

2024.4Q

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.....	2
1. Q4 TREND	2
2. Q4 Ransomware Activity Statistics.....	3
3. Ransomware Trends	5
✓ Ransomware Attacks Targeting Healthcare Providers.....	5
✓ Active Operation of the RansomHub Group.....	5
✓ Clop Ransomware Attack Exploiting Cleo's Zero-Day Vulnerabilities.....	6
✓ Ransomware Attack Exploiting a New Vulnerability in Veeam Products	7
4. New Ransomware and Group Activities.....	8
■ Detailed Analysis of the Akira Ransomware Group	11
1. Overview	11
2. Akira Ransomware Attack Scenario.....	14
3. Analysis of Akira Ransomware	15
4. List of Files and Folders Subject to Encryption.....	19
5. IoCs	20
■ Ransomware Mitigations.....	21
1. Guidance for Mitigating Akira Ransomware	21
2. SK Shieldus MDR Service.....	22

■ Ransomware Trends

1. Q4 TREND

TREND

- Clop : Exploiting vulnerabilities in Cleo's systems (CVE-2024-50623, CVE-2024-55956)
- Akira : Exploiting vulnerabilities in Veeam's products (CVE-2024-40711)

THREAT

- Q4 Top 5 Ransomware: RansomHub, Akira, Play, KillSec, FunkSec
- Akira Ransomware: C++/Rust 기반 Akira v1/v2, Megazord

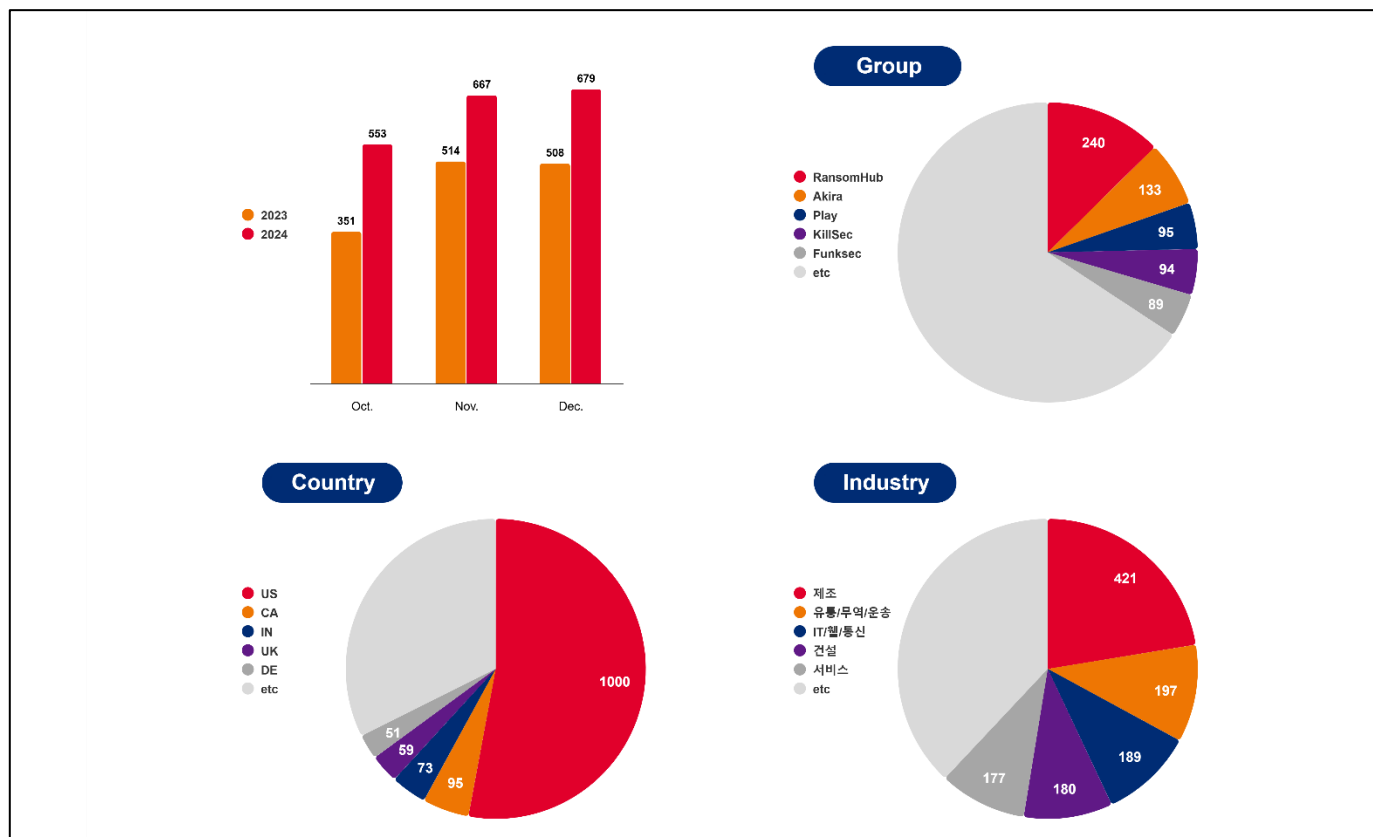
EXPLOIT

- 0-day : CVE-2024-50623, CVE-2024-55956, CVE-2024-40711
- 1-day : CVE-2020-3259, CVE-2023-20269

TARGET

- Initial infiltration via vulnerabilities in **Cleo (Harmony, VLTrader, LexiCom)**
- Among all attacks, 22% target the **manufacturing sector** while 53% target entities in the **United States**

2. Q4 Ransomware Activity Statistics



[Figure 1] Ransomware Group Activities

In the fourth quarter of 2024, the number of ransomware incidents reached 1,899, marking an approximate 38% increase compared to the same period in 2023 and a 44% rise relative to the third quarter of 2024. The Akira group's activities, which had amounted to a mere 48 incidents in the third quarter, surged dramatically to 133 incidents in the fourth quarter, while the RansomHub group likewise escalated its tally from 195 to 240 incidents. Additionally, the incorporation of figures from emergent ransomware groups such as FunkSec, Bashe, and SafePay has contributed to the precipitous uptick observed during this period. Conversely, despite the proliferation of new ransomware entities, the influence of the notoriously infamous LockBit group has steadily waned. This decline is chiefly attributable to the apprehension of individuals suspected of developing the LockBit ransomware, coupled with the ongoing seizure of their infrastructure, which has constrained data leakage incidents to a total of 12.

In the fourth quarter alone, the RansomHub group emerged as the most active, exfiltrating data in 240 incidents. Notably, they executed cyberattacks against the Mexican government and a renowned international football club, and even targeted a domestic manufacturing enterprise, subsequently publicizing in excess of 60GB of internal data

to assert their influence. Their primary tactics include employing a BYOVD¹ strategy to neutralize EDR² systems, in addition to initiating intrusions via exploited vulnerabilities and the abuse of RMM³ tools, among various other sophisticated strategies.

Similarly, the Akira ransomware group maintained a consistent level of activity in the fourth quarter by publicizing 133 instances of leaked data. It has been corroborated that the Akira ransomware propagated in October by exploiting the CVE-2024-40711 vulnerability in Veeam Backup & Replication⁴. This vulnerability arises during the process in which the software ingests untrusted data, and it appears that the Akira ransomware operators exploited this flaw to deploy their malicious payload.

