Keep up with Ransomware

The appearance of a decryption tool that exploits BlackBasta's loopholes

■ Overview

In January 2024, the number of damage cases caused by ransomware attacks decreased by about 30% to 299 compared to the previous month (420). With the cooperation of international investigative agencies, ransomware attackers were arrested one after another, and as this news spread quickly, the activities of ransomware groups slowed down. In addition, it is believed that there was decrease because there were no additional attack activities by new ransomware groups discovered last December.

However, many ransomware attacks using various means and methods occurred. In particular, a case where a commercial RMM (Remote Monitoring and Management)[1] tool was exploited for a ransomware attack attracted popular attention. The Cactus ransomware group used RMM solutions such as AnyDesk, Splashtop, and SuperOps[2] to attack the global energy company Schneider Electric's corporate network.

Also, a variant of the LockBit ransomware was found to be spreading through remote control software TeamViewer[3]. It carried out the attack by logging into TeamViewer using a leaked account, then accessing PCs within the network and spreading ransomware. The ransomware used in the attack has the same source codes as the existing LockBit ransomware, but the ransom note had differences. So it is thought to be a ransomware created with the leaked LockBit builder.

[1] RMM: Remote monitoring and management tool

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

[3] TeamViewer: Software that allows users to remotely access and control other computers via the Internet

Ransomware groups such as Akira, BlackByte, AvosLocker, RobbinHood, and Kasseika are conducting attacks using BYOVD (Bring-Your-Own-Vulnerable-Driver)[4]. In particular, it was confirmed that the Kasseika ransomware group used BYOVD to prevent ransomware from being detected by security solutions.

Since 2022, the LockBit ransomware has been distributed in Korea through phishing emails disguised as resumes and copyright infringement. As the phishing emails have an NSIS (Nullsoft Scriptable Install System)[5] exe file disguised as a document file attached, when the file is executed, it is exposed to encryption and data leakage attacks. In the past, phishing emails were suspected because they used awkward Korean, but recently, with the development of generative AI, they are evolving into a more natural and plausible form. Therefore, you should not open emails from unknown sources, and be careful not to execute attachments to MS Office document files (.XLSM, .DOCM) containing macros or files that can be executed (.EXE, .SCR, .BAT).

Meanwhile, a new ransomware group NoName is suspected of being related to LockBit. The format of the NoName ransomware group's dark web leak site is similar to LockBit's leak site, and the same cases are posted as victims. Also, the contents of the ransom note are quite similar, raising the possibility that the NoName group is an organization related to LockBit. However, it remains to be seen as it may be an intention to use LockBit's popularity to increase the influence of the NoName group.

While various types of ransomware threats continue, a decryption tool for variant BlackBasta ransomware and Babuk-based Tortilla ransomware has been released. If infected by the variant BlackBasta ransomware in April 2023, recovery is possible if the file size is 5 KB to 1 GB. Because the Tortilla ransomware encrypts all victims using the same private key, anyone who sustained damage caused by Tortilla can recover using the decryption tool.

[4] BYOVD: An attack technique in which an attacker bypasses system security by using an already existing vulnerable driver

[5] NSIS: Script-based installation system for Windows

■ Ransomware news

infosec

SRLabs release tool to decrypt part of BlackBasta ransomware

- Decryption tool released for variant ransomware used around April 23
- Recover files 5KB~1GB; > 1GB, except first 5KB; others not recoverable
- Decryption possible only if the plaintext of the 64-byte encrypted data is known

Babuk variant Tortilla ransomware decryption tool released

- Cisco Talos releases decryption tool for Tortilla ransomware, a variant of Babuk ransomware
- Threat intelligence shared with Dutch law enforcement leads to attackers being apprehended
- The Tortilla campaign exploits the ProxyShell vulnerability in Microsoft Exchange servers

LockBit claims attack on global sandwich chain Subway

- LockBit claims to have stolen Subway's data, threatening to sell it to competitors if negotiation fail
- Subway issued a private statement to the media saying it was investigating the matter

Medusa ransomware group attacks Water for People non-profit organization

- The Medusa ransomware group posted on a dark web leak site that it had attacked Water for People
- Currently, negotiations have collapsed and leaked data has been published

3AM ransomware claims links to BlackSuit ransomware group

- Royal(now BlackSuit), formed by former Conti members, shares similar tactics and infrastructure
- Attacks using infrastructure such as the same, IP, proxy, port, etc.
- In addition, traces of IcedID being used for attacks were found

* IcedID : Malware used to deliver other malware

BlackCat(Alphv) ransomware source code sold for around 40 million won on XSS forum

- A user posted a post selling the source code of BlackCat ransomware on the XSS forum
- The account that posted this post has been banned and is presumed to be a scam

* XSS forum : A dark web forum that sells data stolen through hacking and ransomware

Russian TrickBot developer and operator sentenced to 5 year in prison

- US sentences 40-year-old Russian man for TrickBot creation and operation
- TrickBot is used for delivering ransomware

