Keep up with Ransomware

Gunra Ransomware Targeting the Korea Financial Sector

■ Overview

In July 2025, the number of ransomware incidents recorded in the South Korea sector declined to 483 cases, down from 512 incidents in June. Although the total number of cases exhibited a slight decrease, the sophistication and strategic diversity of the attacks were, in fact, further intensified. Notably, the exploitation of vulnerabilities for initial intrusion, attempts at automating negotiations through AI-driven mechanisms, and direct confrontations with law enforcement agencies emerged as defining characteristics of ransomware activity in July.

Evidence has also surfaced indicating that the Gunra group, which emerged in April, conducted attacks targeting Korea financial institutions. On July 14, a victim institution experienced a temporary disruption in service delivery due to a ransomware attack, but was able to complete recovery and resume operations within approximately four days. However, the impact of the incident extended beyond mere service interruption, as it escalated into a data breach. The perpetrator claimed, via their dedicated Leak Sites, to have exfiltrated the institution's database and posted messages soliciting collaborators to assist in data analysis. The leaked data was confirmed to comprise compressed files totaling 13.2 terabytes, with the attacker further escalating pressure on the victim by threatening to release the stolen data incrementally.

The Akira group appears to have achieved infiltration even within environments protected by multi-factor authentication (MFA[1]), exploiting patched SonicWall SSL-VPN [2]appliances. This has raised concerns regarding the potential existence of a zero-day vulnerability, underscoring the persistent threat posed by sophisticated attacks that remain difficult to defend against until such vulnerabilities are officially disclosed and patched. Another notable case involved the proliferation of Warlock ransomware through exploitation of the ToolShell vulnerability (CVE-2025-53770) in Microsoft SharePoint. This attack affected approximately 400 servers, including those belonging to critical U.S. government agencies such as the National Nuclear Security Administration (NNSA) and the National Institutes of Health (NIH).

Attackers are exhibiting not only heightened technical sophistication but also continuous evolution in their operational strategies. The Global group, for instance, incorporated AI chatbots into negotiations with victim organizations, automating the interface and seeking to expedite the negotiation process. This development is regarded as a representative example of the growing trend toward service-oriented and automated operations within the RaaS[3] ecosystem.

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

[2] SSL-VPN (Secure Sockets Layer Virtual Private Network): A device that enables remote access to internal networks over the internet via an encrypted communication channel.

[3] RaaS (Ransomware-as-a-Service): A business model in which ransomware is offered as a service, enabling virtually anyone to easily create and deploy ransomware attacks.

Law enforcement agencies are further intensifying their measures in response to adversarial activities. The U.S. Federal Bureau of Investigation (FBI) has initiated legal proceedings to seize approximately $2.4 million worth of Bitcoin held by members of the Chaos ransomware group. On July 25, the FBI, Europol, and the police forces of Germany and the Netherlands jointly succeeded in seizing the dedicated Leak Sites operated by the BlackSuit ransomware group. This group had listed more than 180 victims on its site, with total ransom demands reportedly amounting to nearly $500 million.

Meanwhile, there have also been instances of groups resuming activity despite law enforcement sanctions. BreachForums—a hacking forum that had been shut down following the arrests of five key operators by the French Cybercrime Brigade (BL2C) in February and June—was restored on July 26. According to an announcement by the forum's administrator, the individuals apprehended did not possess actual administrative privileges and were merely assigned titles to obscure the identities of the true operators. The administrator further acknowledged that the forum's temporary suspension in April was indeed caused by a vulnerability in the MyBB forum software, but asserted that the issue has since been resolved and that the previous domain was taken down at the request of law enforcement agencies.

In contrast, the Russian hacking forum XSS remains offline. In July, international law enforcement agencies—including Europol—arrested an individual in Ukraine who is believed to have been one of the forum's administrators. The arrested suspect is reported to have been active within the cybercrime ecosystem for approximately two decades, accumulating around 7 million euros through advertising and brokerage commissions. Since this arrest, the XSS forum has not been restored.

Ransomware News

Gunra group ransomware and data theft attack on South Korean financial institution

- On 14 July, a ransomware attack on a South Korean financial institution caused a service outage.
- Despite service restoration, a 13.2TB database was exfiltrated.
- Stolen data analysed and disclosure announced

Seizure of illicit cryptocurrency proceeds from the Chaos group

- The U.S. FBI initiated legal proceedings to seize approximately USD 2.4 million worth of Bitcoin assets held by the Chaos ransomware group
- The U.S. Department of Justice seeks forfeiture of ransomware proceeds from victim wallets
- This action, aimed directly at criminal proceeds, is regarded as a significant expansion of law enforcement efforts beyond infrastructure takedowns.

International joint operation to dismantle BlackSuit group infrastructure

- Through a coordinated operation, the FBI, Europol, and the German and Dutch police seized BlackSuit group's Dedicated Leak Site
- This action, which directly dismantled infrastructure, is regarded as a notable case of delivering tangible impact on the ransomware ecosystem.

BreachForums re-emerges despite law enforcement pressure

- BreachForums, previously shut down following the operator's arrest, returned on 26 July.
- The operator claimed that those arrested never held actual administrative authority and had only been given titles to attract attention.
- Resumption of Operations Following Completion of Security Vulnerability Patching and Domain Replacement

Hacking forum XSS shut down by law enforcement

- In July, Europol and other law enforcement agencies arrested the XSS forum operator in Ukraine.
- The operator is estimated to have been active for 20 years, generating approximately € 7 million in profits.
- Following the arrest operation, the XSS forum remains closed.

