Keeping up with Ransomware

InterLock ransomware targets both Windows and Linux environments

■ Overview

In October 2024, there were a total of 550 cases of ransomware damage, an increase of about 35% compared to September (406 cases). The reason for this increase is the emergence of several new ransomware groups and the resumption of activities by many other groups.

A new group called Sarcoma posted 41 attacks in its first month of activity, which was the third most attacks among ransomware groups in October. The APT73 group rebranded as Bashe two months after announcing it was going inactive, and resumed operations, posting 20 attack incidents.

As the amount of damages caused by ransomware continues to increase, international investigative agencies are also becoming more aggressive. The NCA, the UK Home Office's law enforcement agency, has released new information regarding Operation Cronos, which aims to take down the criminal infrastructure of the LockBit group. The main content is the disclosure of personal information and the arrest of LockBit officials. The NCA has released key information about Beverly, which extorted at least $100 million (approximately KRW 138 billion) for ransom while operating as an affiliate of LockBit, and through international cooperation, arrested the developer of LockBit, two suspects involved in the operation, and an official who provided BPH services.[1] They also seized nine of LockBit's infrastructure servers.

An analysis of the seized infrastructure revealed that LockBit group only removed posts from the dark web leak site, rather than deleting the data itself, after receiving the ransom. Due to the prolonged infrastructure neutralization operation, LockBit saw a noticeable decrease in activity, with only two new victim postings in October.

Recently, many ransomware attacks that exploit vulnerabilities have been discovered. The Akira and Fog ransomware groups exploited the CVE-2024-40711 vulnerability discovered in Veeam Backup and Replication, a recovery solution for virtualized environments such as VMware vSphere and Hyper-V. The vulnerability allows remote code execution from untrusted data or a malicious payload.[2] This is an example of a

[1] BPH (Bullet Proof Hosting): A service that provides web hosting while ignoring or avoiding requests from law enforcement agencies; primarily used for illegal online activities.

[2] Payload: Code designed to penetrate, modify, or otherwise damage a computer system.

ransomware group exploiting vulnerability technology analysis and publicly available PoC code[3] after a patch.

A remote code execution vulnerability (CVE-2024-51378[4]) has been found in CyberPanel, a web hosting control panel. The PSUAX ransomware exploited this vulnerability to gain root privileges on the system and encrypt files, and when it was discovered, approximately 20,000 servers were exposed to the threat. However, since the encryption script of the ransomware exposes the RSA private key as it is, it is possible to recover encrypted files without paying anything by using the publicly available decryption script. In addition, two other ransomware and cryptominer[5] programs using the extensions .locked (based on Conti v3) and .encryp (based on the Babuk source code) were distributed.

North Korea-backed threat groups Andariel and Play were found to have used the same accounts for attacks. Last May, Andariel initially infiltrated the attack target by exploiting compromised user accounts, and used the open source C2[6] framework Silver and DTrack, a remote management tool developed by the Lazarus group, to infiltrate internal infrastructure and maintain sessions. In September, they were found to have accessed targets again using the accounts they used during the initial infiltration, collected credentials, disabled EDR,[7] and distributed the Play ransomware. However, since the Play group officially stated that it does not provide RaaS[8] services, it is unclear whether Andariel joined as an affiliate of the Play group or only played the role of IAB.[9]

Ransomware threats have continued, with two cases of ransomware incidents in South Korea discovered on the dark web and Telegram. The KillSec group released data stolen from a real estate data platform in Korea. The data included personal information, proof of enrollments, and business registration certificates. The CyberVolk group, which operates on Telegram, uploaded a post on the website of a Korean bio lab offering to sell the logs it collected by accessing the admin panel.

---

[3] PoC (Proof of Concept): Code that proves that a particular vulnerability is executable.

[4] CVE-2024-51378: A remote code execution vulnerability that allows attackers to bypass authentication and execute arbitrary commands

[5] Cryptominer: Malware that uses the hardware resources of an infected PC or server to mine cryptocurrency

[6] C2 (Command and Control): A server that maintains communication with infected PCs or servers and performs additional command delivery or malware downloading

[7] EDR (Endpoint Detection and Response): A solution that detects, analyzes, and responds to malicious activity occurring on terminals such as computers, mobile devices, and servers in real time to prevent the spread of damage

[8] RaaS (Ransomware-as-a-Service): A business model that provides ransomware code or the tools needed for attacks in exchange for money

[9] IAB (Initial Access Broker): A threat actor who gains access to networks and systems and then sells them for money

■ News About Ransomware

infosec

NCA releases additional information on Cronos Operation

- NCA reveals identity of LockBit affiliate Beverly, of Evil Corp.
- NCA arrests LockBit developers, BPH service officials and two suspects involved in LockBit activities
- NCA seizes nine servers used by LockBit for criminal infrastructure, including dark web leak sites
- NCA reveals LockBit has retained stolen data after 2022, even if ransom is paid

Ransomware groups exploit Veeam backup solution vulnerability (CVE-2024-40711)

- CVE-2024-40711: Vulnerability that allows remote code execution with untrusted data or malicious payload due to deserialization
- Akira group and Fog group conducted attacks targeting unpatched servers

PSAUX ransomware exploits 0-day vulnerability in web hosting control panel

- Gained root privileges by exploiting remote code execution vulnerability (CVE-2024-51378), encrypted files, and then demanded ransom of $200 (about KRW 280,000)
- Decryption possible because private key was stored in script (.sh) used for encryption

KillSec attacks real estate data platform in Korea

- KillSec posted data release threat on October 5 along with sample data
- Claimed data included personal information, tax-related data, government documents, business registration certificates and more
- Released all data (105 MB) on October 8

CyberVolk attacks bio lab in Korea

- Attacker gained access to lab's website administrator panel
- Posted on Telegram channel that they were selling page logs

