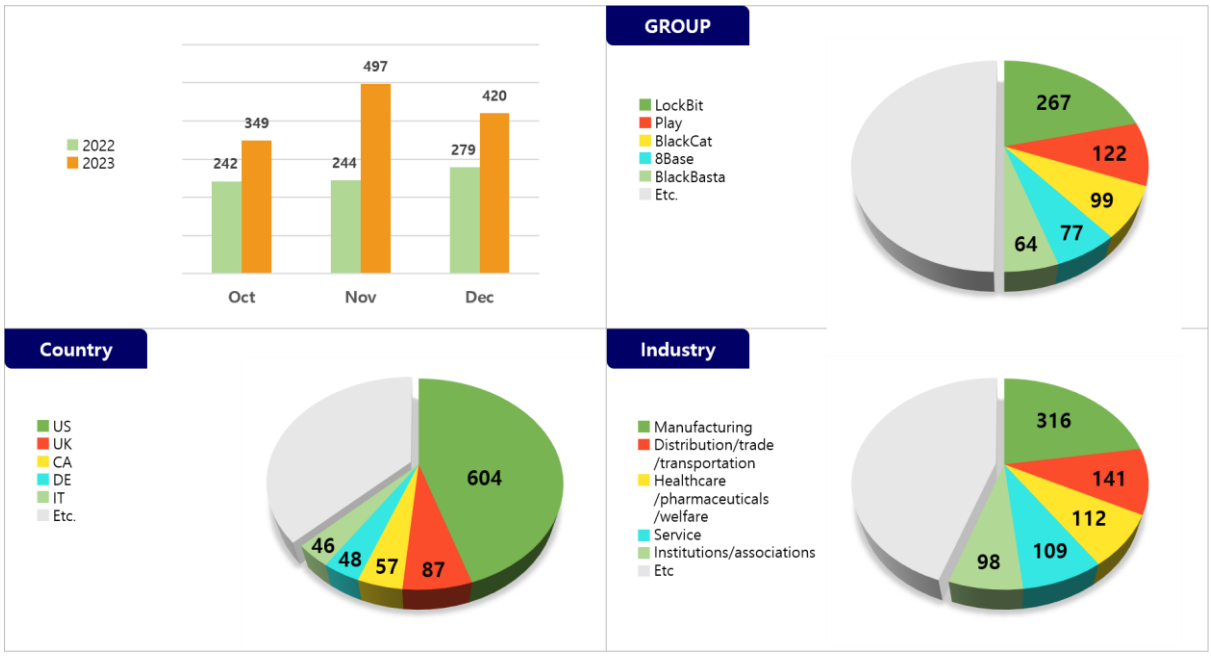
KARA
Korea Anti Ransomware Alliance

2024.02.

KARA ransomware trend report

KARA Ransomware Trend Report

■ Ransomware trends



[Figure 1] Ransomware activity statistics of the 4th quarter

In the fourth quarter, 1,266 damage cases were confirmed, a 9% decrease from the previous quarter. This can be attributed to the fact that data leakage by the Clop group, which carried out large-scale attacks through software vulnerabilities in the second quarter, continued into the third quarter, but in the fourth quarter, the activities of the Clop group decreased and at the same time, the Trigona, RagnarLocker, RansomedVC, NoEscape, and BlackCat ransomware group were shut down or had operational problems. When issues related to the operation and closure of the NoEscape and BlackCat group arose in December, the LockBit group posted a message on the dark web forum in an attempt to recruit the affiliates and ransomware developers of the NoEscape and BlackCat group.

About 10% of the 1,266 cases that occurred in the fourth quarter were caused by eight groups that newly started activities: Hunters, WereWolves, DragonForce, SiegedSec, Raznatovic, Meow, Malek Team, and Soldiers of Solomon. It was also confirmed that hactivist groups, i.e. the Soldiers of Solomon group were using ransomware.

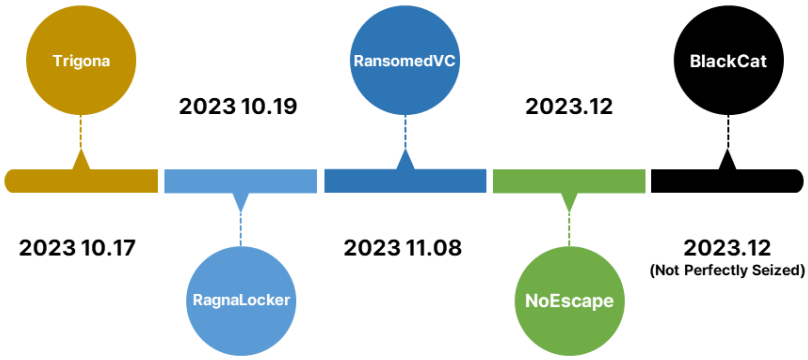
Recently, ransomware groups have shown a tendency to prefer a strategy of carrying out ransomware attacks by exploiting software vulnerabilities. As attacks that exploit vulnerabilities can target multiple victims through a single vulnerability, and select unpatched targets to approach them with relative ease, vulnerabilities are continuously exploited for attacks.

Lastly, as a result of analyzing damage cases of domestic companies on the dark web, a total of 4 domestic damage cases were confirmed in the fourth quarter. In October, oil manufacturing companies were infected by the NoEscape group, in November, international organizations and electronic component manufacturers were infected by the LockBit and Qilin groups, and in December, personal information of golf-related software developers were leaked due to an attack by the BlackSuit group. An attack occurred that could cause secondary damage due to the distribution of impersonated text messages targeting users of the leaked data. If you receive a phishing text message saying, "Thank you for using our company so far. To express our apologies due to server problems, we are giving 3 treasury stocks (worth KRW270,000) as a gift to a small number of members. If you wish to receive the gift, please leave a reply saying 'Receive', a staff member will contact you as soon as possible to provide friendly assistance," you must be careful not to sustain damage by treating the originating number as spam.

✓ Ransomware trends

1. Successive shutdowns of ransomware groups

In the fourth quarter, cases were confirmed where ransomware groups were shut down thanks to the cooperation of international agencies such as FBI[1], Europol[2], and JIT[3], or suspended operations due to pressure from investigative agencies. Such groups include the Trigona, RagnarLocker, RansomedVC, NoEscape, and BlackCat.



[Figure 2] Groups that are closed and suspended operation

On October 17, the pro-Russian Trigona group was shut down by the Ukrainian Cyber Alliance (UCA). Two days later, on October 19, the RagnarLocker group was also shut down by Europol. Meanwhile, the RansomedVC group suspended its activities on November 8 after announcing that six group officials were arrested and 98 affiliates were fired. On October 30, before the news of the arrest, the RansomedVC group announced that it wanted to sell projects through the dark web forum and the Telegram messenger, but it seems that it was continuously under investigative pressure, and the arrest of the affiliates due to inexperienced operations also had a significant impact.

[1] FBI (Federal Bureau of Investigation): An investigative and intelligence agency under the U.S. Department of Justice

[2] Europol: Anti-crime agency of the European Union

[3] JIT (Joint Investigation Team): A joint investigation team jointly established by European national investigative agencies

Meanwhile, in December, the NoEscape and BlackCat group's data leakage sites were shut down. Seeing that an affiliate of the NoEscape group stated, "The operator took millions of dollars in ransom and shut down the leak site," it is presumed that the operator conducted an exit scam[4]. It was suggested that the BlackCat group was shut down by an investigative agency after the data leakage site was shut down on December 7, but the BlackCat group's administrator said that it would soon resume operations as the disruption was caused by a hardware error. On December 19, the FBI's confiscation poster was posted on the BlackCat group's site, and it seemed like the group would be shut down. But on the same day, the BlackCat group posted a message to the effect that it would allow its affiliates to attack the United States and related organizations as part of retaliation after restoring the data leakage site. Then, the data leakage site was shut down and restored repeatedly, and a war of nerves continued between the FBI and the BlackCat group, but the BlackCat group reopened the data leakage site and posted new victims.

In addition, in December, five people suspected of being in charge of a group that used ransomware such as Dharma, Hive, LockerGoga, and MegaCortex in Ukraine were arrested through the cooperation of Europol and JIT, and there were confirmed cases of ransomware groups being shut down by the cooperation of international investigative agencies.

