Keep up with Ransomware

Underground ransomware targeting Korean manufacturers already twice this year

■ Overview

In December 2024, there were 673 cases reported of ransomware damage, an increase of nine from November's 664 cases. This rise is attributed to the emergence of the FunkSec group, which reported 89 victims, and the Clop ransomware group's exploitation of vulnerabilities in Cleo's file-sharing solution, causing 66 victims.

Clop exploited file writing vulnerabilities (CVE-2024-50623 and CVE-2024-55956) Cleo's file transfer products—Harmony, VLTrader, and LexiCom. Specifically, CVE-2024-50623 was discovered in October last year and patched, and although a patch was distributed, it did not fully mitigate the original vulnerability. Two months later, a new vulnerability, CVE-2024-55956, emerged, allowing only file reading. These flaws enabled Clop to upload and execute malicious code, such as the Java-based backdoor[1] Malichus, facilitating data theft and other malicious activities. Clop listed 66 affected companies, with their names partially filtered, on their dark web leak site, threatening to disclose their identities in 2025 if the victim companies do not take any action.

LockBit Group showed declining activities following Operation Cronos, which disrupted the group's infrastructure. However, on December 19, it announced the release of LockBit 4.0 on its dark website, seeking new affiliates. It offered access to a management panel for USD 777 (about KRW 1.1 million) in cryptocurrency, providing tools for ransomware creation across Windows, ESXi, and Linux platforms, along with infrastructure such as victim management. However, details about LockBit 4.0's capabilities have not been released yet, warranting ongoing monitoring.

[1] Backdoor: Malware that can access the target system without going through the normal authentication process.

Ransomware threats have continued, two cases of ransomware incidents involving Korean companies were reported in December. The RansomHub group targeted a Korean specialty wire product manufacturer, leaking financial, accounting, and insurance-related data. Moreover, Underground Group disclosed data from a Korean semiconductor parts manufacturer through a dark web leak site and Telegram, releasing 745 GB of data, including employee personal information and financial documents, within two days of the initial breach.

In a related development, IntelBroker, which stole 4.5 TB of data from network and security service provider Cisco in October and posted a sale ad on BreachForums, has released some of the stolen data for free. The investigation into the data breach revealed that the data was stolen via DevHub, a resource center for accessing source code, scripts, and other content. IntelBroker claimed the stolen data included source code, credentials, and corporate documents. It released 4.84 GB of data for free on December 25.

News About Ransomware

Clop group launches large-scale attack exploiting Cleo vulnerabilities

- Exploitation of Cleo Harmony, VLTrader, and LexiCom Vulnerabilities (CVE-2024-50623, CVE-2024-55956)
- The vulnerabilities allow file read/write access, enabling Java backdoor upload and further malicious actions.
- Claimed to have stolen data from a total of 66 companies.
- If no action is taken, the list of all victims will be released in 2025.

LockBit 4.0 released

- The LockBit group has announced the release of LockBit 4.0 on their DLS.
- The group is recruiting new partners, offering ransomware and panel access for $777.

IntelBroker has released some Cisco data for free

- IntelBroker released 4.84GB of the 4.5TB of Cisco data stolen in October for free on December 25.
- They claim to have stolen the data through the DevHub resource center.

RansomHub attacked a Korean semiconductor manufacturer

- On December 3, RansomHub posted a message threatening to release data along with sample files.
- They claim the data includes financial, accounting, and insurance-related information.
- On December 10, they fully released approximately 58GB of data.

Underground attacked a Korean semiconductor parts manufacturer

- On December 17, they posted a ransom note and sample data on Telegram and dark web leak sites.
- It includes employee personal information and financial documents.
- On December 19, they fully released approximately 745GB of data.
- The victim company was attacked in November and restored the system without paying the ransom.