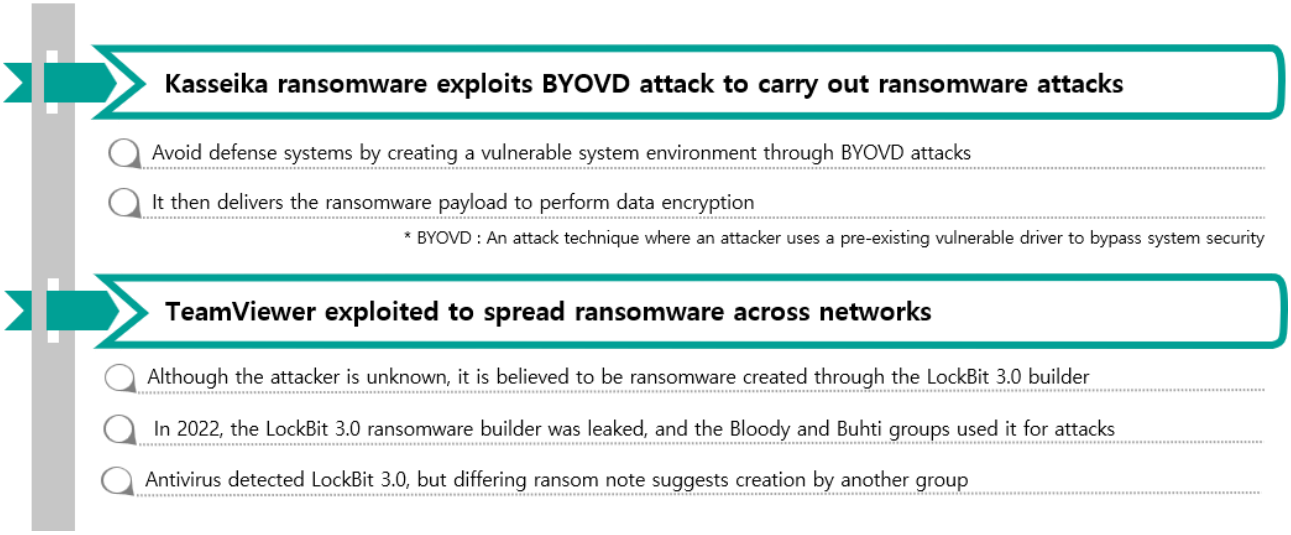


Figure 1. Ransomware trends

■ Ransomware threats

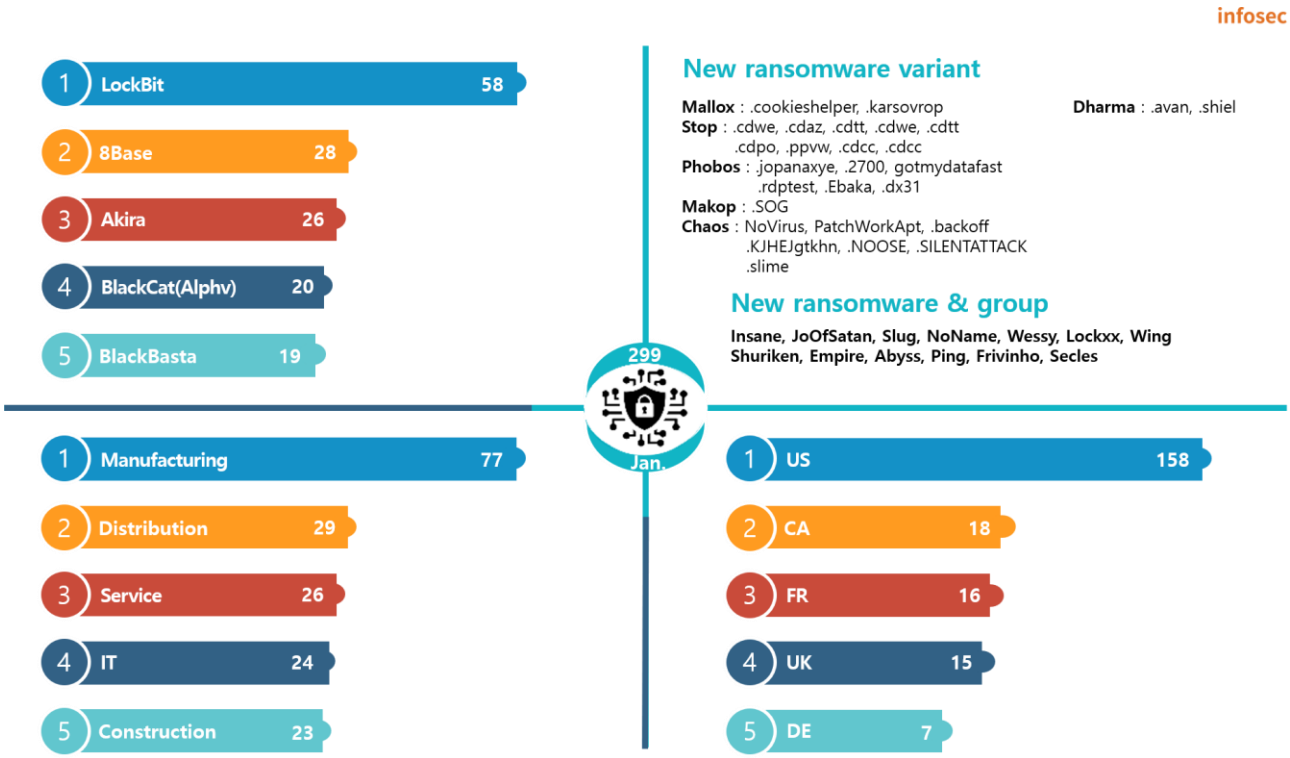


Figure 2. Ransomware threats as of January 2024

New threats

In January 2024, cases of damage caused by ransomware decreased by about 30% compared to December of last year, but the threat of variant ransomware continues: e.g., new ransomware groups are continuously discovered.

The Insane ransomware group disclosed the characteristics of its ransomware on a main dark web leak site. It claimed that it infects all files within the network through AES encryption and steals system information, and also stated that it is never detected by Anti-Virus. However, since this claim has no record of detection due to the nature of new ransomware, it seems possible to avoid only detection by security solutions that detect ransomware based on signatures.