[4] Exit scam: A type of fraud in which operations are ceased after payment is received

2. Ransomware activities of hactivist groups

In the fourth quarter, a number of ransomware groups began their activities. Among them, ransomware activities by hactivist groups such as GhostSec and Soldiers of Solomon were discovered, and it was also confirmed that a Hamas activist group used BiBi-Wiper[5] to perform attacks as part of the Hamas-Israel war.

Among them, GhostSec is a group for carrying out cyber attacks against the Islamic extremist group ISIS, and began selling GhostLocker RaaS (ransomware as a service)[6] through the Telegram messenger from October 8, 2023. Currently, GhostLocker's affiliate price is $999, and GhostSec said that it would increase the price up to $4,999 in the future. Also, the Soldiers of Solomon group is a pro-Palestine hactivist group that carries out attacks mainly targeting Israeli companies. It publicizes its actions through SNS channels like X (former Twitter) and the Telegram messenger, which can spread news quickly, and leaks stolen data through the dark web forum. In particular, the group is known to carry out attacks using RaaS called Crucio.

[5] BiBi-Wiper: Data deletion malware used by the Hamas hacktivist group against Israeli companies

[6] Ransomware-as-a-Service: It is abbreviated as RaaS. A service that provides ransomware in exchange for money

3. Ransomware attacks exploiting vulnerabilities

The vulnerabilities and ransomware groups exploited for attacks in the fourth quarter were 'Apache ActiveMQ[7] / HelloKitty', 'Atlassian Confluence[8] / Cerber', 'SysAid[9] / Clop', 'Critix NetScaler[10] / LockBit', and 'Qlik Sense[11] / Cactus'. To prevent these attacks, it is necessary to take immediate action against vulnerable versions of software.

Ransomware	Target vulnerability	Vulnerability number	Patched Y/N
HelloKitty	Apache ActiveMQ	CVE-2023-46604	Y
Cerber	Atlassian Confluence	CVE-2023-22518	Y
Clop	SysAid	CVE-2023-47246	Y
LockBit	Critix NetScaler	CVE-2023-4966	Y
Cactus	Qlik Sense	CVE-2023-41265 CVE-2023-41266 CVE-2023-48365	Y

Table 1. Ransomware attacks exploiting vulnerabilities

[7] Apache ActiveMQ: Open source software that securely delivers and manages messages between senders and receivers.

[8] Atlassian Confluence: Collaboration software that can manage documents centrally

[9] SysAid: An IT service management solution for managing IT services within an organization

[10] Critix NetScaler: A networking platform that manages and complements server and SQL database traffic

[11] Qulk Sense: A platform or solution for data visualization and analysis

4. Ransomware with ChatGPT

At the end of November, four ransomware attackers were arrested in China. They said they created various ransomware variants, and in particular, used OpenAI's ChatGPT to improve the ransomware's functionality and performed attacks by scanning the vulnerabilities of victims' networks.

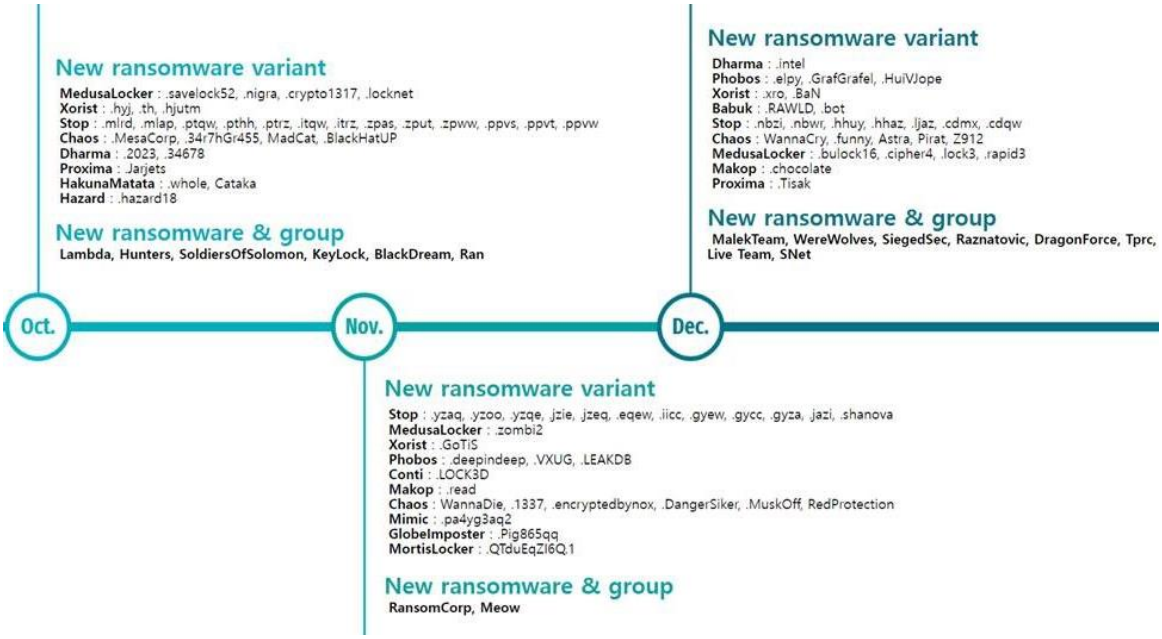
As AI technology develops rapidly like this, it is continuously confirmed that attempts are being made to not only use ChatGPT for ransomware maintenance/repair, but also carry out cyber attacks through WormGPT[12] and FraudGPT[13], which are used for phishing attacks and BEC attacks[14], and DarkBart and DarkBert, the dark web version of Google AI Chatbot Bard.

[12] WormGPT: An AI model developed for the purpose of performing phishing and BEC attacks

[13] FraudGPT: An AI model developed for the purpose of performing malicious actions such as writing malware and creating phishing pages

[14] BEC (Business Email Compromise): Cybercrime where scammers trick you into divulging confidential company information via email

✓ **New ransomwares and group activities**

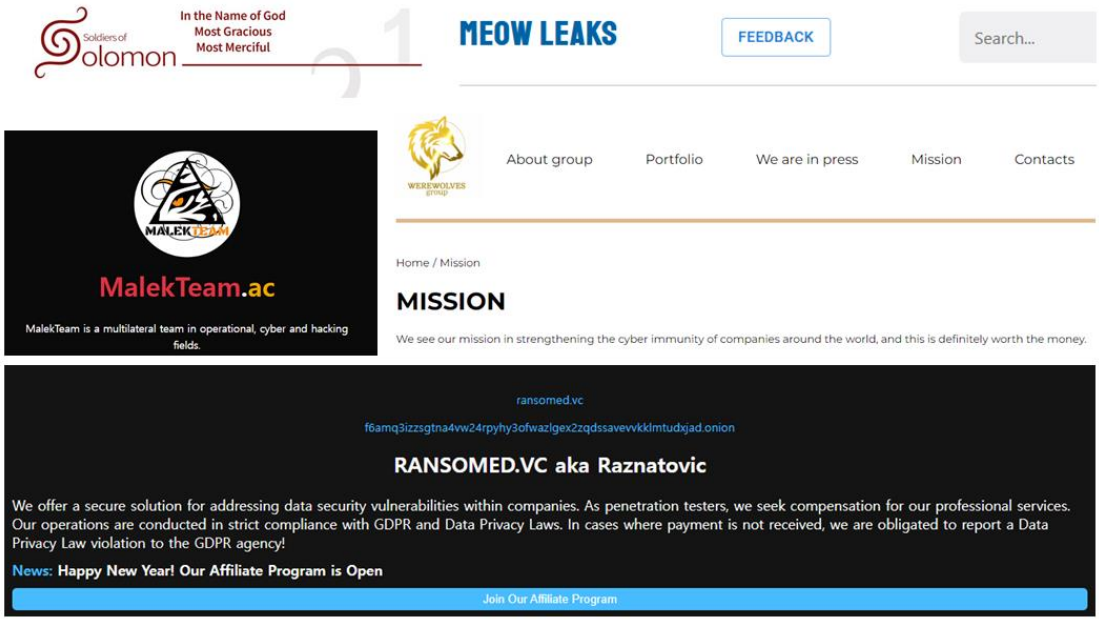


[Figure 3] New/variant ransomware activities

In November 2023, it was confirmed that an attacker from the 8Base group was carrying out an attack using the Phobos ransomware, a Ransomware-as-a-Service. Also, in the same month, CISA[15] issued a security advisory stating that an attacker who used to use the ViceSociety ransomware was carrying out an attack using the Rhysida ransomware. The number of affiliates and attackers who carry out attacks by partnering with multiple RaaS rather than partnering with only one ransomware group continues to increase.