Moreover, the Play ransomware group demonstrated sustained resilience in the fourth quarter by reporting 95 victim incidents. Of particular note is the observation that the Andariel group—an Advanced Persistent Threat (APT) entity operating under North Korea’s Reconnaissance General Bureau—may have engaged in collaborative activities with the Play group. Although there is speculation that Andariel might be functioning as an affiliate of the Play group, it is well-documented that the Play group does not offer RaaS⁵, thereby suggesting that Andariel likely operated merely in an ancillary IAB⁶ capacity.

The KillSec group similarly exhibited vigorous activity, having publicized 94 instances of leaked data, a figure comparable to that of the Play group. They claimed responsibility for an attack on a domestic real estate data platform and subsequently disseminated the compromised data, which encompassed various types of personally identifiable information and other sensitive details, thereby engendering concerns regarding potential secondary damage.

Lastly, the FunckSec group, a newly identified ransomware entity discovered in December, reportedly employed a generative AI system known as WormGPT—developed in-house—to facilitate tasks such as the creation of tools and phishing templates. Over the course of December, they recorded an impressive total of 89 data leakage incidents, among which was the publication of leaked data following an assault on a domestic specialty product distribution company.

¹ BYOVD(Bring Your Own Vulnerable Driver) : An attack technique in which a driver is recognized as legitimate due to its valid signature, yet it actually exploits vulnerable drivers.

² EDR(Endpoint Detection Response) : A security system that detects and responds to suspicious activities occurring at endpoints.

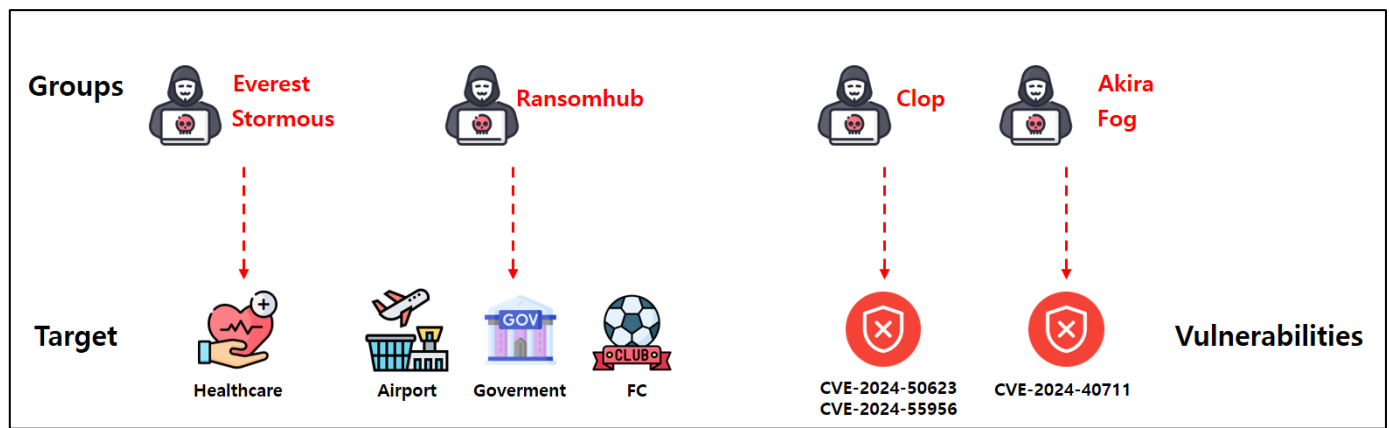
³ RMM(Remote Monitoring and Management) Tool : A legitimate tool used for remotely managing or monitoring systems.

⁴ Veeam Backup & Replication : A solution that backs up and monitors data.

⁵ Ransomware-as-a-Service : An abbreviation for ransomware-as-a-service, a revenue model in which ransomware is offered as a service in exchange for money.

⁶ IAB(Initial Access Broker) : A broker who sells access privileges after initially infiltrating a victim's system.

3. Ransomware Trends



[Figure 2] 2024 Q4 Ransomware Trends

✓ Ransomware Attacks Targeting Healthcare Providers

Healthcare organizations have increasingly become the targets of ransomware attacks. In the Dallas–Fort Worth area, Aspen Healthcare Services—a major Texas provider of home health and hospice care—suffered a significant breach at the hands of the Everest ransomware group, active since 2020. The attackers exfiltrated over 1,500 medical records and personal data, subsequently threatening to disclose or sell the compromised information with a deadline set for November 9. Following an attempted breach on October 22, Aspen Healthcare detected the intrusion on October 23 and immediately enacted stringent security measures, simultaneously notifying state and federal authorities. Subsequent investigations revealed unauthorized access to portions of its IT network, with the stolen data including sensitive details such as patient names, dates of birth, addresses, insurance IDs, health records, and Social Security numbers. Consequently, on November 18, the organization issued an official notification to affected parties regarding the data breach.

In a related incident, Guardian Healthcare—a provider of specialized nursing and care services in Pennsylvania and West Virginia—was also compromised. The Stormous ransomware group infiltrated its corporate systems, exfiltrating approximately 3GB of sensitive data. Although negotiations were initiated, they ultimately did not culminate in an agreement.

✓ Active Operation of the RansomHub Group

In 2024, the RansomHub group, noted for its high operational tempo, sustained its aggressive activities into the fourth quarter by targeting both governmental and sporting institutions. The group claimed to have penetrated the internal systems of Italian football club Bologna FC, exfiltrating in excess of 200GB of sensitive data that encompassed player contract details, employee records, match infrastructure information, and various personal data. Bologna FC subsequently acknowledged the breach and issued an official statement demanding that possession

and dissemination of the stolen data be prohibited.

Moreover, the Mexican government was not spared; the group targeted the Attorney General's Office of the Mexican executive branch, exfiltrating 313GB of data, which reportedly included contracts, insurance documents, and financial records. The breach was publicly disclosed on the group's DLS⁷ platform, accompanied by a 10-day negotiation window, though subsequent negotiation progress remains indeterminate. Additionally, the group has continued its assertive posture by disclosing further breaches, such as alleging the exfiltration of 3TB of data from Grupo Aeroportuario del Centro Norte, the operator of Mexican airports.

✓ Clop Ransomware Attack Exploiting Cleo's Zero-Day Vulnerabilities

A recent incident revealed that the Clop ransomware group exploited previously unknown zero-day vulnerabilities in Cleo's managed file transfer solutions to launch a targeted attack. Specifically, the attackers exploited vulnerabilities CVE-2024-50623 and CVE-2024-55956 in Cleo's suite of file transfer solutions—including Cleo Harmony, VLTrader, and LexiCom—to infiltrate corporate networks and exfiltrate sensitive data. Although Cleo released version 5.8.0.21 in October to patch CVE-2024-50623, residual issues necessitated the subsequent deployment of an additional patch, version 5.8.0.24.

Initially attributed to another ransomware group, further analysis confirmed that the Clop group was responsible. The attack was executed via a complex chain of tactics that extended beyond a simple file write vulnerability, incorporating remote command execution via a reverse shell⁸, lateral movement within networks, and the employment of an overpass-the-hash⁹ technique. Notably, the newly discovered CVE-2024-55956 vulnerability, which manifests at Cleo's "/Synchronization" endpoint, was also exploited to deploy a Java-based Cleopatra backdoor.

