KARA
Korea Anti Ransomware Alliance

2024.3Q

KARA ransomware trend report

KARA Ransomware Trend Report

Ho-seok Lee, Min-su Jung, Hyo-je Jo, Hyun-ah Lee / EQST Lab Team

Ransomware Trends

1. Insight for the 3rd quarter

TREND

- **Embargo :** Cloud compromise via Active Directory directory
- **RansomEXX :** Attack exploiting the Jenkins vulnerability (CVE-2024-23897)

THREAT

- Top 5 ransomwares in Q3: RansomHub, Play, LockBit, Meow, Hunterse
- Conti-based ransomware: Meow, Mimic, Monti, BlueSky, Putin, ScareCrowe

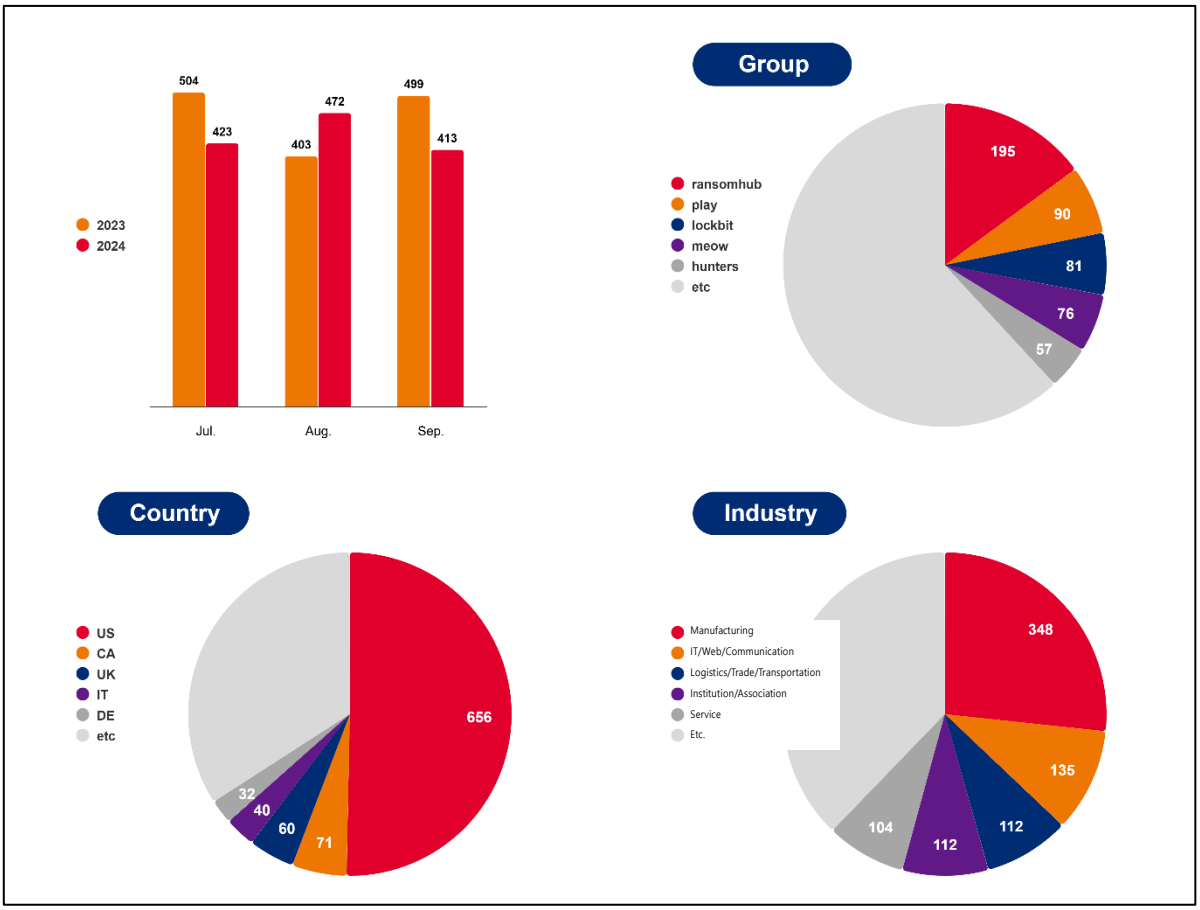
EXPLOIT

- **0-day :** CVE-2024-23897, CVE-2024-40766
- **1-day :** CVE-2023-48788

TARGET

- Initial access using the FortiEMS, Jenkins and SonicWall vulnerabilities
- Manufacturing accounts for 26% of all attacks, and the US accounts for 50%.

2. Q3 ransomware activity statistics



[Ransomware group activities]

The number of cases of ransomware damage in the third quarter of 2024 was 1,314, which is approximately a 7% decrease compared to the same period last year and a 3% decrease quarter-on-quarter. This appears to be because attackers either stopped their activities due to the psychological pressure of punishment and persistent investigations by law enforcement agencies or had their infrastructure confiscated, leading to a decrease in the number of attacks. In particular, SiegedSec, a hactivist group, ended its activities due to fear of pressure from investigative authorities, while the ransomware group Dispossessor was shut down after its infrastructure was seized. The seized infrastructure included 24 servers and 9 domains, and the FBI's investigation concluded that the group had attacked a total of 43 companies. This quarter, most ransomware attacks were against the US and manufacturing industries overall, with RansomHub recording the largest number of damage cases.

Although incidences of damage appear to have decreased slightly, ransomware attackers are continuing their attacks using advanced strategies in the third quarter. In particular, the RansomHub group, which has been the most active recently, has used EDRKillShifter to gain initial access by exploiting a spear phishing or

Zerologon[1] vulnerability, and then neutralize EDR solutions to evade detection by utilizing the bring your own vulnerable driver (BYOVD)[2] technique. The RansomHub group has been the most active since LockBit's influence diminished, and has taken over the ransomware ecosystem by providing ransomware-as-a-service and acquiring many affiliates such as the Scattered Spider group and Noname group.

Meanwhile, the Play ransomware group, although not an RaaS group, has been consistently creating many victims, and has recently expanded its attack range by releasing a variant targeting ESXi. The domain used to host this variant is associated with an attacker called Prolific Puma and also contains legitimate tools previously used by the Play ransomware group, such as PsExec, NetScan, and WinSCP, which are used in attacks to evade detection.

Although the LockBit group has become less active than before due to the arrests of members, pressure from investigative agencies, and departures from affiliates, it still poses a threat. As the LockBit group's threat level and influence grew, ransomware that copied it or used builders leaked by the group was steadily discovered. NotLockBit ransomware, discovered in October 2024, uses the same desktop image as LockBit 2.0 and targets macOS. NotLockBit ransomware, developed as a copycat of LockBit, is written as x86-64-based binaries rather than ARM binaries that run on Apple Silicon MacOS, so it only infects MacOS that uses Intel CPUs or MacOS that uses Rosetta. Although there is no evidence of this ransomware being distributed to date, it suggests that MacOS, which was perceived as relatively safer than Windows or Linux, is also being targeted by ransomware attacks.