Since the Phobos ransomware was discovered in January 2019, many variants have been derived and used for attacks. Among the variants of the Phobos ransomware, a ransomware that imitates vx-underground was discovered. vx-underground is a malware repository website and a group active in relation to malware through X (former Twitter). When the ransomware was discovered, vx-underground said, "We do not use ransomware and we do not use such old ransomware."

[15] CISA (Cybersecurity and Infrastructure Security Agency): An agency under the U.S. Department of Homeland Security, dedicated to cybersecurity in the U.S.



[Figure 4] New ransomware dark web activities

In the fourth quarter, a total of 7 ransomware groups began their activities as shown below.

- **Soldiers of Solomon**

  It began its activities in October 2023 and is a pro-Palestine hactivist group that mainly carries out attacks targeting Israeli facilities and institutions. It is disclosing stolen data through dark web forums and is additionally leaving records of attacks through the Telegram messenger and X (former Twitter). Meanwhile, it is carrying out attacks using the Crucio ransomware, a ransomware-as-a-service.

- **Hunters International**

  It began its activities in October 2023. As more than 56% code similarity was confirmed between the ransomware of the now closed Hive group and the ransomware used by Hunters, and it was guessed that the backend codes of the dark web site listed in the Hunters ransom note are quite similar to those of the existing dark web site used by the Hive group, it is presumed to be a rebranding[16] of the Hive group. As if the Hunters group were aware of these views, however, it posted a message on their dark web saying, "The public's guess was wrong, and it just purchased the source codes sold by the Hive group."

- **Meow**

  The group began its activities in August 2022, took a break in February 2023, and began activities again in November. It is carrying out attacks using the variants of the Conti v2 ransomware that uses the ChaCha20 and RSA-4096 algorithms, and in March, an unknown person posted 257 decryption keys, decryption tools, and decryption tool source codes used in the Meow ransomware attack on a dark web forum, and Kaspersky distributed a decryption tool based on the above information.

- **WereWolves**

  This group started its activities in December 2023, uses Russian, and is carrying out attacks targeting Russian companies. "We believe that our mission is to strengthen the cyber immunity of companies around the world." Similar to the LockBit group, it is conducting bug bounties[17] for websites and ransomwares, and is also offering rewards to people who succeed in doxing[18] ransomware group officials.

- **DragonForce**

  This group began its activities in December 2023, and became an issue through a data leak from Yakult's Australian branch in the same month. It is separate from the pro-Palestine hactivist

[16] Rebranding: The act of a ransomware group suspending operations and then returning or operating again under a new name

[17] Bug bounty: A system that pays rewards to those who find vulnerabilities in software or web services

[18] Doxing: A word derived from dropping docx, which refers to the act of disclosing personal information of a specific person online

group DragonForce Malaysia, and although it is a newly emerged ransomware organization, it is believed to be experienced in light of its attacking strategy, negotiating style, data leakage site, etc.

- **Raznatovic**

  This group started its activities in December 2023, and is characterized by the phrase "RANSOMED.VC aka Raznatovic" posted on its data leakage site. On October 30, before its closure, the RansomedVC group posted that it was afraid of surveillance by investigative agencies and wanted to sell all projects, and then on November 8, 6 officials were arrested, 98 affiliates were fired, and operations were suspended. It is guessed that the Razatovic group is using the infrastructure it purchased from the RansomedVC group.

- **MalekTeam**

  This group began its activities in December 2023, and mainly carries out attacks targeting Israeli companies and facilities. On the dark web data leakage site, it posted six cases of data after performing attacks on Israel's military-related institutions, hospitals, etc., and through this, it is guessed that it is an Iranian attack group that has a hostile relationship with Israel.

BlackCat History

[Figure 5] BlackCat group's closed dark website (part)

The BlackCat group is known by three names: BlackCat, ALPHV, and Noberus. Among them, the name BlackCat is a name given by Malware HunterTeam, which operates ID Ransomware that can identify ransomware, and Recorded Future, a cyber security company, and Noberus is a name given by Symantec, an American security software company. In fact, it calls itself ALPHV. The BlackCat group is a group that began its activities in November 2021 and has been performing attacks most actively after the LockBit group, creating 227 victims in 2022 and 431 in 2023.

It only recruited affiliates who are fluent in Russian, and even during ransomware attacks, it checked the language used on the PC and did not carry out an attack if a CIS (Commonwealth of Independent States) language was used. So it is presumed to be a group based in Russia. Also, the BlackCat ransomware became a major issue as it was the first Rust language-based ransomware discovered at the time.

The BlackCat group created many victims shortly after starting its activities and became one of the most active ransomware groups, presumably because it recruited many affiliates in a short period of

time by guaranteeing a higher rate of return to affiliates compared to other groups. Considering that the rate of return of the LockBit group affiliates, which are currently carrying out attacks most actively, is 70% of the ransom obtained through attacks, the rate of return of the BlackCat group affiliates up to 90% of the ransom can be seen as a fairly unconventional condition.

The BlackCat group's ransomware released Version 1, Version 2 and Version 3, and BlackCat Sphynx, which can attack Windows and Linux. Many BlackCat ransomware variants were discovered, including ALPHV MORPH variants created to bypass anti-virus software by applying obfuscation, and SafeBoot variants for rebooting in safe mode.

The threat-based strategy the group used is also worth noting. It encrypted data and used a double extortion strategy under the pretext of file leakage, and began supporting crawlers and APIs that could obtain detailed information about victimized companies. It used through TypoSquatting[19] to leak the data of the victimized companies, and filed a complaint against companies that did not pay the ransom with the SEC (Securities and Exchange Commission).

Meanwhile, the BlackCat group is known as a rebranding of the DarkSide/BlackMatter group. When the BlackCat group began its activities, the LockBit group was the first to raise suspicions. Additionally, ExMatter, a data leakage tool used only by the BlackMatter group, was used in the BlackCat ransomware attack, and the C2 server[20] IP used in the BlackMatter ransomware attack was confirmed in the BlackCat ransomware attack. In conclusion, it was officially confirmed by the FBI's Flash report[21] that several developers of the BlackCat group and money launderers were connected to the DarkSide/BlackMatter group.

In December 2023, the FBI's confiscation poster was posted on the BlackCat group's data leakage site, and the group's activities seemed to be ended, but the group's activities are continuing after the infrastructure was restored. Moreover, because it allowed attacks on core infrastructure for the purpose of retaliating against the FBI, which used to be prohibited, the threat is expected to grow further.

---

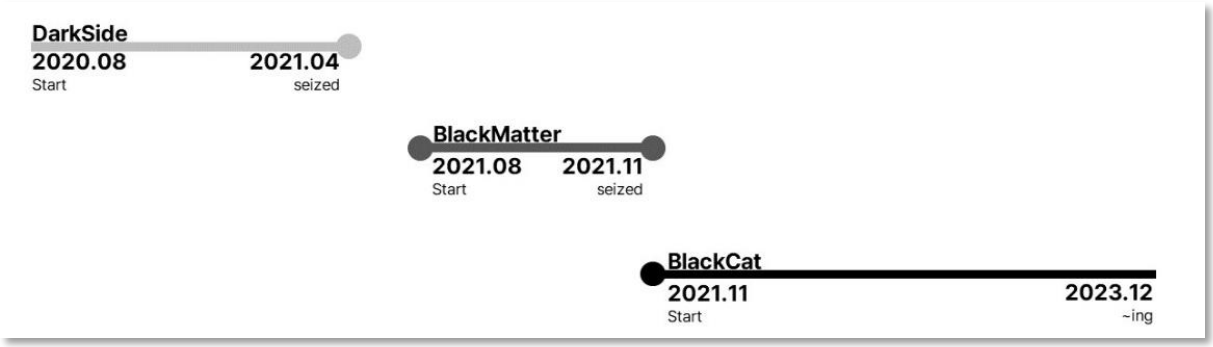
[19] TypoSquatting: Using misspelled domain names to pass off fake domains as legitimate ones

