Keep up with Ransomware

Threat of 8Base ransomware to small-and-medium-sized businesses

■ Overview

In April 2024, the reported cases of damage caused by ransomware numbered 385, a decrease of 20 cases compared to the previous month (405 cases), despite active attacks by new ransomware groups. This is because attacks by the LockBit ransomware group, which had caused a lot of damage previously, were down by half compared to the previous month.

The RansomHub ransomware group attracted attention by posting data related to an exit scam[1] by the BlackCat(Alphv) ransomware group. This data was leaked from Change HealthCare, an American healthcare system company. Last February, an attack by BlackCat(Alphv) caused a disruption in Change HealthCare's system operations, and the attacker threatened to disclose 4TB of data containing personal information. Change HealthCare deposited $22 million (approximately KRW 30 billion) into the Bitcoin wallet designated by BlackCat(Alphv) to solve the problem, but BlackCat(Alphv) disappeared in an exit scam. After BlackCat(Alphv) disappeared, affiliates who had signed contracts with the organization did not receive any money, and it appears that one of these affiliates joined the RansomHub group and posted the Change HealthCare data he or she had.

The HelloKitty ransomware group returned with a new name, HelloGookie, after a hiatus of about six months. They released decryption keys and some of the data used by the HelloKitty ransomware group through a new dark web leak site, including data from CD Projekt RED, a Polish game developer and distributor, and the source codes of some games. They appear to be preparing for full-fledged activities as they promote their new leak site and recruit employees through dark web forums.

The LAPSUS$ ransomware group suspended its activities in September 2022, but returned to business in December and began selling ransomware services and source codes in March of this year. From 2021 to September 2022, the LAPSUS$ group mainly carried out activities such as infiltrating

[1] Exit Scam: A fraudulent practice in which a ransomware group collects money from ransomware victims and then disappears without paying fees to affiliates or returning files

networks or stealing accounts and data from famous companies such as NVIDIA and Microsoft. Since becoming active again, the LAPSUS$ ransomware group has continued to distribute ransomware and provide updates, and it began full-fledged activities in April by improving encryption speed. In addition, the group recently began selling a version of Exploit[2] that allows users to download and execute of ransomware through vulnerabilities in MS Word documents (.doc). Caution is required, as the LAPSUS$ group is known to be a notorious attack organization that has hacked famous companies in the past.

Trisec, a Tunisia-based ransomware group, appeared in February of this year, but appears to have ceased activities in April. They posted three attack cases in February, but nothing else since, and their dark web leak site was deactivated in April. In addition, no additional posts have appeared on the dark web forum other than the promotional posts from February for member recruitment and the dark web leak site. Taking all the above into account, it appears that they have virtually ceased activities.

Meanwhile, the threat of ransomware that can infect multiple virtual servers through a single attack on ESXi[3] continues. The SEXi ransomware first surfaced in April when it infected Chilean web services hosting company IxMetro PowerHost. The SEXi ransomware group does not own a separate dark web leak site, and negotiates through the Session Messenger[4] app address listed in the ransom note. The amount of ransom they demanded was revealed to be $140 million (approximately KRW 191.5 billion), but it has been confirmed that IxMetro PowerHost did not pay.

The 8Base ransomware group posted data of a Korean paint-related manufacturer on a dark web leak site in early April. 8Base is a ransomware group that mainly targets small and medium-sized businesses with relatively weak security. The posted data included sensitive information such as invoices and accounting data, personal information, certificates, and confidential documents. The documents were released on April 8, and the download link is now expired.

---

[2] Exploit: A type of attack that allows an attacker to perform an intended action by exploiting a bug or security vulnerability in software or hardware

[3] ESXi: A UNIX-based logical platform used to run multiple operating systems simultaneously on a host computer developed by VMware

[4] Session Messenger: A decentralized messenger with no central server to manage. This messenger uses a separate Session ID instead of an account for communication.

■ Ransomware news

infosec

Change HealthCare attacked by RansomHub again.

- A victim associated with the exit scam of BlackCat(Alphv) group, and a data sale post published on RansomHub DLS.
- RansomHub claims that they were able to obtain data because affiliates joined after the BlackCat(Alphv)'s exit scam.
- They incurred losses of $872M due to ransom payments, attack response, and business disruptions.

INC Ransom attacks Leicester City Council.

- It is related to the disruption of key services(e.g. child protection, social welfare) of Leicester, UK, in March.
- Leicester City Council's IT infra restored, but they've discovered an extra 1.3TB of exposed data.

LockBit exposes data of Washington D.C. State *DISB.

- Posted on LockBit DLS on April 13th, confirmed by DC DISB that it leaked through a private cloud.
- Details of negotiation undisclosed; the data released on April 23rd indicated the breakdown of negotiations.

* DISB : Department of Insurance, Securities and Banking

New Psoglav ransomware group recruiting partners.

- The ransomware is developed in C#, and they have disclosed its key features and partner recruitment criteria.
- They have set a decryption cost of $ 150 per ID and they are recruiting partners for long-term collaboration.

HelloKitty ransomware has disclosed its decryption key and rebranded as HelloGookie.

- Active from November 2020 to October 2023, with a history of attacking the CD Projekt Red.
- Returning as HelloGookie, they've released data from CD Projekt Red, Cisco internal data, and decryption Key.
- Posting "Caller" recruitment ad on XSS forum.

LAPSUS$ group begins selling ransomware.

- Active from 2021 to September 2022, they resurfaced with the same name in December 2023.
- They claims to be the same LAPSUS$ group that ceased activity a year ago.
- They began selling ransomware in March 2024 and have been updating with added features or improvements.

The Trisec ransomware group's DLS has been deactivated.

- A Tunisia-based group emerged in February 2024, posting about three victims.
- All three active DLS domains deactivated, suggesting cessation of operations.

