# 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 CIS[1] and BRIC[2]

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

countries from their attack targets, that they would use Windows and ESXi[3] 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.

[2] BRIC: Brazil, Russia, India and China

[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.

## Ransomware news

infosec

### 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

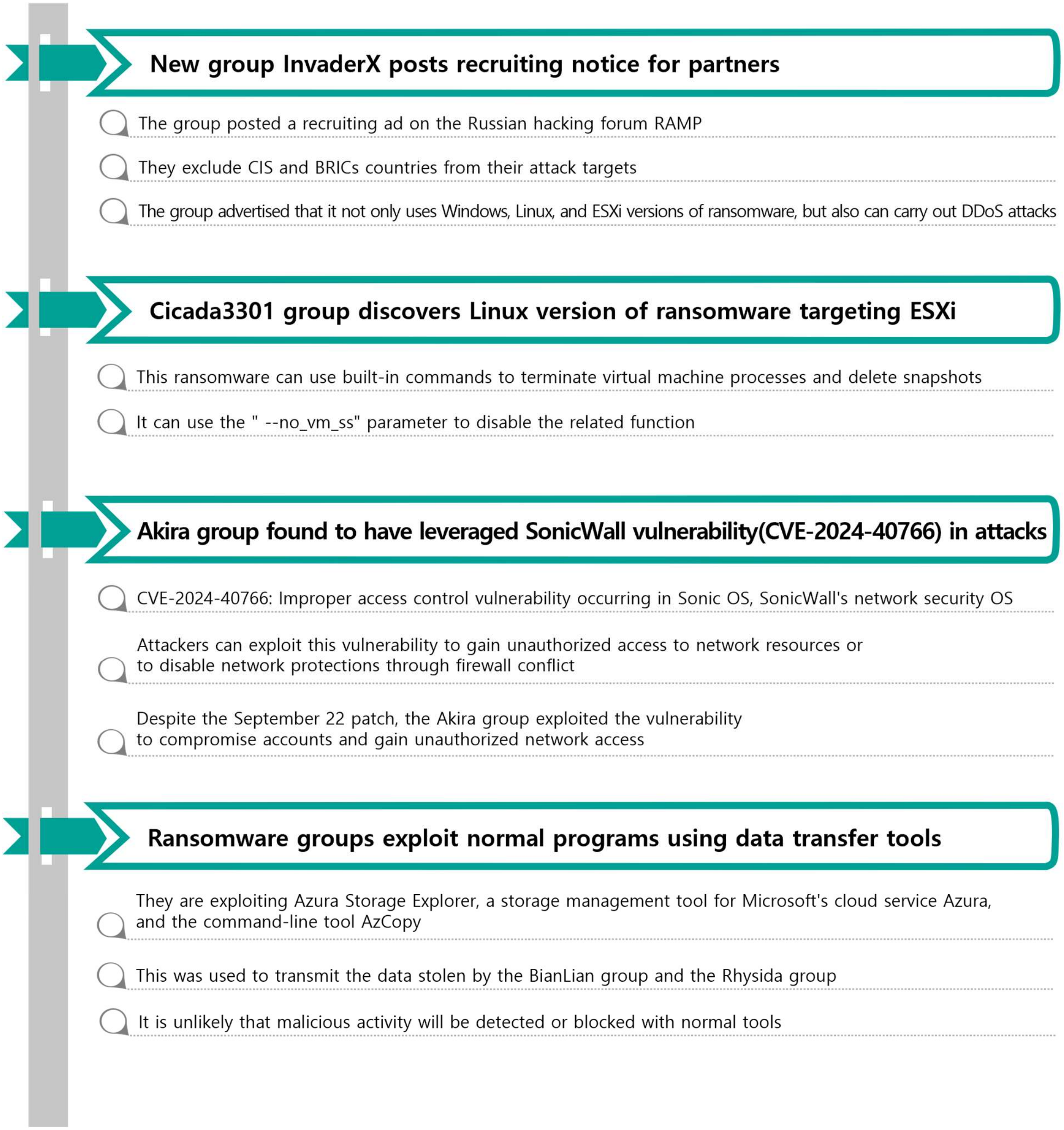
- They released data and claimed that Korean workers in Indonesia have committed racial discrimination against Indonesians and Muslims
- The disclosed data was found to be available from a public data portal

### 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 Azura, 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

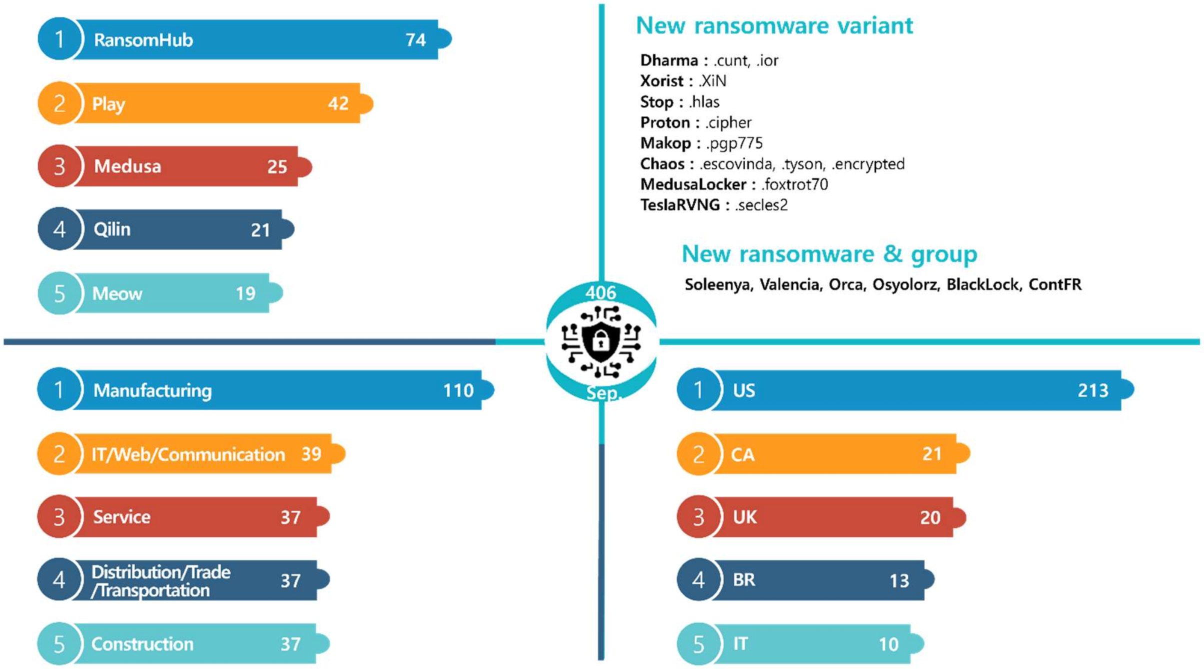
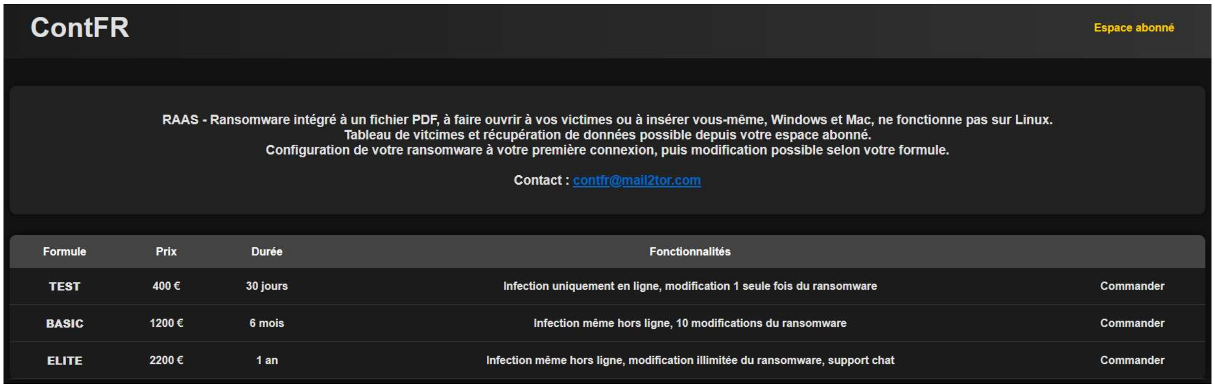