[20] C2 server: The server used by the attacker to maintain communication with the device that was successfully accessed in the initial stage

[21] FLASH (FBI Liaison Alert System) report: A report published by the FBI to counter cyber threats

1. BlackCat's connection to DarkSide/BlackMatter

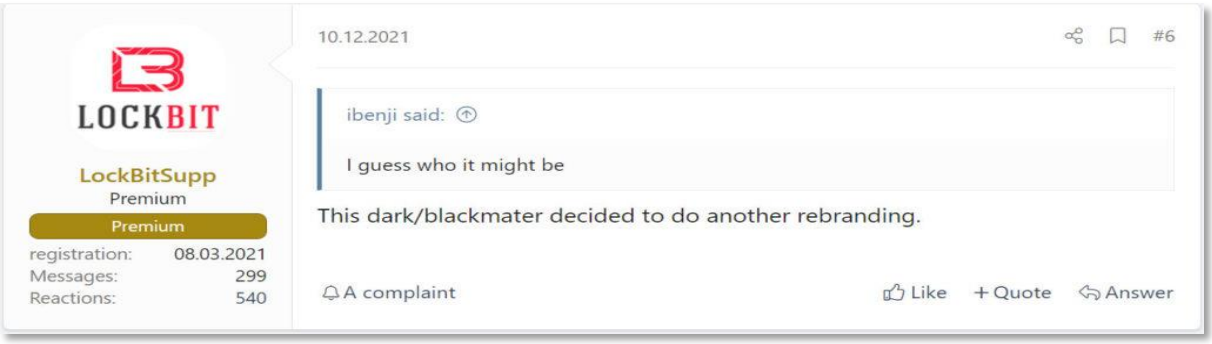
- **The period of activity of the BlackMatter, DarkSide and BlackCat group**



[Figure 6] The period of activity of DarkSide, BlackMatter and BlackCat

The DarkSide group is a group that began its activities in August 2020 and was active until April 2021, when the data leakage site was closed due to pressure from the U.S. Department of Justice and the FBI, and the ransom money extorted from victims was confiscated and its activities were suspended. In August 2021, four months after the DarkSide group was shut down, the BlackMatter group also declared that it would cease operations due to pressure from investigative agencies after four months of activity and shut down the group. Immediately after the BlackMatter group was shut down, the BlackCat group began its activities at the end of November. In this way, the timing of the start and end of these groups' activities are all conveniently connected, hinting at the correlation among the three groups.

Meanwhile, when the BlackCat group began its activities, the LockBit group posted a message on the forum, saying "The BlackCat group is a rebranding of the DarkSide/BlackMatter group," which became an issue.



[Figure 7] LockBit's opinion on the BlackCat group

- Using the ExMatter takeover tool for the BlackMatter ransomware attack

ExMatter is a hacking tool known to be used by the BlackCat group to steal data. ExMatter was confirmed to be a custom data takeover tool discovered after Ryuk Stealer used by the Ryuk group and StealBit used by the LockBit group. In November 2021, it was confirmed that the ExMatter information takeover tool was also used in the BlackMatter group's attacks. Although it was a previously unknown tool, some connections are confirmed in that it was used in the two ransomware attacks.

- BlackCat group started as an affiliate of the DarkSide/BlackMatter group.

In an interview with Recorded Future, the BlackCat group said, "We are a group that simply started out as an affiliate of the DarkSide/BlackMatter group." However, security researchers say that the group would rather not believe it due to the reputation of the DarkSide and BlackMatter group, which were shut down due to pressure from investigative agencies.

- **C2, which was used for the BlackMatter ransomware attack, was also discovered in the BlackCat ransomware attack.**

It was confirmed that C2 used in the BlackCat ransomware attack that occurred in December 2021 was also used in the BlackMatter attack in September 2021. In particular, in December 2021, it was not long after the BlackCat group began its activities, as soon as BlackMatter was rebranded as BlackCat, BlackMatter's affiliates could have partnered with the BlackCat group, but as there are cases where ransomware affiliates act as affiliates of multiple ransomwares, however, it is difficult to view this case alone as telltale evidence.

- **FBI Flash Report**

An FBI Flash report published in April 2022 mentions that several developers of the BlackCat ransomware group and money launderers are connected to the DarkSide/BlackMatter group, which suggests that the BlackCat group has an extensive network and experience in ransomware operations.

2. BlackCat group issues

- **BlackCat was discovered for the first time.**

[Figure 8] First discovery of the BlackCat ransomware

In November 2021, the existence of the group became known when the BlackCat ransomware sample was discovered for the first time by MalwareHunterTeam, and it became a big issue because it was the first Rust language-based ransomware discovered among the ransomwares identified to date.

- **Recruiting affiliates and penetration testers through the Russian dark web forum**

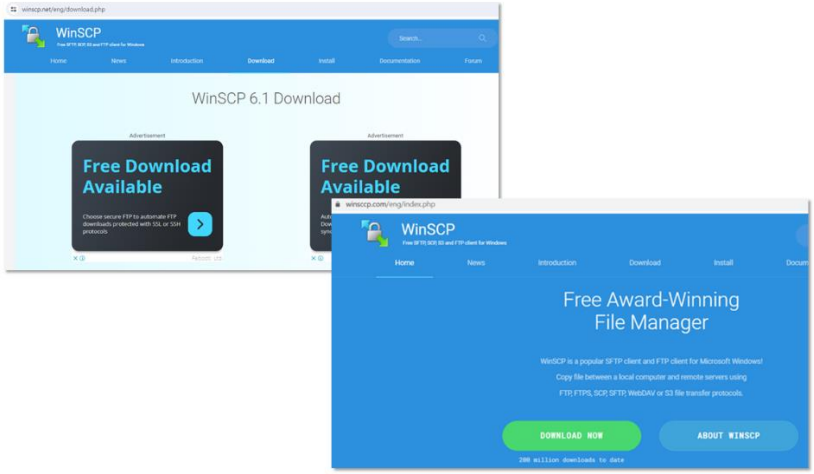
In December 2021, the BlackCat group showed signs of expanding its scope of activity by recruiting affiliates under the nickname alphv in the hacking forum, i.e. the XSS and Exploit Forum, and by working under the nickname 'Ransom' in RAMP, a Russian cyber crime forum, and recruiting penetration testers.

- **BlackCat affiliate used the Veritas Backup Exec vulnerability.**

According to Mandiant, a security company, BlackCat ransomware attacks, which exploited Veritas Backup Exec's open vulnerabilities (CVE-2021-27876, CVE-2021-27877, and CVE-2021-27878), have been discovered since October 2022. These vulnerabilities were patched in March 2021, and were added to Metasploit, a penetration testing framework, on September 23, 2022. The affiliate of the BlackCat group that carried out the attacks is known to be UNC4466, and it was confirmed that it used Metasploit to access Windows servers using the Veritas Backup Exec solution and carried out ransomware attacks.

- **Performing the BlackCat ransomware attack through Malvertising**

Malvertsing is a compound word of Malicious and Advertising, and refers to the act of spreading malware through online advertising. This type of malware distribution was also used by the BlackCat group. In July 2023, it advertised by disguising itself as popular software such as Advanced IP Scanner, Slack, WinSCP, and Cisco AnyConnect through Google Ads, an advertising service provided by Google. It is designed so that when you actually download and run the file, the Nitrogen malware is executed. The Nitrogen malware is a malware that downloads CobaltStrike Beacon[22] and then executes additional malwares. It is confirmed that the group performed attacks by distributing the BlackCat ransomware through the malwares installed afterwards.