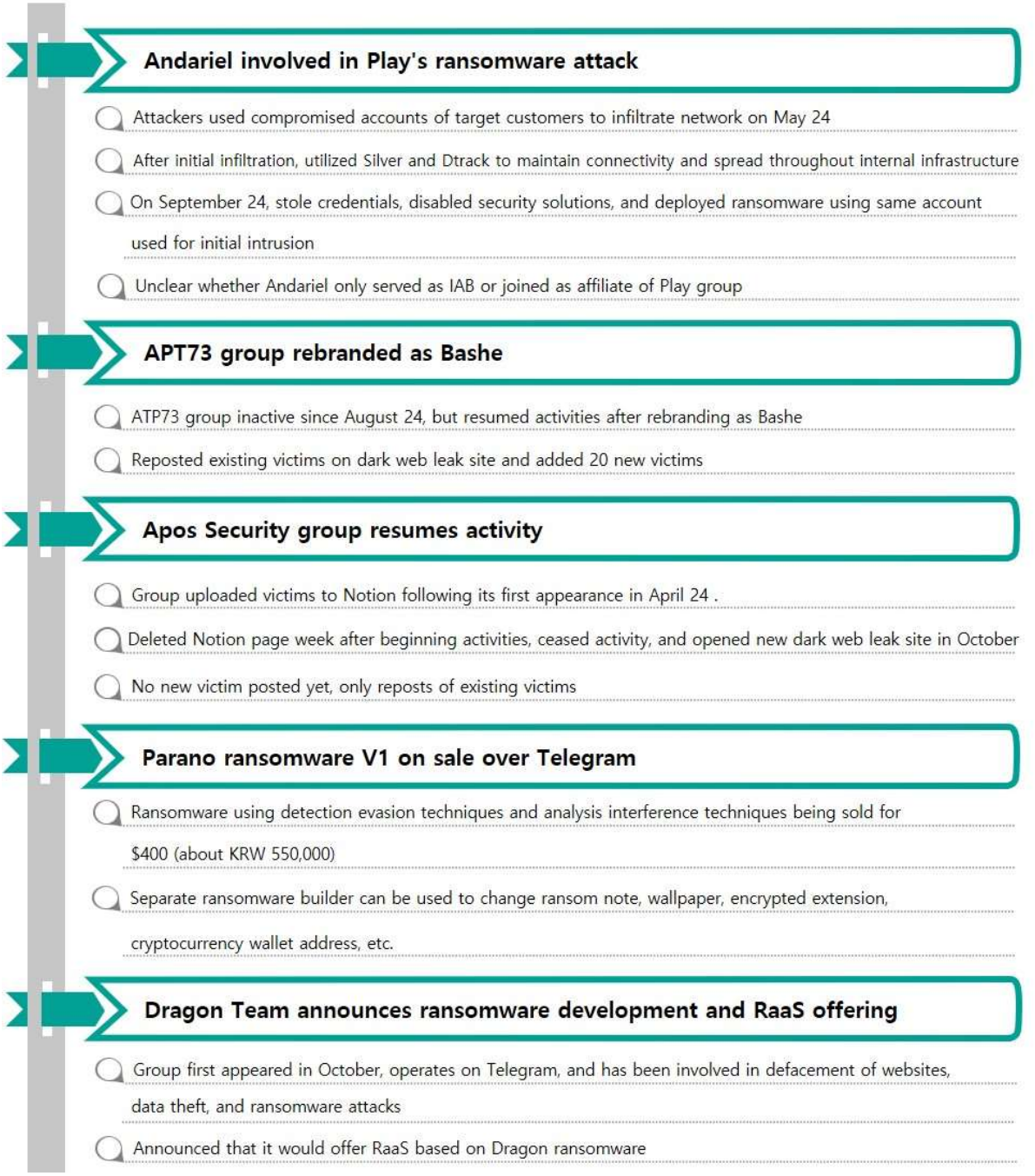


Figure 1. Trends of ransomware

■ Ransomware Threats

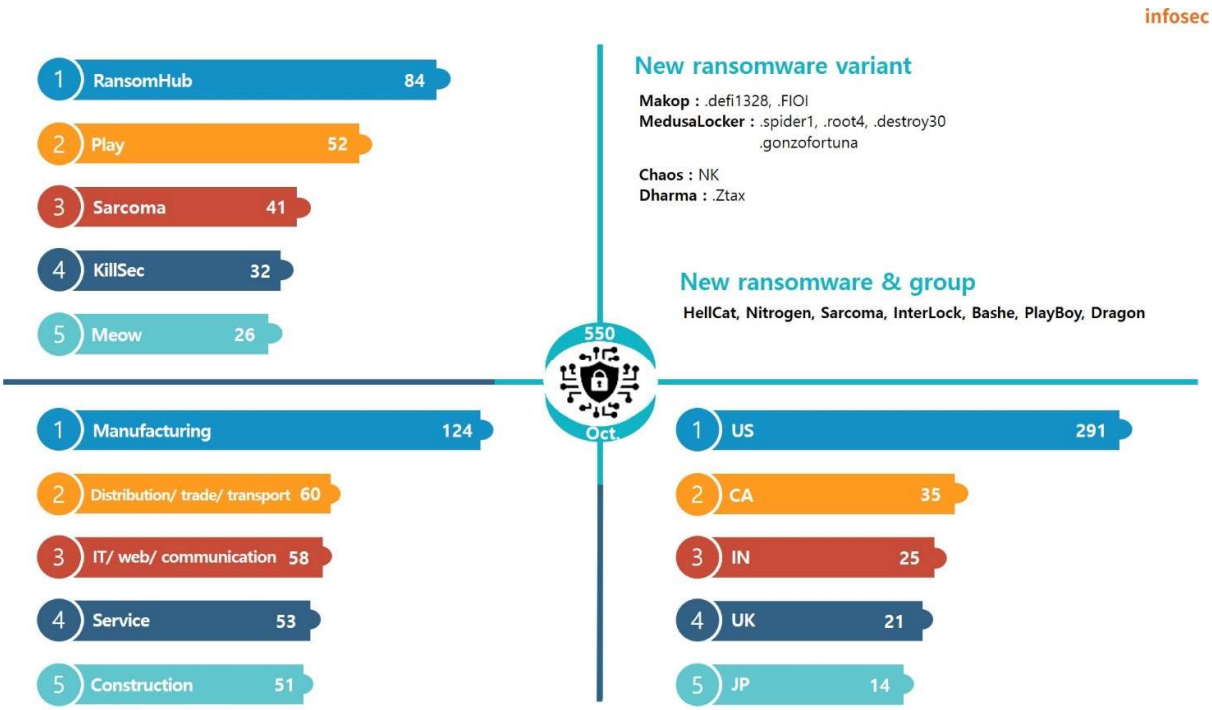


Figure 2. Ransomware threats in October 2024

New threats

In October, several existing ransomware groups rebranded and resumed operations. The Apos Security group appeared in April and posted victims on their Notion page, but after a week of activity, they deleted the posts and disappeared. In October, they opened a new dark web leak site and posted one additional case along with the existing victims. The APT73 group suspended its activities on August 29, then changed its name to Bashe in October and resumed activities by uploading 20 new victims. In addition, the activity of new ransomware groups also increased, with the Nitrogen group posting 11 cases, the Sarcoma group posting 41 cases, the InterLock group posting six cases, the HellCat group posting one case, and the PlayBoy group posting one case.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

On [22/10/2024], HELLCAT was just an idea. Only two days later, we launched our first attack quick, right?