The Meow ransomware group uses a ransomware variant created using the leaked source code of the Conti ransomware group. It started its activities in August 2022 and disappeared for a while in March 2023 when a decryption tool was released. The group started posting victims after launching a data breach site in November 2023, and the number of victims increased significantly every month, establishing Meow as a threatening ransomware group. On dark web leak sites, it lists prices based on the value of the information.

Hunters International group is a group based on Hive ransomware, and it recently started attacks using SharpRhino RAT (remote access trojan). SharpRhino built a website using a typosquatting[3] domain, which is a modified version of a normal domain, in order to exploit user typos. When a user accesses the domain, he/she finds malware disguised as a legitimate open source program, Angry IP Scanner, and downloads and runs it. The malware, signed with a valid certificate, appears to be a legitimate program, allowing it to bypass security solutions and resides on the system and performs malicious activites without raising suspicion from the user. As this demonstrates, ransomware groups are increasingly adopting a strategy of using malware

---

[1] Zerologon: A vulnerability in Netlogon, an authentication protocol for Microsoft Windows and Samba

[2] BYOVD: An attack technique that exploits vulnerabilities in drivers signed with trusted certificates

[3] Typosquatting: A technique of changing a normal URL name and then registering it so that users will be directed to the website when entering the domain incorrectly

such as infostealers and RATs in their attacks.

3. Ransomware trends

✓ Ransomware attacks targeting cloud environments

As enterprises increasingly adopt the cloud computing, hybrid clouds that have both the security of on-premises[4] and the flexibility of the cloud are attracting attention. As these changes are increasingly moving companies' core assets and data to the cloud, cyber attackers' targets are naturally expanding from within the company to the cloud environment.

The attack group distributing the Embargo ransomware recently breached a specific company, stole internal account information, took control of system through lateral movement, used the account information to compromise the company's cloud environment, and then stole the information. Based on the account information stolen from inside, the attack group appears to have abuse the Microsoft Entra Connect Sync[5] service, which synchronizes passwords between the on-premises Active Directory and Entra IDs in the cloud, and then accessed the cloud service. In addition, the attack group found an account without multi-factor authentication using an account they had stolen in the system, and used it to access the company's cloud environment to perform the attack.

In addition to attacks exploiting stolen account information, there have also been instance of ransomware attacks that compromise web service environments. Due to a configuration error by an AWS (Amazon Web Services) service user, an .env file, which is an environment configuration file, was exposed to the outside. Using this file, the attacker collected AWS IAM (identity and access management)[6] access keys without authorization, accessed the hosted cloud service, took control of the system, and distributed ransomware.

✓ Exploitation of vulnerabilities by ransomware groups

Attacks exploiting vulnerabilities continued in the third quarter. The Medusa ransomware group has exploited the CVE-2023-48788 vulnerability, which allows them to execute arbitrary commands on the FortiClientEMS[7] system, while the RansomEXX group has exploited the CVE-2024-23897 vulnerability. The CVE-2024-23897 vulnerability, disclosed in January 2024, allows for the reading of files within the system due to incorrect

---

[4] On-premise: A method in which a company owns its own servers and operates its own cloud

[5] Microsoft Entra Connect Sync: The tool that connects and synchronizes the on-premises Active Directory with a Microsoft Entra ID

[6] AWS Identity and Access Management: The service that manages access permissions for users and groups to AWS resources

[7] FortiClientEMS: Fortinet's FortiClient central management console program

argument handling during the command parsing process in Jenkins, a software build and distribution automation system. On August 1, the RansomEXX group exploited the Jenkins vulnerability to infiltrate Brontoo Technology Solutions, a banking service technology provider, and spread ransomware, which resulted in a payment interruption at a bank in India that was using Brontoo's solution.

CVE-2024-40766, the vulnerability in SonicWall products revealed in August 2024, was also used in the attack. This vulnerability allows unauthorized access due to improper access control on SonicWall SonicOS Management Access and SSLVPN[8] equipment. The Akira ransomware group, which was carrying out attacks using the CVE-2023-27532 vulnerability last quarter, has been found to be carrying out attacks using a vulnerability in SonicWall products.

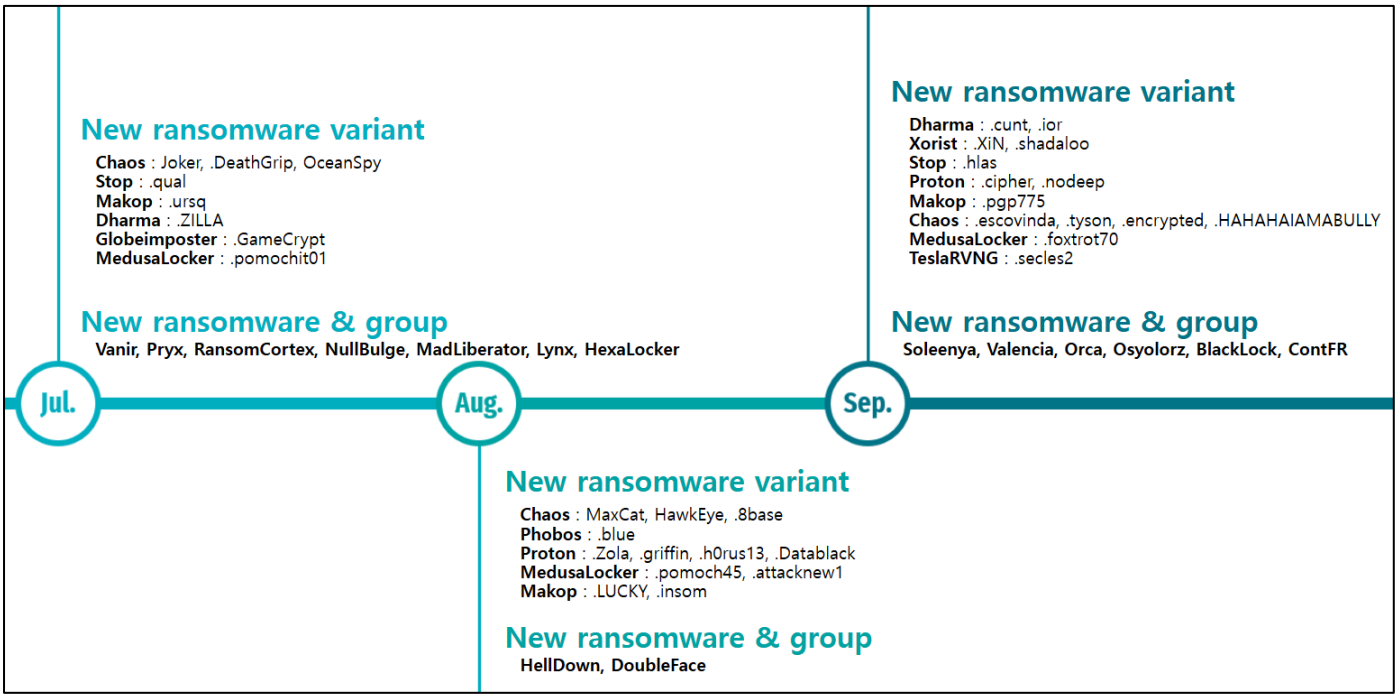
CVE	Attacker	Description	Affected versions
CVE-2023-48788	Medusa	An attacker could have executed remote code using the xp_cmdshell function through an SQL Injection attack.	FortiClientEMS 7.0.1 - 7.0.10, 7.2.0 - 7.2.2
CVE-2024-23897	RansomEXX	An attacker could read a file by replacing the @ character with the contents of the file during the CLI[9] command parsing process.	Jenkins (< 2.441) LTS 2.426.2
CVE-2024-40766	Akira	Attackers could gain unauthorized access from SonicWall SonicOS Management Access and SSLVPN.	SOHO Gen 5 (<5.9.2.14-13o) Gen6 Firewalls (<= 6.5.4.14-109n) Gen7 Firewalls (<= 7.0.1-5035)

