# Keep up with Ransomware

## Ransomware threats targeting the ESXI server

Recently, reports of ransomware damage in Korea have increased 14 times from 22 cases in 2018 to 325 cases in 2022, and numerous companies are facing cyber security threats. In particular, ransomware attack groups share identified vulnerabilities and apply various strategies and detection avoidance techniques to become more sophisticated and advanced. Accordingly, EQST, the largest white hacker group in Korea and a group of security technology research experts, analyzes monthly ransomware threat trends and shares information necessary for responding to ransomware threats.

### ■ Outline

The source of ransomware threats is shifting to Ransomware as a Service (RaaS). In February 2023, while the number of confirmed ransomware damage cases increased compared to the previous month, the number of damage cases caused by the LockBit group, which is RaaS, occurred overwhelmingly in February, unlike the previous month when damage was caused by the top 5 groups and various other groups.

It turned out to be due to the downfall of the Hive ransomware group and the slowdown of other small groups, while the LockBit group is growing in size through numerous partner groups absorbed from other groups.

The Hive ransomware group, which started its activity in June 2021, is a large hacking organization that has damaged 1,500 or more companies around the world through a service-type model and earned about $100 million from the damaged companies. However, the Hive ransomware group fell due to network penetration carried out covertly by the FBI since July 2022. This is because the FBI penetrated the network and obtained and distributed more than 1,300 decryption keys. Due to this attack, the Hive group lost its profit model and ended its activities.

Unfortunately, however, another large-scale ransomware attack occurred last month. A vulnerable ESXi[1] server was attacked, and it was revealed that it used the CVE-2021-21974[2] vulnerability that was already discovered 2 years ago. This vulnerability has already been patched, but a vulnerable server that has not been patched was searched, and encryption is attempted through a ransomware (shell script and ELF file) called ESXiArgs[3].

CISA[4] released a tool that can restore the ESXi virtual machine environment infected through an encryption-type loophole to mitigate damage in the event of a large-scale ransomware attack. However, the attacker recognized this and changed the encryption method and tries to attack again, and the ransomware attack continues to target vulnerable servers.

Another Nevada ransomware attempting to attack Linux and ESXi servers was also discovered. It has been confirmed that this ransomware is also using the CVE-2021-21974 vulnerability and attempting a large-scale attack like the ESXiArgs ransomware. As such, large-scale infection of vulnerable ESXi servers is constantly confirmed. So caution is needed.

In addition to these large-scale ransomware attacks, new ransomware groups DarkBit and Medusa, which use a dual threat strategy through the dark web, are being discovered. Also, the activities of the V IS VENDETTA group are also detected on the dark web. It contains the same URL as the leak site URL of the existing Cuba ransomware group, and it is identified as a subdomain of the Cuba ransomware group as it uses the URL with 'test.' added.

Lastly, it was confirmed that one of the small and medium-sized manufacturing companies in Korea was infected with the Mallox ransomware, and the leaked data was posted on the dark web. The Mallox ransomware is a ransomware that attempts to attack vulnerable MS-SQL, and uses a dual threat strategy through file encryption and data leakage. After accessing the server through an MS-SQL account related attack, it attempts a ransomware attack with an additionally installed remote program, or uses SQL to execute a ransomware attack through the script or power shell command. If the database server is infected, most of the services provided by the company cannot be operated normally. So it is an important system that needs to decrypt the encrypted files first. A vulnerable database is one of the paths that attackers can easily penetrate, and domestic companies using MS-SQL need to take appropriate security measures.

---

[1] Virtualization OS developed in VMware

[2] A remote code execution vulnerability occurring in VMware ESXi OpenSLP due to heap overflow

[3] It is a kind of ransomware. France's Computer Emergency Response Team (CERT) first discovered it on February 3, and issued a warning. France announced that it is a ransomware that targets the hypervisor of VMWare called ESXi.

[4] CISA (Cybersecurity and Infrastructure Security Agency)

## ■ Ransomware news

### ESXiArgs ransomware attacks ESXi servers around the world.

- Attackers look for ESXi servers through information from public sources such as Shodan and Censys.
- Early penetration using the OpenSLP[5] remote code execution vulnerability (CVE-2021-21974)
- It is estimated that more than 3,000 servers worldwide and at least 20 servers in Korea are infected.
- The infection environment restoration tool was disclosed by US CISA, but it was modified to prevent restoration through an update.

