

TLP: GREEN

The Major Ransomware Trends Over the Last Two Years

AhnLab Contents Planning Team

2022. 12. 06

Guide on Document Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Notices
TLP: RED	Reports only provided for certain clients and tenants	Documents that can be only accessed by the recipient or the recipient department Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	Can be copied and distributed within the recipient organization (company) of reports Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

This report is protected by copyright law and as such, reprinting and reproducing it without permission is prohibited in all cases.

Seek permission from AhnLab in advance if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liability.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-12-06	The Major Ransomware Trends over the Last Two Years



CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Overview

"Have you ever been attacked by ransomware?"

A lot of companies would answer "yes" to the question above. Damages caused by ransomware have been piling up again this year, with numerous groups around the world using various ransomware to deploy their attacks.

We've all heard of some infamous ransomware groups, but how do they actually operate their campaigns? And what changes have been made to the ransomware they're using? In this report, we will look into key ransomware groups and their trends over the last two years.

Major Trends

1) Characteristics of Ransomware Groups

The first thing to note is that many ransomware groups are starting to resemble actual companies; they use the RaaS (Ransomware-as-a-Service) model for their operation, and they recruit associates to split their revenues in the ratio of 2:8 or 1:9.

Due to the attention of the media and the public as well as investigations from law enforcement agencies, some ransomware group members were arrested. Threatened by this, ransomware groups took action to dissolve or re-brand themselves. For example, the DarkSide ransomware group was put under law enforcement's scrutiny after its attack on the Colonial Pipeline of the United States, which led the group to shut down and re-brand itself as BlackMatter.

The problem here is that those arrested are mostly money launderers or distributors, meaning that the key members, mostly developers have escaped. Sometimes, the members of dissolved groups are "recruited" by other ransomware organizations.

Aside from cyber-criminal organizations, threat actors suspected to be supported by national governments also use ransomware. Andariel, a group speculated to be backed by North Korea, [had launched a ransomware attack against South Korea](#). The US government also announced that the North Korean threat group [used Maui Ransomware to target medical facilities](#), and Kaspersky disclosed [the relevance between Maui Ransomware and Andariel](#).

Meanwhile, some ransomware groups operate only in specific regions. In Korea, ransomware in action includes Gwisin, Magniber, and Masscan.

Some attackers infect the target with InfoStealer along with ransomware during the campaign. They attempt to go beyond making threats with encrypted data to maximize profit by leaking the victim's credentials.

2) Evolution of Ransomware Techniques

The ransomware attack techniques are also evolving. Not only do they attach malicious links or files in emails, but they also infiltrate systems by exploiting vulnerabilities in the mail or

web servers. Also, a few attackers compromise supply chains, but they are not common. [Some ransomware even have the ability of self-propagation.](#)

Attacks against specific targets are similar to normal hacking and APTs(Advanced Persistent Threats). They share the process of taking control of the internal system piece by piece and leaking information after the initial breach, with the only difference being the distribution of the ransomware at the end. Furthermore, as defenders use a wide range of security products to protect themselves from ransomware, the attackers make various attempts to nullify or bypass their measures.

In terms of ransomware techniques, they show three major characteristics.

#1. While the cloud has become more popular, attackers are also adapting to this trend. They began creating Linux ransomware aimed at cloud environments on top of the ones for Windows.

#2. In the past, the ransomware encrypted files immediately after execution and displayed ransom notes. However, the latest ransomware such as Gwisin, Hive, and LockBit, require the argument value for execution. Without the value, they do not perform malicious functions. That is how they can bypass the scans from behavior-based security products, which makes it difficult for analysts to determine the existence of ransomware in their systems.

#3. Windows ransomware terminates normal processes that might disrupt file encryption and uses tools such as vssadmin.exe to delete copies of the volume shadow or identify backup systems, making data recovery difficult.

3)Key Targets of Ransomware Attacks and Actual Cases

According to analysis reports published over the past year and our collected data, major ransomware attack cases from 2021 to 2022 are as below.

