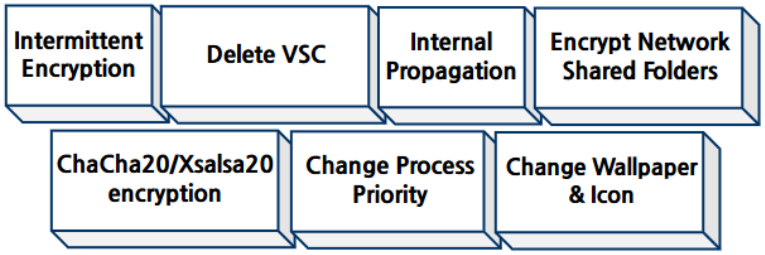
Encrypt files with ChaCha20-Poly1305 algorithm and protect the key with Curve25519 shared secret



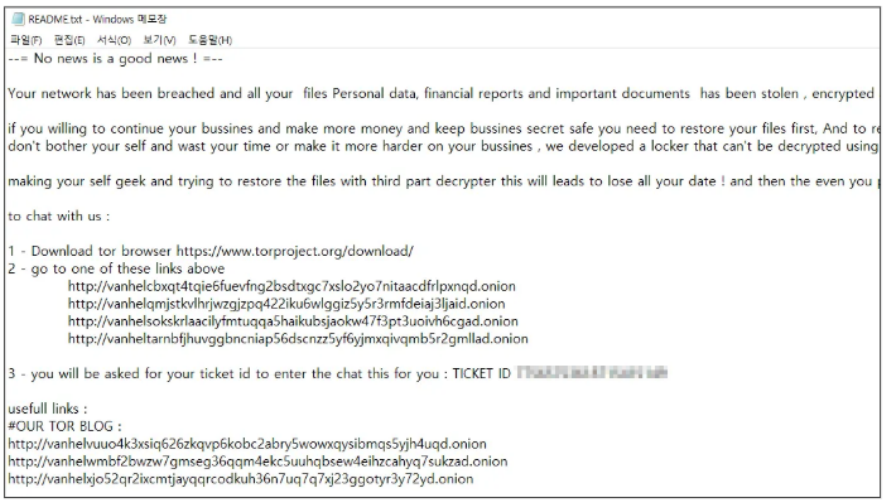
Encryption Method

1GB or less: Encrypt the entire file
More than 1GB: Encrypt 30% of total size

Features



Ransom Note



README.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

--= No news is a good news ! =--

Your network has been breached and all your files Personal data, financial reports and important documents has been stolen , encrypted

if you willing to continue your bussines and make more money and keep bussines secret safe you need to restore your files first, And to r
don't bother your self and wast your time or make it more harder on your bussines , we developed a locker that can't be decrypted using

making your self geek and trying to restore the files with third part decrypter this will leads to lose all your date ! and then the even you

to chat with us :

1 - Download tor browser https://www.torproject.org/download/
2 - go to one of these links above
http://vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd.onion
http://vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid.onion
http://vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad.onion
http://vanheltarnbfjhuvggbncniap56dscnzz5yf6yjmxqivqmb5r2gmllad.onion

3 - you will be asked for your ticket id to enter the chat this for you : TICKET ID

usefull links :
#OUR TOR BLOG :
http://vanhelvuuo4k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd.onion
http://vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad.onion
http://vanhelxjo52qr2ixcmtjayqqrcodkuh36n7uq7q7xj23ggotyr3y72yd.onion

README.txt

Extension

.vanhelsing, .vanlocker

Production Language

C/C++

Figure 8. Overview of Vanhelsing Ransomware

Vanhelsing Ransomware Strategy

Figure 9. Vanhelsing Ransomware Attack Strategy

The Vanhelsing ransomware is capable of utilizing a variety of execution parameters to determine the targets and methods of encryption, as well as to decide whether to enable functions such as changing the desktop background or deleting backup copies. However, there is a discrepancy between the help messages displayed by the ransomware and the actual parameters used; some parameters are merely verified without being employed, and in some instances, the functionalities are not implemented. The parameters and functionalities that are actually verified are as follows in the table below.