Now, were taking the HELLCAT servers offline for a few days to get ready for whats next. Weve got targets, and were making sure everythings in place.

Wait for us ... #HELLCAT.

-----BEGIN PGP SIGNATURE-----

iHUEARYKAB0WIQQqAxqbiuUi4RkM//sHznxV9M4/gQUCZx42jwAKCRAHznxV9M4/
gU5sAQCACwLfBEnjdmzdg/hE8WDJncY81HLVG9Lk2ZIRGJIJkQD+KKQFElhPoJ+Y
l1iWVw69RH2V5B31bjelts6WmogNdAQ=
=lfkz
-----END PGP SIGNATURE-----
```

Figure 3. HellCat notice

A new ransomware group, the HellCat group, stole about 45 GB of internal documents from the Knesset, Israel's unicameral legislature, and demanded a ransom of $200,000 (about KRW 280 million) on their dark web leak site. They deleted the post about three days later and left a notice that they would disable the server until further activity and return if the next attack was successful.

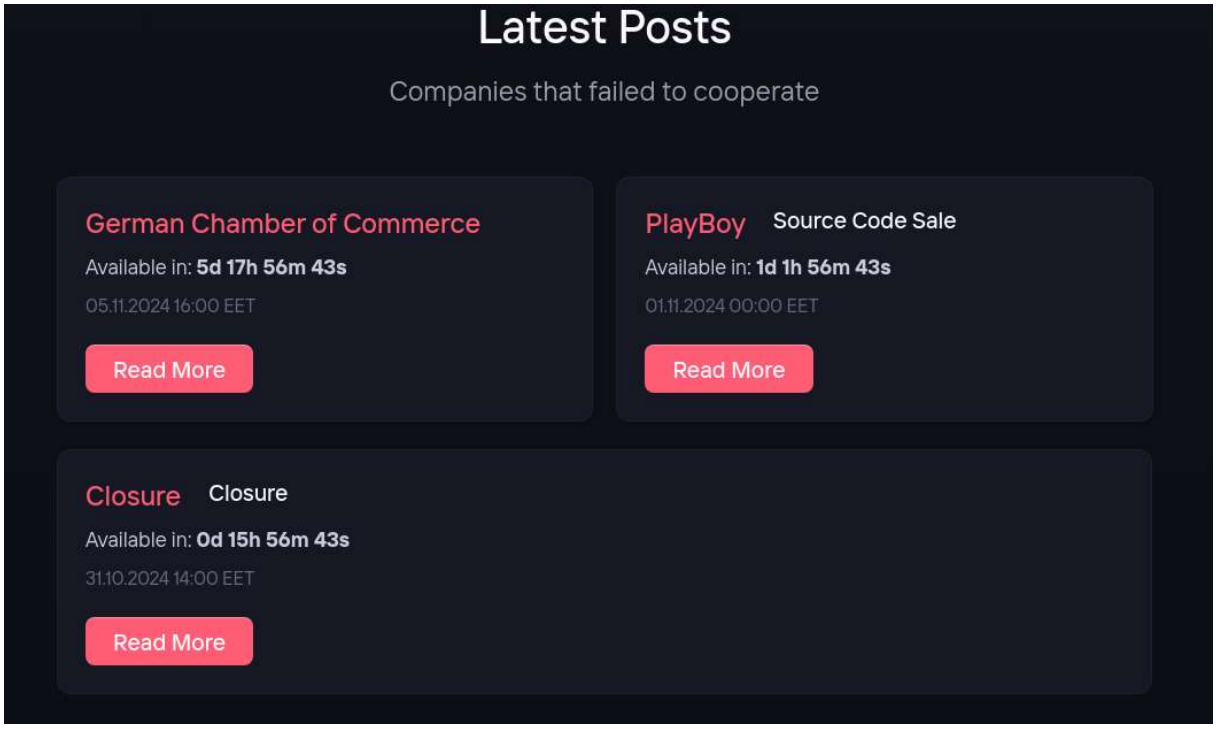


Figure 4. PlayBoy's dark web leak site

Meanwhile, there was a group that ended its activities just two days after its appearance. The PlayBoy group, which first appeared on October 28, attacked the German Chamber of Commerce and demanded $28 million (about KRW 38.6 billion). However, the post did not include stolen sample data, the type of data, or the size of the data. Two days later, they announced the abrupt closure of the site and posted an advertisement for the sale of all infrastructure, including the source code, dark web leak site, and admin panel. Since the 31st, their dark web leak site has been inaccessible.

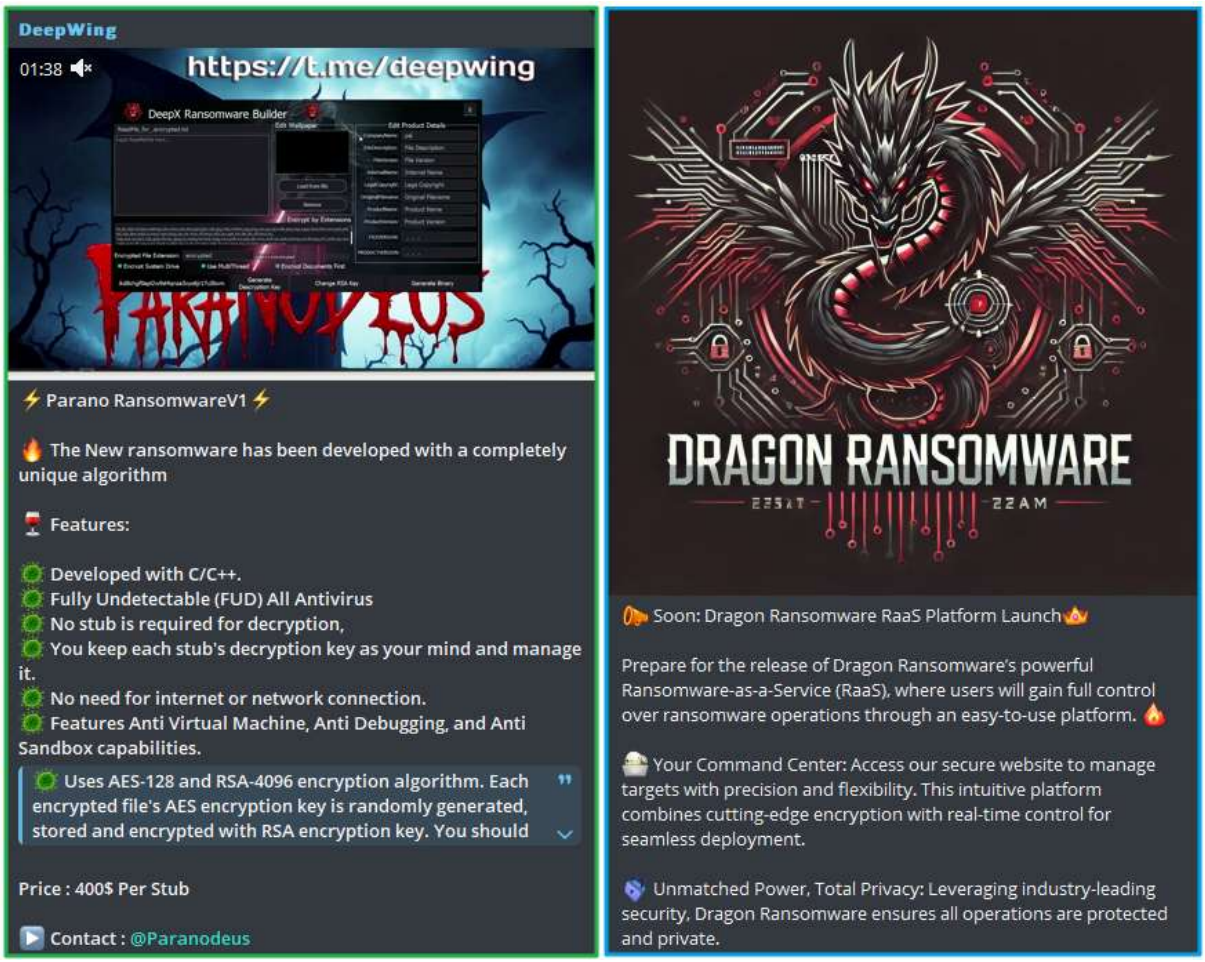


Figure 5. Ransomwares using Telegram (left: Parano Ransomware V1, right: Dragon Ransomware)

Ransomware threats using Telegram also continue to occur. On October 19, a post selling Parano ransomware along with various detection evasion techniques for $400 (about 550,000 won) was uploaded to a channel. A new ransomware group called Dragon operates on Telegram. They sell the data they steal using their ransomware via Telegram, and recently introduced Dragon RaaS, which provides ransomware as a service. Although they do not provide services, yet as only the ransomware has been developed, they announced that they will provide RaaS services that include ransomware and management pages in the future.

