KARA
Korea Anti Ransomware Alliance

2025.2Q

KARA ransomware trend report

KARA Ransomware Trend Report

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

Ransomware Trends

1. Q2 Trend

TREND

- **RansomEXX :** Exploiting Microsoft's Privilege Escalation (CVE-2025-29824)
- **Qilin :** Exploiting SAP NetWeaver Vulnerabilities (CVE-2025-31324, CVE-2025-

THREAT

- **Top 5 Ransomeware Groups in Q2 :** Qilin, Akira, Play, SafePay, Lynx
- **Qilin Ransomware :** Increased Activity Following RansomHub Group's Dissolution

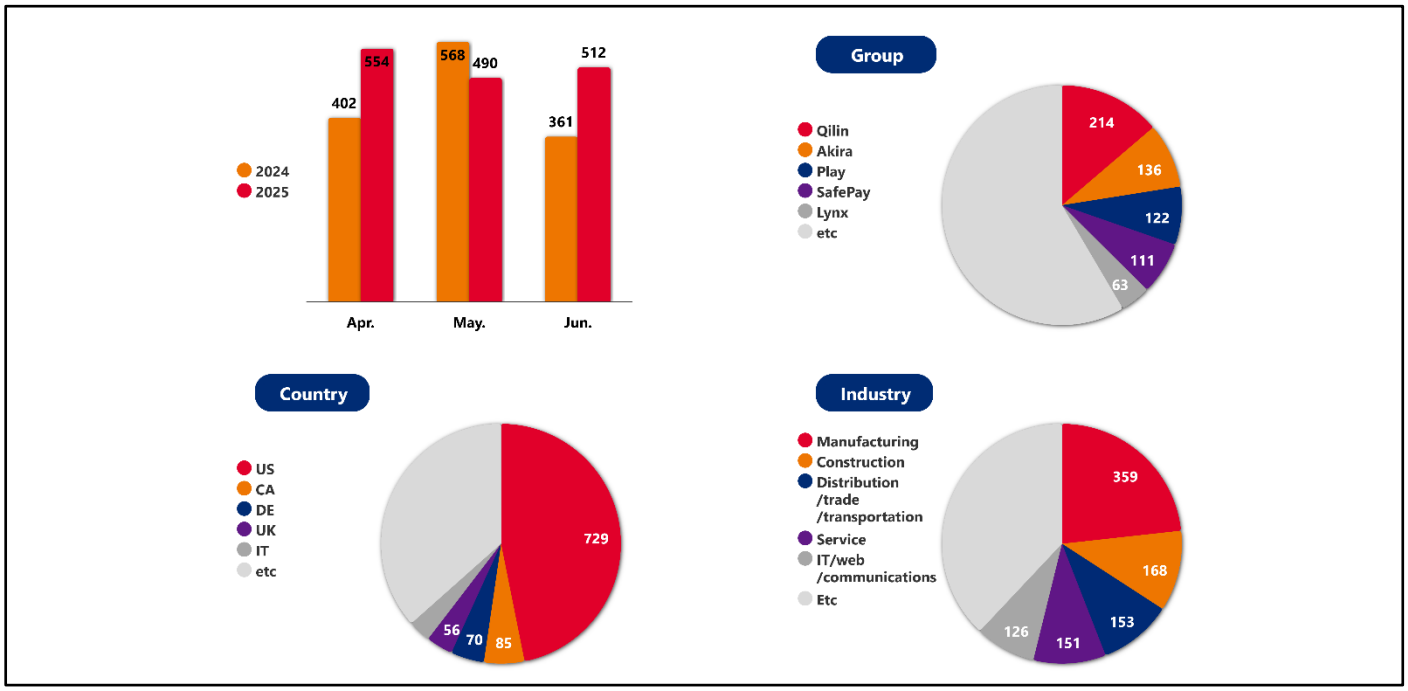
EXPLOIT

- **0-day :** CVE-2025-29824, CVE-2025-31324, CVE-2025-42999
- **1-day :** CVE-2024-57727, CVE-2024-21762, CVE-2024-55591

TARGET

- Initial Access via SAP NetWeaver Vulnerability
- Of Total Attacks Manufacturing 23%, USA 47%

2. Ransomware Activity Statistics for the 2Q



[Figure 1] Ransomware Group Activities

In the second quarter of 2025, a total of 1,556 ransomware incidents were reported—an increase of approximately 17% compared to the same period in 2024, yet a sharp decline of about 40% from the first quarter of 2025. This significant downturn appears largely attributable to the suspension of operations by several major ransomware groups that had been highly active in the preceding quarter, generating numerous victims. In particular, the overall drop in attack frequency coincided with a marked reduction in the activities of the Clop ransomware group—known for actively exploiting critical zero-day vulnerabilities when they emerge—and the complete cessation of operations by the RansomHub group, which had maintained high activity levels in recent years but officially halted its operations on April 1. Together, these factors contributed to a substantial decrease in ransomware incidents during the period.

Following RansomHub's shutdown on April 1, 2025, the activities of the Qilin group rose markedly. Some analysts suggest that a portion of RansomHub's operators migrated to Qilin. Supporting this assessment, statistical data show that Qilin's average monthly victim count has nearly doubled—from around 35 cases to roughly 70—since RansomHub's closure.

The Akira ransomware group, which recorded 222 attacks in the previous quarter, carried out 136 attacks in Q2 2025, reflecting a moderate contraction in operations. Nevertheless, Akira ranked second in attack volume after Qilin. The

group primarily exploited environments where Cisco and SonicWall VPN[1] devices lacked MFA[2] or where RDP[3] configurations were insecure, targeting enterprises predominantly in the United States, Canada, and Europe.

The Play ransomware group also demonstrated high activity levels in Q2, publicly listing 122 victims on the dark web. The group primarily leveraged vulnerabilities in Cisco ASA (Adaptive Security Appliance) firewalls for initial access, subsequently exploiting a privilege escalation flaw in the Windows Common Log File System (CLFS)—CVE-2025-29824—to gain SYSTEM-level privileges. This flaw was a zero-day vulnerability, weaponised in attacks before the release of an official patch. Upon confirmation of the exploitation, Microsoft issued an emergency security update on April 8.

In addition, both the SafePay ransomware group and Lynx—believed to be a successor to INC ransomware—have maintained elevated activity in recent months.

The list of countries most frequently targeted by ransomware remained unchanged from the previous quarter, with the United States and Canada topping the chart. Germany recorded 70 cases this quarter, rising from fifth to third place in the global ranking. The United Kingdom and Italy also reported substantial attack volumes, placing them among the most severely affected nations.

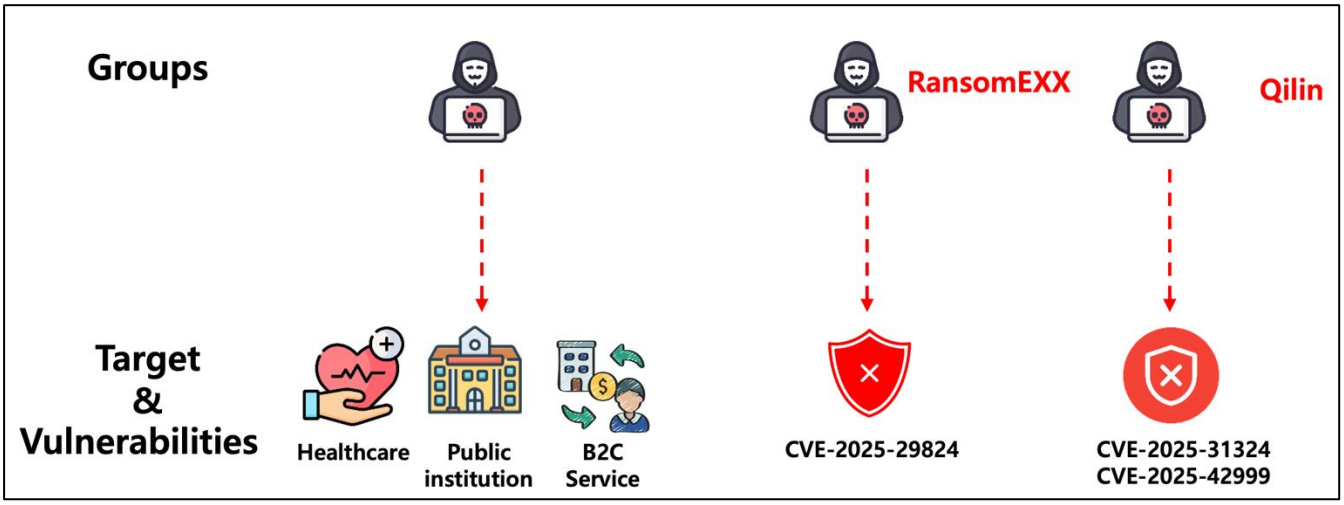
Sector-based analysis shows that the manufacturing industry continues to be the most targeted, followed by construction, distribution, trade, transportation, services, and IT/web/telecommunications. Notably, the construction sector recorded a sharp rise in incidents, climbing two places from the previous quarter to become the second most targeted sector in Q2.

[1] VPN (Virtual Private Network): A virtual private network technology that encrypts data transmitted over public networks, enabling secure communication.

[2] MFA (Multi-Factor Authentication): An authentication method that enhances security by requiring users to provide two or more distinct authentication factors when accessing an account.