Parameters	Description
-h	Display help for command-line parameters
-v	Display logs
--skipshadow	Skip deleting Volume Shadow Copy(VSC)
--Driver <driver>	Encrypt only specified drives
--Directory <directory>	Encrypt only specified folders
--File <file>	Encrypt only specified files
--Force	Allow concurrent execution of the ransomware
--no-priority	Skip setting ransomware priority
--no-wallpaper	Skip changing the desktop background
--no-local	Skip encrypting local files
--no-mounted	Encrypt only fixed local drives
--no-network	Skip encrypting network shared folders
--spread-smb	Propagate within the internal network
--no-logs	Disable log output
--no-admin	Execute regardless of administrative privileges
--Silent	Bulk convert file extensions after encrypting all target files
--system	Feature not implemented
--no-autostart	Feature not implemented
--spread-vcenter	Feature not implemented

Table 1. Execution Parameters of Vanhelsing Ransomware

Upon verifying the execution parameters, several measures are undertaken to prevent errors during the encryption process. These include changing the desktop background and icon, and accessing network shared folders, which necessitate administrative privileges. Consequently, it is essential to ascertain whether the ransomware is currently running with administrative rights. If it is not executing under administrative privileges, the ransomware will terminate, unless the "--no-admin" Parameter is employed, which allows the ransomware to continue operating without administrative rights. Additionally, to prevent the ransomware from executing multiple instances, a mutex[9] is created using the string "Global\\VanHelsing". To enhance the encryption speed, the ransomware's process priority is set to the highest level. Both of these functionalities can be deactivated using the "--Force" and "--no-priority" parameters, respectively.

Additionally, the encrypted files are rendered irrecoverable by the user through the deletion of backup copies. Similarly, employing the "--skipshadow" Parameter prevents the deletion of these backup copies. The command used to delete the backup copies is as follows.

cmd.exe /c C:\\Windows\\System32\\wbem\\WMIC.exe shadowcopy where "ID='%s'" delete

Table 2. Command for Deleting VSC

When the "--spread-smb" Parameter is employed, propagation within the internal network becomes feasible. To execute ransomware on PCs or servers connected to the internal network, psexec[10] is utilized. This program is stored alongside the ransomware, hence it is saved in a temporary folder before being deployed.

```
network_list = WSAStartup_sub_40CA90(pMemoryBlock: pMemoryBlock_1);
GetTempPathW(nBufferLength: 0x1F4u, lpBuffer: temp_path);
m_format_string_sub_40D890(Buffer: psexec_path, Format: L"%s\\psexec.exe", temp_path);
m_print_message_sub_4011D0(L"[*]\tpsexec_path : %s \n");
memset(buf: stream, value: 0, n0x20: 0xB0u);
m_wfsopen_sub_40BB30(buf: stream, Buffer: psexec_path, n48: 0x30, v43, Buffer: psexec_path);// open %TEMP%psexec.exe stream
m_write_stream_sub_40BD50(this: stream, &psexec_data, 0xAED90i64);
m_close_stream_sub_406660(buf: stream);
```

Figure 10. Storage of psexec

[9] Mutex: synchronization mechanism that prevents multiple threads or processes from accessing a shared resource simultaneously, often used in ransomware to block duplicate executions.

[10] psexec: Tool designed for remotely managing and launching processes on Windows platforms via the command line.

After saving psexec, the next step is to retrieve the IP address of the system running the ransomware. Then, the final octet[11] is varied from 1 to 255 to determine if any internal network addresses are reachable. Once a reachable address is identified, the ransomware is copied to a network folder on that address with write permissions and renamed 'vanlocker.exe'. Using psexec, the ransomware is then executed on PCs or servers connected to the internal network. During this operation, the execution parameters '--no-mounted' and '--no-network' are used, and the following command is executed:"

```
cmd.exe /c %TEMP%psexec.exe -accepteula \\${shared_folder} -c -f
${shared_folder}\vanlocker.exe -d --no-mounted --no-network < NUL
```

Table 3. Internal Propagation Commands

In addition to propagation within internal networks, the configuration of targets for file encryption can be facilitated through various execution parameters, which are primarily categorized into files, folders, local drives, and network shared folders. Utilizing the "--File" Parameter encrypts only a single specified file, whereas the "--Directory" Parameter encrypts the designated folder along with all its subfolders, and the "--Driver" Parameter encrypts the entirety of the specified drive. Should no encryption-related execution parameters be employed, all drives and network shared folders are encrypted. Moreover, the use of the "--no-network" Parameter deactivates the encryption of network shared folders, the "--no-local" Parameter omits the encryption of local files, and the "--no-mounted" Parameter enables the encryption of solely the fixed local drives.