In response, the Cybersecurity and Infrastructure Security Agency (CISA) confirmed the exploitation of Cleo's vulnerability in ransomware attacks, added it to the KEV¹⁰ list, and advised federal civilian agencies and users of Cleo's Managed File Transfer solutions to apply patches by January 3. CISA further recommended additional security measures—including disabling Autorun functionality, configuring firewall settings, implementing IP allowlisting, and rigorously monitoring for suspicious activities such as unauthorized PowerShell executions—given that other major software vulnerabilities, such as those affecting CyberPanel, are also being targeted

⁷ DLS (Dedicated Leaks Sites) : Ransomware PR and data exfiltration sharing sites operated by attackers.

⁸ Reverse Shell: A shell where the victim's system establishes a connection to the attacker's server to execute commands.

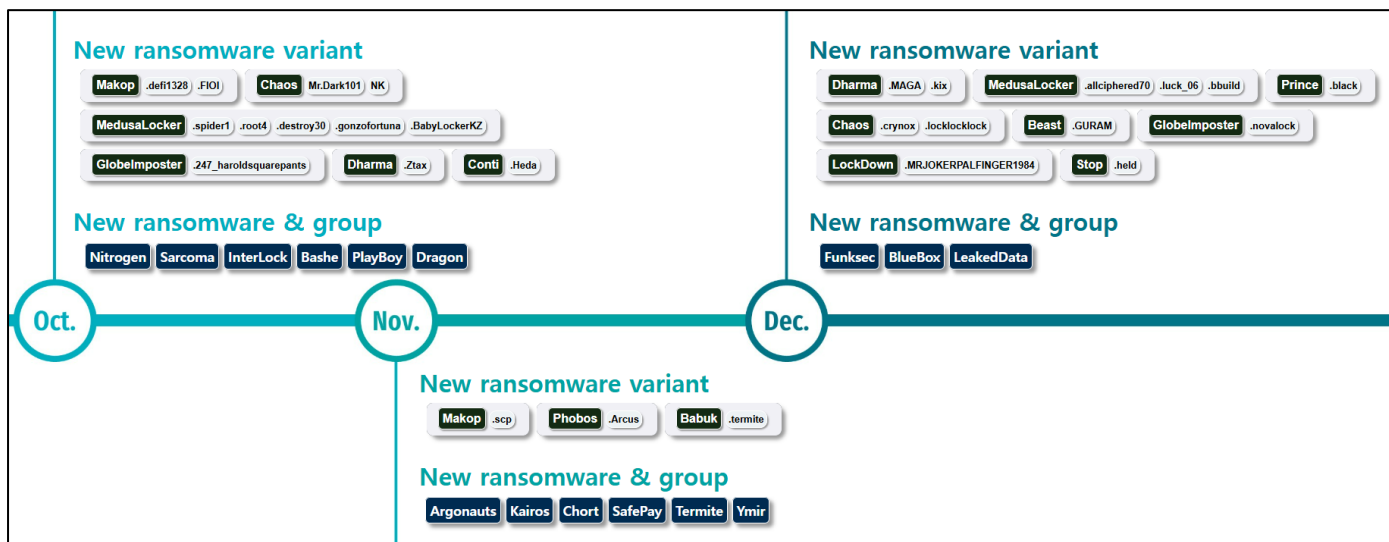
⁹ Overpass-the-Hash: A technique that bypasses Kerberos or NTLM authentication by directly using hashed passwords.

¹⁰ KEV (Known Exploited Vulnerabilities): A list of vulnerabilities that are actively exploited in attacks.

✓ Ransomware Attack Exploiting a New Vulnerability in Veeam Products

Since October 2024, critical vulnerabilities have been identified in Veeam products, leading to a proliferation of ransomware attacks exploiting these security flaws. The CVE-2024-40711 vulnerability, which bears a CVSS score of 9.8, affects Veeam Backup & Replication, Veeam Agent for Linux, Veeam ONE, and other related products. Exploitation of this vulnerability permits remote code execution without authentication, a vector that has been leveraged by both the Akira and Fog ransomware groups. These threat actors infiltrated networks via vulnerable VPN connections that lacked multi-factor authentication and subsequently exploited the vulnerability to create local administrator accounts, exfiltrate data, and execute encryption operations.

4. New Ransomware and Group Activities



[Figure 3] New/Variant Ransomware

In the fourth quarter, a multitude of ransomware groups—both those that have undergone recent rebranding and entirely new entrants—have emerged. Notably, there has been an increasing trend of groups disclosing large-scale victimization immediately upon their inception. For instance, the Sarcoma ransomware group, which surfaced in October, revealed over 40 victims within a single month, while SafePay ransomware, initiating its operations in November, disclosed more than 40 compromised companies from the outset. Furthermore, the InterLock ransomware group reported in excess of 85 victim cases throughout December, thereby exacerbating the scale of corporate damages. Additionally, the APT73 group, which had ceased operations in August, rebranded itself as Bashe upon its return and simultaneously initiated 20 attack cases, thus resuming its malicious activities. Other ransomware groups have also surfaced; descriptions of the principal entities are as follows:

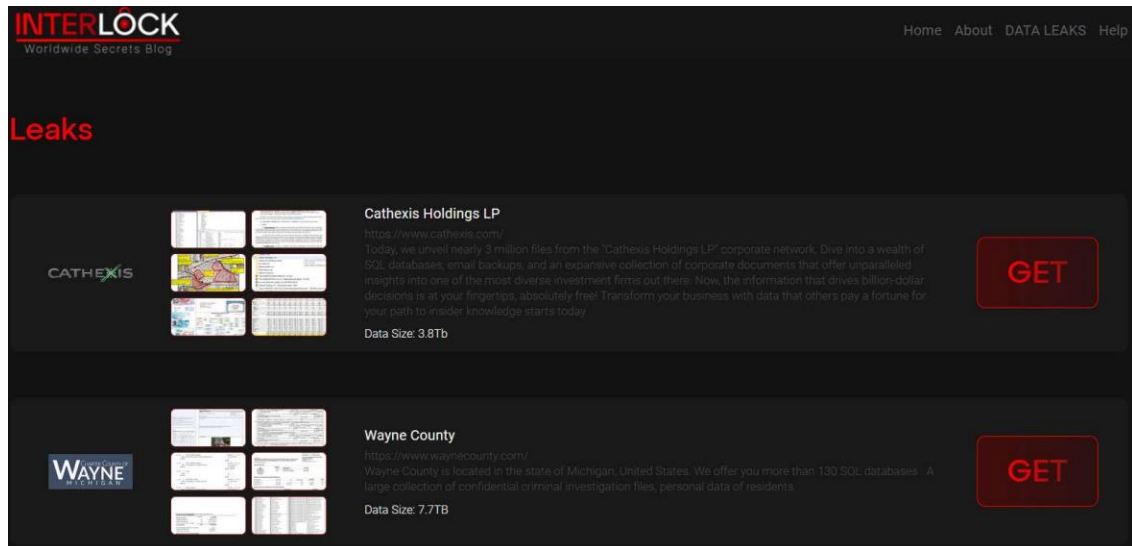
- **Sarcoma**

Emerging in October, Sarcoma disclosed that by December it had attacked a total of 56 companies and exfiltrated sensitive data. The group targeted enterprises in nations including the United States, Canada, Australia, and Spain. In a provocative display, it posted sample data on its Data Leak Site (DLS) alongside a message insinuating that the affected companies were woefully insecure, and it employed a dual extortion tactic by threatening to sell the stolen data on the dark web if negotiations failed.