[3] RDP (Remote Desktop Protocol): A remote access protocol developed by Microsoft

3. Ransomware Trends



[Figure 2] Ransomware Trends in Q2 2025

✓ Ransomware Attacks Targeting B2C[4] Entities That Directly Inflict User Damages

In the second quarter of 2025, ransomware attacks against B2C services went beyond typical information theft or file encryption incidents, causing direct and measurable harm to consumers. In May 2025, MathWorks, the developer of MATLAB and Simulink, widely used for engineering and scientific computation, was hit by a ransomware attack that crippled several core platforms, including the Cloud Center, License Center, File Exchange, and its online store. The sudden service outage on May 18 severely disrupted global users' ability to authenticate licenses, download software, and log in to their accounts. This impact was felt most severely by researchers, engineers, professors, and students in the midst of ongoing projects, leading to significant research delays and operational disruptions.

Immediately after the attack, MathWorks reported the incident to federal authorities and began an investigation with external cybersecurity experts. By May 21, the company had restored MFA and SSO[5] systems, allowing gradual restoration of access to certain functions. Full recovery, however, required more time, with some services delayed for more than two weeks or experiencing degraded performance.

A few days later, MathWorks confirmed that ransomware was responsible for the disruption but withheld details about the perpetrators. To date, no group has claimed responsibility, and no evidence of customer data exfiltration has been found. Forensic analysis revealed no signs of persistent compromise, and the company assessed the incident as a financially motivated, commercially targeted ransomware attack. MathWorks stated that it is strengthening its security systems to defend against future threats.

On June 9, 2025, YES24 also suffered a ransomware attack that paralysed its systems. The attack encrypted server data, completely halting core services such as book search and ordering, e-book access, and ticket reservations for

[4] B2C (Business to Consumer): A business model in which a company sells or provides products and services directly to end consumers.

[5] SSO (Single Sign-On): An authentication method that allows users to access multiple systems or services with a single login, without the need for repeated authentication.

performances and fan meetings. Both the website and mobile app were inaccessible for over four days; in particular, users could not access previously purchased e-book content, causing widespread frustration. The postponement or cancellation of scheduled performances and fan meetings further aggravated consumer dissatisfaction. YES24 restored administrator account access shortly after the attack and began investigating whether personal data had been compromised. On June 16, the company formally acknowledged the incident, issued a public apology, and prioritised the recovery of essential functions directly affecting consumers, such as book and ticket purchases, before sequentially restoring ancillary services like user reviews.

Around August 11 nearly two months after the first attack—YES24 suffered a second ransomware incident, again disabling its systems. During the subsequent recovery period, consumers faced renewed service disruptions and associated inconvenience.

Unlike earlier cases confined to straightforward data breaches or inter-corporate service interruptions, these two consecutive incidents highlight a growing trend in which ordinary consumers suffer direct inconvenience and material loss because of ransomware attacks.

✓ Ongoing Damages in the Healthcare Sector

During the second quarter of 2025, numerous ransomware groups maintained relentless attack campaigns against the global healthcare sector. Notably, the Interlock group targeted DaVita, a leading dialysis treatment provider in the United States, encrypting parts of its network and claiming to have exfiltrated approximately 20 terabytes of data. After negotiations collapsed, the group disclosed around 1.5 terabytes of patient information on the dark web.

In May, Kettering Health in Ohio suffered a severe disruption to its hospital information network due to an Interlock attack, causing significant operational setbacks across its entire clinical system. On May 26, the Qilin group targeted Covenant Health, a healthcare network in the New England region of the United States, infiltrating the clinical systems of three affiliated hospitals and exfiltrating the personal data of at least 7,864 patients. Evidence indicates that the institution was first listed on and later removed from a dark web data leak site.

Meanwhile, in Germany, the SafePay ransomware group attacked AWO Stadtkreis Gießen e.V., a healthcare and welfare institution, in late April. In Taiwan, ChangShen Hospital reportedly suffered a breach by the NightSpire group, resulting in the theft of approximately 800GB of patient data. In early June, the Middle East also saw incidents: American Hospital Dubai in the United Arab Emirates fell victim to a Gunra ransomware attack that incapacitated critical systems, with the attackers claiming to have encrypted about 450 million medical records.

Some breaches from the past have only recently been disclosed. In June 2025, McLaren Health Care in Michigan announced that a ransomware attack between July and August 2024 had compromised the personal data of more than 740,000 patients. This underscores the ongoing vulnerability of the healthcare sector, which has been consistently targeted since last year.

In response to this series of incidents, the FBI, CISA, and the U.S. Department of Health and Human Services (HHS) jointly issued an advisory in July, warning that the Interlock group poses a significant threat to healthcare institutions. Similarly, the Health Information Sharing and Analysis Center (H-ISAC) reported in June a sharp rise in ransomware

attacks on medical organizations and the exploitation of VPN vulnerabilities, urging heightened vigilance. Whereas ransomware groups once tended to avoid targeting healthcare providers and critical infrastructure to reduce law enforcement scrutiny, there is now a clear trend of focusing attacks on entities handling sensitive information, on the premise that such organizations are more likely to comply with ransom demands.

✓ Proliferation of Ransomware Attacks Crippling Public Services

In the second quarter of 2025, a series of ransomware attacks targeting public institutions, including local governments, county sheriff's offices, and courts—took place in rapid succession across the globe.

In mid-April, the Hamilton County Sheriff's Office in Tennessee experienced a complete system shutdown due to a ransomware attack. Around the same time, suspicious network activity was detected in Iowa County, Wisconsin, prompting authorities to take all systems offline as a precaution. On May 9, officials confirmed to residents that the resulting service delays were caused by a ransomware infection. On April 29, DuPage County in Illinois suffered a coordinated attack on the sheriff's office, courts, and clerk's office, forcing the suspension of their respective systems.

In some cases, entire local governments were brought to a standstill. On April 18, the city of Abilene, Texas, was attacked by the Qilin ransomware group, leading to server outages and the encryption of approximately 477GB of data. The attackers demanded payment by May 27, but the city refused to negotiate and instead undertook a complete replacement of its infrastructure. While no evidence has yet emerged of the stolen data being misused, residents were advised to monitor their accounts and change passwords as a precautionary measure.

On June 1, the city of Durant, Oklahoma, suffered a ransomware attack that disrupted its website and digital payment systems. The police communications centre also experienced network outages, raising concerns about potential delays in 911 emergency response. Around the same time, Lorain County in Ohio saw dozens of systems taken offline, causing a temporary suspension of court operations until restoration. Similarly, the Puerto Rico Department of Justice faced an attack on its Bureau of Criminal Information systems, which forced the temporary suspension of certificate issuance services.

Between April and June 2025, ransomware campaigns against public institutions primarily targeted administrative and judicial bodies, such as government agencies and courts, resulting in service disruptions that directly affected citizens' daily lives. Such attacks not only disrupt public services but also carry the risk of secondary damage, as stolen sensitive data may be exploited for malicious purposes. Heightened vigilance and robust security measures remain essential to counter these threats.

✓ Ransomware Attacks Exploiting Vulnerabilities

On April 8, 2025, Microsoft's security division, MSTIC, identified active exploitation of a zero-day vulnerability (CVE-2025-29824) in the Windows Common Log File System (CLFS) that enables privilege escalation from standard user privileges to SYSTEM level. In response, Microsoft promptly released an emergency patch. Analysis indicated that the RansomEXX (Storm-2460) group had exploited this flaw in a ransomware campaign, using the CLFS driver to

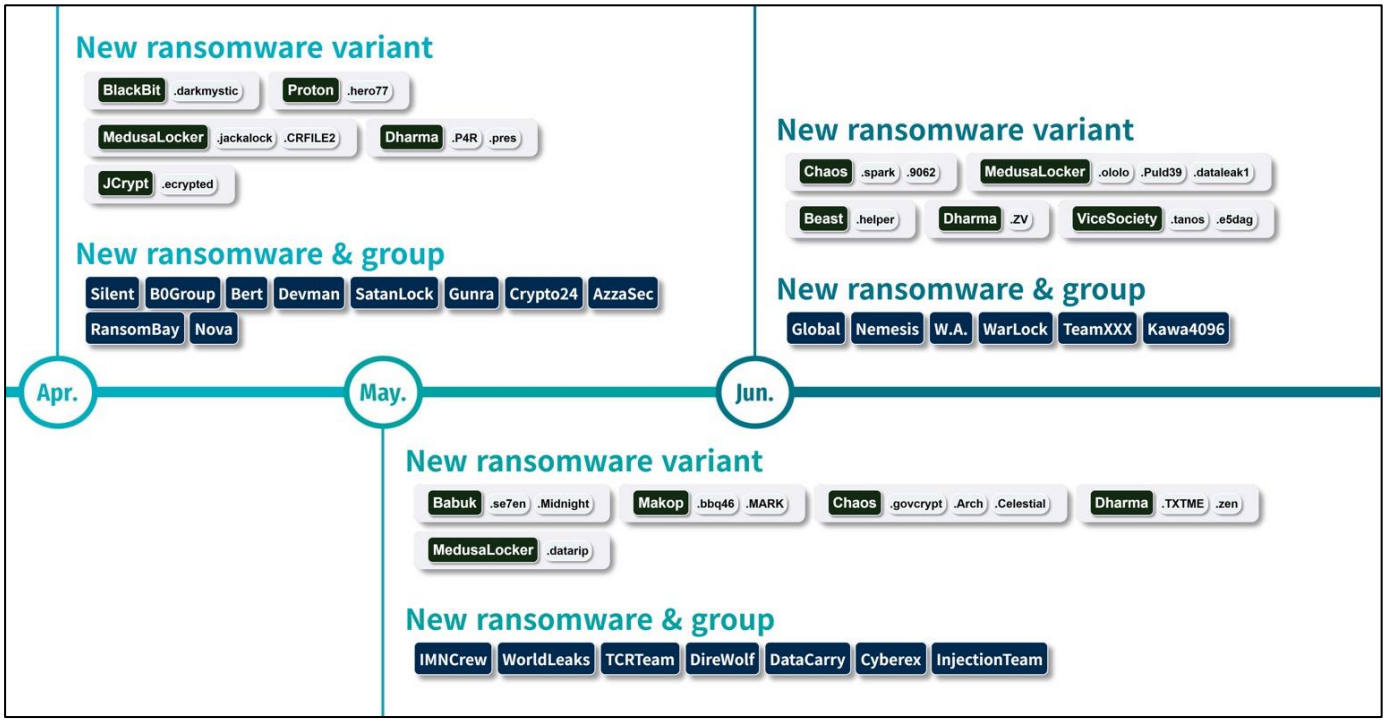
escalate privileges before deploying the PipeMagic[6] malware to inject a payload into winlogon.exe, subsequently performing LSASS[7] memory dumps and encrypting files.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) reported that the ransomware group KillSec (also known as Kill Security) exploited an authentication bypass vulnerability (CVE-2025-31161) in CrushFTP servers. This flaw allowed attackers to access file transfer servers without authentication and exfiltrate large volumes of sensitive data. The threat actors then attempted to extort victims, demanding payment in exchange for withholding the stolen information from public disclosure.

