Keep up with Ransomware

Hive look-alike, Hunters, goes into action

■ Overview

In October 2023, the number of damage cases caused by ransomware attacks decreased by about 30% to 349 compared to the previous month (496). However, tensions are still maintained as LockBit is active and various ransomware issues continue to occur.

This month, the distribution of malware Qakbot[1] was captured again. Late last August, it was reported that the FBI conducted a 'Duck Hunt' operation through international cooperation to seize Qakbot-related infrastructure and cryptocurrency assets and neutralize its activities, but this month it was confirmed that Qakbot is distributed through phishing e-mail. This distribution attack is believed to be the work of a Qakbot affiliate, but some speculate that the organization distributing Knight is using Qakbot.

The Qakbot attacks are carried out by attackers distributing the Knight ransomware and Remcos RAT[2] through phishing e-mails with LNK files attached. The LNK file contains a command to run PowerShell and download the Knight ransomware from the C2 server[3]. Therefore, you need to be careful because you can be infected with the Knight ransomware just by running the LNK file. Knight Ransomware Group is a rebrand of the Cyclops Ransomware Group, and since starting its activities this August, it has been expanding its influence by actively carrying out attacks using various strategies, including its own ransomware.

[1] Qakbot: Malware used to steal credentials and deliver ransomware

[2] Remcos RAT: Malware used to remotely control infected PCs

[3] C2 server: A server used by an attacker to issue commands and control from a remote location.

This month, the source codes of the early versions of the HelloKitty ransomware were leaked at the dark web's XSS hacking forum. HelloKitty is an RaaS[4] known as affiliated with DeathRansom, FiveHands, etc., and the leakage of the source codes enables anyone to exploit it. Caution is necessary as there have been many cases of variant attacks in the past due to leakage of the source codes of the ransomwares, such as the HiddenTear and Conti ransomware.

The user who leaked the source codes is known as an attacker named 'kapuchin0' and uses the alias 'Gookee'. This user has a history of participating in hacking crimes in the past, and in particular, sold the GooKee ransomware, which operates as an initial access route to Sony Network Japan and RaaS (Ransomware-as-a-Service), in 2020. In addition, he expressed his intention to develop more ransomware if he received financial support, and showed his will to be active, e.g., boasting about the encryption function of the ransomware scheduled to be released at the end of this year.

Looking at recent ransomware attack trends, cases of double ransomware attacks in which attacks are attempted using two types of ransomware instead of a single type are frequently discovered. The double ransomware attacks are characterized by the fact that the attackers perform other types of ransomware attacks within two days after the initial attacks on average. In a situation where a single ransomware attack causes significant damage due to data leakage, system encryption, down-time, etc., if you suffer from a double ransomware attack, the losses can more than double and take a very heavy toll. Therefore, you must work hard to prevent ransomware infections.

This month, various new ransomwares such as Hunters, KeyLock, BlackDream, and Ran were discovered as well. In particular, the Hunters ransomware is attracting attention as it was found to be linked to the Hive ransomware, which was shut down earlier this year. Hunters shows about 56% similarity to the sample of Hive versions 6, and in particular, suspicions are raised that Hunters is a rebrand of Hive due to the similar pattern of encryption logic. However, Hunters denies the rebranding allegations, claiming that it purchased the source codes of the Hive ransomware to develop the Hunters ransomware. Nevertheless, there is evidence showing a connection between the two ransomware in several areas, making Hunters' claims somewhat less credible.

[4] RaaS (Ransomware-as-a-Service): Ransomware-as-a-Service, a form in which ransomware groups provide ransomware to affiliates or attackers for a price

■ Ransomware news

infosec

FBI, Europol shut down RagnarLocker ransomware, arrest developer

○ RagnarLocker group closed with cooperation from Europol, FBI etc

○ RagnarLocker is a ransomware group discovered in late 2019

○ Quite a threatening group until 2022, but in 2023, it did not show any active activity

Hamas-supporting hacktivist target Israel with BiBi-Linux Wiper

○ Wiper 'BiBi-Linux' targeting Israel Linux systems discovered

○ Wiper pretends to encrypt files but actually destroys data and operating systems

○ BiBi-Linux overwrites the file contents and renames the file with the string 'BiBi"

* Hacktivist : Activist who uses hacking as a meaning of struggle

LockBit steals data after Boeing attack

○ Aircraft manufacturing giant Boeing suffered cyberattack, claims LockBit group stole data

○ Boeing says flight safety was not affected and that it is cooperating with investigators

New LostTrust ransomware raises possibility of MetaEncryptor rebranding

○ Both ransomware variants share similar data leak sites and ransomware samples, raising rebranding suspicions

○ LostTrust steals data from specific companies and will leak data if a ransom is not paid

FBI warns of dual ransomware attacks

○ FBI warns of dual ransomware attacks, with multiple strains hitting at once in a single strike