Top 5 Ransomwares

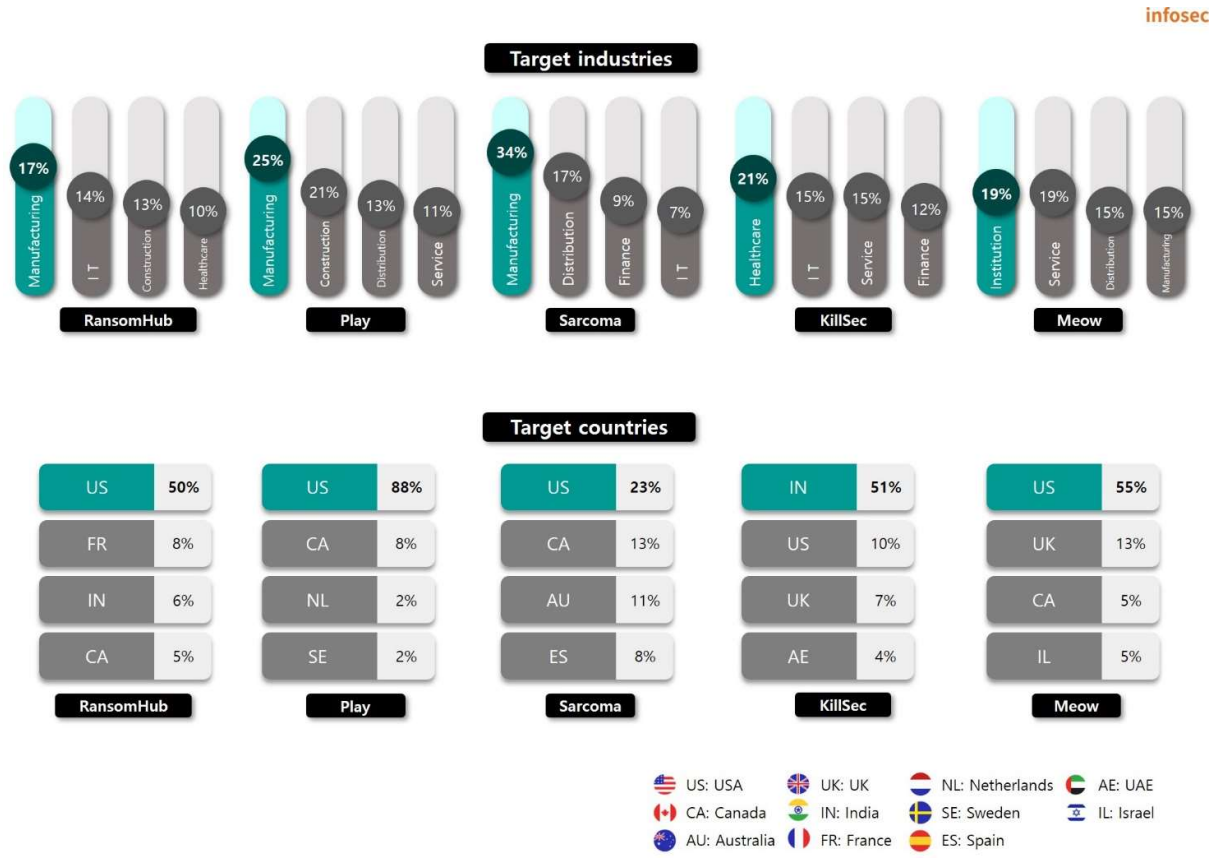


Figure 6. Major ransomware attacks by industry/country

The RansomHub group has established itself as a threat group, posting 84 victims in October alone. They recently attacked Grupo Aeroportuario del Centro Norte (OMA), an airport security agency in parts of Mexico, and stole 3 TB of data, including accounting and investment data, customer personal information, credentials and passwords, and databases. This attack also led to the paralysis of systems at the airports managed by OMA, and caused major disruptions in work such as the malfunction of airport screens.

The Play group attacked OzarksGo, a US broadband service provider, disrupting its services and stealing data including personal information, confidential documents, customer documents, budget information, payrolls and contracts. Due to this attack, OzarksGO has been unable to provide smooth TV services to its customers since October 7. According to an official statement from the company, the service disruption is expected to last for a long time, and the company is implementing measures such as exempting TV service fees and converting existing TV services to streaming services for free. The company is suffering significant losses due to service disruptions caused by the ransomware attack and the costs of follow-up measures.

The Sarcoma group, which emerged in October, posted 41 victims in just one month. They attacked Ferrer & Ojeda, an insurance company for businesses and corporations, and stole

and released 1.27 TB of data containing contracts, personal information of employees, and key database information.

