KARA
Korea Anti Ransomware Alliance

2024.05

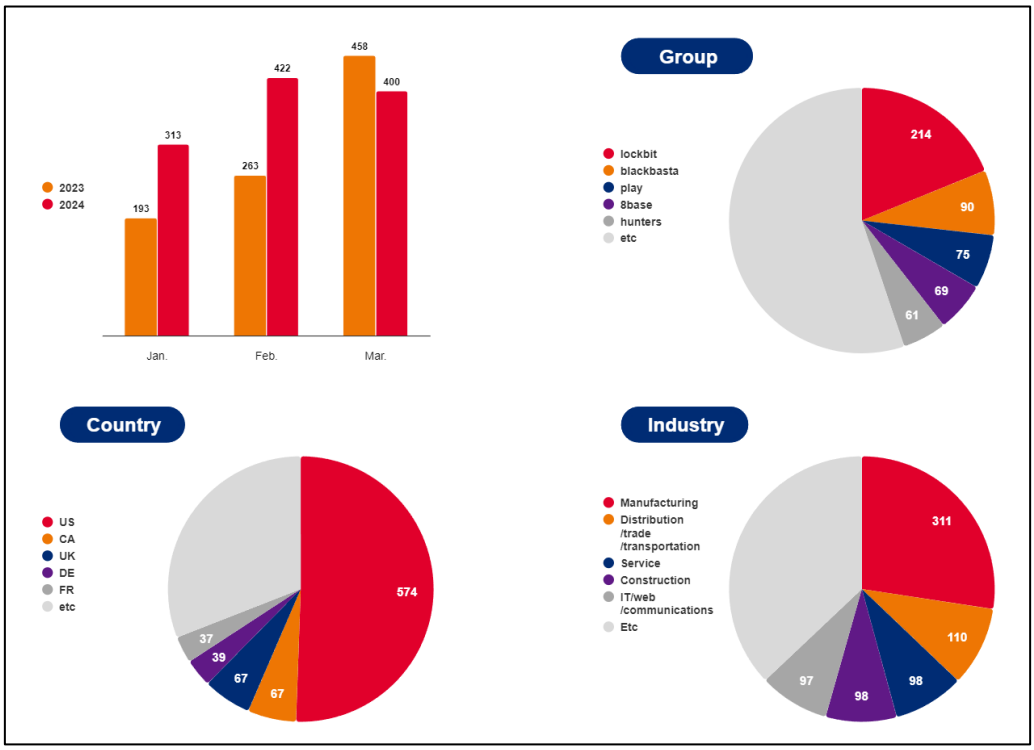
KARA ransomware trend report

KARA ransomware trends report

Lee Hyuna, Jeong Minsu, Lee Hoseok, EQST Lab Team

Ransomware trends

1. Q1 Statistics on Ransomware Activities



[Activity of ransomware groups]

The number of cases of damage from ransomware in the first quarter of 2024 increased by about 23% to 1,122 compared to 914 in the previous quarter. Despite a succession of news reports about the suspension of BlackCat(Alphv)'s activities, the seizure of LockBit's infrastructure, and the release of a decryption tool for the Rhysida ransomware, ransomware continues to cause damage.

The LockBit group, which is the biggest culprit, had major infrastructure seized and group members arrested as a result of the international collaboration Operation Cronos.[1] Nonetheless, LockBit has resumed its activities using new infrastructure.

[1] Operation Cronos: A cyber disruption operation to destroy the criminal ecosystem of LockBit.

As for Black Basta, after a flaw in encryption logic was found in some samples discovered around April 2023, the decryption tool Black Basta Buster was developed. However, the flaw was eventually patched and the decryption tool no longer works with newer versions of the ransomware. Recently, it was confirmed that Black Basta had attacked a vulnerable server by exploiting the CVE-2024-1709[2] ScreenConnect[3] vulnerability of ConnectWise. This caused a big issue and it was found that the ScreenConnect vulnerability was being exploited not only by Black Basta, but also by the LockBit and Bloody groups. Recently, the Play group was also confirmed to have joined the ranks.

The Play group became an issue after its attack last year on Xplain, a company that provides software solutions to the Swiss government and military, was officially confirmed. Approximately 65,000 government documents were leaked in the attack, and these were posted on a dark web leak site in May of last year. However, the Swiss government only revealed in an official statement in March that government documents were part of the leak and that the documents contained sensitive information and confidential information, raising the possibility of secondary damage. So there is a clear need for measures to address the problem of ransomware.

In early March, the BlackCat(Alphv) group extorted approximately 350 BTC (KRW 31 billion) from UnitedHealth's Change Healthcare, but did not distribute the profits to its affiliates. As a result, a user named "notchy," presumed to be an affiliate, posted a report on a dark web forum expressing dissatisfaction. notchy also posted a Bitcoin address as proof of the fraudulent activity of BlackCat(Alphv) and provided transaction records showing the receipt of 350 BTC on March 1. A few days later, BlackCat(Alphv) pretended that the dark web leak site had been seized by law enforcement agencies and disappeared, suspending its activities.

As in the above case, various ransomware incidents are occurring and more cases of damage are steadily being discovered, including cases of vulnerabilities being exploited for large-scale or supply-chain attacks.[4] In addition, ransomware groups use a variety of strategies, such as exploiting legitimate tools or drivers[5] to bypass detection or broadening their attack targets to make up for poor performance. So organizations are recommended to put the proper security policies in place and keep their systems up to date.

---

[2] CVE-2024-1709: Authentication bypass vulnerability occurring in ScreenConnect version 23.9.7 and earlier

[3] ScreenConnect: Remote desktop software that allows you to remotely control your computer over the Internet or another network

[4] Supply chain attack: A technique in which the attacker penetrates the supply process of a product or service, affecting all users

[5] Driver: Software that enables communication between the operating system and hardware devices

2. Trends in Ransomware

✓ Attackers abusing legitimate tools

Previously, ransomware groups tended to create and use customized tools for attacks. Representative examples include the Ryuk group's customized data theft tool Ryuk Stealer and the LockBit group's StealBit. However, such groups have recently switched to LotL (Living off the Land) attacks,[6] which exploit legitimate tools or commercial RMM (remote monitoring and management) tools[7] in the victims' systems to bypass detection.

Recently, after the Cactus ransomware group carried out an attack on Schneider Electric, a global energy company, it was found that tools such as AnyDesk, Splashtop, and SuperOps[8] had been distributed to the victims' systems and exploited for initial access and internal propagation. The LockBit ransomware group has exploited the Citrix Bleed vulnerability CVE-2023-4966[9] to gain initial access, then installed remote access solutions (ScreenConnect, TeamViewer, etc.), and exploited legitimate tools on the victims' systems to perform attacks.

Ransomware groups are strategically using RMM and other tools already installed on systems for various attacks to bypass detection in initial access, information leakage, internal propagation, and so on.

✓ Vulnerable drivers used in ransomware attacks

The BYOVD (bring-your-own-vulnerable-driver) technique exploits a vulnerable driver that is recognized as a normal driver by the system because it has a legitimate signature. This technique began to attract attention last year after its use was confirmed in ransomware attacks, and this year, it was confirmed that the Kasseika ransomware group used the BYOVD technique in an attack to bypass security solutions.

---

[6] LotL attack: An technique in which the attacker uses software or tools already installed on the system to evade detection and perform malicious actions

[7] RMM tool: Software that allows you to monitor and manage computers and network equipment from a remote location

[8] AnyDesk, Splashtop, SuperOps: Cloud-based remote desktop and IT management solutions

[9] CVE-2023-4966: A sensitive information exposure vulnerability that occurs in certain and earlier versions of NetScaler ADC and Citrix NetScaler Gateway

As the BYOVD technique is executed at the kernel level using a signed driver, it is able to easily bypass security solutions due to having system privileges, which are higher than administrator privileges. A representative case of a BYOVD attack is the Lazarus group's[10] exploitation of domestic security solutions for initial access followed by the use of a vulnerable driver module to neutralize anti-virus software. Originally, the BYOVD technique was mainly used by APT groups[11] such as Lazarus, but it has now been taken up by ransomware groups such as BlackByte, Cuba, Akira, and AvosLocker for ransomware attacks. In the first quarter, the Kasseika group also joined the ranks when they disabled a security solution by downloading a vulnerable driver from the victim's system with the privilege to disable the solution and executing it, and then distributed ransomware to encrypt the system.

✓ **Diversification of attack targets**

Many RaaS (Ransomware-as-a-Service)[12] groups operate by establishing their own regulations and imposing penalties on affiliates that do not comply with them. Of course, the regulations are different for each group, but one common rule is the prohibition of attacks on major infrastructure, such as medical, educational, and non-profit organizations. As attacking such organizations can cause significant social chaos, ransomware groups that do so are more likely to be targeted by investigative agencies, so the majority of them exercise caution.

As the rate of ransom payments by victims of ransomware decreases, however, ransomware groups have faced a decline in profits. Consequently, attackers are increasingly turning their attention to major infrastructure due the fact that paralyzing such a system will inevitably result in public inconvenience and significant damage.

The Cactus ransomware group attacked Petersen Health Care, a healthcare organization in the United States that was experiencing financial difficulties, leading it to bankruptcy. BlackCat(Alphv) extorted about 350 BTC (KRW 31 billion) from UnitedHealth's Change Healthcare, and one attacker halted the operation of about 100 hospitals across Romania through the BackMyData ransomware attack, a variant of Phobos ransomware. If the number of attackers who aim to inflict greater damage by disrupting or threatening to disrupt the operations of major infrastructure to extort large sums of money increases, so does the risk of social chaos. So there is a need to closely monitor these trends and prepare for them.

---

[10] Lazarus group: A hacking group affiliated with North Korea's Reconnaissance General Bureau

[11] APT group: A state-sponsored hacking organization focused on conducting sophisticated and long-term cyberattacks

[12] RaaS: Short for 'Ransomware as a Service,' where ransomware groups provide ransomware to affiliates or attackers in exchange for compensation.

✓ **Closure of ransomware groups and emergence of decryption tools**

The bad news continued for ransomware attackers in the first quarter of 2024 with the successive seizures of infrastructure of large ransomware groups by law enforcement agencies and the release of various ransomware decryption tools.

LockBit, a representative of the RaaS group, had infrastructure seized by international law enforcement agencies in February 2024. It was expected that this would lead to the group shutting down due to the disclosure of LockBit-NG-Dev (LockBit-NextGeneration-Development), which is presumed to be LockBit 4.0, and StealBit, a customized data theft tool, as well as the decryption keys and more, but they resumed activities through a new dark web leak site.

Indications of an exit scam[13] by BlackCat(Alphv), another large RaaS group, were also discovered. On the Russian hacking forum RAMP,[14] an affiliate called "notchy" posted an article expressing dissatisfaction over not receiving any of the 350 BTC (approximately KRW 31 billion) in profits earned from the Change Healthcare attack, and provided a Bitcoin wallet address and transaction details as evidence, igniting a controversy. Afterwards, BlackCat (Alphv) pretended that the dark web leak site had been shut down by law enforcement agencies, but the NCA and FBI claim that they had nothing to do with it, raising suspicions about an exit scam. Later, BlackCat(Alphv)'s Tox messenger[15] status message was changed to "Selling source codes 5kk," indicating an intention to sell the ransomware source codes for USD 5 million (approximately KRW 6.7 billion) and practically confirming the suspicions of an exit scam.

Ransomware decryption tools are also being released steadily. Some representative examples include the decryption tool for the Rhysida ransomware developed by Kookmin University and KISA, and decryption tools for the Tortilla ransomware, a variant of the Babuk ransomware, BlackBasta samples distributed in April, and some variants of the Mallox ransomware distributed from October 2022 to February 2024.