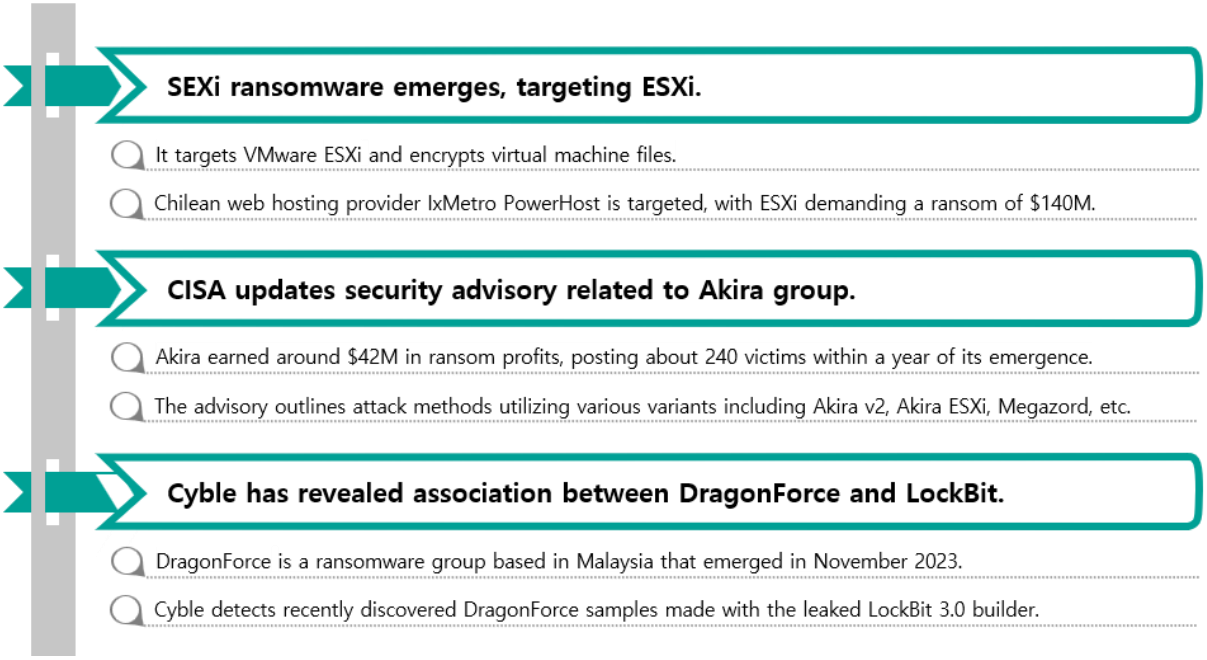


Figure 1. Ransomware trends

■ Ransomware threats

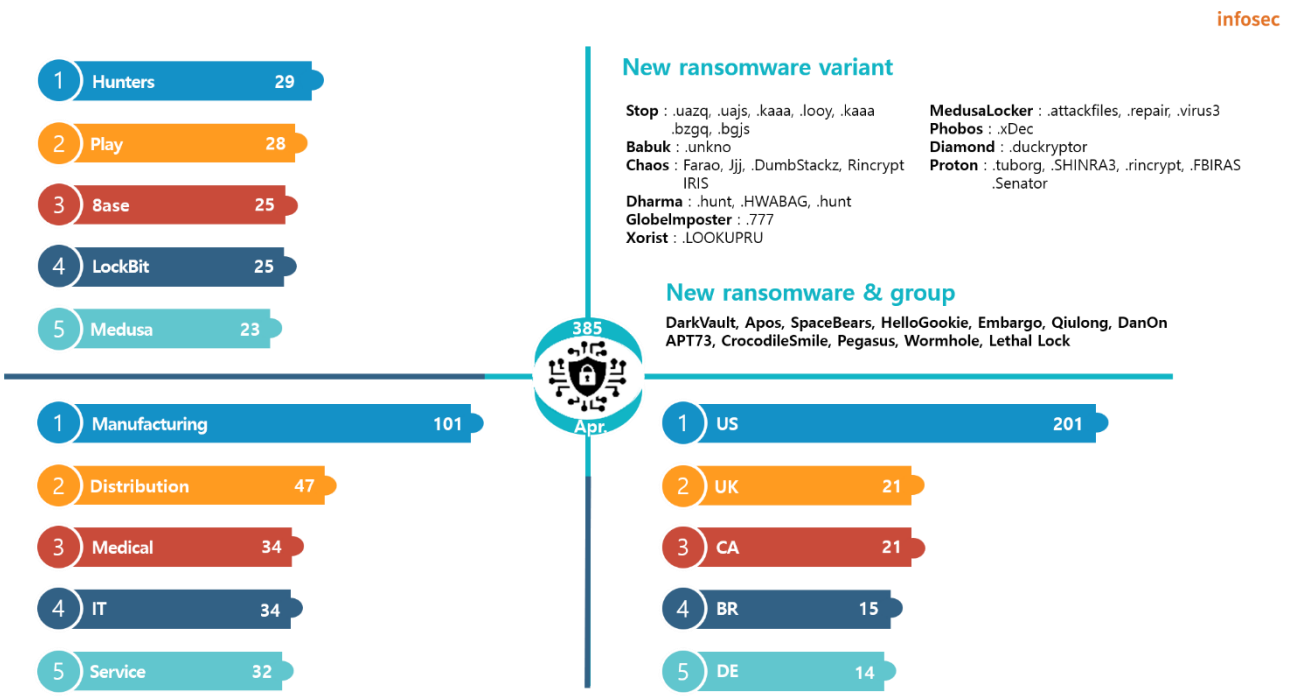


Figure 2. Ransomware threats status as of April 2024

New threats

In April, it was discovered that several ransomware groups, including a number of new ones, were preparing for full-fledged activities such as selling ransomware and recruiting partners. On a Russian hacking forum posts were found advertising the Ultra ransomware, which can infect Windows, Linux, and ESXi systems, as well as posts recruiting long-term partners posted by the Psoglav ransomware group. In addition, it was discovered that the LAPSUS$ group has been selling and continuously updating its ransomware for Windows since March.

The HelloKitty group, which suspended its activities in October 2023, has reappeared with the new name HelloGookie. 'kapuchin0,' presumed to be a HelloKitty administrator, disclosed the group's ransomware source code on the XSS forum, a Russian hacking forum, before they suspended activities. Approximately five months later, they announced their return by posting a new dark web leak site address. On the new site, they revealed the decryption key used for the HelloKitty ransomware and posted NTLM hash[5] data obtained from Cisco during their time as HelloKitty along with a torrent magnet address[6] where the source codes for the CD Projekt Red games The Witcher 3, Cyberpunk,

[5] NTLM hash: Hash value used instead of a password for NTLM (NT LAN Manager), the Windows authentication protocol

[6] Torrent magnet address: URI schema that can be used instead of a torrent file in Torrent, a protocol or program that allows users to share files directly with each other

and Gwent were stored. In addition, based on posts on the XSS forum requesting contact with the LockBit and Yanluowang/Saint groups and recruiting employees, they appear to be preparing for full-scale activities.

On top of existing groups resuming activities, many new ransomware groups have also been discovered. In April, seven new dark web leak sites were discovered. The Apos ransomware group posted its victims on Notion,[7] an unusual case. However, the page was deleted as of April 30, and no additional activity has been found since then. The Qiulong ransomware group has focuses its attacks on specific countries and industries. All six victims posted were Brazilian companies, and five of them were medical service-related companies. Unusually, the group posted as samples photos that explicitly revealed patients bodies.