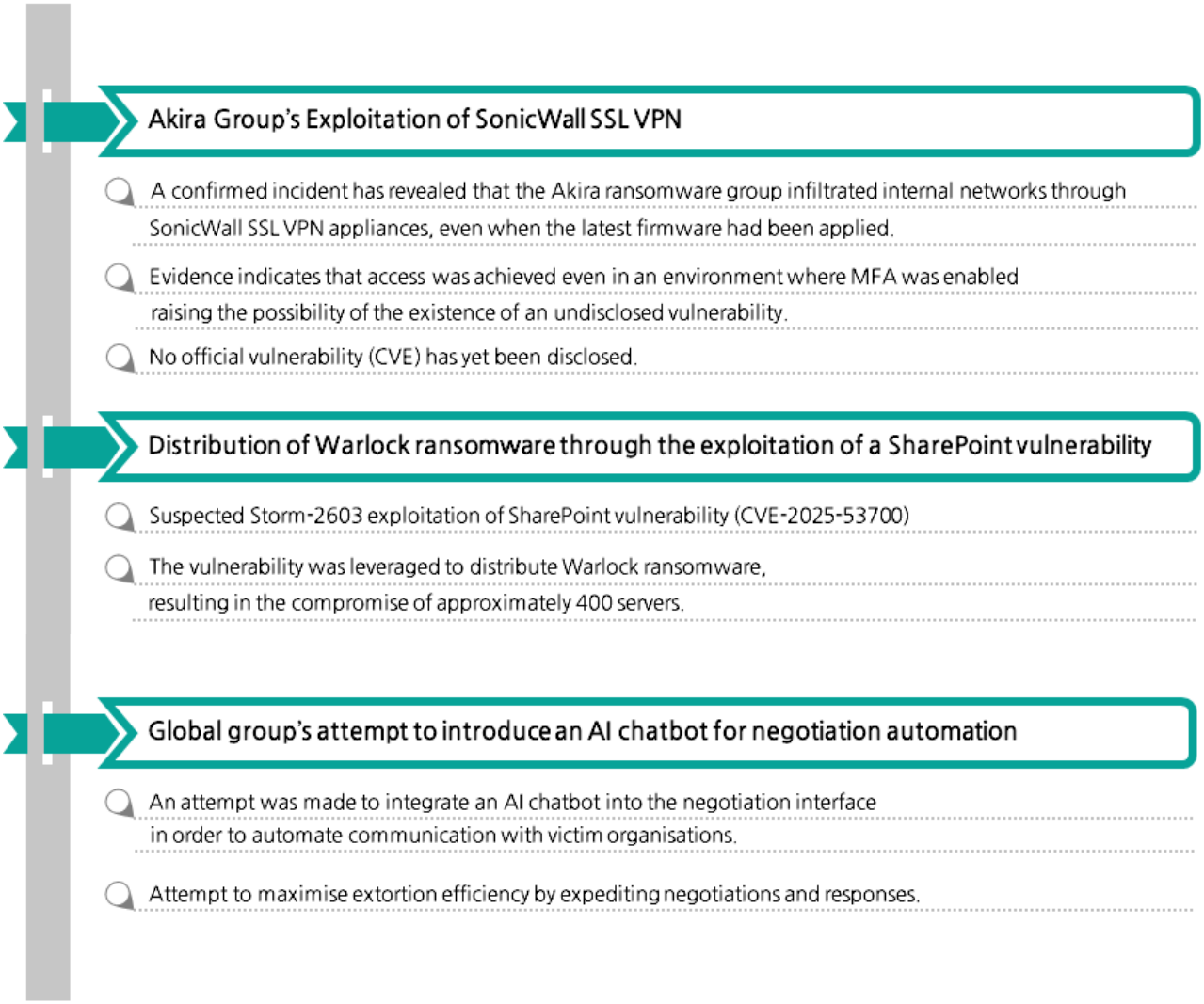

Figure 1. Ransomware Trends

Ransomware Threats

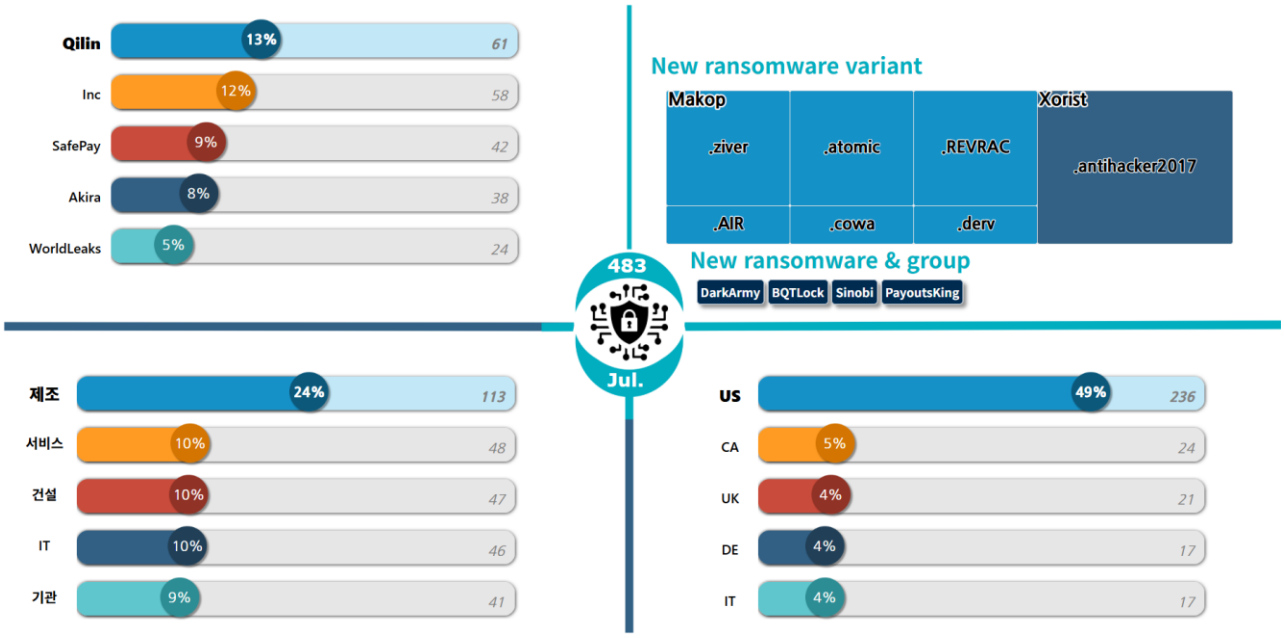

Figure 2. Status of Ransomware Threats in July 2025

New Threats

A total of 483 ransomware incidents were confirmed in July, during which four new ransomware groups emerged. Each of these groups published details of their attacks on dedicated Leak Sites under their own operation. The confirmed number of incidents attributed to each group was as follows: DarkArmy with 11 cases, BQTLock with 2 cases, Sinobi with 5 cases, and Payoutsking with 18 cases.