### Royal ransomware Linux variant targeting VMware ESXi servers

- Functions that support Linux were added, and it attacks VMware ESXi servers.
- Execution options are provided, and the encryption process function is performed according to options.

### Nevada ransomware targeting Windows and VMware ESXi servers

- In December, Russian and Chinese hackers and affiliate companies were recruited through 2022 RAMP Forum.
- Windows and Linux files were encrypted through the Salsa20 algorithm.
- Execution options are provided, and malicious functions are performed according to options.

### SentinelLabs distributes the Clop variant ransomware decryption tool.

- On December 26, 2022, the Clop ransomware targeting Linux OS were discovered.
- Flaws were discovered in the process of protecting the keys used for file encryption.
- SentinelLabs distributed a decryption tool free of charge.

[5] A service search protocol that makes it possible to locate services in the local area network. (Open-source Service Location Protocol)

## Clop ransomware claims that it infringed 130 organizations using the GoAnywhere vulnerability.

- The Clop ransomware attacker claims to have stolen data from more than 130 organizations with the RCE vulnerability (CVE-2023-0669) in the GoAnywhere MFT security file transfer tool.
- The situation similar is similar to the stealing of data from about 100 companies through the Accellion FTA Zero-day vulnerability (CVE-2021-27101~27104) in December 2020.

## A new MortalKombat ransomware targeting systems in the US

- Financial gains were obtained through the MortalKombat ransomware, a variant of the Xorist ransomware, and an information leaking malware Laplas Clipper.
- It caused damage mostly in the US, and it was distributed through phishing mail.
- As the main files of the system are included in encryption targets, the system may not operate normally.

## Tonga, one of the Pacific island nations hit by ransomware

- Tonga's state-run telecommunications company, TCC, was attacked by the Medusa ransomware group, delaying its work process.
- The Medusa group mainly penetrated through the RDP vulnerability.

## North Korea's ransomware attacks against medical and other key infrastructures

- US government agencies and National Intelligence Service published a joint report about North Korea's ransomware attacks.
- The CVE-2021-44228, CVE-2021-20038, CVE-2022-24990 vulnerability are used for the attack.
- The Maui, H0lyGh0st ransomware is used.

## US and UK sanctions against members of the TrickBot and Conti ransomware organizations.

- A wide range of attacks were conducted against health services and hospitals in the US and UK, and the UK confirmed that these groups made a profit of £27 million, and carried out more than 149 attacks.
- All the properties and funds of the members of 7 Russian organizations in the US and UK were frozen.

## Russia's Dubnikov pleads guilty to the money laundering of the Ryuk ransomware group.

- Denis Mihaqlovic Dubnikov and 13 accomplices participated in Ryuk ransomware money laundering.
- On April 11, 2023, the final verdict will be delivered, and if they are found guilty, they can face up to 20 years in prison, 3 years of supervised release and fines of up to $500,000