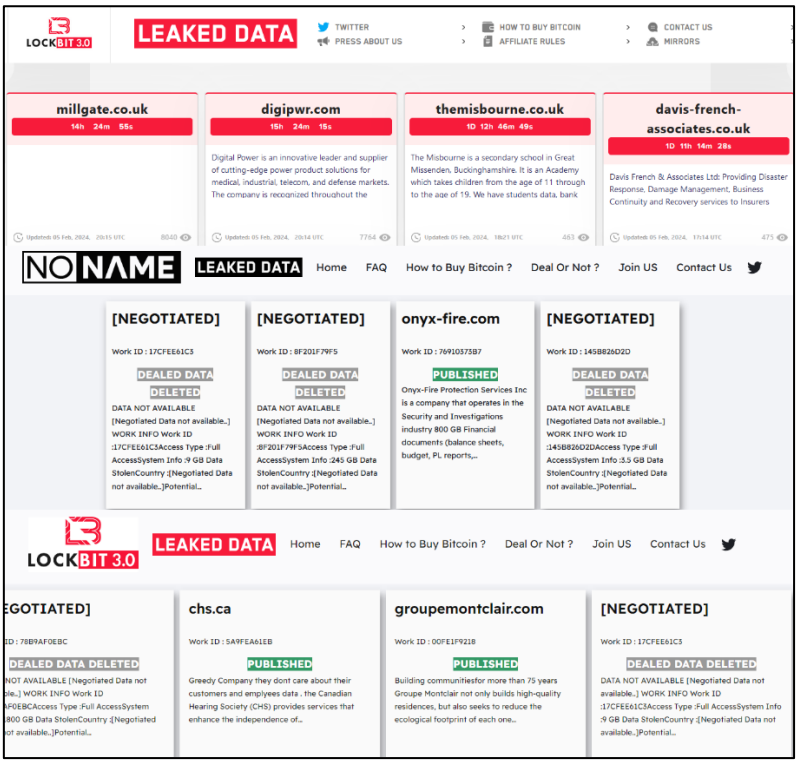


Figure 3. Comparison of the LockBit, NoName, and Fake LockBit leak site

The NoName group is a group that has been thought to be related to the LockBit ransomware group. The attack cases posted on the NoName group's dark web leak site match the attack cases that LockBit posted in 2023, and the format of the dark web leak site is also similar to that of LockBit. Another LockBit imitation group, Fake LockBit, was also discovered. These are fake LockBit groups that are operating under the name of LockBit on the Surface web, which is commonly used by most people, rather than on the dark web where ordinary ransomware groups are operating.

A connection between the NoName ransomware group and the Fake LockBit group was also discovered. The leak sites of the two ransomware groups use the same domain registrar (NameCheap) and were registered on the same date (November 4, 2023). This adds weight to the theory that the mastermind behind NoName and fake LockBit is an affiliate of LockBit, but rather an imitation group using the leaked builder. In other words, weight is being given to the possibility that it is part of a strategy to take advantage of LockBit's popularity. It seems that we will have to watch their actions further in the future to be able to draw a conclusion.

The majority of newly discovered ransomwares is confirmed to be variants of ransomwares whose ransomware builder or codes were leaked in the past. The Wessy ransomware, a variant of Chaos ransomware, is written in .NET and .NET Reactor obfuscation is applied to it. Shuriken, a variant of the LokiLocker ransomware, is registered in the startup program and task scheduler and executed under the disguise of winlogon.exe when a user logs on, disabling the task manager and preventing its execution. This ransomware is set to contact you through a separate Telegram messenger account. The Abyss ransomware, a variant of the Babuk ransomware, provides contact information through the desktop and ransom notes after encryption, but the dark web address currently provided is not accessible.

Top 5 ransomwares

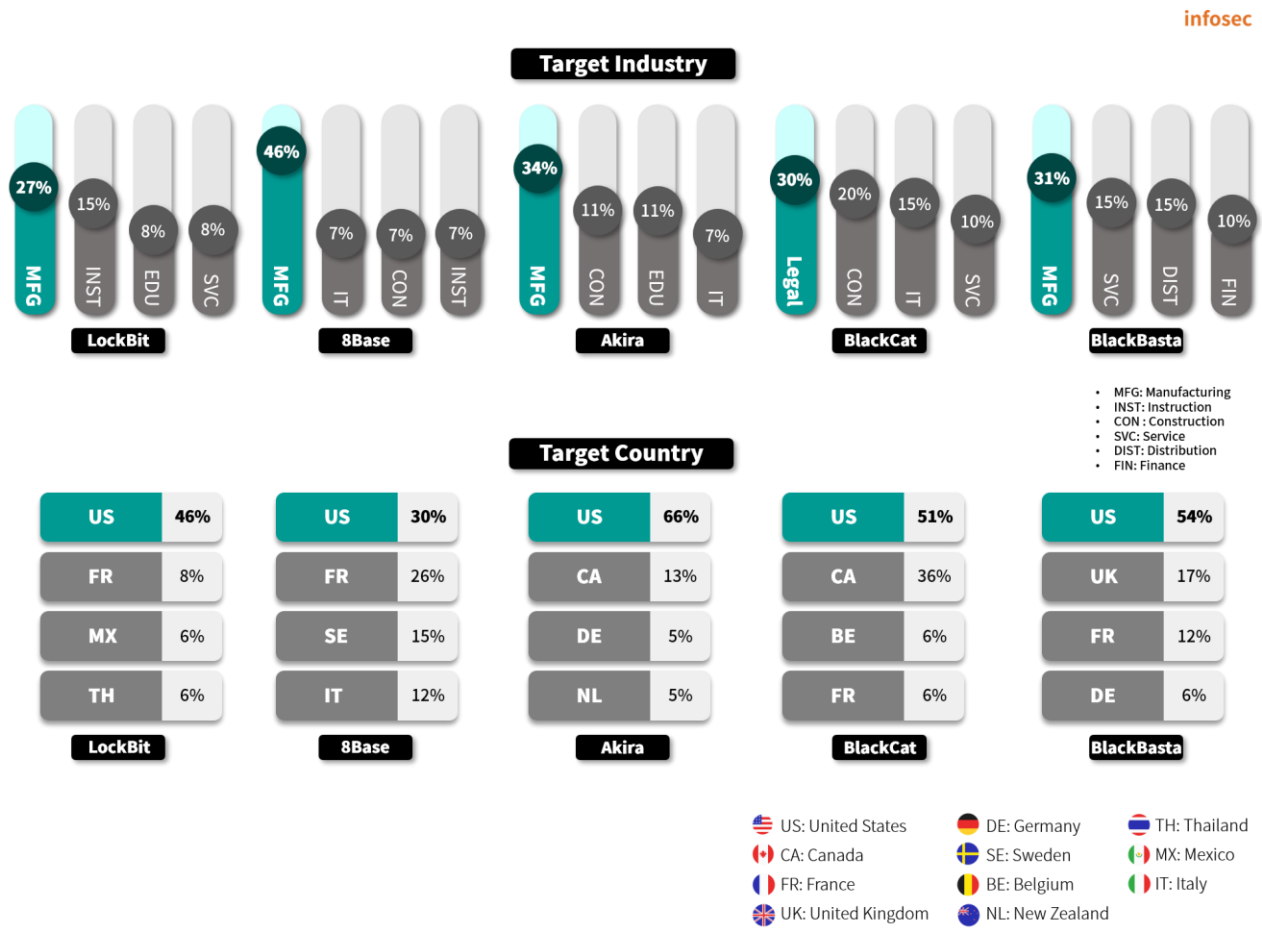


Figure 4. Major ransomware attacks by industry/country

LockBit is active again after overcoming operational issues, e.g., the desertion of affiliates that occurred a few months ago. Recently, it said it attacked global sandwich franchise company Subway. Even in Korea, ransomware in the form of MS Office document files containing malicious macros is still distributed under the disguise of resumes, job applications, etc.