- **InterLock**

Discovered on October 9, InterLock has actively expanded its operations through December. The group initiates

intrusions via phishing websites and, after gaining access to internal systems, deploys data-stealing malware to harvest system information. Subsequently, it exploits legitimate tools—such as PuTTY and Remote Desktop Protocol (RDP)—to propagate through the internal network. Once internal dominance is secured, the group executes the InterLock ransomware, encrypting files and appending a “.interlock” extension. Thereafter, it updates the roster of victim companies on the DLS and allocates a four-day negotiation period, after which, if negotiations collapse, it destroys the decryption keys and either sells or publicly discloses the data. Notably, this group is capable of attacking both Windows and Linux environments, thereby broadening its target scope across a diverse array of systems and enterprises.



[Figure 4] Interlock Ransomware DLS

- **SafePay**

The SafePay ransomware group, which emerged in November, has launched attacks against small and medium-sized enterprises across several countries—including the United States, the United Kingdom, Canada, and Brazil—utilizing a variant derived from the leaked LockBit source code. The attackers infiltrate internal systems by leveraging the Remote Desktop Protocol, subsequently employing PowerShell scripts and Windows command-line utilities to execute their attacks. Ultimately, they encrypt the files, modify their extensions to “.safepay,” and leave behind ransom notes containing threatening messages that demand monetary compensation from the victims.

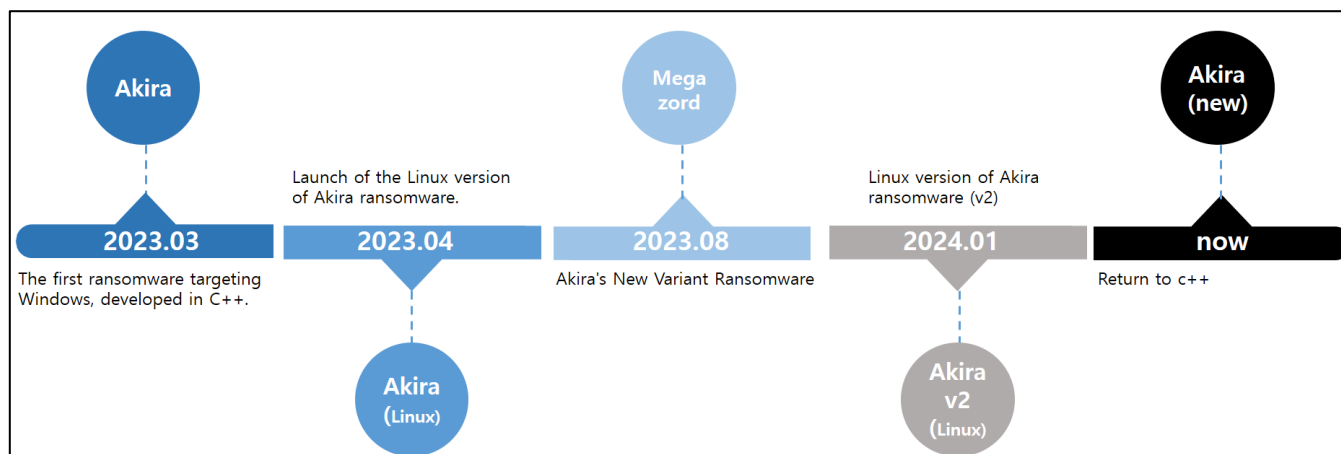
- **FunkSec**

FunkSec ransomware, which emerged in December, rapidly commenced its operations by disclosing over 85 victim companies on the DLS. However, it has been confirmed that some of the data it released originated from previous hacktivism-related breaches, rendering it difficult to categorically assert that all listed victim companies

were directly compromised in this instance. The malware utilized by FunkSec is developed in Rust, encrypting the files on infected systems with a ".funksec" extension and generating a ransom note formatted as README-[A-z0-9]{10}.md. Furthermore, the group operates under a Ransomware-as-a-Service (RaaS) model, offering not only ransomware but also an array of malicious services, including Distributed Denial of Service (DDoS) tools, HVNC clients, and account hijacking utilities

Detailed Analysis of the Akira Ransomware Group

1. Overview



[Figure 5] Akira Ransomware Evolution Process

Akira ransomware operates under a RaaS (Ransomware-as-a-Service) model, wherein it monetizes by selling access credentials to its ransomware and DLS platform and distributing a share of its illicit proceeds. Following the initial detection of its Windows-compatible variant, subsequent strains targeting Linux environments have also been identified, and it now executes attacks irrespective of the operating system. Predominantly targeting enterprises in North America and Europe, the DLS site has publicly disclosed 240 victim companies; when considering cases resolved through confidential negotiations and undisclosed victims, the actual extent of the damage is likely even greater.



[Figure 6] Akira Ransomware DLS

This group employs not only straightforward file encryption threats but also a sophisticated double extortion strategy that leverages the exfiltrated data. Although its encryption targets and string obfuscation techniques bear similarities to those of the Conti ransomware, the direct correlation is difficult to ascertain given the emergence of numerous ransomware variants based on the leaked Conti source code. Nevertheless, blockchain transaction tracing has revealed that the Akira ransomware group transferred cryptocurrency to the Conti group, suggesting that a faction of Conti may have merged with Akira or that both groups might be collaborating on their attack methodologies.

Initially detected in March 2023, Akira ransomware was originally developed in C++ for Windows environments. In April, a variant targeting Linux surfaced, and by early 2024, a second iteration written in Rust was employed in attacks. Subsequently, another C++-based variant was produced, which continues to be actively deployed.

The Megazord ransomware, discovered in August 2023, exhibits notable similarities in code and operational techniques to Akira ransomware, with the common attribute of being developed in Rust. Although differences exist in the encrypted file extensions and ransom note filenames, the two share initial access methods and segments of code, implying that Megazord may represent either a rebranded version of Akira or a derivative variant.

Distinctively, the data leak site associated with Akira ransomware features a command-line interface (CLI), diverging from the conventional web-based DLS platforms. Its primary commands include: leaks—which enables the downloading of lists of victim companies and their exfiltrated data; news—which displays promotional materials and announcements; contact—which provides negotiation-related contact details; help—which outputs a list of available commands; and clear—which clears the display screen.