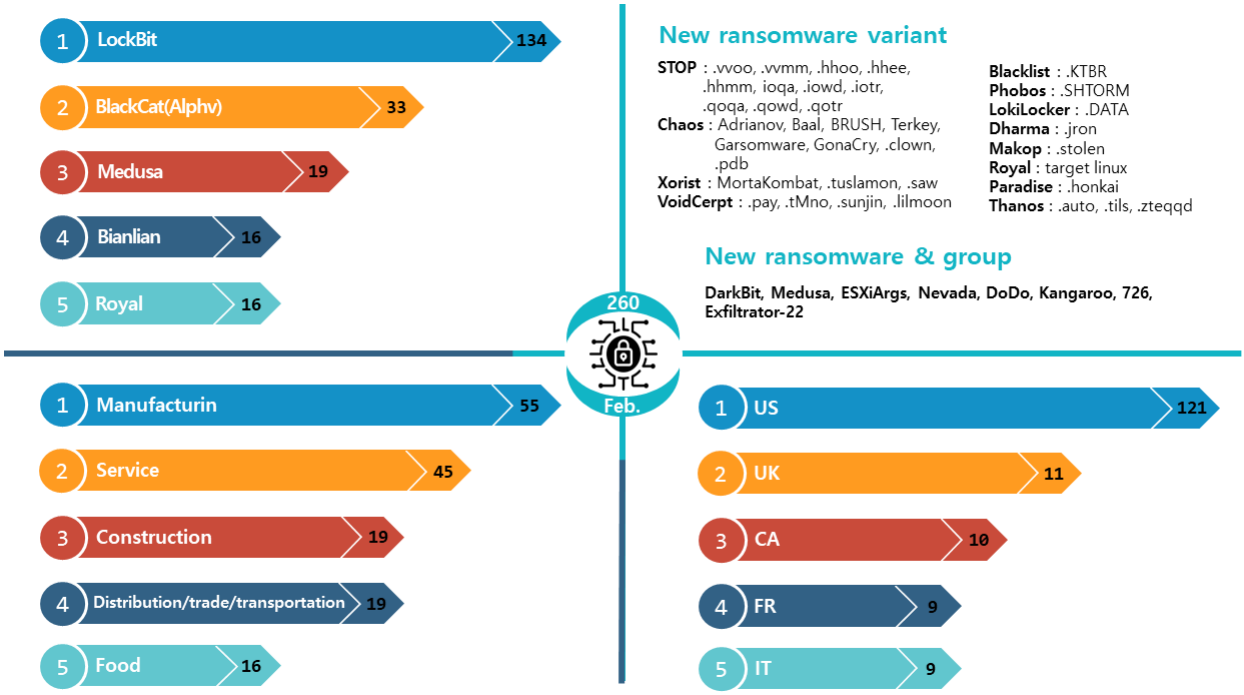
## Attack framework Exfiltrator-22 related to the Lockbit ransomware

- Attack framework demo video including various functions such as ransomware and data leakage was released.
- As it uses the same C2 infrastructure as the domain fronting technology, used in Lockbit 3.0, it is presumed to be a tool developed by an affiliate or member of Lockbit 3.0.

## MortalKombat ransomware free decryption tool is released.

- Bitdefender released a free decryption tool for the MortalKombat ransomware.
- The Laplas clipboard hijacker needs to be removed manually.