Figure 3. DarkArmy's dedicated Leak Sites

At the bottom banner of DarkArmy's dedicated Leak Sites, the Chinese slogan "睡觉的乌鸦" (which translates to "Sleeping Crow") is prominently displayed, alongside contact information listing both QQ and WeChat accounts. Taken together, these elements strongly suggest that the developers and operators are likely Chinese-speaking individuals or entities.

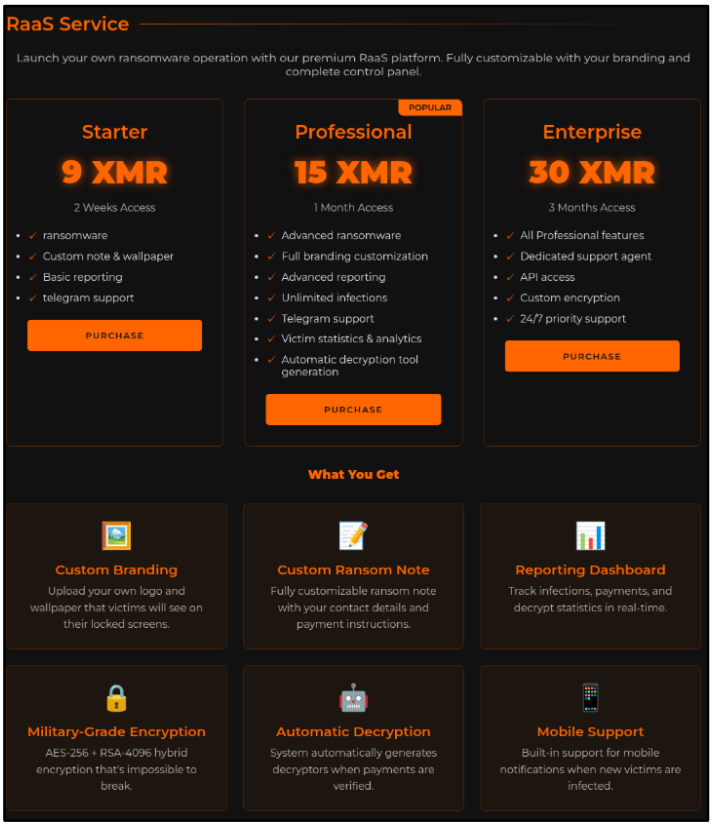

Figure 4. BQTLock RaaS Dashboard

BQTLock operates its own portal, known as BQT RaaS, which provides subscribers with a fully customizable builder[4] and a comprehensive statistics dashboard. The portal delineates three tiers of subscription plans—Starter, Professional, and Enterprise—priced at 9 XMR, 15 XMR, and 30 XMR, respectively. Subscriptions at the Professional level or higher unlock additional features, including ransom note branding customization, victim statistics and reporting, and automatic decryption tool generation. This all-in-one RaaS platform structure is poised to accelerate market proliferation by enabling even non-developer threat actors to rapidly establish and manage ransomware campaigns.

[4] Builder: A tool that enables attackers to configure detailed options—such as the ransomware's encryption algorithm, ransom amount, victim message, and target directories—via a graphical user interface (GUI) or command-line interface, and automatically generates the final executable file.

Top 5 Ransomware

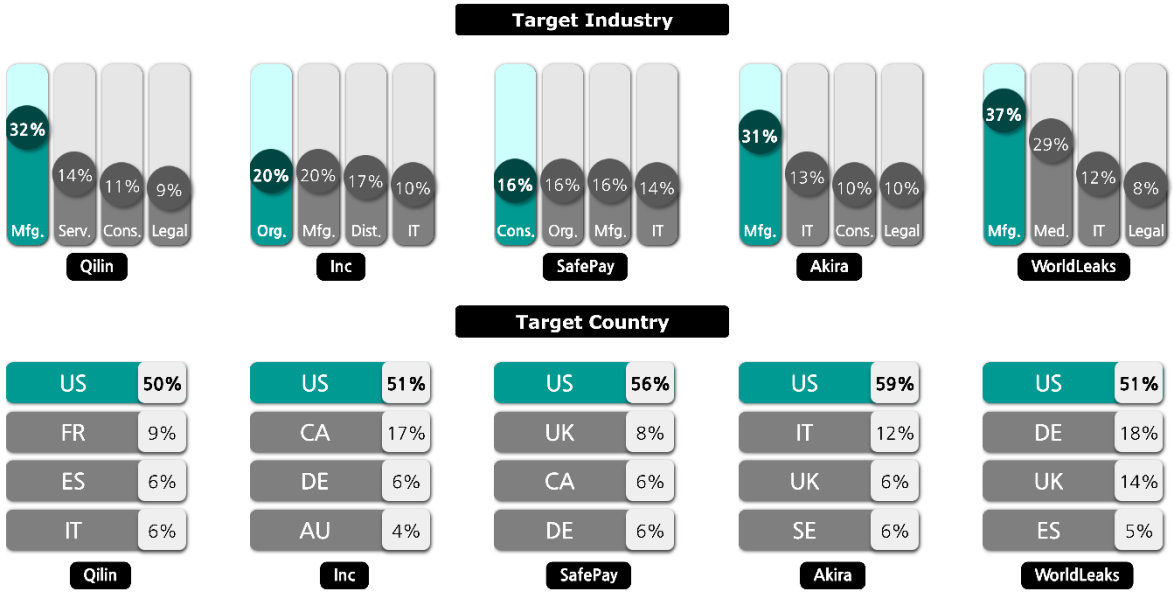

Figure 5. Major Ransomware Attacks by Industry and Country

On July 29, the Qilin group claimed responsibility for an attack on Custom Food Ingredients, a Malaysian food ingredient manufacturer, asserting that they had penetrated the company's core manufacturing systems and exfiltrated internal data. The group heightened pressure on the victim by publishing a list of production and operations-related documents on their dedicated leak site.