The KillSec group reported 32 victims in October alone, the highest number since they began their activities. They also launched a new dark web leak site, KillSecurity 3.0, with an improved UI. Last October, they attacked a real estate data platform in Korea and stole and released data such as personal information, proof of enrollments, and business registration certificates.

The Meow group attacked Israeli security company Modi'in Ezrachi, a company that provides security and guard services in Israeli-occupied territories and Jewish settlements, protects educational institutions and government facilities under contract with the Israeli government, and operates key checkpoints in the West Bank. The Meow group stole 486 GB of sensitive data from Modi'in Ezrachi, including employee information, government contracts, and security passes.

■ Ransomware Focus

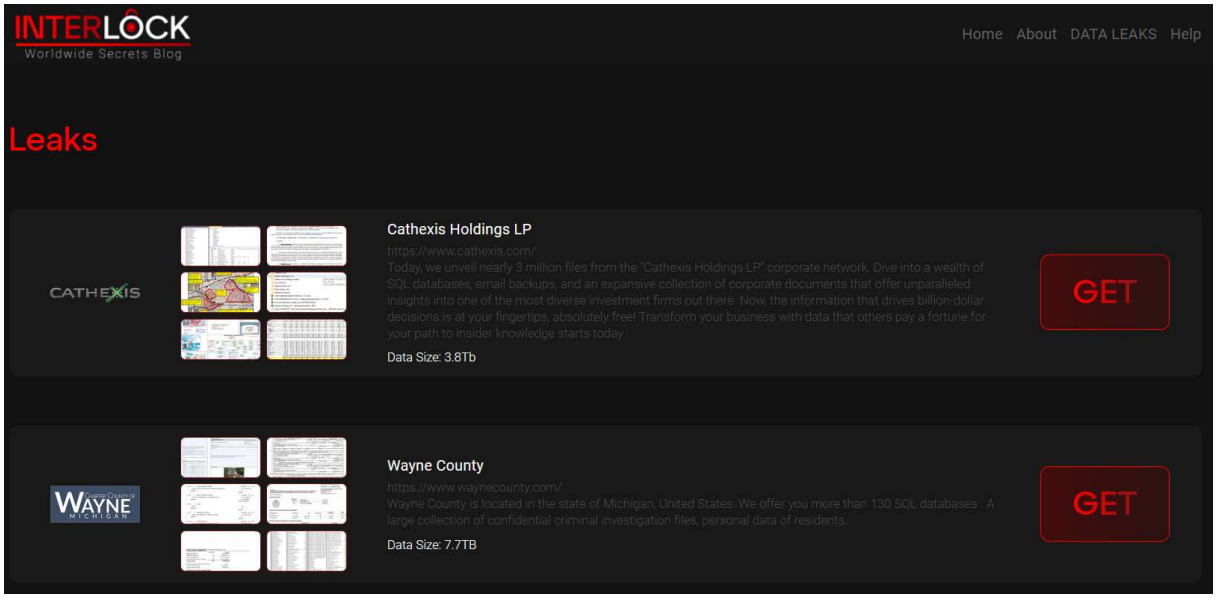


Figure 7. InterLock's dark web leak site

The InterLock group was first discovered on October 9, at which point their dark web leak site had no victims posted, but they started posting victims on the 13th. After an attack, they give victims a total of four days to decrypt their files and prevent the leaked data from being made public. If the victim pays the ransom within this period, the stolen data is destroyed along with the decryption, but if the negotiation period passes or negotiations do not go well, they threaten to destroy the decryption key and sell or disclose the data.

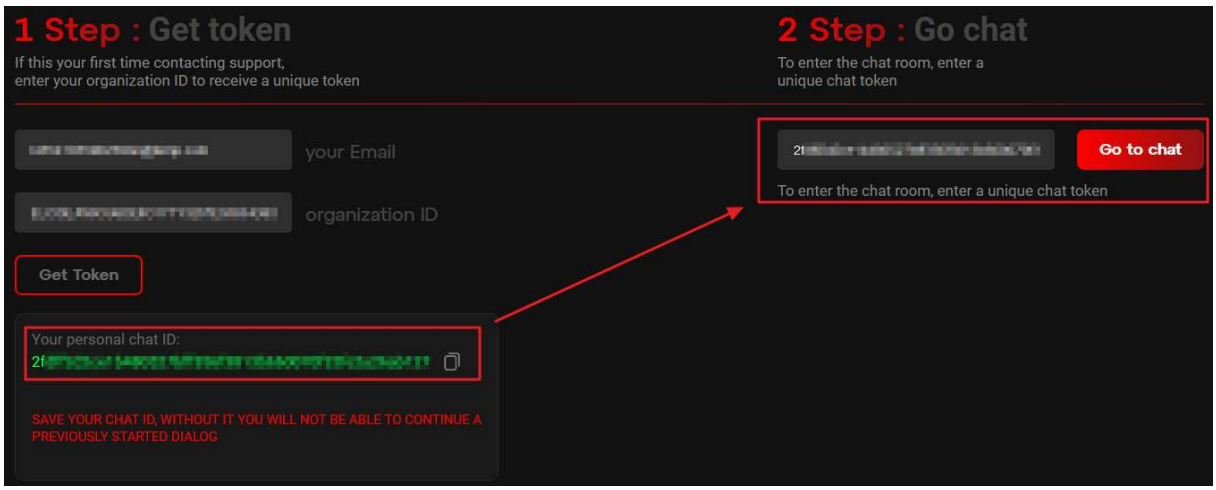


Figure 8. InterLock's dark web negotiation page

The InterLock group uses ransom notes to guide victims to access a chat page. After providing the page address and explaining the access method, they provide the victim with a token that allows them to create a unique chat room by entering the ID and user email address listed in the ransom note. The victim can then negotiate with the attacker in the chat room.