## ■ Ransomware news




### New threats

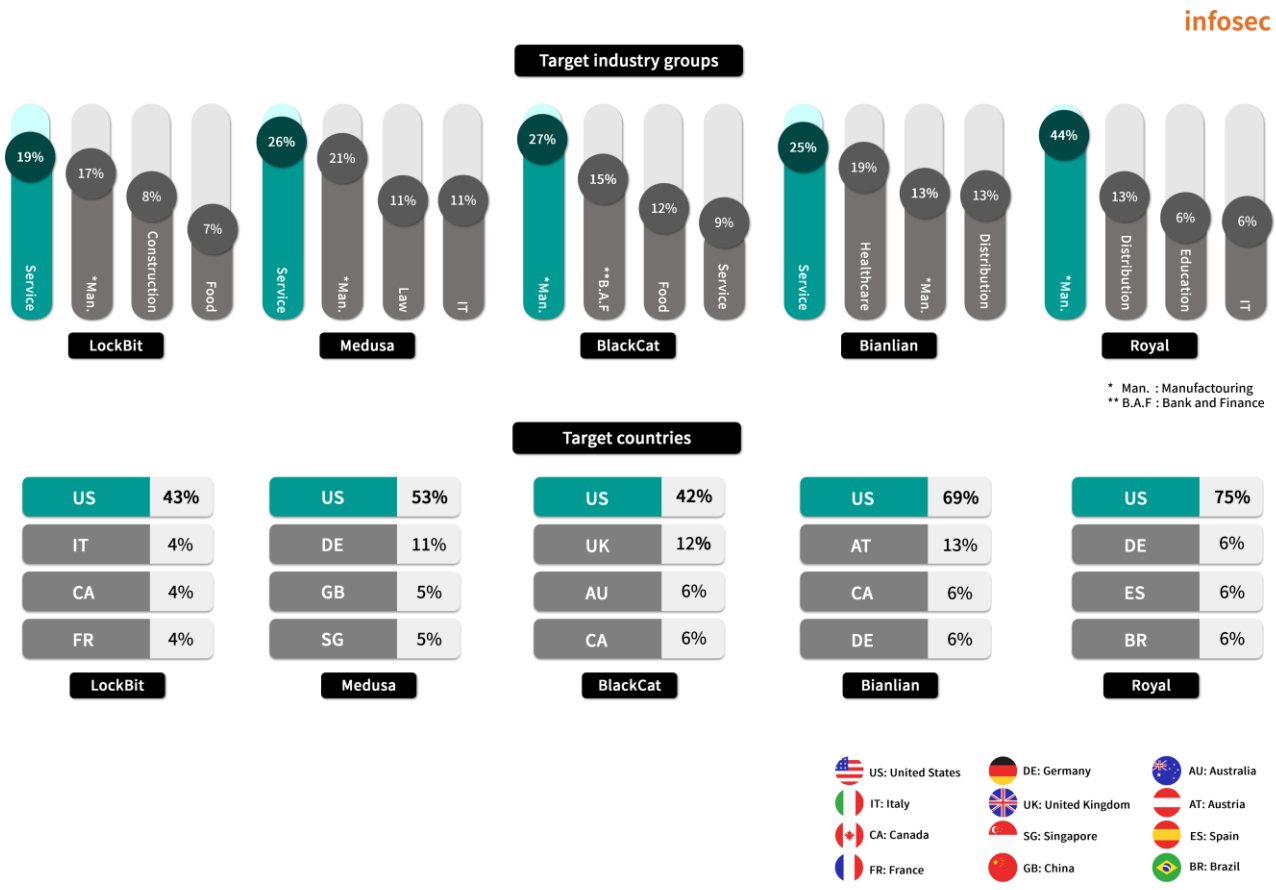
Many variants of the Stop and Chaos ransomware are appearing, and the DarkBit, Medusa, ESXiArgs, Nevada, DoDo, Kangaroo, 726, and Exfiltrator-22 ransomware are newly discovered. The DarkBit and Medusa ransomware are identified as groups that leak data through the dark web and use a double threat strategy. In particular, though it is a new group, the Medusa ransomware is causing a lot of damage: e.g. it posted a total of 19 victims through the dark web. In addition, large-scale damage cases continue to occur around the world, such as large-scale attacks by the ESXiArgs and Nevada ransomware targeting Linux and ESXi servers, and the discovery of Linux variants of the Royal ransomware. So the new threats require special attention.

## Top 5 ransomwares

Checking the number of ransomware damages, last February, a total of 134 attacks by the LockBit ransomware group, one of the existing ransomware groups, were confirmed. This is a significant increase compared to the previous month, and it is significantly higher than other ransomware groups. Also, it has become the biggest threat among RaaS as it increased the number of victims by the largest margin compared to the previous month.

Analyzing the Top 5 ransomwares, most ransomware attacks are still concentrated in the manufacturing and service industries. In particular, the BlackCat (Alphv) and the Bianlian ransomware group showed a high number of attacks targeting banking/finance and healthcare/pharmaceutical/welfare industries along with manufacturing and service.

Looking at the countries where there are victims to ransomwares active in February, including the Top 5 ransomwares, it was confirmed that the largest number of attacks targeted the US, and other attacks were distributed in unspecified countries.