On July 31, the Inc group disclosed that it had compromised West Virginia Primary Care Association, a public healthcare organization in the United States. The group posted details of the incident on its dedicated leak site, demanding contact from the victim and warning that the stolen data would be published if negotiations failed. Additionally, Inc targeted the administrative office of Albemarle County, Virginia, exfiltrating thousands of personal records—including residents' and employees' names, addresses, Social Security Numbers (SSN), and driver's license numbers.

In early July, the SafePay group claimed responsibility for an attack on Ingram Micro, a global IT distribution company. In the immediate aftermath, the company's website and order processing systems experienced temporary outages. SafePay subsequently listed the victim's name on its dedicated leak site and threatened to release approximately 3.5TB of exfiltrated data. On July 26, the group further announced an attack against Southwest Florida Dermatology, a U.S. dermatology clinic, stating that they had exfiltrated sensitive internal data, including patients' medical records.

On July 25, the Akira group claimed to have exfiltrated data from Dunlap Codding, an intellectual property law firm based in Oklahoma City, United States. On its dedicated leak site, the group posted a notice announcing the impending release of approximately 19GB of data, including client files, financial documents, and records related to patents and court proceedings. Additionally, the Spanish online beauty retailer Druni fell victim to an attack, resulting in the leakage of 40GB of data, which included employee identification cards, financial records, and customer information.

On July 21, the WorldLeaks group claimed responsibility for an attack against Proactive Engineering Consultants, a U.S.-based engineering services firm. The group subsequently disclosed the incident on its dedicated leak site and released approximately 5.3TB of design and project-related data. WorldLeaks also targeted the American construction company Thomas Bennett & Hunter, publishing internal project and operational data exfiltrated from the organization.

■ Focus on Ransomware

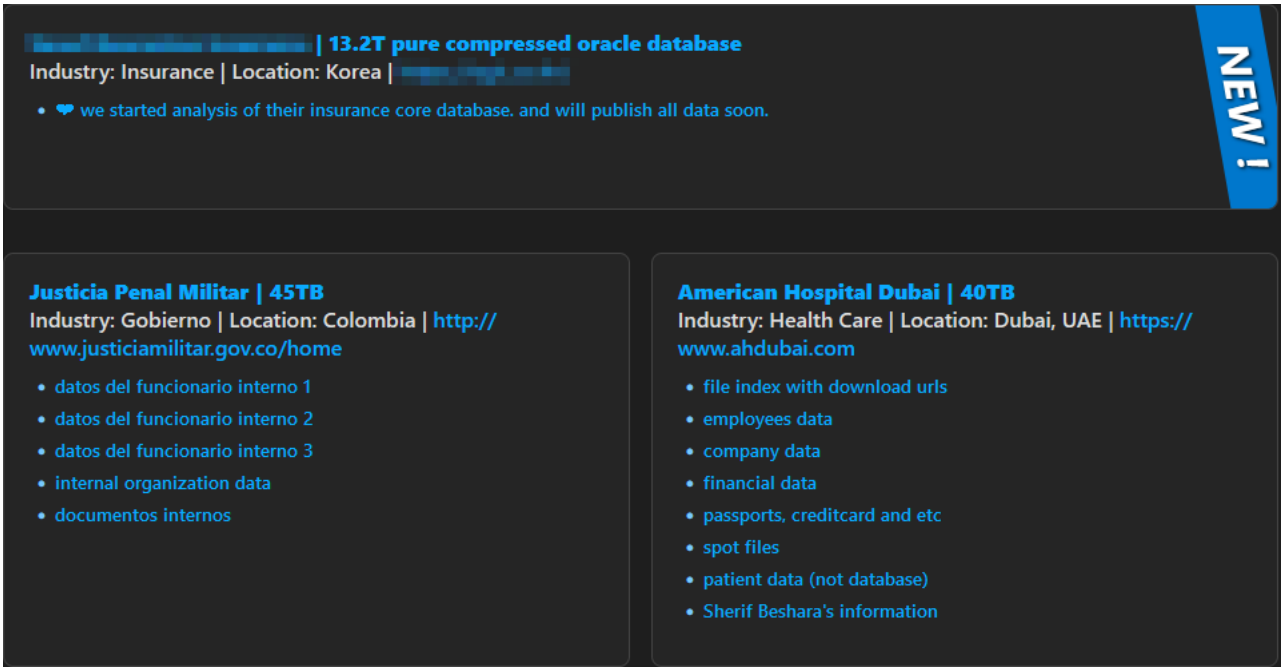

Figure 6. Gunra Dedicated Leak Site

The Gunra ransomware group was first identified in April 2025 and has since listed a total of 16 victims on its dedicated leak site. The site operates on the Tor network and specifies, for each victim, details such as company name, industry, country, the types of data exfiltrated, date of posting, and negotiation deadline. Gunra publicly discloses the nature and posting time of stolen data for each victim, and, if negotiations fail or the designated deadline passes, the group proceeds to release the exfiltrated materials in full on the dark web.

Gunra is characterized by the imposition of short negotiation deadlines and the use of multiple anonymous communication channels. Its ransom notes emphasize that victims must make contact within five days, providing both a Tox ID and an email address to facilitate communication. Initially, the group may offer complimentary decryption of selected files; if the victim fails to respond, Gunra escalates the pressure by listing the victim on its dedicated leak site and releasing a portion of the exfiltrated data. Should negotiations become protracted, the group threatens to publish additional data or even the entire dataset, thereby applying incremental pressure on the victim. Notably, among the published victims is a Korea financial sector company that suffered an attack in July 2025, for which Gunra issued an explicit warning regarding the release of the compromised data, significantly intensifying the coercion.