[13] Exit Scam: Fraudulently stopping business without paying and then disappearing

[14] RAMP: A Russian-based hacking forum that sells hacking tools or exchanges related information on the deep and dark web

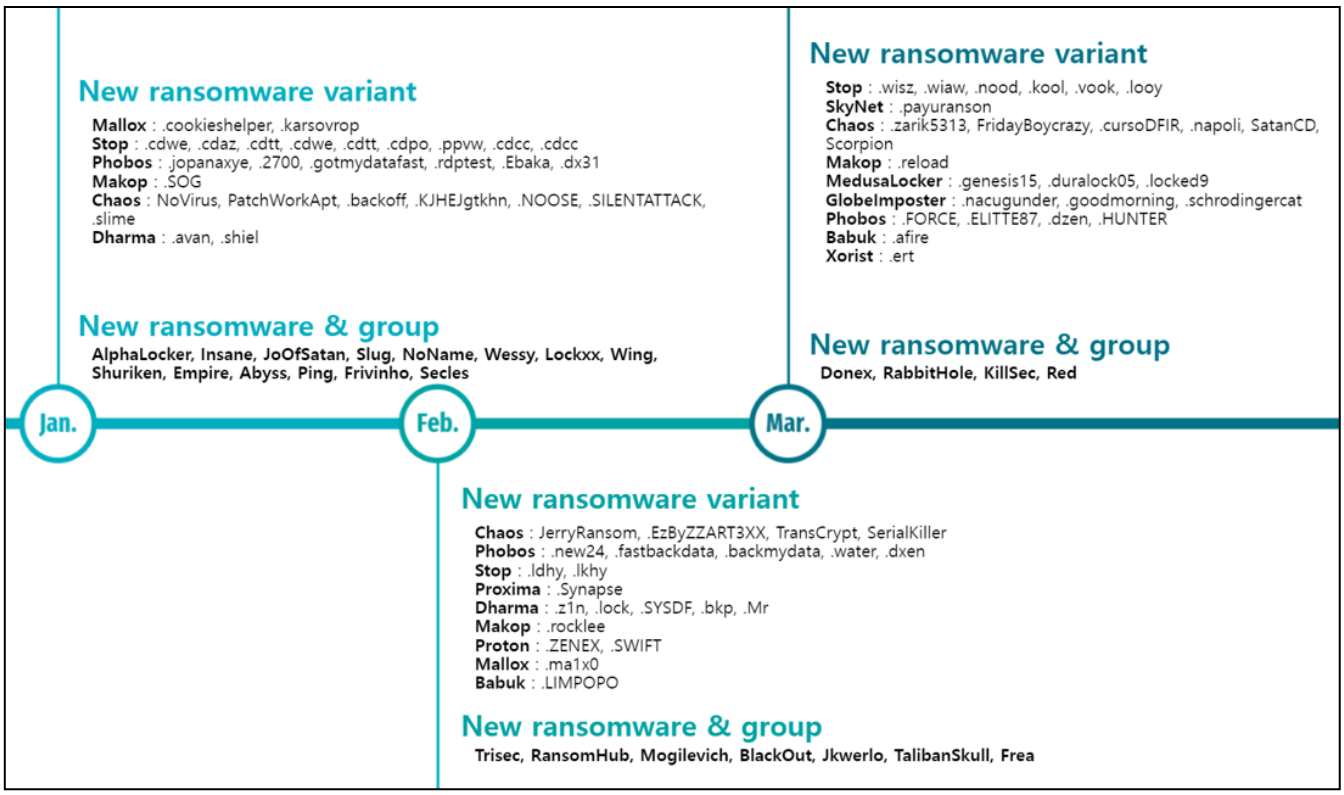
[15] Tox messenger: A messenger that provides messaging and user privacy features

Considering the above, one might conclude that ransomware threats have decreased, but in reality, the number of recruitment advertisements for affiliates has been rapidly increasing in dark web forums. The vacancies are being filled by small RaaS groups. In one example, the Medusa group says in its recruitment announcement that, in addition to cooperating with existing RaaS groups, it will increase the share paid to affiliates to 70-90% and it operates a premium membership system, both attractive options.

In order to restore trust in the RaaS ecosystem, which was damaged by BlackCat (Alphv), the RansomHub group operates in such a way that affiliates extort ransom money directly and then deliver only a portion of the payment to the operator. It has also established rules that allow affiliates to work for multiple RaaS groups at the same time, declaring that this would calm the anxiety of its affiliates. The Cloak ransomware group provides 85% of ransom payments to affiliates and recruits only through an interview process, with no need to make a down payment.

While large ransomware groups are experiencing a crisis, the movement of small RaaS groups to attract departing personnel to their organizations is expected to continue for some time. In other words, ransomware attackers who were previously active are now moving to other groups. So rather than saying that the actual threat of ransomware has been reduced, we can say that changes are taking place in the RaaS ecosystem.

3. New Ransomware and Group Activities



[New/variant ransomware]

In the first quarter, 11 new ransomware groups were discovered. The AlphaLocker group has claimed attacks on nine organizations so far, and has already leaked data from eight. The Insane, JoOfSatan, and Slug groups recently opened dark web leak sites, but these sites are currently not accessible. The Donex group is using the DarkRace series of ransomware, and has so far leaked data from five organizations. The RabbitHole group has only opened a dark web leak site, while the BlackOut group has posted data they stole from a Canadian manufacturer and a French general hospital on the dark web leak site they operate. Below are descriptions of the major new ransomware groups.

- **NoName**

  The NoName group's dark web leak site uses a format similar to that of LockBit's leak site, so a connection between the two groups is suspected. In addition, in 2023 the leaks by the NoName group were found to be consistent with the organizations victimized by LockBit, and even the format of the ransom note was found to be very similar. This appears to be a move by the NoName group to gain prominence by imitating LockBit. Recently, it was confirmed that NoName's DDoS attacks led law enforcement agencies to carry out Operation PowerOFF,[16] under which a clear website[17] was seized.

- **Trisec**

  Unlike other ransomware groups that demand the ransom directly from the victims, the Trisec group asks the victims to make the initial ransom offer. In addition, they are presumed to be based in Tunisia, not Russia or China. The Telegram channel and dark web leak site operated by Trisec contain the Tunisian flag and phrases praising Tunisia, and posts articles on forums that recruit attackers from Tunisia. Currently, their dark web leak site is shut down.

- **RansomHub**

  The ransomware used by the RansomHub group is based on the Go language,[18] and they claim they don't carry out attacks against Cuba, North Korea, China, Romania, or CIS countries.[19] In addition, they will not carry out additional attacks against organizations that have already paid a ransom once. The company announced that they will take action against affiliates that violate these rules. A BlackCat(Alphv) affiliate, 'notchy,' claimed that he or she possessed company data used during an attack, and that he or she used it to attack Change Healthcare once again in cooperation with RansomHub.

---

[16] Operation PowerOFF: An operation launched by a coalition of international law enforcement agencies to shut down DDoS attack service infrastructure

[17] Clear web: A website accessible through a common search engine

[18] Go language: An open source programming language developed by Google to increase productivity

[19] CIS countries: An international organization of countries that gained independence after the dissolution of the Soviet Union. They include Russia, Moldova, Belarus, Uzbekistan, Kazakhstan, etc.

- **Mogilevich**

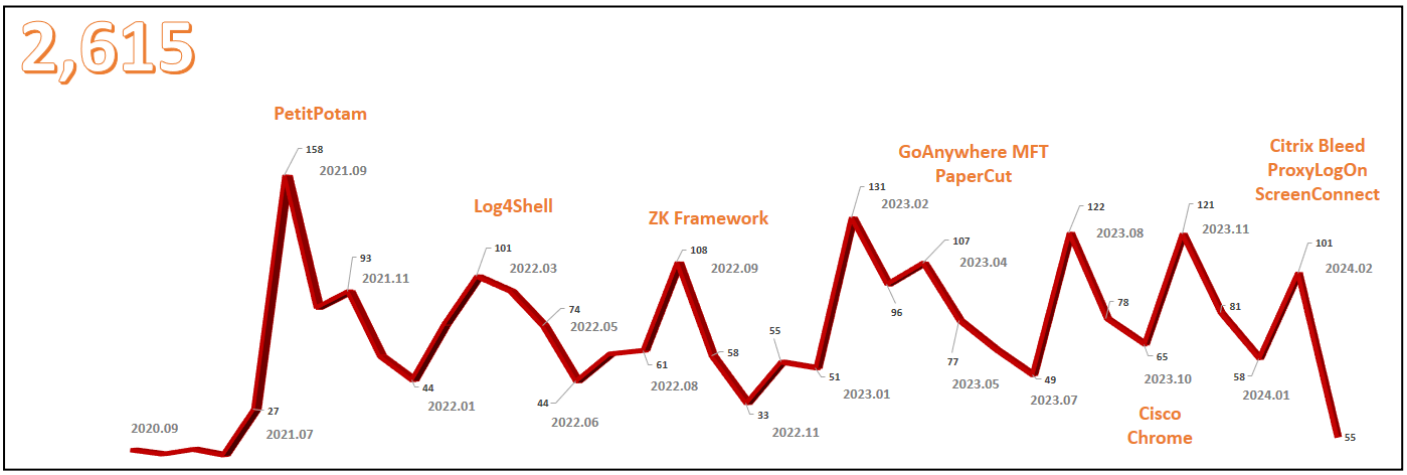
  Mogilevich claimed to have stolen data about Epic Games, an American video game distributor and software developer, and documents from the Irish Ministry of Foreign Affairs, but as no evidence was provided, opinions varied as to the veracity of the claim. In the end, they admitted to being a fraudulent organization, not an attack group, and after disclosing profits amounting to approximately KRW 160 million, they disappeared.

- **KillSec**

  This group started operation in 2023, and on October 24, 2023, they opened a Telegram channel to continued their activities. On November 13, they posted 200,000 pieces of data stolen from a Romanian police organization on Telegram and claimed to have extorted EUR 1,500 (approximately KRW2.21 million), but the authenticity of this claim has not been confirmed. Later, on March 22, their dark web leak site was confirmed and an overview was revealed, and they posted the data previously disclosed on Telegram along with the leaked data of four organizations.

■ Detailed Analysis of the LockBit Group

1. LockBit Profile



[Attack cases of the LockBit group]

The LockBit group started operation in September 2019 with ransomware called ABCD. Then, in January 2020, they appeared on a Russian-based forum under the name LockBit and began full-scale ransomware activities. They subsequently launched LockBit 2.0(Red), LockBit 3.0(Black), and LockBit Green, and gradually expanded their RaaS activities, establishing themselves as a large-scale ransomware group both in name and reality. In addition, LockBit has consistently performed phishing attacks disguised as resumes and attacks exploiting one-day vulnerabilities to carry out large-scale attacks.

In June 2022, the builder[20] for LockBit 3.0 was leaked, and various ransomware groups including the Bloody, Synapse, Buhti, and Darkrace groups borrowed the leaked builder and created several variants, which are still being used to this day.

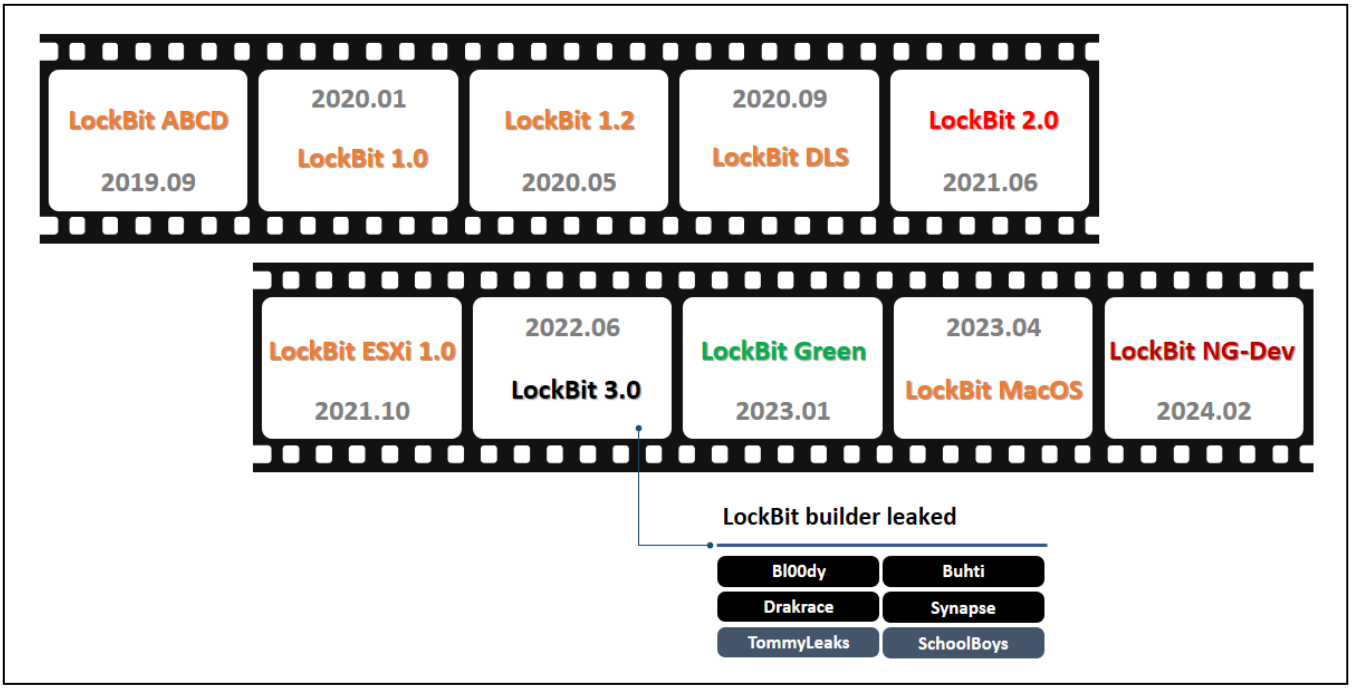
Other than the "LockBit" and "LockBitSupp" accounts, used by at least three people presumed to be operators, the members of LockBit were not known. However, when the group suffered a major blow through Operation Cronos, a list of active affiliates was leaked by law enforcement agencies. According to this list, there are about 200 affiliates, and it is said that these affiliates were recruited over a two-year period. But according to the operator of LockBit, these 200 affiliates were not linked to actual identities, and the group's infrastructure was not completely destroyed. Nevertheless, the battle with the LockBit group continues. A Russian-Canadian who previously worked as a LockBit affiliate was sentenced to four years in prison and ordered by court to pay a fine equivalent to approximately KRW 1.14 billion.