Figure 2. Ransomware threats in September 2024

### 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

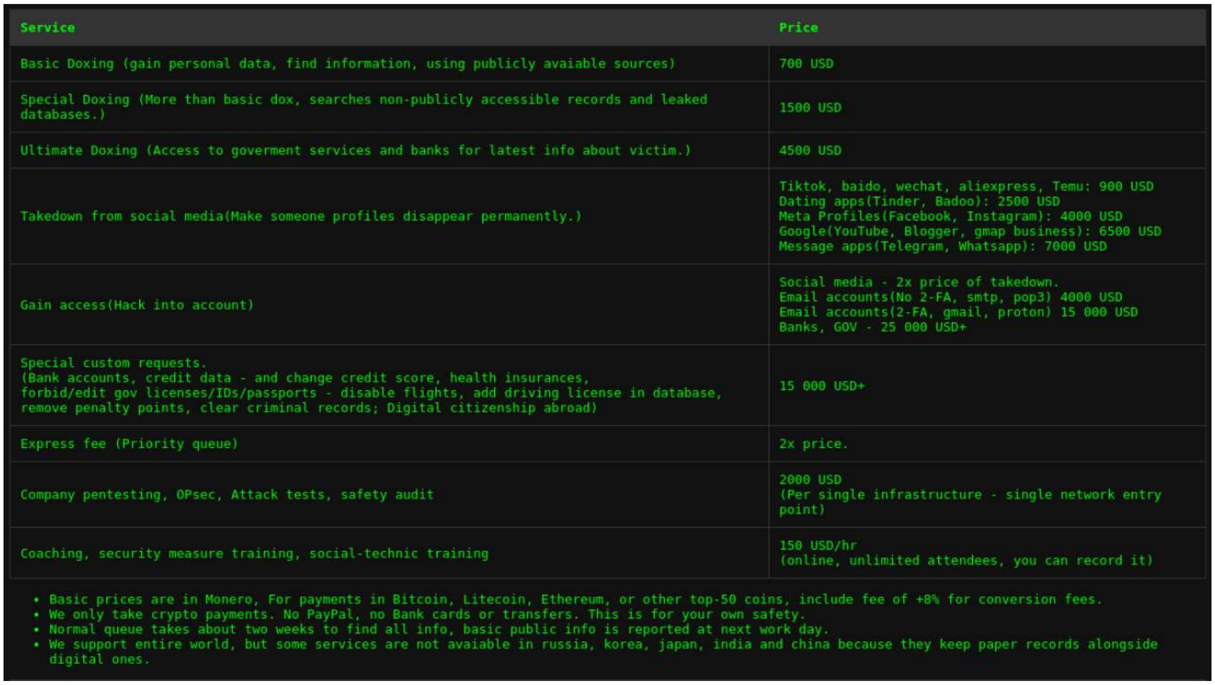
RAAS - Ransomware intégré à un fichier PDF, à faire ouvrir à vos victimes ou à insérer vous-même, Windows et Mac, ne fonctionne pas sur Linux.
Tableau de vitcimes et récupération de données possible depuis votre espace abonné.
Configuration de votre ransomware à votre première connexion, puis modification 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 avaiable sources) | 700 USD |
| Special Doxing (More than basic dox, searches non-publicly accessible records and leaked databases.) | 1500 USD |
| Ultimate Doxing (Access to goverment 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<br>Dating apps(Tinder, Badoo): 2500 USD<br>Meta Profiles(Facebook, Instagram): 4000 USD<br>Google(YouTube, Blogger, gmap business): 6500 USD<br>Message apps(Telegram, Whatsapp): 7000 USD |
| Gain access(Hack into account) | Social media - 2x price of takedown.<br>Email accounts(No 2-FA, smtp, pop3) 4000 USD<br>Email accounts(2-FA, gmail, proton) 15 000 USD<br>Banks, GOV - 25 000 USD+ |
| Special custom requests.<br>(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<br>(Per single infrastructure - single network entry point) |
| Coaching, security measure training, social-technic training | 150 USD/hr<br>(online, unlimited attendees, you can record it) |

- 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 avaiable 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