[List of vulnerabilities exploited by ransomware groups in Q3]

[8] SSLVPN: A virtual private network technology that provides secure communication by providing an encrypted tunnel for remote access over the Internet

[9] CLI: Stands for command line interface and is used for command line execution.

4. New ransomware and group activities



[New/variant ransomwares]

In Q3, 15 new ransomware groups were discovered.

The NullBulge ransomware group, which emerged in July, targets AI-centric applications and the gaming community. They spread malware through fake developer accounts, and recently claimed that they had leaked more than a terabyte of data from Disney's internal Slack[10] channel. Currently, NullBulge's website is temporarily closed.

HexaLocker is a new ransomware group run by the former administrator of the LAPSUS$ group. It exfiltrates file attacks using ransomware written in Golang and extorts money under the pretext of encrypting files and disclosing stolen data. However, the group recently announced over its Telegram channel that it would be withdrawing its affiliation with groups such as LAPSUS$ and that it would cease its activities, revealing that it was selling the source code of the HexaLocker and LAPSUS$ ransomware.

HellDown, a new ransomware group discovered in August, announced itself by posting 17 victims in just 10 days after starting its activities, but has been inactive since August 24. The Doubleface ransomware group, which began its activities by opening a Telegram channel on August 5, has formed partnerships with various ransomware groups and is carrying out ransomware distribution and website defacement attacks.

A total of six new ransomware groups were discovered in September. Within these groups, the Soleenya

[10] Slack: Cloud-based collaboration tools and messengers for intra-enterprise collaboration

ransomware based on LockBit 3.0 and the Orca ransomware based on the ZEPPELIN ransomware are examples of leveraging existing ransomware. Below is a description of the major ransomware groups discovered in Q3.

- **Lynx**

  The Lynx ransomware group, which began operations in July, has disclosed more than 20 victims on its data breach site. It has targeted a variety of industries including retail, real estate, construction, and finance across North America and Europe, and has been consistently active so far. The Lynx ransomware encrypts files using the AES-128 algorithm and Curve25519,[11] and adds .lynx extensions to encrypted files. In addition, depending on the argument when running, a print-related function operates, and if the option is activated, this ransomware finds a printer device connected to the infected system and outputs a ransom note.

- **Vanir**

  The Vanir ransomware group, a new group that emerged in July 2024, has revealed three companies on its data breach site. The group's dark web data leak site is structured to resemble the Akira ransomware group's command-line tool-style interface, leading some to suspect that it has ties to the Akira Group, but it could also simply be a copycat. BlackEyedBastard, who operated the Vanir group, has been advertising that they are a former affiliate of ransomware groups such as Karakurt, LockBit, and Knight, and that they are looking for affiliates for their ransomware service. However, their data leak site was shut down by German law enforcement authorities in September, and since then, no further activity has been detected.

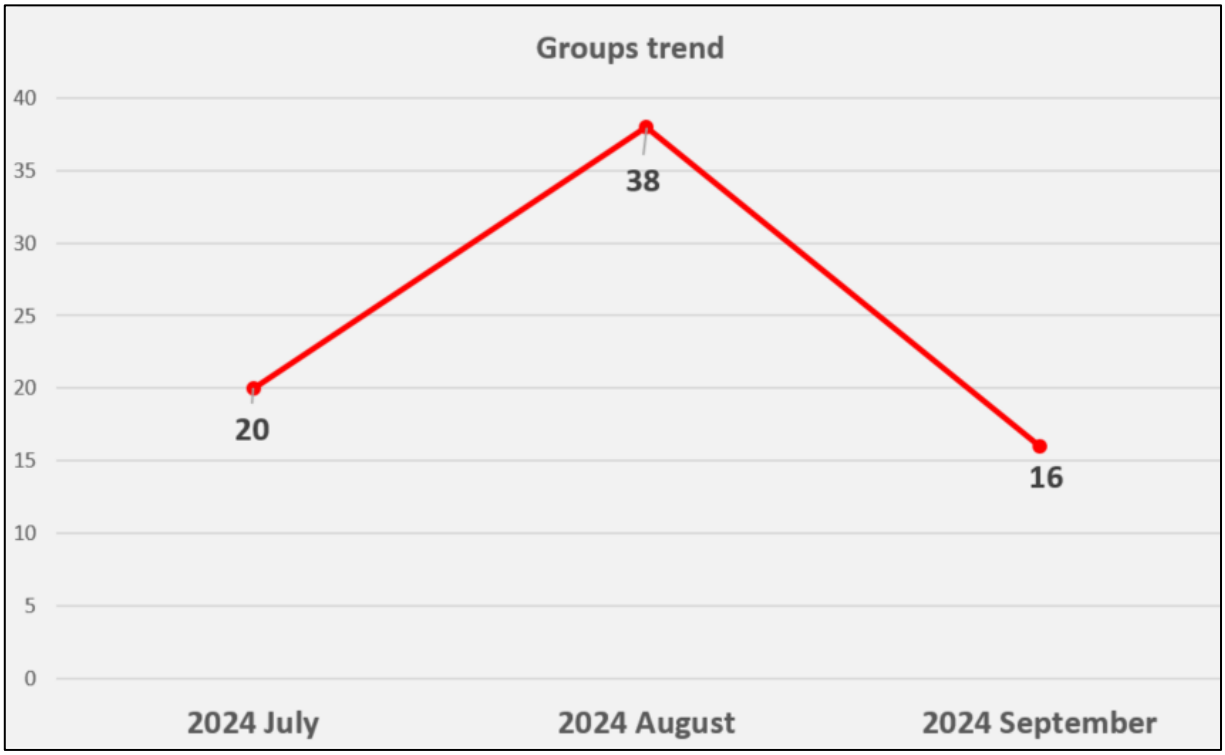
- **RansomCortex**

  The RansomCortex group began its activities on July 11, 2024, when it revealed its first victim on a data breach site. Interestingly, in an interview with one media outlet, a member of RansomCortex stated that they have a rule of not attacking the CIS, Iran, North Korea, China, or police stations, and that their main targets are hospitals that handle the most sensitive and important data and speak English, Italian, Spanish or Portuguese. The RansomCortex group said it exploits vulnerabilities, but also works with a range of experts to gather information and carry out attacks on its own.

