Keeping Up with Ransomware

Emergence of Lynx ransomware and analysis of connectivity with INC Group

■ Overview

The number of cases of damage caused by ransomware in August 2024 was 464, which is an increase of approximately 12% compared to July (415 cases). This month, not only the total number of cases but also the number of domestic cases have increased slightly.

On August 15, IntelBroker, a member of the hacker group CyberNiggers, posted on the hacker community BreachForums that they were selling the database of CareerNet, a Korean job information site. IntelBroker claims that they stole about 1.6 million user IDs, passwords, email addresses and other pieces of personal information. On August 23, CareerNet acknowledged and announced the leak of personal information held by the company. CareerNet claimed that the leaked data was created before April 2018, and that aside from IDs, key information such as names and passwords were encrypted and could not be decrypted.

IntelBroker additionally disclosed domestic data. On August 24, they posted Ministry of National Defense data on BreachForums, claiming that the South Korean government had attempted to interfere with CareerNet DB postings. The information posted was related to the country's disaster and safety communication network. IntelBroker presented screenshots of the administrator dashboard as evidence and claimed that they had replaced the voice file for alerts. In addition, they posted that they were selling the membership information of four million customers and trainers of a domestic personal trainer platform, and membership information of Toping, a domestic reading and learning management system (LMS[1]) platform company.

There have been cases of damage to Korean companies from the dark web leak sites of ransomware groups. On August 11, Hunters Group posted an article saying it was selling data from Hanon Systems, a Korean automotive thermal management solution provider. On August 14, they released all 2.3 TB of data, which included personal information and internal confidential data such as employee information, resumes and financial statements. Hanon

[1] LMS (Learning Management System): An online system that supports and manages the learning of users

Systems has already suffered two ransomware breaches in the past, from Snatch (January 2022) and Egregor (November 2020), so this incident shows the importance of taking appropriate measures after an incident occurs.

On August 23, the Eldorado ransomware group claimed to have attacked DevOps, a professional consulting firm in Korea. According to dark web posts, they are offering a sample list of files containing source codes, which they are selling for 1.5 BTC (approximately KRW 120 million).

The Dispossessor group, which has been active since last year, has been repeatedly posting ransomware data, but had its main infrastructure seized in August. On August 13, the US Federal Bureau of Investigation (FBI), the US Department of Justice (DoJ), the German State Criminal Police (Landeskriminalamt, LKA), the UK's National Crime Agency (NCA), and the Bamberg Public Prosecutor's Office in Germany seized Dispossessor's data leak site and the servers used in its attacks. The seized assets included three servers in the United States, three servers in the United Kingdom, eighteen servers in Germany, eight domains based in the United States and one domain based in Germany.

One ransomware attack discovered in August exploited a vulnerability in Jenkins, an automation tool that provides deployment and integration services during software development. This vulnerability is a problem in the command processing phase that was patched in January 2024. It allows attackers to read files on the internal system. The Jenkins vulnerability has been actively exploited since March, and was used by the RansomEXX group in July when they attacked Brontoo Technology Solutions, a provider of technology services to Indian banks. It was also found that IntelBroker had exploited it in August when it attacked IT service provider BORN Group.

Lynx ransomware, which first appeared at the end of July, was found to be using a source code bought from INC Ransom. INC Ransom posted on a dark web forum in May this year that it was selling its ransomware source code for $300,000 (approx. KRW 400 million). According to our analysis, the Lynx ransomware is functionally nearly identical to the INC ransomware, and a comparison using the binary analysis program BinDiff showed approximately 45% code similarity between the two.

■ Ransomware news

infosec

DB of Korean job information site CareerNet sold through hacking forum site

- On August 15, IntelBroker posted on BreachForums that they were selling CareerNet's DB.
- Approximately 1.6 million pieces of data were being sold in total, and according to the sample data released, it is presumed to be member information such as IDs, PWs, and email addresses.

IntelBroker releases Ministry of National Defense data

- IntelBroker released Ministry of National Defense data on August 23 in retaliation for the South Korean government's alleged interference in an August 15 upload of an advertisement for the sale of CareerNet DB.
- Based on the released samples and images, this is presumed to be data related to the disaster and safety communication network.
- They released screenshots of the logged-in admin panel and arbitrarily altered the alarm voice file.

Hacking forum BreachForums replaces admin

- ShinyHunters has been in control of the forums since the FBI and US DOJ seized the BreachForums systems in May 2024.
- On August 22, the owner of BreachForums was changed from ShinyHunters to IntelBroker.

LockBit ransomware group releases contact information on dark web leak site

- Recruiting through the hacking forum BreachForums.
- They listed "white and racist" as qualifications for membership and required evidence of an actual attack, such as a free release of leaked data.

Dispossessor ransomware group has attack assets seized

- On August 13, major assets were seized by the FBI, DOJ, LKA, NCA and the Bamberg Public Prosecutor's Office in Germany.
- The seized assets included three servers in the US, three servers in the UK, eighteen servers in Germany, eight domains based in the US and one domain based in Germany.
- The FBI has asked victims to share information about the Dispossessor group through its Internet Crime Reporting Hotline or by phone.