On April 28, it was disclosed that a vulnerability (CVE-2025-31324) in the metadatauploader endpoint of SAP NetWeaver Visual Composer was being actively exploited in the wild. The flaw enables attackers to upload web shells (helper.jsp, cache.jsp) to the server simply by sending specially crafted POST requests without authentication. Exploiting this access, adversaries established persistent footholds and attempted lateral movement within internal networks.

In June, evidence emerged of active exploitation of a path traversal vulnerability (CVE-2024-57727) in the SimpleHelp remote administration tool. CISA issued an urgent security advisory, warning that the flaw permits attackers to access arbitrary file system paths and upload malicious files. Incidents have been reported in which ransomware groups such as Play and DragonForce leveraged this vulnerability in their operations.

4. Activities of Emerging Ransomware and Groups



[Figure 3] New and Variant Ransomware

[6] PipeMagic: A plugin-based backdoor discovered in 2022

[7] LSASS (Local Security Authority Subsystem Service): A core process in the Windows operating system responsible for enforcing security policies, authenticating users, and generating access tokens.

In the second quarter of 2025, there was a marked increase in newly emerging ransomware groups, accompanied by a notable rebranding trend among established actors—continuing the patterns observed in the previous quarter. New entrants such as Gunra, Devman, and Kawa4096 conducted attacks across a range of platforms, including Windows, Linux, and ESXi[8]. Some actively adopted double extortion tactics, exfiltrating sensitive data prior to file encryption to increase pressure on victims. Notably, certain groups operated RaaS[9] platforms, rapidly expanding their reach by recruiting affiliates and implementing profit-sharing models. The following section outlines the major ransomware groups that either emerged or became active during this quarter.

- Gunra

Gunra emerged in April 2025 as a newly formed ransomware group, deploying a Conti-based variant in its operations. The group's initial intrusion vector remains unknown; however, once inside a target environment, it conducts internal reconnaissance before distributing ransomware variants for both Windows and Linux systems. Gunra employs a double extortion strategy, exfiltrating data prior to file encryption, and, in cases where negotiations fail, publishes the stolen information on its proprietary DLS[10] to increase pressure on victims.

- Devman

  Devman group, which began operations in April 2025, remains an active ransomware actor. In its early campaigns, the group leveraged ransomware developed by other threat actors rather than their own. However, from May—approximately one month after commencing operations Devman began deploying a custom ransomware strain based on the Mamona ransomware family. The group also operates its own DLS, branded Devman's Place, and actively uses X (formerly Twitter) to post about victim organizations or to showcase its technical capabilities, including sharing screenshots of its ransomware development environment.

- Nova

  Nova, a rebranded incarnation of the RALord group, launched its operations on April 28 with the establishment of its DLS Several victims listed on the DLS have been confirmed to be carryovers from the group's RALord period. Nova operates as a RaaS platform, collecting a percentage-based commission from its affiliates. The group offers ransomware variants for Windows, Linux, and VMware ESXi environments and is rapidly expanding its operations.

[8] ESXi: A hypervisor developed by VMware that is installed directly on server hardware, enabling the creation and management of virtual machines.

[9] RaaS (Ransomware as a Service): A profit model in which ransomware is offered as a service in exchange for payment.

[10] DLS (Dedicated Leak Sites): Websites operated by ransomware actors for publicity and the distribution of stolen data.

- Global

  Launched on June 2, 2025, Global is believed to be a newly established Ransomware-as-a-Service (RaaS) platform created by a threat actor previously involved in operating the BlackLock and Mamona ransomware strains. Similar to Nova, the group operates on a profit-sharing model with its affiliates and is actively recruiting partners. In addition to ransomware distribution, Global offers services such as VPS[11] based DLS hosting and multilingual negotiation capabilities via AI chatbots, providing a range of tools designed to enable attackers to conduct operations with greater ease.

[11] VPS (Virtual Private Server): A hosting service that uses virtualisation technology to partition a physical server, allowing each user to operate in an isolated environment as if using a dedicated server.

- Kawa4096

  Kawa4096 was identified in June 2025 as a newly emerging ransomware group. The group launched a Data Leak Site (DLS) featuring a design similar to that of the Akira group and adopted a ransom note format closely resembling Qilin's. In its first month of activity, Kawa4096 posted leak data pertaining to eight victim organizations, with most incidents reported in the United States and Japan.

- WorldLeaks

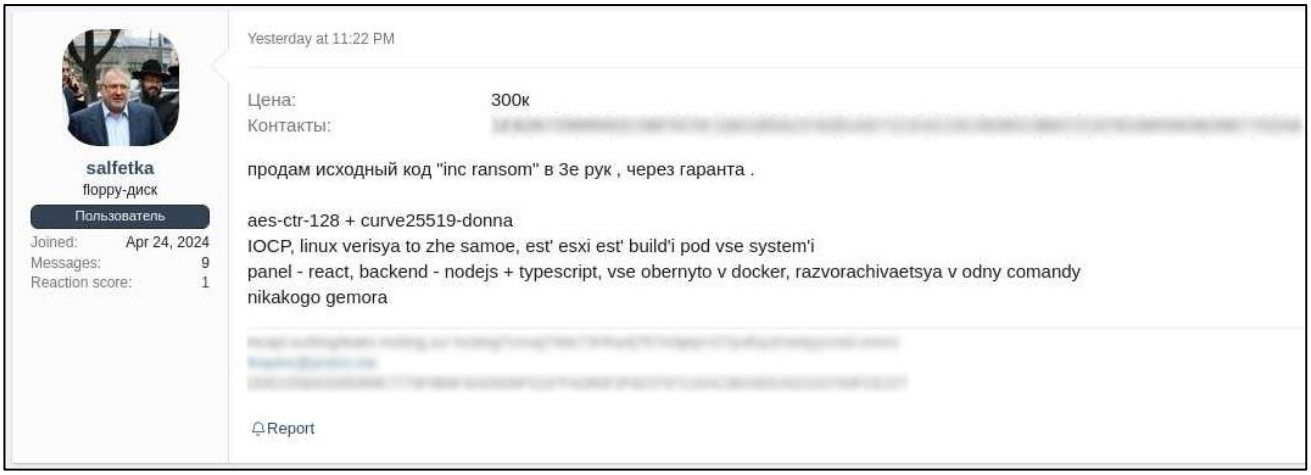
  WorldLeaks, believed to be a rebranded incarnation of the Hunters International group, which ceased operations on November 17, 2024, has shifted its strategy from conducting ransomware attacks to pursuing financial gain exclusively through data theft. The group claims to use custom-developed malware for data exfiltration, asserting that it is undetectable. Its DLS features categories for leaked data listings, announcements, and a dedicated section offering preview access to leaked data for verified journalists. Established in May, WorldLeaks claimed responsibility for attacks on 31 organizations during the second quarter, with most victims located in the United States and operating in the manufacturing or healthcare sectors.

- DireWolf

  DireWolf, which commenced operations in May 2025, claimed responsibility for attacks on 16 organizations during the second quarter, with Singapore and the manufacturing sector identified as the most affected. For each victim, the group documents which files were stolen and when they were uploaded subsequently publish the data on the Dark Web if negotiations fail or a set deadline passes. DireWolf ransomware creates an empty file at the path C:\runfinish.exe upon initial execution to determine whether the system has already been infected. It also disables and deletes event logs to hinder forensic investigations or analysis and removes recovery and backup files to prevent data restoration.