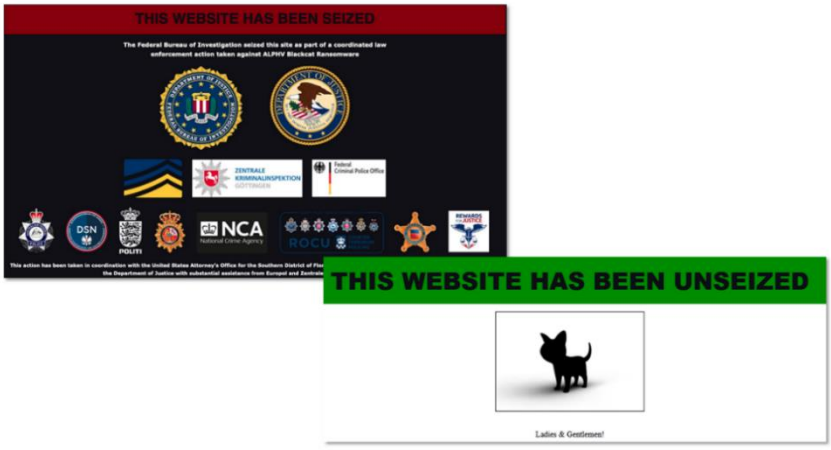


[Figure 9] winscp.net, winsccp.com

Similar to the case of spreading the BlackCat ransomware through malvertising, in June 2023, a case of luring people to a fake page (winsccp.com) that imitated the official website (winscp.net) of the WinSCP file transfer application for Windows, and then downloading CobaltStrike Beacon, disguised as a normal file, when downloading files and performing BlackCat ransomware attacks was also discovered.

[22] CobaltStrike Beacon: A file or backdoor that can perform tasks such as collecting information and executing commands, used in CobaltStrike, a mock hacking tool

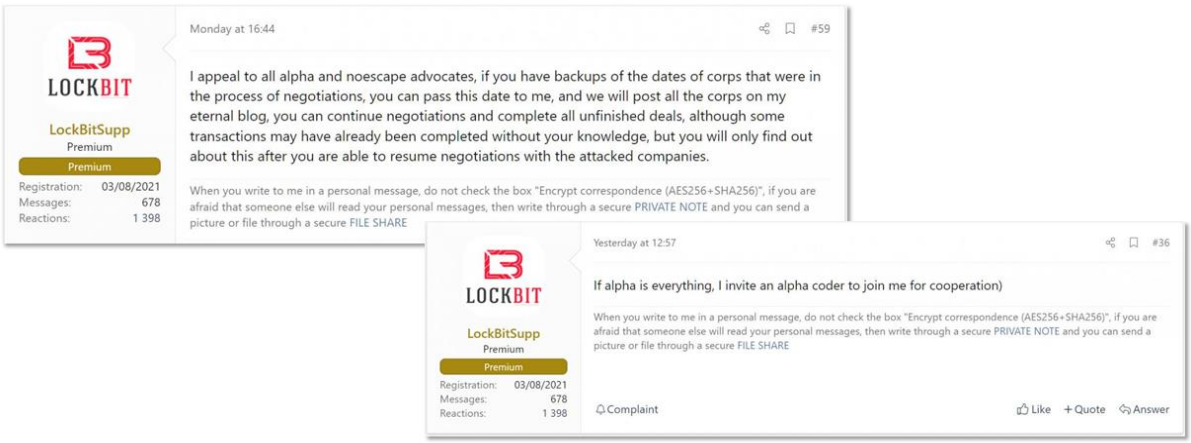
- **Data leakage site Seized, Restore**



[Figure 10] FBI vs BlackCat

On December 7, 2023, the BlackCat group's data leakage site became inaccessible. Afterwards, the BlackCat group's administrator said that the site's operation would resume again, but on December 19, immediately after the FBI's confiscation poster was posted on the BlackCat group's data leakage site, an official statement from the FBI was announced, and the closure of the BlackCat group seemed to be confirmed. However, on the same day, the BlackCat group posted a message to the effect that it restored the data leakage site and the FBI accessed a data center, and the keys obtained were keys that had been used for a month and a half, equivalent to about 400 companies, and more than 3,000 companies can no longer receive keys, and have it would allow its affiliates to attack the United States and related organizations due to the FBI's actions. Then, the data leakage site was shut down and restored repeatedly, and a war of nerves continued between the FBI and the BlackCat group, but the BlackCat group reopened the data leakage site and is posting new victims.

- **LockBit group attempted to recruit affiliates and developers.**



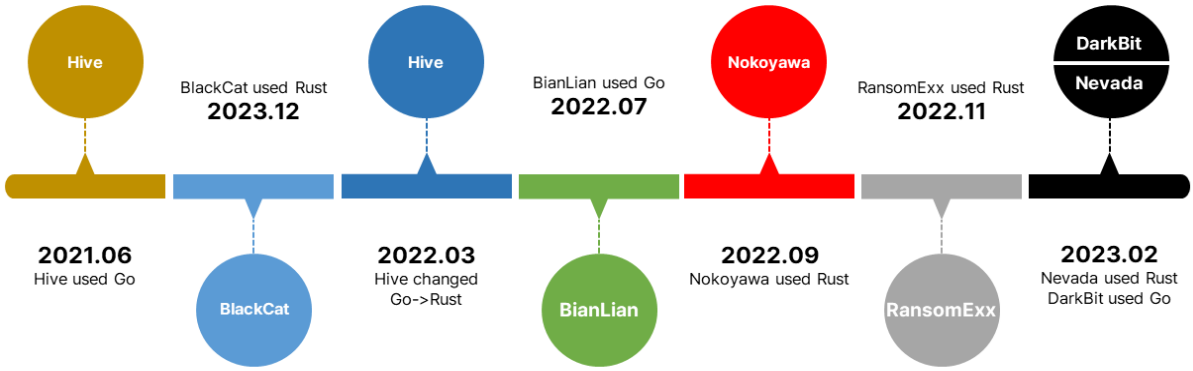
[Figure 11] LockBit group's recruitment of BlackCat affiliates and developers

As signs of the BlackCat group's closure appeared, the LockBit group began recruiting the affiliates and developers of the BlackCat group. In particular, the LockBit group posted a message on the dark web forum to recruit developers by posting a message saying, "We respect the partners who moved from the BlackCat group to the LockBit group and they want to work with familiar software." In fact, the German Energy Agency, which was posted on the BlackCat group's data leakage site, was also registered on LockBit's data leakage site. Through this, it can be guessed that some affiliates of the BlackCat group have already moved over to the LockBit group.

3. BlackCat ransomware and ExMatter update

- **Rust-based ransomware discovered first**

The BlackCat ransomware is a ransomware discovered in November 2021, and is the first Rust language-based ransomware discovered among the ransomwares identified to date. When asked why they used the Rust language to make ransomware, the BlackCat group said in an interview with Recorded Future, "We simply created new ransomwares with a new approach that meets modern requirements." However, the BlackCat ransomware based on the Rust language has too many advantages as malware to simply meet modern requirements.



[Figure 12] Ransomware groups' use of non-mainstream languages

The Rust language is a language officially distributed by Mozilla in 2015. It not only has a fast execution speed like an exe file written in C/C++, but also has the advantage of preventing malfunctions due to memory conflicts. Therefore, if you develop a ransomware by exploiting these advantages, you will be able to encrypt files at high speed without error, and the memory logic added by the compiler will delay analysis and increase the possibility of avoiding detection. Furthermore, the Rust language is a cross-compile language that can create exe files targeting various operating systems without dependency on the operating system. So it has recently been used by some ransomware groups.

- **ExMatter, a tool for stealing information**

ExMatter is an information takeover tool used by the BlackCat group. It is used before ransomware attacks and is designed to find files with a specified extension in a specific directory and upload them to a pre-configured server via SFTP.

Then, in August 2022, it was confirmed that the BlackCat group carried out attacks using ExMatter, which had updated functions. The updated ExMatter has added FTP protocol support, a report writing function showing a list of stolen files, a function to damage files, and a self-delete function to existing functions.

Meanwhile, ExMatter is a tool that was discovered while it was used in the BlackMatter group's attack in November 2021. ExMatter is a custom data leakage tool discovered after Ryuk Stealer used by the Ryuk group and StealBit used by the LockBit group. It was also confirmed that it was also used in the BlackMatter group's attack in November 2021.

- **In February 2023, BlackCat 2.0 Sphynx version was updated.**

In February 2023, BlackCat 2.0 Sphynx was updated. In version 1, an access token argument was required to execute ransomware, but it was deleted. When ransomware is executed, the Config value, which contains various settings such as extensions to be encrypted, processes to be terminated, and encryption methods, was changed from the Json format of the existing version to a regular character-string type. Also, it includes Impacket, an open source framework that allows you to perform lateral movements between networks, and Remcom, a remote shell that allows you to remotely execute commands on other devices.