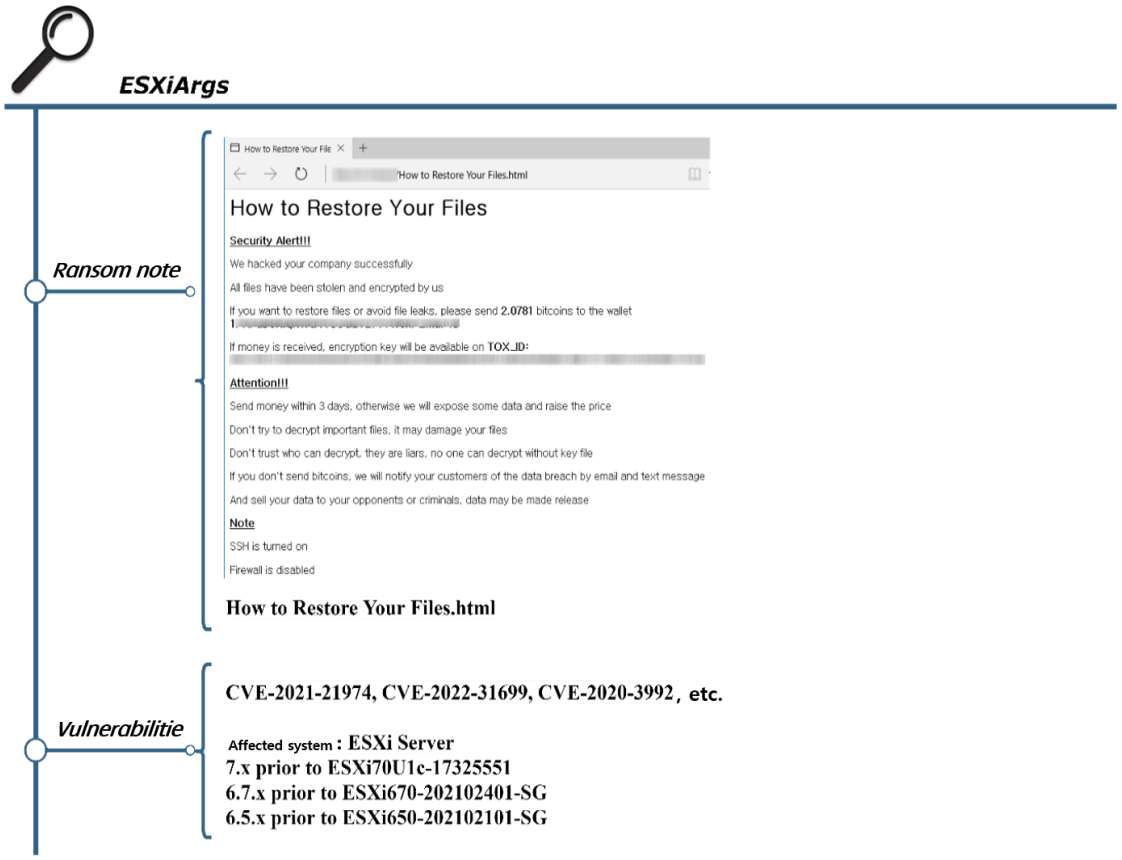


## ■ Focus of ransomware

### ESXiArgs ransomware

A ransomware attack targeting the ESXi server was discovered by CERT-FR (French Computer Emergency Response Team) in early February. This attack was made using the CVE-2021-21974 vulnerability of ESXi, and in February 2021 VMVMware released a patch that corrected the vulnerability. However, there are still many vulnerable ESXi servers to which patches have not been applied, resulting in large-scale infection cases, and as it is easy to look for them using open search services such as Shodan and Censys, attackers collected this information and used it for attacks. Looking at what has been revealed so far, in addition to the CVE-2021-21974 vulnerability, the possibility of using various vulnerabilities such as CVE-2022-31699[6] and CVE-2020-3992[7] cannot be ruled out.

The ESXiArgs ransomware encrypts files using the Sosemanuk encryption algorithm, and the algorithm used to be found in the CheersCrypt, PrideLocker, and Yanluowang ransomware designed for Linux, and as it is used in some derived ransomwares after the leakage of the Babuk ransomware code, it is presumed to have been written on the basis of the Babuk ransomware.




[6] Heap overflow vulnerability in VMware ESXi OpenSLP

[7] Remote code execution vulnerability due to use-after-free in VMware ESXi OpenSLPA

## ESXiArgs

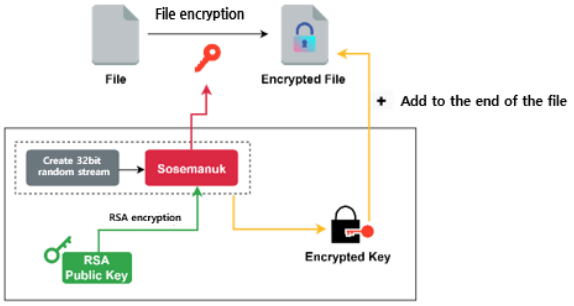
### Encryption

**encrypt.sh (ELF encryrptor loader) -----call-----> encrypt (ELF encryptor)**

```
"usage: encrypt <public_key> <file_to_encrypt> [<enc_step>] [<enc_size>] [<file_size>]");
"       enc_step    -   number of MB to skip while encryption");
"       enc_size    -   number of MB in encryption block");
"       file_size   -   file size in bytes (for sparse files)\n");
```

### Encryption key

Using the Sosemanuk stream encryption to encrypt the file, protecting it with the RSA public key, and add it to the end of the file.