In-depth Analysis of the INC Ransomware Group

1. Overview



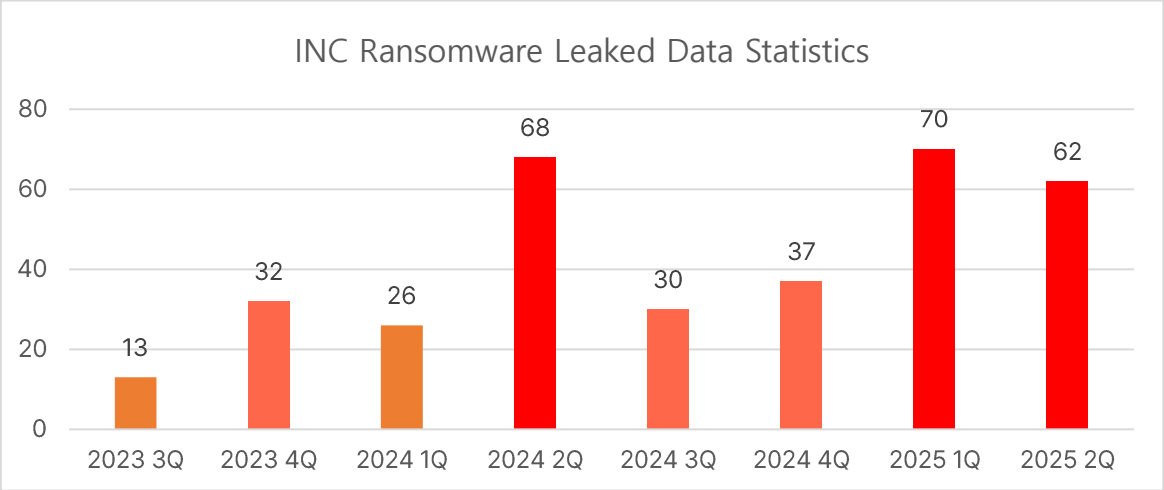
[Figure 4] Suspicion of INC Ransomware Source Code Sale

The INC ransomware group, which emerged in July 2023 as a Ransomware-as-a-Service (RaaS) operation, has claimed responsibility for attacks on 386 organizations to date, with the majority of victims located in the United States. Notably, the group exhibits strong similarities to the Lynx ransomware group, which appeared in late July 2024. This correlation aligns with intelligence indicating that INC sold its ransomware source code on dark web forums, strongly suggesting a potential link between the two groups.

The user “salfetka,” who is believed to have sold the ransomware source code, posted on two dark web forums offering both Windows and Linux/ESXi versions of the ransomware for sale. The asking price was set at USD 300,000 (approximately 420,000,000 KRW), with the number of buyers limited to three. According to details provided in the listing, the ransomware employs a hybrid encryption scheme combining AES-CTR-128 and Curve25519-Donna algorithms. Records indicate that salfetka has been active on the forum since March 2024. There is also evidence that he attempted to purchase network access rights for up to USD 7,000 and offered to share a portion of ransomware profits with initial access brokers—factors that further reinforce the likelihood that he is the genuine seller of the INC ransomware source code.

A critical piece of evidence is that salfetka included the URL to the INC ransomware’s dedicated page in his forum signature. Around the same period, Lynx ransomware—functionally similar to INC—made its debut. While some analysts interpret this as part of a rebranding effort, it is also plausible that the Lynx group is an entirely separate entity that acquired the source code and launched operations independently.

2. INC Ransomware Statistics



The INC ransomware group primarily targets sectors where disruption to operational continuity could result in severe consequences, such as healthcare, manufacturing, and public institutions. In practice, the majority of its victims belong to these high-impact industries. This targeting strategy is likely based on the assessment that attacks against entities handling highly sensitive data—such as medical institutions or major associations—carry a greater potential for leveraging stolen data to issue threats or cause secondary harm, thereby increasing the likelihood that victims will pay the ransom.

Furthermore, most recorded incidents have been concentrated in English-speaking countries, particularly the United States and the United Kingdom. Considering that the individual suspected of selling the ransomware source code on dark web forums is a Russian speaker, it is plausible that the INC group operates from within a Russian-speaking environment.

3. In-depth Analysis of INC Ransomware

The INC ransomware exists in two primary variants: a C++-based version developed in 2024 and a more recent Rust-based version, with slight differences in their respective encryption mechanisms. This report focuses on an analysis of the 2024 C++ version, with a brief comparison to the Rust variant provided in the concluding section.

Upon execution, the ransomware initiates its encryption preparation phase. The INC ransomware accepts a total of ten publicly documented parameters, along with one undocumented parameter, --safe-mode. Each parameter configures specific flag values that determine how the encryption process is carried out.

```
int __thiscall f_Help_4073D0(void *this)
{
  logging_406110("USAGE:\n");
  sub_404800(L"\t%s [ARGUMENTS]\n\n", this);
  logging_406110("ARGUMENTS:\n");
  logging_406110("\t--file <FILE>\t\tEncrypt only selected file\n");
  logging_406110("\t--dir <DIRECTORY>\tEncrypt only selected directory\n");
  logging_406110("\t--mode <MODE>\t\tChoose mode for file encryption (fast, medium, slow)\n");
  logging_406110("\t--ens\t\t\tEncrypt network shares\n");
  logging_406110("\t--lhd\t\t\tLoad hidden drives\n");
  logging_406110("\t--sup\t\t\tStop using process\n");
  logging_406110("\t--hide\t\t\tHide console window\n");
  logging_406110("\t--kill\t\t\tKill processes/services by mask\n");
  logging_406110("\t--debug\t\t\tEnable debug mode\n");
  return logging_406110("\t--help\t\t\tDisplay this message\n");
```

[Figure 5] INC Ransomware Execution Parameters

Execution Option	Description
--file	Encrypt specific files
--dir	Encrypt files located in a specified path
--mode	Set the encryption block size to fast, medium, or slow
--ens	Encrypt folders shared over the network
--lhd	Connects to and encrypt previously disconnected shared folders
--sup	Terminates backup, document, and similar programs to enable encryption
--hide	Hides the active ransomware console window
--kill	Terminates running processes and services
--debug	Displays debug messages during the encryption process
--help	Outputs the execution options
--safe-mode	Registers itself as a service and reboots in Safe Mode

Once the execution options have been configured based on the parameters provided, the ransomware proceeds to its encryption preparation stage. If the kill option is enabled, it enumerates all running processes and services, identifying those whose names contain specific strings, and terminates them to ensure that all files can be encrypted without interference.

```
pe.dwSize = 556;
hSnapshot = CreateToolhelp32Snapshot(0xFu, 0);
Process32FirstW(hSnapshot, &pe);
do
{
  pTargetProcess = TargetProcess;
  do
  {
    if ( wcsstr(pe.szExeFile, *pTargetProcess) )// "sql"
                                                // "veeam"
                                                // "backup"
                                                // "exchange"
                                                // "java"
    {
      v1 = OpenProcess(1u, 0, pe.th32ProcessID);
      v2 = v1;
      if ( v1 )
      {
        TerminateProcess(v1, 9u);
        CloseHandle(v2);
      }
    }
    ++pTargetProcess;
  }
  while ( pTargetProcess < &NumbOfProcess );
}
while ( Process32NextW(hSnapshot, &pe) );
return CloseHandle(hSnapshot);
```

[Figure 6] Exploration of Active Processes

Target Process Strings		
sql	veeam	backup
exchange	java	
Target Service Strings		
sql	veeam	backup
exchange		

Before commencing file encryption, the program determines the number of available processors and pre-allocates a worker thread pool sized at processor count × 4. It then creates an I/O Completion Port (IOCP) using the CreateIoCompletionPort function. The spawned worker threads are configured to wait for and process encryption task packets by invoking the GetQueuedCompletionStatus function.

```
HANDLE Create_IO_Port_4056A0()
{
  signed int v0; // edi
  signed int i; // esi
  HANDLE result; // eax

  GetSystemInfo(&SystemInfo);
  v0 = 4 * SystemInfo.dwNumberOfProcessors;
  CompletionPort = CreateIoCompletionPort(0xFFFFFFFF, 0, 0, 0);
  lpHandles = malloc(v0 >> 30 != 0 ? -1 : 4 * v0);
  for ( i = 0; i < v0; ++i )
    lpHandles[i] = CreateThread(0, 0, t_ReadAndWriteFile_405DC0, CompletionPort, 0, 0);
  result = CompletionPort;
  ExistingCompletionPort = CompletionPort;
  return result;
```

[Figure 7] Thread Pool Creation

The ransomware decodes the ransom note to be created within the encrypted folders. The ransom notes, in both text and HTML formats, are stored within the binary as Base64-encoded data. After decoding, the malware appends the victim's ID—retrieved from the file—to the content and stores the address of the decrypted data in a global variable. It then generates the ransom note as a file within each targeted folder.

```
pcbBinary = 0;
v0 = lstrlenA(b64_note);
CryptStringToBinaryA(b64_note, v0, 1u, 0, &pcbBinary, 0, 0);
v1 = malloc(pcbBinary);
CryptStringToBinaryA(b64_note, v0, 1u, v1, &pcbBinary, 0, 0);
lpString2 = v1;
v1[pcbBinary] = 0;
lpString2 = ChangeUserID_4062C0(v1);
v2 = lstrlenA(b64_note_html);
CryptStringToBinaryA(b64_note_html, v2, 1u, 0, &pcbBinary, 0, 0);
v3 = malloc(pcbBinary);
CryptStringToBinaryA(b64_note_html, v2, 1u, v3, &pcbBinary, 0, 0);
RansomNote = v3;
v3[pcbBinary] = 0;
result = ChangeUserID_4062C0(v3);
RansomNote = result;
return result;
```

[Figure 8] Ransom Note Decryption and Victim ID Appending

If the lhd option is enabled, the ransomware scans drives from A through Z to locate all hidden network drives on the system. When such a drive is found, it attempts to mount it in order to encrypt its contents.

```
do
{
  if ( !v0 )
    break;
  if ( GetVolumePathNamesForVolumeNameW(v4, szVolumePathNames, 0x78u, &cchReturnLength)
    && lstrlenW(szVolumePathNames) == 3 )
  {
    szVolumePathNames[0] = 0;
  }
  else
  {
    v6 = lpszVolumeMountPoint[v0--];
    if ( SetVolumeMountPointW(v6, v4) )
    {
      if ( flag_dbg_4287B0 )
        logging_404800(L"   [+] Mounted %s\n", v6);
    }
    else if ( flag_dbg_4287B0 )
    {
      LastError = GetLastError();
      logging_404800(L"   [-] Failed to mount %s Error: %d\n", v6, LastError);
    }
    v5 = FirstVolumeW;
  }
}
while ( FindNextVolumeW(v5, v4, 0x8000u) );
```

[Figure 9] Hidden Drive Mounting

Once the thread pool for encryption has been created, the ransomware proceeds to execute its encryption routine. Unless a specific file or directory has been designated, it scans all drives from A through Z. When an accessible drive is detected, the ransomware deletes its Volume Shadow Copies to prevent data recovery.