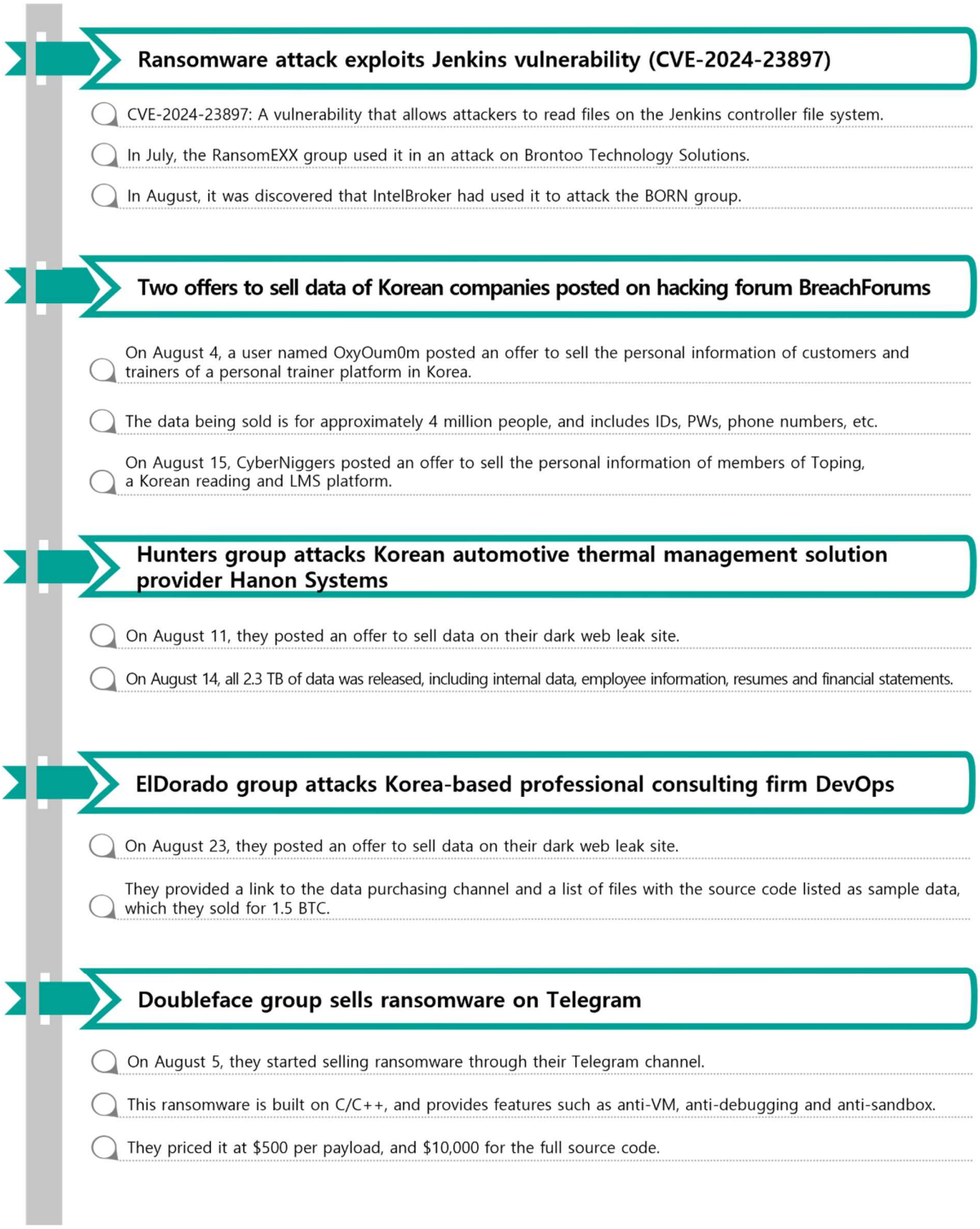

Ransomware attack exploits Jenkins vulnerability (CVE-2024-23897)
CVE-2024-23897: A vulnerability that allows attackers to read files on the Jenkins controller file system.
In July, the RansomEXX group used it in an attack on Brontoo Technology Solutions.
In August, it was discovered that IntelBroker had used it to attack the BORN group.
Two offers to sell data of Korean companies posted on hacking forum BreachForums
On August 4, a user named OxyOum0m posted an offer to sell the personal information of customers and trainers of a personal trainer platform in Korea.
The data being sold is for approximately 4 million people, and includes IDs, PWs, phone numbers, etc.
On August 15, CyberNiggers posted an offer to sell the personal information of members of Toping, a Korean reading and LMS platform.
Hunters group attacks Korean automotive thermal management solution provider Hanon Systems
On August 11, they posted an offer to sell data on their dark web leak site.
On August 14, all 2.3 TB of data was released, including internal data, employee information, resumes and financial statements.
ElDorado group attacks Korea-based professional consulting firm DevOps
On August 23, they posted an offer to sell data on their dark web leak site.
They provided a link to the data purchasing channel and a list of files with the source code listed as sample data, which they sold for 1.5 BTC.
Doubleface group sells ransomware on Telegram
On August 5, they started selling ransomware through their Telegram channel.
This ransomware is built on C/C++, and provides features such as anti-VM, anti-debugging and anti-sandbox.
They priced it at $500 per payload, and $10,000 for the full source code.

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

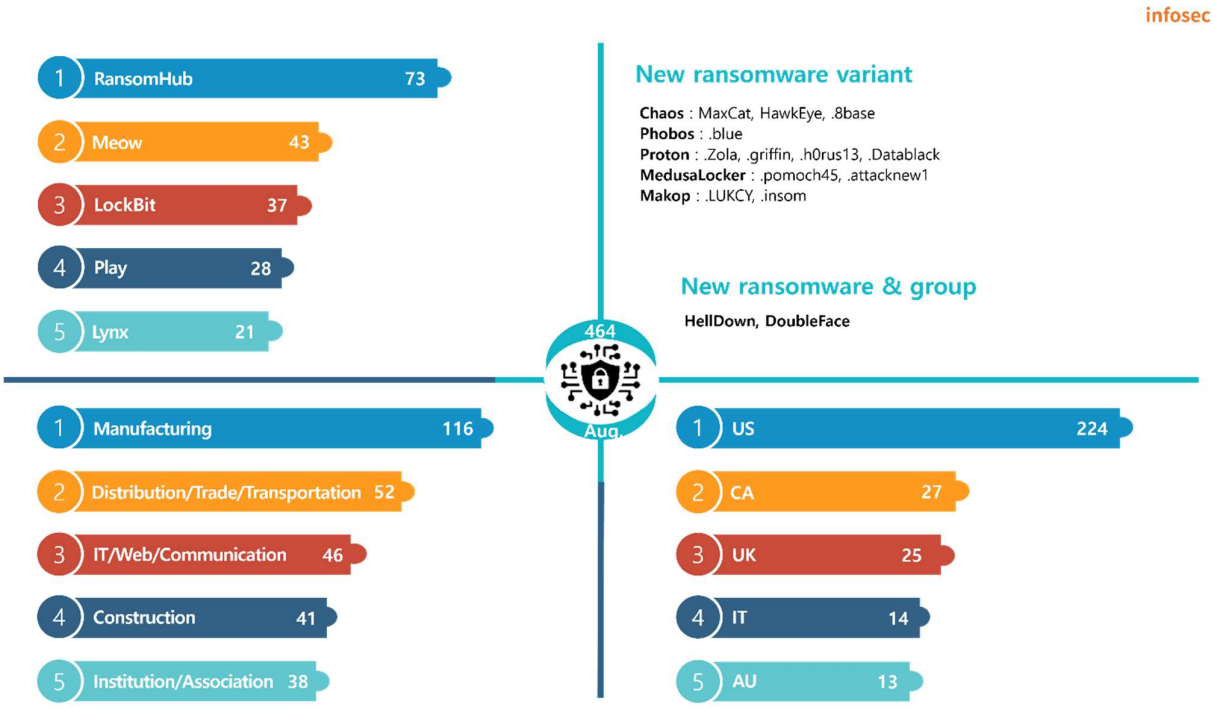


그림 2. 2024 년 8 월 랜섬웨어 위협 현황

Figure 2. Ransomware threats as of August 2024

New threats

A total of two new cyber threats were discovered in August, which is a significant decrease from the previous month. The HellDown ransomware group, which emerged on August 13, set up a data leak site on the dark web, revealing nine victims on the first day alone. Over the next 10 days, they added 8 more victims, for a total of 17 victims reported since they started their activities. Among the victims was Zyxel Networks, a Taiwan-based global networking and security solutions provider. HellDown claimed to have stolen 253 GB of the company's internal data, including pay slips and financial statements. Since August 24th, however, their dark web leak site has remained inaccessible.

Meanwhile, the Doubleface group opened a Telegram channel on August 5 and is using this channel as its main means of activity. The group is also active on X (formerly Twitter) and has revealed in a Telegram message that they are a group of hackers whose goal is to obtain money. In their X introduction, they refer to themselves as the Russian hacker group APT66. They announced that they are carrying out not only ransomware attacks but also numerous website defacement attacks, and that they are affiliated with attack groups such as HexaLocker, RansomHub, God Team and LETGH0STsp. However, the post about the partnership with RansomHub has now been deleted.

Figure 3. Doubleface ransomware

On the day the Telegram channel was launched, the Doubleface group posted a ransomware sales offer in which they advertised that the ransomware encrypts files using AES and RSA algorithms and provides anti-VM, anti-debugging and anti-sandbox features. According to the ransomware demonstration video, it not only encrypts files, but also provides a function to control the screen by forcibly fixing the decryption key input window. However, since this ransomware attempts to decrypt without verifying the authenticity of the decryption key, there is a risk of permanently damaging files if the wrong key is entered. The price of the ransomware payload is $500 (approx. KRW 670,000) per unit, and the price of the entire source code is $10,000 (approx. KRW 13.4 million).