[11] Curve25519: Elliptic curve-based asymmetric key encryption algorithm that supports high speed and security

■ Detailed Analysis of the Meow Ransomware Group

1. Overview of Meow



[Number of attacks by the Meow ransomware group in Q3]

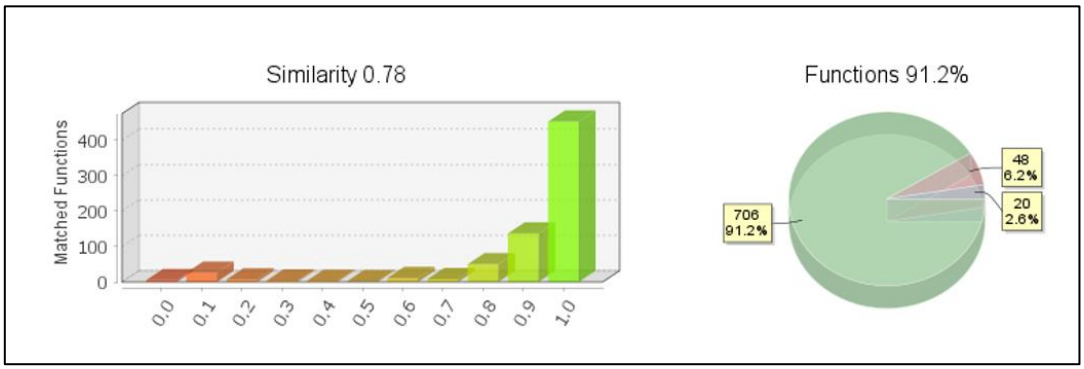
In March 2022, there was an incident where the source code of the Conti ransomware was leaked. Following the Russian invasion of Ukraine, a Russian-based cybercrime group called the Conti group released a pro-Russian message, and in retaliation, a Ukrainian researcher leaked messages from the chat server of the Conti group and the Ryuk ransomware gang, as well as ransomware materials including ransomware decryptors, builders, etc.

The source code was leaked, and attackers carried out various attacks by developing and distributing new variants of ransomware based on it.

Ransomware	Extension	Date of discovery
Mimic	.QUIETPLACE	2022-06
Monti	.monti	2022-06
Meow	.meow	2022.09 -
BlueSky	.bluesky	2022-06 -
Putin	.PUTIN	2022-08 - 2022-11
ScareCrow	.CROW	2022-11

[Ransomware derived from Conti]

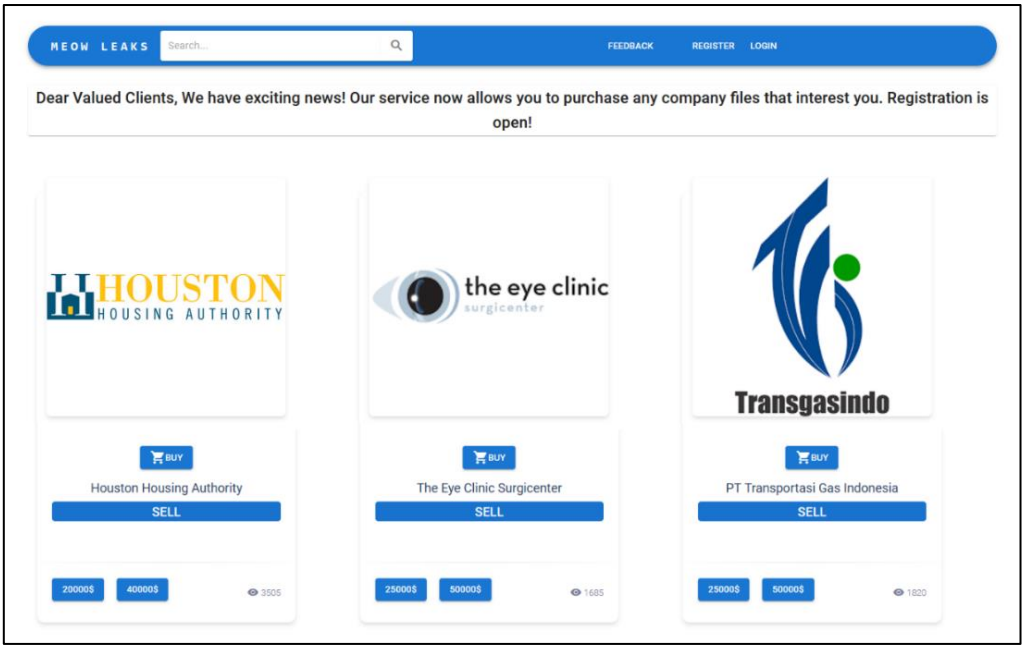
The Meow ransomware is one of the variants developed with the leaked Conti source code, and it was launched in August 2022, around the same time as other variants. Since then, it has been actively used to carry out various attacks, and infecting approximately 257 victims.



[Similarities between the Meow ransomware and the Conti ransomware]

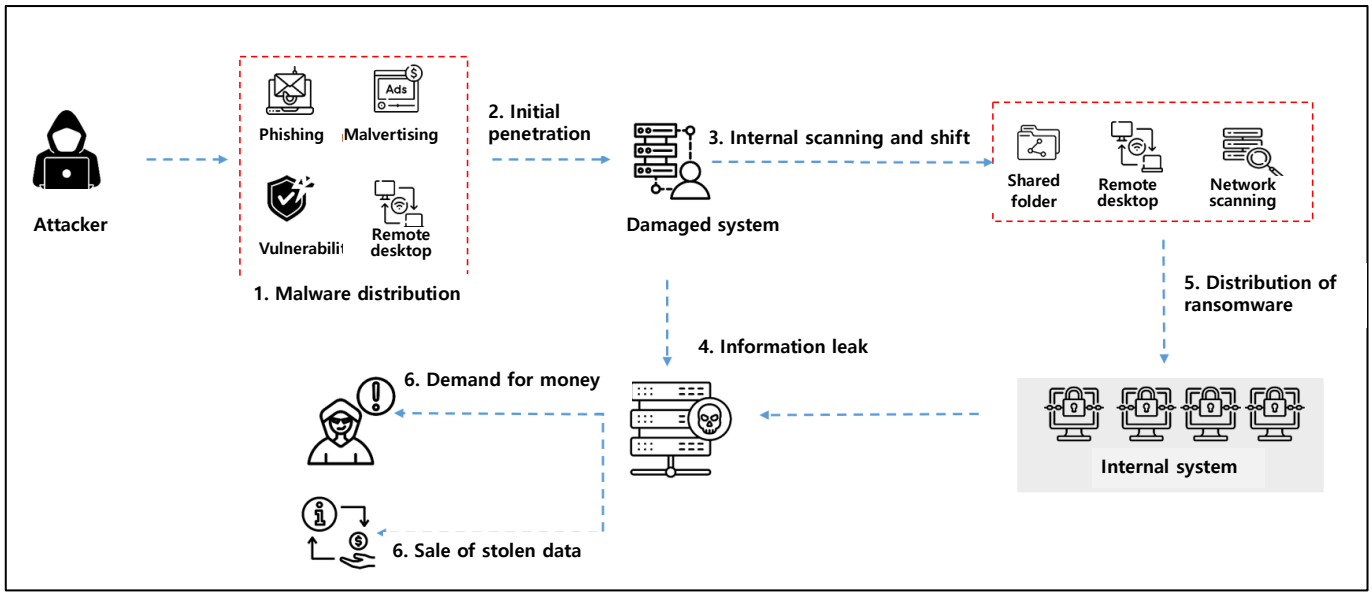
Around February 2023, the Meow ransomware group announced on their forums that they were ceasing activities and released all their private keys and decryption tools. Kaspersky developed and distributed a decryption tool based on this data, and the Meow group has since ceased its activities. Kaspersky, which developed and distributed a decryption tool by analyzing publicly available information, said that approximately 257 groups or individuals were compromised and 14 victims appear to have paid the ransom.