Unlike typical ransomware, which removes stored Volume Shadows via PowerShell or WMI, INC ransomware achieves this by invoking the DeviceIoControl API and passing the value 0x53c028—corresponding to IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE—to restrict the shadow copy storage size, effectively eliminating the Volume Shadow Copies.

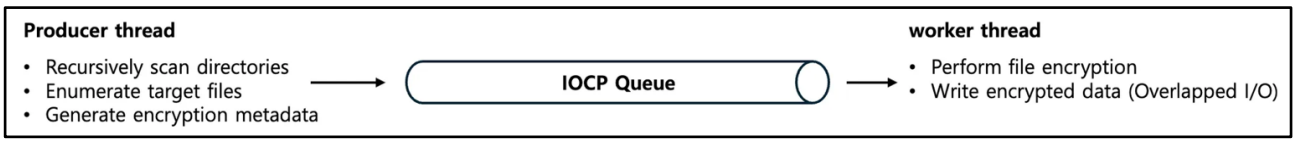
```
else
{
  if ( DeviceIoControl(result, 0x53C028u, InBuffer, 0x18u, 0, 0, &BytesReturned, 0) )
  {
    if ( dword_4287B0 )
      print_log(L"[+] Successfully delete shadow copies from %c:/ \n", a1);
  }
```

[Figure 10] Deletion of Volume Shadow Copies via DeviceIoControl

Once the deletion is complete, the ransomware creates a thread for each drive path as an argument, designating all files—excluding those in exception paths or with excluded extensions—as targets for encryption.

Excluded File Extensions		
exe	msi	dll
inc	INC	
Excluded Paths		
windows	program files	program files(x86)
$RECYCLE.BIN	appdata	

The INC ransomware utilises Windows' I/O Completion Port (IOCP)–based asynchronous processing model to perform file encryption. It first creates an IOCP queue and spawns dedicated threads for each target drive to enumerate files, compiling a list of files to be encrypted. The ransomware then sends a work structure—containing the necessary encryption details such as the file path, handle, and encryption key—to the IOCP queue. Worker threads retrieve the work structures from the queue via GetQueuedCompletionStatus and execute the encryption tasks accordingly.



[Figure 11] Asynchronous File Encryption Using IOCP

Before generating encryption, keys and commencing the encryption process, the malware performs a write test of approximately 0x23 bytes on the target file to verify access and write permissions. If the write operation fails, it proceeds to take ownership of the file and modify its Access Control List (ACL) to forcibly obtain write privileges. Additionally, if the sup option is enabled, the malware forcibly terminates any process occupying the target file, rechecks its write accessibility, and then initiates the encryption preparation phase.

```
FileAttributesW = GetFileAttributesW(pObjectName);
SetFileAttributesW(pObjectName, FileAttributesW & 0xFFFFFFFE);
if ( ChekeFileWrite_405800(pObjectName)
  || f_sup_42927C && Kill_Related_Process_4053E0(pObjectName) == 1 && ChekeFileWrite_405800(pObjectName)
  || (FileW = SetACL_407280(pObjectName), FileW == HANDLE_FLAG_INHERIT)
  && (LOBYTE(FileW) = ChekeFileWrite_405800(pObjectName), FileW) )
```

[Figure 12] Asynchronous File Encryption Using IOCP

First, the malware decodes the attacker's Curve25519 public key, which is stored in the binary in Base64-encoded form. It then uses the CryptGenRandom API to generate a random 32-byte private key. Using this private key and the attacker's public key, it performs a Curve25519 Elliptic Curve Diffie-Hellman (ECDH) operation to derive a shared secret. Because a shared secret can be computed using one party's public key and the other party's private key, the ransomware can encrypt files without exposing the attacker's private key, and decryption is possible by generating the same shared secret with the attacker's private key and the victim's public key.

The resulting shared secret is hashed using the SHA-512 algorithm, and the first 16 bytes of the hash are used as the AES encryption key. This AES key undergoes a Key Expansion process to produce a 176-byte key schedule table, which is passed to worker threads via the IOCP queue for use in file encryption.

After key generation, the ransomware creates a structure containing the target file's metadata and a footer to be appended to the end of the encrypted file. This structure is then sent to the encryption worker through the queue. The worker parses the received structure and executes conditional branches in the order 1 → 2 → 0 → 3, based on the value of a specific flag field.

Flag Value	Flag Description
0	Reads the target encryption block based on the size of the file to be encrypted.
1	Encrypt the file data into the buffer using AES-128.
2	Appends a footer containing the generated public key to the end of the file.
3	After encryption, renames the original file's extension to .INC using the MoveFile API.

```
switch ( Overlapped->flag )
{
  case 0:                                   // case 0: get block
    field_encMode_138 = Overlapped->file_pubkey_F8.enc_process_init_flag_40;
    if ( !field_encMode_138 )
    {
      filesize_high_24 = Overlapped->filesize_high_24;
      szTargetFile = Overlapped->szTargetFile;
      giga_2_flag = Overlapped->file_pubkey_F8.szBlock_44 >> 31;// check_2gigabyte
      szBlock = Overlapped->file_pubkey_F8.szBlock_44;
      v39 = filesize_high_24;
      if ( szBlock + *&Overlapped->next_block_offset_low_28 >= __SPAIR64__(filesize_high_24, szTarget
```

```
case 1:                                   // case 1: encrypt
  szWriteBlock_4 = Overlapped->szWriteBlock_4;
  expand_key_38 = Overlapped->sha_first16_expand_key_38;
  enc_data_buf = Overlapped->bufEncFile;
  ++Overlapped->file_pubkey_F8.encBlockCount_4c;
  v4->flag = 2;
  encrypt_401300(expand_key_38, enc_data_buf, szWriteBlock_4);
  WriteFile(v4->hEncTarget_14, v4->bufEncFile, szWriteBlock_4, 0, v4);
  hIoPort = lpThreadParameter;
  ReadFile = ::ReadFile;
  goto LABEL_2;
```

```
case 2:                                   // case 2: write footer
  v38 = Overlapped;
  Overlapped->cur_block_offset_low_8 = Overlapped->szTargetFile;
  v4->cur_block_offset_high_C = v4->filesize_high_24;
  hFile = v4->hEncTarget_14;
  v4->flag = 0;
  WriteFile(hFile, &v4->file_pubkey_F8, 0x50u, 0, v38);
  hIoPort = lpThreadParameter;
```

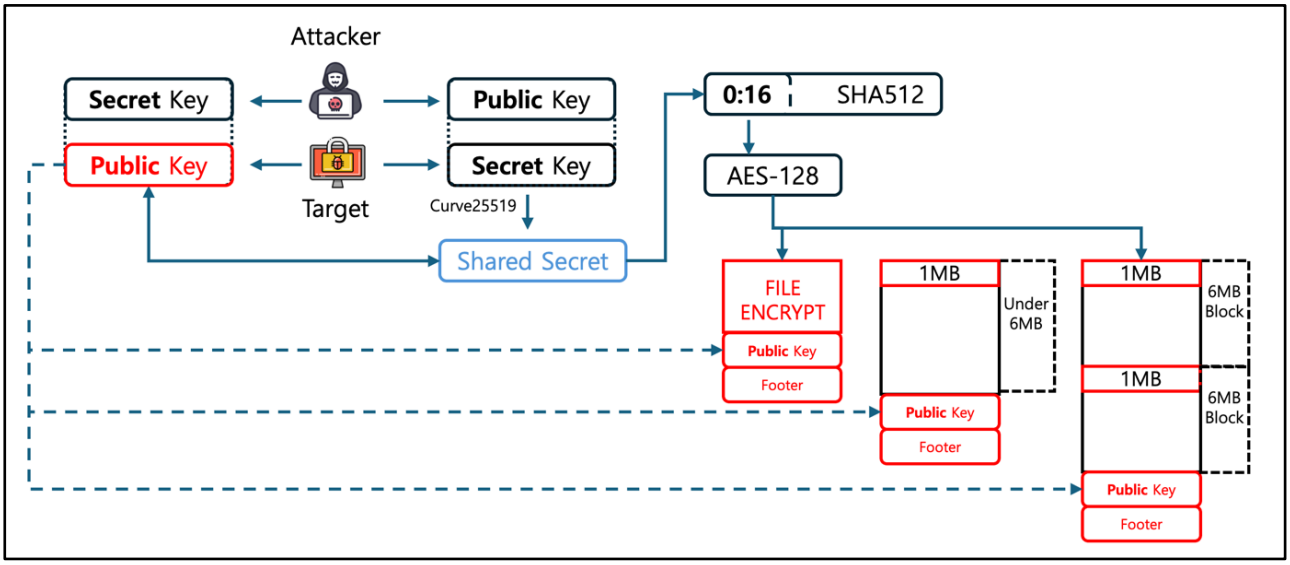
```
case 3:                                   // case 3: End
  CloseHandle(Overlapped->hEncTarget_14);
  InterlockedDecrement(&Addend);
  MoveFileExW(v4->buf_origin_target_filename_18, v4->p_EncryptedFileName_1c, 9u);
  j___free_base(v4->buf_origin_target_filename_18);
  j___free_base(v4->p_EncryptedFileName_1c);
  j___free_base(v4->bufEncFile);
  j___free_base(v4);
  hIoPort = lpThreadParameter;
```

[Figure 13] Processing Logic by Flag

INC ransomware encrypts files using 1MB blocks by default and performs partial encryption depending on the file size.