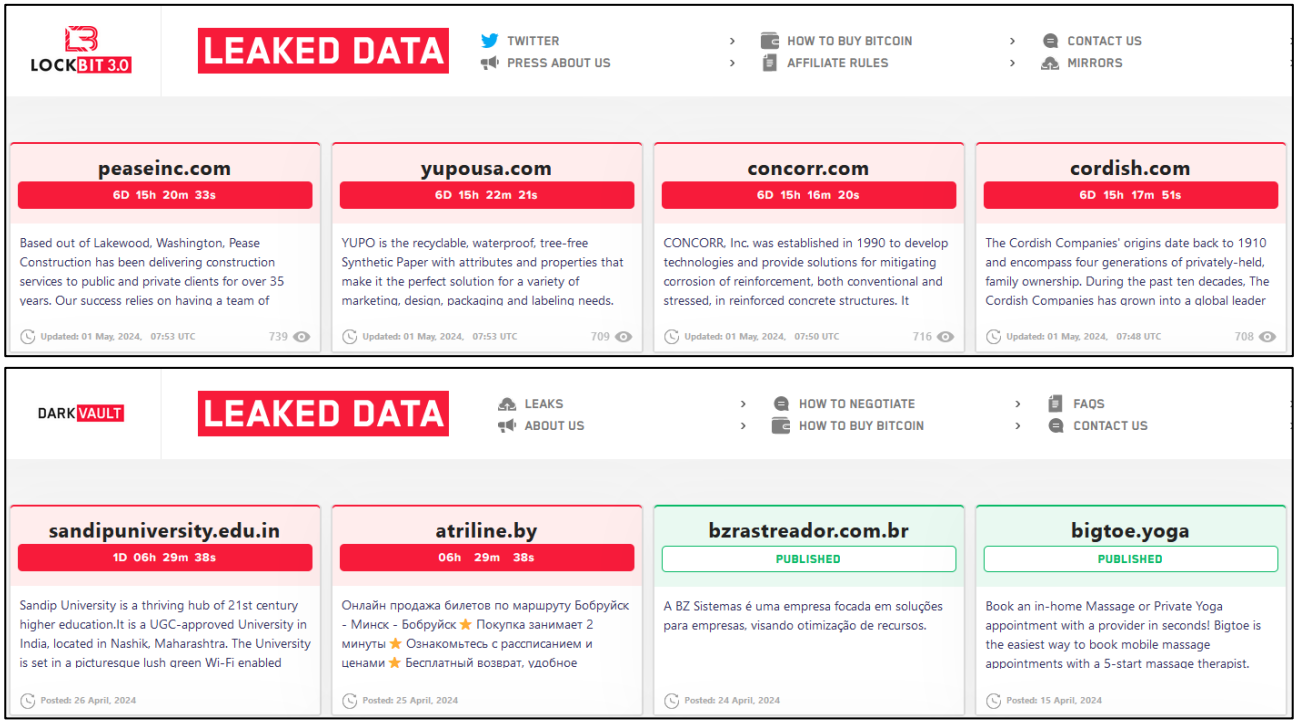


Figure 3. Comparison of dark web leak websites (top: LockBit 3.0, bottom: DarkVault)

[7] Notion: An all-in-one application that provides notes, databases, Kanban boards, Wikis, calendar, etc.

In addition, groups with leaked pages with a similar design and structure to those of the LockBit ransomware group were discovered. The APT73 (Eraleign) ransomware group opened and then closed a clear web leak site,[8] but are currently posting data on dark web leak sites. A dark web leak site belonging to the DarkVault group, which began operating in February, was discovered in April. This leak site uses a similar design, including logo, to LockBit's dark web leak site, and the contents of the bug bounty[9] page. Therefore, this group appears to be imitating the LockBit group.

[8] Clear Web: General information found with search engines

[9] Bug Bounty: A system that provides compensation to people who find security vulnerabilities in software or systems