### Encryption targets

.vmdk .vmx .vmxf .vmsd .vmsn .vswp .vmss .vmem .nvram

### Update

As the part excluded from encryption increases according to file size, CISA presented a method of restoring the setting file using this. Update is made so that the attacker skip only 1MB after checking it.

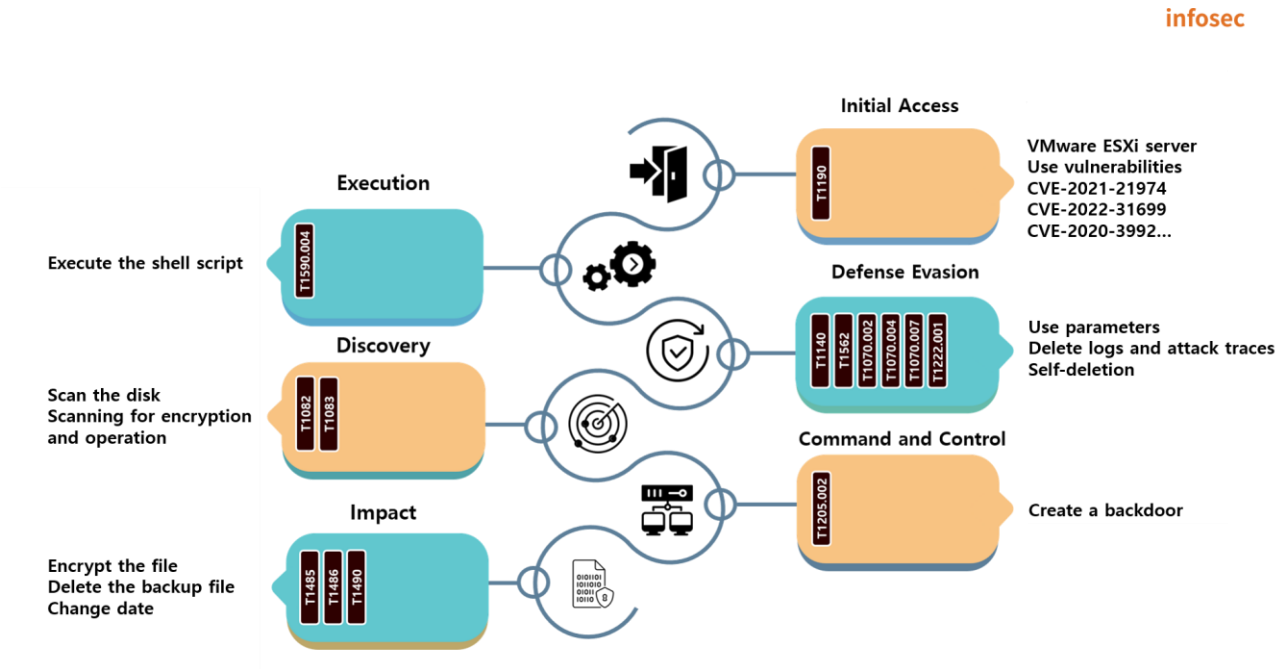
```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=0
if [[ $(($size_kb/1024)) -gt 128 ]]; then
  size_step=$((($size_kb/1024/100)-1))
fi
```

```
size_kb=$(du -k $file_e | awk '{print $1}')
if [[ $size_kb -eq 0 ]]; then
  size_kb=1
fi
size_step=1
```

### Characteristics

- Sosemanuk algorithm
- Encryption key protection (RSA)
- Partial encryption
- Delete logs, files used for the attack, backup, scheduler and network traces
- vmtools.py python script backdoor
- ESXi vulnerabilities

ESXiArgs ransomware strategy




The ESXiArgs ransomware attempts an attack targeting a vulnerable server among ESXi servers through open information. After searching the ESXi server through the open search service, it attempts the first penetration into the unpatched server using the remote code execution or authentication bypass vulnerability. After selecting the encryption target through the shell script and ELF file, it used the Sosemanuk algorithm to encrypt it, and the used encryption key was encrypted with the RSA public key for protection.