Time	Country	Industry	Details
Apr 2021	UK	Railroad	Merseyrail infected with LockBit
Aug 2021	US	Medical	Memorial Health System in Ohio, infected with Hive
Aug 2021	Thailand	Airlines	Bangkok Airways hit by LockBit, and customer information leaked

The Major Ransomware Trends over the Last Two Years

Nov 2021	Korea	Food	Infected with Hive
Jan 2022	France	Ministry of Justice	Infected with LockBit
Jan 2022	-	Manufacture	Electrical parts supplier infected with Conti
Feb 2022	Korea	Heavy Industry	Infected with Hive
Apr 2022	Korea	Medical	Linux version of Gwisin detected
May 2022	Korea	Medical	Infected with Gwisin
May 2022	Costa Rica	Government	Costa Rican gov declared a state of emergency due to Conti ransomware infection.
July 2022	Korea	IT	Infected with Masscan
July 2022	Korea	Energy	Infected with Masscan
July 2022	Korea	Medical	Infected with Gwisin
July 2022	Korea	IT	Infected with LockBit 3.0
July 2022	Korea	Manufacture	Infected with BlueCrab(Sodinokibi / REvil)
July 2022	Korea	Textile Manufacture	Files encrypted with BitLocker
July 2022	Korea	Heavy Industry	Infected with Hive
July 2022	Korea	Medical	Infected with Masscan
Aug 2022	Korea	Company	Files encrypted with BitLocker

Table 1. Major ransomware attacks in 2021-2022

In Korea, ransomware including Hive, LockBit, and Magniber are highly active, and ransomware activities specifically aimed at Korean organizations are also being reported continuously.

4) Attack Vectors

The way ransomware operators carry out their campaigns is not so different from normal attackers.

For attacks against individuals, the most common method is to compromise user systems by hacking mail and websites they visit.

On the other hand, various methods are utilized for attacks targeting businesses. According to the investigation details on Clop Ransomware, the attacker sent an email with malware to 700 employees of the target company. Three of them opened the attachment, becoming infected with malware and within 52 hours, the ransomware was spread to the entire organization.

Some threat actors also distribute ransomware by first infiltrating the company by exploiting flaws in the database, email, and web server. Then, they take additional control over the internal system and utilize asset management programs equipped with file distribution features.

Many companies affected by ransomware were operating AD(Active Directory). The damaged systems had their local admin account activated and connected to the RDP(Remote Desktop Protocol). Group policies were generated in the AD server's domain controller, and ransomware files were distributed to other computers connected to the domain.

Also, it was easier for attackers to compromise internal systems as corporate servers or devices provided to staff often had identical passwords to make management convenient.

Major Ransomware and Their Activities

The activities of major ransomware groups in 2022 are shown in Table 2. More details on six ransomware groups that have been highly active in recent times will be followed.

Group Name	Ransomware	Activity Level	Description
BlackCat (ALPHV)	BlackCat	High	Speculated to be the successor of DarkSide and BlackMatter
REvil	BlueCrab(Sodinokibi)	Moderate	Successor of GandCrab
BlueSky	BlueSky	Moderate	-
Clop	Clop	Moderate	-
Wizard Spider	Conti	Dissolved	Inactive after internal info was leaked
Globelmposter	Globelmposter	Moderate	-
Gwisin	Gwisin	Moderate	Active only in Korea
Hive	Hive	High	-
LockBit	LockBit	High	-
Magniber	Magniber	High	Highly active only in Korea
Masscan	Masscan	High	Active only in Korea
Yanluowang	Yanluowang	Moderate	-

Table 2. Activity trends of major ransomware groups

1) Attacks using BitLocker

There are some cases when threat actors don't use ransomware but instead use BitLocker, a disk encryption feature built into ▲Windows Server 2008 ▲Windows 7 ▲Vista 8, 8.1, 10, and 11. It supports GUI(Graphic User Interface) and CLI(Command-Line Interface), rendering a potential for abuse as it supports remote encryption.