Top 5 ransomwares

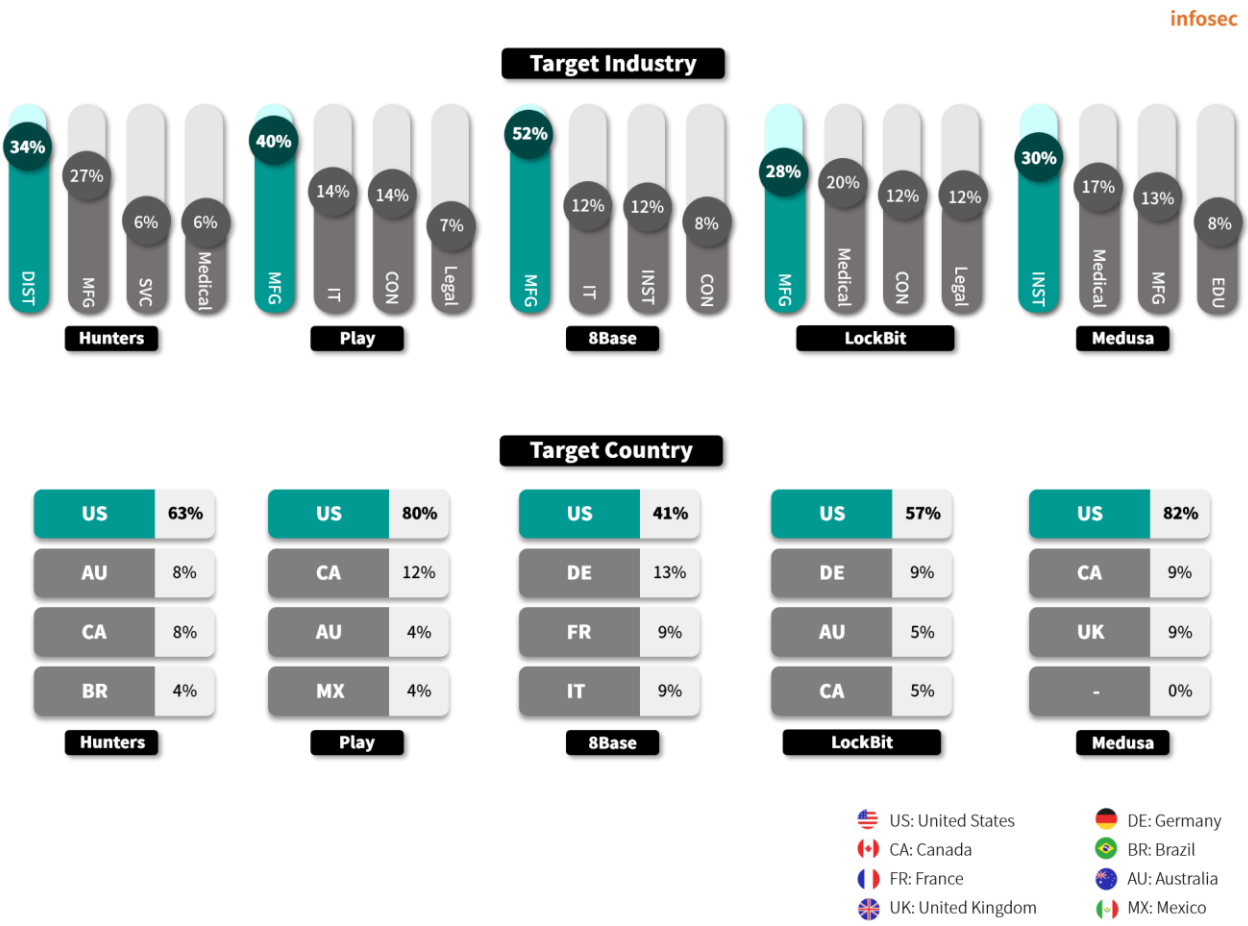


Figure 4. Major ransomware attacks by industry/country

The Hunters ransomware group, which has been active since October 2023, has posted about 120 leaks so far. In April, they attacked Chicony Electronics, a Taiwanese electronic component manufacturer, and posted data from the attack on a dark web leak site. The data they posted includes data from Korean companies as well as many famous companies such as American camera brand GoPro, aerospace company SpaceX, and electronics manufacturers DELL, HP, and Google. Chicony Electronics is a company that mainly manufactures and supplies computer/laptop components and imaging devices, and therefore, information such as product blueprints of the above-mentioned companies is likely to have been leaked. The Hunters group is demanding $3.3 billion (about KRW 4.51 trillion) in return for preventing data leaks.

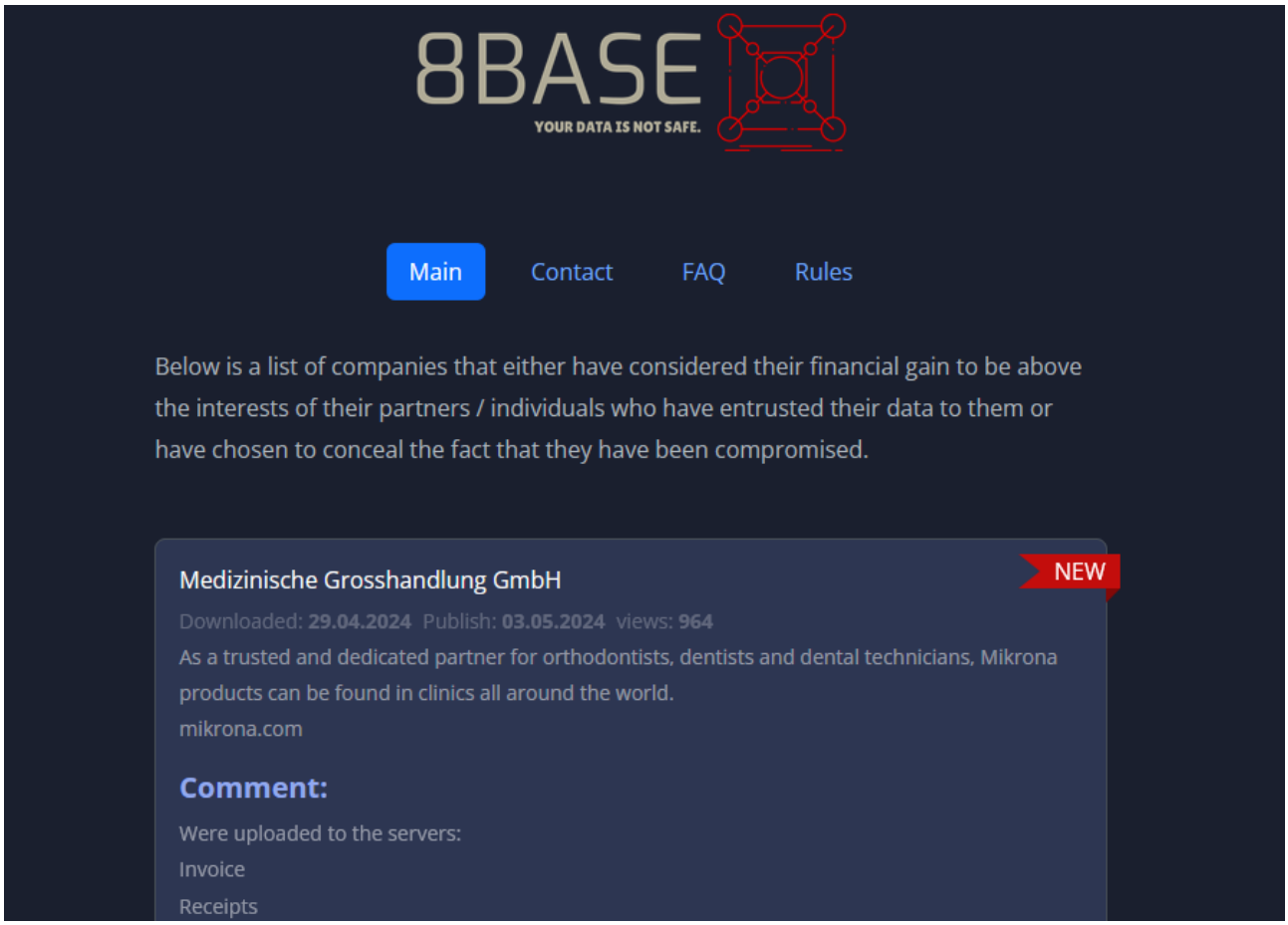
The LockBit ransomware group, whose infrastructure was confiscated by Operation Cronos[10] in February of this year, has since made a quick return, but their activity is gradually decreasing. In February, when their infrastructure was confiscated, they posted 100 leaks, showing off their health by posting leaked data immediately after the infrastructure was restored. However, they posted 55 posts in March, down about 50% from February, and only 25 posts in April, down about 55% from March. This appears to be a result of Operation Cronos. LockBit also told its affiliates, "We would like to remind all partners that discounts of over 50% are strictly prohibited." Based on this, it appears that they are focusing on profits rather than securing affiliates. They appear to be taking a tough stance, unlike many ransomware groups that return a lot of profits to their affiliates.

Most ransomware primarily targets manufacturers and distributors with relatively weak security. The Hunters ransomware group has the highest rate of attacks on retailers at 34%, while the Play ransomware group and LockBit ransomware group have the highest rates of attacks on manufacturers at 40% and 28%, respectively. The 8Base ransomware group mainly targets small-and-medium-sized businesses with relatively weak security, and in particular, half of the attacks in April on small and medium-sized businesses targeted manufacturing businesses. Meanwhile, the Medusa ransomware group shows a slightly different attack pattern than other ransomware groups, mainly targeting medical institutions, government institutions, and educational institutions. Of the attacks carried out by the Medusa ransomware group in April, 53% were against medical institutions, government agencies, and educational institutions, which is 33 percentage points higher than the average of 20% for attacks in these fields by other groups.