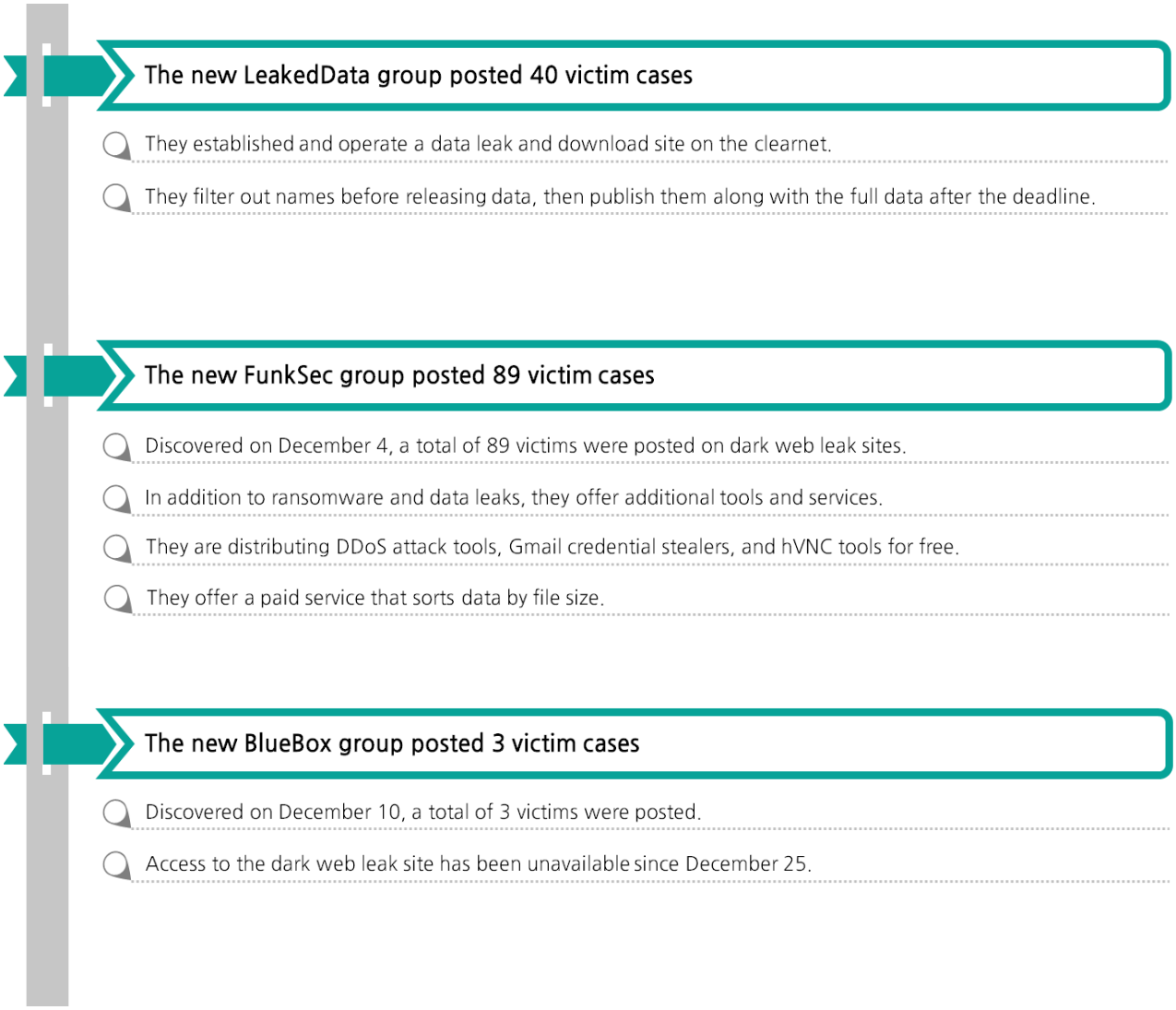


Figure 1. Trends of ransomware

Ransomware Threats

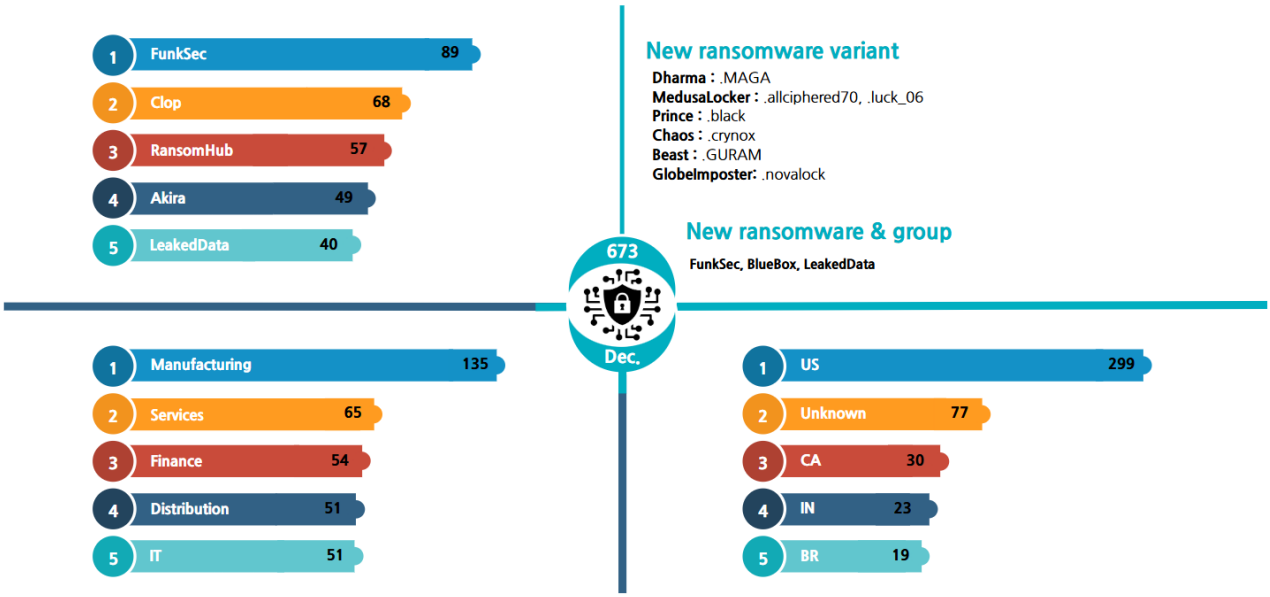


Figure 2. Ransomware Threats in December 2024

New Threats

Three new ransomware groups were discovered in December. BlueBox Group was discovered on December 10, with two victim postings at the time. One more post was made a week later, but as of December 25, the dark web leak site has been inaccessible.

