



Energy and Utilities Sector **Deep Dive**

Ransomware Threat Groups

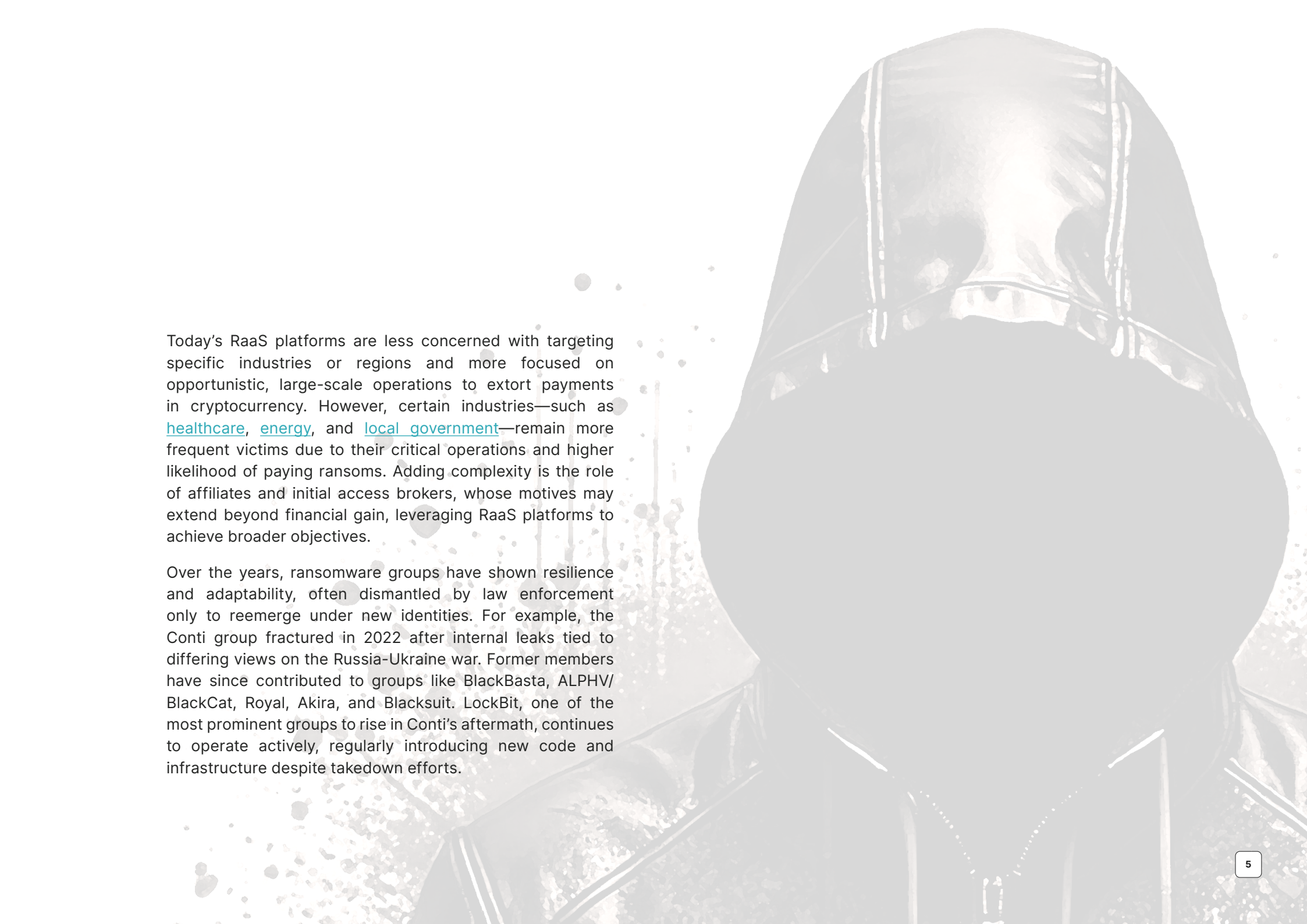
Contents

Threat Groups Targeting Energy and Utilities.....	6
Play	8
8Base	13
Hunters International	21
Qilin	28
References	32

Since its inception in 1989 with the [AIDS Trojan](#), ransomware has evolved into one of the most disruptive threats facing organizations worldwide.