After a period of dormancy, the Meow ransomware group resumed its activities in November 2023 by posting Vanderbilt University Medical Center on a dark web data leak site. Since resuming operations, their attack methods have shifted from encrypting files through ransomware to focusing on data leaks. The Meow ransomware group compromises systems, exfiltrates sensitive information, deploys ransomware, and subsequently extorts victims for financial gain. If negotiations fail, the group resorts to selling the stolen data on the dark web .



[Meow ransomware's data leak site]

2. Meow ransomware attack scenario



[Meow ransomware attack scenario]

Meow ransomware attackers use various methods to achieve initial access, but mainly the following four:

The first method is a malvertising[12] attack. In this method, the attacker attacks an advertising site, injects malicious scripts, and then exploits vulnerabilities to penetrate the company's system when the advertisement is displayed. Unlike spear phishing,[13] which has a specific target, these attacks target an unspecified number of people. If a user infected through this vulnerability is a company that can be significantly affected by ransomware attacks, the attacker performs additional access.

The second is a classic attack using phishing emails. The attacker sends an email with a malicious link attached to a company's public email address, and when the user clicks or downloads the file, the malware is executed, infecting the system. The attacker then makes the initial access.

The third attack method is an attack that exploits vulnerabilities. Attackers use vulnerabilities in servers or services that have access to the Internet to install malicious scripts and then perform initial access.

Lastly, the attacker gains initial access using an RDP (remote desktop protocol), a remote connection. The attacker gains access to the company by obtaining RDP account information of the company that is known to the outside world or sold on the dark web, or infiltrates the company through publicly disclosed remote access vulnerabilities.

After the initial access, the attacker scans the internal network, manipulates files in remote shared folders, exploits the remote connection system of the internal system, etc., to take control of the entire system. The attacker then steals important information from the infiltrated network, transfers it to the attacker's C2, distributes the Meow ransomware to perform encryption, and then demands money.

3. In-depth analysis of the Meow ransomware

✓ Functional analysis

1) Analysis checklist

- Decryption of strings

When the Meow ransomware is executed, it encrypts all the strings required for malicious actions and uses them for malicious actions after decryption.

```
v26[66] = 96;
v26[67] = 95;
v26[68] = 31;
qmemcpy(v27, "_2_2_l_2_E_e_E_9_'_w___", sizeof(v27));
v28 = v7;
for ( i = 0; i < 0x5C; ++i )
  v26[i] = (11 * (95 - v26[i]) % 127 + 127) % 127;
```

[12] Malvertising: A technology for distributing malware by inserting it into advertisements

[13] Spear phishing: A type of phishing attack that targets specific individuals or groups

[String decryption logic]

```
#Decrypt routine 1
dec = ((((key1 - enc) * key2 ) % 0x7F) + 0x7F) % 0x7F
#Decrypt routine 2
dec = ((((enc - key1 ) * key2 ) % 0x7F) + 0x7F) % 0x7F
```

[Python code for string decryption]

- Dynamic API Resolution

The program reconstructs and uses the dynamic API table, and for this purpose, calls a specific function before calling the Windows API. The function returns the address if it exists at the API offset location in the received table. If there is no address stored, it searches for the API address using the 4-byte hash received at the same time, stores it in the table, and then returns it.

```
addr = *(g_api_table_43939C + 4 * a3);
v8 = addr + 6035901;
v4 = ((addr + 6035901) & 0x80000003) == 0;
if ( addr + 6035901 < 0 )
  v4 = ((((addr - 67) & 3) - 1) | 0xFFFFFFFC) == -1;
if ( v4 )
{
  do
    ++v8;
  while ( !(v8 % 4) );
}
if ( addr )
  return addr;
addr = GetApiAddr_4044B0(0, hash);
```

[String dynamic load]

2) Detailed functional analysis

- Setting up execution arguments

The ransomware stores a setting value for execution based on the arguments received when the program is executed at the initial execution stage. It retrieves the argument information received at the execution stage based on the function, compares it with the arguments, and then sets the execution flag. There are a total of five execution arguments, and the table below provides information on each option.

Set value	Description
-p	Perform encryption by specifying a specific directory
-m	Use with the local/net/all option to specify the files to be encrypted (local/network/all)

-size	Specify the chunk size for encrypting large files
-log	Specify a log file to store encryption information
-nomutex	Perform malicious behavior without Creating a Mutex[14]

[Ransomware execution parameters]

The string is decrypted to compare the received arguments.

```
v43[11] = 29;                                   // -log
LogFlag = CheckArgv_41C600(v5, NumberOfArgv, v44);
for ( m = 0; m < 0xC; ++m )
  v43[m] = (36 * (29 - v43[m]) % 0x7F + 127) % 0x7F;
v37 = 0;
v9 = CheckArgv_41C600(v36, NumberOfArgv, v43);
v38 = 16;
qmemcpy(v39, "BcBpBVB?B2BmBfBBB", 17);
v45 = v9;
for ( n = 0; n < 0x12; ++n )                    // -size
  v39[n - 1] = (39 * (66 - v39[n - 1]) % 0x7F + 127) % 0x7F;
v11 = v36;
p_NumOfArgv = NumberOfArgv;
```

[Decrypting strings to compare arguments]

- Setting up the ransom note

After encrypting files, the ransom note information that informs the user of the infection status and the public key to be used for encryption are copied to a specific memory area. The code that makes up the note of this ransomware is checked, the user's ransom note is inserted into a specific memory area, the remaining space is filled with 0s, and then it is copied it back to the memory area with the string "__DECRYPT_NOTE__." Also, the attacker's public key is copied to a specific area with the string "__public_key__."

```
memset_422210(&ransom_note[283], 0, 0x3EF1u);
memcpy_4228D0("__DECRYPT_NOTE__", ransom_note, 0x400Cu);
memcpy_4228D0("__public_key__", &pubkey_430E40, 0x1000u);
return 1;
```

[Copying the ransom note and public key]

[14] Mutex: Synchronization mechanism to prevent duplicate execution

- Creating the Mutex

The flags that are activated according to the -nomutex option among the arguments received when executing the program are checked. If the flag is not activated, a Mutex is created with the following name.