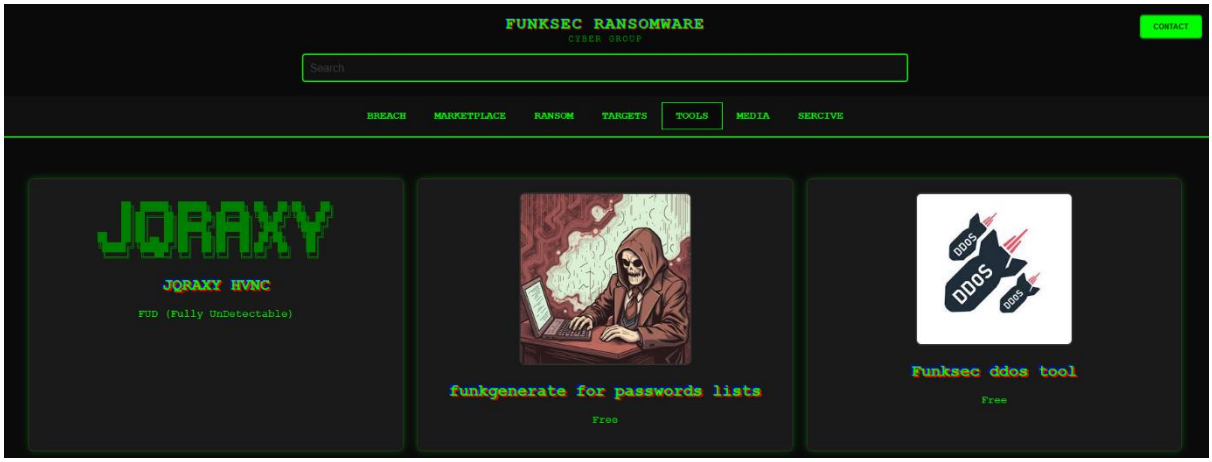


Figure 3. FunkSec Dark Web Site

A new ransomware group called FunkSec was discovered on December 4 and is posting victim companies' data on its dark website. It reported 89 new victim claims in December alone and is selling stolen corporate data and personal information of unknown origin (passports, account information, etc.). FunkSec promotes FunkLocker, which has features such as file encryption using the AES algorithm, stealing account data from browsers, and reverse shell[2]. In addition, it offers various tools and services for free, such as DDoS attack tools, Gmail account hijacking tools, and hVNC malware that builds a virtual network and allows remote access without the user's knowledge.

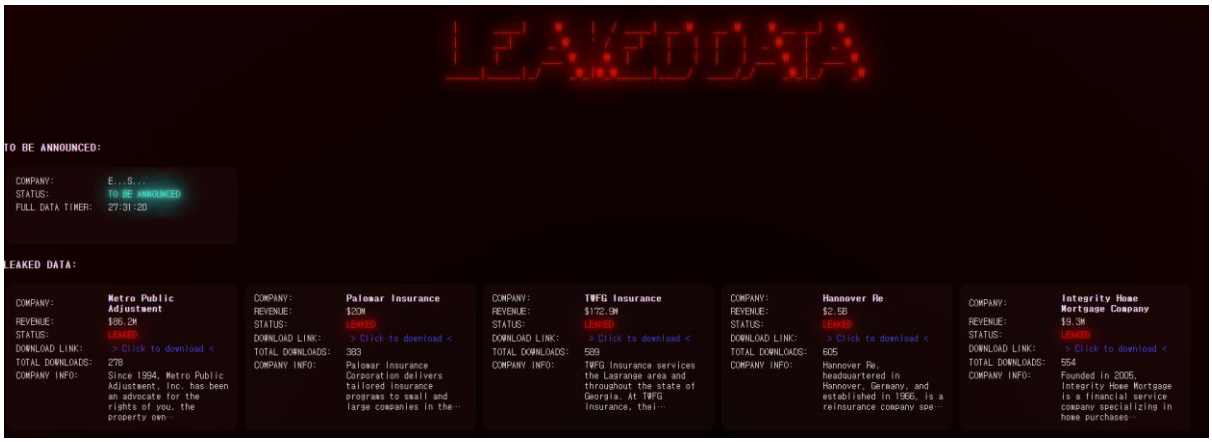


Figure 4. LeakedData Leak Site

Groups active on the Clearnet were also identified. The LeakedData group has been releasing data via Clearnet and uploaded 40 victims in December. Initially, the names of companies scheduled to be disclosed were filtered, and after a set period of time, the company names and download links for all data will be disclosed.

[2] Reverse shell: Malware that connects to a receiving server set in advance by the attacker and allows the attacker to execute commands on the system.