```
initRand();
params(argc, argv);
if ( systemArg )
  return addScheduledTask(argc, argv);
ThreadInit();
if ( pathFile )
  threadStart(&pathFile);
if ( pathDir )
  loopdir(&pathDir);
if ( !pathDir && !pathFile )
  allloop();
sleep(1);
waitThread();
threadFree();
sleep(2);
if ( delArg )
  deleteme();
jEvtClearLog();
return 0;
```

```
initRand();
params(argc, argv);
threadInit();
if ( pathFile )
  threadStart(&pathFile);
if ( pathDir )
  loopdir(&pathDir);
if ( !pathDir && !pathFile )
  allLoop();
sleep(1u);
waitThread();
threadFree();
sleep(2u);
if ( (del & 1) != 0 )
  removeme(*argv);
return 0;
```

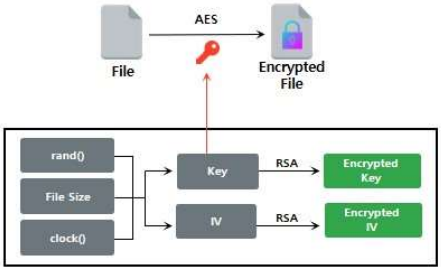
Figure 9. Comparison of InterLock ransomware code (left: Windows, right: Linux)

The InterLock ransomware exists in two versions: Windows and Linux. The two versions operate almost identically in terms of checking parameters and encrypting files based on multithreading. However, reflecting OS differences, there are differences between the two versions for some modules, functions, exception directories, and files. There are also other functional differences. For example, in the Windows version, the attacker registers the ransomware in the task scheduler and deletes the event log after encrypting the files. Therefore, this report analyzes the similarities and differences between the two versions and discusses in detail how they work on each operating system.

InterLock Ransomware

Encryption key

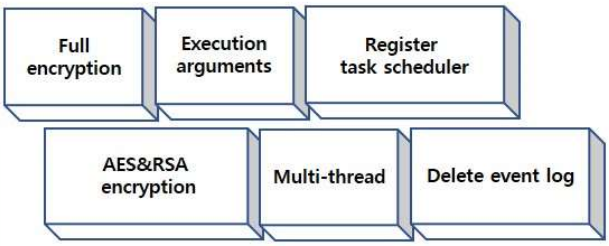
Encrypt files with the AES algorithm and protect the keys and IV with the RSA algorithm



Encryption method

Encrypt the entire file after padding in 1 MB block units

Characteristics



Ransom note

!_README_!.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

INTERLOCK - CRITICAL SECURITY ALERT

To Whom It May Concern,
Your organization has experienced a serious security breach. Immediate action is required to mitigate further risks.

THE CURRENT SITUATION
- Your systems have been infiltrated by unauthorized entities.
- Key files have been encrypted and are now inaccessible to you.
- Sensitive data has been extracted and is in our possession.

WHAT YOU NEED TO DO NOW
1. Contact us via our secure, anonymous platform listed below.
2. Follow all instructions to recover your encrypted data.

Access Point: http://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid.onion/support/step.php
Use your unique Company ID: [redacted]

DO NOT ATTEMPT:
- File alterations: Renaming, moving, or tampering with files will lead to irreversible damage.
- Third-party software: Using any recovery tools will corrupt the encryption keys, making recovery impossible.
- Reboots or shutdowns: System restarts may cause key damage. Proceed at your own risk.

!_README_!.txt

Change extension

.interlock

Production language

C/C++

Figure 10. Overview of the InterLock ransomware

Strategy of the InterLock ransomware

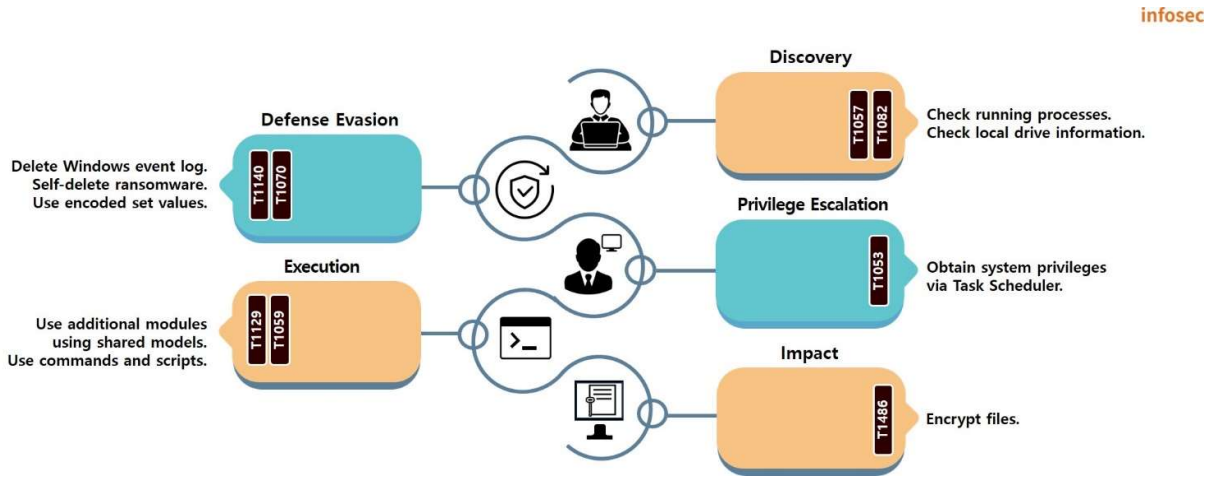


Figure 11. Attack strategy of the InterLock ransomware

The Linux version of the ransomware immediately checks the execution arguments, while the Windows version recovers the executable original code and then executes it (code patching technique). Therefore, the Windows version prioritizes the process of restoring the original code.

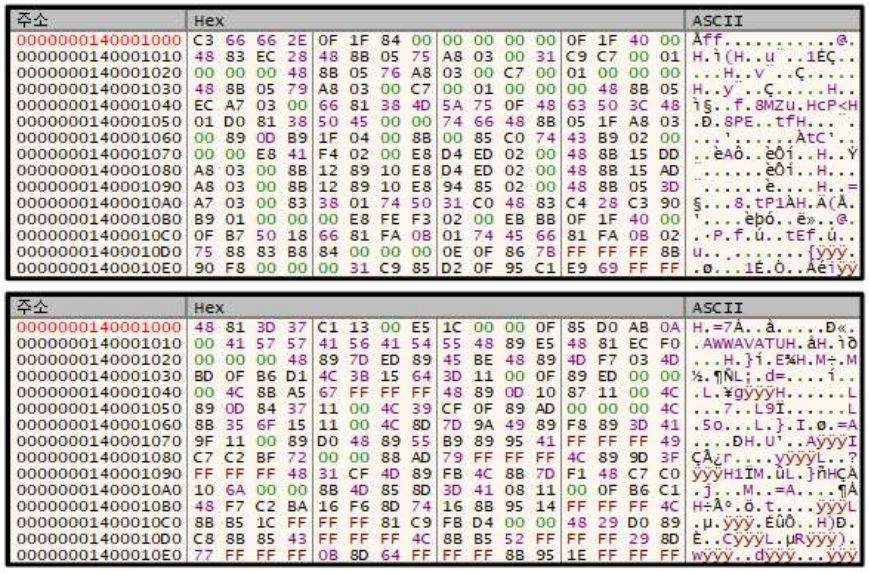


Figure 12. Comparison of memory before and after the code patch (Top: Before the code patch, Bottom: After the code patch)

If you check the identical part in the area where the executing code is stored, you can find that the data stored after the code patch, that is, the code, has changed. The Windows version of the InterLock ransomware uses a technique in which it recovers and then executes the original executable code to avoid detection by security programs such as vaccines.

Both the Windows version and the Linux version check the execution arguments first, and then decide whether to perform a specific action. Both versions check the same four types of argument. There are arguments that encrypt specified directories or files only, and arguments that delete the ransomware files themselves after execution. For the "-s" argument, both versions check for input. However, the Linux version only checks and does not add or remove features, while the Windows version adds the ability to register ransomware in the scheduler. The table below shows the execution arguments and their functions.

Argument	Description
--directory [target]	Encrypt the specified directories only
--file [target]	Encrypt the specified files only
--delete	Self-delete after file encryption
--system	Register Task Scheduler and increase privileges (Windows)

Table 1. Execution arguments

The Windows version uses a total of four task scheduler commands. First, to register the task, it deletes the existing task and removes the --system argument from the ransomware execution command. It registers a task to run the command at 20:00 every day with arguments removed and with system privileges, and then runs the task immediately and deletes it. Task Scheduler is usually used to secure persistence or to escalate privileges. The InterLock ransomware is believed to have used Task Scheduler to escalate privileges, as it immediately deletes tasks after executing them with system privileges. The table below lists the commands used and descriptions.

Command	Description
schtasks /delete /tn TaskSystem /f > nul	Delete current task
schtasks /create /sc DAILY /tn "TaskSystem" /tr "cmd /C cd {path} && {execute_command}" /st 20:00 /ru system > nul	Register ransomware task (system privilege)
schtasks /run /tn TaskSystem > nul	Execute TaskSystem task
schtasks /delete /tn TaskSystem /f > nul	Delete TaskSystem task

Table 2. Task scheduler commands

Next, the ransomware sets the encryption target based on the input arguments and encrypts the files based on multi-threads. Both versions encrypt only the file in question when using the --file argument, and all files in the directory and its subdirectories when using the --directory argument. If neither argument is used, the ransomware will encrypt everything starting from the top directory (in the case of Windows, it will encrypt from the top directory of the C drive, and in the case of Linux, from the root directory).