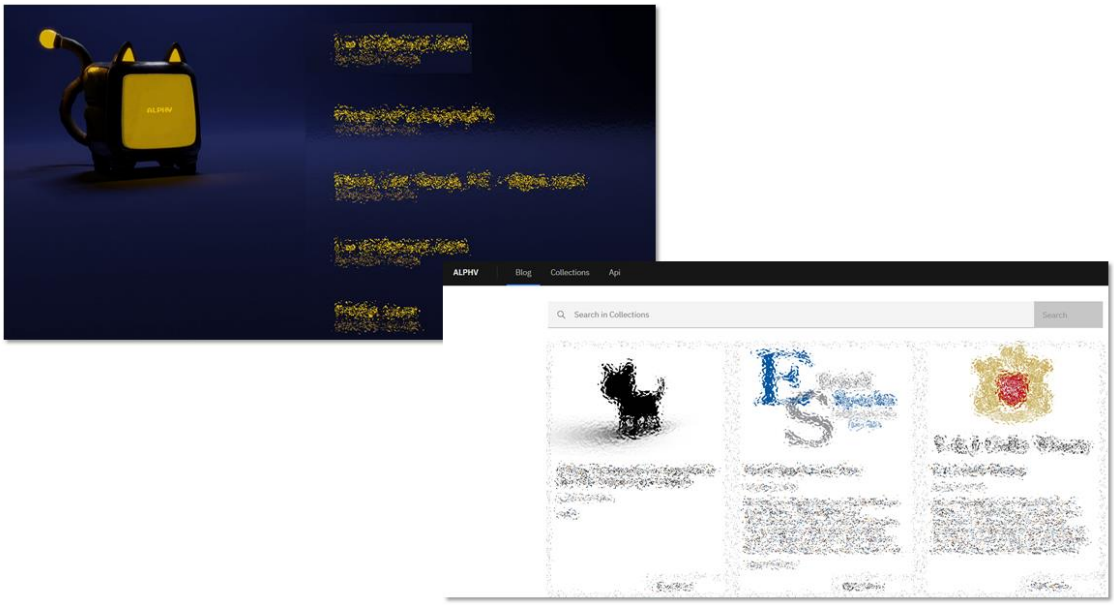
The BlackCat group stated that the ransomware update "completely rewrote the source codes," said the BlackCat group. "This update put the first priority on minimizing AV[23] and EDR[24] detection."

[23] AV (Anti-Virus): Software to detect and defend against viruses and malware

[24] EDR (Endpoint Detection and Response): A solution that detects and responds to malicious behavior occurring on terminals such as computers and mobile devices in real time

4. Evolving data leaks and threat-based strategies

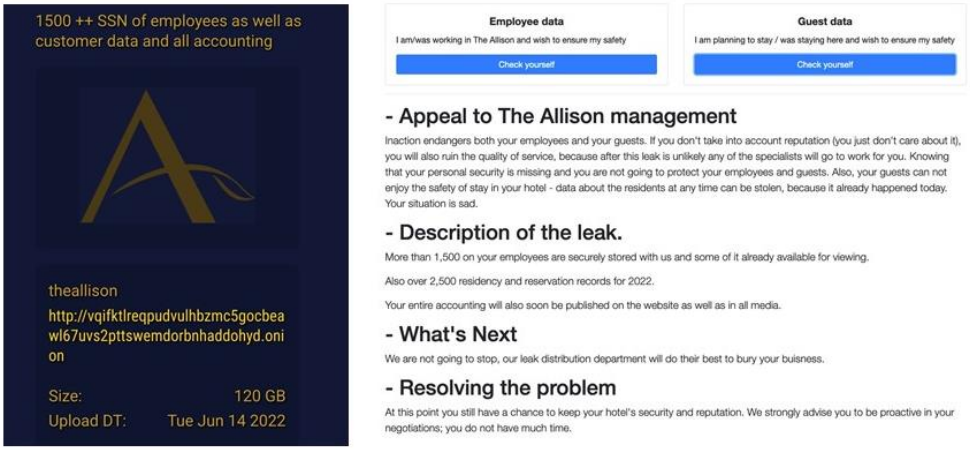
- **Opening a data leakage site**



[Figure 13] BlackCat group data leakage site (past/present)

In December 2021, the BlackCat group opened a data leakage site to recruit affiliates and attackers through the dark web, and carry out double extortion. In addition, the BlackCat group has adopted the DDoS strategy and is using a triple threat strategy.

- **Opening a site where leaked data can be searched**

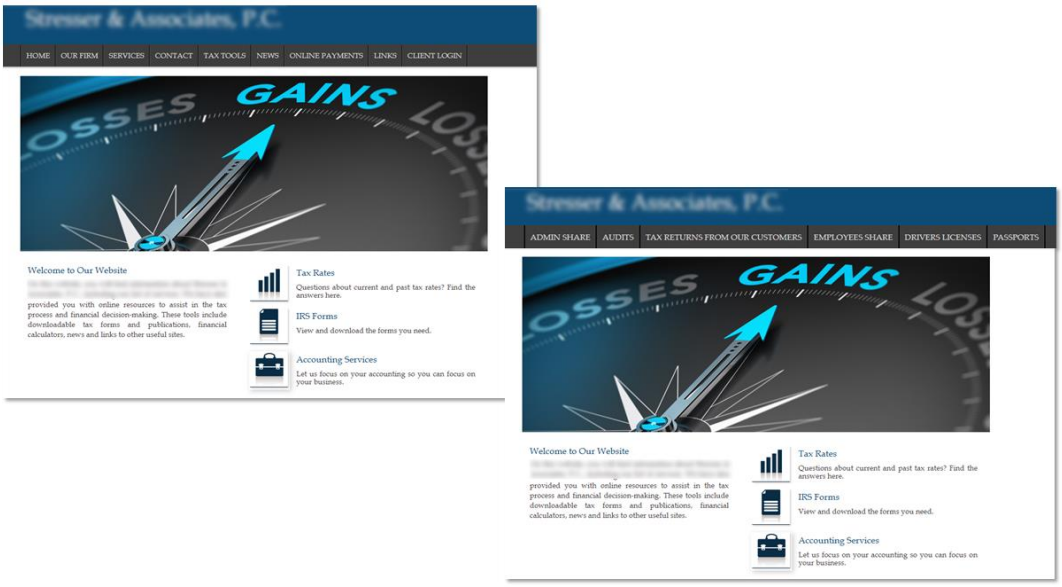


[Figure 14] Opening a dark web leak and search site

In June 2022, the BlackCat group began to leak 112GB of data stolen from Allison Hotel. After posting the data on the leak site, it opened ClearNet[25], which allows you to search for sensitive information about 1,500 employees and guests leaked from the hotel. In addition, data related to the hotel was posted so that it could be exposed at the top in search engines. Possibly, the purpose of opening such a site is to scare employees and customers and induce companies to request deletion of their data from ClearNet.

[25] ClearNet: An Internet site or website that anyone can access publicly

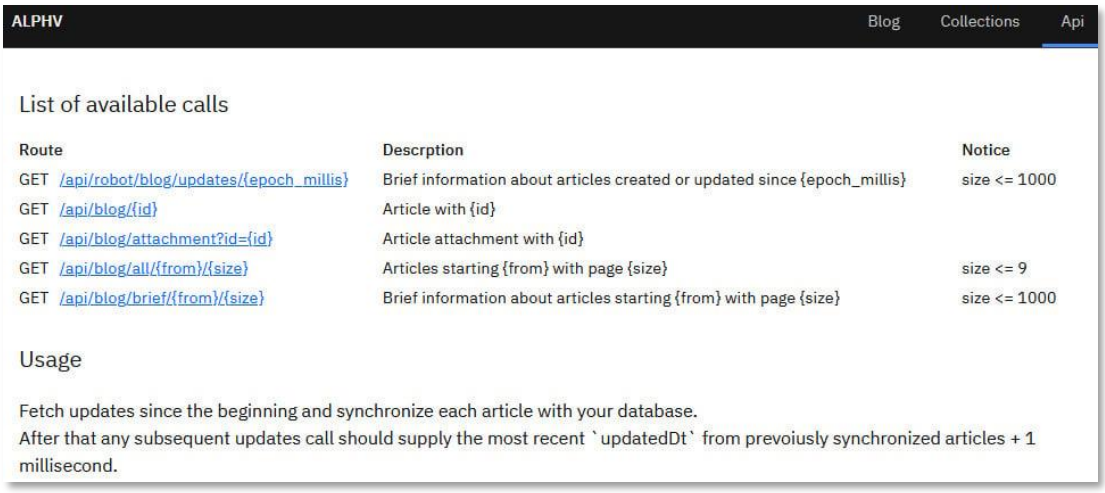
- **Through TypoSquatting, the data of the victimized company is leaked from a page which it was lured to.**



[Figure 15] TypoSquatting and imitating the victimized company's webpage
(victimized company's page/BlackCat data leak page)

In December 2022, the BlackCat group included financial companies on the data leakage site list and began to leak data when ransom negotiations failed. Furthermore, the BlackCat group induced TypoSquatting by creating a domain similar to the company's domain, and even imitated the victimized company's website, leaking 3.5GB of data, including employee information, assets and expenditure details, and passports.