To date, two variants of the Gunra ransomware have been identified: one targeting Windows and the other targeting Linux environments. The Windows version leaves a ransom note in each directory following encryption, whereas the Linux variant does not generate a ransom note. Instead, it selectively encrypts files based on the path, file extension, and encryption ratio specified as execution parameters. Both versions employ a combination of full and partial encryption techniques—determined by file size and type—to maximize efficiency and speed. This report analyzes both variants, systematically outlining Gunra's operational methodologies and technical characteristics in order to facilitate effective preparedness against ransomware threats.

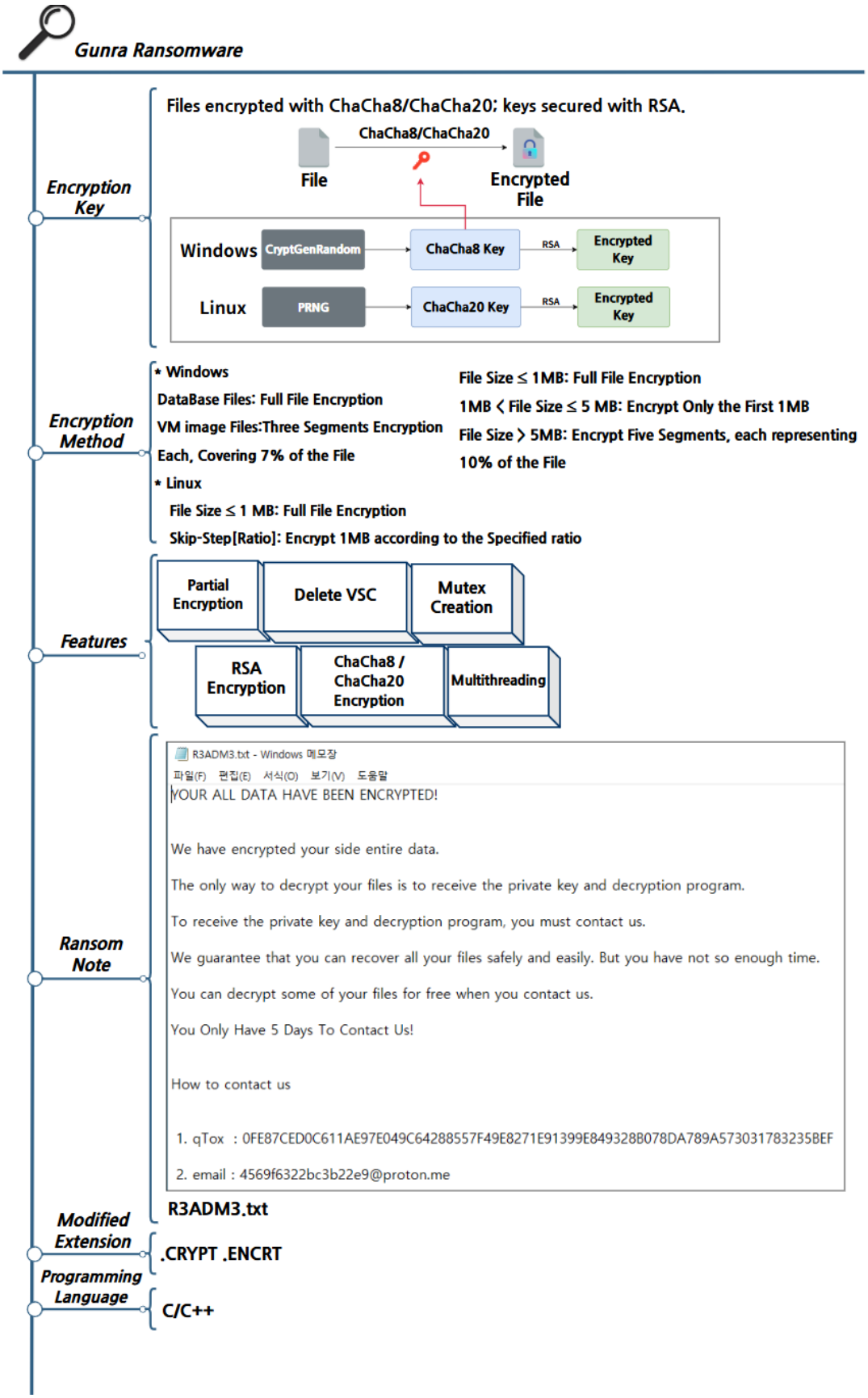

Figure 7. Overview of Gunra Ransomware

Gunra Ransomware Strategy

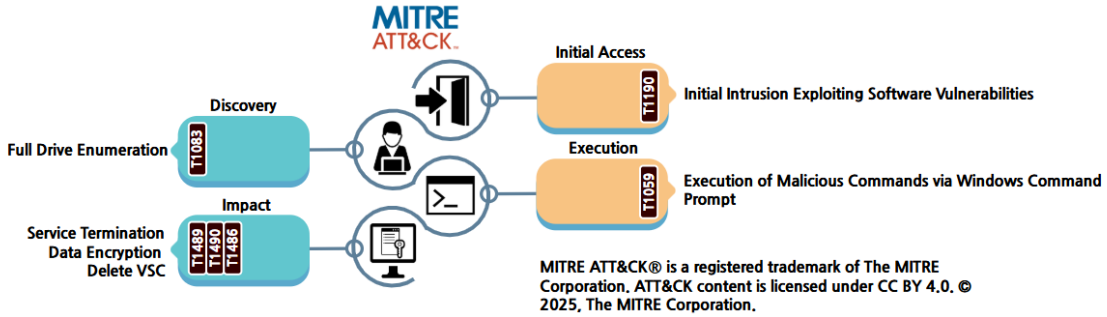

Figure 8. Gunra Ransomware Attack Strategy

Gunra Ransomware (Linux Version)

The Linux variant of Gunra ransomware is engineered to enable precise control over encryption behavior through a wide array of execution parameters, allowing attackers to flexibly specify target file locations, extensions, encryption intensity, and key storage methods. The arguments and functionalities of the Linux version are summarized in the table below.