The ransomware uses the partial encryption strategy, i.e. encrypting only part of the file to perform encryption quickly. As the size of the file increases, the non-encrypted part increases. In particular, since there are many large files due to the nature of the virtual environment, CISA has released a script that can be run normally through environment setting restoration. When the issue of partial encryption occurred, the attacker responded immediately, modified the shell script, and used it for the attack. It can be seen that the attacker behind the ESXiArgs ransomware is responding quickly through monitoring, and periodically performing large-scale attacks targeting vulnerable servers late at night when immediate response is difficult.

A backdoor written in Python was also found on the server where the ESXiArgs ransomware was discovered. The backdoor executes the transmitted command or executes a Reverse shell[8] to connect to the designated host and port. In other words, it is not continuously executed, but when all encryption work is finished, it is deleted along with the log file, backup file traces of attack, etc. to avoid detection.

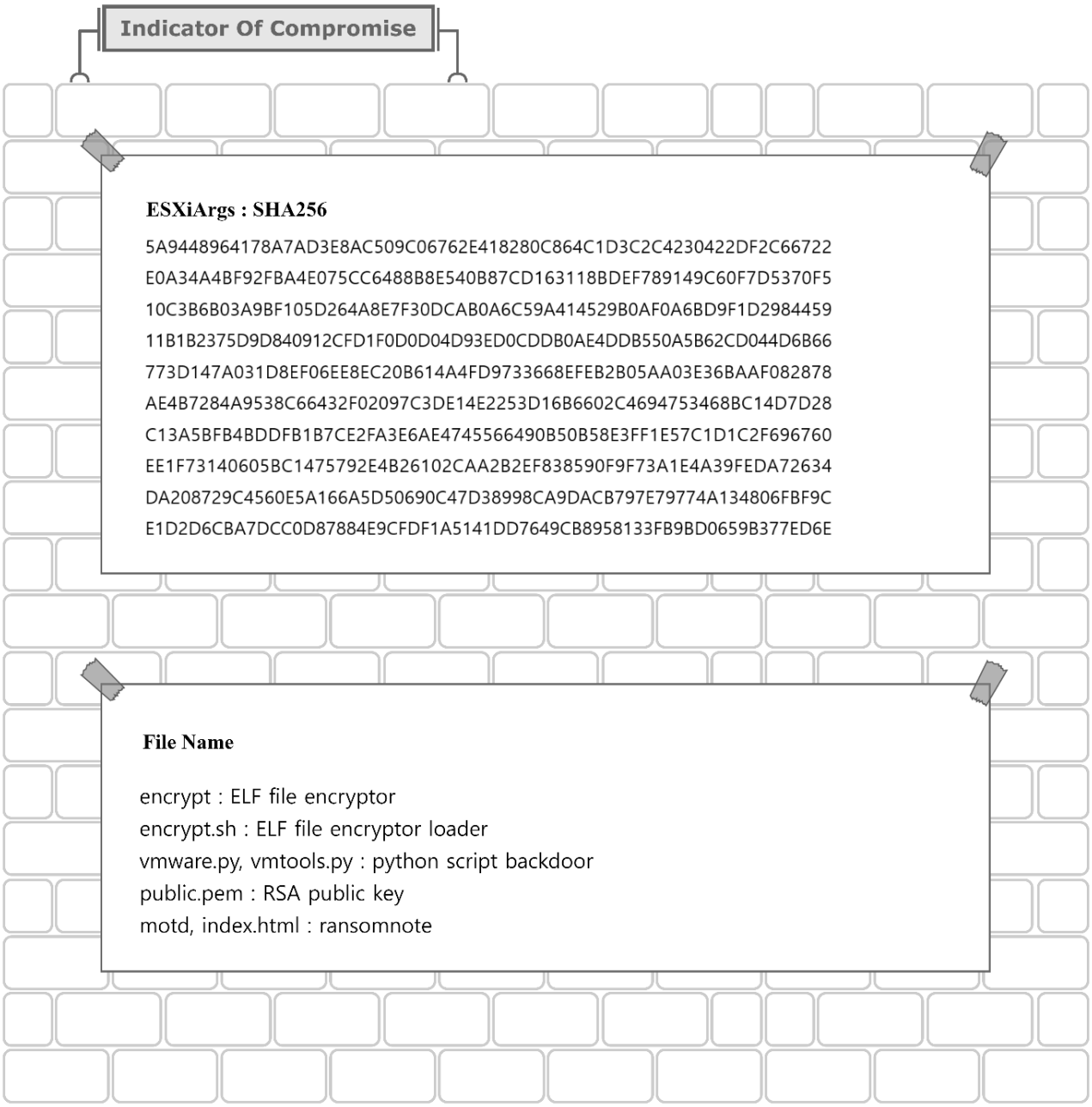
Lastly, the ESXiArgs ransomware does not operate a dark web site and guides you to contact by providing a Bitcoin address and Tox Chat[9] ID. Rather than performing sophisticated attacks, it uses an easy approach, i.e. using known vulnerabilities to attack unpatched servers. In addition, considering that it is presumed to be a ransomware based on the leaked Babuk ransomware and that it does not use a dual threat strategy, it seems that it has chosen a strategy to secure many unspecified infected servers and make financial gains.