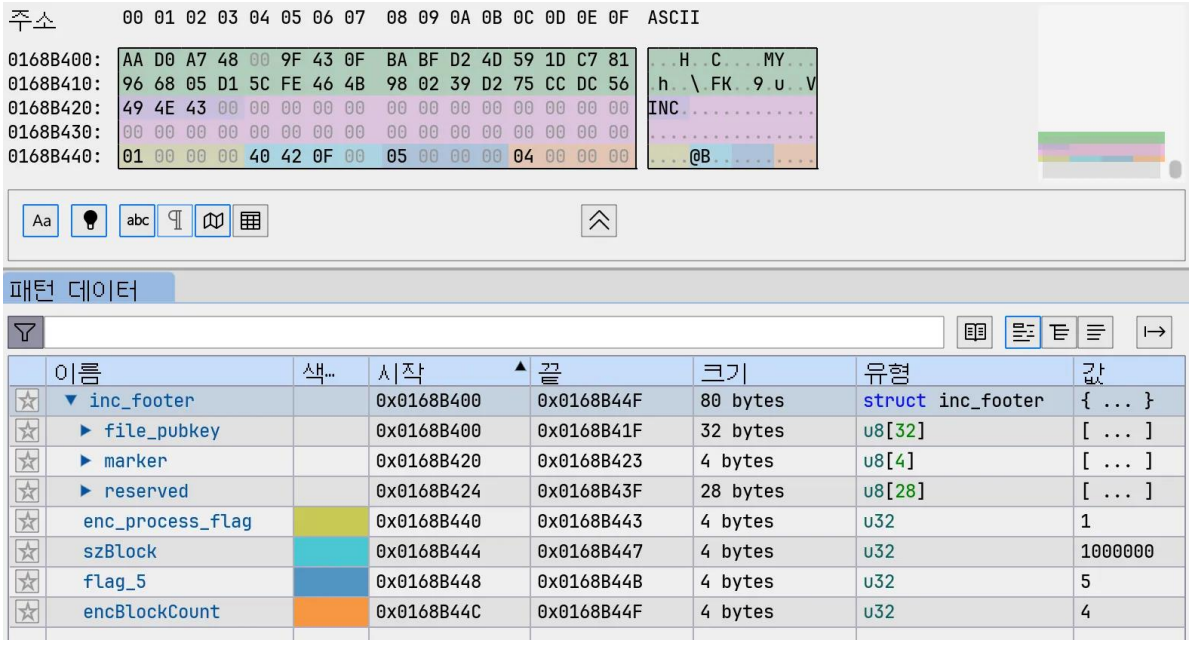
- If the file size is 1MB or less, the entire file is encrypted.

- If the file size exceeds 1MB but is 6MB or less, only the first 1MB of the file is encrypted.
- If the file size exceeds 6MB, it is split into 6MB blocks, with the first 1MB of each block encrypted.



[Figure 14] File Encryption Using Shared Secret

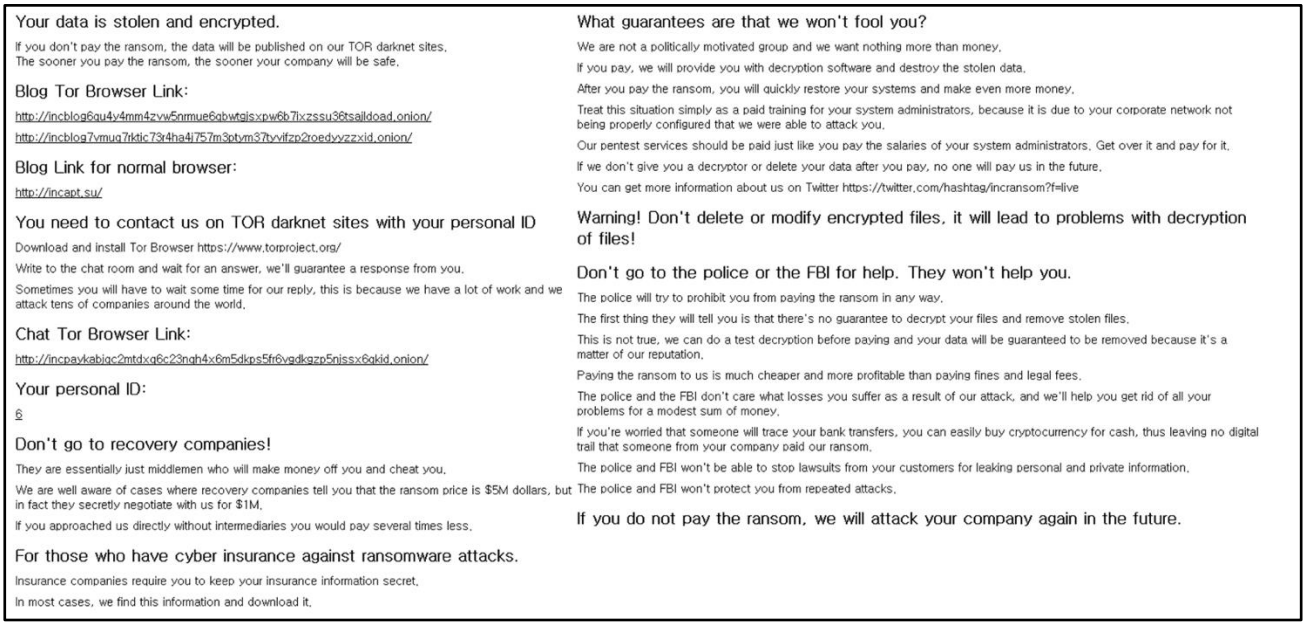
When file encryption is complete, a 0x50-byte footer structure is appended to the end of the file. This structure contains the public key paired with the secret key used for encryption, the marker string “INC,” encryption options, block size, and the number of encrypted blocks.



[Figure 15] INC Ransomware Footer Information

After completing file encryption, the ransomware changes the desktop wallpaper to display the ransom note's contents and then terminates.

[Figure 16] Desktop Wallpaper of a System Infected with INC Ransomware



[Figure 17] INC Ransomware HTML Ransom Note

4. Rust-based INC Ransomware

In May 2025, a new Rust-based variant of the INC ransomware—believed to be the successor to the original C++ version—emerged. Like its predecessor, the Rust version retains the core operational mechanisms, including its IOCP-based architecture, the use of structures to deliver target file information to worker threads, file encryption and storage based on flag values, and block-based encryption. However, certain implementation details, such as program execution parameters and aspects of the encryption process, have been modified.

Execution Option	Function Description	Original	Rust-Based
--file	Encrypt specific files	O	O
--dir	Encrypt files in a specified path	O	O
--mode	Sets encryption block size to fast, medium, or slow	O	O
--ens	Encrypt folders shared over the network	O	X
--lhd	Connects to and encrypt disconnected shared folders	O	X
--sup	Terminates backup and document programs before encryption	O	O
--hide	Hides the active ransomware console window	O	O
--kill	Terminates running processes and services	O	X
--debug	Displays debug messages during encryption	O	X
--def	Outputs only the ransom note without encrypting files	X	O
--help	Outputs the execution options	X	O
--version	Displays the executable file name	X	O
--proc	Terminates a specified process (split from original --kill option)	X	O
--serv	Terminates services by mask (split from original --kill option)	X	O

[Figure 18] Execution Options in Rust Version

The ransomware collects all files within the target directory excluding those located in specified folders or with certain extensions and proceeds with encryption. In the Rust version, some target paths and extensions have been

modified. These changes are reflected by filtering out the newly excluded paths and extensions from the scan scope, then encrypting the remaining files. In the table below, extensions and paths highlighted in red indicate new targets in the Rust version, while items shown with strikethrough represent strings that have been removed.

Excluded File Extensions		
exe	~~msi~~	dll
~~inc~~	INC	log
Excluded Paths		
windows	program files	program files(x86)
$RECYCLE.BIN	appdata	programdata
all users	sophos	

As with the C++ version, the file encryption process in the Rust variant still uses Curve25519 to generate a shared secret. However, the subsequent hashing method and encryption algorithm have been altered. In the original version, the shared secret was hashed with SHA-512, and the first 16 bytes of the hash were used as the AES-128 encryption key. In the Rust version, SHA-256 is used instead, and file encryption is performed with the Salsa20 algorithm.