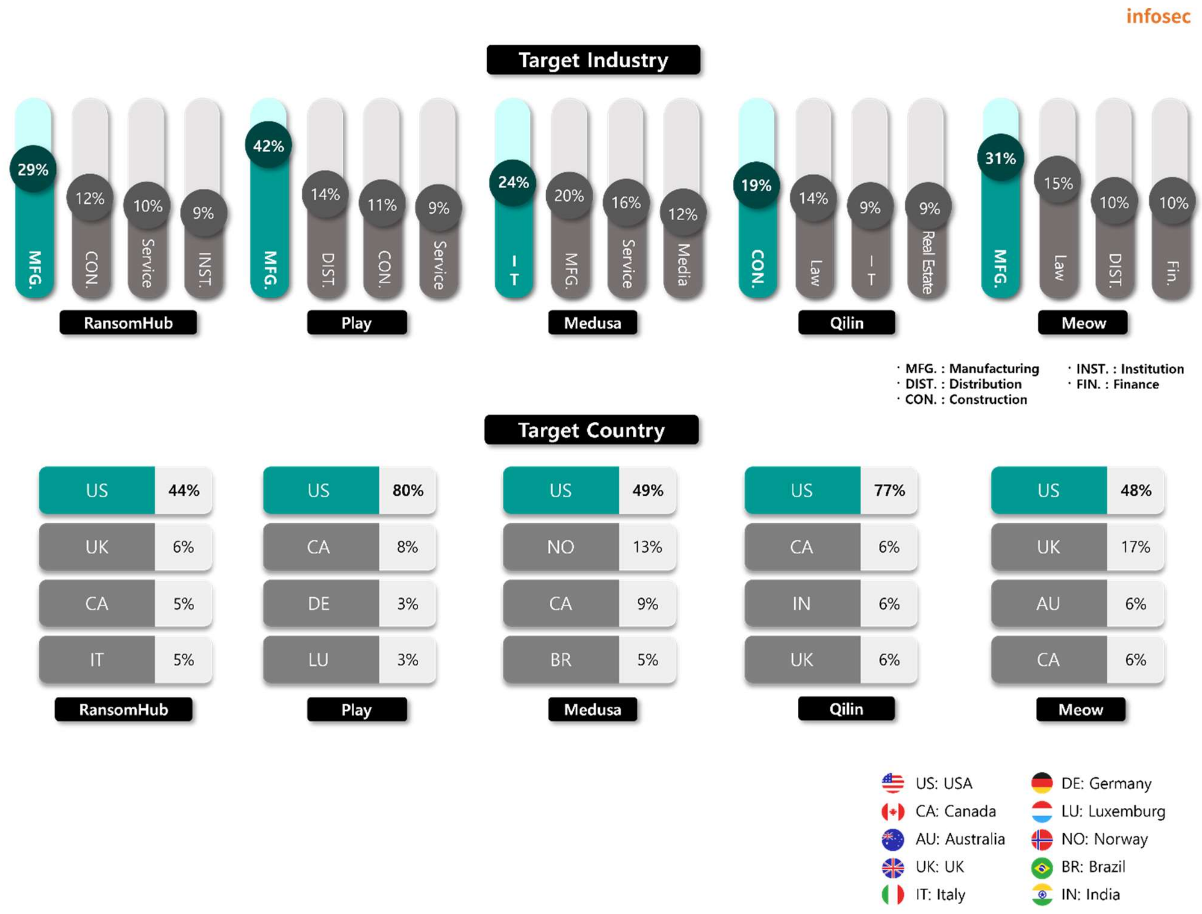


Figure 5. Major ransomware attacks by industry/country

The number of victims reported by the RansomHub group in September amounted to 19% of all ransomware victims. To disable EDR[6] solutions, RansomHub was recently found to have used TDSSKiller, a rootkit[7] and bootkit[8] 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

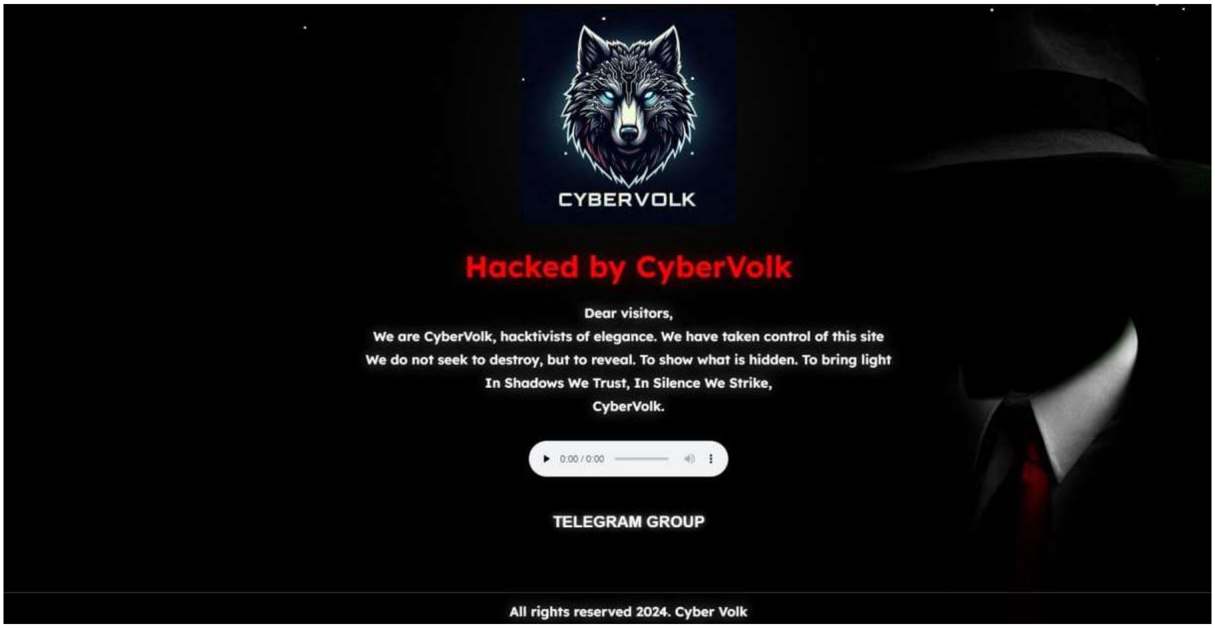
[8] Bootkit: Malware that damages the area used to boot the operating system, preventing it from booting properly

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).



CYBERVOLK

Hacked by CyberVolk

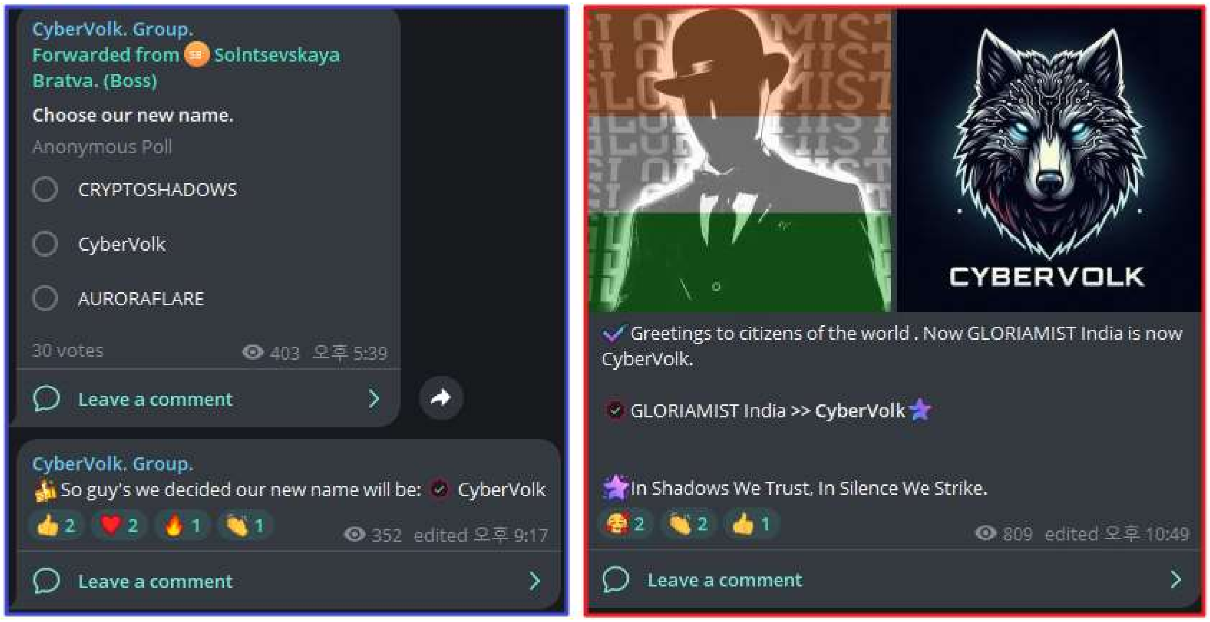
Dear visitors,
We are CyberVolk, hacktivists of elegance. We have taken control of this site
We do not seek to destroy, but to reveal. To show what is hidden. To bring light
In Shadows We Trust, In Silence We Strike,
CyberVolk.