[20] Builder: A ransomware creation tool with environmental settings for creating ransomware with the desired functions

LockBit has carried out attacks on approximately 2,610 organizations worldwide and the group exerts significant influence, having extorted approximately KRW 200 billion in criminal profits. As such, the LockBit ransomware is continuously distributed in Korea as well. In particular, since phishing e-mails are distributed under the disguise of resumes, job applications, etc., it is necessary to raise security awareness and refrain from downloading attachments to suspicious e-mails.

2. LockBit timeline

✓ **Version history**



[LockBit ransomware version history]

- **LockBit ABCD**

  LockBit version ABCD was discovered in September 2019, and there are three versions depending on the ransom note generated. An unstable version was discovered with a ransom note that contained only the attacker's e-mail address, dark web negotiation site address, and personal ID encoded in Base64.[21] As this was an early version, it appears that several versions exist for strategic selection.

- **LockBit 1.0**

  LockBit version 1.0 was discovered in January 2020, and 74% of its code is similar to that of the existing ABCD ransomware. On January 17, LockBit claimed in the XSS Russian hacking forum that its ransomware, an RaaS, provides several functions and had never been decrypted as of the time of writing. They posted to the effect that they prohibited attacks on CIS countries, individually negotiated ransomware rental conditions, and gave preferential treatment to experienced attackers. RaaS stands for 'Ransomware-as-a-Service' and refers to a cybercrime business model in which a ransomware operator lends their ransomware to affiliates for use in attacks in exchange for payment.

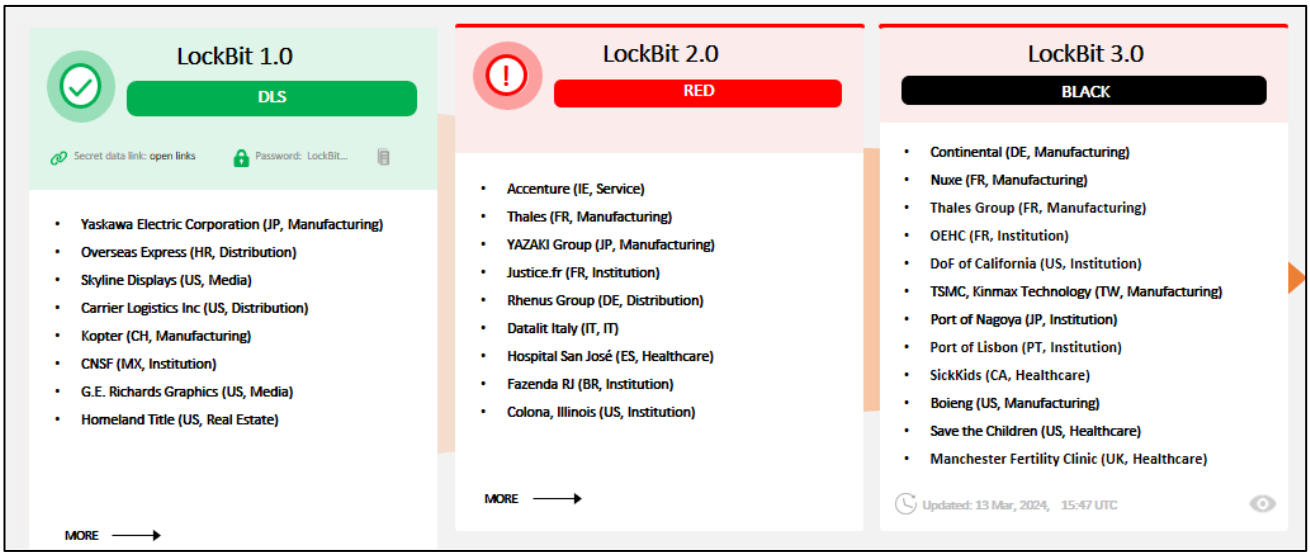
- **LockBit 1.2**

  LockBit version 1.2 was discovered in May 2020, and the major differences from the previous version are that the contents of the ransom note have been changed and an hta ransom note creation and output function has been added. In addition, from then on, it has been operating a dark web leak site.

[21] Base64: An encoding method to convert binary data to ASCII character strings

- **LockBit DLS(Dedicated/Data Leak Site)**

LockBit has also renewed its dark web leak site, as the sample version was updated, and the dark web leak site of LockBit version 1.0 was discovered on September 16, 2020. They employed a double extortion method, wherein they opened a leak site on the dark web to post victims' data, but in the beginning, they did not use their own leak site for several months and cooperated with the Maze ransomware group by posting on its leak site. Then, the renewed leak site for version 2.0 was discovered in early July 2021, and the leak site for version 3.0, which is currently in use, was discovered on June 17, 2022.



[Data leak site changes and cases of damage]

- **LockBit 2.0 (Red)**

  The code of LockBit 2.0 is not similar to that of version 1.0, and LockBit 2.0 was discovered in June 2021. After going through many trials and errors, it has taken shape to a certain extent and this version shows a level of completion similar to the current LockBit. In addition, it has established a more sophisticated attack method through the use of the customized data theft tool StealBit and the use of PsExec[22] for internal propagation. In version 2.0, LockBit applied multi-threading,[23] an I/O completion port,[24] and partial encryption to perform fast and effective encryption, and the encryption algorithm also changed from the existing AES[25] + RSA[26] combination to the AES + Curve-25519[27]/Xsalsa20-Poly1305[28] combination. With this, it is now possible to quickly encrypt even large files while preventing the encryption key from being identified.

ransomware	encryption speeds	Time taken to encrypt a 100GB file
LockBit 2.0	373 MB/s	4 minutes 28 seconds
LockBit 1.0	266 MB/s	6 minutes 16 minutes
Cuba	185 MB/s	9 minutes
BlackMatter	185 MB/s	9 minutes
Babuk	166 MB/s	10 minutes
Sodinokibi	151 MB/s	11 minutes
RagnarLocker	151 MB/s	11 minutes

[Comparison of LockBit ransomware encryption speeds, source: GRIDINSOFT]

[22] PsExec: A utility that allows you to remotely execute programs on another computer on a network

[23] Multi-threading: A technique for creating and executing multiple threads within a program to process multiple tasks simultaneously

[24] I/O Completion Port: System API for efficient asynchronous input/output processing

[25] AES: A type of symmetric key encryption method that encrypts data blocks of a fixed size. It is an algorithm mainly used in ransomware to encrypt files.

[26] RSA: One of the public key encryption methods. It is an algorithm used in ransomware mainly to protect keys that have encrypted files

[27] Curve-25519: A public key encryption algorithm. It performs key exchange using an elliptic curve, which is fast, secure, and easy to implement. In ransomware, it is mainly used to protect the keys that encrypt files.

[28] Xsalsa20-Poly1305: An encryption technique that combines high-performance stream encryption (Xsalsa20) with message authentication code generation (Poly1305) to ensure integrity. In ransomware, it is mainly used to encrypt files.

- **LockBit ESXi 1.0**

  LockBit has created a version of ransomware that can infect Linux and ESXi[29] environments with the goal of targeting various platforms. The basics are the same as LockBit 2.0, but this time, it has adopted a method of selecting full encryption or partial encryption based on execution arguments. The reason for using this encryption method appears to be to perform encryption according to the circumstances of each organization, given that many of corporate servers are Linux or ESXi-based. All VMs (virtual machines)[30] managed through ESXi functions can be encrypted. Once they are infected, serious damage can occur, so caution is needed.

- **LockBit 3.0(Black)**

  LockBit 3.0, the version released in June 2022, is also identified as LockBit Black because the code is approximately 60% similar to that of the BlackMatter ransomware, and a connection between the groups is suspected. There is no evidence of BlackMatter selling source codes, but LockBit 3.0 shows fairly high code similarity and flow. In addition, it was revealed that BlackMatter developers participated in the development of LockBit 3.0, and after BlackMatter's activities were stopped, victims were guided to LockBit's negotiation site, earning it the name LockBit Black.

  In September 2022, three months after LockBit 3.0 was discovered, the LockBit 3.0 builder was leaked. According to "LockBitSupp," an internal developer was dissatisfied with the attitude of the LockBit operators and leaked the builder in retaliation. Just as the Conti and Babuk source codes were leaked in the past, leading to numerous variants, groups such as Bloody, Buhti, and Darkrace have arisen using the leaked LockBit 3.0 builder. The Bloody group is still active today and is known to exploit the PaperCut, PrintNightmare, and ScreenConnect vulnerabilities.

[29] ESXi: A hypervisor that allows the user to run multiple virtual machines on top of physical hardware

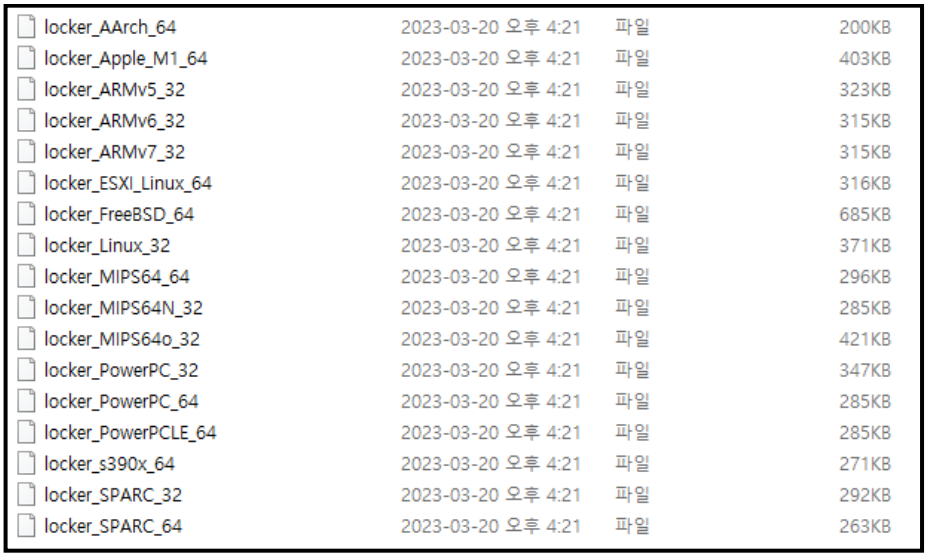
[30] VM: A virtual machine, implemented using software rather than actual physical hardware

- **LockBit Green**

  In January 2023, LockBit released LockBit Green, which borrows from the source code of the leaked Conti ransomware. The source codes of LockBit Green and Conti v3 are about 89% identical. In fact, this version uses the Conti ransomware codes as is, with only partial improvements to the settings and design. Although there are some cases of the Conti ransomware being used in actual attacks, it was confirmed that Conti affiliates preferred to release it rather than using it as a major service.

- **LockBit MacOS**

  LockBit, which was active with LockBit 3.0 and Green, is known to have targeted MacOS as well. The code of the LockBit MacOS variant, which seems to have been made in November 2022, is quite similar to that of a variant of the ESXi version. However, strings related to the Windows OS are listed, and the signature is invalid, so it will not run, and even if it does run, a crash occurs due to BOF (buffer over flow),[31] so it is presumed to be a test version. Variants targeting various platforms such as ARM,[32] FreeBSD,[33] and MIPS[34] were also discovered, indicating that LockBit was aiming to further solidify its position in the ransomware ecosystem.



locker_AArch_64	2023-03-20 오후 4:21	파일	200KB
locker_Apple_M1_64	2023-03-20 오후 4:21	파일	403KB
locker_ARMv5_32	2023-03-20 오후 4:21	파일	323KB
locker_ARMv6_32	2023-03-20 오후 4:21	파일	315KB
locker_ARMv7_32	2023-03-20 오후 4:21	파일	315KB
locker_ESXI_Linux_64	2023-03-20 오후 4:21	파일	316KB
locker_FreeBSD_64	2023-03-20 오후 4:21	파일	685KB
locker_Linux_32	2023-03-20 오후 4:21	파일	371KB
locker_MIPS64_64	2023-03-20 오후 4:21	파일	296KB
locker_MIPS64N_32	2023-03-20 오후 4:21	파일	285KB
locker_MIPS64o_32	2023-03-20 오후 4:21	파일	421KB
locker_PowerPC_32	2023-03-20 오후 4:21	파일	347KB
locker_PowerPC_64	2023-03-20 오후 4:21	파일	285KB
locker_PowerPCLE_64	2023-03-20 오후 4:21	파일	285KB
locker_s390x_64	2023-03-20 오후 4:21	파일	271KB
locker_SPARC_32	2023-03-20 오후 4:21	파일	292KB
locker_SPARC_64	2023-03-20 오후 4:21	파일	263KB

[LockBit ransomware targeting various platforms]

[31] BOF: When a program stores data in a buffer, an error occurs when data is written beyond the allocated memory, which can lead to a security vulnerability.