Top 5 Ransomwares

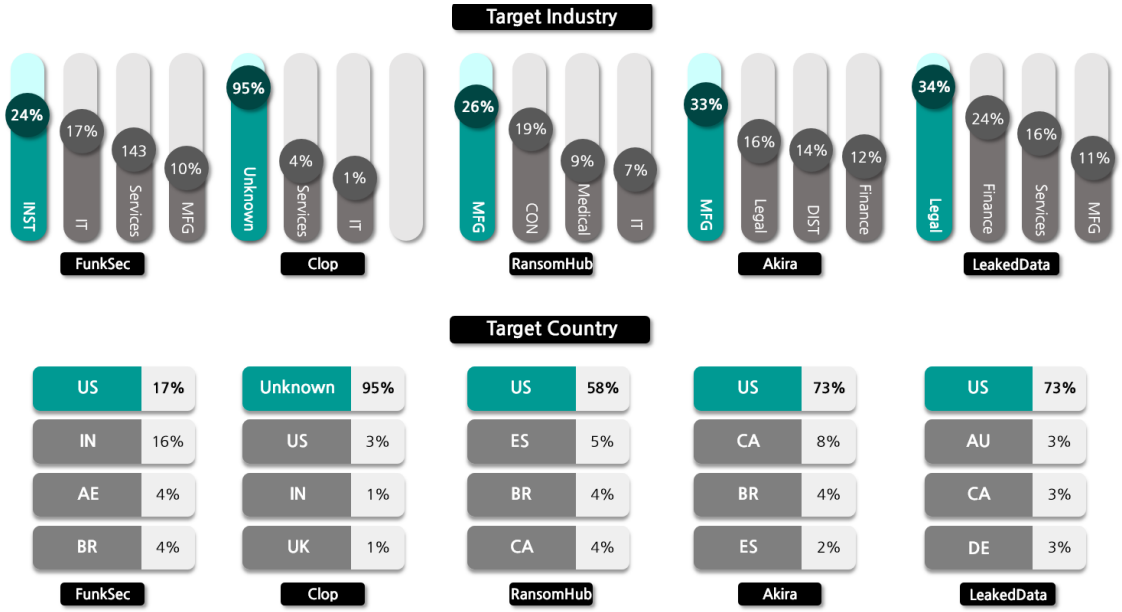


Figure 5. Major Ransomware Attacks by Industry/Country

The FunkSec group was the most active, posting 89 victim accounts despite only appearing in December. The group steals and sells corporate data, trades access rights to company infrastructure or website management pages and sells the personal information of individuals from specific nationalities. In addition to selling such data, it freely distributes tools like DDoS attack utilities, account hijacking software, and hVNC. Moreover, some companies attacked by the FunkSec group have been defaced[3], with FunkSec's images inserted onto their websites.

Clop Group, which exploited an SQL injection vulnerability (CVE-2023-34362) in the managed file transfer (MFT) tools MOVEit Transfer and MOVEit Cloud to cause a large-scale data breach in 2023, caused a breach again in 2024 by exploiting a vulnerability in an MFT tool. The group targeted file write vulnerabilities (CVE-2024-50623 and CVE-2024-55956) in Cleo's file transfer solutions, including Cleo Harmony, VLTrader, and LexiCom, compromising 66 companies. When the list of victims was first disclosed, the company names were filtered out, but it was announced that if there was no progress in negotiations, the full list would be released in 2025.

[3] Deface: An attack method that changes the design of a website to the hacker's intention to notify that the hacking was successful.

On December 5, RansomHub Group attacked the US subsidiary of a Korean company, stealing approximately 200 GB of data. The victim company is an American high-pressure tank manufacturer acquired in 2020, and the victim company, a high-pressure tank manufacturer acquired in 2020. RansomHub released the entire data in a compressed file seven days later, on December 12. RansomHub attacked the US-based medical and consumer products company Tekni-Plex, stealing around 420 GB of sensitive data and releasing samples, including several contracts and real estate documents. As negotiations stalled, RansomHub gradually leaked parts of the stolen data and negotiation chat records every three days, finally releasing the entire dataset on December 23.

Akira Group, which had surged in activity in November by leaking data from 74 victims, remained highly active in December, causing 49 more victims. One of its major attacks was against the US investment firm Luxor Capital Group, from which it stole medical records, passports, birth certificates, confidential correspondence, financial information, and contract details.

A new group, LeakedData, emerged in December, has disclosed data from 40 victims and listed them on its Clearnet-operated leak site. It filtered company names during the negotiation period but later fully disclosed names and data if demands were not met. Among the 40 publicly disclosed victims, 29 were US-based, primarily operating in the finance, legal, and tax sectors.