Category	Description
--threads / -t	Specify the number of file encryption threads
--path / -p	Designate encryption targets
--exts / -e	Specify extensions of files to be encrypted (all: all files, disk: block devices)
--ratio / -r	Set encryption interval (in MB)
--keyfile / -k	Path to RSA public key file (.pem)
--store / -s	Path to store the encryption key
--limit / -l	Maximum encryption size (GB; 0: encrypt the entire file)

Table 1. Execution Parameters for Gunra Ransomware (Linux Version)

In the Linux version, the -p parameter is used to specify the target file or directory for encryption. If the specified target is a single file, only that file will be encrypted; if a directory is provided, the ransomware recursively traverses the directory and its subdirectories, encrypting all eligible files within.

-The -e option designates the file extensions to be targeted for encryption. If this option is omitted or set to 'all', all files—except those with explicitly excluded extensions—will be subject to encryption. When set to ‘disk’, only block device files present on the system are encrypted. Notably, files with the extension .ENCRT (indicating already encrypted files) and ransom note files named R3ADM3.txt are included in the list of extensions excluded from encryption.

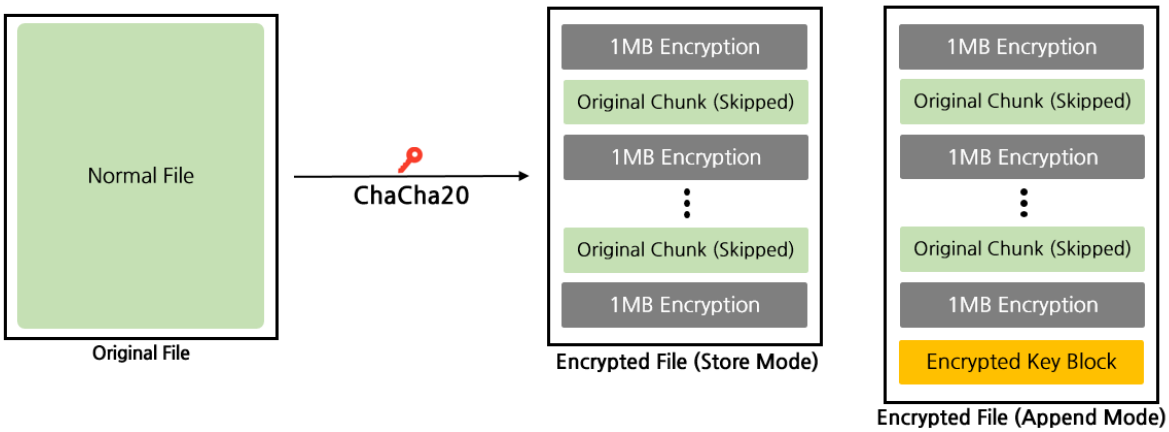

Figure 9. Encryption Process of Gunra Ransomware (Linux Version)

The Linux version of Gunra ransomware utilizes the ChaCha20 algorithm for file encryption. Target files are selected according to the path and file extension specified via the -p and -e parameters, and encryption is performed using a partial encryption method based on the value of the -r parameter. Gunra encrypts files in 1MB segments and, by employing the -r parameter, defines the size of the interval to skip after each encrypted 1MB block. For example, with -r=5, the ransomware encrypts 1MB, skips the next 5MB, then encrypts another 1MB, repeating this pattern throughout the file. Although the interval between encrypted segments varies according to the parameter, the size of each encrypted segment remains fixed at 1MB. Additionally, the -l parameter allows the attacker to specify the maximum encryption size in gigabytes. Upon completion of encryption, the ChaCha20 key, nonce,[5] as well as the values for the -r and -l parameters are stored separately, with the storage method determined by the presence or absence of the -s parameter.

When the -s parameter is used, Store Mode is enabled, and the encrypted key block is stored separately in the specified directory. During this process, the ransomware verifies the existence of the target directory and generates a key file named [Filename].keystore, based on the original file name. If the -s parameter is not specified, Append Mode is applied, and the encrypted key block is appended to the end of the encrypted file.

[5] Nonce: A randomly generated value used in encryption to ensure security and uniqueness.

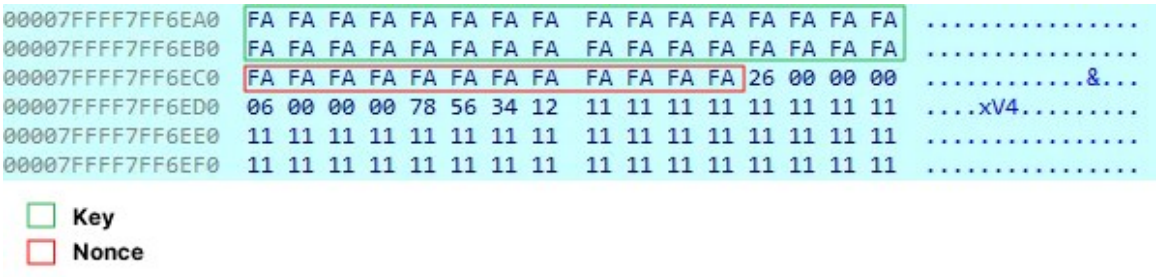

Figure 10. Vulnerable Key Generation in Gunra Ransomware (Linux Version)

Additionally, a design-level vulnerability has been identified in the key generation process of the Linux version. In standard implementations, the encryption key and nonce should be generated with sufficient randomness to ensure unpredictability, and then encrypted with an asymmetric key so that only the attacker can decrypt them. However, Gunra's Linux variant employs an inefficient approach, generating random values one byte at a time and concatenating them. During this process, the program calls the time(0) function for each byte, setting the current time in seconds as the seed. Since generating a 32-byte key and a 12-byte nonce takes less than one second, it is highly likely that multiple bytes will be generated using the same seed, resulting in repeated values. Even if the time changes during the generation process, the change in the seed is minimal, making it relatively easy for an attacker to predict the key and nonce.