○ Double damage, making it harder to block and react

○ Ransomware attackers sometimes damage of delete to pressure victims into paying a ransom

Suspicion of Qakbot's revival raised by Knight ransomware distribution

○ Qakbot has been shut down, but recent spam emails indicate that its affiliates are still active

○ There is a possibility of revival as infrastructure and affiliates remain

Ukrainian hacktivist group shuts down Trigona ransomware

○ Ukrainian hacktivist group steals data from Trigona ransomware group and shuts it down

○ Trigona is a group that appeared in October 2022 and was very active

Hacktivist group Ghostsec release GhostLocker ransomware

- Hacktivist groups GhostSec and SiegedSec offer GhostLocker Raas
- Some ransomware groups such as Stormous declare that they will use GhostLocker
- Hacktivist want to promote their cause, but sometimes engage in cybercrime for cost reasons

HelloKitty ransomware source code leaked on hacking forum

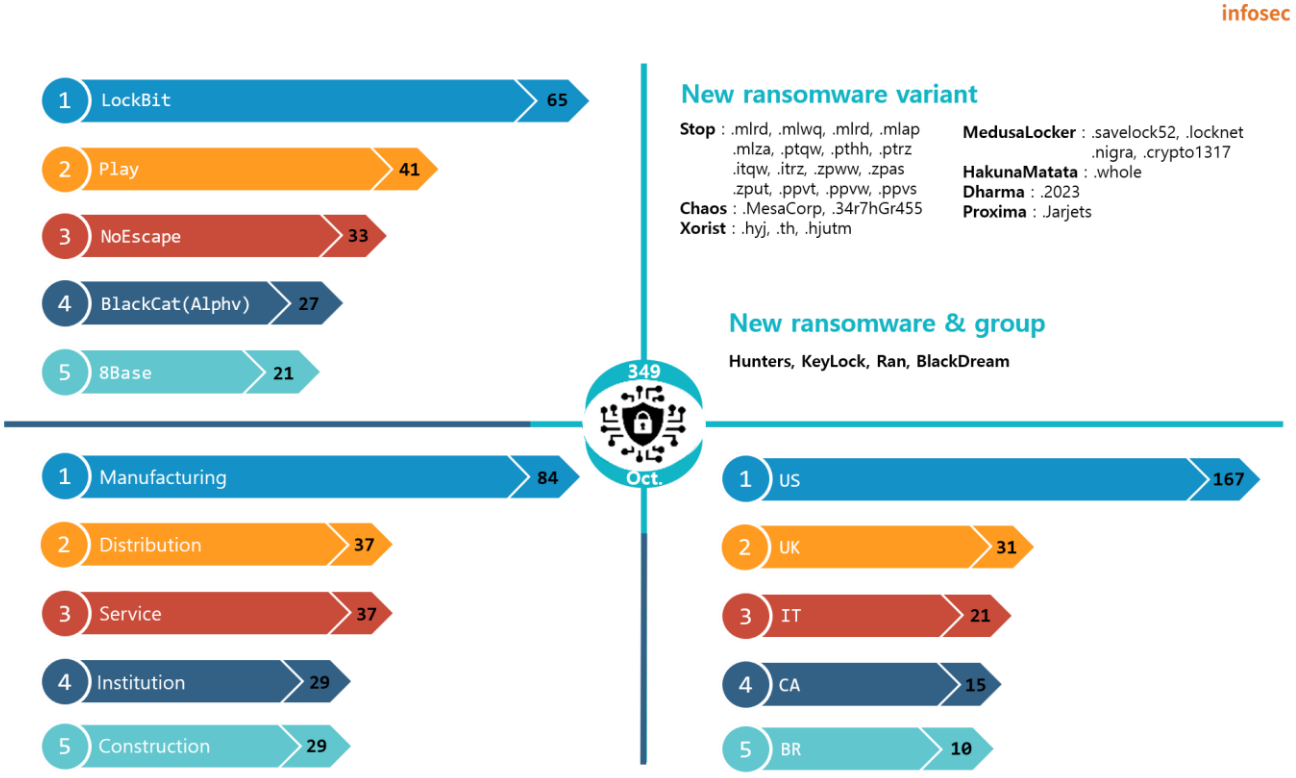
- HelloKitty ransomware creators release source code for early version
- They claim that they are developing a new ransomware with superior performance
- The creator has a history of selling ransomware source code before

SEIKO discloses damage caused by BlackCat(Alphv) attack

- Customer and partner data was leaked due to the SEIKO attack by BlackCat(Alphv) that occurred in July
- BlackCat(Alphv) purchases SEIKO's initial access path from IAB
- SEIKO declares to strengthen security to prevent similar incidents in the future..