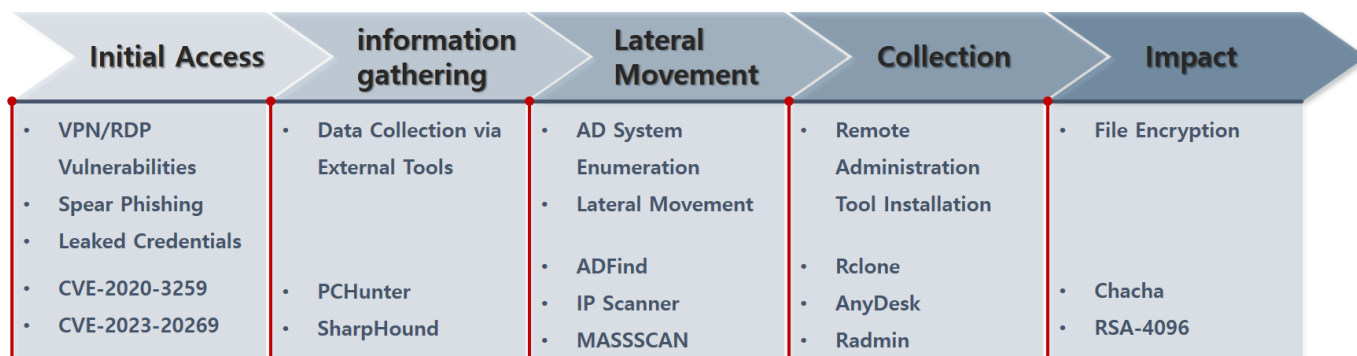
```

[ AKIRA ]
guest@akira:~$ leaks
+-----+-----+-----+-----+
| name | desc | progress | link |
+-----+-----+-----+-----+
| P- [REDACTED] | P- [REDACTED] designs and fabricates custom foam, plastic, and corrugated components. They can provide these components individually or integrate them into our creative package designs. We'd like to announce that P- [REDACTED] company is going to provide their own corporate and personal information to everyone who is interested in it. P- [REDACTED] company information is available for downloading and they are the first data providers in our blog. We are happy to share this new with you! Welcome to everyone! We have made the process of uploading company data as simple as possible for our users. All you need is any torrent client (like Vuze, Utorrent, qBittorrent or Transmission to use magnet links). You will find the torrent file above. 1. Open uTorrent, or any another torrent client. 2. Add torrent file or paste the magnet URL to upload the data safely. 3. Archives have no passwords. MAGNET URL: magnet:?xt=urn:btih:A45C[REDACTED]F88B8C0D0CFDE28B17A9823&dn=[REDACTED]openbittorrent.com:80/announce&tr=uop://tracker.opentrackr.org:1337/announce | [=====>] 100% | download |
+-----+-----+-----+-----+

```

[Figure 7] Victim Company Information and Download Link

2. Akira Ransomware Attack Scenario



[Figure 8] Akira Ransomware Attack Scenario

The Akira group infiltrates its targets through a multifaceted approach that includes exploiting VPN vulnerabilities, conducting spear-phishing campaigns, leveraging RDP vulnerabilities, and utilizing compromised credentials. Notably, the group specifically targets VPN software from vendors such as Cisco, SonicWall, and Fortinet, exploiting vulnerabilities like CVE-2020-3259 and CVE-2023-20269. Furthermore, evidence indicates that access to networks has been gained through previously leaked accounts lacking multi-factor authentication (MFA), which suggests either collaboration with other hacking groups or the procurement of accounts from initial access brokers.

Following initial penetration, the attackers consolidate internal control by employing tools such as PCHunter and SharpHound to gather system information, while using ADFind and Windows command-line utilities to ascertain Active Directory (AD) details. Subsequently, they utilize IP Scanner and MASSCAN to meticulously probe the internal network for additional propagation vectors. Once internal system data has been accumulated, the attackers either exploit further vulnerabilities or register new domain controllers to escalate privileges, concurrently deploying PowerTool to disable antivirus software as a means to obfuscate their malicious activities.

Prior to executing the ransomware, the adversaries install remote control utilities like AnyDesk and Radmin, as well as file transfer applications such as FileZilla and WinSCP, to exfiltrate sensitive information. Thereafter, they launch the ransomware, encrypting files within the system, and conclude their assault. The Akira ransomware group not only exploits software vulnerabilities but also actively capitalizes on leaked credentials; post-infiltration, they further utilize publicly available tools to navigate the internal network and exchange commands, thereby employing highly sophisticated attack methodologies.

3. Analysis of Akira Ransomware

- Decryption of Encrypted Strings

Akira ransomware employs an identical string decryption logic to that utilized by Conti. The strings indispensable for executing its malicious functions are maintained in an encrypted state and are decrypted within the `initterm` routine prior to the invocation of the main function. Within the `initterm` table, an array of functions is stored and executed sequentially; this table encompasses the file extensions targeted for encryption, items exempted from encryption, details of exception folders, and functions specifically designed to decrypt the strings critical to the ransomware's operations. Upon execution, these functions are triggered to decrypt the strings, which are subsequently stored in memory. Additionally, certain strings exist in an unencrypted form and are directly copied into memory without undergoing any decryption process.

```
memset(v11, 0, sizeof(v11));
wstrcpy_14003E600(v11, L"Trend Micro", 0xBuLL);
memset(v12, 0, sizeof(v12));
wstrcpy_14003E600(v12, L"ProgramData", 0xBuLL);
v1[0] = v2;
v1[1] = &vars0;
sub_14006FE60(&exclude_dir, v1);
`eh vector destructor iterator'(v2, 0x20uLL, 0xBuLL, unknown_libname_4);
return atexit(sub_1400CBBC0);
```

[Figure 9] Loading of Unencrypted Strings

```
00
    ++v7;
while ( *&v50[2 * v7] );
wstrcpy_14003E600(v71, v50, v7);
v43[14] = 0;
qmemcpy(v44, "c0", 2);
v44[2] = 1;
v44[3] = 48;
v44[4] = 96;
v44[5] = 48;
v44[6] = 17;
memset(&v44[7], 48, 3);
for ( m = 0LL; m < 0xA; ++m )
    v44[m] = (24 * (48 - v44[m]) % 127 + 127) % 127;
memset(v72, 0, sizeof(v72)); // .pvm
```

[Figure 10] Decryption of Encrypted Strings

- Log File Generation

A distinctive feature of Akira ransomware is its capability to generate a log file during execution. This file records runtime details such as the number of threads configured by the ransomware and the success status of the file encryption process. The log file is created in the directory from which the ransomware is executed, following a filename format of "Log-%d-%m-%Y-%H-%M-%S.txt."

```

GetSystemTimeAsFileTime_0(&Time, hPrevInstance, lpCmdLine, nShowCmd);
v4 = localtime64(&Time);
strftime(Buffer, 0x50uLL, "Log-%d-%m-%Y-%H-%M-%S", v4);
v222 = 0LL;
v223 = 0LL;
v224 = 0LL;
v5 = -1LL;
do
    ++v5;
while ( Buffer[v5] );
sub_1400371E0(&v222, Buffer, v5);
sub_14004C6E0(v6, &v222);

```

[Figure 11] Log File Generation

```

2025-01-20 10:17:52.373 [file_logger] [info] Number of thread to folder parsers = 1
2025-01-20 10:17:52.373 [file_logger] [info] Number of thread to root folder parsers = 1
2025-01-20 10:17:52.373 [file_logger] [info] Number of threads to encrypt = 2
2025-01-20 10:17:52.373 [file_logger] [error] File handle not found! (C:\BOOTSECT.BAK.MEOW)
2025-01-20 10:17:52.373 [file_logger] [error] File handle not found! (C:\bootmgr)
2025-01-20 10:17:53.107 [file_logger] [error] Get file size failed! (C:\123\Log-05-02-2025-09-24-27.txt)
2025-01-20 10:17:53.123 [file_logger] [error] File handle not found! (C:\Program Files\7-Zip\7-zip.chm)
2025-01-20 10:17:53.123 [file_logger] [error] File handle not found! (C:\Program Files\7-Zip\7z.sfx)

```

[Figure 12] Malicious Activity Records in the Log File

- Parsing of Execution Arguments

Upon program initiation, the supplied execution arguments are parsed to set flag values or designate the options requisite for encryption. A total of five arguments are provided, and the execution environment is configured in accordance with the values input.