[10] Operation Cronos: An operation in which international investigative agencies coordinated to destroy criminal infrastructure, including LockBit's attack servers and dark web leak sites

■ Ransomware in focus

Outline of the 8Base ransomware



Source: 8Base ransomware group data leak website

Since its emergence in March 2022, the 8Base ransomware group has posted about 380 attack cases on dark web data leak sites. They launched a dark web data leak site in May 2023 and have posted attack cases in batches, including 47 cases in June of the same year, when they began full-fledged activities. In particular, in April 2024, a Korean paint manufacturing company was posted on the dark web leak site. This company's accounting data, personal information, and confidential documents were leaked, showing that 8Base ransomware group could also have an impact on Korea.

Figure 5. Comparison of encryption extensions (left: Phobos, right: 8Base)

Currently, 8Base is using the Phobos-based ransomware discovered in 2019. The Phobos ransomware is a variant of the Dharma/Crysis ransomware that was disguised as a file management program when it was distributed in Korea, and Phobos variants with different extensions are continuously appearing. 8Base used Phobos version 2.9.1, which is why it is similar to Phobos ransomware, not only in source code, but also in the content and design of the ransom note and the method of adding the drive volume ID and attacker's email before the encryption extension. In addition, the encryption exceptions include the extensions of other Phobos variants, and 8Base uses the same RSA public key as Phobos ransomware, which shows the relationship between 8Base and Phobos ransomware.

In November 2023, in addition to the .NET[11]-based ransomware that 8Base had been using until then, a variant distributed using SmokeLoader was discovered. SmokeLoader, which is downloader malware, can access the C2 server[12] and download additional tools or malware according to commands. 8Base's SmokeLoader variant uses the payload stored inside SmokeLoader or accessed the C2 server (command & control server) to download, decrypt, and then execute the encrypted ransomware payload.[13] The final ransomware payload executed is a variant of the Phobos ransomware that is identical to the .NET-based ransomware.

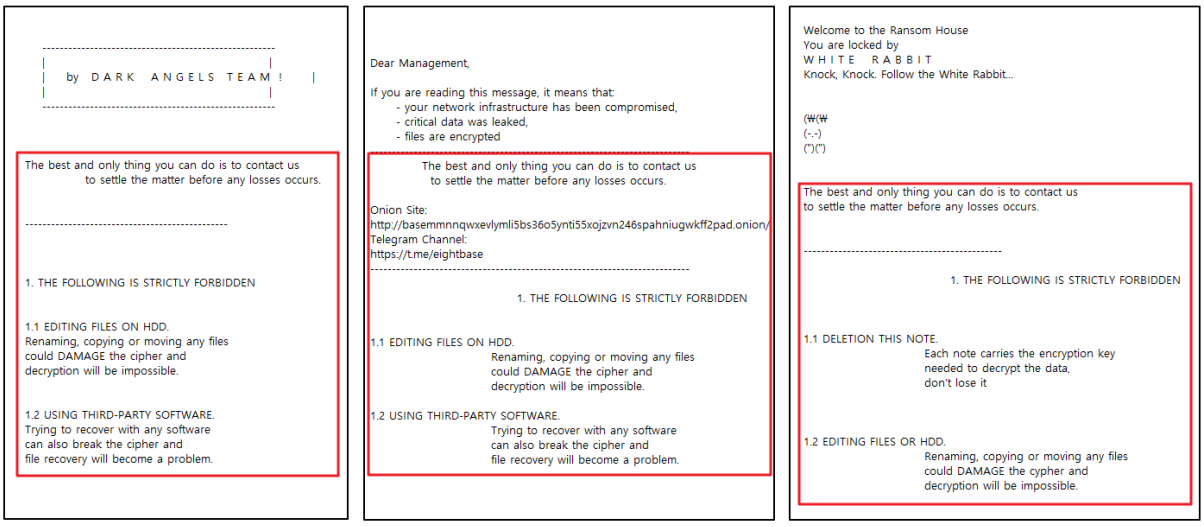


Figure 6. Comparison of ransom notes (left: DarkAngels, center: 8Base, right: RansomHouse)

[11] .NET: A Windows program development and execution environment (framework) developed by MS

[12] C2 Server(Command & Control Server): A server on which an attacker maintains communication with or passes commands to the device that he/she initially penetrated

[13] Payload: Code designed to penetrate, alter, or otherwise damage a computer system

8Base was found to be related to various groups in addition to the Phobos ransomware. The ransom note discovered around May 2023, when these groups ramped up activities, is very similar in content to the ransom note of the DarkAngels ransomware and RansomHouse(Mario/WhiteRabbit) ransomware using the leaked Babuk builder, although this is not currently being used in attacks. In addition, the main page, FAQ page, and text of the rules page of the 8Base group's dark web data leak site are similar to those of the RansomHouse group's site.

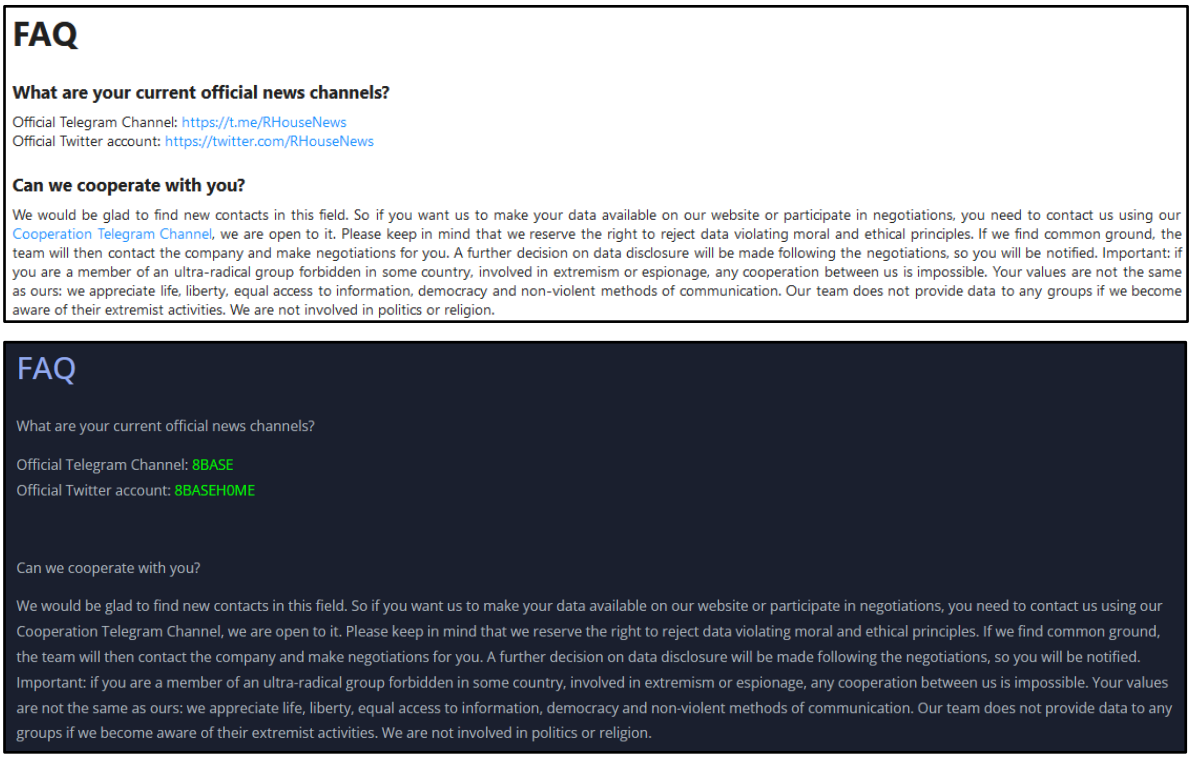


Figure 7. Comparison of dark web leak websites (top: RansomHouse, bottom: 8Base)