[11] Octet: 8-bit unit used to represent a 32-bit IP address by partitioning it into 8-bit segments.

Once the encryption targets have been established, each directory is traversed to ascertain whether it corresponds to an exception item. Initially, it is imperative to verify if the target directory itself is an exception item. Upon completion of this directory verification, it is then necessary to determine whether each file within the directory qualifies as an exception item. The encryption exceptions under consideration are outlined in the table below.

Directory Name	File Extension and File Name
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, Trend Micro, program files, program files(x86), tor browser, windows, intel, all users, msocache, perflogs, default, microsoft	.vanlocker, .exe, .dll, .lnk, .sys, .msi, .bat, .bin, .com, .cmd, .386, .adv, .ani, .cab, .ico, .bod, .msstyles, .msu, .nomedia, .ps1, .rtp, .syss, .prf, .deskthemepack, .cur, .cpl, .diagcab, .diagcfg, .dll, .drv, .hlp, .pdb, .hta, .key, .lock, .ldf, .icns, .ics, .idx, .mod, .mpa, .msc, .msp, .nls, .rom, .scr, .shs,. spl, .theme, .themepack, .wpx, boot.ini, autorun.inf, bootfont.bin, bootsect.bak, desktop.ini, iconcache.db, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini, thumbs.db, GDIPFONTCACHEV1.DAT, d3d9caps.dat, LOGS.txt, .README.txt

Table 4. Exceptions to Encryption

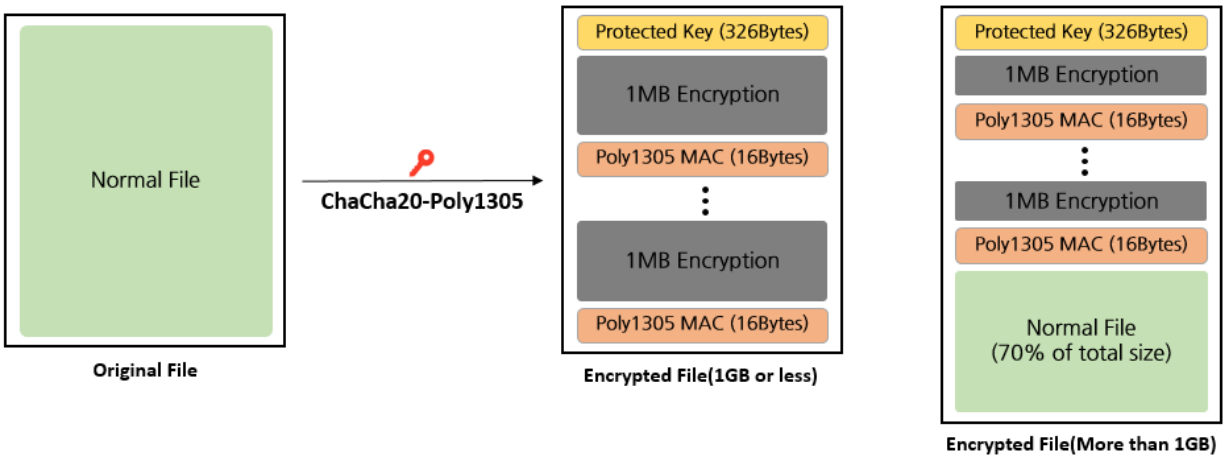


Figure 11. File Encryption Methods by Size

File encryption involves encrypting the entirety of files smaller than 1GB, while for files exceeding 1GB, only 30% of their total size is encrypted. For each file, a random 32-byte key and a 12-byte nonce are generated, and the file is encrypted using the ChaCha20-Poly1305 algorithm. The encryption process is conducted in 1MB increments. Owing to the characteristics of the ChaCha20-Poly1305 algorithm, a Message Authentication Code (MAC) is generated to ensure data integrity. Consequently, each 1MB segment of the encrypted file includes a 16-byte MAC stored alongside it.