설정	설정 정보
-encryption_path, -p	Designation of encryption target paths
-share_file, -s	Designation of encryption for specific network drives
-encryption_percent, -n	Specification of file encryption ratios
-localonly	Encryption is performed exclusively on local drives
-exclude, -e	Designation of encryption exclusions
-l	Recording of encrypted drive information in the log file

- Deletion of Volume Shadow Copies

Prior to initiating file encryption, the ransomware eradicates volume shadow copies to preclude any possibility of system recovery. Upon the invocation of the corresponding function, it decrypts an encrypted PowerShell string, instantiates a COM object to facilitate its execution, and constructs the requisite command line to run the script. Following the execution of the command, the ransomware employs OpenProcess to await the command's completion before proceeding to subsequent malicious activities.

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObjectz
```

[Volume Shadow Copy Deletion Command]

```

qmemcpy(v6, "c:9{o!Zrc]", 10);
v6[10] = 17;
v6[11] = 25;
v6[12] = 50;
for ( i = 0LL; i < 0x4C; ++i )
    enc_str[i] = (42 * (50 - enc_str[i]) % 127 + 127) % 127;
hPowershell = RunPowershell_140078890(enc_str); // Get-WmiObject Win32_Shadowcopy | Remove-WmiObject
if ( hPowershell )
{
    // powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
    v2 = OpenProcess(0x100000u, 0, hPowershell);
    v3 = v2;
    if ( v2 )
    {
        WaitForSingleObject(v2, 0x3A98u);
        CloseHandle(v3);
    }
}
CoUninitialize();

```

[Figure 13] PowerShell Script Execution

- Loading of the attacker's public key

Although Akira ransomware utilizes symmetric encryption for file protection, the symmetric keys employed are subsequently re-encrypted using the attacker's public key and stored securely. Prior to executing its malicious operations, the ransomware loads the attacker's public key—embedded within the file—into memory, and after file encryption concludes, it encrypts the symmetric key with this public key.

```

30 82 02 0A 02 82 02 01 00 F4 86 C1 AB 44 5F AE 0.....D_
67 A5 4B 9E 56 AB 48 EF FB 83 08 93 A7 87 AB DF g.K.V.H.....
F0 89 27 75 23 76 CE 22 D3 7A 9C 37 75 3E AF 24 ....#v.....7u>.$
F9 F2 76 E2 A7 2A 1E A0 6C 80 29 47 33 C3 CD 88 .....*.l.)G3...
A8 40 E9 C6 ED 25 F2 10 63 B9 68 FF F2 E3 59 09 .@...%....h....
34 1F 42 FF 11 2D B4 24 36 33 87 BF EB AA 2A 58 4.B...-$63....X
13 E9 F3 7F CF AB 62 D4 0B 89 C0 A3 45 25 2C 93 ....x.b....E%,
6C 03 19 41 79 D4 D0 2A D1 F1 F8 AD A4 D5 31 3B l..Ay..*.....;
50 73 2C 8E 61 0F 2F C5 41 4C 0E 0B 53 E2 78 A1 Ps,.a./..L..S...
03 0F 27 B5 B4 92 5F 56 4B 53 1F 3D B0 94 BF 43 ..'...._VKS.=...C
7E B7 5B 41 C0 B2 AF 85 81 6F 08 73 5A B7 71 95 ~.[A.....o.sZ.q.
11 A0 21 DF 6F D8 68 47 14 98 6A AF B1 B9 9F FE !.....G..j.....
D4 C9 65 83 A2 75 A7 E0 1B E0 E5 EF BE 9A EF 76 ..e..u.....
16 B2 63 FB BA 76 50 6B B0 2C 06 09 32 B3 AC 95 ..C..vPK.,..2...
6D 70 4E 6C 97 7F B8 01 64 D8 8F 2B A0 13 F6 BE mpNl....d_+....
15 28 18 02 E2 4B 3B FA 3C 71 A5 C1 85 C5 D5 49 (. ....<q.....I
5A 93 D4 37 8B 44 E7 23 C7 18 6F D5 DE 27 C3 0C Z....D....o..'.
51 AF AE 67 14 12 92 BF C5 B1 60 04 90 B4 10 D8 Q..g....u`.....
96 4A 4A 81 6E 2F 0F EE 83 2C D9 D7 DA F9 BB 8C .JJ.n/.....
17 15 05 5D 94 AA D1 10 56 BF 87 BF 4D 4A 98 88 ...]....V...MJ..
DB 8A B0 1E BF 6F 55 58 D0 A2 C1 ED 21 16 80 95 3'....oUXT...!...
92 B0 FD 9A 49 F6 62 CE B7 B2 DB 5F CD F6 F9 EE ....I.....
D1 00 20 81 4E 7D C7 53 86 04 FA 73 DB 5F F3 F5 ..'.N}....s....
A6 10 5A 17 C6 B3 4C 3E F7 B9 36 47 83 E5 77 8D ..Z.Y.L>.....
29 F4 05 77 E8 A4 73 59 67 79 0F 89 9B B4 97 F6 ). ....sYgy.....
70 0D 17 22 E5 E2 D7 4E BD B7 10 E6 8C 24 27 E4 p..".N.....'.
6B 16 B1 96 3A 54 81 FE 8E 67 5A FC DA 9E 38 9B k...:T...gZ.8.ش.
49 B7 00 FF E0 2A 6B 7D 03 EF D0 76 2A 25 48 0F I.....}....*H.
40 AD 12 C4 14 95 76 44 BF A8 CF 48 41 27 EB F2 @.....vD....A'.
09 C9 AA D3 E2 8D F8 E7 08 4E 05 B8 44 16 28 61 .I.....D.(a
BB 8B ED 76 B0 97 7F 9D E2 41 E3 E1 BC 0B 0B B6 .....jx...W..u~
2C C3 F2 92 CD 18 6A 78 EE 0B 41 57 A8 BA 75 7E ,...E.P...[.....
A6 1B 45 1A 50 18 D0 32 5B 02 03 01 00 01 00 00