5. Conclusion

The INC ransomware group operates under a Ransomware-as-a-Service (RaaS) model, enabling attackers to easily execute campaigns without developing ransomware themselves. This structure significantly lowers the entry barrier to cybercrime, attracting a wide range of affiliates and accelerating the "sterilization" and industrialization of criminal activity. Given the evidence that INC's source code has been sold, there is a risk that other threat actors could use it to develop similar ransomware or propagate new variants. Such secondary threats are not confined to the activities of a single group but may lead to the emergence of multiple-treat actors, underscoring the importance of implementing robust security measures in response.

6. IoCs

INC Ransomware SHA256
508a644d552f237615d1504aa1628566fe0e752a5bc0c882fa72b3155c322cef
7f104a3dfda3a7fbdd9b910d00b0169328c5d2facc10dc17b4378612ffa82d51
463075274e328bd47d8092f4901e67f7fff6c5d972b5ffcf821d3c988797e8e3
502332b1b5a04ec85ef72e75535469f9e1ae61fe6b1aa6b55274626f320415c2
02472036db9ec498ae565b344f099263f3218ecb785282150e8565d5cac92461
b97417afbd789a21c3f4fe33bf7501bf2cf3f5c735cb4a1258ffd8a32b443e6a
33c1f433dcd7dcccbd8bdd6d418f63285b42484a3022c9ccfb88cc24be18cd5d
e17c601551dfded76ab99a233957c5c4acf0229b46cd7fc2175ead7fe1e3d261
b62c5c88f31f9c06ac7302fab1a5d05aa7a46a302c32a63ffa238f3b5b6aa3fb
5a8883ad96a944593103f2f7f3a692ea3cde1ede71cf3de6750eb7a044a61486
864c1c803ef3b4ca6ab50482820d4da1c5cb23378ca52c689b32e205ae4c1ccf
a5925db043e3142e31f21bc18549eb7df289d7c938d56dffe3f5905af11ab97a
909033ac13a6114191e0821fa49aee1bf5517d7849251b4d1c135f4cd7ffeecf
4da86516bf85633f3db22c328825e5fe1e30ef4581179a3b886a1a2ed8ecb401
26cca9c6d1c591761dd3c1cdbadc589f28bd87b7ddfe1961491396de09577fc8
1df4a74fbe8a9875a4386960f1006d29de7907af830b4c8a30a643e752299030
ee1d8ac9fef147f0751000c38ca5d72feceeaae803049a2cd49dcce15223b720
d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6
INC Ransomware(Rust Ver) SHA256
b1815ef993b2649be791f0cf4249e502e7c3763fe69451b8b32508089e15d103
61f70b9a0bde499d764807fe24517e64ea0130a3f6e493ead360058e59854776
e86487e21cde16fb15341fa7f9cee283944873c82bb06a4c25e32c0b16d08a85
fd0dbc6d941ff76e5204df4c644ba0d3241d05995f30e6b837618cd9dcc8b99c
17317ee3c9bd706ef2942a38f55c05176e4abdf377a5b72250d89ebf2a795ca0
71a2cdf9d39c4ba7b7bc3091c38b0be1624b3171fb3a649ad2a6430f9ae30f82
5bcb8a717e160a88b7cf95f0ad778ad7446041565356beb332676e33ff4f1829
c3d8c86844d7bb86dea31bcb0510542fb59bc3bc67a4e3df59f72da5c8509f54
56da934a117689fe0f26d0cf6cf7650f94e2f9d625d9ac066ae0096a3fc7eab4
be9e1fd4dcf8a644aba70c8e92fa07a54d0ce96fb74217b48991700d281083bd
INC Ransomware Structs
struct struct_enc // size = 0x148 {

```
    int overlapped_status;              // IOCP status flag or result code
    int write_block_size;               // Current write block size
    int cur_block_offset_low;           // Current block offset (lower 32 bits)
    int cur_block_offset_high;          // Current block offset (upper 32 bits)
    int reserved;                       // Reserved field
    int h_target_file;                  // Target file handle
    int p_original_filename_buf;        // Pointer to original filename buffer
    int p_encrypted_filename;           // Pointer to encrypted filename
    int target_file_size_low;           // Target file size (lower 32 bits)
    int target_file_size_high;          // Target file size (upper 32 bits)
    int next_block_offset_low;          // Next block offset (lower 32 bits)
    int next_block_offset_high;         // Next block offset (upper 32 bits)
    int p_encryption_buffer;            // Pointer to encrypted data buffer
    int enc_flags;                      // Flag (e.g., full encryption indicator)
   char sha_first16_expand_key[176]; // AES key expansion from the first 16 bytes of the SHA-512 output

    int sha_second16;                   // Second 16-byte value from the SHA-512 output
    char reserved_EC[12];               // Reserved field
    inc_footer footer;                  // INC footer appended to the end of the encrypted file}

struct inc_footer // size = 0x50
{
    char file_public_key[32];       // File public key used for encryption
    char footer_marker[4];          // Fixed marker "INC\0"
    char reserved[28];              // Reserved space
    int init_flag;                  // Initialisation flag indicating encryption status (1 = encrypted)
    int encryption_block_size;      // Block encryption size (e.g., 0x100000 = 1MB)
    int reserved_flag;              // Reserved flag
    int encrypted_block_count; // Number of encrypted blocks
};
```

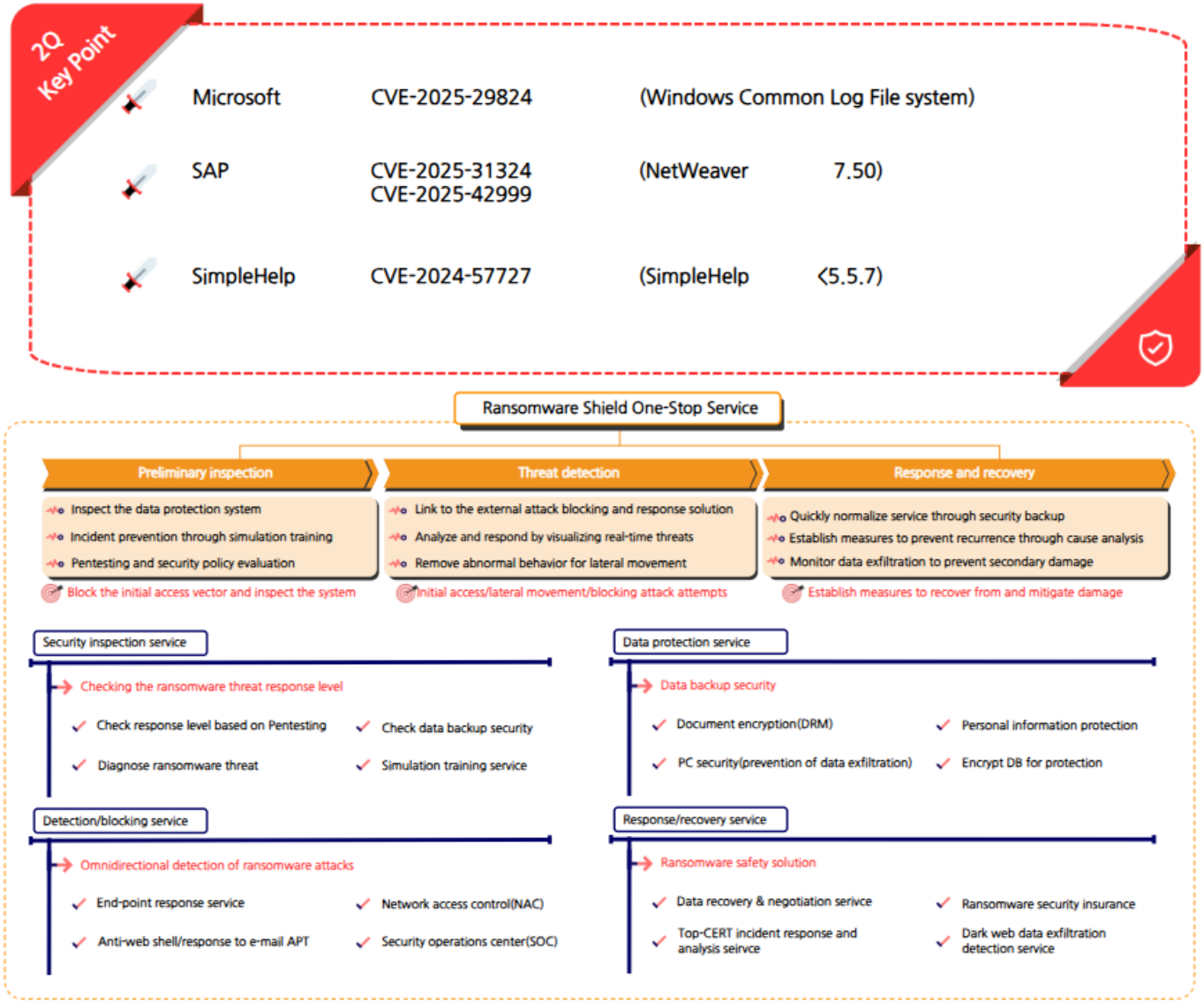
Ransomware Mitigations

1. Guidelines for Ransomware Response

This quarter, the Play ransomware group exploited vulnerabilities in Cisco ASA firewalls in conjunction with the CLFS privilege escalation zero-day (CVE-2025-29824) to achieve both initial access and privilege escalation. Qilin, believed to have absorbed members from RansomHub, nearly doubled its number of attacks, demonstrating a surge in activity.