The AIDS Trojan demanded a \$189 ransom via a PO Box in Panama, introducing a concept that has since reshaped the cyber threat landscape. The emergence of CryptoLocker in 2013 marked a turning point, [leveraging the GameOver Zeus botnet](#) to distribute ransomware on a massive scale.

This innovation laid the groundwork for the Ransomware-as-a-Service (RaaS) model, first formalized by the [Tox platform in 2015](#). Tox allowed users to create custom ransomware in exchange for a share of the ransom, inspiring more sophisticated platforms like Cerber, Sodinokibi/REvil, and DarkSide, which integrated affiliate programs and professionalized ransom negotiations.



Today's RaaS platforms are less concerned with targeting specific industries or regions and more focused on opportunistic, large-scale operations to extort payments in cryptocurrency. However, certain industries—such as [healthcare](#), [energy](#), and [local government](#)—remain more frequent victims due to their critical operations and higher likelihood of paying ransoms. Adding complexity is the role of affiliates and initial access brokers, whose motives may extend beyond financial gain, leveraging RaaS platforms to achieve broader objectives.

Over the years, ransomware groups have shown resilience and adaptability, often dismantled by law enforcement only to reemerge under new identities. For example, the Conti group fractured in 2022 after internal leaks tied to differing views on the Russia-Ukraine war. Former members have since contributed to groups like BlackBasta, ALPHV/BlackCat, Royal, Akira, and Blacksuit. LockBit, one of the most prominent groups to rise in Conti's aftermath, continues to operate actively, regularly introducing new code and infrastructure despite takedown efforts.

Threat Groups Targeting Energy and Utilities

In this report, we delve deeper into the research presented in our [accompanying analysis on ransomware trends](#), and profile some of the lesser-known ransomware groups that are targeting the energy and utilities sector.

While groups such as Conti, LockBit, ClOp, and others dominate the headlines, this report shifts the focus to lesser-known but active ransomware groups from the past year—specifically Play, 8Base, Hunters International, and Qilin—providing a comprehensive understanding of the evolving threat landscape.

Top Ransomware Groups Since H2 2022

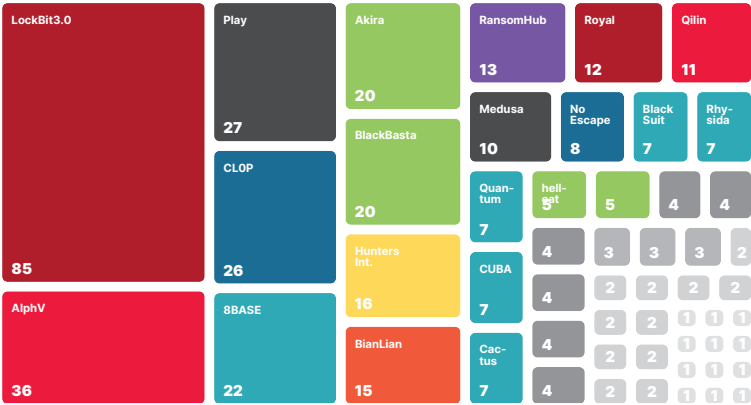


Figure 1. Ransomware groups targeting energy and utilities and count of attacks since H2 2022

Top Ransomware Groups in H2 2024



Figure 2. Ransomware groups targeting the energy and utilities sector and the number of attacks waged by each group in H2 2024



Play

Background

The Play ransomware group, also referred to as 'PlayCrypt,' has been active since June 2022 when it was first discussed in the [Bleeping Computer forum](#). The group targets a broad spectrum of businesses and critical infrastructure across North America, South America, and Europe. By October 2023, the FBI estimated that approximately 300 entities had been impacted by this group.

Initially, Play operated as an exclusive group, emphasizing confidentiality in their operations. Statements on their data leak website indicated that this structure was meant to ensure secure negotiations. They employ a double-extortion tactic, where data was stolen before systems were encrypted. Instead of providing victims with an upfront ransom demand or detailed payment instructions, they were directed to contact the attackers via an email address for further negotiations. The group also maintains an online TOR leak site where they publish information about their attacks, including summaries of the stolen data.