Ransomware Focus

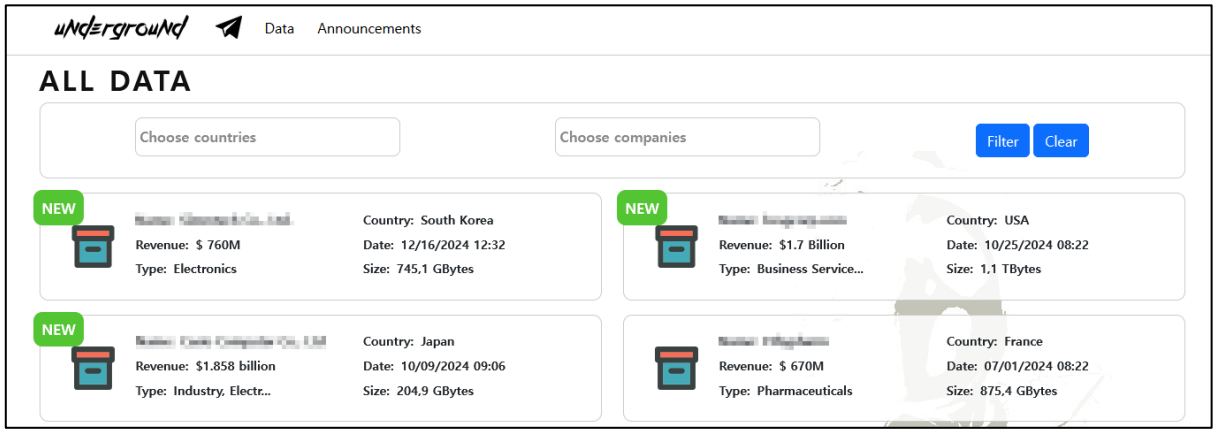


Figure 6. Underground's Dark Web Leak Site

Underground Group was discovered in July 2023. The group did not operate a separate dark web leak site in the early stages of its activities and instead used a chat site listed in the ransom note to negotiate ransoms. In May 2024, a new dark web leak site posting data stolen from comprised companies was discovered. As of December 24, the site had listed a total of 19 victims. Two of the victims were identified as domestic manufacturers, and the stolen data was uploaded in March and December.

Figure 7. Underground Group Telegram Channel

It also started operating a Telegram channel in March 2024, where it not only shared updates on newly added victims and sample data but also uploaded full datasets to the online storage service MEGA and shared its links via Telegram.

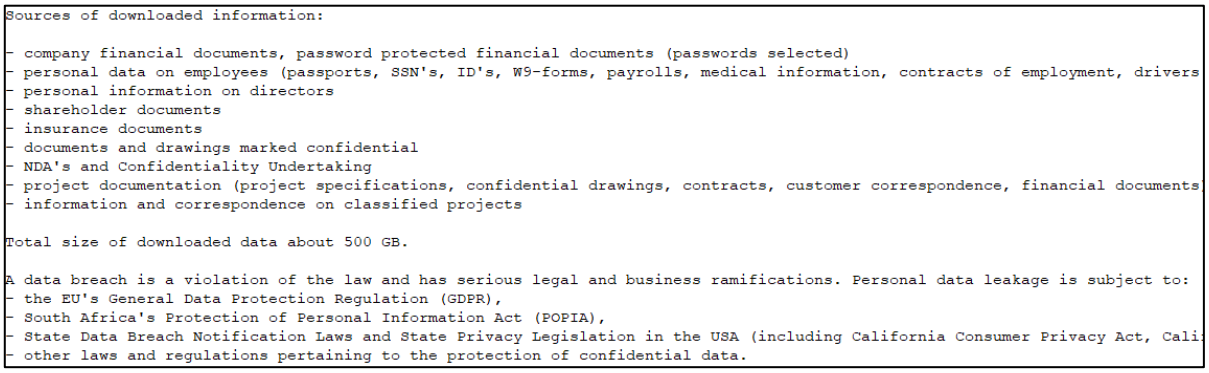


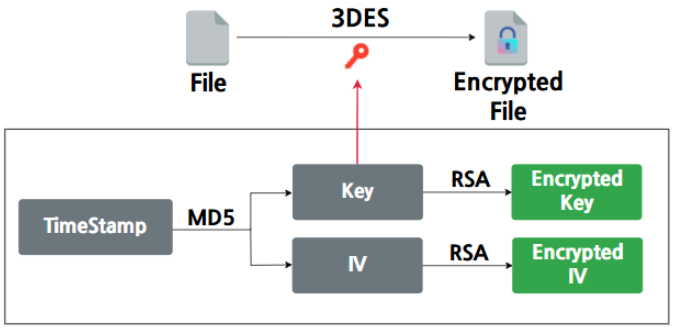
Figure 8. Underground Ransom Note

Underground Group customizes ransom notes for each target. The ransom note states a list of stolen data and its total size, as well as legal violations that can arise from the data leak, using this as leverage to threaten victims. Additionally, the ransom note provides the address of a dark web chat site along with the necessary ID and password, encouraging victims to negotiate directly.

Underground Ransomware

Encryption Key

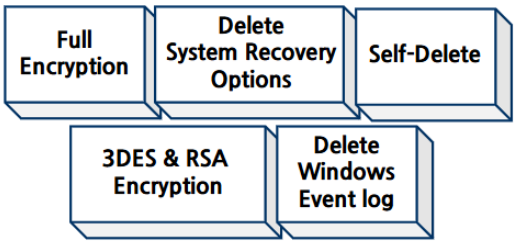
Encrypt files with 3DES algorithm and protect the key and IV with RSA