The major ransomware groups continued to employ a double extortion strategy: exploiting vulnerabilities in network infrastructure and weaknesses in authentication to gain initial access, escalating privileges to system level, exfiltrating data, and ultimately leaking the stolen information if negotiations failed.

To counter these threats, organisations should promptly apply security patches to externally exposed assets such as firewalls and VPN appliances, strengthen account-based authentication with MFA, and implement behaviour-based monitoring within internal systems to detect suspicious privilege escalation and data movement.

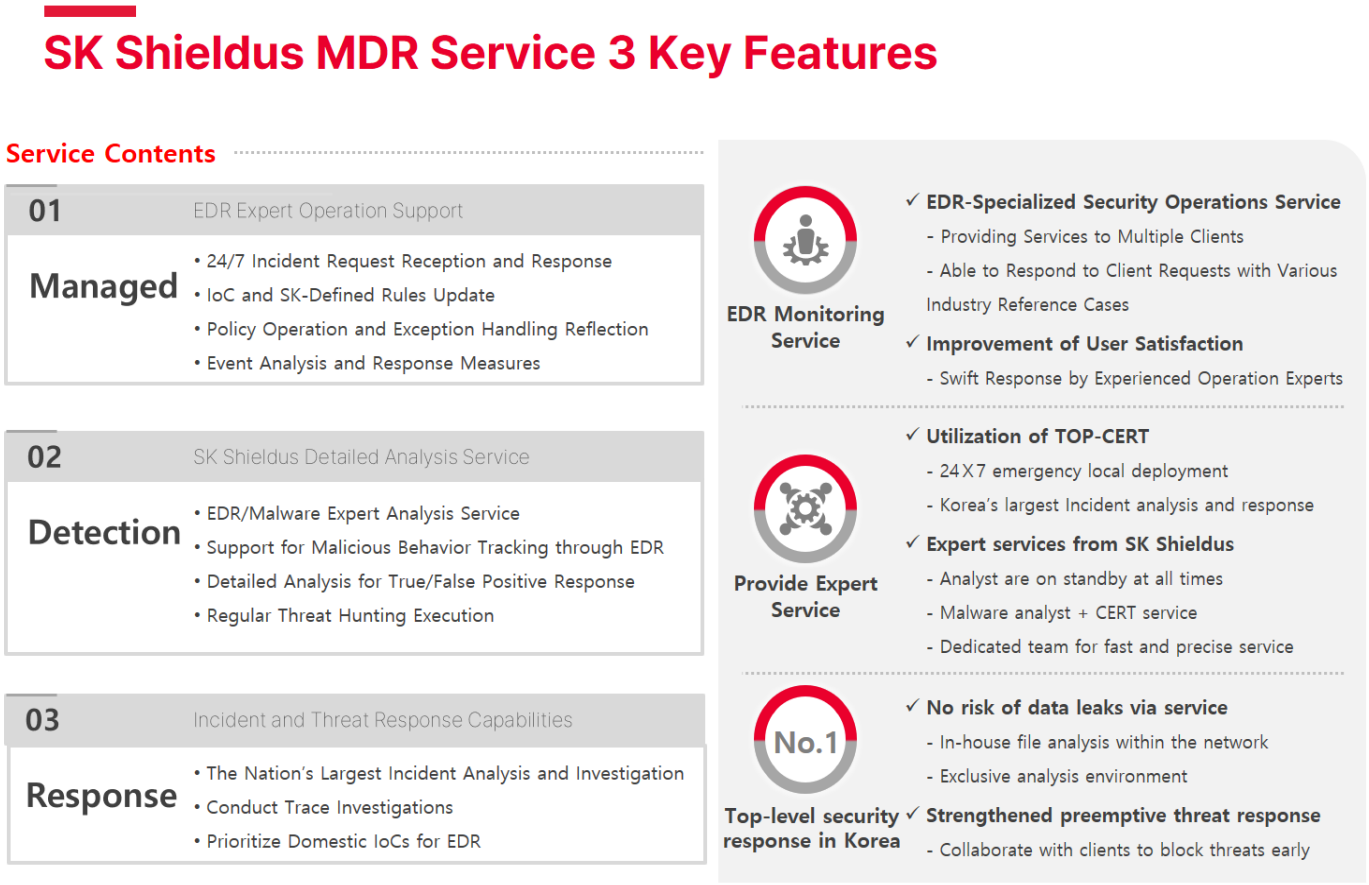


2. SK Shieldus MDR Service

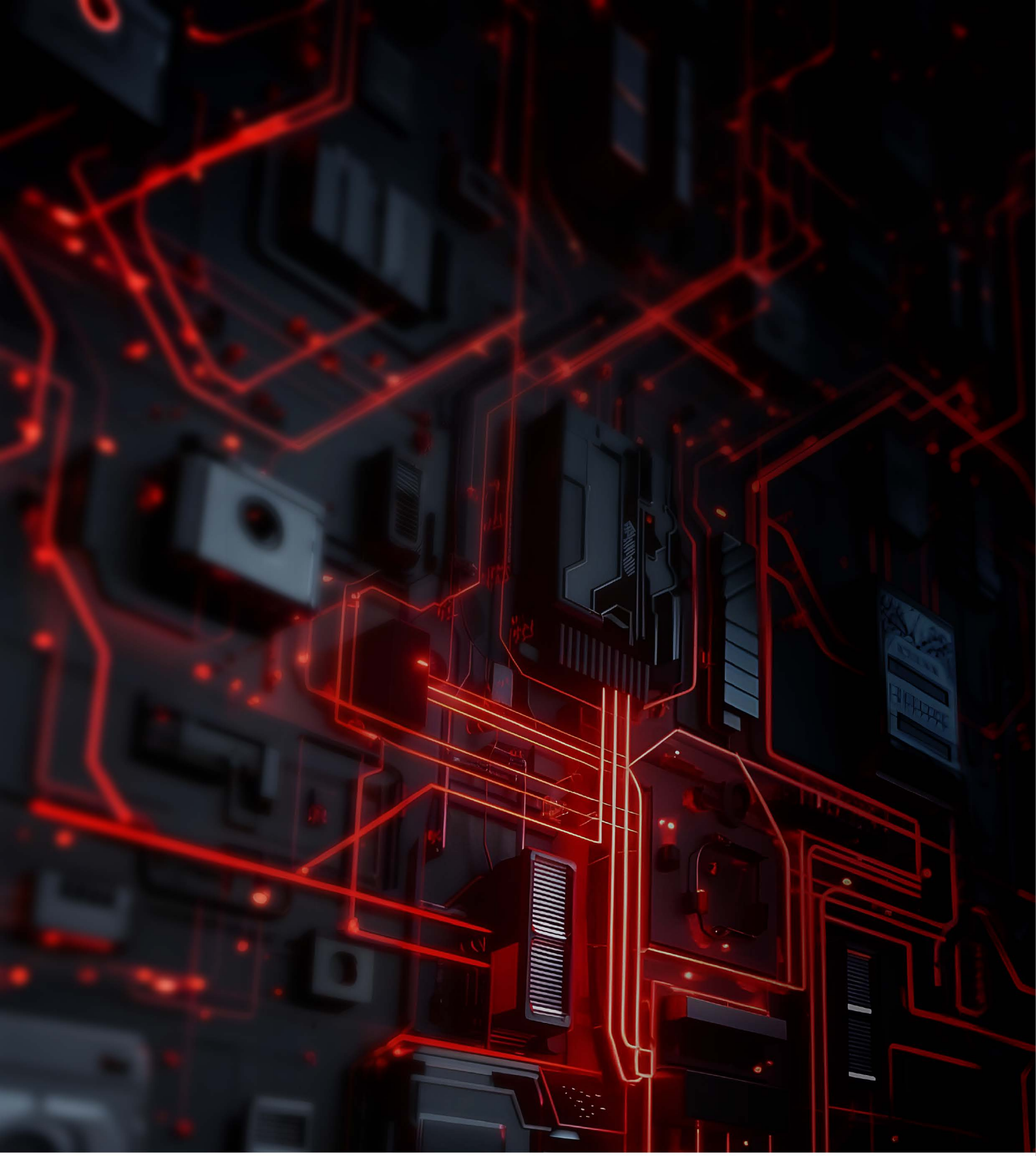
To effectively combat ransomware, leveraging SK Shieldus MDR (Managed Detection and Response) service [12]can be a highly effective approach. With ransomware operators now employing sophisticated strategies and advanced evasion techniques, traditional security measures alone are often insufficient to mitigate the threat.

SK Shieldus addresses this challenge by offering an MDR (Managed Detection and Response) service that provides real-time network monitoring, detects abnormal activity, and enables immediate response when necessary. While proactive prevention remains the most critical defence against ransomware, swift action following an incident is equally vital to minimise damage.

Accordingly, organisations are advised to consider SK Shieldus' MDR (Managed Detection and Response) service, which delivers tailored security solutions based on rapid and accurate incident investigation and analysis conducted by dedicated experts.



[12] MDR (Managed Detection and Response) Service: A managed security service that protects organisations from cyberattacks through real-time threat detection and response.



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