Top 5 ransomware groups

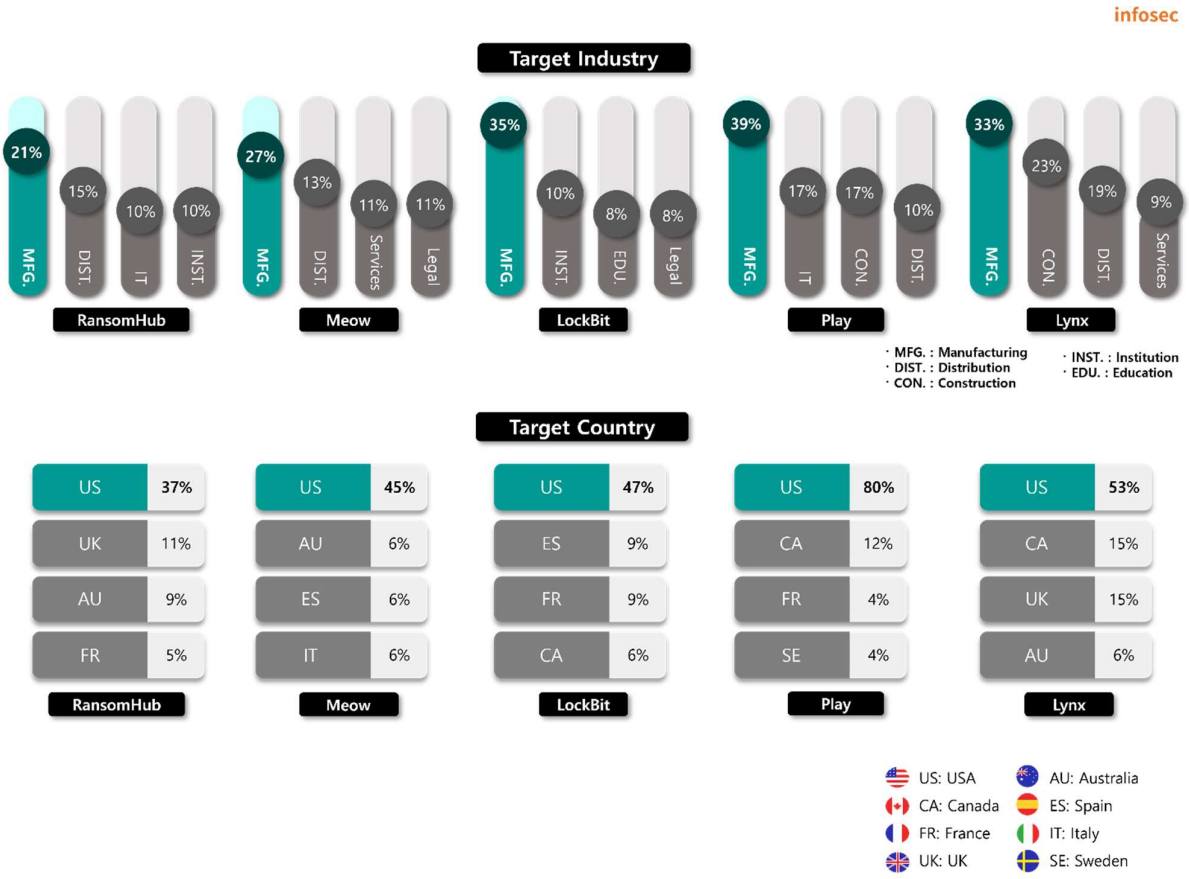


Figure 4. Major ransomware attacks by industry/country

The RansomHub ransomware group posted 48 victims in July alone, and then 73 in August, an increase of 25. Notably, in August, they were found to have used EDRKillShifter, a malicious tool that disables endpoint detection and response (EDR) solutions. This tool requires a specific key value to decrypt the encrypted resources, and disables the protection of EDR solutions with the bring your own vulnerable driver (BYOVD) technique that exploits vulnerabilities in legitimate drivers. The malware tool is sold on the dark web, so other attacker groups may also exploit it. Since the BYOVD technique ensures that attacks occur through trusted drivers, appropriate responses such as EDR solutions and permission management are needed. A more detailed analysis of the RansomHub group can be found in the 2nd Quarter KARA Ransomware Trends Report.

The Meow ransomware was built based on the leaked source code of the Conti v2 ransomware. Since launching their dark web leak site in 2023, the group has been posting less than 10 victims per month. The number of victims began to increase in July 2024, and in August, the group exploded with activity, posting 43 victims, which represents 51% of its total victims. The group reportedly attacked Zydus Pharmaceuticals, a global pharmaceutical company with branches in 50 countries, in August and stole 20 GB of data, including financial documents, customer information and research data.

The LockBit ransomware group posted around 90 victims on a dark web leak site on August 11 and 12, most of whom had previously been posted between 2022 and 2024. There were only 15 new victims. The group then became less active, posting only two more victims before posting another 11 on August 30.

The Play ransomware primarily targets US-based companies. In August, the group claimed they had attacked U.S. semiconductor manufacturer Microchip Technology and stolen confidential internal data, personal information, budgets, and payroll and accounting data. The group released some confidential documents, customer information and accounting information, and warned that they would release all the data if no further action were taken.

Lynx, a new ransomware group that appeared in July, continued to post victims in August, with the fifth highest number. The group claimed they had attacked asset management firm Pyle Group and stolen sensitive corporate information, and released the data well after the originally announced release date. On August 15, the Pyle Group was also listed as a victim on the Medusa ransomware group's dark web leak site. The Medusa group announced that the data was available via TOX Chat.

■ Ransomware focus

Overview of the Lynx ransomware

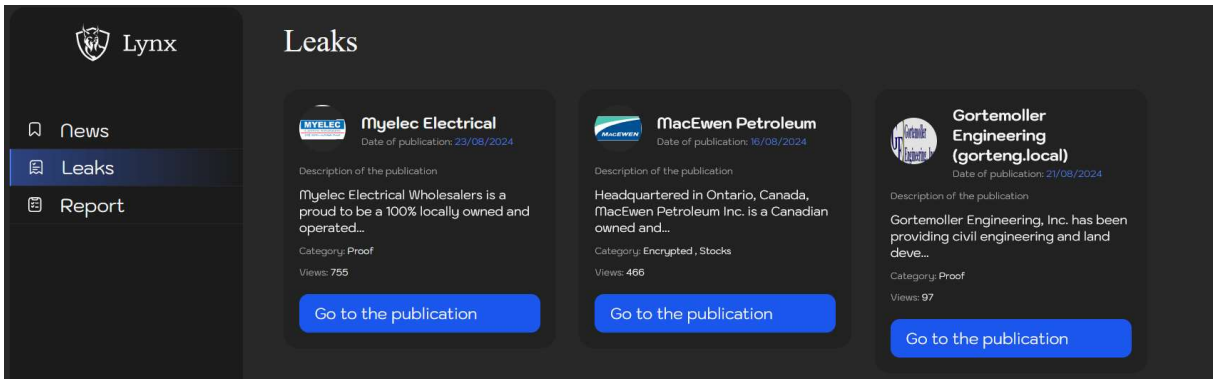


Figure 5. Data leak site for Lynx ransomware

The Lynx ransomware first began to draw attention on July 29 when its leak site was discovered. At the time, there were already two posts dating back to July 17, and both dark web-based sites and clearnet sites were discovered. Currently, only the clearnet site is accessible. In an introduction uploaded to a dark web leak site on July 24, Lynx described itself as conducting attacks for financial gain, but stated that it has a strict policy of limiting attacks on socially important organizations such as government agencies, hospitals and non-profit organizations. In fact, they are carrying out attacks targeting various industries other than these organizations, and are emerging as a new threat, with 21 victims posted in just one month after they started their activities.

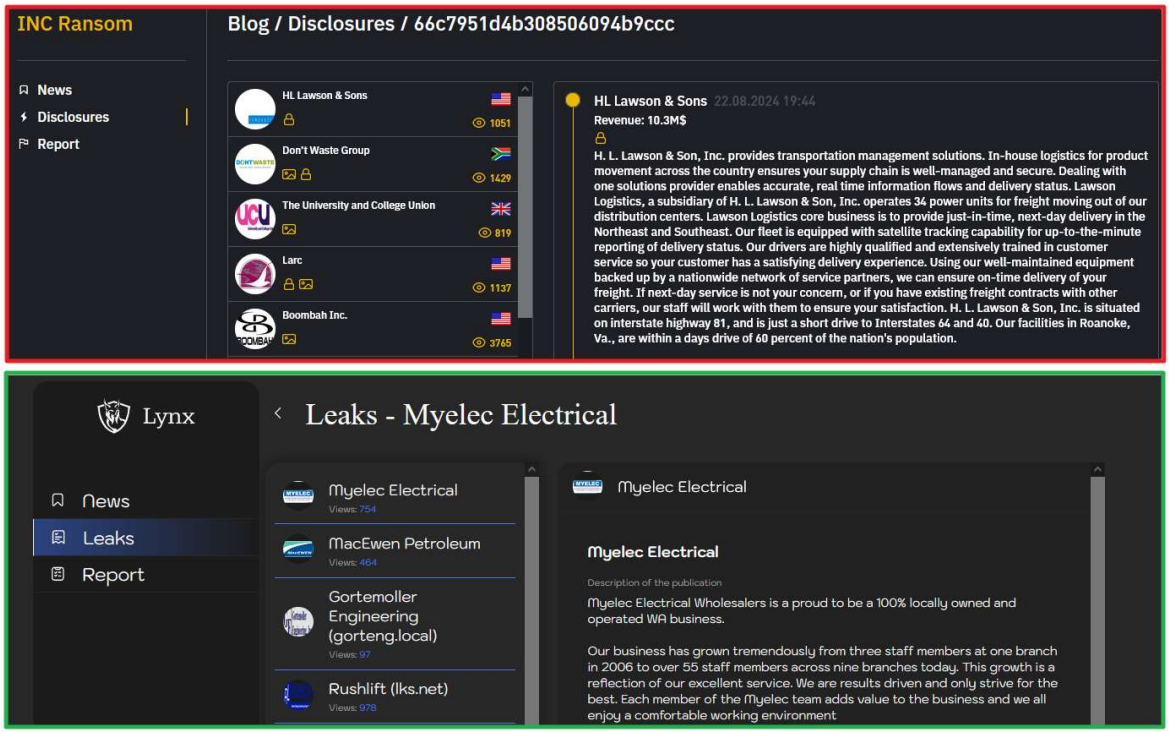


Figure 6. Comparison of dark web leak sites (top: INC ransom, bottom: Lynx)

Several pieces of evidence have been discovered that suggest a possible connection between the Lynx ransomware and the INC ransomware. First, the Lynx ransomware dark web leak site uses a very similar design to the INC ransomware group's dark web leak site, which changed its design in May.