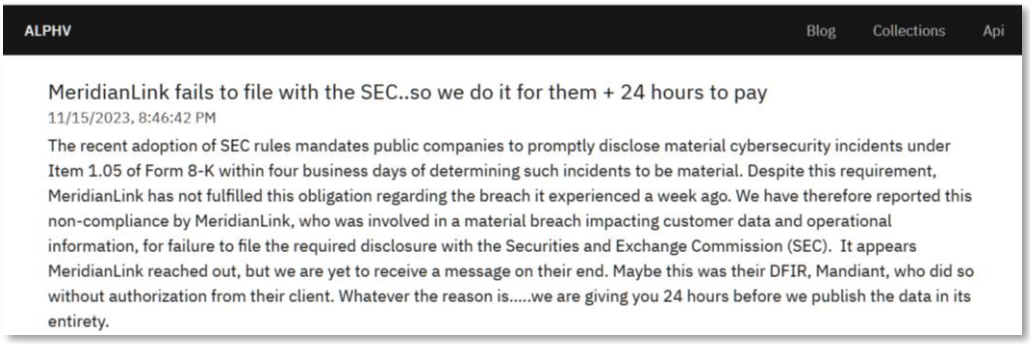
- **Providing API to obtain detailed information of the victimized company**



[Figure 16] Providing API to obtain detailed information of victimized companies

In July 2023, the BlackCat group began to support an API that can fetch detailed information about victimized companies posted on data leakage sites, and also provided a crawler written in Python that can use the API. It seems that the purpose is to raise the level of threats to collect ransom money as the number of victims paying ransom to the BlackCat group decreases.

- **Companies that did not pay the ransom can be sued by the SEC (Securities and Exchange Commission).**



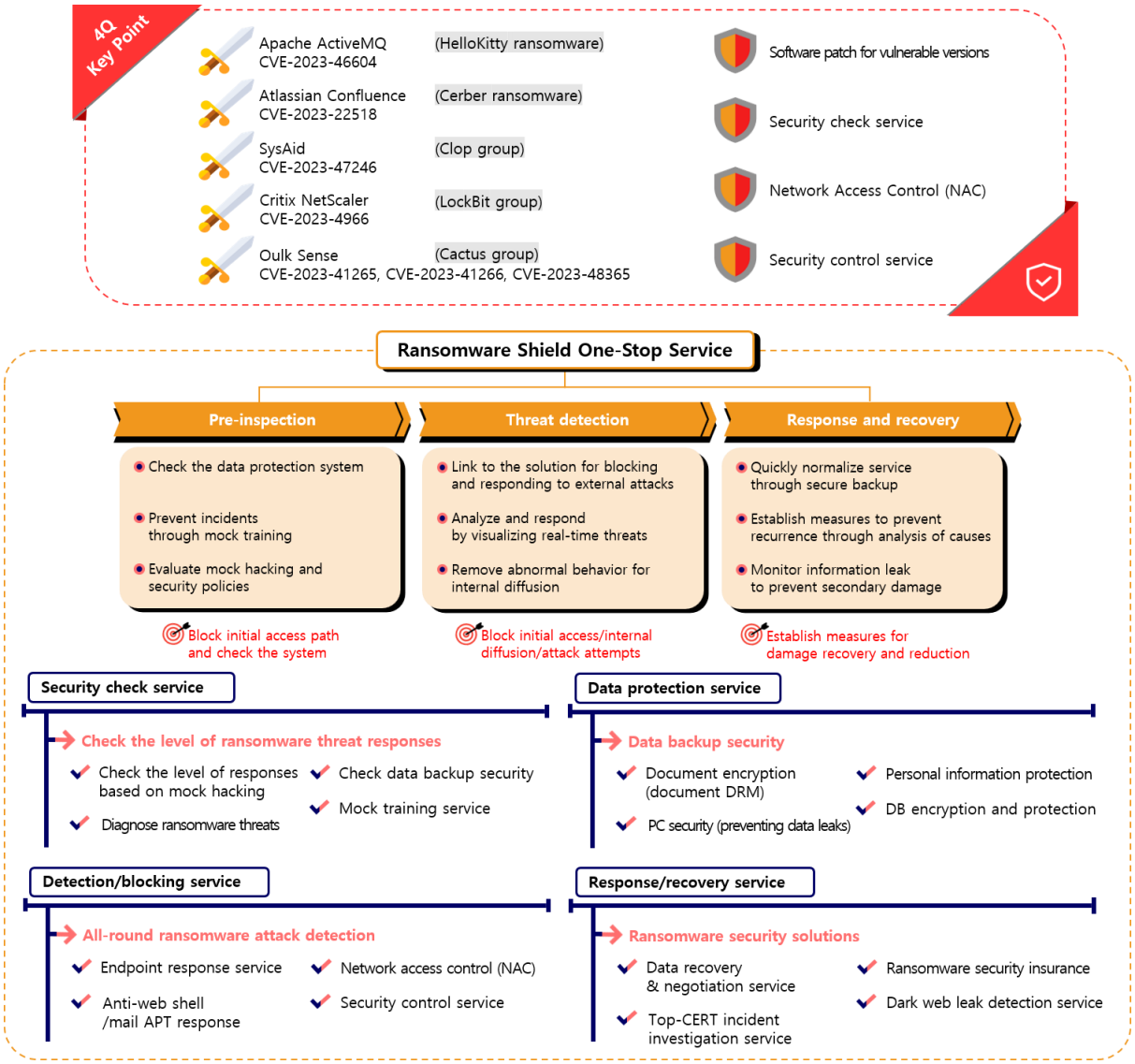
[Figure 17] Threatening to file a complaint about the victimized company with the SEC

In November 2023, the BlackCat group posted MeridianLink, a software company, on a data leakage site and began threatening to leak data if a ransom was not paid within 24 hours. Furthermore, the BlackCat group posted a photo of the complaint form, saying that it would file a complaint against MerdianLink for failing to report to the SEC (Securities and Exchange Commission) despite an incident in which customer data and operational information was stolen. When the ransom was not paid 24 hours later, it posted the photo of the complaint.

It can be seen as a strategy to induce ransom payments by exploiting the fact that listed companies must report within 4 days when an incident that has a significant impact or affects investment decisions occurs to the SEC (the Securities and Exchange Commission of the US), as cyber incidents continue to occur in the United States. However, since the regulation was scheduled to take effect on December 15, 2023, it is known that it had no actual legal effect.

Ransomware mitigations

To select attack targets, attackers perform reconnaissance in various ways through the strategies established by the attacker group. Then, the attackers access the internal infrastructure, encrypt files, threaten assets, and attempt to threaten by leaking data. To prevent such damage, it is necessary to provide against targeted APT attacks and prepare appropriate security elements and processes for each stage of penetration to be able to detect and block the attacker group before it achieves its goal.