[32] ARM: Processor architecture optimized for low power consumption; primarily used in mobile devices and embedded systems

[33] FreeBSD: A Unix-series open source operating system

[34] MIPS: RISC(reduced instruction set computing)-based processor architecture

- **LockBit NG-Dev(Next Generation-Development)**

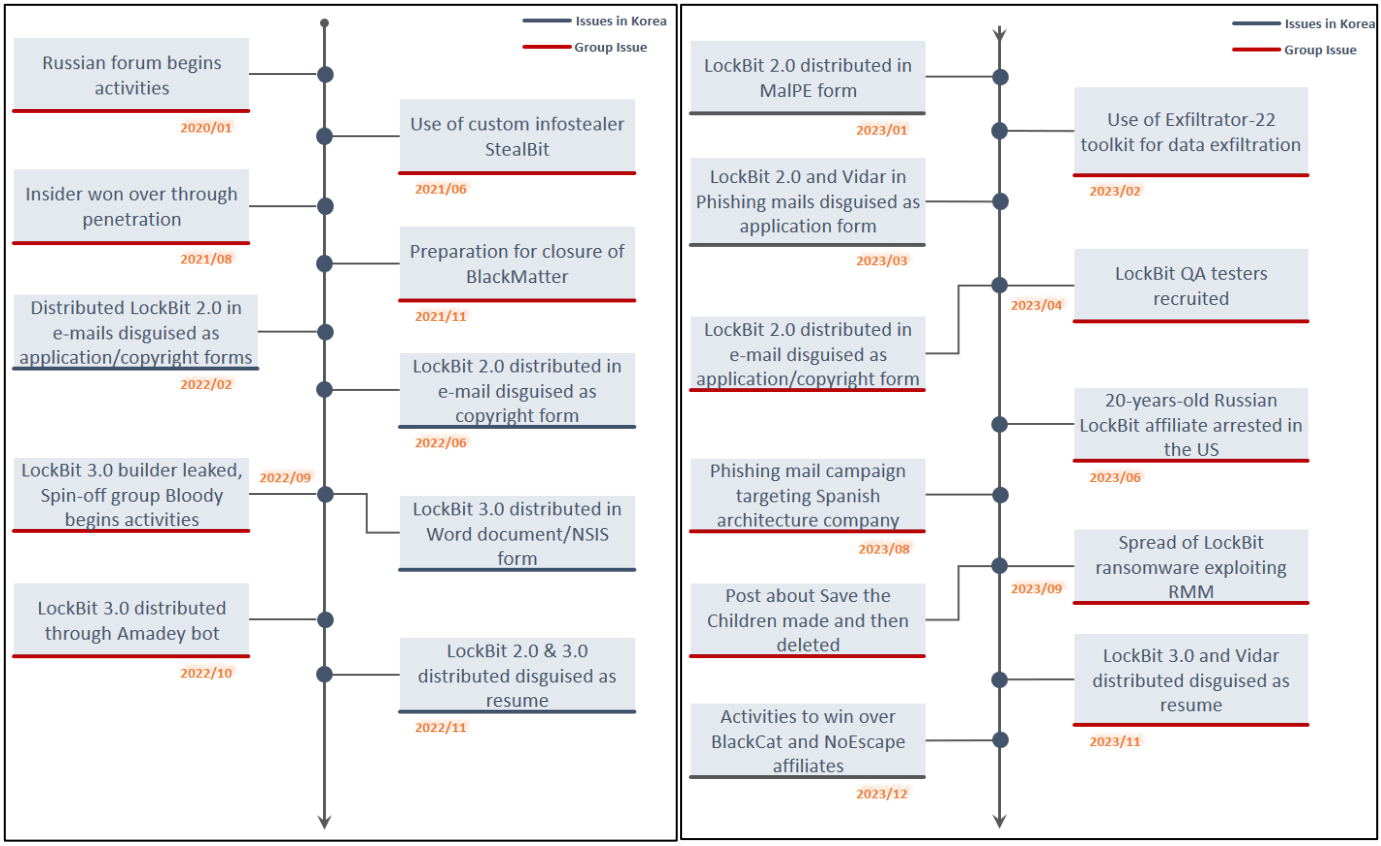
  On February 19, 2024, after an international investigation involving the FBI, LockBit appeared to have finally been neutralized. Its dark web leak site, which had had a long list of victimized organizations, was replaced with a page stating that it had been seized by an investigative agency. Because of CVE-2023-3824[35] vulnerability, the internal system of LockBit was seized, and this is how the NG-Dev version came to light. It is quite different from the previous version of LockBit. It was developed in .NET,[36] and the configuration included some new functions while excluding other functions that had existed in previous versions.[37] Of course, since LockBit did not officially distribute it, there is a possibility that excluded functions will be added, but compared to version 3.0, it was confirmed that the number of functions have been reduced. As of February 24, this was expected to be a new turning point in the ransomware market after LockBit 3.0, assuming that LockBit returns to its original position, resumes activities, supplements NG-Dev and uses it for attacks.

[35] CVE-2023-3824: Improper buffer handling of certain functions in PHP extensions can cause a buffer overflow, leading to a remote code execution vulnerability.

[36] .NET: Windows program development and execution environment developed by MS

[37] Configuration: Files or data containing settings when running ransomware

✓ **Major incidents**



[First major incident of the LockBit group]

The start of LockBit's full-fledged RaaS activities was captured in a Russian forum in January 2020. In June of the following year, StealBit, a customized data theft tool, was launched and began to be used for attacks. StealBit is a customized data theft tool produced by the LockBit group, and is similar to Ryuk Group's[38] Ryuk Stealer and BlackMatter's ExMatter. In February 2023, two years later, LockBit was found to have used Exfiltrator-22, a data theft tool developed by an attacker who was a former affiliate, in an attack, and it appears that they made considerable efforts to build their own infrastructure.

[38] Ryuk group: A group that provides RaaS and is mainly spread through phishing emails or banking malware (currently discontinued)

In a similar context, LockBit also recruited company insiders to reduce fees and establish its own strategy. For ransomware attacks, initial access is performed through methods such as purchasing infostealer[39] logs containing stolen credentials. But in order to reduce the cost and human resources necessary for this process, LockBit decided to carry out the initial access process on its own. In addition, it was the first ransomware group to conduct its own QA test and bug bounty,[40] and it put great effort into strengthening its own technology.

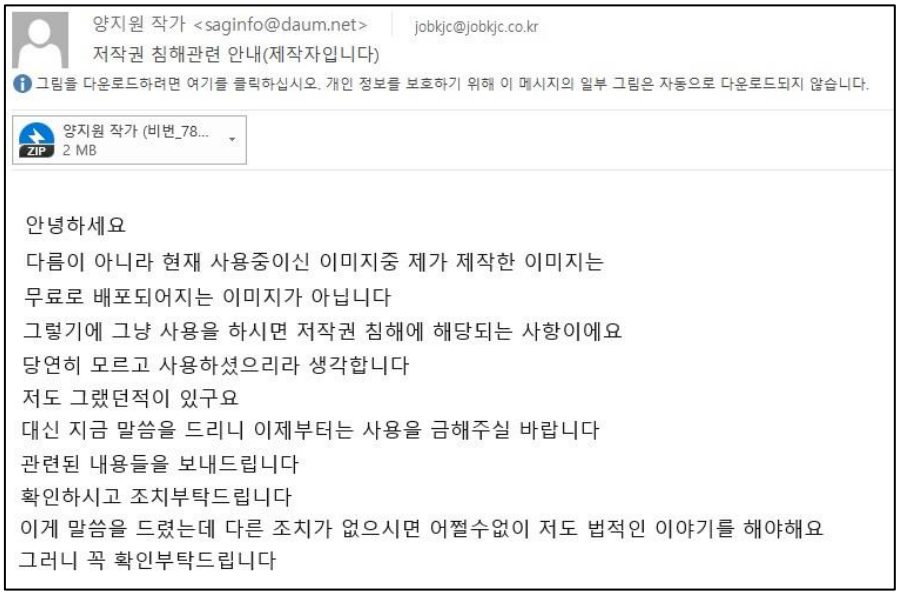
However, starting around September 2023, legitimate RMM tools began to be used for attacks, showing a different trend from before. The use of existing self-made customized tools can be detected and neutralized by security solutions. In order to prevent this, LockBit performed LotL attacks or installed legitimate RMM tools on the victim's system and began exploiting them for information leakage and network expansion.

LockBit has actively been establishing various strategies, but could not avoid a decline in ransom payments. To overcome this, it expanded the targets of attacks by breaking away from the rule prohibiting attacks on sensitive organizations such as non-profit organizations or hospitals. For example, when controversy arose over an incident in which a specific LockBit affiliate attacked the pediatric hospital SickKids Children, they announced that they would expel the affiliate responsible, but within a few months, they attacked the child protection organization Save the Children. Despite receiving social criticism for the attack on a pediatric hospital, following Save the Children, they deleted the announcement from the dark web and attacked a medical institution called Capital Health, demanding money in exchange for 7 TB of data. This suggests that this series of actions was not a coincidence but a planned strategy.

[39] Infostealer: Information-stealing malware that steals credentials or virtual currency wallet addresses

[40] Bug bounty: A system that provides compensation for finding security vulnerabilities in a company's software or system

Meanwhile, the LockBit ransomware is steadily spreading in Korea. It is mainly distributed through malicious e-mails containing attached files disguised as document files, such as copyright infringement and job application forms. In order to avoid classification as spam mail or detection by security solutions, they have shown great care by attaching a compressed file with a password.


양지원 작가 <saginfo@daum.net> jobkjc@jobkjc.co.kr
저작권 침해관련 안내(제작자입니다)
그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.
양지원 작가 (비번_78...
2 MB

안녕하세요
다름이 아니라 현재 사용중이신 이미지중 제가 제작한 이미지는
무료로 배포되어지는 이미지가 아닙니다
그렇기에 그냥 사용을 하시면 저작권 침해에 해당되는 사항이에요
당연히 모르고 사용하셨으리라 생각합니다
저도 그랬던적이 있구요
대신 지금 말씀을 드리니 이제부터는 사용을 금해주실 바랍니다
관련된 내용들을 보내드립니다
확인하시고 조치부탁드립니다
이게 말씀을 드렸는데 다른 조치가 없으시면 어쩔수없이 저도 법적인 이야기를 해야해요
그러니 꼭 확인부탁드립니다

Writer Yang Ji-won
Information on copyright infringement(from the producer)

Writer Yang Ji-won(password_78...
2MB

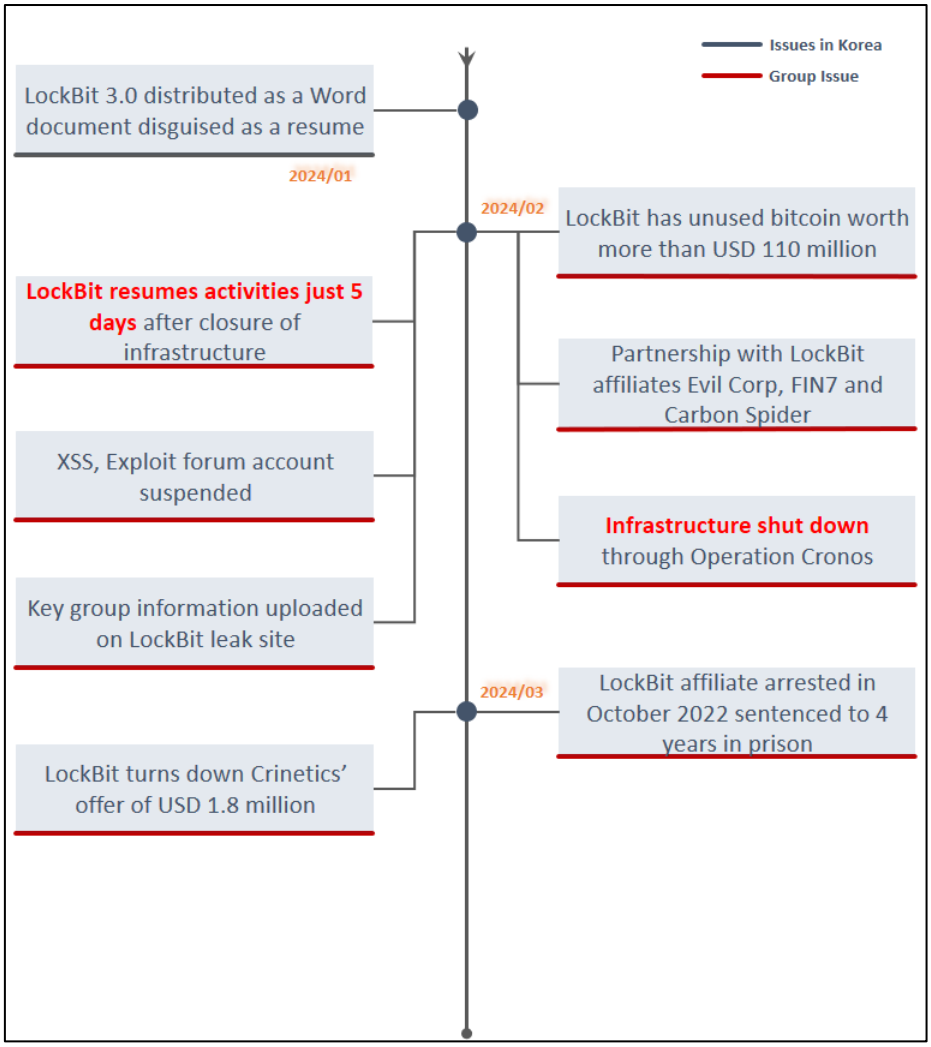
Hi.