- Mutex Name: hsfjuukjzloqu28oajh727190

```
v35[16] = 123;
v35[17] = 22;
qmemcpy(v36, "s,V,EN4}", sizeof(v36));      // Decrypt Mutex Name
for ( i = 0; i < 0x1A; ++i )
  v35[i] = (15 * (v35[i] - 125) % 127 + 127) % 127;
CreateMutexA = GetApiAddress_4052D0(15, 0x20D8FA8C, 84);
v8 = CreateMutexA(0, 1, v35);                // v35 = "hsfjuukjzloqu28oajh727190"
WaitForSingleObject = GetApiAddress_4052D0(15, 0xE0C23134, 98);
```

[Setting up the Mutex]

- Deleting volume shadow copies

Windows systems provide volume shadow copies, which can save and restore a specific point in time. Since this feature allows the infected system to be restored, the ransomware deletes these volume shadow copies. WMIC is used to execute the "SELECT * FROM Win32_ShadowCopy" command to retrieve all recovery images in the system, then the command below is passed as an argument to the CreateProcess function to delete the images.

```
cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where
"ID='{[VOLUME_SHADOW_ID] }'" delete
```

[Command for deleting volume shadow copies]

- Encryption preparation phase

When the thread performing the encryption is executed, the public key of the malware for encryption is registered via CryptoImportKey. This value is used to encrypt the key and Nonce value used for file encryption.

```
memcpy_4228D0(ransom_pubkey, "__public_key__", 0x1000u);
p_hCrypt = hCrypt;
CryptImportKey = GetApiAddress_4052D0(16, 1892860132, 55);
if ( !CryptImportKey(p_hCrypt, ransom_pubkey, 0x1000, 0, 0, &v28) )
{
  v5 = GetApiAddress_4052D0(15, -1480703512, 71);
  v5(1);
}
```

[Creating a client ID]

- Encryption phase

After the attacker's public key is registered, encryption is performed by traversing the directory and checking the excluded directories and file names, the file extensions to be encrypted, etc. The directories and extensions that the ransomware does not infect are as follows:

Folder	Extension
tmp	.MEOW
winnt	.exe
temp	.dll
thumb	.lnk
$Recyce.Bin	.sys
$RECYCE.BIN	.msi
Boot	readme.txt
Windows	CONTI
Trend Micro	.bat
perflogs	

[Exclusions from encryption]

All files are encrypted except for the list of excluded directories and files. The CryptGenRandom function is used to generate a 32-byte encryption key and an 8-byte Nonce, and based on these values, the files are encrypted using the chacha8 encryption algorithm.

In order to efficiently encrypt the files, the ransomware checks the extensions and sizes of the files and performs encryption accordingly.

- Encrypting database files

The ransomware checks whether the file extension is a database file, and if so, encrypts the entire file without checking any other conditions. The malware checks the following database file extensions:

4dd	4dl	accdb	accdc	accde	accdr	accdt	accft	adb	ade
adf	adp	arc	ora	alf	ask	btr	bdf	cat	cdb
ckp	cma	cpd	dacpac	dad	dadiagrams	daschema	db	db-shm	db-wal
db3	dbc	dbf	dbs	dbt	dbv	dbx	dcb	dct	dcx
ddl	dlis	dp1	dqy	dsk	dsn	dtsx	dxl	eco	ecx
edb	epim	exb	fcd	fdb	fic	fmp	fmp12	fmpsl	fol
fp3	fp4	fp5	fp7	fpt	frm	gdb	grdb	gwi	hdb
his	ib	idb	ihx	itdb	itw	jet	jtx	kdb	kexi
kexic	kexis	lgc	lwx	maf	maq	mar	mas	mav	mdb
mdf	mpd	mrg	mud	mwb	myd	ndf	nnt	nrmlib	ns2
ns3	ns4	nsf	nv	nv2	nwdb	nyf	odb	oqy	orx
owc	p96	p97	pan	pdb	pdm	pnz	qry	qvd	rbf
rctd	rod	rodx	rpd	rsd	sas7bdat	sbf	scx	sdb	sdc
sdf	sis	spq	sql	sqlite	sqlite3	sqlitedb	te	temx	tmd
tps	trc	trm	udb	udl	usr	v12	vis	vpd	vvv
wdb	wmdb	wrk	xdb	xld	xmlff	abcddb	abs	abx	accdw
adn	db2	fm5	hjt	icg	icr	kdb	lut	maw	mdn
mdt									

[Database files to be encrypted]

The file extension is checked to determine if it is a disk image file. Disk images are usually large in size, so instead of performing a full encryption, partial encryption is performed for the sake of speed. The following is a list of extensions for disk image encryption.

vdi	vhd	vmdk	pvm	vmem	vmsn	vmsd	nvram	vmx	raw
qcow2	subvol	bin	vsv	avhd	vmrs	vhdx	avdx	vmcx	iso

[Disk image files to be encrypted]

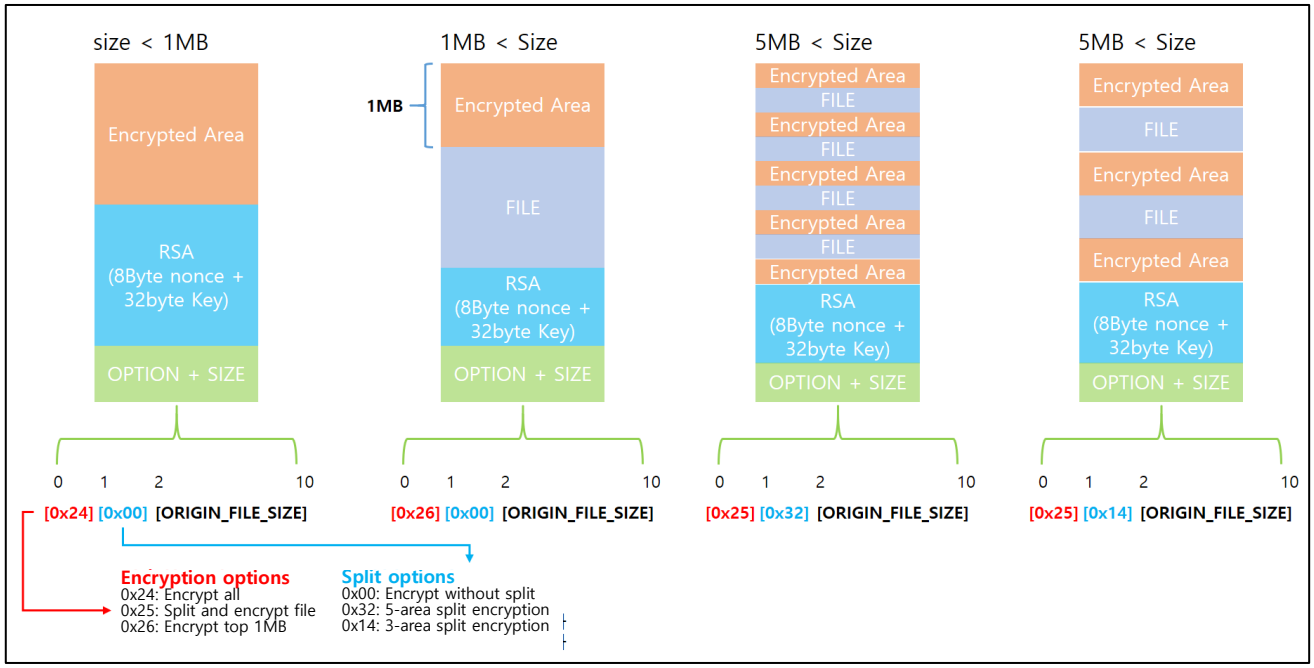
A coding error was identified in the logic that checks the extension to determine whether it is a disk image file. If the target file is a disk image file, the function should return 1 and proceed with partial encryption according to the file size. But, the ransomware is written to always return 0 after comparing the extensions within the function, so encryption proceeds according to the general file encryption logic instead of the disk image encryption logic.

```
    strstrIA = GetApiAddress_4052D0(22, -122749343, 23);
    if ( strstrIA(extension, target_extension[v22]) )
      break;
    ++v22;
  }
  while ( v22 < 20 );
  return 0;
}
```