As it uses known vulnerabilities to attack, if you are using the VMware ESXi server, you must apply the latest patch and disable the SLP service. In addition, it is necessary to take action on the ESXi server so that it is not exposed to the outside.

[8] A form in which the target maintains the received state and the attacker accesses the target

[9] A messenger that supports end-to-end encryption

## ■ IoC


Indicator Of Compromise
ESXiArgs : SHA256
5A9448964178A7AD3E8AC509C06762E418280C864C1D3C2C4230422DF2C66722
E0A34A4BF92FBA4E075CC6488B8E540B87CD163118BDEF789149C60F7D5370F5
10C3B6B03A9BF105D264A8E7F30DCAB0A6C59A414529B0AF0A6BD9F1D2984459
11B1B2375D9D840912CFD1F0D0D04D93ED0CDDB0AE4DDB550A5B62CD044D6B66
773D147A031D8EF06EE8EC20B614A4FD9733668EFEB2B05AA03E36BAAF082878
AE4B7284A9538C66432F02097C3DE14E2253D16B6602C4694753468BC14D7D28
C13A5BFB4BDDFB1B7CE2FA3E6AE4745566490B50B58E3FF1E57C1D1C2F696760
EE1F73140605BC1475792E4B26102CAA2B2EF838590F9F73A1E4A39FEDA72634
DA208729C4560E5A166A5D50690C47D38998CA9DACB797E79774A134806FBF9C
E1D2D6CBA7DCC0D87884E9CFDF1A5141DD7649CB8958133FB9BD0659B377ED6E
File Name
encrypt : ELF file encryptor
encrypt.sh : ELF file encryptor loader
vmware.py, vmtools.py : python script backdoor
public.pem : RSA public key
motd, index.html : ransomnote

## ■ Reference sites


URL: https://www.cisa.gov/uscert/ncas/alerts/aa23-039a

URL: https://www.vmware.com/security/advisories/VMSA-2021-0002.html

URL: https://www.vmware.com/security/advisories/VMSA-2022-0030.html

URL: https://www.vmware.com/security/advisories/VMSA-2020-0023.html

URL: https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

URL: https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

URL: https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/

URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-targets-systems-in-the-us/

URL: https://therecord.media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware/

URL: https://www.bleepingcomputer.com/news/security/north-korean-ransomware-attacks-on-healthcare-fund-govt-operations/

URL: https://www.bleepingcomputer.com/news/security/us-and-uk-sanction-trickbot-and-conti-ransomware-operation-members/

URL: https://www.bleepingcomputer.com/news/security/linux-version-of-royal-ransomware-targets-vmware-esxi-servers/

URL: https://www.bleepingcomputer.com/news/security/new-nevada-ransomware-targets-windows-and-vmware-esxi-systems/

URL: https://www.bleepingcomputer.com/news/security/new-exfiltrator-22-post-exploitation-kit-linked-to-lockbit-ransomware/

URL: https://www.bleepingcomputer.com/news/security/new-mortalkombat-ransomware-decryptor-recovers-your-files-for-free/