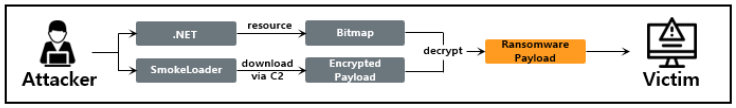
Because a similar type of ransom note was discovered and the phrases on the dark web leak site were similar, there was an opinion that the 8Base group was derived from the RansomHouse group or a rebranded[14] RansomHouse group. However, since it is not uncommon to quote or copy phrases from other groups and use leaked tools, there is not enough evidence to determine their connection.

[14] Rebranding: The act of attackers shutting down operations and then restarting them under a new name

8Base Ransomware

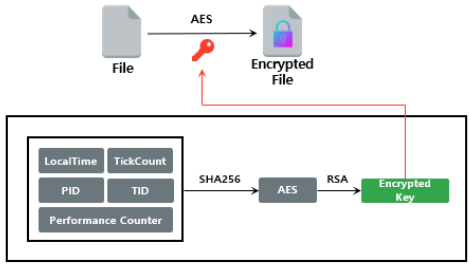
Attack Scenarios

Distribute ransomware through .NET forms or SmokeLoader variants.



Encryption Key

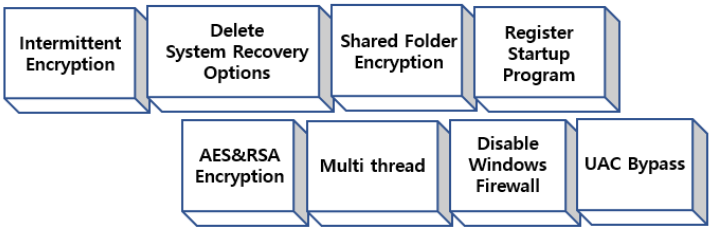
Encrypt files with AES-256(CBC) algorithm and protect the key with RSA-1024



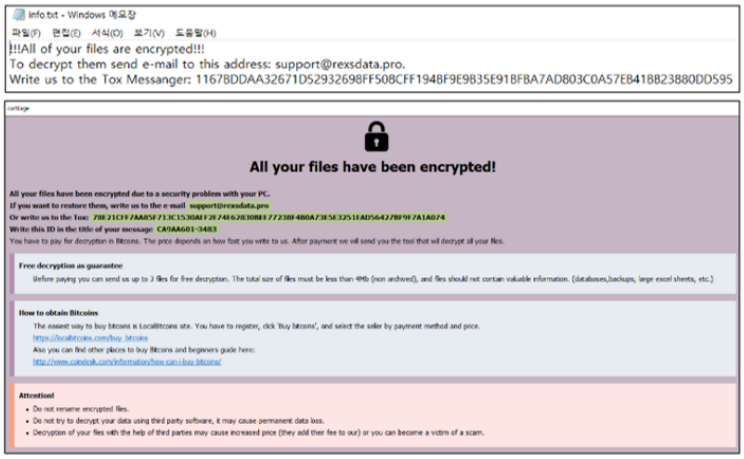
Encryption Method

For files below 1.5MB : Full file encryption
For files 1.5MB or more : After dividing the file into three parts, encrypt only 256KB of each part

Features



Ransom Note



info.txt, info.hta

Extension

Id[A-Z0-9]{8}-[0-9]{4}].[support@rexsdata.pro].8base

Production Language

C# / C++

Figure 8. 8Base ransomware Outline

8Base ransomware strategy

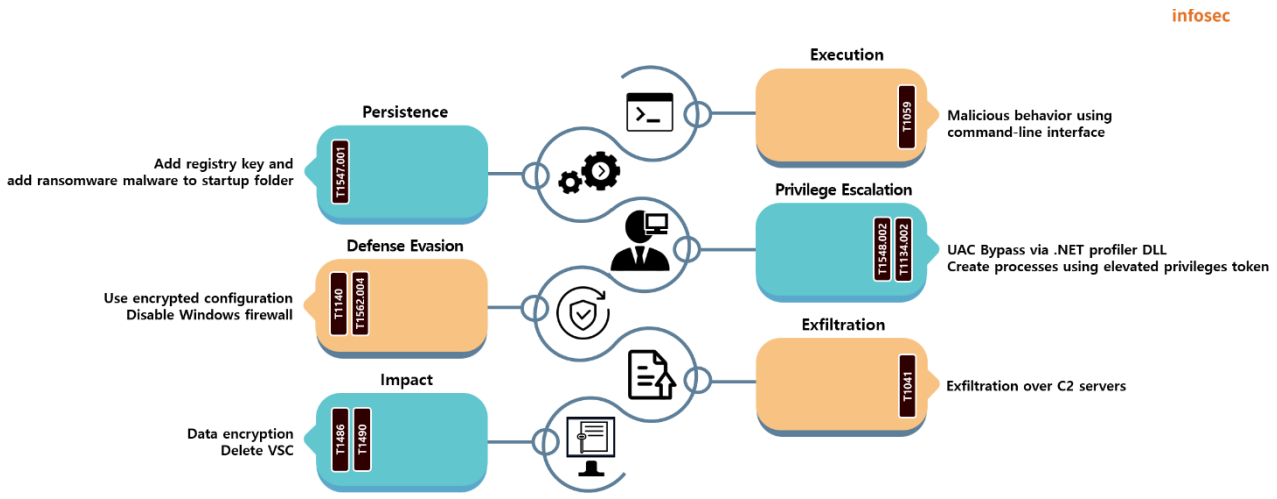


Figure 9. 8Base ransomware attack strategy

The 8Base ransomware group distributes ransomware directly through .NET or by using the downloadable malware SmokeLoader. SmokeLoader downloads the encrypted ransomware payload from the C2 server, then decrypts and executes it. In the case of .NET-based ransomware, the payload is stored in the form of a bitmap file, and is decrypted and executed using a new process. Both of these distribution methods execute the same Phobos variant ransomware payload.