Among the images you are using, the images I produced are not distributed for free. So if you are just using them, you are infringing on copyright. I am sure that you were not aware of it. I used to be like that too.

I am telling you now. Please do not use them from now on. I am sending related information. Check it and take necessary measures.

If you are not taking any action even though I told you about it,
I cannot but talk about law. So please check it.

[Malicious e-mail with the LockBit ransomware attached]

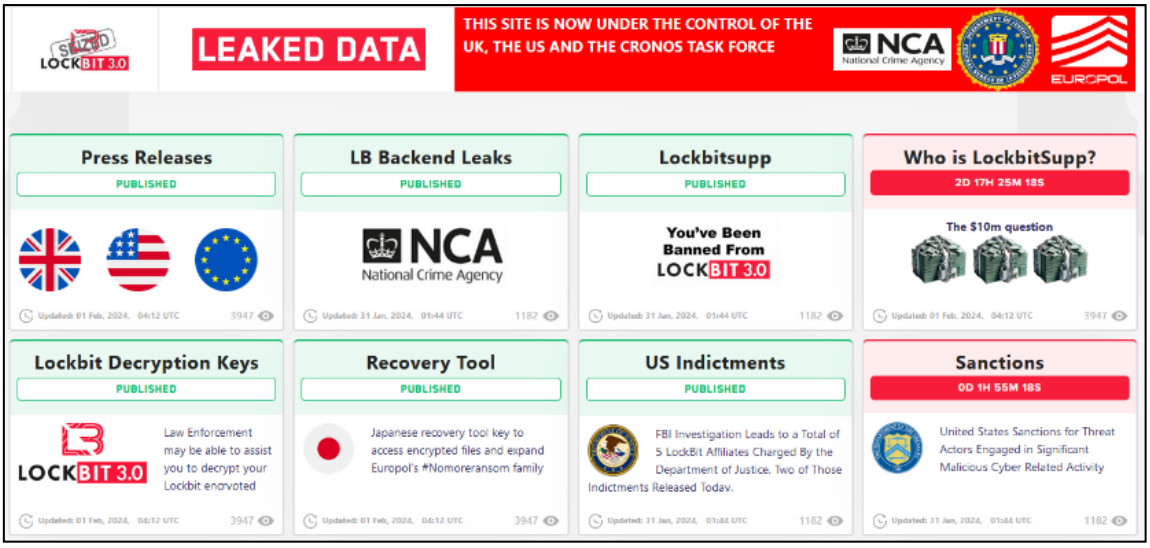


[Second major incident of LockBit group]

BlackCat(Alphv), whose activities are currently suspended due to an exit scam on the operation side, had its infrastructure temporarily suspended due to an error in December 2023. It seems that this occurred due to an operational problem. In addition, around the same time, the NoEscape ransomware group lost its way when affiliates did not receive payment due to an exit scam by the operator. LockBit took advantage of this to recruit affiliates by posting an article on a dark web forum to placate BlackCat(Alphv) and NoEscape ransomware developers.

[Dark web forum post by LockBitSupp]

LockBit's activities, which had been on the rise for several years, seemed like they would last forever, but they also could not avoid the closing police net. On February 20, 2024, LockBit's infrastructure was finally shut down by investigative agencies. Affiliates who participated in attacks were also arrested, one after another, and a bounty of USD 15 million (approximately KRW 20 billion) was placed on the CEO of LockBit. Investigative agencies not only shut down the infrastructure, but also seized internal resources such as StealBit's transit servers, decryption keys, and samples of LockBit NG-Dev, a new version of its ransomware, and disclosed related data.



[Seized LockBit leak site]

The starting point of the incident that broke LockBit's momentum was more mundane than might be expected. LockBit was using an unpatched version of PHP[41] in its internal infrastructure, and the investigative agency penetrated LockBit's system through CVE-2023-3824.[42] The operation became known to the public as Operation Cronos, and it seemed that LockBit, a huge ransomware group, had finally come to an end. However, five days after the infrastructure was seized, LockBit returned with new infrastructure and said in a foreign-media interview that the problem was simply caused by being lazy and not patching the PHP, and that there was nothing wrong with the business. They seemed confident that investigative agencies would not be able to stop them in the future.

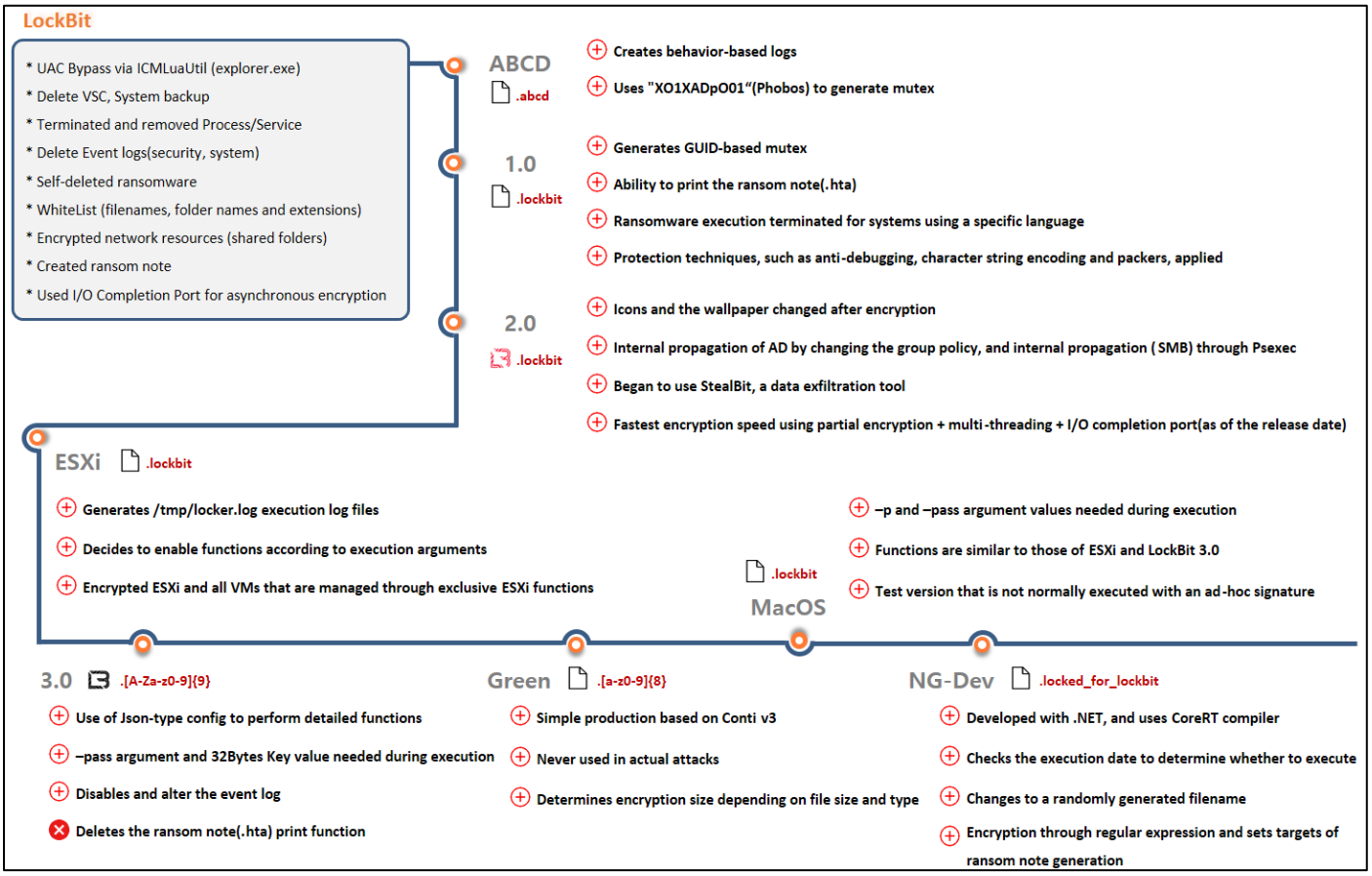
After LockBit's return, affiliate Mikhail Vasiliev, who was arrested in October 2022, was sentenced to 4 years in prison and ordered to pay compensation of USD 860,000 (approximately KRW 1.16 billion). However, LockBit has since attacked more than 70 organizations and continued to make threats by posting stolen data on dark web leak sites. Among them, LockBit threatened Crinetics, a pharmaceutical company, threatening to leak confidential information unless they were paid USD 4 million (approximately KRW 5.3 billion). But Crinetics took a strong stance and ended the negotiations, even though the demand was reduced to USD 1.8 million for financial reasons.

[41] PHP: A scripting language executed on the server side

[42] CVE-2023-3824: A vulnerability resulting from insufficient length checking of filenames within PHP's Phar archive

3. In-depth Analysis of the LockBit Ransomware

✓ Characteristics of each version



[Characteristics of each LockBit ransomware version]

There are several versions of the LockBit ransomware targeting various platforms. Similar functions are supported for each platform, or the different versions have commonalities and differences. They perform common functions such as bypassing UAC (user access control)[43], deleting VSC (volume shadow copy),[44] and terminating processes and services. Details of each version of the LockBit ransomware are provided below.

[43] UAC: A security mechanism that determines whether operations that can affect the system are permitted

[44] VSC: The ability to create point-in-time backup copies of files or volumes in the Windows system

- **ABCD**

  ABCD is the predecessor of LockBit. It records the actions performed by creating "resultlog.reg" and "resultlog.dll" files. A mutex[45] is created to prevent duplicate execution, and the character string used at this time is "XO1XADpO01," which is the same as the mutex used by the Phobos ransomware. In addition, the ransom note named "Restore-My-Files.txt" also appears to be the same as the one used by Phobos, suggesting a connection between the two groups at the beginning of LockBit's activities.

```
strcpy(mutex_name, "XO1XADpO01");
if ( OpenMutexA(0x1F0001u, 0, mutex_name)
  || (CreateMutexA(0, 0, mutex_name),
      SetUnhandledExceptionFilter(TopLevelExceptionFilter),
      SetErrorMode(2u),
      SetPriorityClass((HANDLE)0xFFFFFFFF, 0x100u),
      !EncryptFunction()) )
{
  ExitProcess(0xFFFFFFFF);
}
```

[ABCD Mutex creation process]

- **LockBit 1.0~1.3**

  Starting with LockBit version 1.0, a GUID was used to create mutexes, and the function to create and print ransom notes in the hta format was added. With the implementation of a function to check the victim's system language, the intention not to carry out attacks against CIS countries became clear. This is understandable given the fact that LockBit originated in a Russian forum. In addition, the initial aim was to use packers and protectors (UPX, ASPack, and zprotect)[46] to interfere with analysis and bypass detection, but LockBit felt that this was not a very effective choice and has not made much effort to protect the code since.