Recently, the LockBit group has been taking bold steps, e.g., not hesitating to launch attacks targeting medical institutions. This is a move that runs counter to the company's policy of posting an apology and providing a free decryption tool after attacking a children's hospital just a year ago.

The reason ransomware groups are reluctant to attack medical institutions is because they are highly likely to become targets of investigative agencies. Nevertheless, LockBit changed its strategy and is attempting to attack medical institutions to increase the probability of ransomware payment. Of course, this does not mean that they are carrying out attacks on medical systems that would endanger the lives of patients. They are carrying out attacks in a sophisticated manner, i.e. stealing patients' sensitive data and forcing medical institutions to pay the ransom.

The Akira ransomware has recently been conducting numerous attacks targeting Finland. It exploits the Cisco VPN[6] vulnerability (CVE-2023-20269[7]) to access the network and deletes and destroys backup data by targeting NAS (Network-Attached Storage)[8] and backup devices. As a result, Finland's National Cyber Security Center (NCSC-FI) warned about Akira ransomware attacks and emphasized following the "3-2-1 backup rule" to minimize damage. The "3-2-1 backup rule" is a rule specifying that you should create at least **three** copies in **two different locations** and keep **one** of the copies completely separated from the network.

A decryption tool for the BlackBasta ransomware was released. This is 'Black Basta Buster', a decryption tool for variant ransomware used in the April 2023 attack, and was created through an encryption flaw in BlackBasta. Files smaller than 5 KB cannot be recovered, but files between 5,000 Bytes and 1 GB can be fully decrypted. If the file size exceeds 1 GB, the first 5 KB is lost and the remainder can be recovered.

The BlackCat group continues its activities using infrastructure other than the sites seized after the confrontation with the FBI last December. Recently, it is deleting traces of existing data from dark web leak sites and posting only new victimized organizations. In January, it attacked a medical care service company in the medical/welfare industry and at one point paralyzed the company's site. Previously, BlackCat had a rule not to carry out attacks on CIS countries and major infrastructure, such as nuclear power plants and hospitals, but after the infrastructure was confiscated by the FBI, it retracted this rule and continues attacks on the medical industry.

---

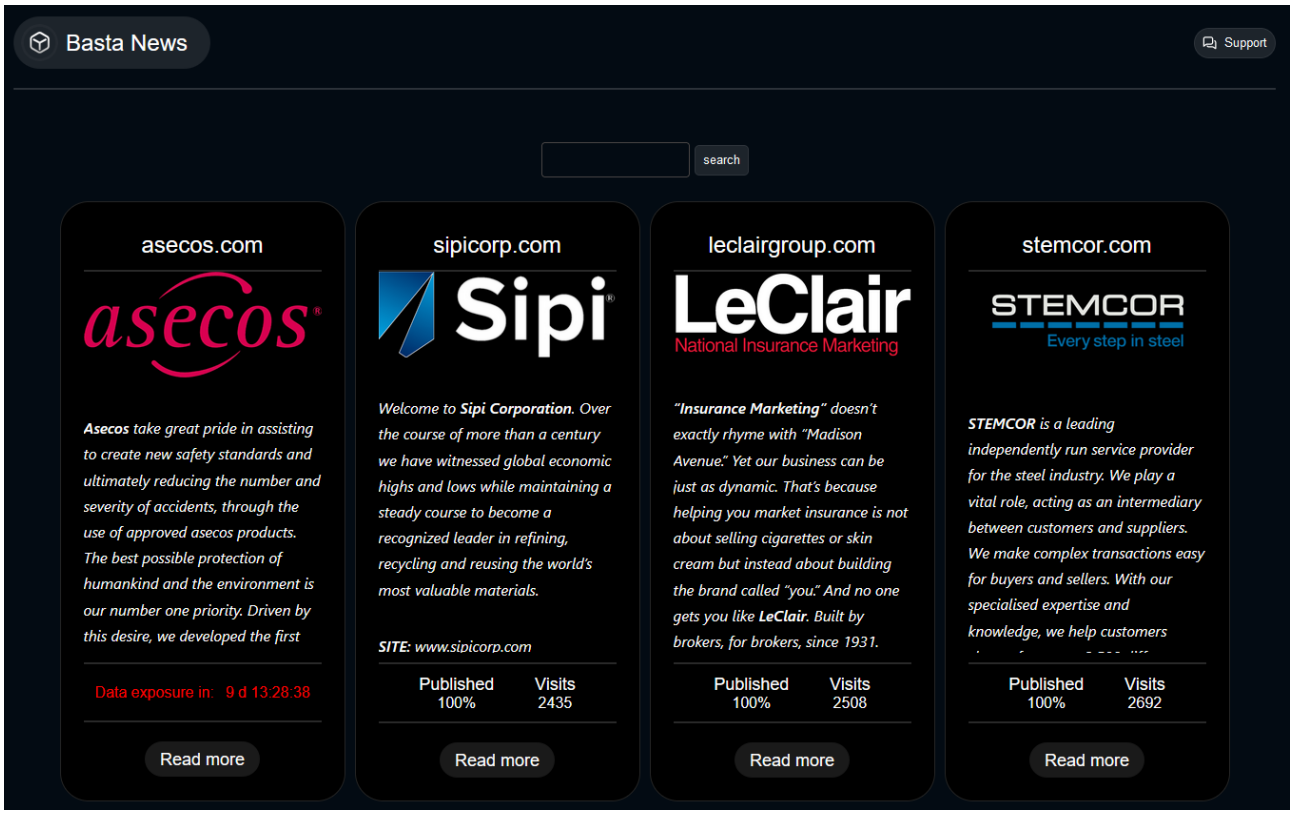
[6] VPN: A virtual security network used to protect personal information and bypass regional restrictions on the Internet

[7] CVE-2023-20269: A vulnerability that could allow an attacker to gain VPN access due to improper authentication, authorization, account management, etc.