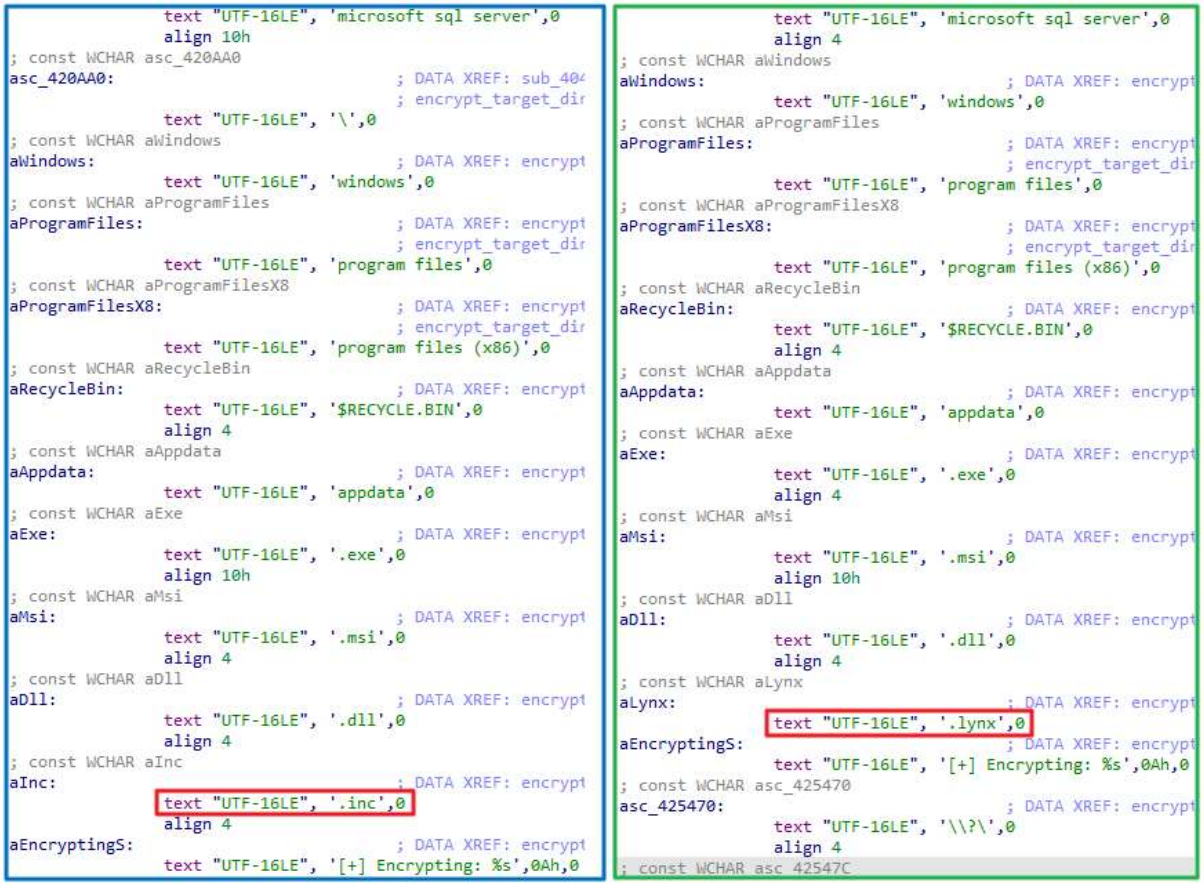


Figure 7. Comparison of ransomware strings (left: INC ransom, right: Lynx)

Second, analysis results show that the Lynx ransomware uses the same strings and encryption algorithms as the INC ransomware, and is also very similar in functional aspects such as program execution flow. This appears to be related to the INC ransomware group selling the source code of key systems, including the ransomware source code and the management panel, for $300,000 (approx. KRW 400 million) on a hacking forum in May. It is highly likely that the Lynx ransomware group purchased this source code before beginning its activities.

Therefore, this report focuses on the similarities and differences between the two ransomwares and provides a detailed analysis of the Lynx ransomware.