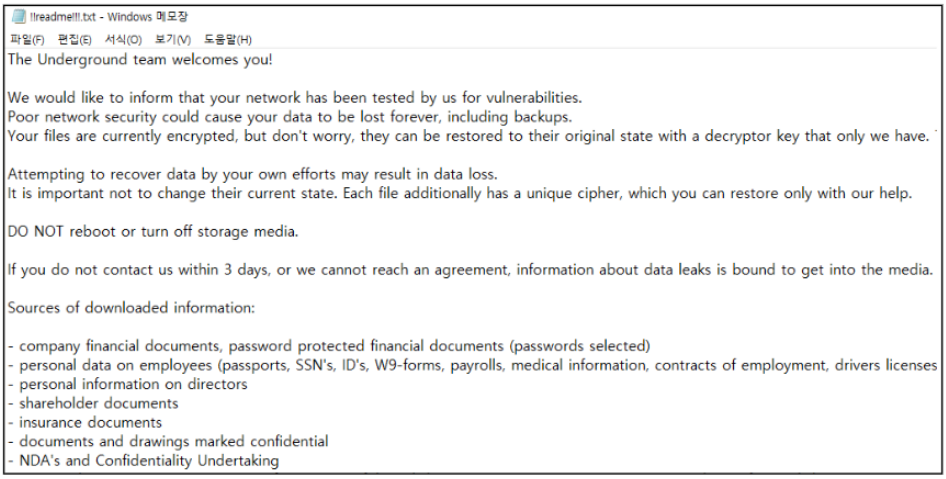
Encryption Method

Encryption of entire files

Features



Ransom Note



!!readme!!!.txt

Extension

No extension change

Production Language

C/C++

Figure 9. Overview of the Underground Ransomware

Strategy of the Underground Ransomware

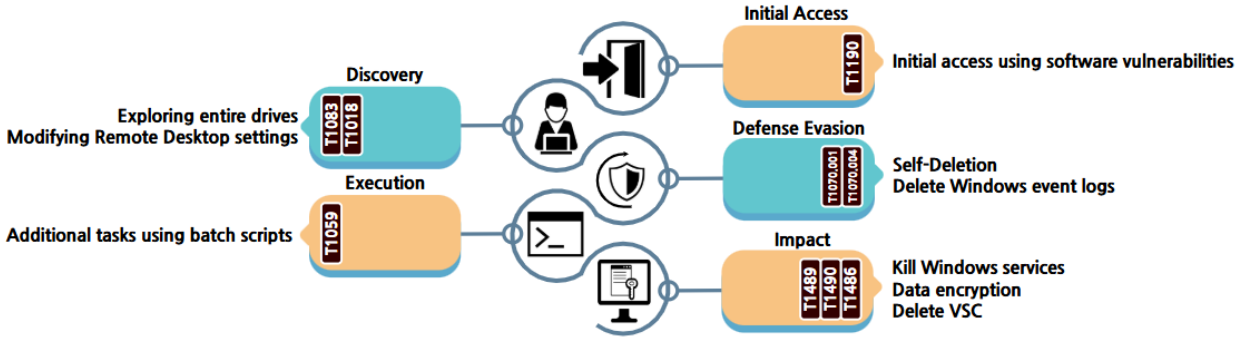


Figure 10. Attack Strategy of the Underground Ransomware

The Underground ransomware first deletes backup copies and stops running the MS SQL server using Windows commands. It modifies the registry to change the maximum retention time for remote desktops used for remote access to 14 days. The full list of commands used is shown in Table 1 below.

Command	Description
vssadmin.exe delete shadows /all /quiet	Deleting backup copy
reg.exe add HKLM₩SOFTWARE₩Policies₩Microsoft₩Windows NT₩Terminal Services / v MaxDisconnectionTime / t REG_DWORD / d 1209600000 / f	Changing the maximum retention time for remote desktop access (to 14 days)
net.exe stop MSSQLSERVER /f /m	Shutting down the MS SQL server

Table 1. Execution Commands

It then performs the encryption process. If an encryption target path is entered as an argument, only files existing in that path and its subpaths are encrypted. If the argument is not entered, it must scan and encrypt the entire drive. Moreover, it checks the exceptions stored internally and does not encrypt files with certain directories and extensions. Exceptions are listed in Table 2 below.

Directory	File Extension
Windows Microsoft google₩chrome mozilla₩firefox opera	.sys, .exe, .dll, .bat, .bin, .cmd, .com, .cpl, .gadget, .inf1, .ins, .inx, .isu, .job, .jse, .lnk, .msc, .msi, .mst, .paf, .pif, .ps1, .reg, .rgs, .scr, .sct, .shb, .shs, .u3p, .vb, .vbe, .vbscript, .ws, .wsh, .wsf

Table 2. Encryption Exceptions

```
*lDistanceToMove = 0i64;
*FileSize = v20 - 4;
*DistanceToMoveHigh = 0i64;
SetFilePointer(FileW, v20 - 4, &FileSize[1], 0);
ReadFile(FileW, v15, 4u, &NumberOfBytesWritten, 0i64);// read last 4Bytes
v26 = *FileSize + 4i64;
*FileSize += 4i64;
if ( *v15 == 0x31415926 )            // Check Last 4Bytes of the file
  goto LABEL_63;
```

Figure 11. Checking for Encryption

It traverses directories, accessing target files one by one to check whether each file has already been encrypted. The Underground Ransomware does not change file extensions after encryption. Instead, it appends a 4-byte signature (0x31415926) at the end of encrypted files to identify them. Therefore, before proceeding with encryption, it verifies the last 4 bytes of the file to determine whether it has already been encrypted.