TELEGRAM GROUP

All rights reserved 2024. Cyber Volk

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.



CyberVolk. Group.
Forwarded from Solntsevskaya Bratva. (Boss)

Choose our new name.

Anonymous Poll

○ CRYPTOSHADOWS

○ CyberVolk

○ AURORAFLARE

30 votes 403 오후 5:39

Leave a comment

CyberVolk. Group.
So guy's we decided our new name will be: ✓ CyberVolk

👍 2 ❤️ 2 🔥 1 👏 1 352 edited 오후 9:17

Leave a comment

✓ Greetings to citizens of the world . Now GLORIAMIST India is now CyberVolk.

✓ GLORIAMIST India >> CyberVolk ⭐

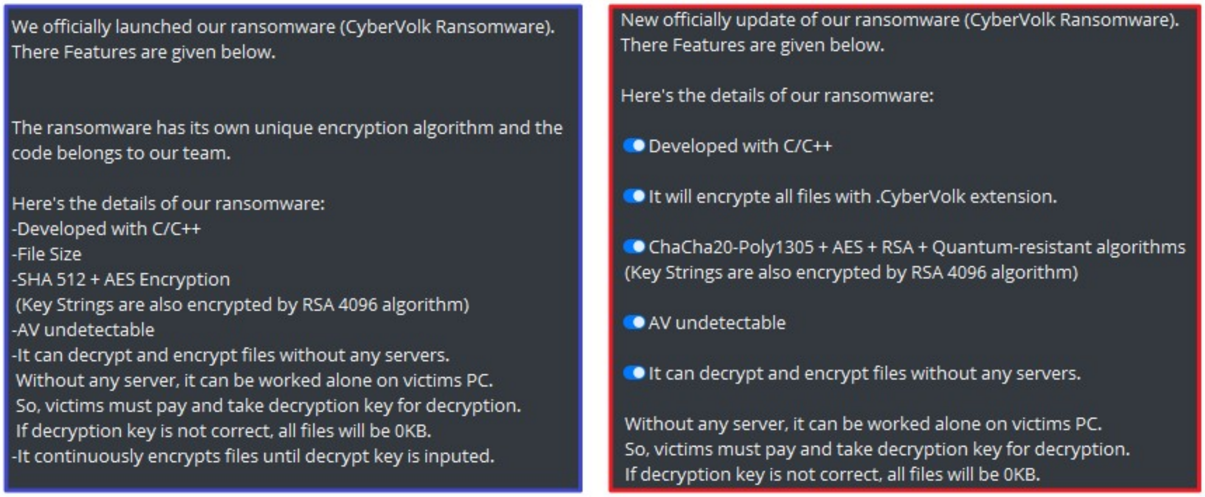
⭐ In Shadows We Trust. In Silence We Strike.

🥰 2 👏 2 👍 1 809 edited 오후 10:49

Leave a comment

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.



We officially launched our ransomware (CyberVolk Ransomware).
There Features are given below.

The ransomware has its own unique encryption algorithm and the code belongs to our team.

Here's the details of our ransomware:
-Developed with C/C++
-File Size
-SHA 512 + AES Encryption
(Key Strings are also encrypted by RSA 4096 algorithm)
-AV undetectable
-It can decrypt and encrypt files without any servers.
Without any server, it can be worked alone on victims PC.
So, victims must pay and take decryption key for decryption.
If decryption key is not correct, all files will be 0KB.
-It continuously encrypts files until decrypt key is inputed.

New officially update of our ransomware (CyberVolk Ransomware).
There Features are given below.

Here's the details of our ransomware:

● Developed with C/C++

● It will encrypte all files with .CyberVolk extension.

● ChaCha20-Poly1305 + AES + RSA + Quantum-resistant algorithms
(Key Strings are also encrypted by RSA 4096 algorithm)

● AV undetectable

● It can decrypt and encrypt files without any servers.