To execute BitLocker remotely, the start type of the target system's BitLocker service must be set to 'manual' (Windows default settings). Operators can also run the feature on 'automatic' service standby if they have administrator privilege.

During the BitLocker's remote encryption of the target system drive, an encryption progress bar appears on the system that receives the command. Therefore, the process can be recognized by the user, but the threat actor can block the user's access to the drive before the encryption is completed using the argument value "-lock."

The major attack trends show that the attacker who used FRP(Fast Reverse Proxy) to target around 20 Korean companies in August 2022 is continuing their attempt to spread ransomware. The cases revealed that the attacker infiltrated vulnerable servers to install web shells, set up reverse shells, and connect to the RDP. Then, the threat actor finally activated BitLocker to encrypt all drives except the C Drive.

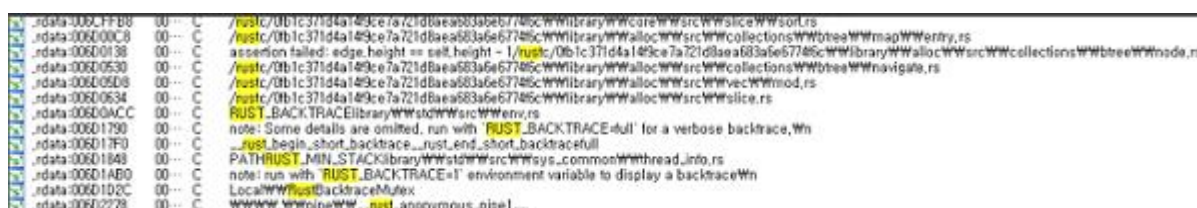
The Lorenz ransomware group leveraged Mitel's MiVoice VoIP (CVE-2022-29499) vulnerability and initiated an attack using Lorenz ransomware and BitLocker.

In order to prevent remote executions of BitLocker, the service must be paused when not in use, with the service start type set to "disable."

2) BlackCat (ALPHV)

BlackCat Ransomware, also known as ALPHV and Noberus, was developed with Rust. Its existence was publicized on a dark web forum in December 2021, but its actual activity started in November of the same year. US companies were mostly infected followed by Canada, Australia, and the UK.

BlackCat ransomware is operated under the RaaS business model; the designer recruits an attacker (subsidiary), and the former takes 10-20% of the profit while the latter takes the rest. Windows and Linux versions of the ransomware have been found, and the notable strings compiled through Rust language can be identified in Figure 1.



```
.rdafa:006c7fbb 00 -- C /rustc/0b1c371d4a149ce7a721d8aa683a6e67745c/.../src/.../slice/.../sort.rs
.rdata:006d00c8 00 -- C /rustc/0b1c371d4a149ce7a721d8aa683a6e67745c/.../src/.../collections/.../map/.../rs
.rdata:006d0130 00 -- C assertion failed: edge.height == self.height - 1, /rustc/0b1c371d4a149ce7a721d8aa683a6e67745c/.../src/.../collections/.../tree/.../node.rs
.rdata:006d0530 00 -- C /rustc/0b1c371d4a149ce7a721d8aa683a6e67745c/.../src/.../collections/.../tree/.../navigate.rs
.rdata:006d05d8 00 -- C /rustc/0b1c371d4a149ce7a721d8aa683a6e67745c/.../src/.../vec/.../mod.rs
.rdata:006d0634 00 -- C /rustc/0b1c371d4a149ce7a721d8aa683a6e67745c/.../src/.../slice.rs
.rdata:006d0acc 00 -- C RUST_BACKTRACE!library/.../Wenv.rs
.rdata:006d1790 00 -- C note: Some details are omitted. run with 'RUST_BACKTRACE=full' for a verbose backtrace.
.rdata:006d17f0 00 -- C _rust_begin_short_backtrace._rust_end_short_backtracefull
.rdata:006d1848 00 -- C PATHRUST_MIN_STACK!library/.../src/.../common/.../thread_info.rs
.rdata:006d1ab0 00 -- C note: run with 'RUST_BACKTRACE=1' environment variable to display a backtrace
.rdata:006d1d2c 00 -- C LocalRustBacktraceMutex
.rdata:006d2278 00 -- C www/.../pipe/.../rust_anonymous_pipe!
```

Figure 1. The notable strings of BlackCat

3) Gwisin

Gwisin is a ransomware group that has been only targeting Korean companies since September 2021. Its name already implies that the group is very well aware of Korea; its website also contains the Korean word for "Gwisin," meaning "ghost."