The ransomware payload that is ultimately executed has settings encrypted with the AES-256 (CBC) algorithm and stored in the ".cdata" area. The settings include the following values needed to run ransomware: the RSA public key used for key protection, commands and strings required to elevate privileges or bypass detection, encryption exception files and folders, and the encryption extension. 8Base uses a hard-coded AES key to decrypt and use the setting value whenever it is needed.

To ensure smooth execution even after rebooting, 8Base sets the ransomware to run automatically, acquires administrator privileges, and disables firewalls. To ensure continuity, 8Base copies the currently running ransomware file to the startup folder location and adds it to the registry so that it automatically runs every time the computer boots. In addition, 8Base executes ransomware by duplicating the token of a process with administrator privileges or uses a vulnerability in the .NET profiler DLL loading process[15] to bypass the approval process required to execute administrator

[15] .NET Profiler DLL Loading Process: A process that loads the .NET profiler DLL, a tool for monitoring the execution of other applications

privileges by using the UAC (user account control)[16] bypass with the .NET profiler technique. Lastly, it also has the ability to delete backup copies and disable firewalls through the command-line interface.[17]

File encryption encrypts the target PC's drive as well as network-shared folders. 8Base uses the AES-256 (CBC) algorithm for file encryption, and randomly generates the AES key used for encryption before creating the encryption thread. Since different keys are not used for each file, 8Base solves the key duplication problem by randomly generating an IV (initialization vector)[18] for each file. The AES key and IV used for encryption are protected with the RSA public key stored in the settings, and are added to the end of the encrypted file.

infosec

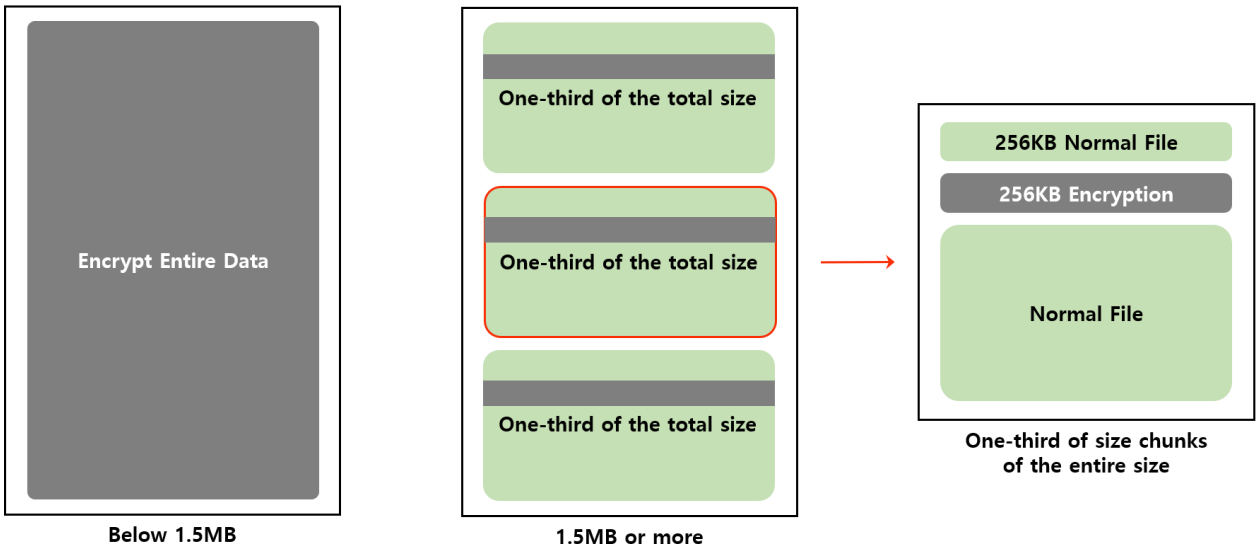


Figure 10. 8Base ransomware's partial encryption method

8Base ransomware uses partial encryption as well as multi-threading for efficient encryption. If the file is smaller than 1.5MB, 8Base encrypts the entire file, and if it is larger than 1.5MB, it divides the file into three parts of equal size and encrypts only 256KB in each area.

[16] UAC(User Account Control): A Windows security feature that requests final consent from the user before execution if administrator privileges are required

[17] Command-line Interface: A text-based interface that allows users to enter commands that interact with their computers' operating systems

[18] IV(Initialization Vector): One of the parameters used in block encryption methods, it ensures that the encryption result does not have any pattern.