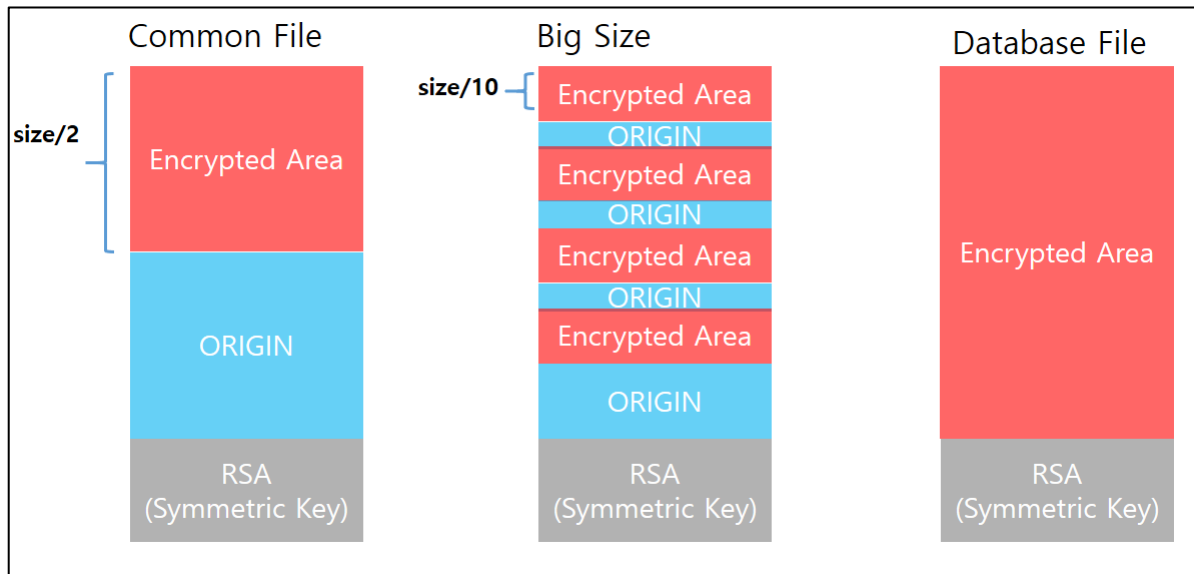
```

[Figure 14] Attacker's Public Key

- File encryption

Within the infected system, the ransomware conducts a meticulous analysis of the file structure to ascertain folder names and file extensions, thereby ensuring that folders and files designated as encryption exceptions remain unaltered. For items not exempted, the file extension is re-evaluated to determine the applicability of

encryption. Owing to the protracted duration required to encrypt disk images or substantially large files, the ransomware opts for partial encryption in such cases; conversely, non-large files with specific extensions are subjected to complete encryption regardless of their size. Files that undergo full encryption are predominantly those associated with databases, which inherently contain critical information, and are thus entirely encrypted irrespective of the encryption speed. The encryption process leverages the ChaCha symmetric encryption algorithm: standard files are only partially encrypted (approximately half of the file), whereas large files or disk images are partitioned into blocks corresponding to one-tenth of the file's size, with encryption executed at four distinct positions. Additionally, files with database-related extensions, as enumerated in the "Encryption Target Files and Folders List," are fully encrypted regardless of their dimensions.



[Figure 15] Encrypted File Structure

- Ransom note generation

In folders where encryption has been completed, a ransom note file is generated containing both installation guidelines for the Tor Browser and a designated address for negotiation, thereby alerting the victim to the infection.

- Ransom note filename: akira_readme.txt

Hi friends,

whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. we're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. we will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to falling of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidentally corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - <https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kol1pj5z3z636bad.onion>.
5. we're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - <https://www.torproject.org/download/>.
2. Paste this link - <https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kol1pj5z3z636bad.onion/d/0832201915-DMFCY>
3. Use this code - 6696-DY-OGIA-UXQX - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

[Figure 16] Akira Ransom Note

4. List of Files and Folders Subject to Encryption

tmp	Winnt	Temp
thumb	\$Recycle.Bin	\$RECYCLE.BIN
System Volume Information	Boot	Windows
Trend Micro	ProgramData	

[Encryption Exclusion Folder List]

exe	Dll	Ink
sys	Msi	

[Encryption Exclusion File Extensions]

.accdc	.accddb	.4dl	.4dd	.accft	.accdt	.accdr
.accde	.adp	.adf	.ade	.adb	.ask	.alf
.ora	.arc	.cdb	.cat	.bdf	.btr	.dacpac
.cpd	.cma	.ckp	.db	.daschema	.dadiagrams	.dad
.dbc	.db3	.db-wal	.db-shm	.dbv	.dbt	.dbs
.dbf	.dcx	.dct	.dcb	.dbx	.dqy	.dp1
.dlis	.ddl	.dxl	.dtsx	.dsn	.dsk	.epim
.edb	.ecx	.eco	.fic	.fdb	.fcd	.exb
.fol	.fmpsl	.fmp12	.fmp	.fp7	.fp5	.fp4
.fp3	.grdb	.gdb	.frm	.fpt	.ib	.his
.hdb	.gwi	.itw	.itdb	.ihx	.idb	.kexi
.kdb	.jtx	.jet	.lwx	.lgc	.kexis	.kexic
.mas	.mar	.maq	.maf	.mpd	.mdf	.mdb
.mav	.myd	.mwb	.mud	.mrg	.ns2	.nrmlib
.nnt	.ndf	.nv	.nsf	.ns4	.ns3	.odb

.nyf	.nwdb	.nv2	.p96	.owc	.orx	.oqy
.pdm	.pdb	.pan	.p97	.rbf	.qvd	.qry
.pnz	.rpd	.rodx	.rod	.rctd	.scx	.sbf
.sas7bdat	.rsd	.sis	.sdf	.sdc	.sdb	.sqlite3
.sqlite	.sql	.spq	.tmd	.temx	.te	.sqlitedb
.udb	.trm	.trc	.tps	.vis	.v12	.usr
.udl	.wmdb	.wdb	.vvv	.vpd	.xmlff	.xld
.xdb	.wrk	.accdw	.abx	.abcddb	.hjt	.fm5
.db2	.adn	.lut	.kdb	.icr	.icg	.mdt
.mdn	.maw					

[Encryption Target Database Files]

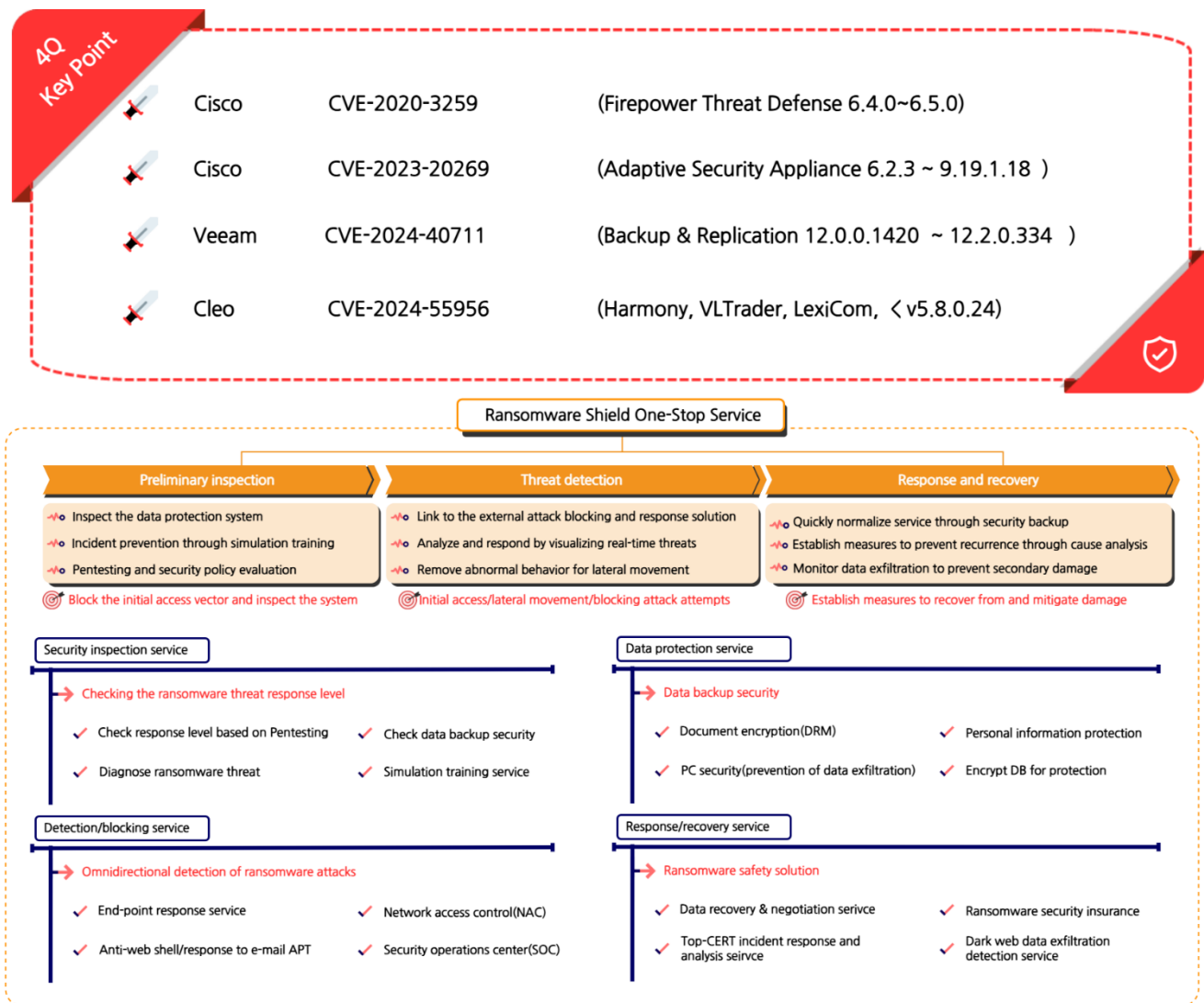
5. IoCs

SHA256
1ba1ccfacffbb6be9480380f5535a30d3eee1dd7787f3c649ebf8ea2a6a5de51
3720cafdd914d70d5fccf8d61593a66b5bdc400432e687c92e66eb3b5e8a9d9e
78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0
ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5
0c662d28268514fab7129fd14d6e3e9d7df29261a861bcf8aab1f318bb8e7d0
f11b60b273e2606e91832edbb014ad229563f5c537ddab11dba80018c11364dd
9f873c29a38dd265dec6517a2a1f3b5d4f90ccd42eb61039086ea0b5e74827e
a5806174261004a0b8b5c0be808a77e5f25b867a4c522813035c2b0dc05d90a2
8c5412298e3c382a1ae3e84fd04ae62bc2d69703e9863ca5478cf3c513e6e232
58e685695afc3a85d2632777a2b54967dc53d6a6fa1b7e2c110b2023b561bfe9
120715377727531a56f32225e196b1536618d224662fa0b3ba6c52dba80f3b29
43b0ac119ff957bb209d86ec206ea1ec3c51dd87bebf7b4a649c7e6c7f3756e7