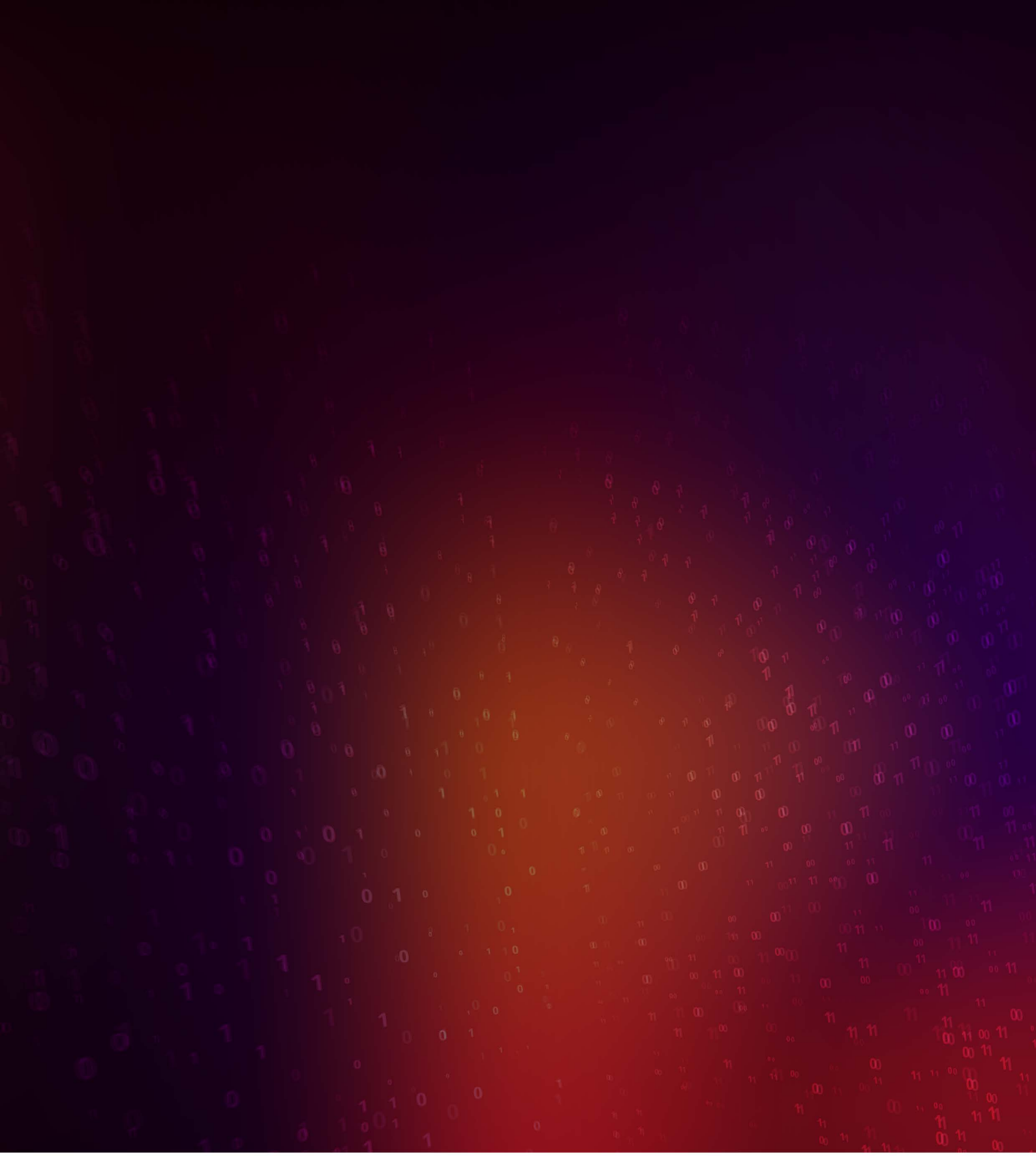
Appendix

Ransomware group	Period of activity	Description
BlackCat	2021.12~	DarkSide/BlackMatter rebranding version, a large group with the third largest number of victims to date
BlackMatter	2021.07~2021.11	It was released through the Exploit Forum, and it is a rebranded version of DarkSide. Its activities were terminated under pressure from investigative agencies such as the FBI.
BlackSuit	2023.05~	This group disclosed domestic golf-related software developer data on the dark web in December 2023.
Cactus	2023.03~	As the data required for ransomware operation is encrypted, a decryption key is required during execution. So a detection avoidance strategy is used.
Cerber	2016.03~2017.09	There are various versions (1-6.0.1), and it is mainly distributed using the normal network of advertising services, and it performs attacks against an unspecified number of people.
Clop	2019.02~	After the release of the decryption tool, it focuses on data takeover and uses large-scale attacks through vulnerabilities as its main strategy. It is a large group with the fourth largest number of victims to date.
DarkSide	2020.08~2021.05	In May 2021, it attacked the Colonial Pipeline, one of the largest oil pipelines in the United States, causing extensive damage, after which the FBI recovered cryptocurrencies and its activities were terminated.
Dharma	2016.11~	While extensions, which are changed after encryption of the variants of the CrySis ransomware, are continuously discovered, the leader of the group using the Dharma ransomware was arrested in December 2023.
DragonForce	2023.12~	This group leaked 95GB of data after an attack on Yakult's Australian branch and stole about 600GB after an attack on the Ohio lottery system

GhostSec	2015~	This group was formed to attack Islamic extremist groups. It began to sell GhostLocker RaaS through the Telegram messenger in October 2023.
HelloKitty	2020.11~	This group performs attacks by exploiting the penetration test tool CobaltStrike or phishing and the vulnerabilities of the Apache server. In October 2023, the source codes of the 2020 version were leaked.
Hive	2021.06~2023.01	There are various versions (1-6), and some versions can be decrypted. It was one of the most active large groups, but was shut down by the FBI in January 2023.
Hunters	2023.10~	This group has some connection with the Hive ransomware. Approximately 56% code similarity was confirmed with the v6 version of the Hive ransomware.
LockBit	2019.10~	It is the most influential ransomware group to date. It is operating LockBit 3.0 through several version updates, and continuously performs attacks in Korea through resume/copyright-related phishing.
LockerGoga	2019.01~2021.10	This group caused an estimated damage of about $104 million. An attacker who jointly operated LockerGoga and MegaCortex, was arrested in October 2021, and a decryption tool was provided in September 2022
MalekTeam	2023.12~	This is an Iranian hacker group. It slanders Israel and Zionism and attacks Israeli military-related institutions and hospitals
MegaCortex	2019.01~	In October 2021, an attacker who jointly operated LockerGoga and MegaCortex, was arrested, and a decryption tool was provided in January 2023.
Meow	2022.08~	This group carries out attacks using the source codes of the Conti ransomware that was leaked in September 2020
NoEscape	2023.06~2023.12	Due to the similarities in encryption methods and ransomwares, its connection with the Avaddon group has been confirmed, which ceased operations in 2021. When the group operator fled after Exit Scam in December 2023, it ceased operations.

Phobos	2018.12~	It is a variant of the Dharma ransomware and mainly performs attacks by initially accessing RDP ports that are using vulnerable passwords.
Qilin	2022.10~	This group disclosed data of a domestic electronic component manufacturer on a dark web leak site in November 2023,
RagnarLocker	2019.12 ~ 2023.10	This group initially accesses vulnerable RDP ports and carries out attacks. When its core manpower was arrested by Europol in October 2023, its activities were suspended.
RansomedVC	2023.08~2023.11	This group partnered with the Stormous Everest group, and in early November 2023, pressure from investigative agencies led to the arrest of officials and suspension of operations.
Raznatovic	2023.12~	A group that purchased and uses the infrastructure of the RANSOMEDVC group which was closed in November 2023
Rhysida	2023.05~	This group posted confidential documents of the Chilean Army on a data leakage site in May 2023
SiegedSec	2022.04~	This group is cooperating with the GhostSec group. It performs attacks by exploiting SQL injections and XSS vulnerabilities, and leaks data through dark web forums.
Soldiers of Solomon	2023.10~	This is a pro-Palestine hactivist group. It uses the Crucio ransomware, a ransomware-as-a-service, and carries out attacks on facilities and institutions in Israel.
Trigona	2023.04~2023.10	This is a ransomware group with pro-Russian tendencies. Its operations were suspended by the Ukrainian Cyber Alliance (UCA) on October 17, 2023.
ViceSociety	2021.05~	The group uses Russian and initially focused its attacks on the education industry, but is currently targeting various industries.
WereWolves	2023.12~	This group carries out attacks against Russian companies, and is conducting website and ransomware bug bounty similar to those of the most influential LockBit group.

[Table 2] Description of ransomwares and groups



Technology for Everyday Safety | SK shieldus

23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea
https://www.skshieldus.com

Publisher : SK shieldus EQST/SI Solution Business Group & KARA (Korea Anti Ransomware Alliance)
Producer : SK shieldus Marketing Group