Gwisin ransomware initiates targeted attacks and remained considerably unknown to the public until it was reported by the Korean press in July 2022. The article stated that the group attacked five or more Korean companies throughout 2022, but the ransomware's specific infiltration method remained a mystery. AhnLab posted the analysis on our ASEC blog after receiving the customer's report in August 2022.

The group's attack starts with taking control of the internal system and distributing malicious MSI files via a file distribution program. There is a Binary.helper file in the MSI file, and it requires argument values(SERIAL, LICENSE, SMM, ORG) to be executed.

The title of the ransom note is '!!!_HOW_TO_UNLOCK_(company name)_FILES_!!!.txt,' and contains English-written data, including the name of the target company and leaked information. The group is known to make negotiations in three steps using the decryption key, information disclosure, and vulnerability to their advantage.

4) Hive

Since its first detection report in June 2021, Hive has been very active. The group initiates a dual attack with information leak and ransomware infection, releasing the stolen information on the Hive Leaks site when negotiations on ransomware decryption fail. In August 2021, the FBI (Federal Bureau of Investigation) made a warning about the activities of the Hive ransomware.

Some of the key characteristics to be noted are that Linux and FreeBSD versions of the ransomware were discovered in October 2021. Then, it was changed to Rust language in July 2022 from its initial use of Go. After infecting the system, it leaves a ransom note with the address and login information to which the victim can connect.