[Returning 0 regardless of whether the extension is verified]

- Encrypting general files

If the file to be encrypted is neither a database file nor a disk image, encryption proceeds based on the file size. If the file size is less than 1MB, the entire file is encrypted. If the file size is more than 1MB, only the top 1MB is encrypted. If the file size is more than 5MB, the file is divided into five areas and partial encryption is performed. After the encryption is complete, the 32-byte Key and 8-byte Nonce value of chacha8 encrypted with the RSA algorithm is added to the end of the file. After that, the encryption (1 byte) and encryption area (1 byte) are set, then the size of the original file (8 bytes) is added to the end of the file and the encryption is finished.



[Encryption methods by option]

- Creating the ransom note

Once encryption is complete, a redeme.txt file is created in the directory and the ransom note is written.

```
"MEOW! MEOW! MEOW!  \n"
"\n"
" Your files has been encrypted! \n"
"\n"
" Need decrypt?  Write to e-mail: \n"
"\n"
" meowcorp2022@aol.com\n"
"\n"
" meowcorp2022@proton.me \n"
"\n"
" meowcorp@msgsafe.io \n"
"\n"
" meowcorp@onionmail.org\n"
"\n"
" or Telegram: \n"
"\n"
" @meowcorp2022 \n"
"\n"
" @meowcorp123 \n"
"\n"
" Uniq ID: 4d2942e6-49a6-410b-9a09-a02423f53e1c");
```

[Meow ransom note]

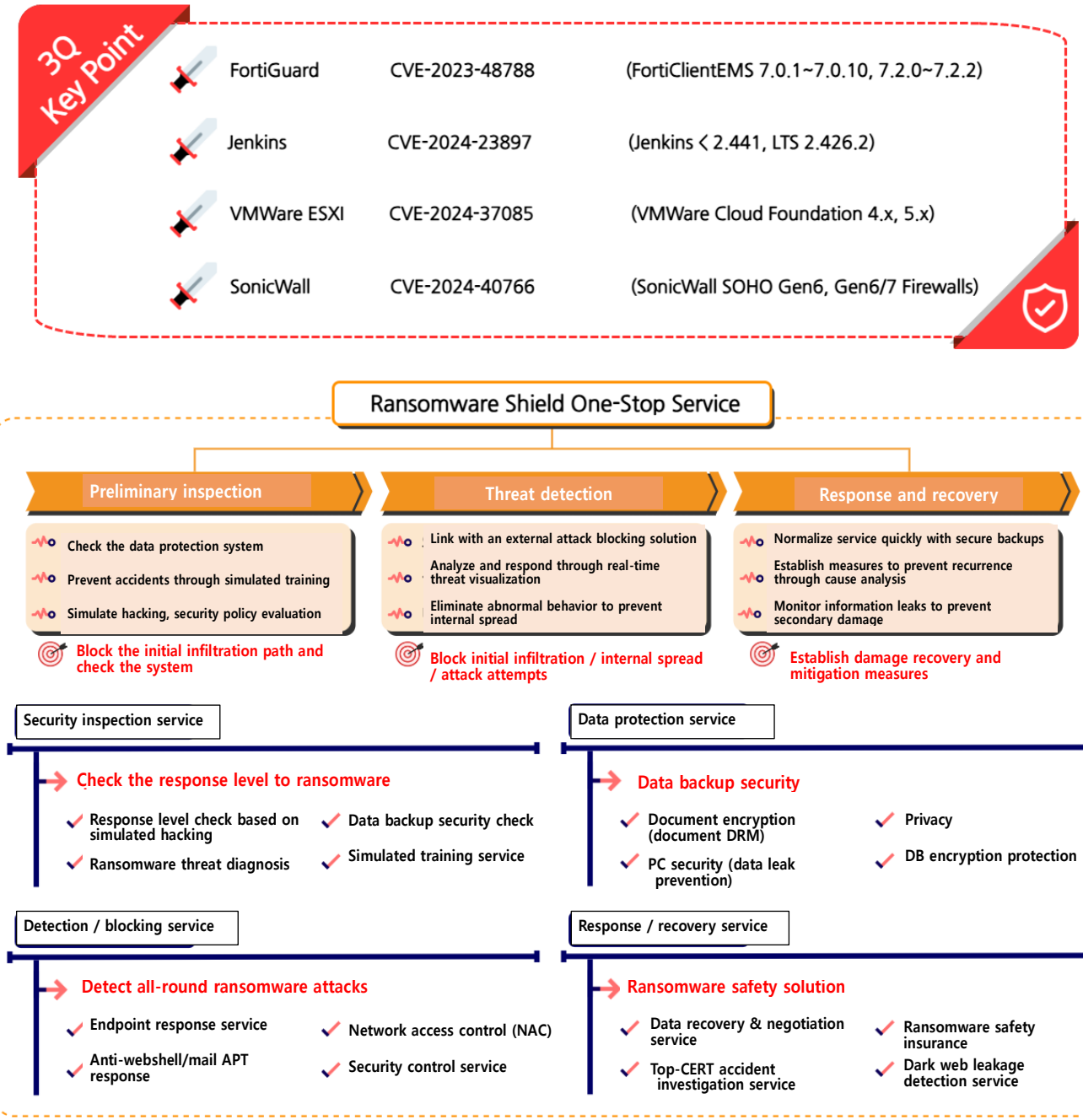
4. IoCs

SHA256
222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853
7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099
0856ab4ba1732ffb7c98fbdf806b3af41ad5015ae6cc08f1c1fbb72bf44de7d8
8ba84d65308e49007860e339dc93c1c4304e39755ba00a4cb4373bee7df37e0f
d7573284c29cf5f68bb64860f1be0a696c852678fac36f176fd88f555ed853f2

■ Ransomware Mitigation

1. Meow ransomware response guide

The Meow ransomware gains initial access through various attack routes such as phishing and malvertising, and then takes over the system through internal propagation using RDP and shared folders. In particular, since attackers sell important information on the dark web after it is leaked, it is important to be especially careful about the fact that additional damage may occur regardless of whether you pay the ransom. Therefore, companies should take proactive security enhancement measures, such as conducting thorough security management for systems with external contact points, performing continuous updates, disabling remote access services such as RDP, or applying strong security policies.