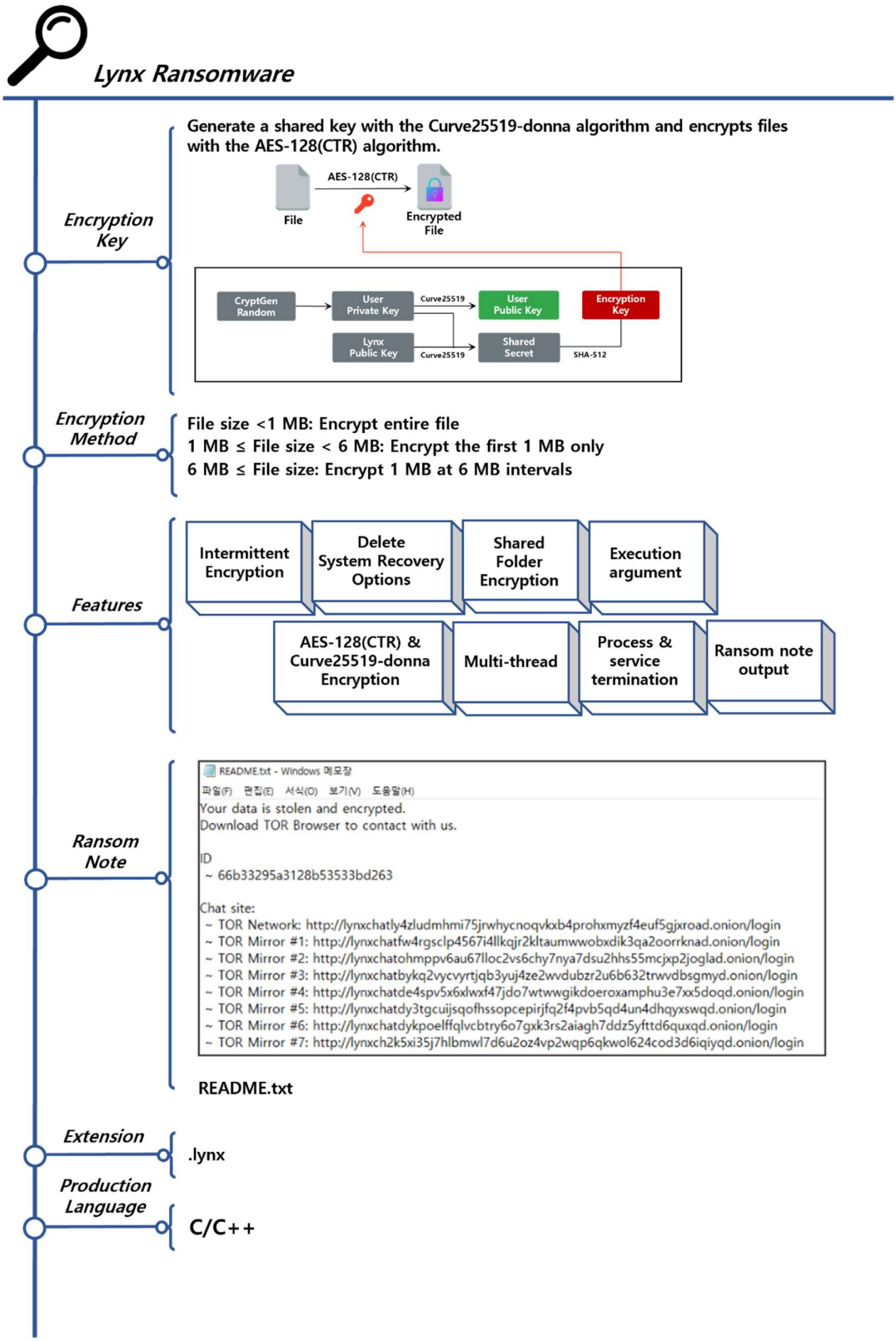


Figure 8. Overview of the Lynx ransomware

Strategies of the Lynx ransomware

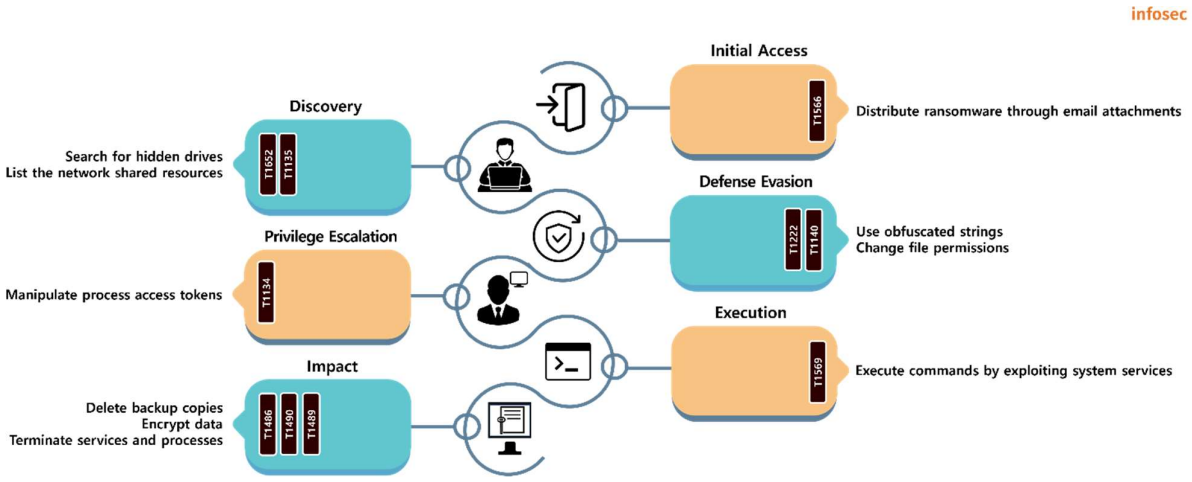


Figure 9. Attack strategy of the Lynx ransomware

The Lynx ransomware can enable or disable several features by providing additional arguments, such as mounting hidden drives or hiding the command prompt window. There are a total of 12 options, which can be executed normally without any specific execution arguments. The execution arguments used by the Lynx ransomware are as follows.

Argument	Description
--file [file path]	Encrypt only the selected file.
--dir [directory path]	Encrypt only the selected directory.
--help	Display descriptions on execution arguments.
--verbose	Display debugging logs.
--stop-processes	Terminate the process if the target file is running immediately before encrypting it.
--encrypt-network	Encrypt the network shared resources.
--load-drives	Mount hidden drives.
--hide-cmd	Hide the command prompt window that appears when the ransomware runs.
--no-background	Disable the wallpaper change function.
--no-print	Disable the ransom note display function.
--kill	Terminate specific processes and services.
--safe-mode	Boot in safe mode (this function does not exist).

Table 1. Lynx ransomware execution arguments

An analysis of the ransomware revealed that among the 12 execution argument options, for the "--safe-mode" function, which is described as a function for booting in safe mode, there is a code to check whether the argument has been entered. But no code was found to actually boot in safe mode or automatically restart the ransomware after rebooting. When actually executed, only a log verifying the argument is displayed, but it does not enter safe mode.

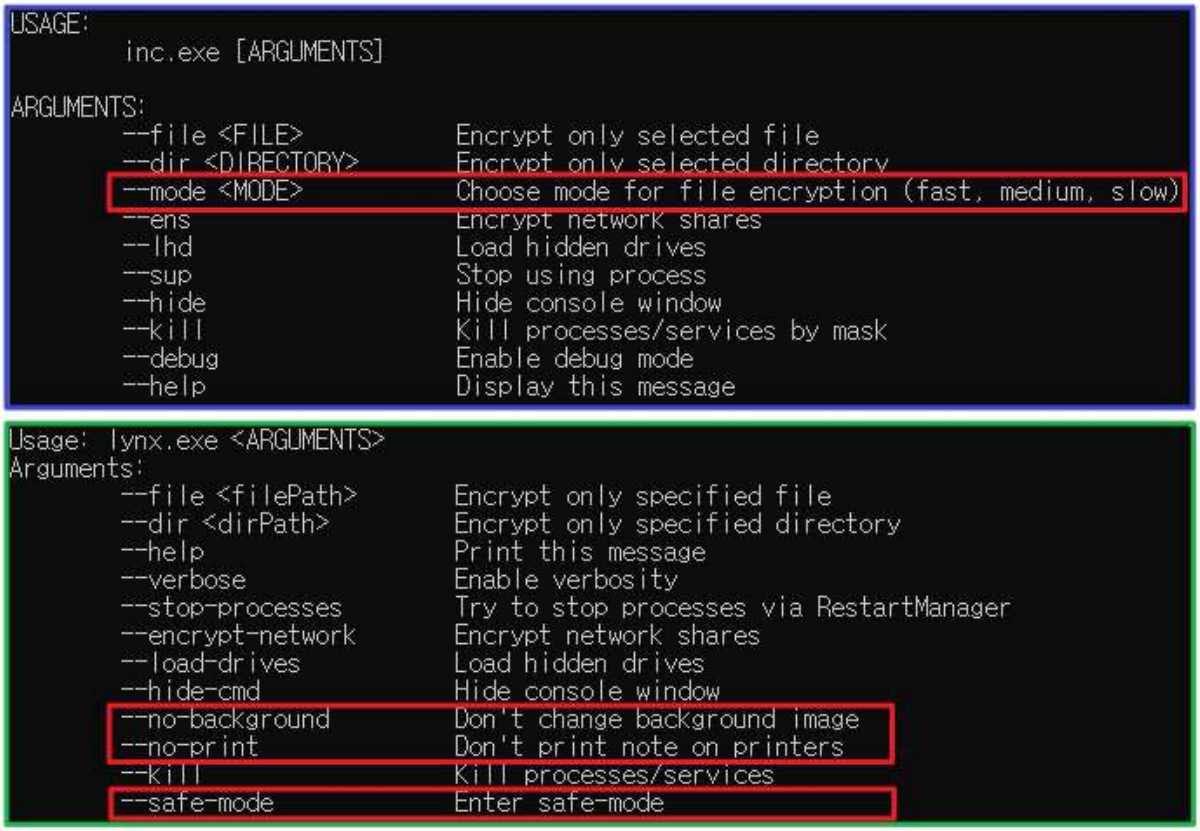


Figure 10. Comparison of execution arguments between ransomwares (top: INC, bottom: Lynx)

The execution arguments of the Lynx ransomware and INC ransomware differ in notation, but the same in terms of the detailed functions and operation methods. However, while the INC ransomware has a "--mode" argument that can set the encryption mode, the Lynx ransomware does not have such a feature.

In addition, it was discovered that executable arguments were added to disable the functions for changing the background and outputting ransom notes. While the INC ransomware registers the ransomware in a startup service and then boots in safe mode, the Lynx ransomware has removed this function and, as explained above, the "--safe-mode" argument has no function.

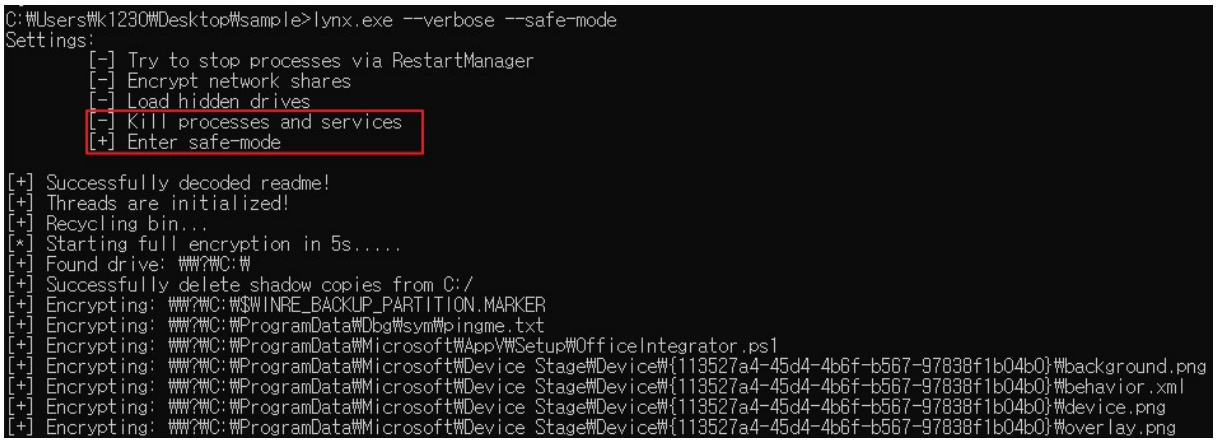


Figure 11. Lynx ransomware --verbose input result

In the Lynx ransomware, the "--verbose" execution argument displays the ransomware's settings and what it is currently doing on the command prompt window. When you activate a feature by entering an execution argument, "Settings" displays a "[+]" symbol instead of a "[-]" symbol to indicate that it is activated. This debugging[2] function is identical to the "--debug" execution argument of the INC ransomware.