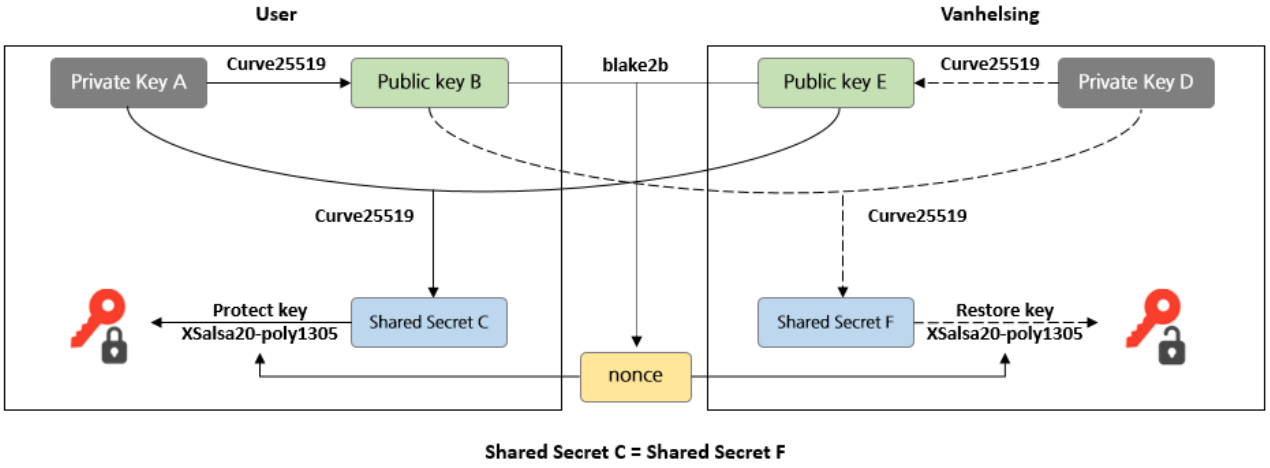


Figure 12. Key Protection Methods

Additionally, the key used for encryption is safeguarded by being stored at the beginning of the file, employing a method that utilizes a shared secret generated via Curve25519 to protect the encryption key and nonce, while concurrently storing the user's public key, which enables key recovery. Separate from the file encryption key, a unique random private key is generated for each file, thereafter, a shared secret can be created using the hardcoded public key of Vanhelsing. This leverages the characteristic of Curve25519, where the shared secret produced using one's private key and another's public key is identical to that generated using one's public key and another's private key. For key protection, the XSalsa20-Poly1305 algorithm is employed, which, in addition to the key, requires supplementary data to be used as a nonce. The nonce is formed by concatenating the user's public key with Vanhelsing's public key, followed by generating a 12-byte hash using the blake2b algorithm.