[45] Mutex: A technology that prevents multiple threads from accessing the same resource simultaneously in an environment running multiple threads

[46] Packers and protectors: Software that compresses, encrypts, and obfuscates ransomware source code to impede analysis

- **LockBit 2.0 (Red)**

  There are several major differences in LockBit 2.0 from the previous version. An attempt has been made to improve speed by processing encryption in parallel using a multi-threading method. Furthermore, instead of selecting the previously used AES+RSA encryption algorithm combination, it was switched to the AES+Curve-25519/XSalsa20-Poly1305 combination, enabling fast encryption even for large files. In addition, a function was added to determine full encryption or partial encryption depending on the file size, and partial encryption is performed for files larger than 1 MB. So it appears that a lot of effort has been put into the encryption work.

```
if ( _RegCreateKeyExW(0x80000001, v45, 0, 0, 0, 0xF003F, 0, &hKey, &v48) )
{
  libsodium_init(user_public_key, &user_private_key);
  curve25519_xsalsa20poly1305(user_public_key, aes_key, 0x40ui64, &lockbit_public_key);
  cleare_user_private_key(&user_private_key, 255, 32);
  goto LABEL_67;
}
```

[LockBit 2.0 encryption algorithm]

- **LockBit ESXi**

  The ESXi version of LockBit is technically not very different from version 2.0. One added feature is the ability to determine full encryption or partial encryption based on execution arguments. In addition, it encrypts not only ESXi files but also all managed VMs, and all of these actions are recorded in /tmp/locker.log.

```
randombytes_buf(v59, 32LL);
if ( curve25519_xsalsa20poly1305(v39, v59, 32LL, publickey, v20) )
  goto LABEL_19;
all_bytes_readed += a4;
if ( iMinfilesize > a4 )
  goto LABEL_19;
v23 = v49;
if ( v49 > a4 )
{
  N_bytes = encrypt_small_file(a1, a3, a4, a5);
  goto LABEL_33;
}
if ( !wholefile_flag )
{
  if ( beginfile_flag )
  {
    N_bytes = encrypt_file_first_N_bytes(a1, a3, a4);
  }
  else
  {
    spots = create_spots(a4, v53, v49);
    N_bytes = encrypt_file_by_spots(a1, a3, a4, spots, v53[0], a5, v23, v9, a8);
  }
```

[LockBit ESXi encryption method]

- **LockBit 3.0(Black)**

  LockBit 3.0 uses the Salsa20+RSA combination encryption algorithm, which is divided into full encryption and partial encryption methods depending on the file size. This version was developed through LockBit's accumulated know-how, and for a while it was known as the ransomware with the fastest encryption speed in the world. Detailed functions can be adjusted using configuration in the json[47] format, and some samples are characterized by the fact that they can be executed only when a 32-byte key is entered along with the -pass argument. There is a function to disable and modify the event log to interfere with post-accident analysis, and the results of checking the builder of the leaked version 3.0 show 30 functional policies, indicating that it was created with considerable effort on the part of the LockBit group.

```
commandline = get_commandline();
key_flag = get_key(commandline, key);          // get -p <key> / --pass <key>
if ( key_flag )
{
  decode_1(v11, key);
  v10 = decode_2(v11, v12, v9);
  ImageBaseAddress = NtCurrentPEB()->ImageBaseAddress;
  v4 = ImageBaseAddress + ImageBaseAddress[15];
  v5 = *(v4 + 3);
  text_section = v4 + 0xF8;
```

[LockBit 3.0 –pass argument passing process]

- **LockBit Green**

  As LockBit Green borrowed the leaked source code of Conti, it operates according to the encryption algorithm of the ChaCha20[48] + RSA combination. It still performs partial encryption according to the file size, but is meticulous enough to encrypt only 20% of VM files, and especially to encrypt DB files with important contents in their entirety.

[47] json: A lightweight data exchange format used to store or transmit data, with a text-based structure that is easy to read and parse

[48] ChaCha20: A high-performance stream encryption algorithm that has a relatively simple structure, high security and fast processing speed. In ransomware, it is mainly used to encrypt files.

- **LockBit MacOS**

The MacOS version of LockBit looks like a mixture of LockBit 2.0 and LockBit version ESXi. The encryption method is the same as version 2.0, and the argument passing and policies are the same as version ESXi. The encryption exception extension includes extensions that are completely unrelated to MacOS, such as ".exe" and ".dll." Even if it is executed, a crash occurs due to BOF (buffer over flow), suggesting it is an incomplete test code.

```
fprintf(
  stderr,
  "%s\n",
  "Usage: %s [OPTION]... -i '/path/to/crypt'\n"
  "Recursively crypts files in a path or by extention.\n"
  "\n"
  "Mandatory arguments to long options are mandatory for short options too.\n"
  "   -i, --indir        path to crypt\n"
  "   -m, --minfile      minimal size of a crypted file, no less than 4096\n"
  "   -r, --remove       self remove this file after work\n"
  "   -l, --log          prints the log to the console\n"
  "   -n, --nolog        do not print the log to the file /tmp/locker.log\n"
  "   -d, --daemonize    runs a program as Unix daemon\n"
  "   -w, --wholefile    encrypts whole file\n"
  "   -b, --beginfile    encrypts first N bytes\n"
  "   -e, --extentions   encrypts files by extentions\n"
  "   -o, --nostop       prevent to stop working VM\n"
  "   -p, --wipe         wipe free space\n"
  "   -s, --spot         upper bound limitation value of spot in Mb\n"
  "\n");
```

```
Usage: %s [OPTION]... -i '/path/to/crypt'
Recursively crypts files in a path or by extention.
Mandatory arguments to long options are mandatory for short options too.
  -i, --indir         path to crypt
  -m, --minfile       minimal size of a crypted file, no less than 4096
  -r, --remove        self remove this file after work
  -l, --log           prints the log to the console
  -n, --nolog         do not print the log to the file /tmp/locker.log
  -d, --daemonize     runs a program as Unix daemon
  -w, --wholefile     encrypts whole file
  -b, --beginfile     encrypts first N bytes
  -e, --extentions    encrypts files by extentions
  -o, --nostop        prevent to stop working VM
  -t, --wipe          wipe free space
  -s, --spot          upper bound limitation value of spot in Mb
  -p, --pass          password
  -f, --full          full log
  -a, --delay         start delay in minutes
  -y, --noexts        do not search for extentions
  -v, --vmdk          search for extentions inside VMDK files
```

[Performed functions by argument (left: LockBit ESXi, right: LockBit MacOS)]

- **LockBit NG-Dev(Next Generation-Development)**

In NG-Dev, LockBit reverted to using the AES+RSA combination and packers for encryption as before version 2.0. One unique thing is that among existing ransomwares, partial encryption according to the file size has been the established method, but NG-Dev provides three encryption modes depending on the file extension. This method can be entered in the configuration, and various functions can be customized, such as determining whether to execute by checking the execution date, self-deleting, and changing the filename. NG-Dev, which has the feel of a customized ransomware, has reduced features compared to version 3.0, but we cannot rule out the possibility that functions will be added in the future.

✓ **Changes in ransom notes**

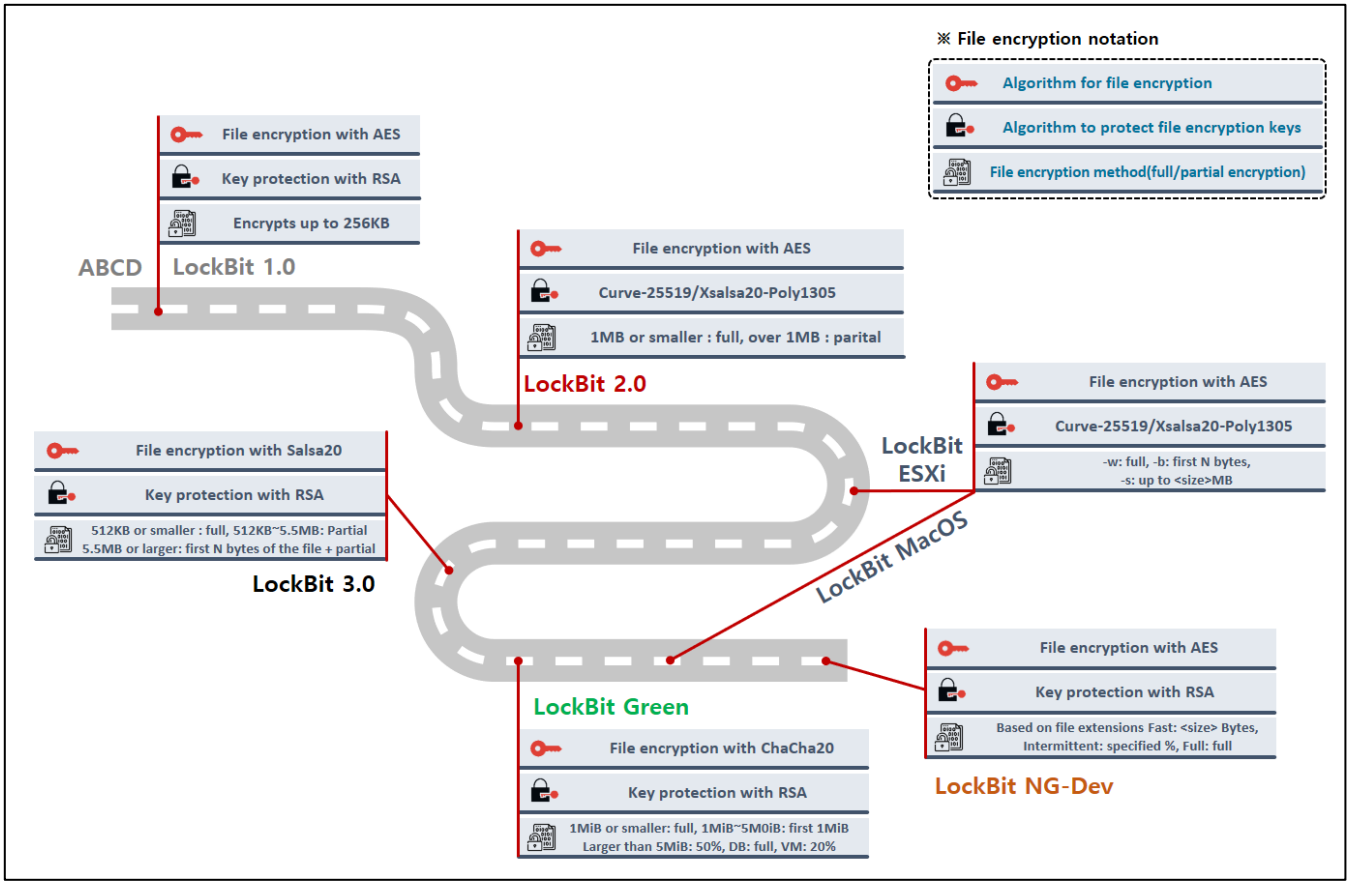
The ransom notes of the LockBit ABCD and 1.0 versions are almost the same, but as ABCD guides you to a dark web negotiation site, and version 1.0 provides not only a dark web but also a clear web negotiation site, the ransom note has been reconfigured in such a way as to induce more victims to pay ransom by increasing accessibility.

LockBit version 2.0 puts the burden of data leakage on the victim by listing the addresses of both the dark web leak site and the negotiation site, and uses the victim's unique decryption ID in the ransom note as a means of distinguishing the victim during negotiations.

The 3.0 and Green versions use the same ransom note, and they list multiple domains in case a specific domain becomes unusable due to a DDoS attack. Likewise, they list multiple clear website domains to improve accessibility.

[Changes in LockBit ransom notes]

✓ **file encryption**



[File encryption methods by LockBit version]

The encryption method used by the LockBit ransomware has changed significantly since version 2.0. To improve speed, instead of choosing RSA in version 2.0, LockBit implemented a fast but difficult to decrypt encryption process through Xsalsa20, which can quickly encrypt large amounts of data after exchanging keys using the Curve-25519 algorithm, and Poly1305, which guarantees the integrity of encryption. Then, they used the same encryption algorithm again in the ESXi and MacOS versions. In LockBit 3.0 and version NG-Dev, they used the Salsa20/AES + RSA encryption algorithm again, but further refined the logic for encrypting files to improve speed.

```
if ( aes_complete_flag
  || (block_size = Size,
      chunk_size_1[0] = *&chunk2[13136].InternalHigh,
      chunk_size_1[1] = *&chunk2[13137].Internal,
      memcpy(&v66, &unk_4169C8, Size),
      Offset = chunk2 + v79,
      RSA_Encyption(&RSA_PublicKey, aes_key, aes_block, 0, block_size + 32, chunk_size_1, &chunk2[29] + v79)) )
```

```
if ( _RegCreateKeyExW(0x80000001, v45, 0, 0, 0, 0xF003F, 0, &hKey, &v48) )
{
  libsodium_init(user_public_key, &user_private_key);
  curve25519_xsalsa20poly1305(user_public_key, aes_key, 0x40ui64, &lockbit_public_key);
  cleare_user_private_key(&user_private_key, 255, 32);
  goto LABEL_67;
}
```

[Change in key protection algorithms (top: LockBit ABCD~1.3, bottomr: LockBit 2.0)]

LockBit's 2.0 and MacOS versions use the AES algorithm for file encryption and the Curve-25519 and Xsalsa20-Poly1305 algorithms to protect the key. The algorithm used for encryption is the same, but one difference is that in the MacOS version, the encryption method varies depending on the passed arguments, and in version 2.0, it varies depending on the size of the file.