Gunra Ransomware (Windows Version)

Unlike its Linux counterpart, the Windows version of Gunra ransomware is designed to operate without any external execution parameters. Critical values—such as the mutex name used to prevent repeated infections during execution and the RSA public key employed to protect the encryption keys—are embedded directly within the binary.

Upon execution, the ransomware creates a mutex named '375345635adfwef39' to prevent duplicate instances from running simultaneously. It then sequentially scans all system drives to generate ransom notes and identify files for encryption. During this process, only the user folder and its subdirectories within the C drive are traversed, whereas all other drives are scanned from their root directories. Specific folders, file extensions, and filenames are excluded from encryption, and the identified exceptions are listed in the table below.

Folder Name	Extension and File Name
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, Trend Micro	.exe, .dll, .lnk, .sys, msi, R3ADM3.txt, CONTI_LOG.txt

Table 2. Encryption Exceptions for Gunra Ransomware (Windows Version)

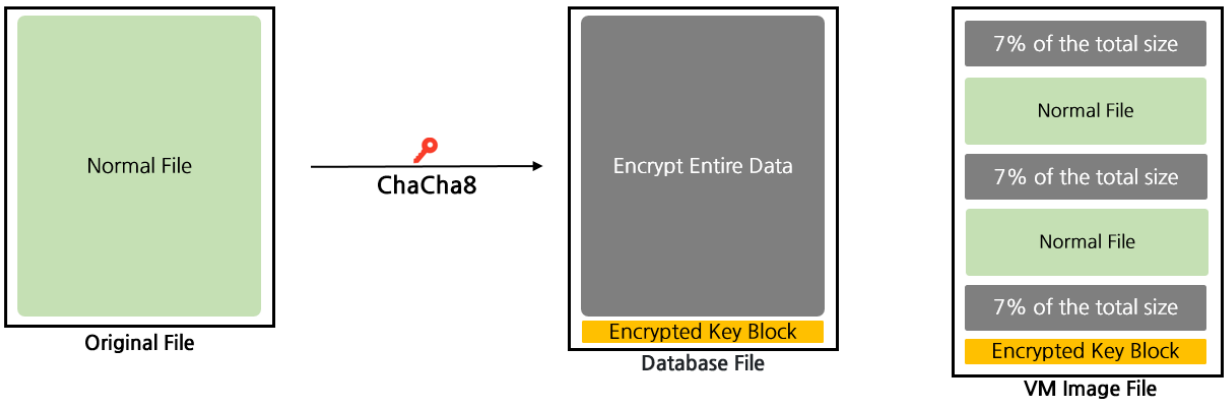

Figure 11. Gunra Ransomware Windows Version Encryption Method (Based on File Extension)

The file encryption method is determined by both the file extension and its size. Files associated with databases are fully encrypted regardless of their size. In contrast, files related to virtual machine (VM) images are partially encrypted: specifically, 7% of the file is encrypted at the beginning, middle, and end of the file—totaling 21% of the entire file, irrespective of its overall size. The corresponding file extensions for each category are listed in the table below.

Database-Related Extensions	VM-Related Extensions
.4dd, .4dl, .accdb, .accdc, .accde, .accdr, .accdt, .accft, .adb, .ade, .adf, .adp, .arc, .ora, .alf, .ask, .btr, .bdf, .cat, .cdb, .ckp, .cma, .cpd, .dacpac, .dad, .dadiagrams, .daschema, .db, .db-shm, .db-wal, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl, .dlis, .dp1, .dqy, .dsk, .dsn, .dtsx, .dxl, .eco, .ecx, .edb, .epim, .exb, .fcd, .fdb, .fic, .fmp, .fmp12, .fmpsl, .fol, .fp3, .fp4, .fp5, .fp7, .fpt, .frm, .gdb, .grdb, .gwi, .hdb, .his, .ib, .idb, .ihx, .itdb, .itw, .jet, .jtx, .kdb, .kexi, .kexic, .kexis, .lgc, .lwx, .maf, .maq, .mar, .mas, .mav, .mdb, .mdf, .mpd, .mrg, .mud, .mwb, .myd, .ndf, .nnt, .nrmlib, .ns2, .ns3, .ns4, .nsf, .nv, .nv2, .nwdb, .nyf, .odb, .oqy, .orx, .owc, .p96, .p97, .pan, .pdb, .pdm, .pnz, .qry, .qvd, .rbf, .rctd, .rod, .rodx, .rpd, .rsd, .sas7bdat, .sbf, .scx, .sdb, .sdc, .sdf, .sis, .spq, .sql, .sqlite, .sqlite3, .sqlitedb, .te, .temx, .tmd, .tps, .trc, .trm, .udb, .udl, .usr, .v12, .vis, .vpd, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff, .abcddb, .abs, .abx, .accdw, .adn, .db2, .fm5, .hjt, .icg, .icr, .kdb, .lut, .maw, .mdn, .mdt	.vdi, .vhd, .vmdk, .pvm, .vmem, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso