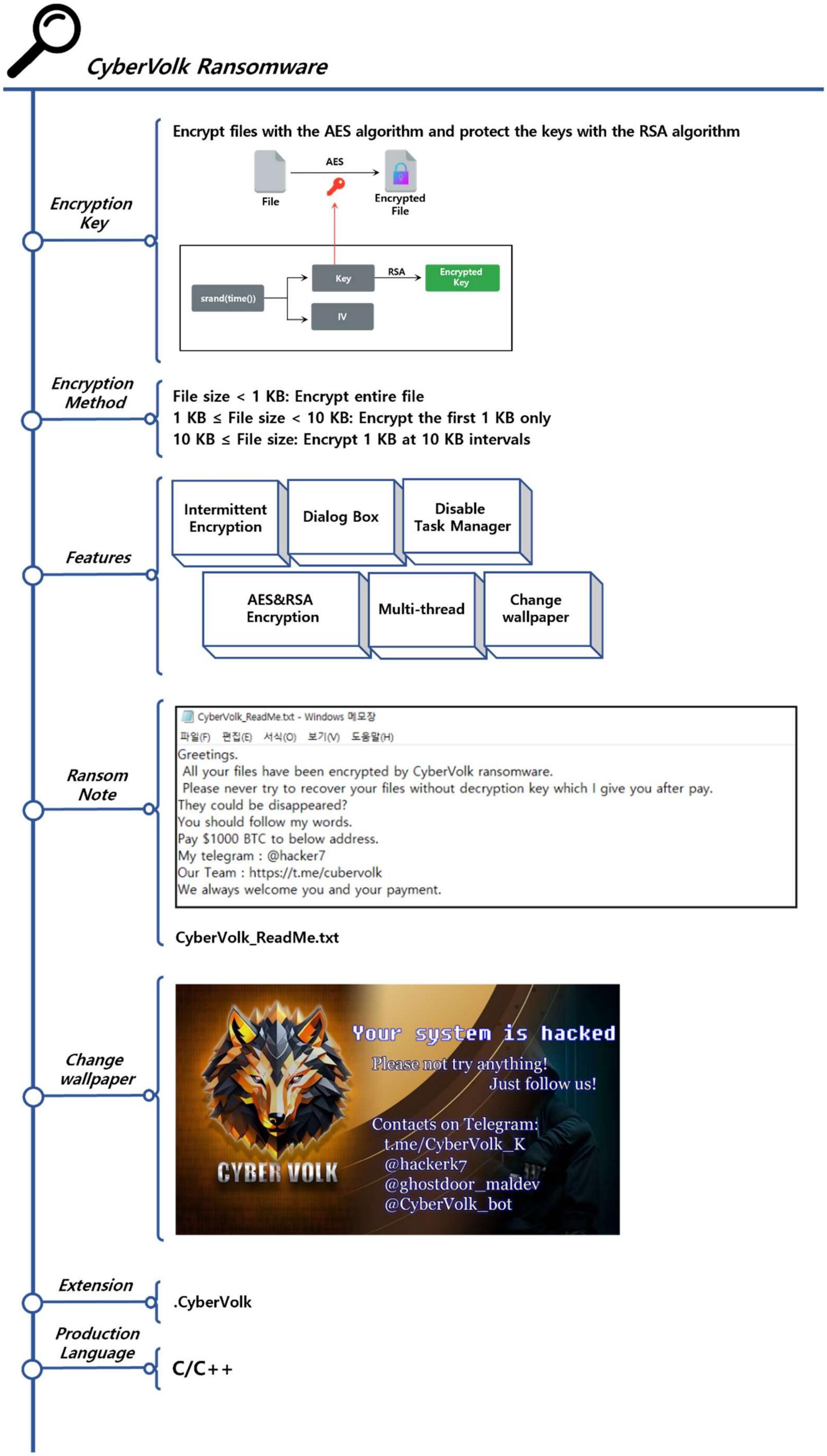
Without any server, it can be worked alone on victims PC.
So, victims must pay and take decryption key for decryption.
If decryption key is not correct, all files will be 0KB.

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



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

File size < 1 KB: Encrypt entire file
1 KB ≤ File size < 10 KB: Encrypt the first 1 KB only
10 KB ≤ File size: Encrypt 1 KB at 10 KB intervals

```
Greetings.
 All your files have been encrypted by CyberVolk ransomware.
 Please never try to recover your files without decryption key which I give you after pay.
They could be disappeared?
You should follow my words.
Pay $1000 BTC to below address.
My telegram : @hacker7
Our Team : https://t.me/cubervolk
We always welcome you and your payment.
```

CyberVolk_ReadMe.txt

.CyberVolk

C/C++

Figure 9. Overview of the CyberVolk ransomware

Strategy of the CyberVolk Ransomware

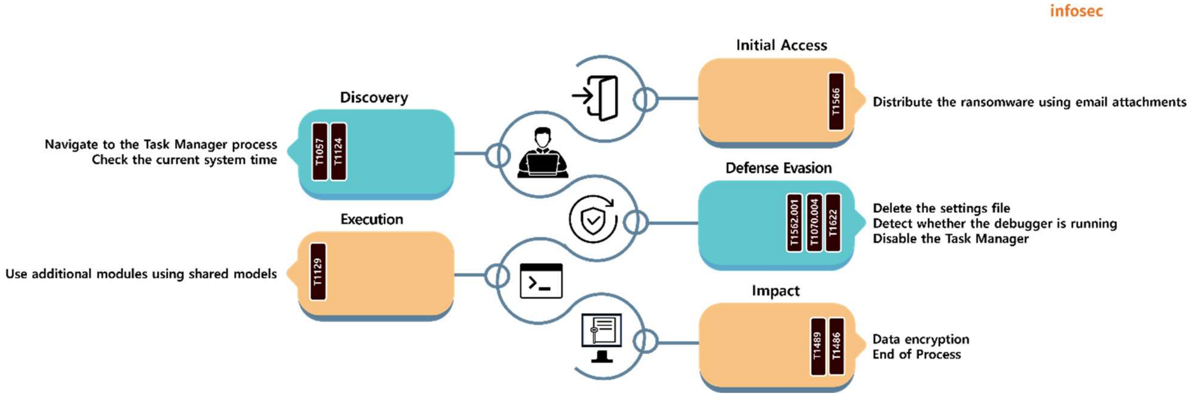

infosec
Initial Access
T1566
Distribute the ransomware using email attachments
Discovery
Navigate to the Task Manager process
Check the current system time
T1057
T1124
Defense Evasion
T1562.001
T1070.004
T1622
Delete the settings file
Detect whether the debugger is running
Disable the Task Manager
Execution
Use additional modules using shared models
T1129
Impact
T1489
T1486
Data encryption
End of Process

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.