The execution argument "--kill" refers to a list of processes and services hardcoded into the ransomware and terminates the target process/service. This argument performs the same function as the "--kill" execution argument of the INC ransomware and has the same kill targets, except for the text editor notepad, which was added to the Lynx ransomware. The table below shows the target processes and services for termination.

Process	Service
sql, veeam, backup, exchange, java, **notepad**	sql, veeam, backup, exchange

Table 2. Lynx ransomware target processes and services for termination

[2] Debugging: The process of finding and correcting system errors that occur during program development

```
if ( DeviceIoControl(FileW, 0x53C028u, InBuffer, 0x18u, 0, 0, &BytesReturned, 0) )// delete vsc (change vsc size 1)
                                        // 0x53c028 = IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE
                                        // resizes the allocated space for shadow copies snapshots cause the deleteion of vsc
```

Figure 12. Deleting backup copies using DeviceIoControl

Before encrypting the entire drive, the ransomware first deletes backup copies. Unlike other ransomware that primarily leverage Windows utilities for managing backup copies (vssadmin, wmic shadowcopy, wbadmin, bcdedit), the Lynx and INC ransomware use the DeviceIoControl function to control devices and delete backup copies. If you use the DeviceIoControl function to reset the storage space for backup copies to a very small size, the system will recognize that there is not enough space to store backups and delete existing backup copies in order to secure storage space. In the Lynx ransomware, this function only works when both the "--file" and "--dir" arguments are not used.

```
if ( GetVolumePathNamesForVolumeNameW(v5, szVolumePathNames, 0x78u, &cchReturnLength)
  && lstrlenW(szVolumePathNames) == 3 )
{
  szVolumePathNames[0] = 0;
}
else
{
  v7 = lpszVolumeMountPoint[v0--];
  if ( SetVolumeMountPointW(v7, v5) )     // Mount Volume
  {
    if ( param_verbose )
      print_message_with__s(L"\t[+] Mounted % s\n", v7);
```

```
while ( !WNetEnumResourceW(hEnum, &cCount, v4, &dwBytes) )
{
  v5 = 0;
  if ( cCount )
  {
    v6 = v4 + 3;
    do
    {
      if ( v4[2] == 3 )
      {
        lstrcpyW(String1, v6[2]);
        lstrcatW(String1, L"\\");
        if ( param_verbose )
          print_message_with__s(L"[+] Found share: %s\n", String1);
        encrypt_target_directory(String1);
```

Figure 13. Collecting targets for encryption (left: Mounting hidden drives, right: Adding network shared resources)

Before encrypting a file, there is a process of collecting the encryption targets. When the "--load-drives" argument is used, the ransomware checks all drives from A to Z for hidden drives before encrypting files, and if such drives exist, mounts them and adds them to the encryption target. When the "--encrypt-network" argument is used, the ransomware also adds network shared resources to the encryption targets. This argument performs the same function as the "--lhd" and "--ens" arguments of the INC ransomware.

The "--file" argument encrypts only specific files, and the "--dir" argument encrypts only files in a specific directory. If neither is entered, the ransomware will encrypt all files except those listed as exceptions. Encryption exceptions and folder names are hardcoded and stored in the ransomware, and the identified exceptions are as shown in the table below.

Extensions and files to be excluded	Folders to be excluded
*.exe, *.msi, *.dll, *.lynx, README.txt	Windows, Program Files, Program Files (x86), $RECYCLE.BIN, AppData

Table 3. Targets excluded from encryption by the Lynx ransomware

The encryption exceptions in the Lynx and INC ransomware are nearly identical, but there are some differences. In the case of the Lynx ransomware, a code has been added to encrypt the “microsoft sql server” folder under the “Program Files” and “Program Files (x86)” folders, which are exceptions. “.lynx,” which is added to avoid double encryption of already encrypted files, is “.inc” in the INC ransomware.

Unlike the INC ransomware, which provides three encryption modes via the “--mode” argument, the Lynx ransomware has no function for selecting encryption options. The INC ransomware supports three encryption modes: Fast mode, which encrypts only 1 MB at the beginning, middle, and end of the file; Medium mode, which encrypts 1 MB of every 6 MB; and Slow mode, which encrypts the entire file. The Lynx ransomware uses the medium mode as its default.

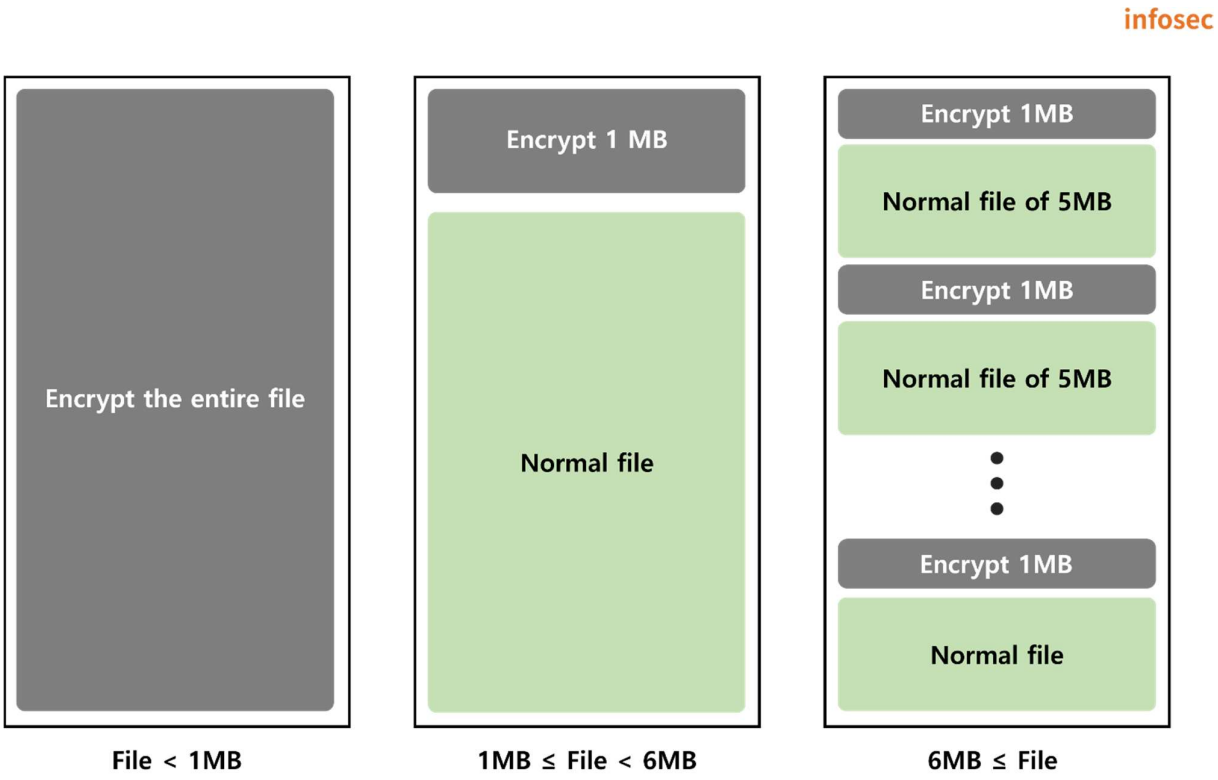


Figure 14. Lynx ransomware’s encryption methods

The figure above shows the Lynx ransomware's encryption method in more detail. For files smaller than 1 MB, the entire file is encrypted. For files equal to or larger than 1 MB but smaller than 6 MB, only the first 1 MB of the file is encrypted. And for files larger than 6 MB, 1 MB of data is encrypted at 6 MB intervals. Files are encrypted using the AES-128 (CTR) algorithm, and Curve25519-donna is used as the key generation algorithm to protect the key.