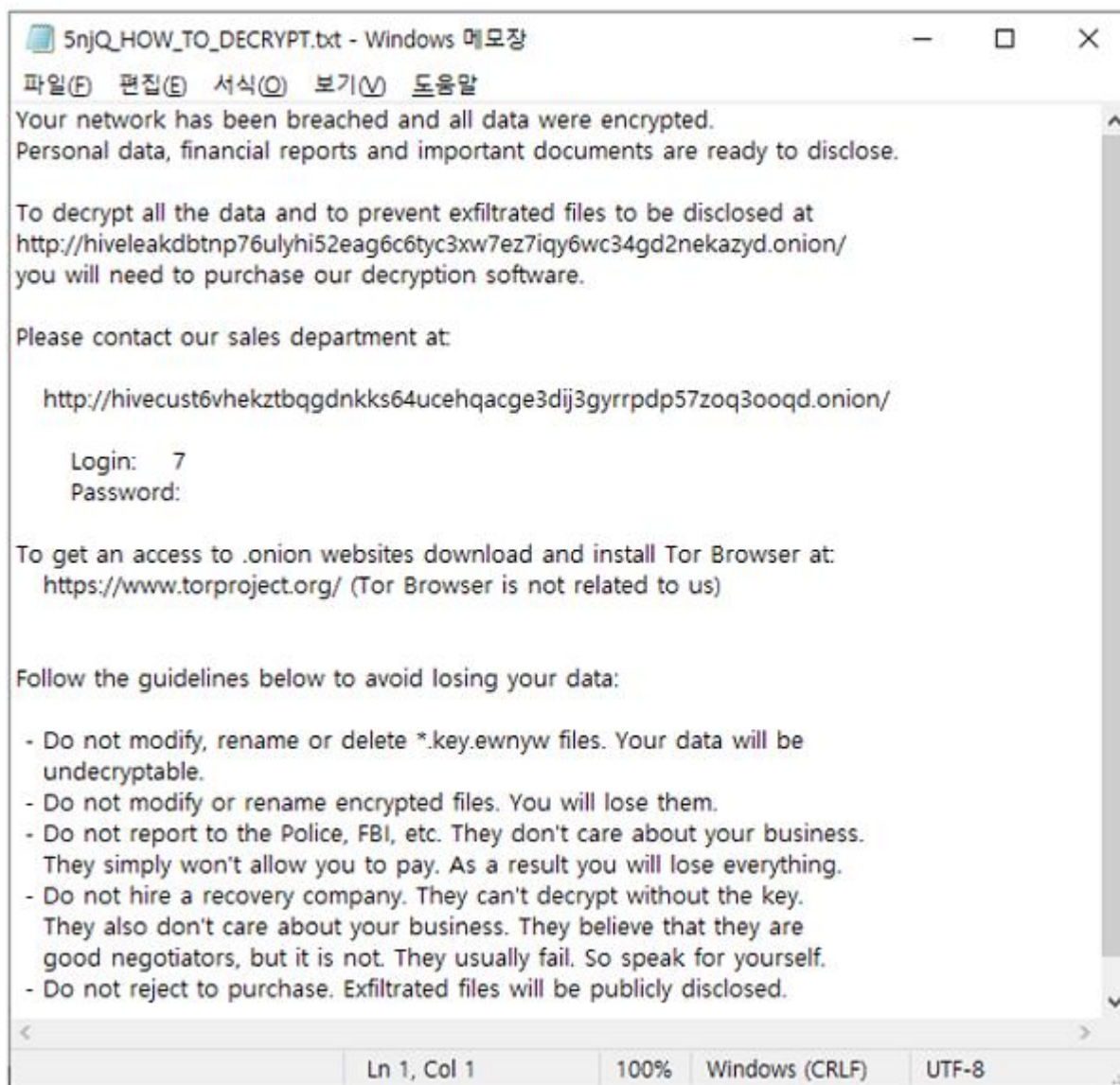


Figure 2. Hive's ransom note

Hive exploits Exchange Server vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) to infiltrate the system. After breaking into the system using the RDP, it takes control of the system using the Cobalt Strike Beacon and deploys ransomware.

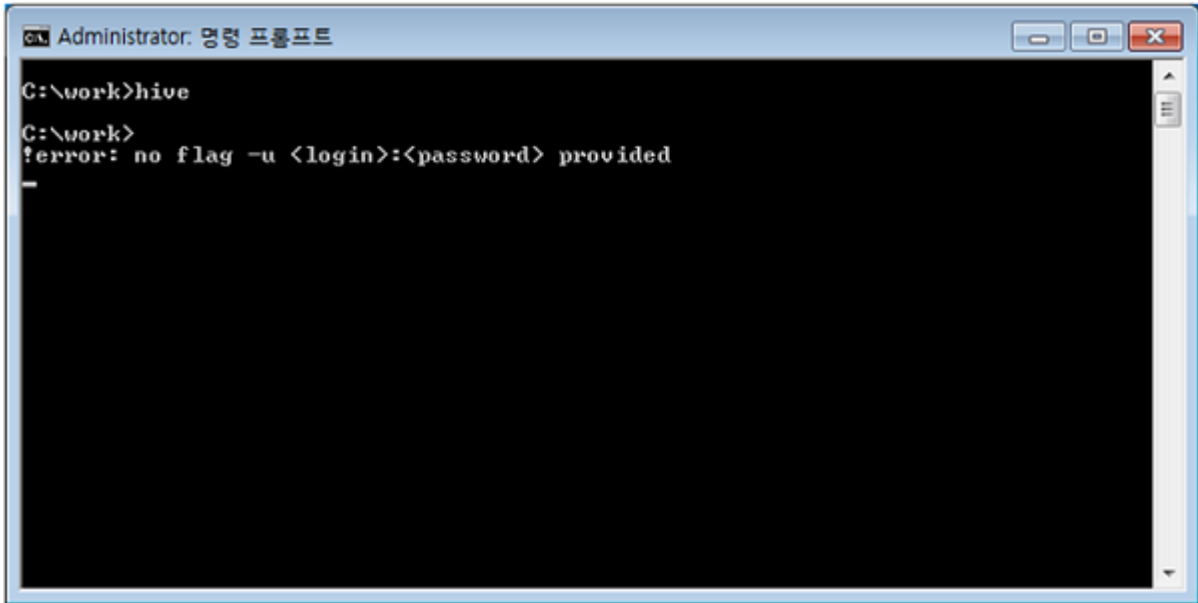


Figure 3. The execution screen of the Hive ransomware without any argument value

5) Masscan

Masscan is a ransomware operator that has been active in Korea since June 2022, without any sighting of it outside the country.