```
if ( pathFile )
  threadStart(&pathFile);       // crypt target file
if ( pathDir )
  loopdir(&pathDir);            // crypt target dir
if ( !pathDir && !pathFile )
  allloop();                    // loop 'C:/'
```

```
if ( pathFile )
  threadStart(&pathFile);    // crypt target file
if ( pathDir )
  loopdir(&pathDir);         // loop target dir
if ( !pathDir && !pathFile
  allLoop();                 // loop root('/') dir
```

Figure 13. Setting the encryption target according to the execution arguments (left: Windows, right: Linux)

If the --directory argument is used to encrypt a specific directory, or if all directories from the top directory are encrypted by using neither the --directory nor --file argument, the ransomware identifies all files and directories in the directory. If it is a file, the ransomware calls an encryption thread to encrypt it; if it is a directory, it creates a ransom note and recursively searches inside the directory.

```
if ( (buf.st_ino & 0xF000) == 0x4000 )  // check directory
{
  if ( entry[8] == '.' && !entry[9]
    || entry[8] == '.' && entry[9] == '.' && !entry[10]// pass "." , ".." dir
    || (checkExceptDir((entry + 8)) & 1) != 0 )// pass exceptDir
  {
    file[buf.__unused[0]] = 0;
  }
  else
  {
    v2 = strlen(entry + 8);
    buf.__unused[0] += (v2 + 1);
    ++buf.__unused[1];
    *(buf.__unused[2] + 4 * buf.__unused[1]) = v2;
    v1 = opendir(file);                 // recursive opendir
```

Figure 14. Directory verification and recursive search

This does not search all directories, and does not encrypt exempted directories. The table below lists the directories that are exempt from encryption by version.

Windows	Linux
.(Current folder), ..(Parent folder), $Recyble.Bin, Boot, Documents and Settings, PerfLogs, ProgramData, Recovery, System Volume Information, Windows, AppData, WindowsApps, Windows Defender, WindowsPowerShell, Windows Defender Advanced Threat Protection	.(Current folder), ..(Parent folder), bin, boot, cdrom, dev, etc, home, lib, lib32, lib64, libx32, lost+found, media, mnt, opt, proc, run, root, sbin, snap, srv, sys, tmp, usr, var

Table 3. Directories exempt from encryption

If the identified object is a file, the ransomware decides whether to encrypt the file based on a separate list of exceptions. The table below lists the files and extensions that are exempt from encryption by version.

Windows	Linux
!__README__!.txt, .bat, .bin, .cab, .cmd, .com, .cur, .diagcab, .diagcfg, .diagpkg, .drv, .hlp, .hta, .ico, .msi, .ocx, .psm1,.scr, .sys, .ini, .url, .dll, .exe, .ps1	!__README__!.txt, . boot.cfg, .sf, .b00, .v00, .v01, .v02, .v03, .v04, .v05, .v06, .v07, t00

Table 4. Files and extensions exempt from encryption

First, whether the .interlock extension exists in the file name is checked to determine whether it is encrypted. If the file is not encrypted, the .interlock extension is added to the file name. A random AES key and initialization vector (IV) are generated based on the system time. The AES key and IV generated in this way are used to encrypt the file, which is encrypted using a hard-coded RSA public key and then save at the end of the original file.

```
if ( !checkFileExt(target_file, ".interlock") )
{
  strcat(strcpy(encrypted_fileName, target_file), ".interlock");
  if ( !rename(target_file, encrypted_fileName) )
  {
    Stream = fopen(encrypted_fileName, "rb+");
    if ( Stream )
    {
      file_size = fsize(Stream);
      key_len = 48;
      key_IV = malloc(0x40ui64);
      generateKey(key_IV, file_size, key_len);// generate random key(32Bytes) & IV(16Bytes)
      file_size = addPaddingFile(Stream, file_size);
      *&ElementCount[1] = malloc(0x500ui64);
      *&ElementCount[1] = rsaCrypt(key_IV, key_len, *&ElementCount[1], ElementCount);// encrypt aes key & IV via RSA
```

Figure 15. Checking the encryption status and generating an encryption key

The ransomware uses the AES algorithm and encrypts files in CBC mode using the generated key and IV. It encrypts the entire file in blocks of 1 MB.