How to respond to the 8Base ransomware

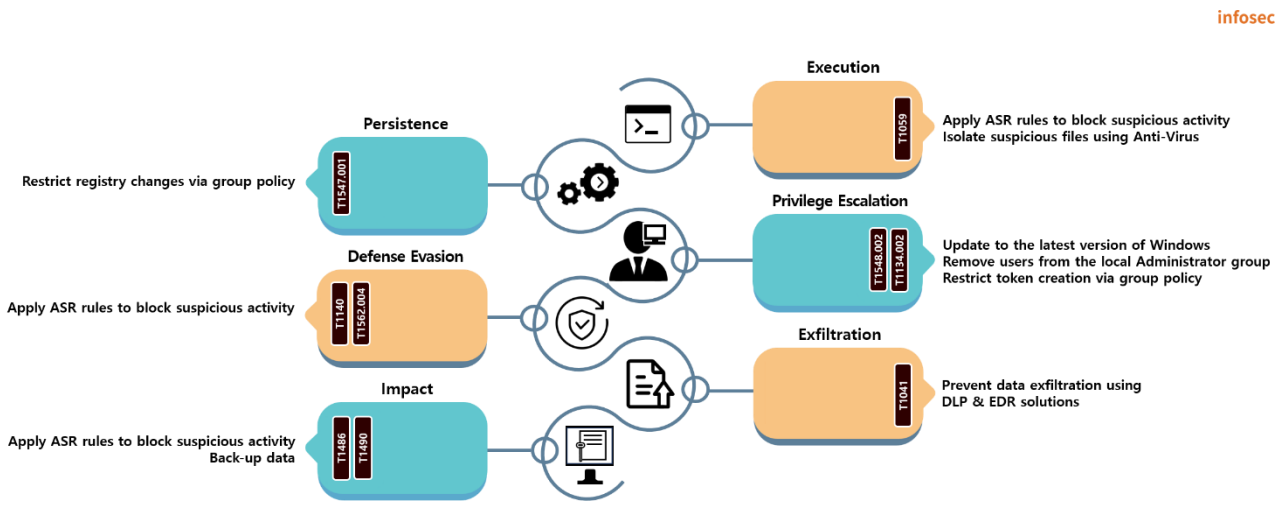


Figure 11. How to respond to the 8Base ransomware

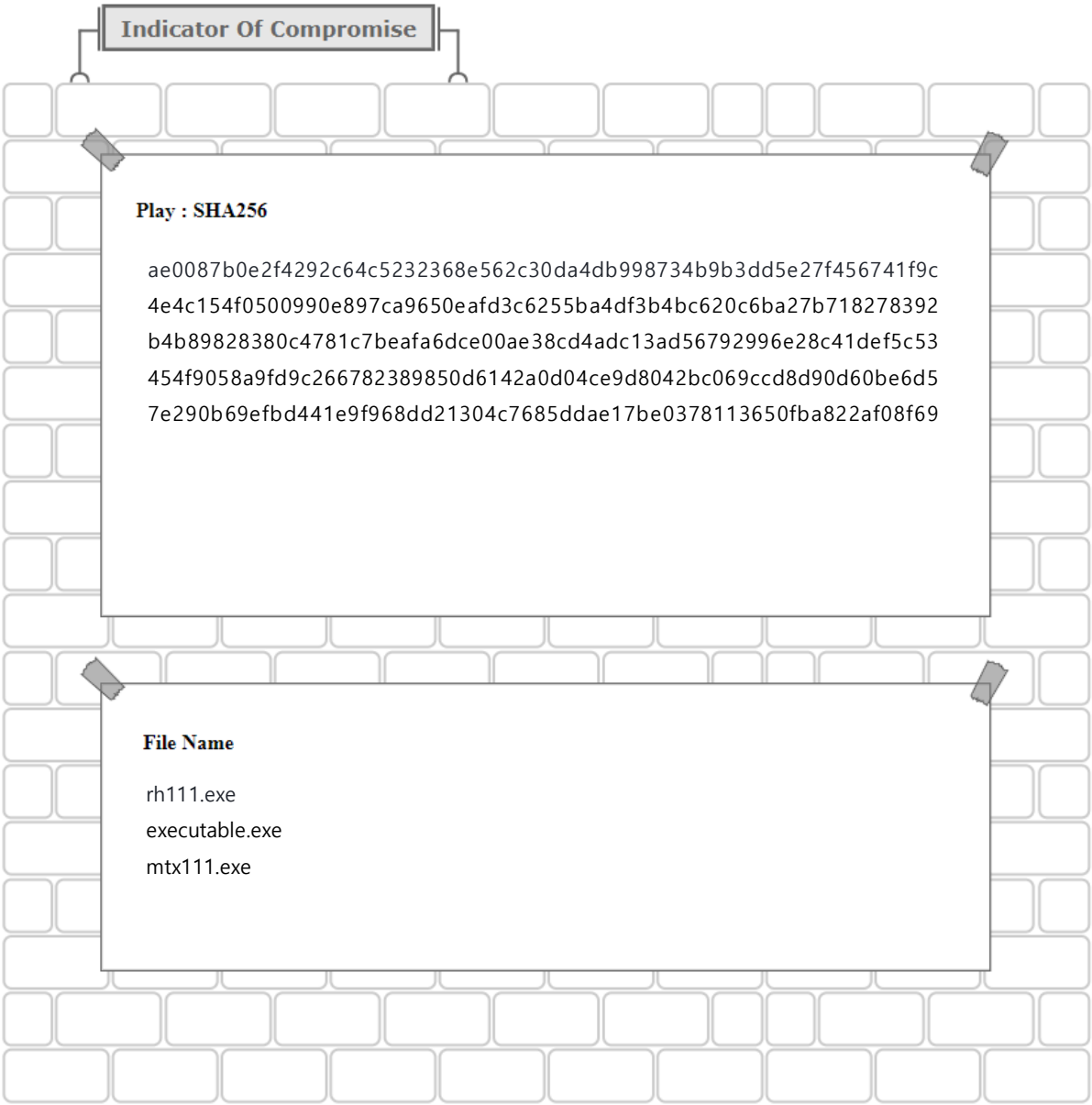
8Base's .NET-based ransomware executes the payload as a new process by decrypting it in memory, and the SmokeLoader variant executes the payload as a new process by downloading the payload from C2 or decrypting the payload stored inside SmokeLoader. Therefore, it is possible to prevent malicious content from being executed through a new process by activating ASR (attack surface reduction) rules[19]. In addition, it is necessary to isolate suspicious files using anti-virus software so that they cannot be executed even if they are downloaded or copied.

To ensure continuous execution, 8Base ransomware copies ransomware files to the startup folder and registers them in the registry so that they automatically run upon booting. Therefore, you can prevent persistence by modifying the Windows group policy to restrict registry editing by non-administrator users.

To perform functions such as encrypting files or deleting backup data, you will need administrator privileges. To this end, 8Base ransomware utilizes the UAC bypass technique or copies the token of a privileged process. It is necessary to update the Windows operating system to a version patched for the bypass technique, or edit the group policy to prevent users from duplicating or creating tokens for other processes.

[19] ASR(Attack Surface Reduction): Technology that blocks the attack path of malicious code

In addition, 8Base ransomware contains encrypted commands that disable firewalls or delete backup data. Because hackers decrypt and use the commands when necessary, the malicious actions must be blocked in advance by activating ASR rules and using EDR (endpoint detection and response) solutions.[20] In addition, you can prevent data leakage by utilizing a DLP (data loss prevention)[21] or EDR solution, and you can respond to file encryption and data deletion in NAS or backup storage by backing up and managing data on a separate network or storage.



[20] EDR(Endpoint Detection and Response): A solution that prevents damage from spreading by detecting, analyzing, and responding to malicious activities occurring on terminals such as computers, mobile devices, and servers in real time

[21] DLP(Data Loss Prevention): A solution that prevents data leaks by monitoring the flow of data and blocking the leakage of important information

■ Reference site

• Leicester City Council, UK (https://news.leicester.gov.uk/news-articles/2024/april/cyber-incident-update-3-april-2024/)

• Leicester City Council, UK (https://news.leicester.gov.uk/news-articles/2024/april/more-data-published-following-leicester-cyber-attack/)

• Security recommendations of CISA (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a)

• Official website of BleepingComputer (https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-rebrands-releases-cd-projekt-and-cisco-data/#google_vignette)

• Official website of BleepingComputer (https://www.bleepingcomputer.com/news/security/8base-ransomware-gang-escalates-double-extortion-attacks-in-june/)

• Cyble Research & Intelligence Labs (https://cyble.com/blog/lockbit-blacks-legacy-unraveling-the-dragonforce-ransomware-connection/)

• Official website of SOCRadar (https://socradar.io/dark-web-profile-8base-ransomware/)

• Official website of Cyberint (https://cyberint.com/blog/research/all-about-that-8base-ransomware-group-the-details/)

• DarkReading new letters (https://www.darkreading.com/threat-intelligence/sexi-ransomware-desires-vmware-hypervisors)

• Official website of Trend Micro (https://www.trendmicro.com/vinfo/tr/security/news/ransomware-spotlight/ransomware-spotlight-8base)

• U.S. Energy and Commerce Commission (https://energycommerce.house.gov/events/oversight-and-investigations-subcommittee-hearing-examining-the-change-healthcare-cyberattack)