* IAB(Initial Access Broker) : Individual or group selling the initial access route

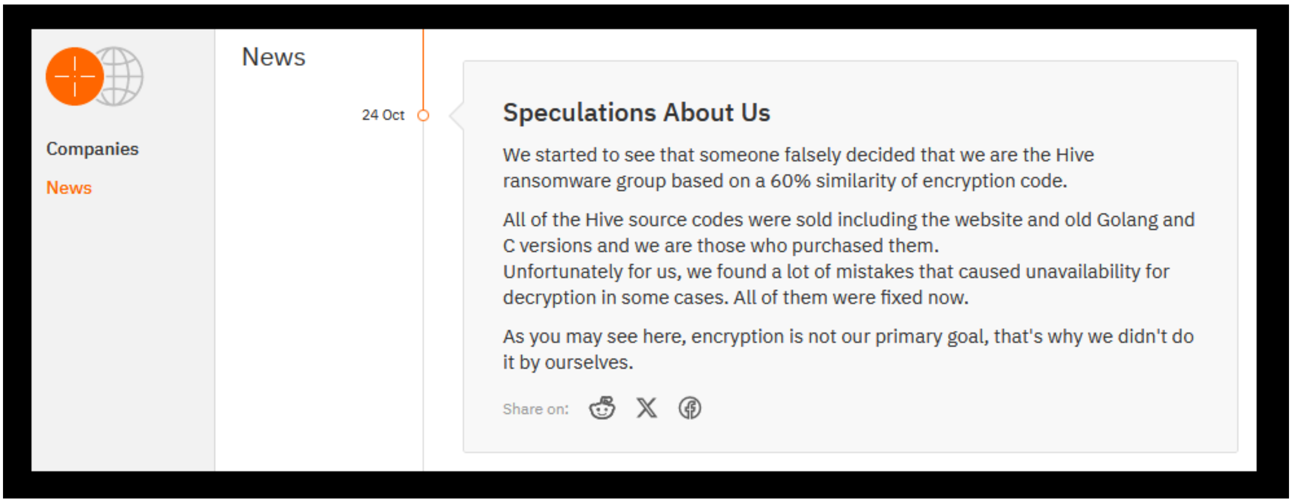
Ransomware threats



New threats

The ransomwares, newly discovered this month, KeyLock and BlackDream, use the AES algorithm to encrypt files, and use the RSA algorithm to encrypt used keys. They are characterized by that fact that they demand money after making system recovery difficult by deleting the VSC[5]. The Ran ransomware uses a hard-coded Base64 value ("This.Is.For.petrolimex.com.vn.2023") as a key to encrypt files through the AES algorithm. At this time, as the key value used for encryption is hard-coded, decryption is possible. The Ran ransomware and the previously described KeyLock ransomware have something in common: they are HiddenTear-family ransomware discovered in August 2015. HiddenTear is an open source project released for educational purposes, but its variants are still released as it is exploited by attackers. BlackDream is a WannaScream-series ransomware discovered in January 2020. WannaScream is also known as the DarkCrypt ransomware and belongs to the same family as ransomwares such as Harma, FOB, Snc, and AWT.

[5] VSC (Volume Shadow Copy): the function to create a backup copy of a file or folder in a Windows system and restore it to its previous state if data is damaged or deleted.



Speculations About Us

We started to see that someone falsely decided that we are the Hive ransomware group based on a 60% similarity of encryption code.

All of the Hive source codes were sold including the website and old Golang and C versions and we are those who purchased them.
Unfortunately for us, we found a lot of mistakes that caused unavailability for decryption in some cases. All of them were fixed now.

As you may see here, encryption is not our primary goal, that's why we didn't do it by ourselves.

* Source: Hunters International dark web leak site

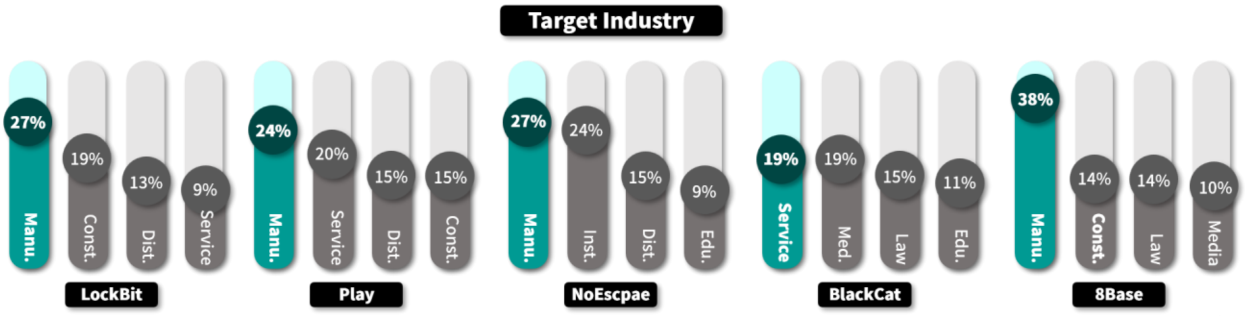
Among the new ransomware groups discovered this month, the Hunters International (hereinafter referred to as Hunters) Ransomware Group is suspected to be a rebrand of Hive, which was shut down earlier this year. The source code similarity between Hunters and Hive is about 56%, and the encryption routines are quite similar, making the situation suspicious. As if aware of this controversy, Hunters posted a short article on a dark web leak site saying, "The public speculation was wrong, and we just purchased the source codes sold by Hive."