```
v5 = find_cipher("aes");
if ( cbc_start(v5, a3, a2, 32, 0, v9) )
{
  free(Block);
  free(v9);
  free(Buffer);
}
else
{
  while ( v17 > 0 )
  {
    v6 = v17;
    if ( v17 > ElementCount )
      v6 = ElementCount;
    v8 = fread(Block, 1ui64, v6, a1);
    if ( cbc_setiv(a3, 0x10ui64) || cbc_encrypt(Block, Buffer, v8, v9) )
      break;
    adjustFilePosition(a1, -v8, 1);
    fwrite(Buffer, 1ui64, v8, a1);
```

Figure 16. File encryption

--If the del argument is used, the ransomware will perform a self-delete function to erase any traces after file encryption is complete. The Linux version uses the rmdir command to delete a specific path to remove the ransomware, while the Windows version first creates a DLL file that deletes the ransomware files and then uses this to perform self-delete.

```
if ( !GetModuleFileNameA(0i64, ransomware, 0x104u) )
  return 0i64;
rand_num = rand();
tmp_path = getenv("tmp");
formatString2(self_deletefile, "%s/tmp%d.wasd", tmp_path, rand_num);
Stream = fopen(self_deletefile, "wb");        // create "%tmp%/tmp{rand_num}.wasd"
if ( !Stream )
  return 0i64;
fwrite(&data, 1ui64, 0xA00ui64, Stream);
fclose(Stream);
formatString2(v4, "rundll32.exe %s,run %s", self_deletefile, ransomware);
return create_process(v4);
```

Figure 17. Create DLL for self-deletion (Windows)

DLL files are hard-coded in ransomware and are stored in a temporary folder. The saved DLL file is a simple file that only contains the function of deleting the file in the path passed as an argument using the remove API. The Windows version uses the DLL file to remove the ransomware.

```
int __fastcall run(__int64 a1, __int64 a2, const char *a3)
{
  return remove(a3);
}
```

Figure 18. tmp.wasd function

In addition, the Windows version has a function to delete the event log. It uses the API to delete all four items: Application, Security, System, and Forwarded Events.

```
EvtClearLog(0i64, L"Application", 0i64, 0);
EvtClearLog(0i64, L"Security", 0i64, 0);
EvtClearLog(0i64, "S", 0i64, 0);
EvtClearLog(0i64, &system, 0i64, 0);
return EvtClearLog(0i64, L"Forwarded Events", 0i64, 0);
```

Figure 19. Deleting event logs

Countermeasures against the InterLock ransomware

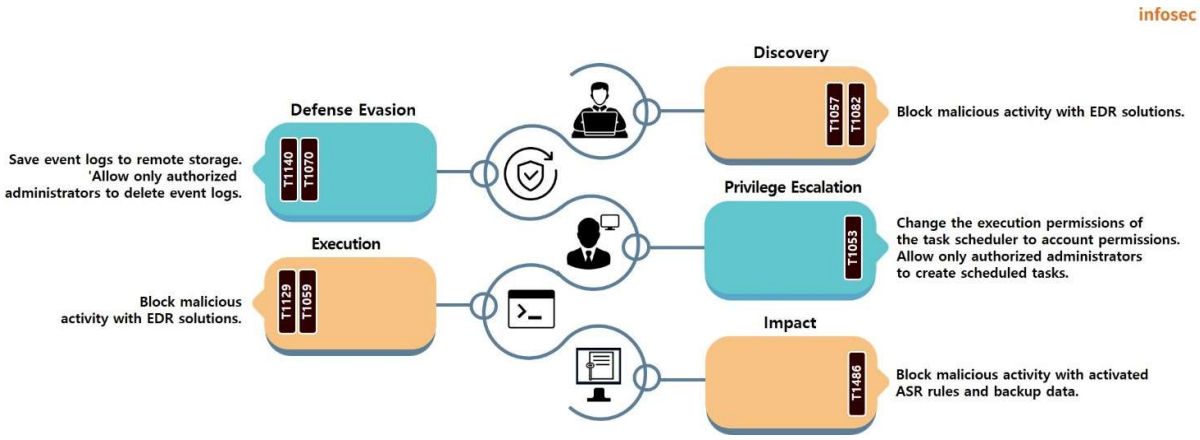


Figure 20. Measures against the InterLock ransomware

Because the Windows version of the InterLock ransomware uses a code patching technique to restore the executable original code, it may not be detected by solutions such as anti-virus programs. However, it is possible to block threats using an EDR solution that identifies and blocks malicious activities based on behavior. Attackers also delete event logs to make it difficult to analyze breach incidents, but it's possible to prevent them from being deleted by storing the event logs remotely or setting them to only allow deletion by authorized administrators.

The Windows version attempts to acquire system privileges using Task Scheduler. Therefore, it is important to take steps to ensure that processes run through Task Scheduler run with the privileges of the account that created the task and not with system privileges, or to prevent tasks from being registered by users who do not have administrator privileges.

You can enable ASR[10] rules to prevent file encryption as well as the creation of processes for self-deleting, or use an EDR solution to block specific processes used by attackers to prevent malicious activity. The InterLock ransomware only has a file encryption function and does not delete backup copies separately, so it is possible to recover some files through system backups created by Windows' default function. Damage can also be minimized by backing up important data to multiple networks or storages.

The Linux version only encrypts files after traversing the file system, and deletes itself after encryption. Therefore, damage can be minimized by granting the user account minimal file and folder handling permissions so that ransomware cannot encrypt important files even if it is executed. An EDR solution can also be used to block the execution of malicious processes or an application whitelist can be set up to allow only pre-approved programs to run. Distributing data across multiple networks or storage locations will minimize damage.

[10] ASR (Attack Surface Reduction): Protection against specific processes used by attackers and executable processes

Indicator Of Compromise

InterLock(Windows)

a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642

InterLock(Linux)

e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1

28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f

File Name(Windows)

FiMatrix**e(Linux)**

Start

■ Reference sites

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/massive-psaux-ransomware-attack-targets-22-000-cyberpanel-instances/)

• SOCRadar's official website (https://socradar.io/over-22000-cyberpanel-servers-at-risk-from-critical-vulnerabilities-exploitation-by-psaux-ransomware/)

• GitHub (https://gist.github.com/gboddin/d78823245b518edd54bfc2301c5f8882)

• NIST vulnerabilities database (https://nvd.nist.gov/vuln/detail/CVE-2024-51378)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/north-korean-govt-hackers-linked-to-play-ransomware-attack/)

• OzarksGo's official website (https://www.ozarksgo.net/tv-outage-update)

• Unit42's official blog (https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/)