According to KISA(Korea Internet & Security Agency), the group infiltrates the system by exploiting vulnerable database servers. The ransomware is called Masscan as it adds "Masscan_alphabet_random eight-digit extension" to the encrypted file. In its variant, the alphabets F, G, and R were found to be added.

As seen in Figure 4] Masscan generates a file called 'RECOVERY INFORMATION !!!.txt' as its ransom note.

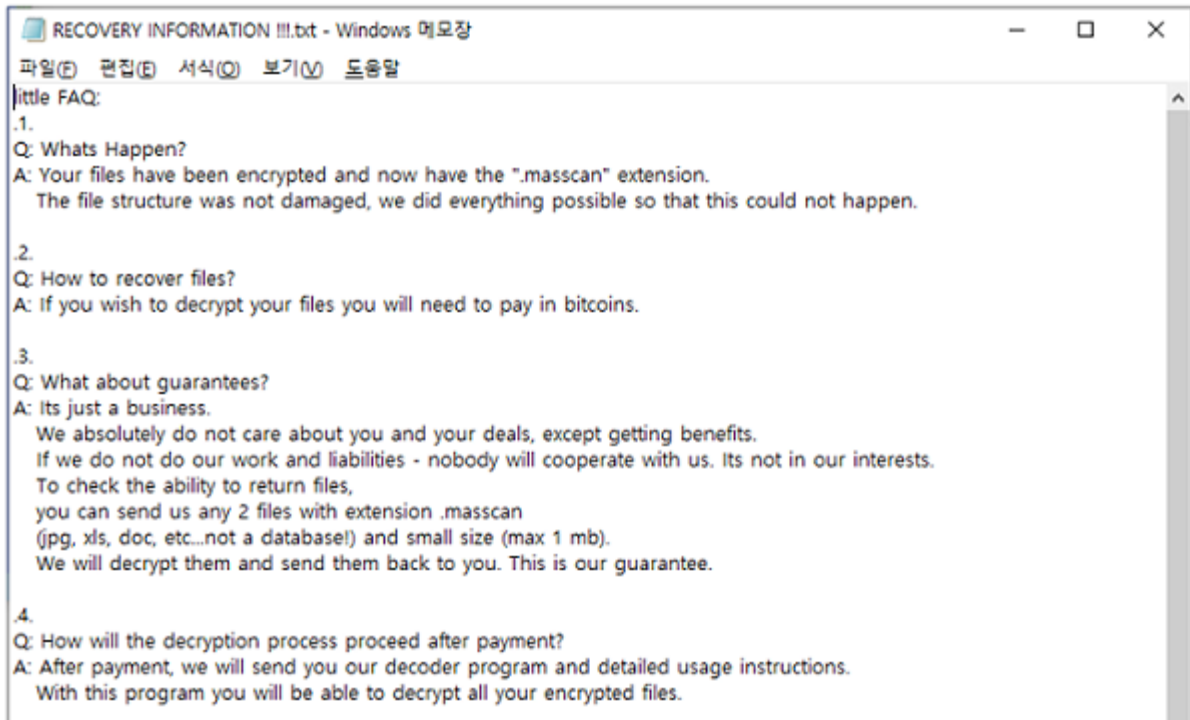


Figure 4. Masscan's ransom note

6) LockBit

Known to have made its first appearance in 2019, LockBit was updated to its 2.0 version and distributed in June 2021. The updated version was equipped with a feature abusing the AD group policy to encrypt the entire Windows domain.