The Hive Ransomware Group is a Russian-based RaaS group that has caused more than 1,500 damage cases around the world since its appearance in 2021, and has generated more than $100 million (approximately KRW129.5 billion) in crime proceeds. In particular, Hive carried out extensive activities targeting not only the medical community but also important infrastructure, causing a lot of damage. It is known that due to this influence, international cooperation was quickly achieved and it was finally shut down at the end of January this year. However, Hunters has appeared with ransomware with a structure similar to that of Hive, causing confusion. There is a possibility that Hive secretly traded source codes and infrastructure with Hunters, but typical RaaS groups work by seeking affiliates or posting transaction posts on the deep web, in the dark web forum, Telegram, etc., but as no source code posts or traces have been found, some questions are raised. Therefore, Hunters' future actions are expected to be a clue to unravel the relationship between the two groups.

Top 5 ransomwares

infosec

Target Industry



- Const. : Construction
- Inst. Institution
- Dist. : Distribution
- Edu. : Education
- Med. : Medical
- Manu. : Manufacturing

Target Country

US	36%	US	76%	US	27%	US	63%	US	67%
IT	11%	UK	10%	MX	9%	CA	4%	CA	10%
CA	8%	BE	2%	UK	9%	FR	4%	UK	10%
AU	3%	AT	2%	AE	6%	IT	4%	AU	5%
LockBit		Play		NoEscape		BlackCat		8Base	

US: United States
CA: Canada
FR: France
UK: United Kingdom
MX: Mexico
BE: Belgium
IT: Italy
AE: United Arab Emirates
AU: Australia
AT: Austria

LockBit is the ransomware group that posted leaked data from various companies and caused the most damage this month. In particular, it became a hot topic as it revealed that it had stolen data from Boeing, the world's largest aircraft manufacturing company, and demanded ransom. At one point, a post about Boeing was deleted from LockBit's leak site, and Boeing said there was no impact on flight safety. So there seemed to be no problem. However, when you later accessed Boeing's website, you received a message saying that the website was down due to a technical issue. In addition, perhaps due to the breakdown in negotiations, LockBit posted 43GB of data believed to belong to Boeing on the leak site on November 10, making it clear that Boeing was actually attacked.

Play is known as one of the ransomware groups that show consistent activity. This month, without exception, it leaked many companies' data, and controversy arose as it claimed that it stole data from Dallas County, Texas. Dallas is the second most populous county in Texas, and is a large city with approximately 2 million residents. Play posted an article claiming to have stolen confidential documents from Dallas.

Last May, Dallas was targeted by Royal and the personal information of more than 30,000 people was leaked. At that time, it was reported that the recovery period alone was about 5 weeks, and the recovery cost was also approximately $8.5 million (approximately KRW11 billion), causing significant damage. Even though it is a large city with more than 2 million citizens, it appears that Dallas has been lacking in measures to check and take action on vulnerable areas in terms of security, as ransomware incidents have occurred twice. If the leaked data in this incident includes citizens' personal information, Dallas citizens may be exposed to additional crimes exploiting this information. So rapid identification and response to the situation is necessary to minimize damage.

NoEscape is a ransomware group that started its activities last June, and is a rebrand of the Avaddon Ransomware Group. Looking at its activities since its launch, the amount of leaked data posted on the dark web is increasing every month. So it can be said that this group has a significant influence in consideration of the fact that it is only 4 months old. In particular, it recently announced that it had stolen 145GB of data from a domestic company, and posted a threatening message saying that there would be great damage if the local victim does not agree to negotiations. In this article, leaked data containing documents, databases, and contracts related to projects being carried out by the company was exposed. It also claimed to have carried out an attack on a French basketball team, and stole and disclosed 32GB of documents, including players' personal information, passports and ID cards.