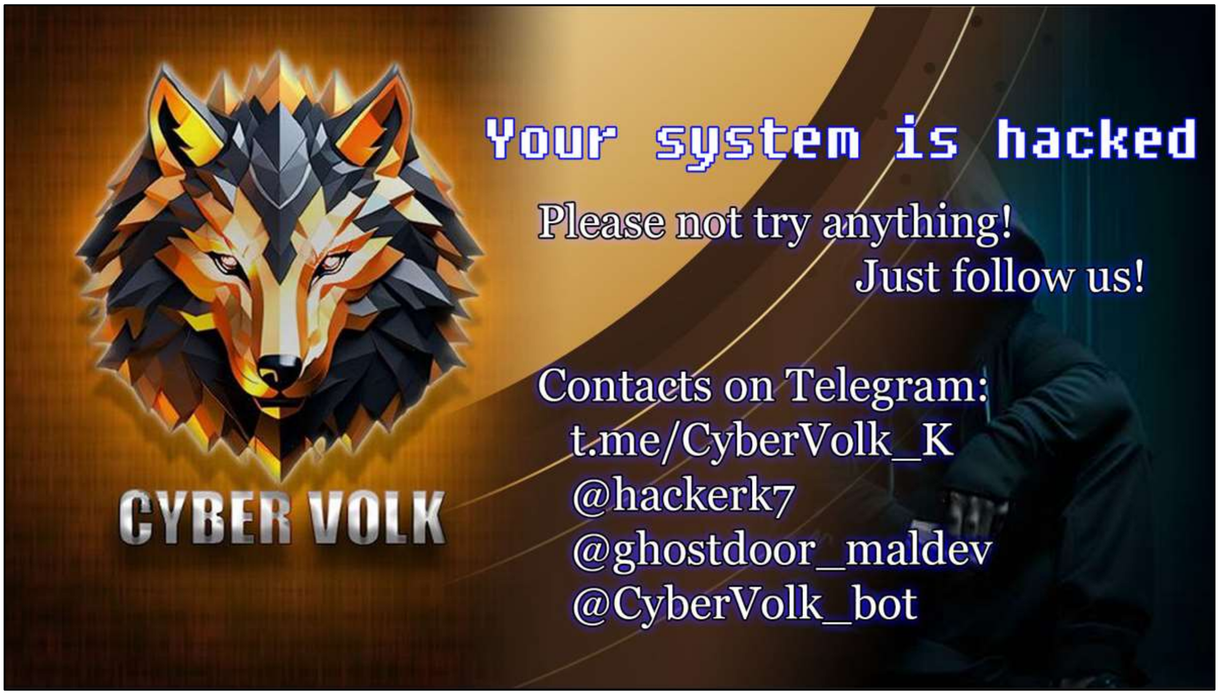
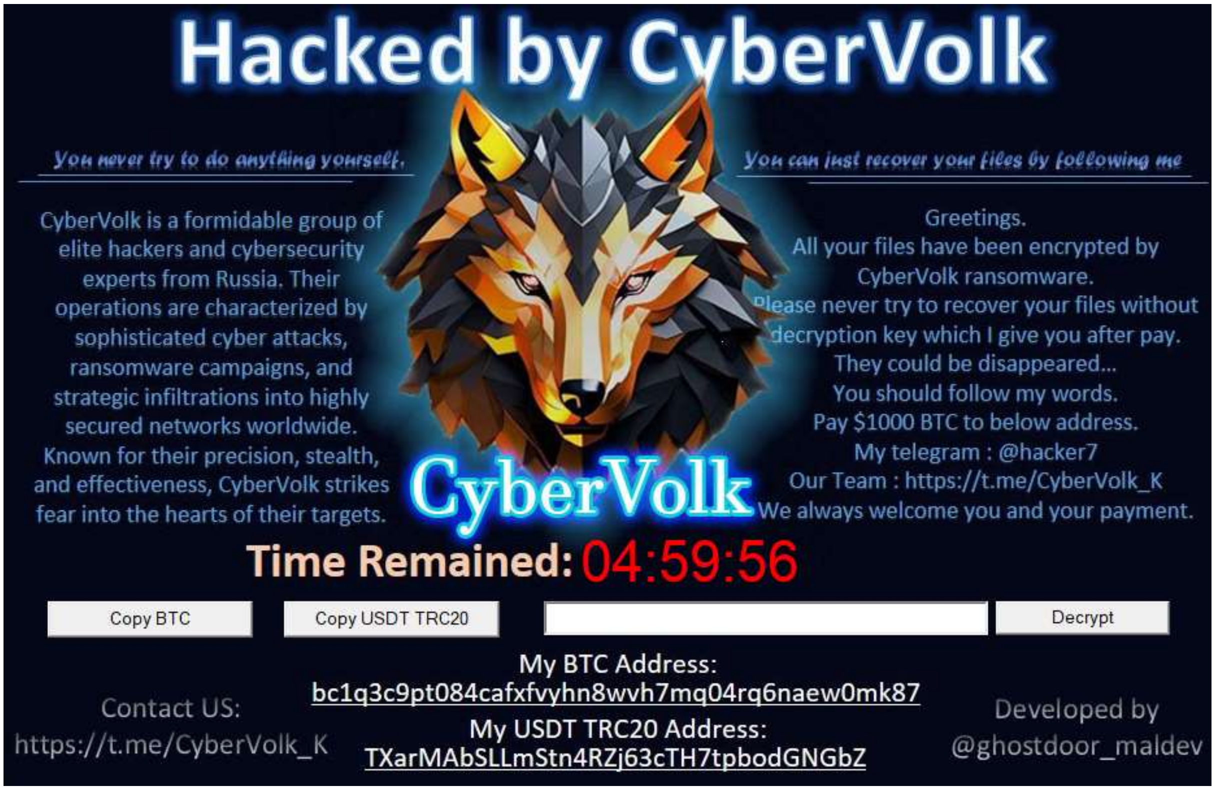


Figure 11. Bitmap file (tmp.bmp) stored in the temporary folder

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.



Hacked by CyberVolk

You never try to do anything yourself.

CyberVolk is a formidable group of elite hackers and cybersecurity experts from Russia. Their operations are characterized by sophisticated cyber attacks, ransomware campaigns, and strategic infiltrations into highly secured networks worldwide. Known for their precision, stealth, and effectiveness, CyberVolk strikes fear into the hearts of their targets.

You can just recover your files by following me

Greetings.
All your files have been encrypted by CyberVolk ransomware.
Please never try to recover your files without decryption key which I give you after pay.
They could be disappeared...
You should follow my words.
Pay $1000 BTC to below address.
My telegram : @hacker7
Our Team : https://t.me/CyberVolk_K
We always welcome you and your payment.

CyberVolk

Time Remained: 04:59:56

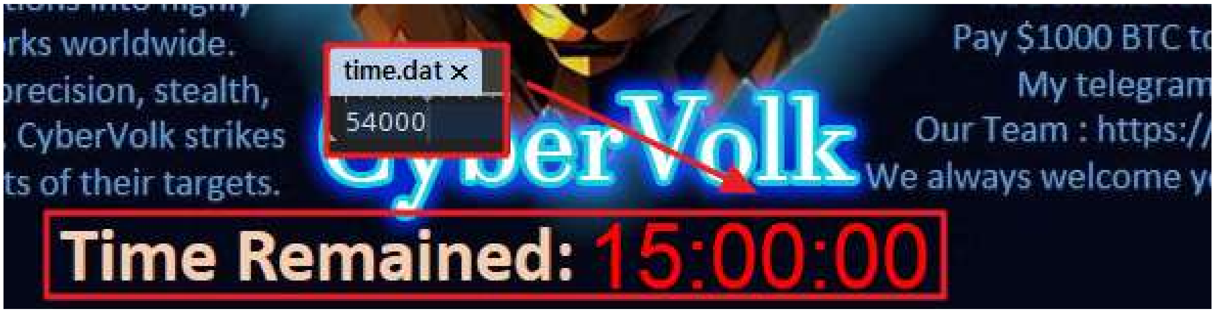
My BTC Address:
bc1q3c9pt084cafxfvyhn8wvh7mq04rq6naew0mk87
My USDT TRC20 Address:
TXarMAbSLLmStn4RZj63cTH7tpbodGNGbZ

Contact US:
https://t.me/CyberVolk_K

Developed by
@ghostdoor_maldev

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.