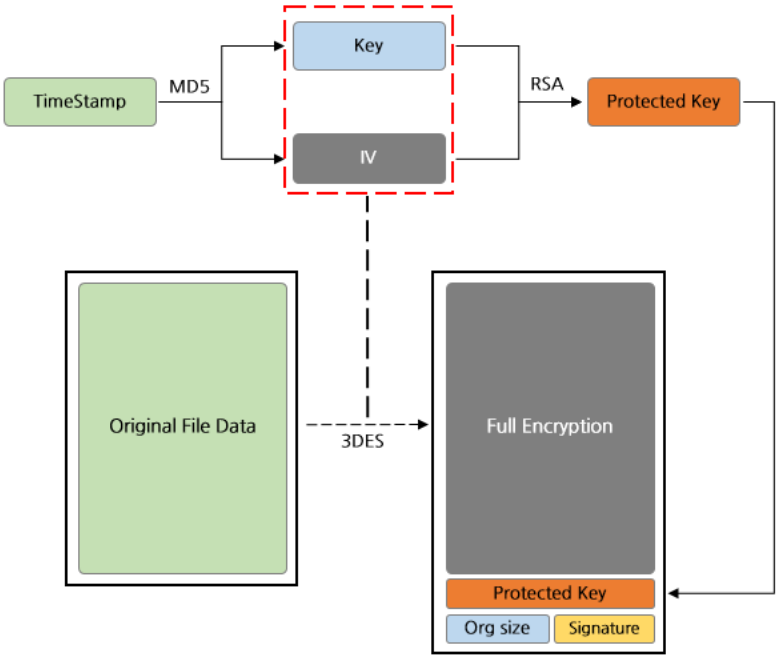


Figure 12. Cryptography Logic

If a target file does not have the signature, Underground Ransomware proceeds with encryption. It retrieves a timestamp representing the current time from each file and generates two MD5 hashes based on it. The first 8 bytes of the first MD5 hash are used as the IV, while the first 24 bytes of the second MD5 hash are used as the encryption key. The entire file is then encrypted using the 3DES algorithm. The encryption key and IV values used for file encryption are encrypted using the RSA algorithm and appended to the end of the file. Additionally, the original file size and a signature (0x31415926) indicating that the file has been encrypted are added at the very end before completing the encryption process. After encrypting the file, a ransom note is created in every directory.

```
FileW = CreateFileW(L"temp.cmd", 0x40000000u, 1u, 0i64, 2u, 0x80u, 0i64);
if ( FileW != -1i64 )
{
  strcpy(
    String,
    "@Echo off\r\n"
    ":rep\r\n"
    "del %1\r\n"
    "if not errorlevel 0 goto rep\r\n"
    "for /F \"tokens=*\" %%1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%%1\"\r\n"
    "del %0\r\n");
  NumberOfBytesWritten = 0;
  memset(Filename, 0, sizeof(Filename));
  memset(CommandLine, 0, sizeof(CommandLine));
  v7 = lstrlenA(String);
  WriteFile(FileW, String, v7, &NumberOfBytesWritten, 0i64);
  CloseHandle(FileW);
  ModuleHandleA = GetModuleHandleA(0i64);
  GetModuleFileNameA(ModuleHandleA, Filename, 0x400u);
  wsprintfA(CommandLine, "temp.cmd %s", Filename);
  StartupInfo.cb = 104;
  memset(&StartupInfo.cb + 1, 0, 100);
  memset(&ProcessInformation, 0, sizeof(ProcessInformation));
  CreateProcessA(0i64, CommandLine, 0i64, 0i64, 0, 0, 0i64, 0i64, &StartupInfo, &ProcessInformation);// self delete
```

Figure 13. Self-delete and Event Log Deletion

After the encryption process is complete, the ransomware and Windows event logs are deleted using a Windows batch script. The hardcoded self-deletion and event log deletion commands are saved in the temp.cmd file, which is then executed before the ransomware terminates.

Countermeasures Against the Underground Ransomware

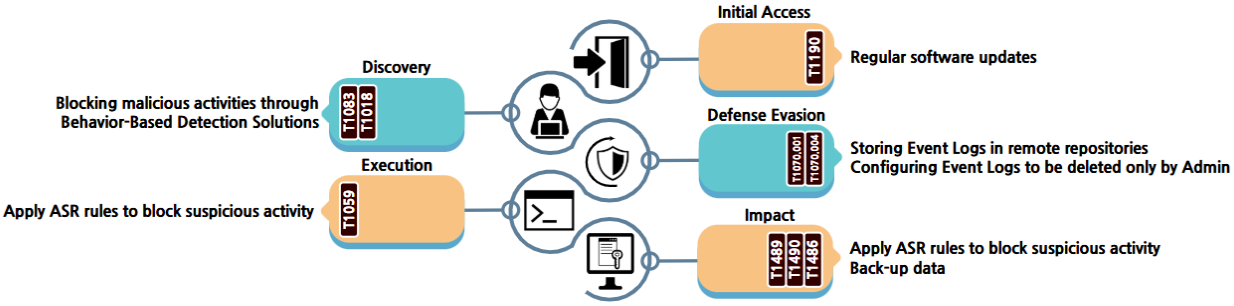


Figure 14. Countermeasures Against the Underground Ransomware

Underground Ransomware is known to distribute its malware by exploiting software vulnerabilities. Therefore, it is essential to regularly inspect the software in use and keep it updated to minimize the risk of intrusion through software vulnerabilities. Additionally, as attackers may attempt to infiltrate systems through links or attachments in phishing emails, anti-virus solutions should be used to prevent the download or execution of malicious files. Damages should be minimized by using a solution that quarantines emails in a virtual environment, such as Email Threat Detection & Response.