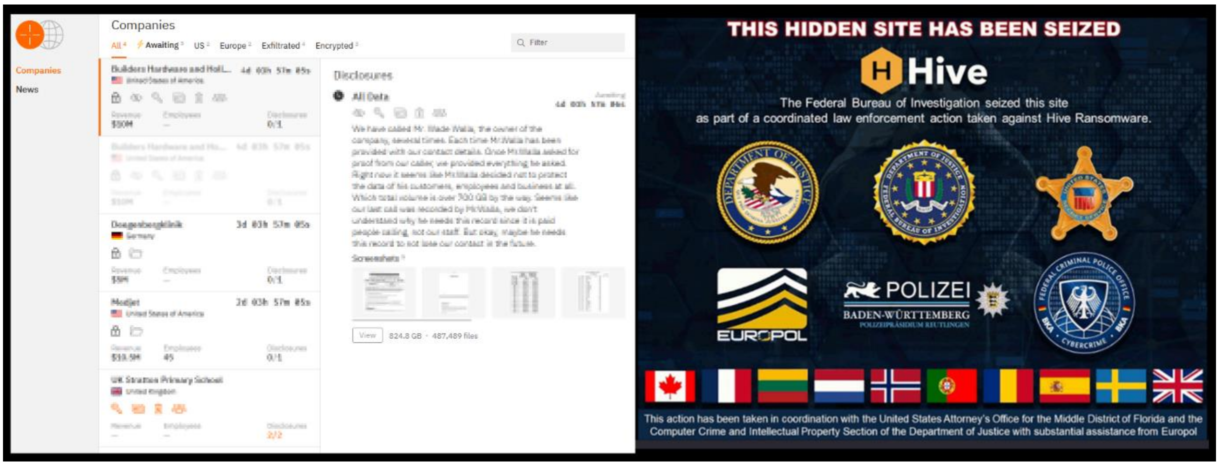
BlackCat(Alphv) is a ransomware group that has been steadily active and is continuously carrying out attacks in various fields such as hotels, healthcare, finance, and manufacturing. In particular, it is characterized by the fact that it is continuously developing ransomware variants and carrying out attacks using various tools. Recently, it was confirmed that it used a Virtual Box ISO file[6] named Munchkin to carry out an attack. In this attack, after the initial access, it creates a new virtual machine through Munchkin, which includes various scripts and utilities, and steals passwords, spreads them on the network, and distributes the ransomware. Because it uses an ISO file, it can be easily adjusted depending on the use and target, allowing various attacks to be carried out. This shows that BlackCat(Alphv)'s strategy is evolving day by day.

8Base is a group that has been active since April of last year, and is showing off its influence by posting 21 damage cases this month alone. In particular, it was confirmed that it was carrying out attacks targeting the manufacturing industry using Phobos-family ransomware, and that it is carrying out extensive attacks in the United States.

[6] Virtual Box ISO file: the disk image file used to install the operating system on a virtual machine.

■ Focus of ransomware

Outline of the Hunters ransomware



We have called Mr. Wade Walla, the owner of the company, several times. Each time Mr.Walla has been provided with our contact details. Once Mr.Walla asked for proof from our caller, we provided everything he asked. Right now it seems like Mr.Walla decided not to protect the data of his customers, employees and business at all. Which total volume is over 700 GB by the way. Seems like our last call was recorded by Mr.Walla, we don't understand why he needs this record since it is paid people calling, not our staff. But okay, maybe he needs this record to not lose our contact in the future.

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

* Source: Hunters International, Hive dark web leak site

The Hunters ransomware is a ransomware used by the Hunters International group, and has about 56% source code similarity with the samples of Hive v6. The main purpose of the Hunters Group's ransomware attacks is not encryption, but rather it is focusing on stealing data to demand ransom from its victims. It is using aggressive tactics, e.g., attacking an American plastic surgery clinic and leaking pre-surgery photos of patients in order to urge victims to pay their ransom. It also revealed that it is planning to send mass e-mails to hospital patients to hasten the payment of ransom. This attack method is similar to a case where the BlackCat (Alphv) Group was morally criticized for leaking photos of cancer patients.

In general, ransomware groups tend to avoid actions that may be morally problematic or attacks that may be life-threatening because they are highly likely to be detected by judicial authorities. In particular, LockBit strictly sets related regulations and expels affiliates that do not comply with them.

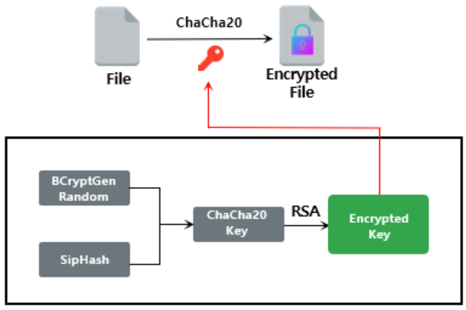
Meanwhile, the now-closed Hive Group has been controversial as it does not hesitate to attack the medical community, and Hunters, which has recently been suspected of being a rebrand of Hive, is also making similar moves, confirming additional clues about the suspected connection between them as well as the source code similarity.