e10cae894e8873c72ae9e5f3590e2f78f6cc2dcfe01e1a5039c8b6532bfab5f8
aaa7799edfd86b52438a9e0d71f8069cbcbbe1988036b95888fcdc553e729b7b9
87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d
442f5b7ae1a60d0cee31290b179b9201902e1f4875c606e6fe58b9ff4907c37e
d323d32cbd906c495a6e9fe7da01bf3e0eca407609a2693c7246346687d59f50
88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2
74fbb7885ee486028fe2723f95911474b771f361b2b40ddb77c46f252059c696
1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218
d07b379369e9faea0fed406b9b37652b2fc6453044ab17c1e2189cf61640ab90
74fbb7885ee486028fe2723f95911474b771f361b2b40ddb77c46f252059c696
a6d68214bf78c925b6fe6ab277589bc28c338e7253625925a674f380f3a52102
2d931f6867e7049b450c8ab36e1f8e6a51f0ee95fc2253d0759e3e3b118fe1d1

Ransomware Mitigations

1. Guidance for Mitigating Akira Ransomware

Akira ransomware initiates its infiltration by exploiting phishing schemes and vulnerabilities in VPNs that lack multi-factor authentication, subsequently leveraging publicly available reconnaissance tools and remote control software to propagate internally. Once the internal systems are compromised, the ransomware exfiltrates data and, upon the expiration of the negotiation period, discloses the stolen information on its Data Leak Site (DLS), thereby rendering preemptive countermeasures indispensable. Consequently, it is imperative to implement proactive security measures, including the application of security patches at external contact points, the activation of multi-factor authentication for VPNs, and the continuous monitoring of publicly available intrusion tools.




2. SK Shieldus MDR Service

To effectively counter ransomware attacks in a specialized manner, the utilization of SK Shieldus's Managed Detection and Response (MDR) service can serve as an efficacious solution. In light of the ransomware attackers' meticulous strategies and their sophisticated evasion techniques—which render conventional defensive systems increasingly inadequate—the threat landscape has evolved beyond the scope of traditional security measures. To address this challenge, SK Shieldus provides an MDR service that continuously monitors networks in real time, detects anomalous behaviors, and, when warranted, initiates immediate counteractions. While preemptive measures remain paramount in mitigating ransomware threats, it is equally critical to implement swift remedial actions to minimize damage should an attack occur. Consequently, enterprises are advised to consider the adoption of SK Shieldus's MDR service, which delivers tailored security solutions predicated upon rapid and precise incident investigation and analysis conducted by a dedicated team.

SK Shieldus MDR Service 3 Key Features


Service Contents

01	EDR Expert Operation Support
Managed	<ul style="list-style-type: none"> • 24/7 Incident Request Reception and Response • IoC and SK-Defined Rules Update • Policy Operation and Exception Handling Reflection • Event Analysis and Response Measures
02	SK Shieldus Detailed Analysis Service
Detection	<ul style="list-style-type: none"> • EDR/Malware Expert Analysis Service • Support for Malicious Behavior Tracking through EDR • Detailed Analysis for True/False Positive Response • Regular Threat Hunting Execution
03	Incident and Threat Response Capabilities
Response	<ul style="list-style-type: none"> • The Nation's Largest Incident Analysis and Investigation • Conduct Trace Investigations • Prioritize Domestic IoCs for EDR




EDR Monitoring Service

- ✓ **EDR-Specialized Security Operations Service**
 - Providing Services to Multiple Clients
 - Able to Respond to Client Requests with Various Industry Reference Cases
- ✓ **Improvement of User Satisfaction**
 - Swift Response by Experienced Operation Experts



Provide Expert Service

- ✓ **Utilization of TOP-CERT**
 - 24X7 emergency local deployment
 - Korea's largest Incident analysis and response
- ✓ **Expert services from SK Shieldus**
 - Analyst are on standby at all times
 - Malware analyst + CERT service
 - Dedicated team for fast and precise service



Top-level security response in Korea

- ✓ **No risk of data leaks via service**
 - In-house file analysis within the network
 - Exclusive analysis environment
- ✓ **Strengthened preemptive threat response**
 - Collaborate with clients to block threats early



Technology for Everyday Safety



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

COPYRIGHT © 2025 SK SHIELDUS. ALL RIGHT RESERVED.

This work cannot be used without the written consent of SK shieldus.