[8] NAS: A storage device connected to a network that allows multiple users to share and access data

■ Focus of ransomware

Outline of the BlackBasta ransomware



Source: BlackBasta ransomware group data leak site

The BlackBasta ransomware is a ransomware group that appeared in April 2022 and showed off its influence by attacking more than 20 locations in two weeks and posting leaked data on a dark web blog. To date, it has ransom from over 340 organizations, and is known to have secured a total of $107 million (about ₩143 billion) in cryptocurrency through negotiations (as of November 2023). It mainly targets organizations in the United States and European countries, and is distributing not only the Windows version but also the Linux version of the ransomware that infects VMware ESXi[9].

[9] VMware ESXi: A Unix-based logical platform that can run multiple operating systems simultaneously on the host computer

It uses email attachments or links to initially access the system. It induces the installation of QakBot by encouraging execution of compressed files or document files attached to malicious emails. Then, it collects internal data using the installed QakBot[10] and carries out a BlackBasta ransomware attack. BlackBasta uses a double extortion method, i.e. demanding ransom from infected targets and conducting additional negotiations under the pretext of data leakage.

QakBot, which BlackBasta used for initial access, is a malware used by several ransomware groups such as LockBit, Knight, and REvil for initial access and ransomware distribution. QakBot, which appeared in 2008, was used for financial fraud for the purpose of initial access and information collection, and began to be used to distribute ransomware in 2019. QakBot's malware infrastructure was neutralized by a large-scale FBI operation in August 2023, but a new version of QakBot appeared in December of the same year and is still used for initial access. BlackBasta also uses Pikabot[11], which is similar to QakBot, for attacks.

SRLabs, a German security research institute, released Black Basta Buster, a BlackBasta decryption tool, on its GitHub[12] on December 27, 2023. SRLabs discovered a vulnerability in which encryption keys are reused in versions of BlackBasta ransomware from November 2022 to early December 2023, and developed a tool that can use this to recover all or part of files. However, the BlackBasta ransomware quickly modified the key reuse vulnerability before the decryption tool was released so that encrypted files could not be recovered even if Black Basta Buster is used.

[10] QakBot (Qbot): A type of malware that provides functions such as backdooring, data takeover, internal propagation, remote code execution, and file downloading

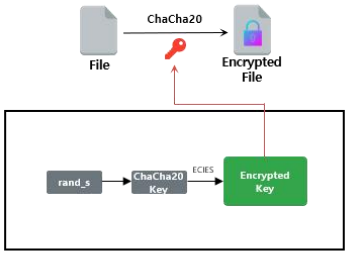
[11] Pikabot: A type of malware that provides functions such as backdooring, data takeover, internal propagation, remote code execution, and file downloading

[12] Github: Web-based source code version management and collaboration platform

BlackBasta Ransomeware

Encryption Key

Encrypt files with the ChaCha20 algorithm and protect the key with ECIES*



Encryption Method

For files less than 5KB : full file encryption

For files greater than 5KB: full encryption of the front part, intermittent encryption of the remaining area

File Size	Full Encryption Size	Intermittent Encryption Interval
0 - 5KB	Entire Data	0B
5KB - 5MB	5KB	640B
5MB - 50MB	5KB	1.28KB
50MB - 1GB	5KB	6.4KB
1GB - 10GB	15KB	12.8KB
10GB or Larger	50KB	64KB

Features

Argument required

System recovery Option removal

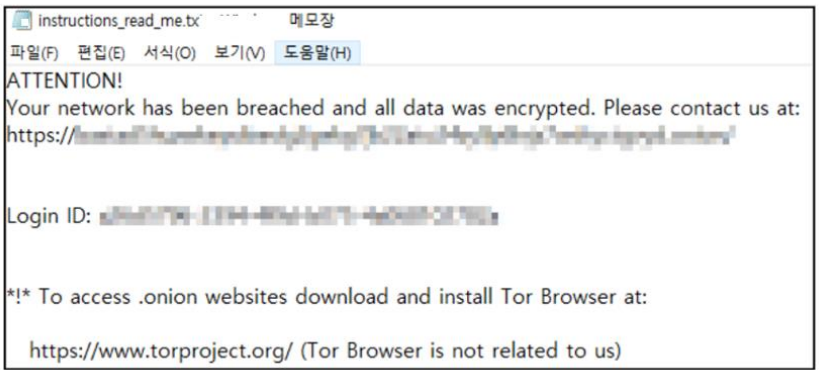
Active Directory Lateral movement

ChaCha20 & ECIES Encryption

Multi thread

Kill Service and processes

Ransom Note



instructions_read_me.txt

Extension

.7wdojib58

Production Language

C/C++

** Elliptic Curve Integrated Encryption Scheme (ECIES): An encryption framework tha creates a symmetric key using an asymmetric key, encrypts data with the generated symmetric key and then adds a message authentication code(MAC)*