The Hunters Group claims that because its main goal is stealing data instead of encryption, it did not develop its own ransomware, but purchased the source codes and infrastructure of Hive, which was sold as RaaS. However, in addition to the high code similarity with Hive v6, the backend codes of the dark web site described in the ransom note are almost the same as those used by Hive previously, and the actions, not focused on attacks against specific industries, further strengthens the suspicion that Hunters may be a rebrand of Hive.

Hunters Ransomware

Encryption Key

Perform file encryption with ChaCha20 and encrypt keys with RSA



Encryption Method

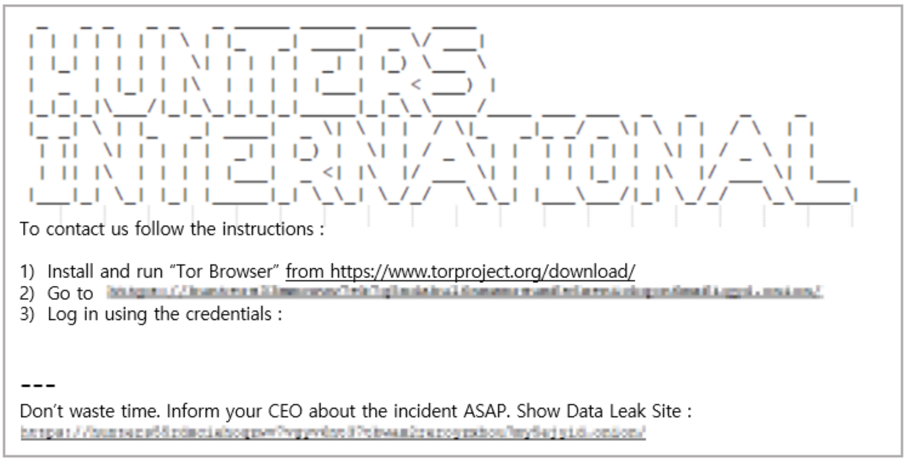
File size greater than 5.25MB : Encrypt the initial 10% of the file, excluding the first 54Bytes, and encrypt the remaining 10% of file at the end

File size less than 5.25MB : Encrypt the entire file, excluding the initial 54Bytes

Characteristics

- **Hive v6**
- **System Recovery Option removal**
- **Partial Encryption**
- **ChaCha20 & RSA Encryption**
- **Rust**
- **Terminate Service and Process**

Ransom Note



To contact us follow the instructions :

1) Install and run "Tor Browser" from https://www.torproject.org/download/
2) Go to [redacted]
3) Log in using the credentials :

Don't waste time. Inform your CEO about the incident ASAP. Show Data Leak Site :
[redacted]

Contact Us.txt

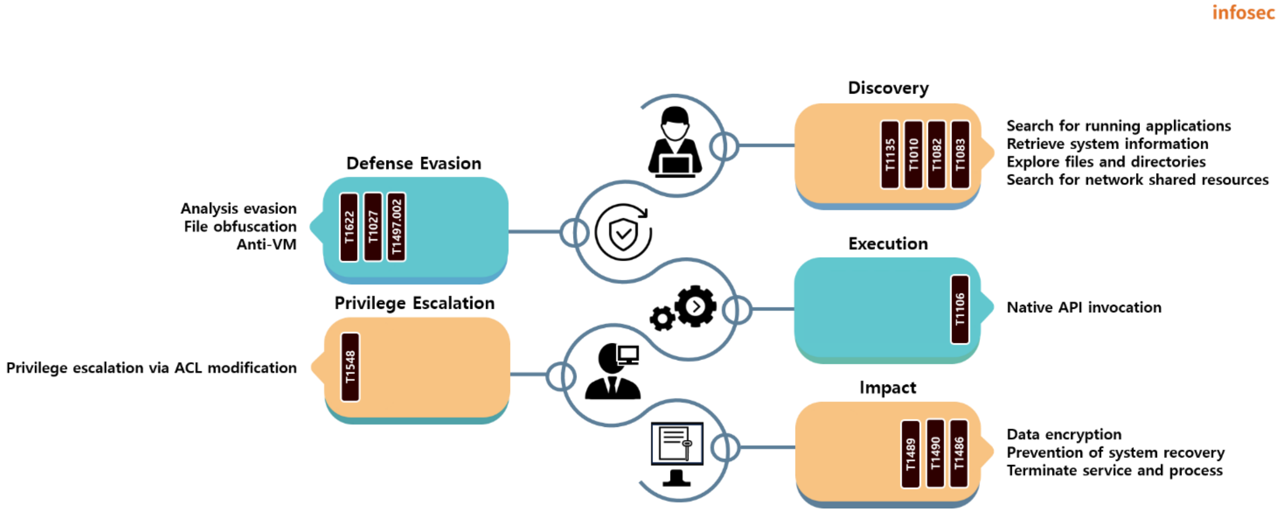
Changed Extension

.locked

Product Language

Rust

Hunters ransomware strategies


infosec
Discovery
T1135
T1010
T1082
T1083
Search for running applications
Retrieve system information
Explore files and directories
Search for network shared resources
Defense Evasion
Analysis evasion
File obfuscation
Anti-VM
T1622
T1027
T1497.002
Execution
T1106
Native API invocation
Privilege Escalation
Privilege escalation via ACL modification
T1548
Impact
T1489
T1490
T1486
Data encryption
Prevention of system recovery
Terminate service and process

The Hunters ransomware uses various technical strategies for ransomware attacks. First, it identifies running applications by searching system information, searches various files and directories, including shared network resources, and terminates specific services and processes to encrypt running files as well.