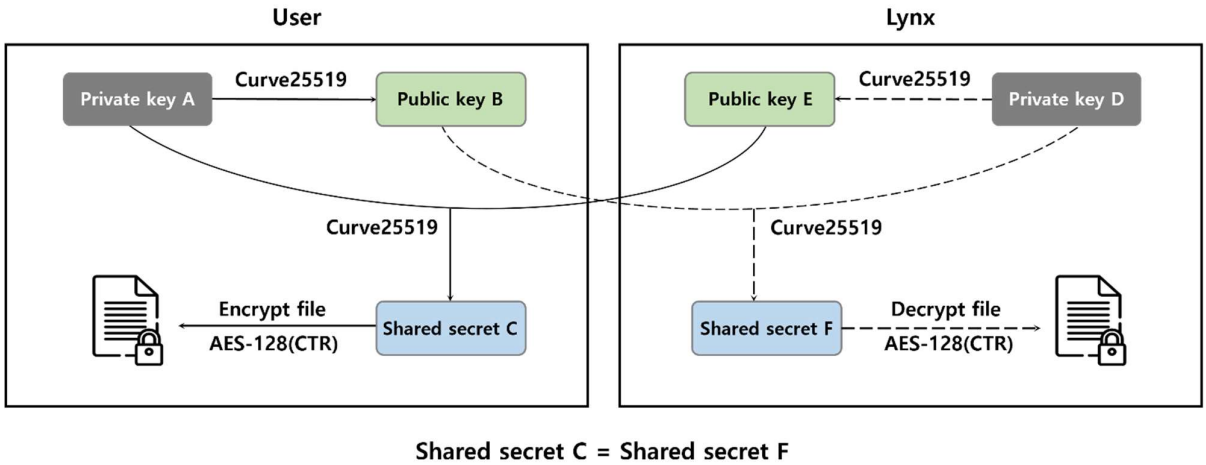


Figure 15. Lynx ransomware's shared secret generation method

When the Lynx ransomware generates an encryption key, the key is protected without having to encrypt it separately because the Curve25519-donna algorithm used is a key distribution algorithm. A key distribution algorithm allows two users to generate the same symmetric keys using their own private key and the other's public key. First, a user generates a public key using his or her private key. Then, the key (C) generated using the user's private key and the other party's public key will have the same value as the key (F) generated using the user's public key and the other party's private key. These identical keys (C, F) are called a 'shared secret.'

The Lynx ransomware generates a private key and a public key randomly for each file to be encrypted, and encrypts the files by generating a shared secret using the private key and the hardcoded attacker's public key. Then, by appending that file's public key to the end of the file, the attacker can use his or her private key and the file's public key to decrypt the file by regenerating the key used to encrypt it.

```
encoded_ransomnote = decode_base64_string(
                     &dwMessageIda,
                     "WW91ciBkYXRhIGlzIHN0b2xlbiBhbmQgZW5jcnlwdGVkLg0KRG93bmxvYWQgVE9SIEJyb3dzZXIgdG8gY29udGFjdCB"
                     "3aXRoIHVzLg0KDQpJRA0KIH4gJWlkJQ0KDQpDaGF0IHNpdGU6DQogfiBUT1IgTmV0d29yazogaHR0cDovL2x5bnhjaG"
                     "F0bHk0emx1ZG1obWk3NWpyd2h5Y25vcXZreGI0cHJvaHhteXpmNGV1ZjVnanhyb2FkLm9uaW9uL2xvZ2luDQogfiBUT"
                     "1IgTWlycm9yICMxOiBodHRwOi8vbHlueGNoYXRmdzRyZ3NjbHA0NTY3aTRsbGtxanIya2x0YXVtd3dvYnhkaWszcWEy"
                     "b29ycmtuYWQub25pb24vbG9naW4NCiB+IFRPUiBNaXJyb3IgIzI6IGh0dHA6Ly9seW54Y2hhdG9obXBwdjZhdTY3bGx"
                     "vYzJ2czZjaHk3bnlhN2RzdTJoaHM1NW1janhwMmpvZ2xhZC5vbmlvbi9sb2dpbg0KIH4gVE9SIE1pcnJvciAjMzogaH"
                     "R0cDovL2x5bnhjaGF0YnlrcTJ2eWN2eXJ0anFiM3l1ajR6ZTJ3dmR1YnpyMnU2YjYzMnRyd3ZkYnNnbXlkLm9uaW9uL"
                     "2xvZ2luDQogfiBUT1IgTWlycm9yICM0OiBodHRwOi8vbHlueGNoYXRkZTRzcHY1eDZ4bHd4ZjQ3amRvN3d0d3dnaWtk"
                     "b2Vyb3hhbXBodTNlN3h4NWRvcWQub25pb24vbG9naW4NCiB+IFRPUiBNaXJyb3IgIzU6IGh0dHA6Ly9seW54Y2hhdGR"
                     "5M3RnY3VpanNxb2Zoc3NvcGNlcGlyamZxMmY0cHZiNXFkNHVuNGRocXl4c3dxZC5vbmlvbi9sb2dpbg0KIH4gVE9SIE"
                     "1pcnJvciAjNjogaHR0cDovL2x5bnhjaGF0ZHlrcG9lbGZmcWx2Y2J0cnk2bzdneGszcnMyYWlhZ2g3ZGR6NXlmdHRkN"
                     "nF1eHFkLm9uaW9uL2xvZ2luDQogfiBUT1IgTWlycm9yICM3OiBodHRwOi8vbHlueGNoMms1eGkzNWo3aGxibXdsN2Q2"
                     "dTJvejR2cDJ3cXA2cWt3b2w2MjRjb2QzZDZpcWl5cWQub25pb24vbG9naW4NCg0KT3VyIGJsb2c6DQogfiBUT1IgTmV"
                     "0d29yazogaHR0cDovL2x5bnhibG9neHN0Z3pzYXJmeWsycHZoZHY0NWlnZ2hiNHptdGhuem1zaXB6ZW9kdXJ1ejN4d3"
                     "FkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjMTogaHR0cDovL2x5bnhibG9nY283cjM3anQ3cDV3cm1meHpxemU3Z2h4d"
                     "zZyaWh6a3FjNDU1cWx1YWN3b3RjaXlkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjMjogaHR0cDovL2x5bnhibG9naWp5"
                     "NGpmb2JsZ2l4MmtseG1rYmdlZTRsZW9ldWdlN3F0NGZwZmtqNHpiaTJzanlkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciA"
                     "jMzogaHR0cDovL2x5bnhibG9nbXgzcmJpd2czcnBqNG5kczI1aGpzbnJ3a3B4dDVnYXpuZXRmaWt6NGd6MmNzeWFkLm"
                     "9uaW9uLw0KIH4gVE9SIE1pcnJvciAjNDogaHR0cDovL2x5bnhibG9nb3hsbHRoNGI0NmNmd2xvcDVwZmo0czdkeXYzN"
                     "3l1eTdxbjJmdGFuNmdkNzJoc2FkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjNTogaHR0cDovL2x5bnhibG9ndHdhdGZz"
                     "cndqM29hdHBland4azVibmdxY2Q1ZjdzMjZpc2thZ2Z1N291YW9tamFkLm9uaW9uLw0KIH4gVE9SIE1pcnJvciAjNjo"
                     "gaHR0cDovL2x5bnhibG9neHV0dWZvc3NhZWF3bGlqM2ozdWlrYWxvbGw1a282Z3J6aGt3ZGNscmpuZ3Jmb2lkLm9uaW"
                     "9uLw0KIH4gTWlycm9yICM3OiBodHRwOi8vbHlueGJsb2cubmV0Lw0KIA==",
                     &args_2);
```