Figure 5. BlackBasta ransomware Outline

BlackBasta ransomware strategies

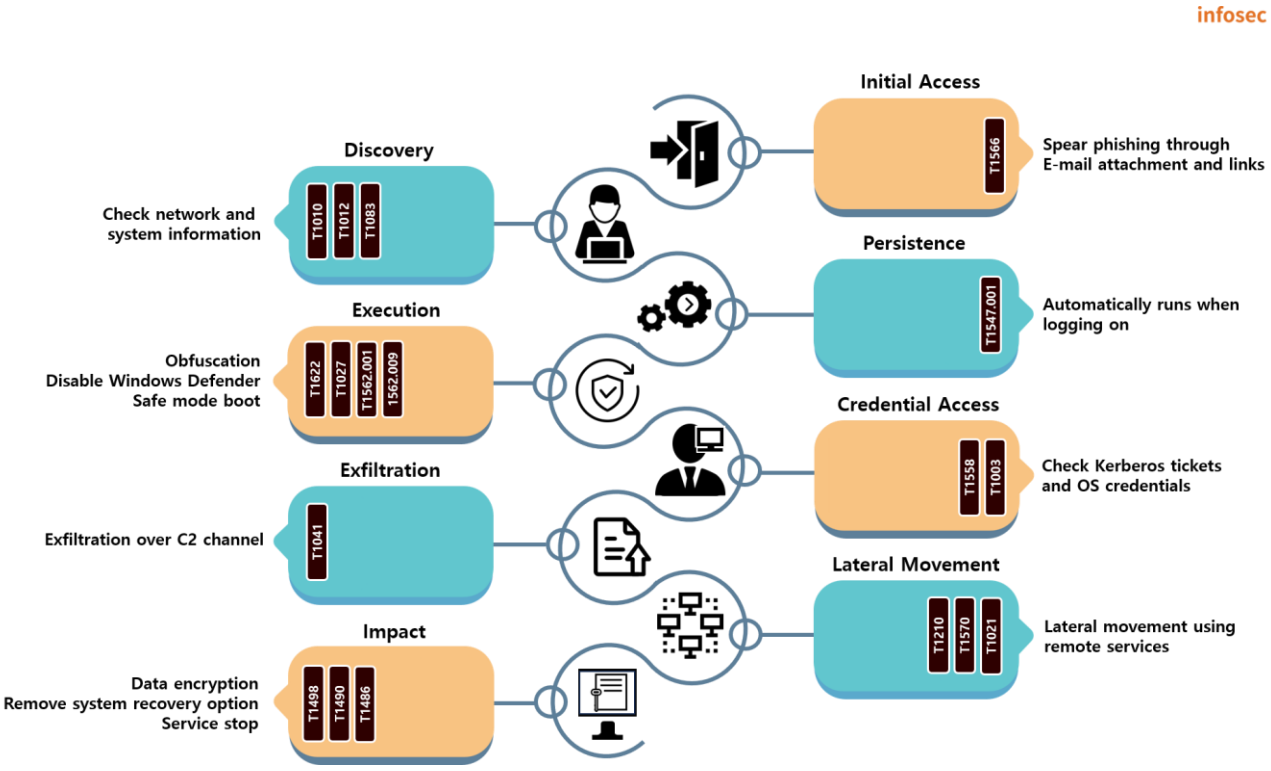


Figure 6. BlackBasta ransomware attack strategies

BlackBasta primarily performs initial access through spear phishing[13]. After attaching a compressed file or a document file with a macro inserted to an email, infection occurs when the user executes the attached file. When you open the attached file or click the link, QakBot is installed through the attached script. QakBot additionally installs several tools such as Mimikatz[14], Cobalt Strike[15], and PsExec[16] for detection bypass, credential takeover, ransomware distribution, and internal propagation.

[13] Spear phishing: An attack targeting a specific person. It is an attack technique that tricks the target into leaking personal information or downloading malware.

[14] Mimikatz: A tool to extract sensitive information such as passwords and credentials from the memory of the Windows system.

[15] Cobalt Strike: A penetration testing tool with capabilities such as gaining system privileges and stealing account information, lateral movement, and C2 communications.

[16] Psexec: A tool that can run arbitrary processes on local/remote systems

First, it performs tasks to bypass detection, e.g., terminating the Anti-Virus service or booting in safe mode using additionally installed tools. Afterwards, it secures sensitive data to be used for threats, such as user folders or company technical documents, and distributes and executes ransomware files. It attempts double extortion using the data collected in this way and the encrypted files.

The BlackBasta ransomware first checks command execution arguments. It can perform various functions through corresponding arguments. Also, given that it is executed normally without passing additional arguments, functions were added for the convenience and efficiency of attacks.

Argument	Description
-thread {int}	Set the number of threads created when performing encryption (the default is 4)
-nomutex	Disable mutex[17] creation
-file {file_name}	Encrypt only designated files
-bomb	Spread BlackBasta internally through AD[18]
-disablewhitelist	Disable encryption exceptions
-forcepath {path}	Encrypt only designated paths
-nordp	Disable the RDP[19] registry setting function

Table 1. BlackBasta ransomware arguments

Among the execution arguments, the -bomb argument performs the function of spreading and executing ransomware files to all PCs existing on the same AD server using LDAP query[20]. The ransomware file is copied and executed in the C:₩Windows₩bb.exe path of all user terminals managed by the AD server.

[17] Mutex: A technique that prevents multiple threads from accessing the same resource simultaneously in an environment running multiple threads.

[18] Active Directory (AD): A directory service function provided by MS. It is a Windows-based centralized management service that can manage resources and permissions within an organization.

[19] Remote Desktop Protocol (RDP): A protocol that makes it possible to remotely control other computers

[20] LDAP query: A command used in the software protocol (LDAP) that allows you to search for organizations, individuals, files, devices, etc. on a network

The BlackBasta ransomware encrypts in units of 64 B, uses multi-threading for fast encryption, and applies different encryption methods depending on the file size. The older version of BlackBasta, created between November 2022 and early December 2023, encrypts files in three ways depending on the file size. For files smaller than 5 KB, all data is encrypted, and for files larger than 5 KB but less than 1 GB, only 64 B of every 192B is encrypted. For files larger than 1 GB, the first 5 KB is encrypted, and for the remainder, only the first 64 B is encrypted every 6.4 KB.