The character string used internally is obfuscated, and is configured in a way to deobfuscate it through arithmetic operation during execution. So it uses a strategy to avoid signature-based detection. If you use the native API[7], the sequence and signature patterns will be different from when using the Windows API[8], making it difficult for security solutions to detect them. So Hunters applied a method to avoid detection by using the native API.

[7] Native API: LowLevel API to access the core functions of the Windows OS

[8] Windows API: API that provides a high-level interface that developers can use easily

In addition, the Hunters ransomware is elaborate enough to apply the Anti-VM technique to detect the presence or absence of files used in virtual machines by exploiting the fact that malware analysis is performed in a virtual environment. When performing data encryption, in order to access multiple system files, it facilitates the encryption work by escalating the privilege through ACL[9] change, and in case the user set up a backup file or VSC, it deletes relevant elements to remove the means of recovering the system.

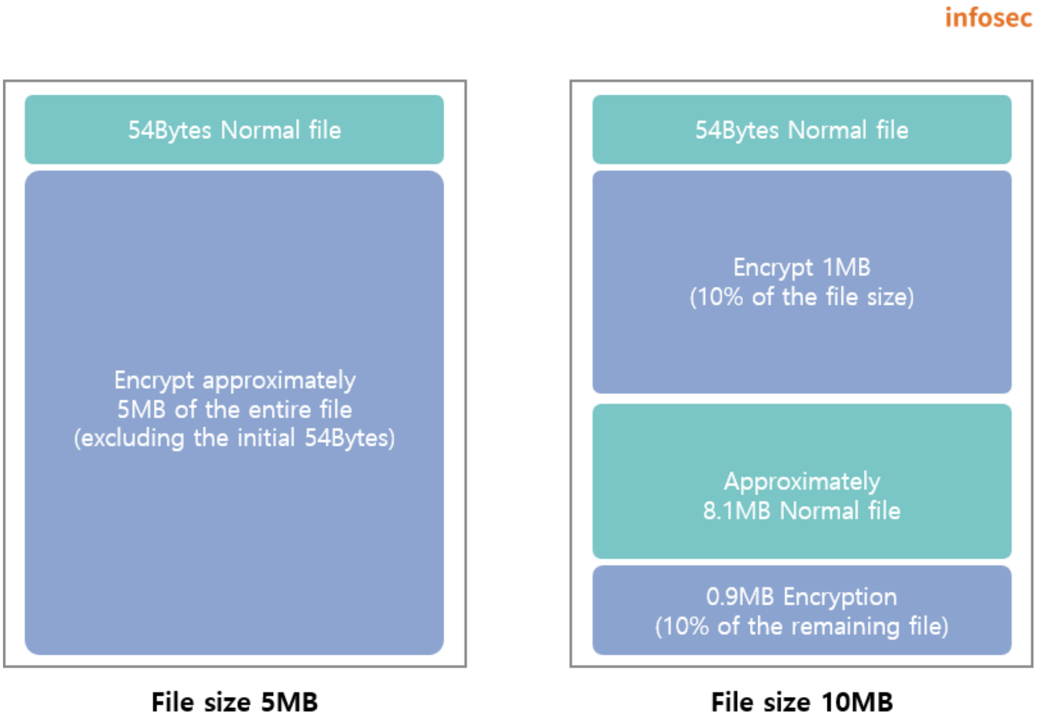
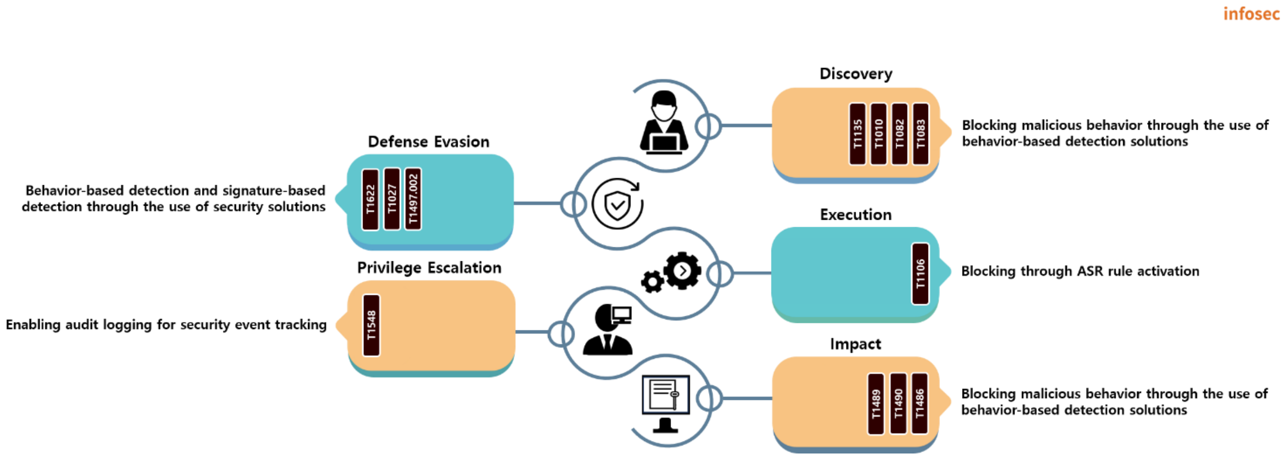