Table 3. Database and VM-Related Extensions

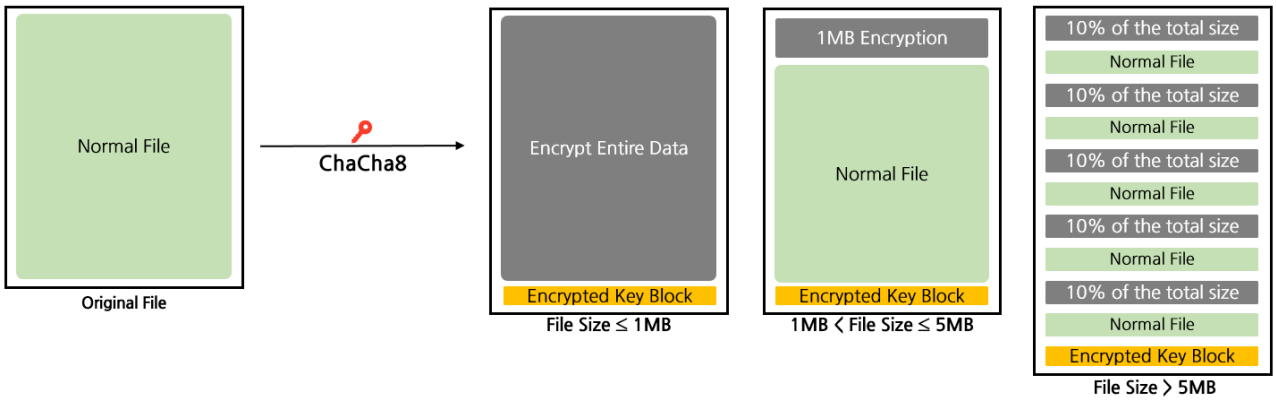

Figure 12. Gunra Ransomware Windows Version Encryption Method

All files other than those associated with virtual machines and databases are encrypted according to their size. Files that are 1MB or smaller are fully encrypted, while files larger than 1MB but not exceeding 5MB have only the first 1MB encrypted. For files exceeding 5MB, the entire file is divided into blocks, each representing 10% of the total file size, and only the odd-numbered blocks are encrypted.

After file encryption, the data required for recovery is appended to the end of the file. This includes the ChaCha8 key and nonce used for encryption, the original file size, and a 2-byte identifier specifying the encryption method employed. All of this information is encrypted with the attacker's RSA public key before being appended.

Gunra ransomware disables the system restore functionality to prevent victims from recovering their data. To achieve this, it enumerates all Volume Shadow Copy Service (VSS) entries and systematically deletes each one. During this process, the ransomware executes the query SELECT * FROM Win32_ShadowCopy via WMI [6]to identify all shadow copies present on the system. It then extracts the unique ID of each volume shadow copy from the query results and proceeds to generate and execute the following command to delete each identified shadow copy.

cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID='%s'" delete

Table 4. VSC Deletion Command

[6] WMI (Windows Management Instrumentation): A management interface that enables standardized querying and administration of components, status, and operational information within the Windows operating system.

Response Strategies for Gunra Ransomware

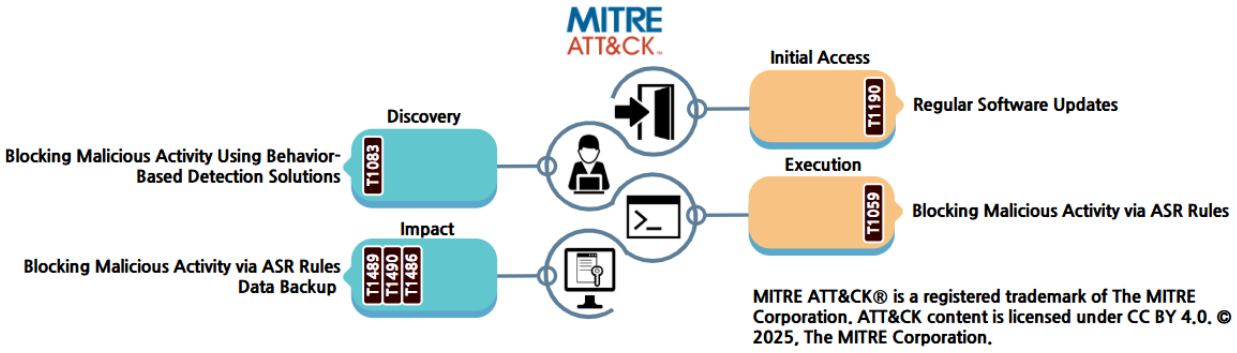

Figure 13. Mitigation Strategies for Gunra Ransomware

The Windows variant of Gunra ransomware utilizes the Windows command prompt to delete backup copies on the system prior to initiating file encryption. Consequently, enabling ASR (Attack Surface Reduction) rules allows for the proactive detection and blocking of abnormal processes related to backup deletion and encryption, thereby effectively mitigating malicious activity. In particular, it is critical to establish an environment capable of detecting and blocking actions such as the deletion of system restore points. Careful pre-configuration of security policies and the immediate blocking of unnecessary script execution attempts can also significantly contribute to the prevention of ransomware damage.

In addition, it is essential to deploy an EDR (Endpoint Detection and Response) solution and apply the latest security patches to swiftly identify and block intrusions exploiting known vulnerabilities or anomalous activities initiated locally. Such measures enable the real-time detection of behavior-based patterns that occur during the file encryption process and allow for the immediate termination of malicious processes. Furthermore, integrating EDR, antivirus, and log analysis systems for centralized monitoring of alert events ensures a robust response capability, even in the event of simultaneous attacks across multiple endpoints.

Additionally, regularly distributing backup copies across separate network segments, external storage, or offline media ensures data recoverability even if the primary system is encrypted. It is crucial to minimize access privileges to backup devices and conduct routine recovery tests to guarantee the integrity of backup data. Furthermore, dispersing backup data across different networks or storage solutions, as well as diversifying backup schedules and retention periods, can effectively mitigate the risk of ransomware attempts to delete backup copies.

These mitigation strategies are equally applicable to the Linux variant of Gunra ransomware as well as to Windows environments. In Linux environments—where critical infrastructure such as servers is frequently targeted—it is essential to enforce access control policies, restrict service ports, and strengthen administrator account management in accordance with the specific characteristics of the operating system. Regardless of the platform, implementing a multilayered security architecture can minimize damage in the event of ransomware infection and ensure rapid recovery.

IoCs

Hash(SHA-256)
91F8FC7A3290611E28A35A403FD815554D9D856006CC2EE91CCDB64057AE53B0
22C47EC98718AB243F2F474170366A1780368E084D1BF6ADCD60450A9289E4BE

References

• ArcticWolf (https://arcticwolf.com/resources/blog/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn/)

• Microsoft (https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/)

• Thehackernews (https://thehackernews.com/2025/07/newly-emerged-global-group-raas-expands.html)

• Securit affairs (https://securityaffairs.com/180578/cyber-crime/fbi-seizes-20-btc-from-chaos-ransomware-affiliate.html)