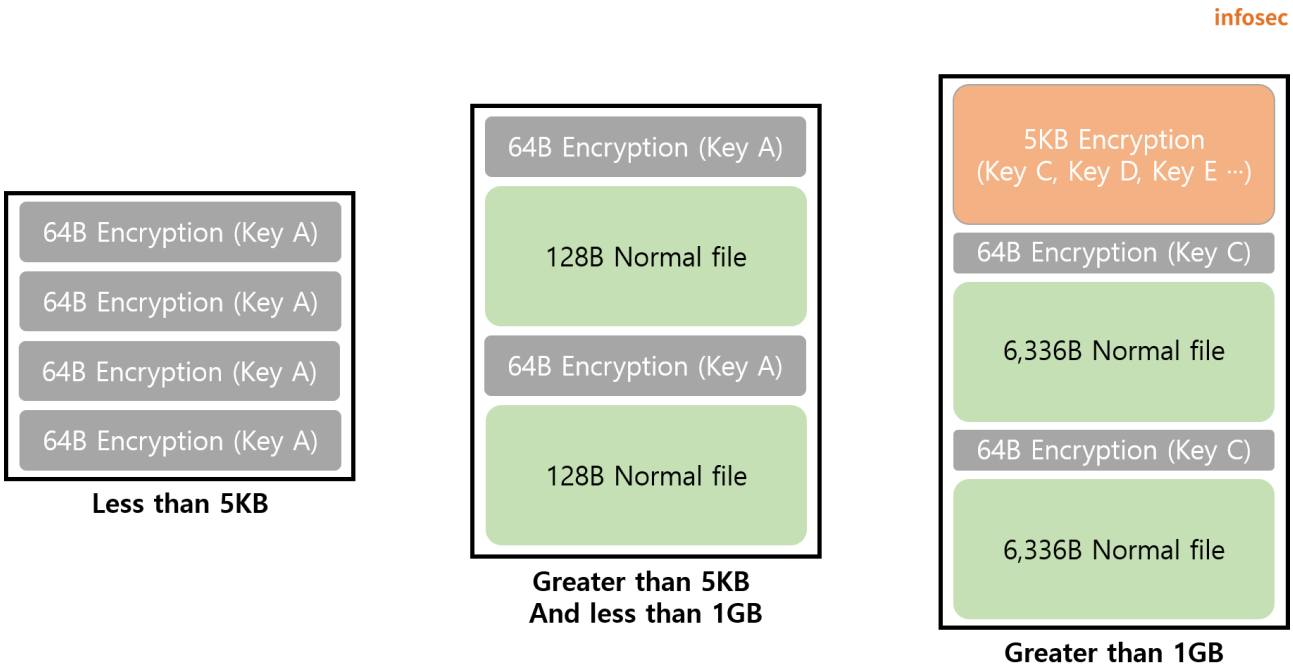


Figure 7. Redundant use of the key of the older-version BlackBasta

When the older version of the BlackBasta ransomware encrypts a file over 1 GB in size, it encrypts the first 5 KB of the file by updating the key each time, and uses the same key in the remaining process without updating the key. This encryption method has a problem, i.e. the encryption key is exposed as is in the area where the file has 0x00 values. If the exposed encryption key is used, all or part of the file can be recovered. The decryption tool distributed by SRLabs also took advantage of this. As only the part where the key is used repeatedly can be recovered, however, the first 5 KB of a file larger than 1 GB cannot be recovered.

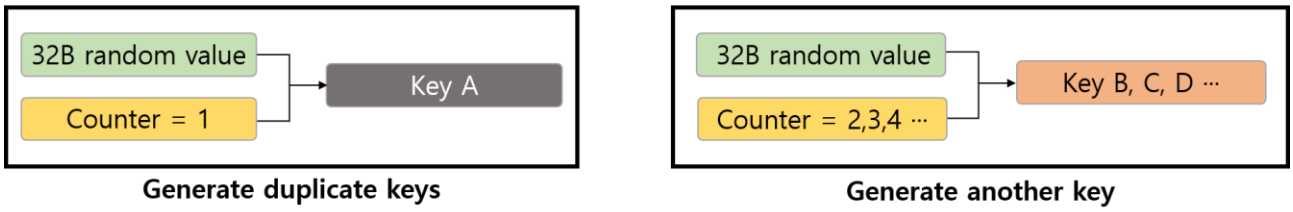


Figure 8. Key creation method

The encryption key is generated using a random value of 32 B and a Counter value set to 1 for each file, and another key can be created by increasing the counter value by 1. In the older version, a key with a counter value set to 1 is used repeatedly for files less than 1 GB, and a different key is created and used only when the first 5 KB of a file over 1 GB is encrypted.

Some improvements have been made in the latest version of the BlackBasta ransomware, created since mid-December 2023. For files smaller than 5 KB, all data is encrypted, and for files larger than 5 KB, only the front part is fully encrypted and the remainder is partially encrypted. For files larger than 5 KB, the full encryption size and partial encryption interval are differently applied depending on the file size. In summary, a total of six file encryption methods are used, with data size standards subdivided further than before.

File size	Full encryption size	Partial encryption interval
0 – 5KB	All data	0B
5KB – 5MB	5KB	640B
5MB – 50MB	5KB	1.28KB
50MB – 1GB	5KB	6.4KB
1GB – 10GB	15KB	12.8KB
10GB or larger	50KB	64KB

Table 2. Encryption methods by file size

In addition, problems with older versions that used the same keys have been corrected. Now, used keys must be initialized to prevent duplicate keys from being used within the file. Therefore, even if the key is exposed, only the part that used the key can be recovered, and it is difficult to recover the entire file.