infosec
54Bytes Normal file
Encrypt approximately 5MB of the entire file (excluding the initial 54Bytes)
File size 5MB
54Bytes Normal file
Encrypt 1MB (10% of the file size)
Approximately 8.1MB Normal file
0.9MB Encryption (10% of the remaining file)
File size 10MB

Figure 1. Examples of encryption processes by file size

When performing subsequent encryption, different encryption methods are applied depending on the size of the file to ensure fast encryption speed. If the file size is 5.25MB or less, the entire file is encrypted after excluding 54Bytes at the beginning of the file till the end of the file. If the file size is 5.25MB or more, similarly, after excluding the 54bytes at the beginning of the file, 10% of the file is encrypted, and the end of the file equivalent to 10% of the remaining file size is encrypted.

[9] ACL (Access Control List): A security mechanism that assigns access rights to users or groups to provide fine-grained control over access to files or directories

How to respond to the Hunters ransomware


infosec
Discovery
T1135
T1010
T1082
T1083
Blocking malicious behavior through the use of behavior-based detection solutions
Defense Evasion
Behavior-based detection and signature-based detection through the use of security solutions
T1622
T1027
T1497.002
Execution
T1106
Blocking through ASR rule activation
Privilege Escalation
Enabling audit logging for security event tracking
T1548
Impact
T1489
T1490
T1486
Blocking malicious behavior through the use of behavior-based detection solutions

The Hunters ransomware was created in Rust, a non-mainstream language, but you can use most of the behavior-based security solutions to detect and prevent it. To bypass detection through the use of native API, you can also block malware actions by enabling ASR[10] rules.

Since ACL changes are performed during privilege escalation, enabling the audit logging policy, which can record security events that occur at this time, can help with future incident investigation. Additionally, since Hunters deletes system backup copies and VSCs, it is recommended to perform vaulting backup[11] in a remote location that is difficult for attackers to access in order to prevent data encryption. When backup is not in progress, it is recommended to use a security backup system that blocks access by attackers by turning off the backup system.

Lastly, as Hunters even encrypts shared network resources, if ransomware infection is suspected, you must separate the system from the network to prevent further infection. In addition, you must take measures to minimize shared network resource access privileges so that only necessary resources can be accessed. As infection with ransomware can cause great damage, it is recommended that you should check the environment to see if these response measures have been applied and take action to address any deficiencies.

[10] ASR (Attack Surface Reduction): A rule to block malware attack paths

[11] Vaulting Backup: keeping backup data in a place physically distant from the local system

■ Reference sites

URL : https://thehackernews.com/2023/10/qakbot-threat-actors-still-in-action.html

URL : https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/

URL : https://ransomware.org/blog/fbi-issues-warning-on-dual-ransomware-attacks/

URL : https://www.scmagazine.com/brief/play-ransomware-attack-confirmed-by-dallas-county

URL : https://www.infosecurity-magazine.com/news/boeing-lockbit-ransomware-breach/

URL : https://therecord.media/white-house-counter-ransomware-initiative-summit-new-measure

URL : https://thehackernews.com/2023/10/pro-hamas-hacktivists-targeting-israeli.html?&web_view=true

URL : https://www.bleepingcomputer.com/news/security/new-hunters-international-ransomware-possible-rebrand-of-hive/

URL : https://www.theregister.com/2023/10/25/rebuilt_hive_ransomware_gang_stings/

URL : https://www.darkreading.com/threat-intelligence/ragnar-locker-ransomware-boss-arrested-paris

URL : https://cybersecuritynews.com/blackcat-hacker-tool-remote-machines/

URL : https://www.bleepingcomputer.com/news/security/ukrainian-activists-hack-trigona-ransomware-gang-wipe-servers/