In addition, as with the ESXi version, the MacOS version determines full encryption or partial encryption depending on the execution arguments. The "-w" argument encrypts the entire file, the "-b" argument encrypts only the first N bytes, and the "-s" argument encrypts only the size that is passed together.

```
if ( _RegCreateKeyExW(0x80000001, v45, 0, 0, 0, 0xF003F, 0, &hKey, &v48) )
{
  libsodium_init(user_public_key, &user_private_key);
  curve25519_xsalsa20poly1305(user_public_key, aes_key, 0x40ui64, &lockbit_public_key);
  cleare_user_private_key(&user_private_key, 255, 32);
  goto LABEL_67;
}
switch ( *chunk_count )
{
  case 1:                                   // encrypt whole file
    v30 = v86 + 1;
    if ( cpu_flag )
    {
      AES_NI_init(v101, v30);
      AES_NI_enc(v15[11], v31, (v15 + 3), v15[10], v15[10]);
      cleare_user_private_key(v32, 0xFF, 4);
    }
    else
    {
      custom_AES_init(v100, v30);
      custom_AES_enc(v15 + 3, v15[10], v15[10]);
      cleare_user_private_key(v100, 0xFF, 280);
    }
```

```
if ( curve25519_xsalsa20_poly1305(v42, v58, 32LL, publickey, v13) || iMinfilesize > a3 )
  goto LABEL_38;
v37 = v35;
mbedtls_aes_init_encrypt(v41, v58);
v57 = v59;
v36 = a7;
if ( a6 )
  v16 = *a6;
else
  v16 = 0LL;
v17 = a3 + 15;
if ( a3 >= 0 )
  v17 = a3;
v39 = v17 & 0xFFFFFFFFFFFFFFF0LL;
*&v56[7] = v17 & 0xFFFFFFFFFFFFFFF0LL;
v40 = time(0LL);
v18 = gmtime(&v40);
strftime(v44, 0x14uLL, &time_fmt, v18);
v19 = pthread_self();
v20 = rand();
v35[0] = v44;
v35[1] = v19;
v35[2] = a1;
v35[3] = v20 + v20 / -v38 * v38 + v38;
PrintLog2(&start_enc_offset);
v21 = mmap_alloc(a1, a2, a5, &v39, v16);
if ( v21 == -1 )
  goto LABEL_18;
v22 = v21;
v23 = v39;
mbedtls_aes_encrypt_cbc(v41, v39, &v57, v22, v22);
```

[Encryption key protection and file encryption process (left: LockBit 2.0, right: LockBit MacOS)]

In LockBit 3.0, a symmetric key is generated through a random number generation command supported by the victim's CPU, and this is protected through encryption with the RSA algorithm and then validated with a checksum.[49]

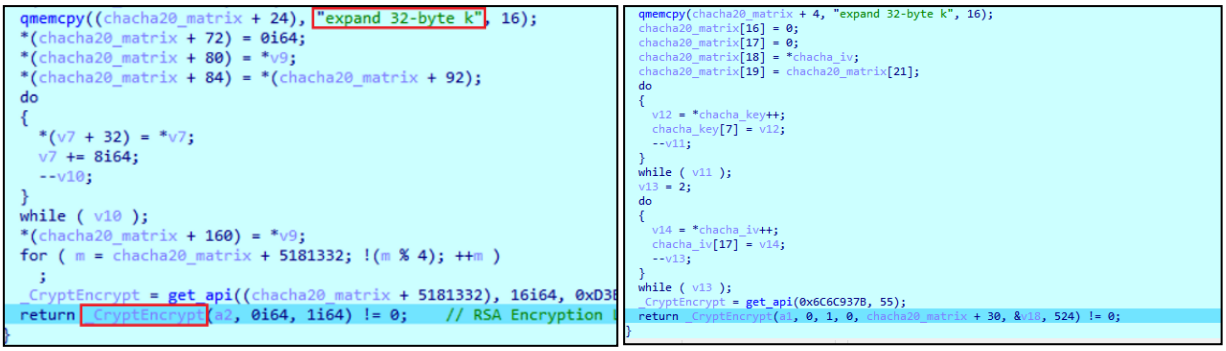
```
__asm { cpuid }
if ( (_ECX & 0x40000000) != 0 )
{
  __asm
  {
    rdrand  eax
    rdrand  edx
  }
}
```

```
CreateKey(&symmetric_key, &unk_424F70);
RtlEncryptMemory(&symmetric_key, 0x80u, 0);
j_qmemcpy(key, &symmetric_key, 0x80u);
RtlDecryptMemory(key, 0x80u, 0);
RSA_crypt(key, &unk_424F70);
checksum = Checksum(key, 128);
```

[LockBit 3.0 key generation and protection process (left: symmetric key generation, right: symmetric key protection)]

[49] Checksum: A value used to verify that the encryption key was created without errors

LockBit Green was created using the ChaCha20 and RSA encryption algorithms. Since the Conti source code is used as is and only some settings were changed, you can see that the codes are largely the same.



[LockBit Green encryption process (left: LockBit Green, right: Conti)]

Major versions of LockBit commonly use an asynchronous encryption method,[50] using the I/O completion port to improve file speed. This guarantees the best performance among the asynchronous I/O processing methods provided by Windows, and can reduce context switching[51] costs compared to existing asynchronous processing methods such as threads and reduce CPU utilization[52] through efficient use of threads. Using this method, LockBit provides relatively fast encryption.

```
NumberOfConcurrentThreads = 2 * SystemInfo.dwNumberOfProcessors;
ExistingCompletionPort = CreateIoCompletionPort(0xFFFFFFFF, 0, 0, 2 * SystemInfo.dwNumberOfProcessors);
v35 = 0;
if ( SystemInfo.dwNumberOfProcessors )
{
  CreateThread = ::CreateThread;
  do
  {
    t_handle1 = CreateThread(0, 0, Encryption_Func, 0, 0, &ThreadId);
    t_handle2 = CreateThread(0, 0, Encryption_Func, 0, 0, &ThreadId);
    v29 = 1 << v35;
    v30 = t_handle2;
    SetThreadAffinityMask(t_handle1, 1 << v35);
    SetThreadAffinityMask(v30, v29);
    CreateThread = ::CreateThread;
    ++v35;
  }
  while ( v35 < SystemInfo.dwNumberOfProcessors );
}
```

```
::NumberOfProcessors = NumberOfProcessors;
_NtCreateIoCompletion = resolve_NtCreateIoCompletion();
if ( _NtCreateIoCompletion(&dword_4E2520, 0x1F0003, 0, v41) >= 0 )
{
  ExistingCompletionPort = sub_4BABA0((4 * ::NumberOfProcessors));
  if ( ExistingCompletionPort )
  {
    v37 = 0;
    if ( !::NumberOfProcessors )
      return 1;
    while ( 1 )
    {
      *(ExistingCompletionPort + 4 * v37) = create_thread(Encryption_Function, 0);
      v38 = *(ExistingCompletionPort + 4 * v37);
      if ( v38 == -1 )
        break;
      v47 = 1 << v37;
      _NtSetInformationThread = resolve_NtSetInformationThread(v38, 4, &v47, 4);
      _NtSetInformationThread();
      if ( ++v37 >= ::NumberOfProcessors )
        return 1;
    }
  }
  NtClose_0(j);
```

```
CpuNum = check_cpunum();
if ( (CpuNum & 0x20) != 0 )
  CpuNum = 32;
v1 = 2 * CpuNum + 1;
v5 = 0;
ExistingCompletionPort = CreateIoCompletionPort(-1, 0, 0, v1);
if ( ExistingCompletionPort )
{
  do
  {
    Thread = CreateThread(0, 0, EncryptFunction, 0, 0, 0);
    v3 = Thread;
    if ( Thread )
    {
      HideThreadFromDebugger(Thread);
      NtClose(v3);
      ++v5;
    }
    --v1;
  }
  while ( v1 );
}
RtlInitializeCriticalSection(&unk_D15888);
```

[Use of the I/O Completion port (top: LockBit 1.0, bottom left: LockBit 2.0, bottom right: LockBit 3.0)]

[50] Asynchronous encryption method: Fast operation is possible as the encryption method is processed in parallel with multi-threads

[51] Context switching: The process of switching CPU control by saving the state of the currently running thread and loading another thread

[52] CPU utilization: The percentage of time the CPU spends performing a specific task. One of the indicators for evaluating the performance efficiency of a system

✓ **Threat of intrusion by exploiting vulnerabilities**

[Vulnerabilities exploited by LockBit]

LockBit prefers initial access by exploiting vulnerabilities during attacks. In Korea, malware spreads through phishing e-mails in most cases, but LockBit's strategy is to perform large-scale attacks by exploiting vulnerabilities in solutions commonly used by organizations such as companies.

LockBit has been carrying out ransomware attacks through various vulnerabilities since the initial version of its ransomware. Many Windows-related vulnerabilities, such as Log4Shell, PaperCut, GoAnywhere MFT, Cisco ASA/FTD, and Citrix Bleed, have been used in attacks, and it was confirmed that LockBit recently exploited the ScreenConnect vulnerability CVE-2024-1709 in many cases.

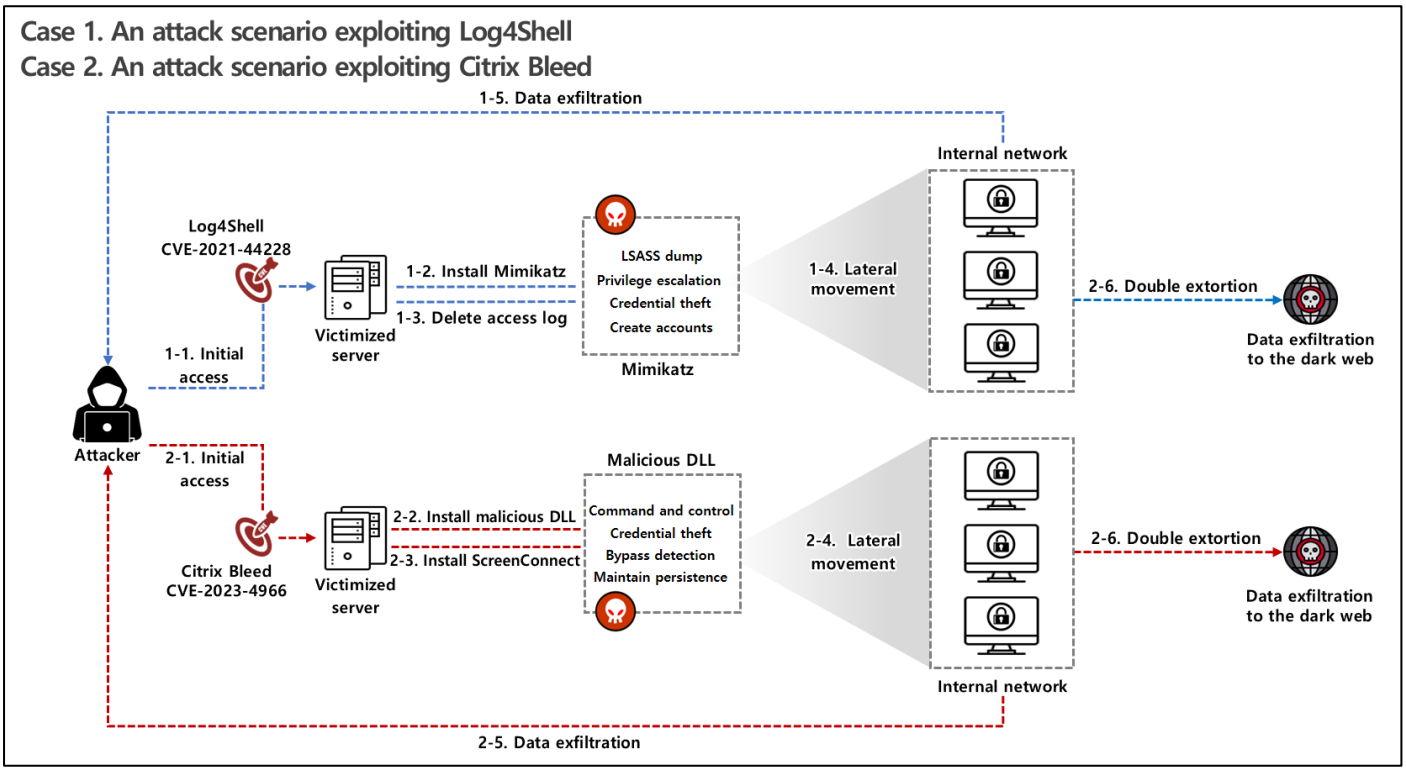
Until last year, the initial access method that was found most often was characterized by use of old vulnerabilities to perform large-scale attacks targeting unpatched servers. As various cases such as PoC (Proof of Concept)[53] have been disclosed, old vulnerabilities consume less resources than a zero-day vulnerability [54] or a one-day vulnerability,[55] but they may be limited depending on the environment and whether patches are applied. Reflecting these limitations, a number of attacks using one-day vulnerabilities have been confirmed in recent years, and not only the LockBit ransomware, but also various groups such as the BlackBasta, Bloody, and Play ransomware groups are exploiting one-day vulnerabilities to carry out attacks. This is currently being confirmed. The reason for exploiting zero-day and one-day vulnerabilities is that they cannot be patched or there is a high probability that patches have not been applied. So it appears to be one strategies for carrying out attacks targeting more people.

[53] PoC: A code that demonstrates that a vulnerability can actually be exploited

[54] Zero-day vulnerability: A security vulnerability for which there is no patch because it is not publicly known. Such vulnerabilities are high-risk because they have the potential to be exploited as soon as they are discovered.

[55] One-day vulnerability: A vulnerability that has already been disclosed and for which a patch has been provided, but as the patch may not yet have been applied in many systems, there is room for an attacker to exploit it.

✓ **Scenario of a LockBit attack**



[Scenario of a LockBit attack exploiting vulnerabilities]

Case 1 is the case of a ransomware attack exploiting Log4Shell that caused great confusion around the world. Log4Shell is a vulnerability that allows remote code execution targeting Log4j, a widely used Java-based logging utility. LockBit accesses the victimized server through Log4Shell and installs Mimikatz[56] within the system to escalate privileges by stealing credentials. Afterwards, it deletes the log containing traces of penetration, moves to the internal network through PsExec and an RDP (remote desktop protocol),[57] and uses FileZilla[58] to leak files existing in the system. After all processes are completed, ransomware is distributed to the system to encrypt it and the stolen data and encrypted files are held hostage for double extortion.