infosec

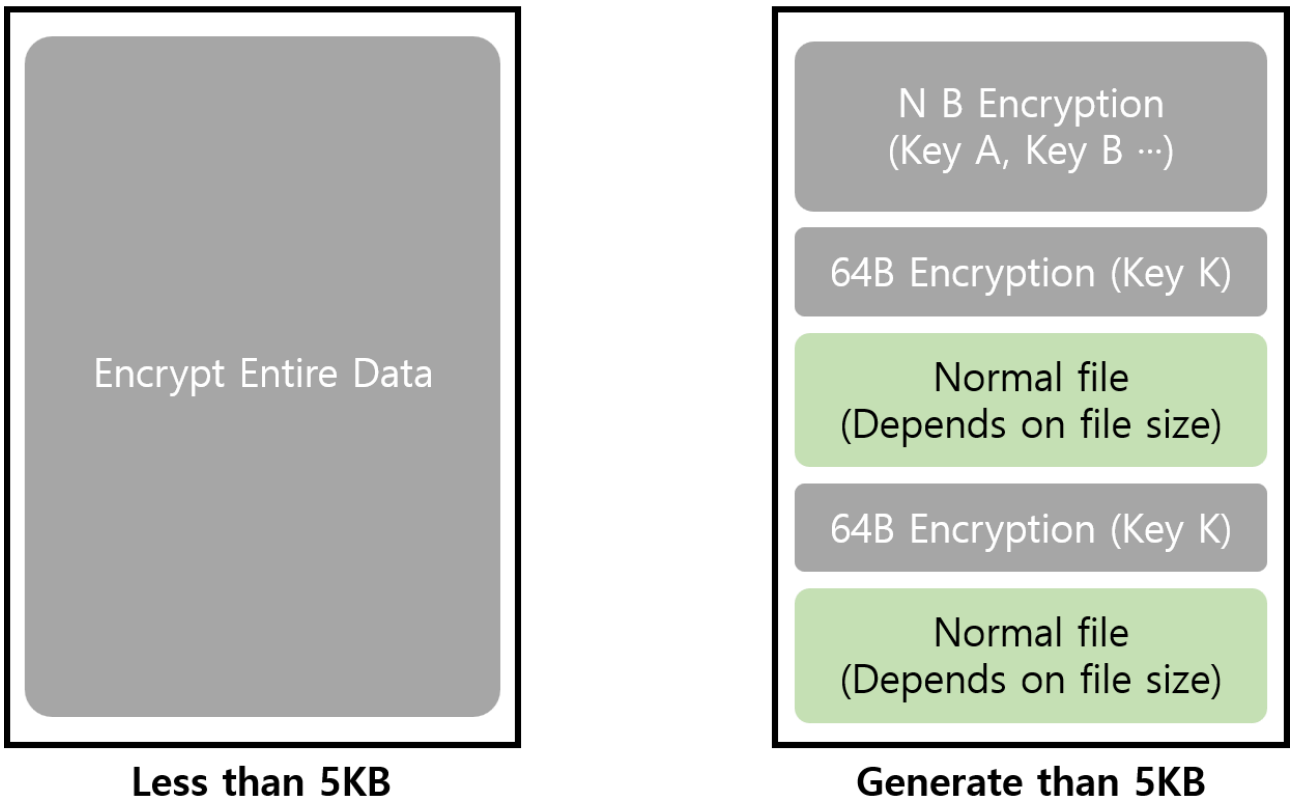


Figure 9. Latest version encryption method

How to respond to the BlackBasta ransomware

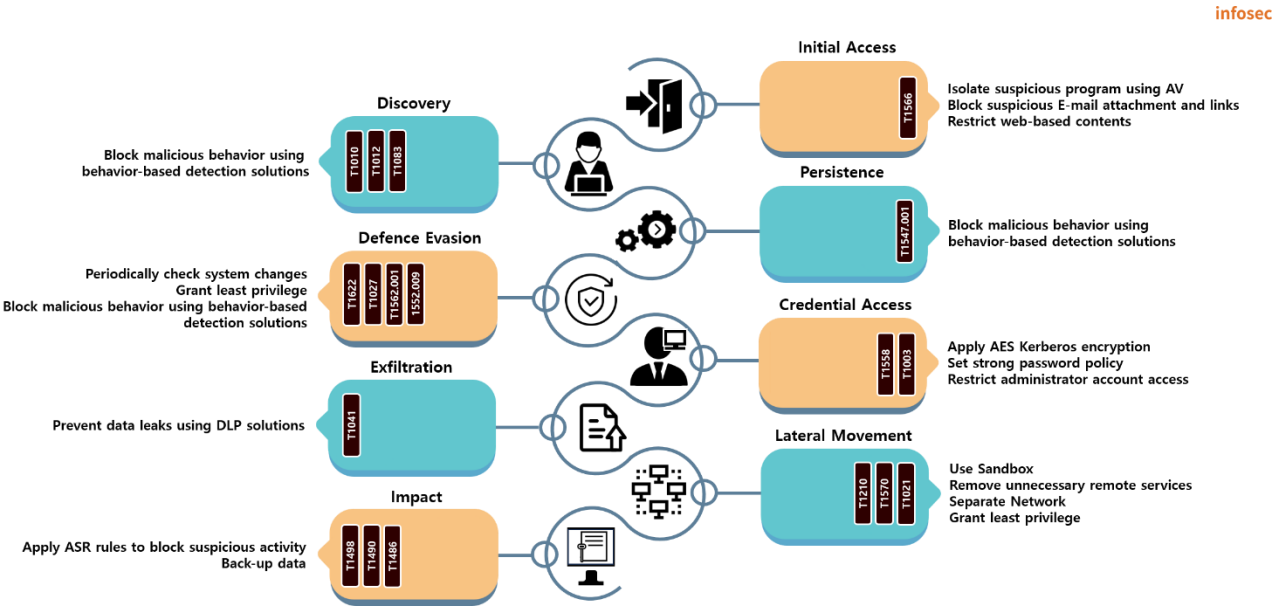


Figure 10. How to respond to the BlackBasta ransomware

BlackBasta attempts initial access through spear phishing. Therefore, you can block contents downloaded from the web or use a separate anti-virus to prevent downloaded malicious files from being executed. In particular, you must be alert not to view links or files in emails from unknown sources, and you must prevent infection through malicious email simulation training to increase security awareness.

After initial access, to avoid detection and continue execution, the registry is manipulated, or the Anti-Virus service is terminated and booting in the safe mode is used. This can be blocked through the use of a behavior-based detection solution.

Also, it attempts to hijack AD accounts and uses the stolen accounts to spread ransomware to all users within the AD server. Therefore, a powerful encryption method must be used to prevent AD server administrator accounts from being easily hijacked. In addition, even if the account is hijacked, preventive measures such as granting minimal permissions to user and service accounts and managing them separately are necessary so that the server cannot be taken over. In addition, through continuous monitoring, you must check whether there is anything suspicious in the list of services and group policies registered in AD.

It is also necessary to prepare for data takeover, deletion of backup data, and file encryption. DLP[21] solutions must be used to prevent data from being leaked and exploited. Additionally, files must be managed through regular backups. Meanwhile, as there are cases where data in NAS and backup storage is deleted, e.g., the Akira ransomware, vaulting backup[22] of the data to a separate network or storage for management is recommended.

[21] Data Loss Prevention (DLP): A data leak prevention solution that monitors the flow of data and monitors/blocks important information leaks.

[22] Vaulting backup: A method of storing backed-up data separately at a certain distance away.

Indicator Of Compromise

BlackBasta(April. 2023) : SHA256

fe87fa7714266548fa5da52455f1788f588417ee800c86768d163abd279d0279
ef2a754a8e713fd6deaa642e2220af372fd310a755a02126938ff233b16a4a83

BlackBasta(December. 2023) : SHA256

f971a05b8540fa6af8cb6c54d2c2de00c54fa99a4e86615daca03a6d7c0e4e6f
b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9

File Name

4WCB3ACCQFJBTGE966849RFVY6.bdq.00000000_BITDEFENDER.out
STUDIO_BBG.dll
RibbonGadgets.EXE

■ Reference site

URL : https://www.bleepingcomputer.com/news/security/new-black-basta-decryptor-exploits-ransomware-flaw-to-recover-files/

URL : https://directoryadmin.blogspot.com/2014/12/ldap-queries-for-users-computers-groups.html

URL : https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware/

URL : https://www.zscaler.com/blogs/security-research/back-black-basta

URL : https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

URL : https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/

URL : https://www.zscaler.com/blogs/security-research/tracking-15-years-qakbot-development