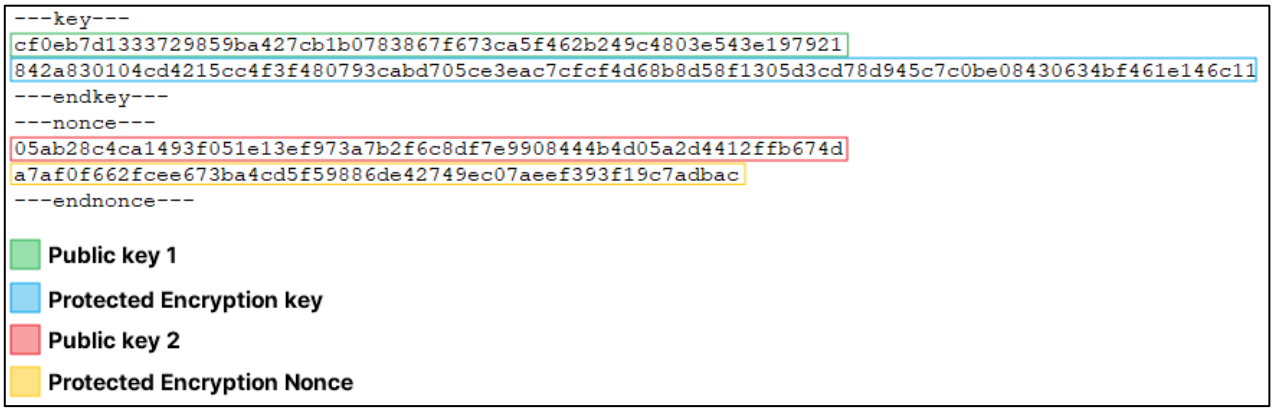


Figure 13. Protected Key Storage Methods

The protected key is stored at the forefront of the encrypted file in text form, alongside the public key intended for recovery. Distinctions are made between the utilized key and nonce, indicated as ---key---, ---nonce---, and the public key and protected key are sequentially saved.

Figure 14. Altered Desktop Background

Following the encryption of files, the ransomware modifies the desktop and the icons of encrypted files to those stored within its own repository, specifically using image and icon files. The desktop wallpaper is altered to "vhlocker.png," and the icon image is changed to "vhlocker.ico." Utilizing the "--no-wallpaper" Parameter precludes alterations to the desktop wallpaper and icon imagery.

Strategies for Responding to Vanhelsing Ransomware

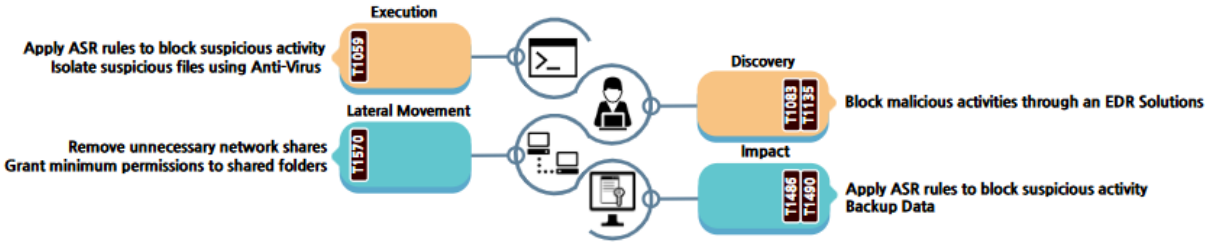


Figure 15. Response Strategies for Vanhelsing Ransomware

The Vanhelsing ransomware utilizes the Windows command prompt to execute commands for deleting backup copies and facilitating internal propagation. Consequently, by activating ASR (Attack Surface Reduction) [12] rules, one can obstruct anomalous processes and thus thwart malicious activities. Additionally, since the ransomware stores programs in temporary folders or replicates itself in network-shared folders, employing Anti-Virus software enables the isolation of suspicious files.

To facilitate encryption for internal dissemination and network shared folders, the current system's internal network bandwidth is explored, and attempts are made to access connectable network addresses and shared folders. Moreover, in the case of file encryption, all drives are scanned and, based on execution parameters, the drives to be encrypted are distinguished. Through the implementation of an Endpoint Detection and Response (EDR) solution, it is possible to thwart the malicious activities of attackers.

Additionally, internal propagation is feasible as ransomware is copied to a shared folder with write permissions before execution; thus, if no separate access rights are granted, it is possible to block internal propagation. Therefore, one strategy involves minimally granting access permissions to network shared folders. Furthermore, if network services such as network shared folders are unnecessary, it is imperative to either disable the service entirely or block the SMB port (445) to minimize damage.

To prevent unauthorized restoration of encrypted files, the ransomware deletes all system backup copies before starting encryption. Enabling ASR rules can block both the deletion of backups and the encryption process. In addition, backups should be stored on separate networks or storage systems to ensure recovery even if the system is compromised."

[12] ASR (Attack Surface Reduction): protective feature that blocks specific processes used by attackers and executable processes.

IoCs

Hash(SHA-256)
86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17
99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98

■ Reference

• BleepingComputer (https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/)

• Cyber Daily (https://www.cyberdaily.au/security/11919-exclusive-contractor-brighton-australia-listed-on-safepay-s-ransomware-leak-site)

• S-rm (https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/ransomware-gang-encrypted-network-from-a-webcam-to-bypass-edr/)

• Trend Micro (https://www.trendmicro.com/en_us/research/25/c/socgholishs-intrusion-techniques-facilitate-distribution-of-rans.html)