[56] Mimikatz: A tool that collects sensitive information such as credentials from a Windows system

[57] RDP: A protocol that allows you to remotely control another computer

[58] FileZilla: File transfer software

Case 2 is the case of an attack exploiting Citrix Bleed. Citrix Bleed can be exploited in NetScaler ADC and NetScaler Gateway [59] environments. It is an information exposure vulnerability that unintentionally discloses sensitive information. LockBit, which successfully penetrates the victimized server through this vulnerability, then installs a malicious DLL that performs C2 communication[60] in the system and continuously executes commands for stealing credentials, etc., on the victimized system. As it also includes a detection bypass function, it moves to the internal network through ScreenConnect, which is installed together with the malicious DLL while remaining undetected by security solutions, leaks important files to the outside, and performs double extortion by encrypting the system.

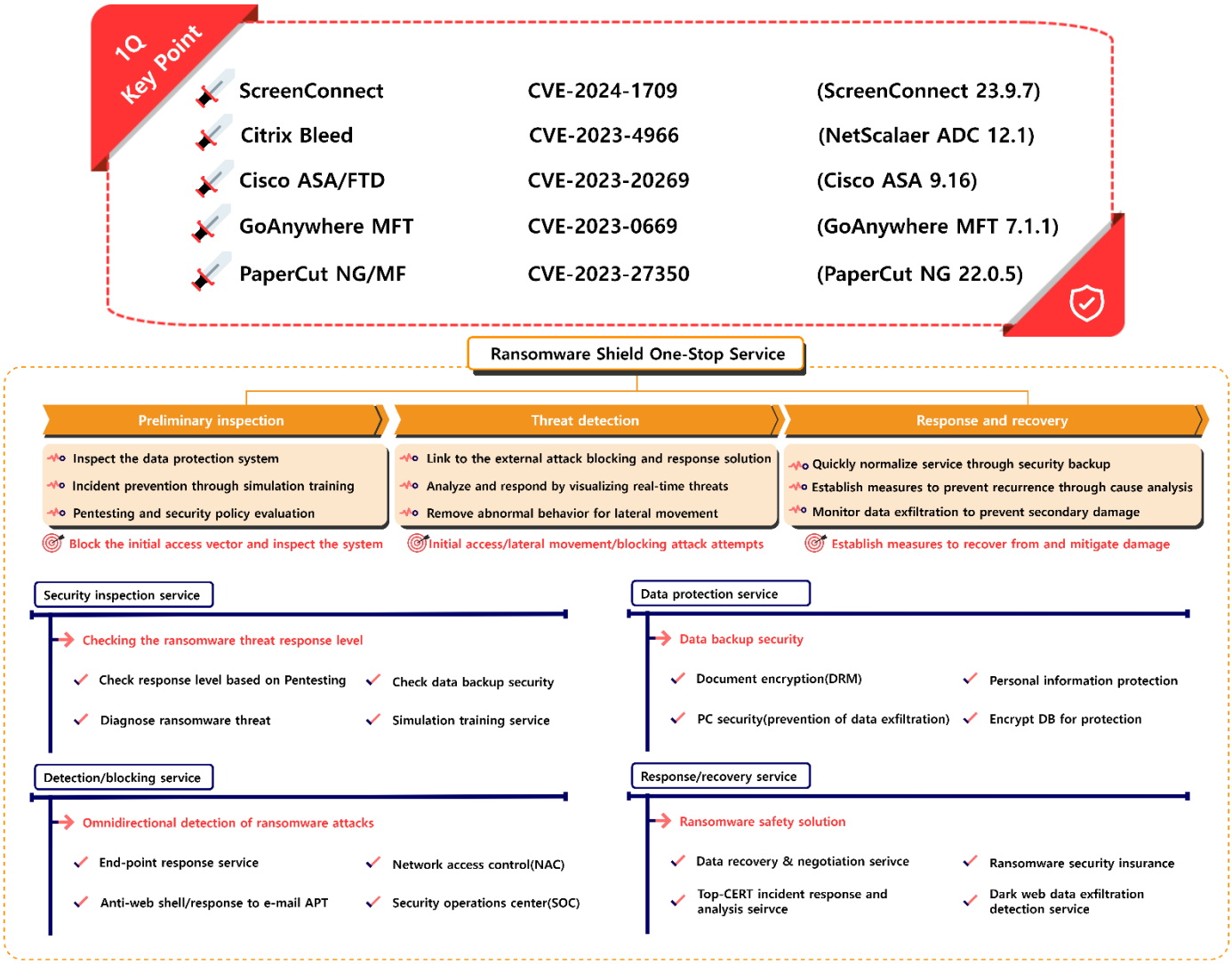
[59] NetScaler ADC and NetScaler Gateway: Network equipment and software solutions provided by Citrix Systems

[60] C2 communication: A communication method that transmits commands and collects data between a host infected with malware and the attacker server

■ Ransomware mitigations

1. How to Respond to a LockBit Ransomware Attack

Systems are mainly infected by the LockBit ransomware through phishing e-mails or initial access exploiting vulnerabilities. In particular, large-scale attacks are attempted by exploiting vulnerabilities in software solutions used by companies and other organizations, and recently there has been a move to attack supply chains. To prevent such damage, it is of utmost importance to apply the latest version of software with vulnerabilities patched, as well as to perform preliminary checks such as malicious e-mail training, mock hacking, and security system inspections, and it is necessary to respond to threats in real time through threat detection. It is recommended that you consider services such as ransomware safety insurance services and monitoring of data leaked on the dark web, which can reduce damage that may occur in the future.



[LockBit ransomware mitigations]

■ Appendix

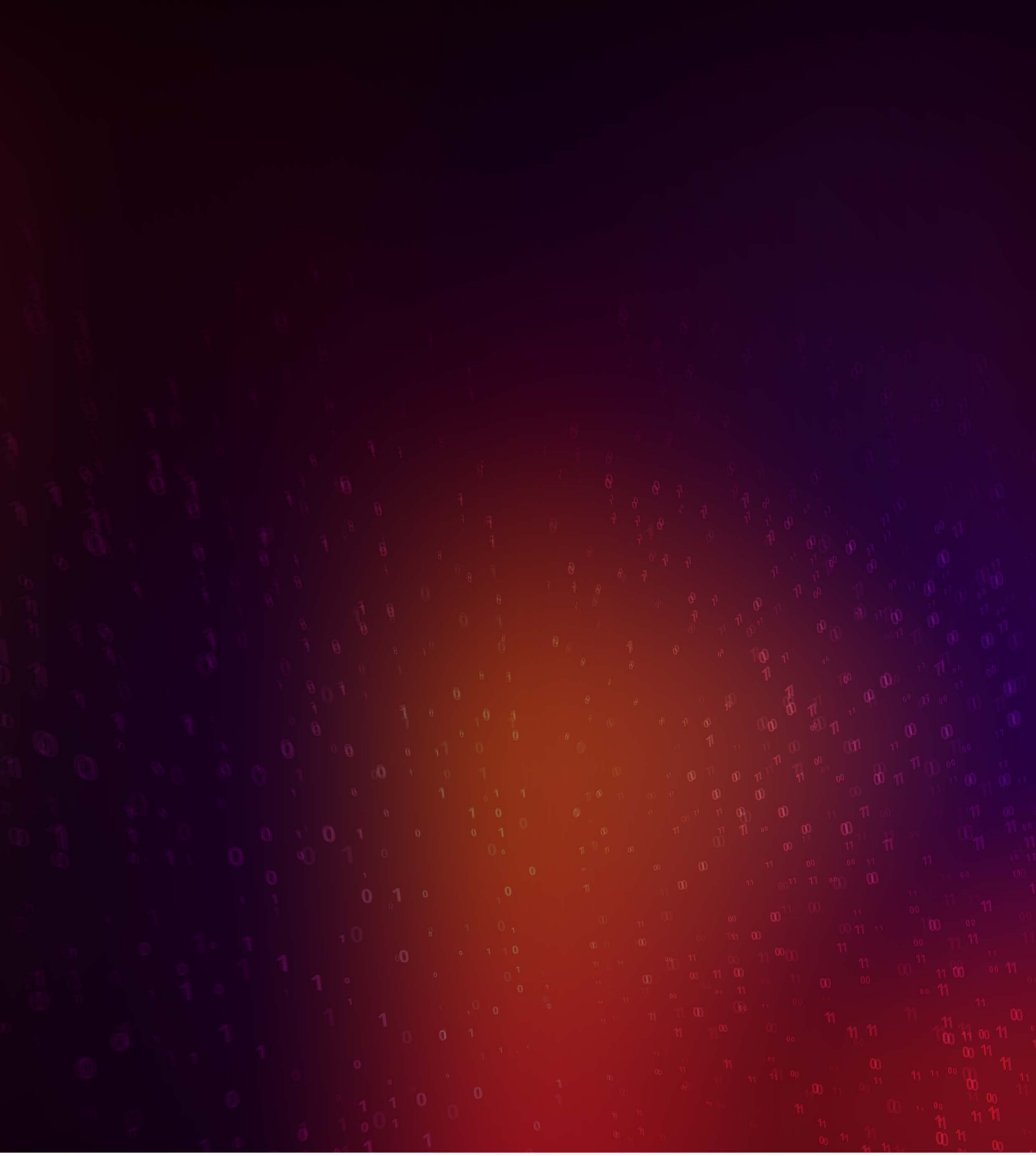
1. Software Vulnerabilities Exploited by LockBit

CVE	Description	Affected version	Patch version
CVE-2018-13379	A file path search vulnerability that allows downloading of system files when SSL VPN[61] is used in Fortinet's security OS, FortiOS	5.4.6 ~ 5.4.12 5.6.3 ~ 5.6.7 6.0.0 ~ 6.0.4	5.6.8 or higher 6.0.5 or higher
CVE-2020-0796	A remote code execution vulnerability that occurs in SMB 3.1.1, a resource sharing protocol used by Windows	Windows 10 & Server 2016 (build 1903, 1909)	KB4551762 update
CVE-2021-44228	A remote code execution vulnerability discovered in Log4j, a JAVA-based open source logging library	2.0-beta9 ~ 2.15.0 (excluding 2.12.2, 2.12.3, and 2.3.1)	2.12.2, 2.12.3, 2.3.1, 2.16.0 or higher
CVE-2021-22986	A remote code execution vulnerability occurring in BIG-IP and BIG-IQ, F5's application distribution network equipment	16.0.*, 15.1.*, 14.1.*, 13.1.*, 12.1.* before the patch version	16.0.1.1 or higher 15.1.2.1 or higher 14.1.4 or higher 13.1.3.6 or higher 12.1.5.3 or higher
CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065	A remote code execution vulnerability occurring on Exchange Server, Microsoft's e-mail server	Exchange Server 2013, 2016, and 2019	KB5000871 update
CVE-2021-36942	A vulnerability in Windows Server that could allow an unauthenticated attacker to be authenticated for another server through the domain controller	2008 r2 sp1, 2016, 2008 sp2, 2012, 2012 r2, 2020 h2, 2004, and 2019	KB5005076 or KB5005106 update
CVE-2022-3653	A heap buffer overflow vulnerability in the Vulkan graphics engine of the Chrome browser	Lower than 107.0.5304.62	107.0.5304.62 or higher
CVE-2022-36537	A vulnerability that occurs in the Zk Framework, an open source JAVA framework, which allows access to sensitive information by manipulating POST requests	9.6.1, 9.6.0.1, 9.0.1.2, 8.6.4.1	9.6.2 or higher
CVE-2023-0669	A vulnerability that allows remote code execution in GoAnywhere MFT, Forta's security management file transfer software	7.1.1 or lower	7.1.2 or higher

[61] VPN (Virtual Private Network): A virtual network used to protect personal information and bypass geo-restrictions

CVE-2023-20269	A vulnerability that can obtain credentials due to a remote access VPN vulnerability of the integrated security platform Cisco ASA and next-generation threat defense platform Cisco FTD software	9.19.1.18 or lower	9.20 or higher
CVE-2023-27350 CVE-2023-27351	A vulnerability that allows remote code execution after accessing the server as an administrator by bypassing user credentials in the print management software PaperCut	15.0.0 ~ 20.1.7, 21.0.0 ~ 21.2.11, 22.0.0 ~ 22.0.9	20.1.7 or higher 21.2.11 or higher 22.0.9 or higher
CVE-2023-4966	An information leak vulnerability occurring in networking products NetScaler ADC and NetScaler Gateway	14.1*, 13.1*, and 13.0* before the patch version	14.1-8.50 or higher 13.1-49.15 or higher 13.0-92.19 or higher
CVE-2024-1709	A remote desktop solution ScreenConnect vulnerability, which is an authentication bypass vulnerability that can create a system administrator account on a remote desktop	23.9.7 or lower	23.9.8 or higher

[Software vulnerabilities exploited by LockBit]



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