2. SK Shieldus MDR service

To respond professionally to ransomware, it may be effective to use SK Shieldus' managed detection and response (MDR) service.[15] Recent ransomware attackers are using sophisticated detection evasion techniques along with sophisticated strategies, making it difficult to escape threats with existing defense systems alone. As a solution to this, SK Shieldus provides an MDR service that can monitor networks in real time, detect

[15] MDR service: A managed security service that protects an organization from cyberattacks through real-time threat detection and response

abnormal signs, and respond immediately when necessary. Prevention is paramount in the case of ransomware attacks, but it is also very important to minimize damage through prompt action in the event of damage. Therefore, we recommend that enterprises consider SK Shieldus MDR service, which provides customized security solutions based on rapid and accurate incident investigation and analysis by a dedicated organization.

3. Features of SK Shieldus MDR service

Service details

01 Managed — Operated by EDR experts

- Receive and respond to control requests 24/7
- Update IoC and SK-defined rules
- Reflect policy operation and exception handling
- Analyze & respond to events

02 Detection — SK Shieldus detailed analysis service

- EDR/malware expert analysis service
- Support for malicious behavior tracking through EDR function
- Respond to true/false detection through detailed analysis
- Periodic threat hunting

03 Response — Insights into breach incidents

- Know-how from the analysis and investigation of the most breach incidents in Korea
- Check for signs of infringement
- Apply domestic IoC EDR first

EDR experts control service

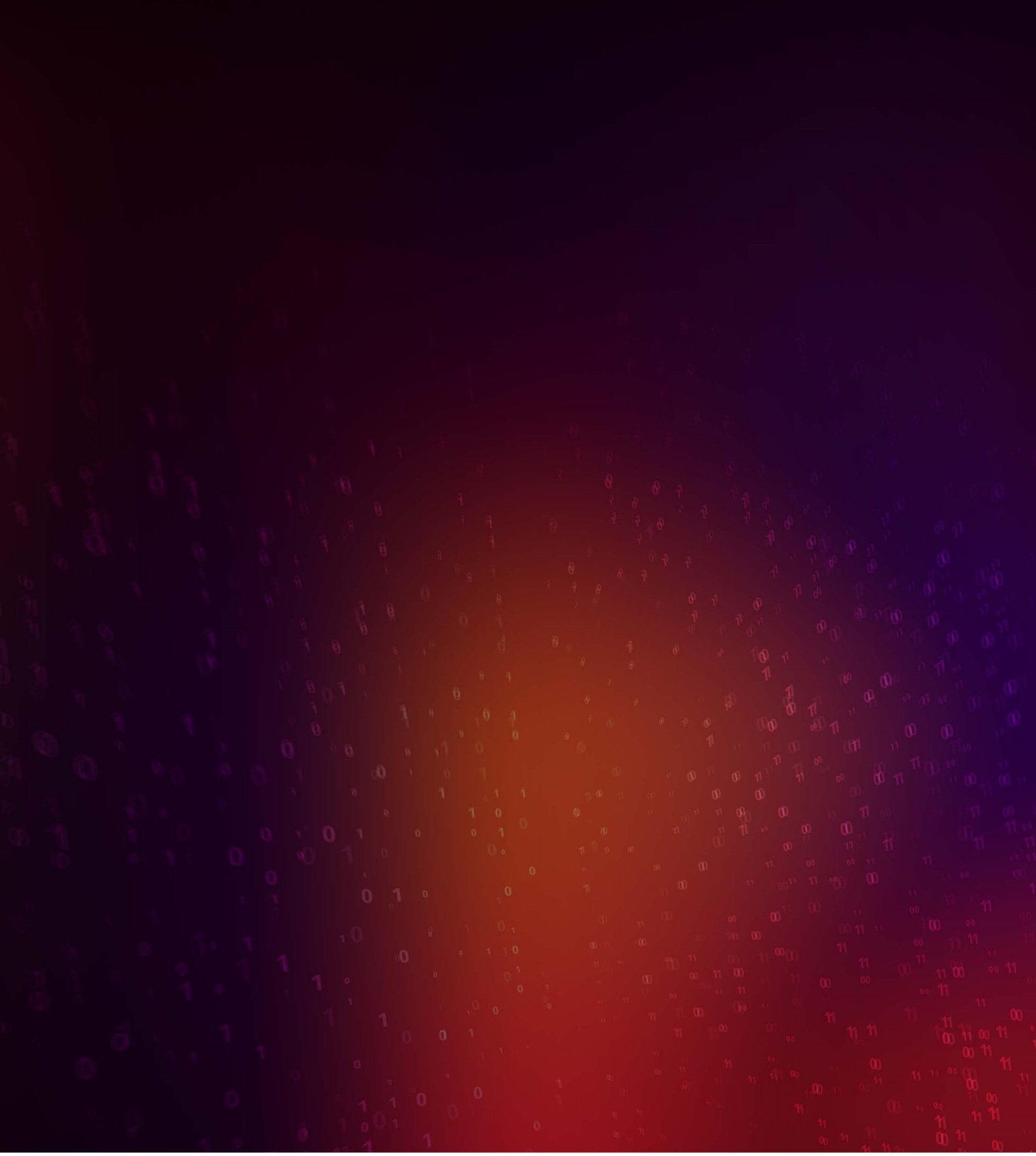
- ✓ **EDR experts control service**
  - Provide service to many customers
  - Respond to customer requests with references across various industries
- ✓ **Improved user satisfaction**
  - Rapid responses from experienced operational experts

Using expert service

- ✓ **TOP-CERT support**
  - 24/7 emergency responses
  - Rich experience in accident analysis and investigation
- ✓ **SK Shieldus security expert service**
  - Analyst experts on standby
  - Security experts analysis service (malware analyst + CERT)
  - Dedicated team for accurate/fast service

Highest level of security response in Korea

- ✓ **No information leak through the service**
  - Analysis of attachment on the company network
  - Support for a dedicated analysis environment
- ✓ **Strengthen proactive security threat response capabilities**
  - Work with customer security team to block the spread of threats



Technology for Everyday Safety | SK shieldus

23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea
https://www.skshieldus.com

Publisher : SK shieldus EQST/SI Solution Business Group & KARA (Korea Anti Ransomware Alliance)
Producer : SK shieldus Marketing Group