Figure 16. Base64 decoding of the Lynx ransomware ransom note

The Lynx ransomware decodes and uses the contents of the ransom note, which is encoded by Base64. The decoded ransom note is saved as a text file in the encrypted folder, converted into an image and set as the wallpaper, and printed on any connected printer. The INC ransomware also recovers and uses Base64-encoded ransom notes. But unlike the Lynx ransomware, it utilizes two types of ransom note: a text file version and an HTML version.

```
                    Your data is stolen and encrypted.
                Download TOR Browser to contact with us.

                                  ID
                        ~ 66b33295a3128b53533bd263

                               Chat site:
 ~ TOR Network: http://lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad.onion/login
~ TOR Mirror #1: http://lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad.onion/login
~ TOR Mirror #2: http://lynxchatohmppv6au671loc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion/login
~ TOR Mirror #3: http://lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion/login
~ TOR Mirror #4: http://lynxchatde4spv5x6x1wxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd.onion/login
~ TOR Mirror #5: http://lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd.onion/login
~ TOR Mirror #6: http://lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd.onion/login
~ TOR Mirror #7: http://lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd.onion/login

                               Our blog:
   ~ TOR Network: http://lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd.onion/
  ~ TOR Mirror #1: http://lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd.onion/
  ~ TOR Mirror #2: http://lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd.onion/
  ~ TOR Mirror #3: http://lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad.onion/
  ~ TOR Mirror #4: http://lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad.onion/
  ~ TOR Mirror #5: http://lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad.onion/
  ~ TOR Mirror #6: http://lynxblogxutufossaeawlij3j3uikalol15ko6grzhkwdclrjngrfoid.onion/
                          ~ Mirror #7: http://lynxblog.net/
```

Figure 17. Changing the Lynx ransomware wallpaper

Measures against the Lynx ransomware

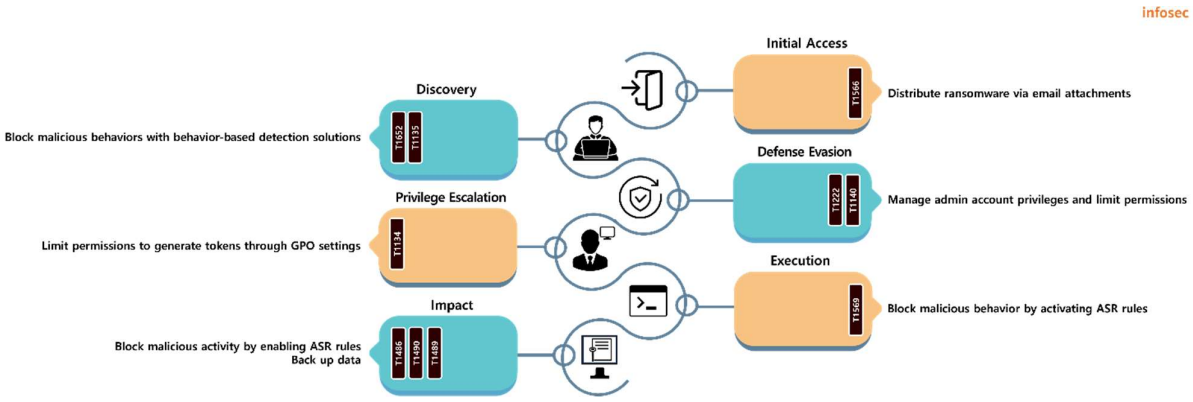


Figure 18. Measures against the Lynx ransomware

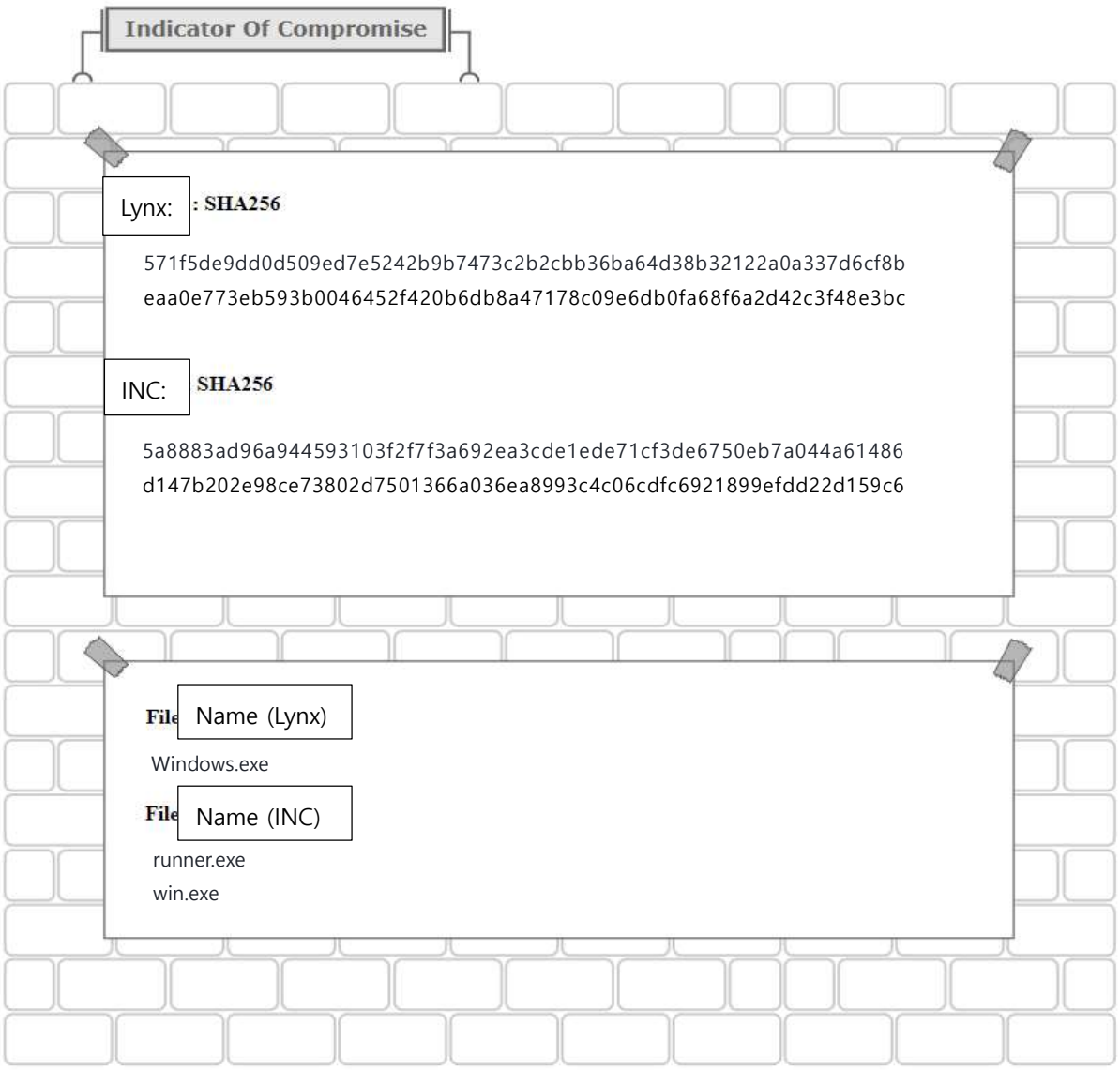
The Lynx ransomware is propagated via email attachments. Therefore, you should be careful not to open emails or attachments from suspicious or unidentified senders. An effective way to prevent ransomware infection is to use an email threat response & detection solution that detects and blocks email threats in a virtual environment.

The ransomware lists connected network shared resources and scans for and mounts hidden drives to secure encrypted targets on infected systems. To prevent this, you can use behavior-based detection solutions to block such malicious activities.

In addition, the Lynx ransomware attempts to change the privileges of files before encrypting them. During this process, the attacker needs administrator privileges. Since the Lynx ransomware does not have a separate privilege escalation function, you can prevent file encryption to some extent by strictly managing the administrator account in advance and granting minimal privileges. You can also prevent malicious activities by enabling attack surface reduction (ASR)[3] rules or blocking specific processes used by attackers.

Lastly, since the Lynx ransomware encrypts network shared files too, you should minimize or disable access to network shared resources in order to prevent access to external resources. In addition, as ransomware attempts to delete backup copies to disable recovery through Windows' basic recovery capabilities, it is important that you back up data in separate networks or storages.

[3] ASR (Attack Surface Reduction): Protection against processes that are used or executable by attackers


Indicator Of Compromise
Lynx:
: SHA256
571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
INC:
SHA256
5a8883ad96a944593103f2f7f3a692ea3cde1ede71cf3de6750eb7a044a61486
d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6
File
Name (Lynx)
Windows.exe
File
Name (INC)
runner.exe
win.exe

■ Reference sites

• Jenkins' official website (https://www.jenkins.io/security/advisory/2024-01-24/)

• CISA's official website (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

• NIST's national vulnerability database (https://nvd.nist.gov/vuln/detail/CVE-2024-23897)

• Fortinet's official blog (https://www.fortinet.com/blog/threat-research/stomping-shadow-copies-a-second-look-into-deletion-methods)

• Sophos's official website (https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/)

• BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/fbi-disrupts-the-dispossessor-ransomware-operation-seizes-servers/)