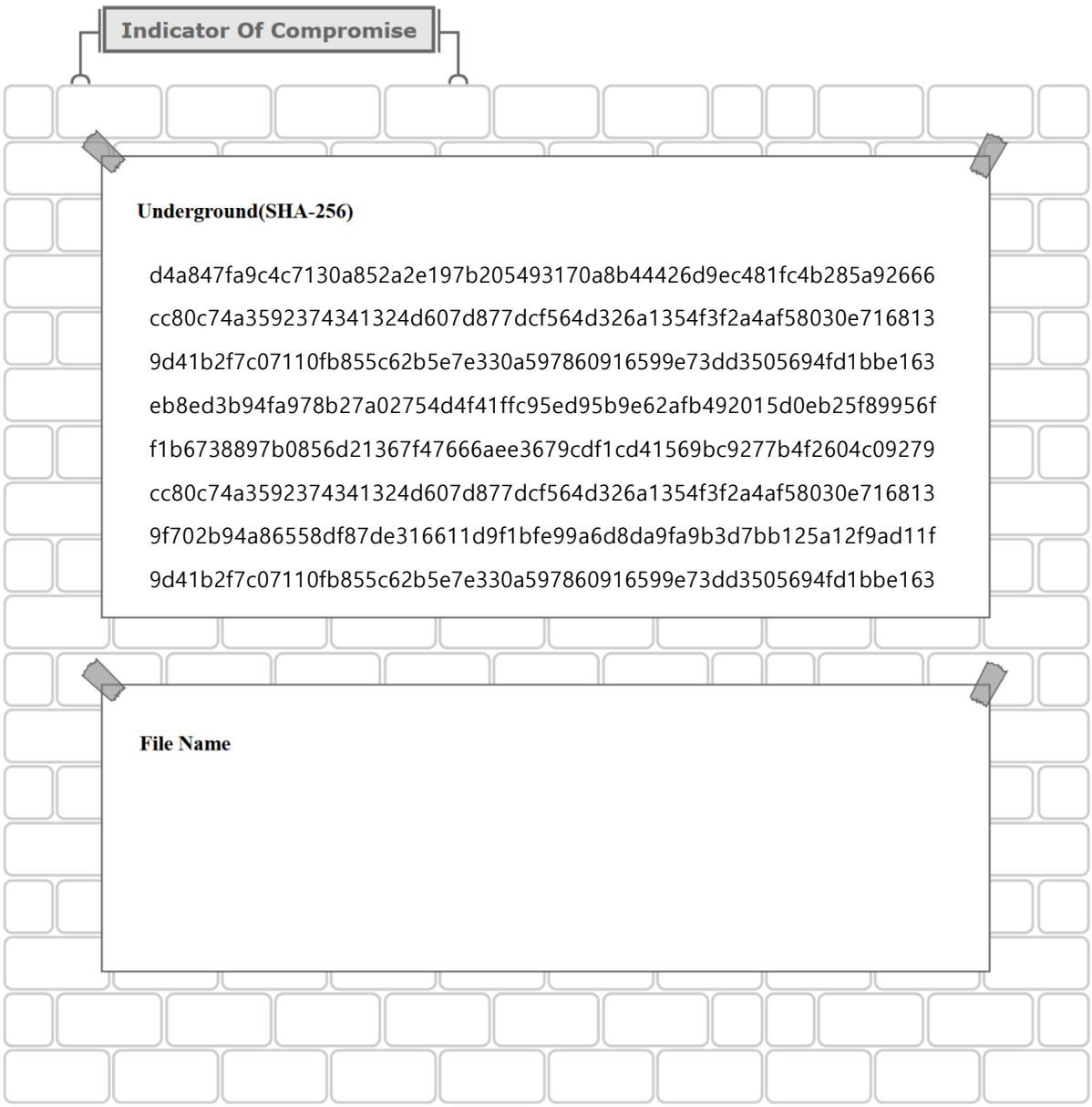
When ransomware is executed, it modifies the remote session timeout settings, terminates specific services, and deletes stored backup copies using Windows commands. Behavior-based detection solutions can block malicious behavior, such as abnormal access attempts to registry paths or service termination. To prepare for possible file encryption by ransomware, backup copies and system recovery files should be stored separately on an isolated network or storage.

Moreover, batch scripts may be used to self-delete ransomware files and erase Windows event logs. To prevent file encryption, ASR (Attack Surface Reduction)[4] rules can be enabled, or an EDR (Endpoint Detection and Response)[5] solution can be utilized to block specific processes used by attackers, thereby preventing malicious activities. Additionally, event logs should be configured to allow access only to authorized users or stored separately in a remote storage location for

[4] ASR: A protection feature that blocks specific processes and executable processes used by attackers.

[5] EDR: 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.

preservation.



■ Reference Sites

• CyberPress (https://cyberpress.org/microsoft-office-zero-day-to-spread-ransomware/)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/)

• Qualys Threat Analysis Report (https://threatprotect.qualys.com/2024/12/03/zyxel-firewall-directory-traversal-vulnerability-exploited-in-ransomware-attack-cve-2024-11667/)

• Security Week (https://www.securityweek.com/hacker-leaks-cisco-data/)

• KBS News (https://news.kbs.co.kr/news/pc/view/view.do?ncd=8133787)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/us-charges-russian-israeli-as-suspected-lockbit-ransomware-coder/)

• Security News (https://www.boannews.com/media/view.asp?idx=135211)

• News Journalism (https://www.ngetnews.com/news/articleView.html?idxno=516169)