time.dat ×

54000

Time Remained: 15:00:00

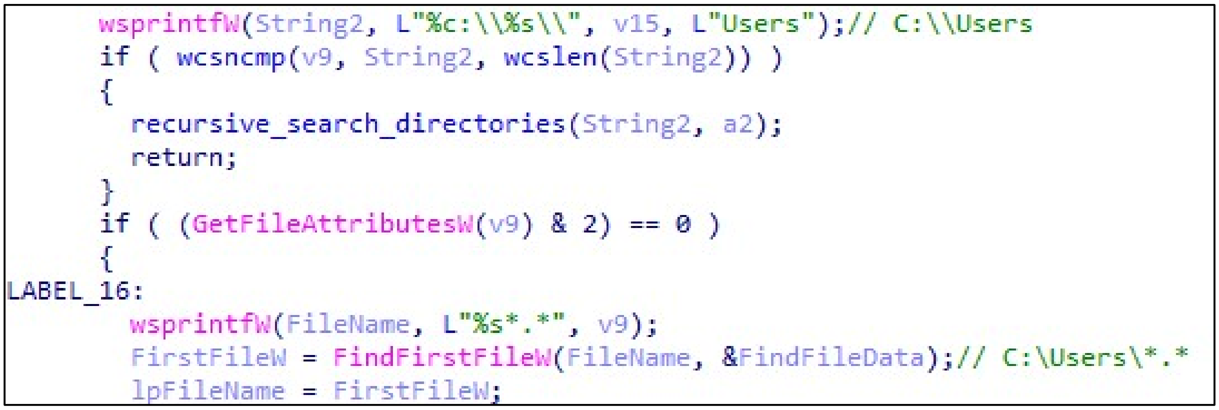
Figure 13. Changing the remaining time

To prevent users from shutting down the ransomware, it checks whether the Task

[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".

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

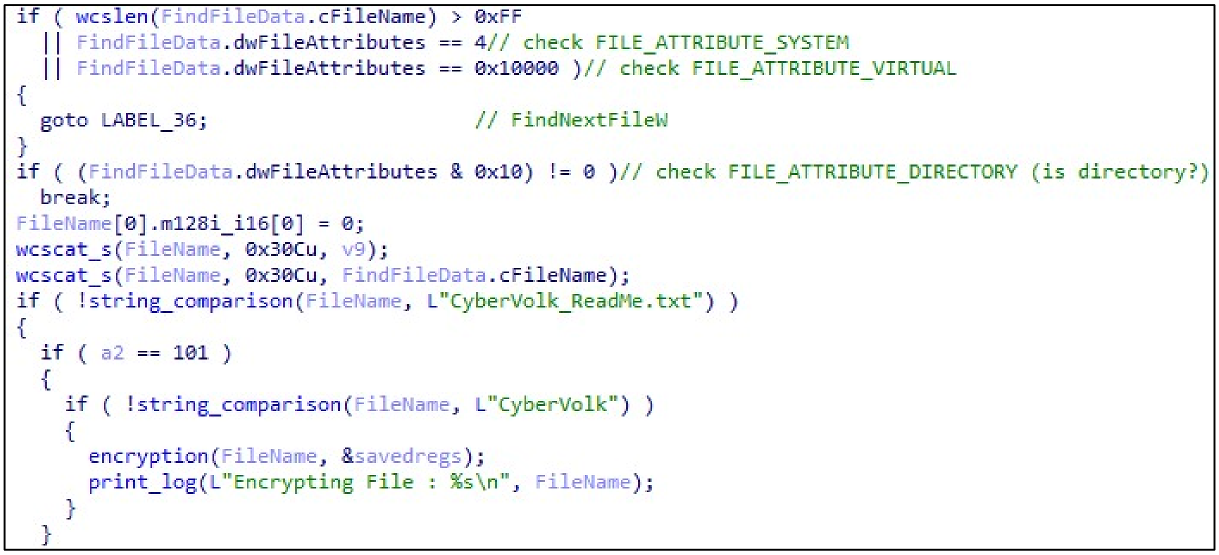
As the time displayed in the pop-up window passes, the CyberVolk ransomware prepares to encrypt your files. The ransomware scans all drives, starting from the root directory on removable disks and hard disks, looking for targets for encryption. It checks whether a Users directory exists in the top-level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

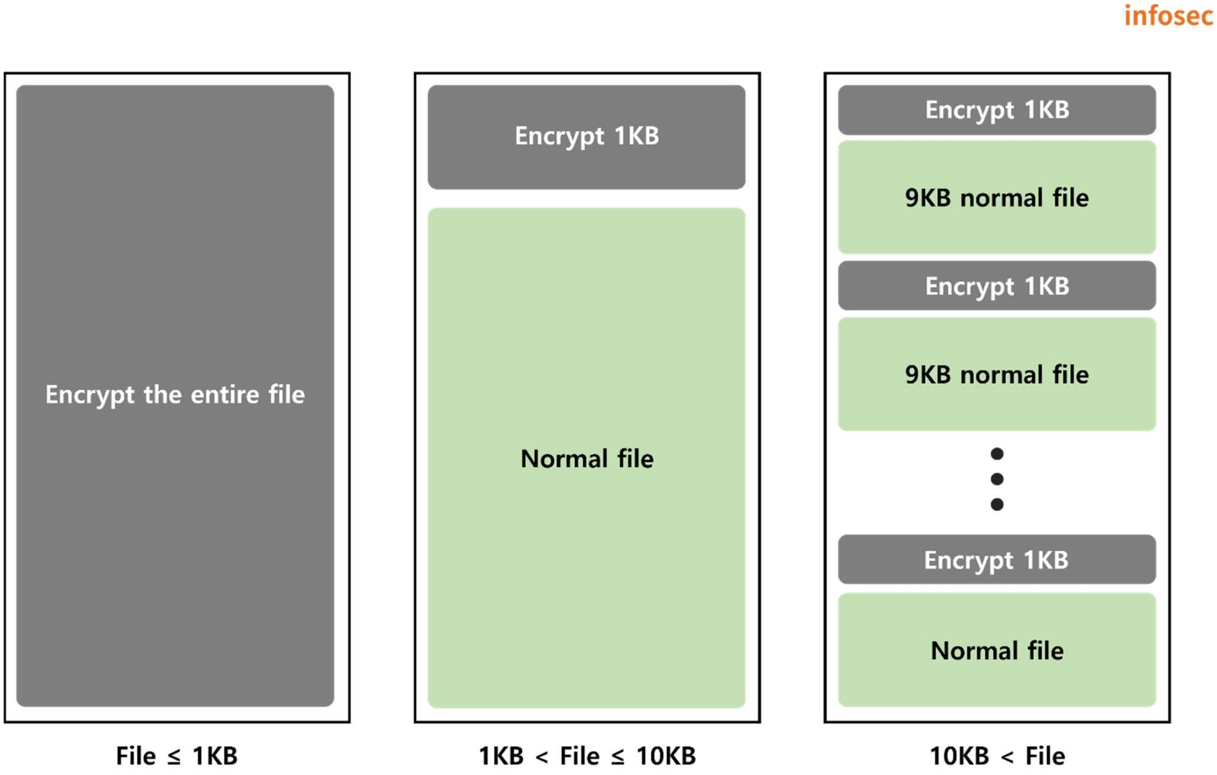
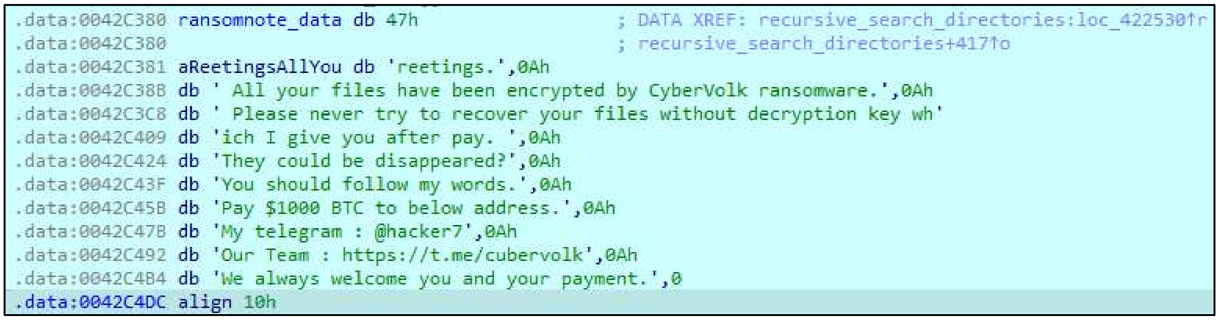