It was once known as the "ABCD ransomware" because it encrypted files and changed their extensions to ".abcd." Since 2019, LockBit has been attacking organizations based in the United States, China, India, Indonesia, Ukraine, and many other European countries. The LockBit ransomware is also operated as a RaaS. On top of that, it propagates itself via emails disguised as resumes targeting Korean companies.

LockBit 3.0 was released in July 2022, and the ransomware is still active to this day. With the release of its latest version, the LockBit drew attention by running a bug bounty, handing out rewards to anyone who found bugs in the group's ransomware. It uses multiple threads during file encryption and only encrypts 4KB of data per file. Like the Hive ransomware, it also requires argument values for execution.

Attempts to Disable and Bypass Security Products

Security products deployed in the computers and servers of companies play a fundamental role in preventing cyber-attack. Due to the increasing damage from ransomware, security products have recently equipped themselves with ransomware protection via features such as blocking suspicious actions, and original file restoration in case of actual encryption. These 'anti-ransomware' features of security products have challenged threat actors, and they are seeking various measures to disable or bypass security products.

1) Disabling Security Products

Threat actors can implement the attack even with the ransomware originally detected by AV as long as they can disable the security product. To make this real, they turn off the real-time or behavior monitoring or delete the whole program after gaining access to the system. [They often use the normal driver to disable Windows Defender and other well-known products.](#)

It is recommended that companies configure their AVs correctly, and individual users should be prohibited from changing the settings to prevent such attacks.

2) Bypassing Security Products

If attackers fail to disable the security products, they try multiple ways to bypass the detection.

In general, attackers are provided with ransomware from developers or create one using a generator. Either way, they would sometimes implement the attack with "known" ransomware detected by a security product. There was a case where an attacker encrypted the ransomware file and created a loader to execute it from the memory after the security product blocked its initial execution twice.

Moreover, security products have the feature of creating a bait file, which is used to detect ransomware when it is modified. Some ransomware bypass it by excluding the bait file generated by security products or the paths where they are installed.

BlueCrab and Black Basta Ransomware boot Windows in safe mode for their encryption. They force the safe mode booting because they might be detected and blocked for carrying out encryption. It allows the ransomware to encrypt files without being disturbed as the security product is deactivated.

The bypass may sometimes succeed on the attacker's first attempt, but in other cases, it can be blocked several times before a successful infiltration. Therefore, security managers must investigate the system and infection route when they identify a ransomware log via a security product.

Conclusion

Ransomware groups are evolving into services, becoming more industrialized and specialized. On the dark web, the role of ransomware groups is already systematically divided into the developer, personal information distributor, initial access brokers(IAB), ransomware distributors, money launderers, and others.

However, the attack method of ransomware groups that aim for specific targets remains similar to average hackers; The process of attackers infiltrating and taking control of internal systems through various measures to leak information is identical. The only difference is that ordinary hackers would disappear after the leak, while ransomware groups would initiate additional attacks with their ransomware. Therefore, efforts to prevent ransomware attacks may also prove beneficial in preventing other attack types.

Unfortunately, damage from ransomware may still occur despite the effort for prevention. Most victims restore their systems after paying a ransom, which may lead to more hacking from other ransomware groups if they do not improve their protection measures by investigating the attacker's infiltration route.

Thus, companies must thoroughly investigate the infection by making a request to professional security vendors and improve their security system deficiencies when hit by ransomware. Moreover, security managers should regularly check whether the employees' personal information and their login credentials have been leaked to the dark web. It should be noted that when emails are sent to all employees to attack a company, it is highly likely that their email addresses were disclosed beforehand.

The Major Ransomware Trends over the Last Two Years

AhnLab has been tracking the activities of multiple threat actors and responding to their malware whenever they have been discovered. As for their most recent activities, AhnLab products might have already detected their malware.

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea

Tel : +82 31 722 8000 | Fax : +82 31 722 8901

www.ahnlab.com

www.asec.ahnlab.com/en

© AhnLab, Inc. All rights reserved.

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.