Figure 16. File encryption method

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.

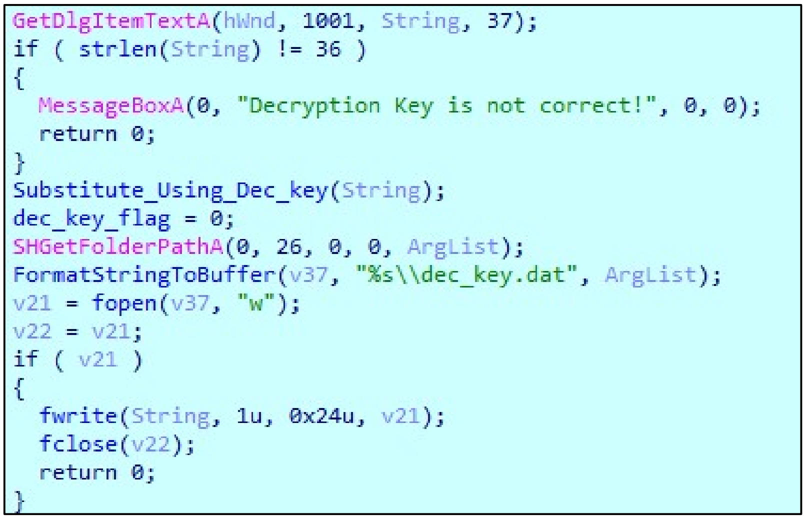
In addition, this ransomware uses its own ransom note data to create a ransom note in each folder during the file encryption process.



```
.data:0042C380 ransomnote_data db 47h                 ; DATA XREF: recursive_search_directories:loc_422530↑r
.data:0042C380                                        ; recursive_search_directories+417↑o
.data:0042C381 aReetingsAllYou db 'reetings.',0Ah
.data:0042C38B 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:0042C45B db 'Pay $1000 BTC to below address.',0Ah
.data:0042C47B 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.

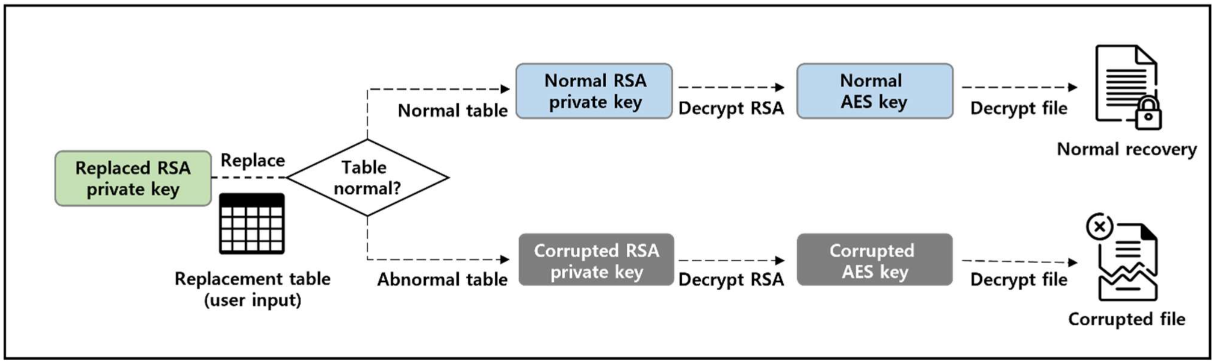


Figure 19. File recovery method

## Measures against the CyberVolk ransomware

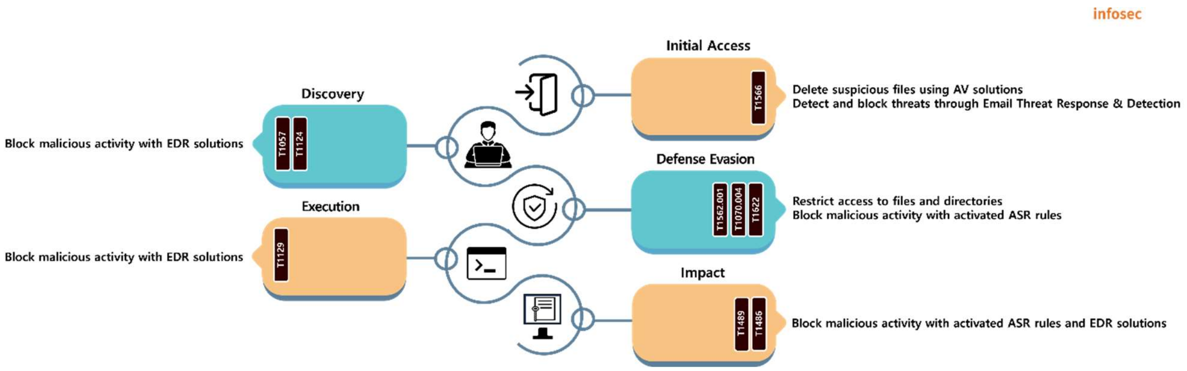

infosec
Initial Access
T1566
Delete suspicious files using AV solutions
Detect and block threats through Email Threat Response & Detection
Discovery
T1057
T1124
Block malicious activity with EDR solutions
Defense Evasion
T1562.001
T1070.004
T1622
Restrict access to files and directories
Block malicious activity with activated ASR rules
Execution
T1129
Block malicious activity with EDR solutions
Impact
T1489
T1486
Block malicious activity with activated ASR rules and EDR solutions

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 ASR[11] 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-blobbery-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)