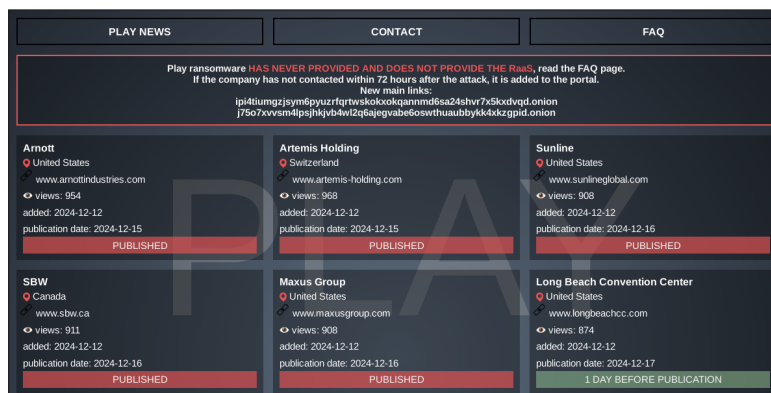


Figure 3. TOR Leak Site

The group came to public attention in June 2022, when a forum user on BleepingComputer reported files being encrypted with a “.play” extension. Shortly afterward, an analysis by [Trend Micro](#) identified this as a new ransomware variant. Although Play appeared to be a newly emerged threat, its techniques showed similarities to methods previously observed in ‘HIVE’ and ‘Nokoyawa’ ransomware families. Play initially focused on the Latin American region, with Brazil being one of the hardest-hit countries but has gone on to target different regions as well.

While Play initially operated as a closed group, by late 2023, evidence surfaced that they had adopted a Ransomware-as-a-Service (RaaS) model. This change made their ransomware available to a wider range of actors, from skilled cybercriminals to less experienced individuals. By adopting this model, the group significantly increased the scale of attacks, expanding its reach and continuing to disrupt organizations globally.

Play ransomware initially concentrated on Windows systems for several years. However, by mid-2024, a [Linux variant emerged](#), specifically designed to target ESXi environments. This development expanded the group’s reach, enabling them to compromise critical systems and broaden their potential victim base.

Attribution

The name of the group comes from the “.play” file extension that is added to files after encryption. The group exhibits behaviors and tactics resembling those of ‘HIVE’ and ‘Nokoyawa’ ransomware, including similarities in file names and paths used for their tools and payloads. Evidence suggests a potential connection between the operators of ‘Nokoyawa’ and ‘HIVE,’ given the overlap in their attack methodologies.

Play ransomware shares significant similarities with the ‘Nokoyawa’ and ‘HIVE’ ransomware strains. [Trend Micro](#) observed that all three groups utilize tools like Nekto/PriviCMD, GMER, and PsExec, while also deploying malware such as Cobalt Strike and Coroxy/SystemBC during their attacks. Additionally, they use similar directories for dropping tools and follow comparable file naming patterns. For instance, Play ransomware has been observed using directories like the Music folder, PerfLogs, and %mytemp%, which align with those seen in ‘Nokoyawa’ and ‘HIVE’ attacks. File names such as sok/socks/soks.exe and xxx.exe have also been noted as common across these ransomware families.

Meanwhile, Play differentiates itself from ‘HIVE’ and ‘Nokoyawa’ by utilizing AdFind, a command-line tool used to extract information from Active Directory (AD). On the other hand, ‘HIVE’ has been observed employing malware for reconnaissance. Despite some differences in their tools and indicators, the shared tactics among Play, ‘HIVE,’ and ‘Nokoyawa’ hint at a possible affiliation.

Further analysis of Play ransomware attacks revealed that its use of Cobalt Strike beacons in some campaigns shares the unique watermark 206546002, a value tied to the CobaltStrike.auth file, which identifies payloads originating from team servers using the same license. This watermark has also been seen in attacks involving the Emotet and SVCReady botnets. These botnets have previously been connected to Quantum ransomware activity, a ransomware variant discovered in August 2021, suggesting a potential overlap in infrastructure or operators. The reuse of this watermark highlights the possibility of shared tooling or collaboration among threat actors.

More recently, [Palo Alto](#) reported that ‘Jumpy Pisces’, a threat group which is North Korea-backed, has been involved with Play Ransomware during a recent ransomware attack in 2024. This is the first time that Play has been reported to work with such threat actors.

Victimology

In August 2022, Play ransomware targeted one of its first notable victims, Argentina's Judiciary of Córdoba, in a reported attack. The cyberattack disrupted the judiciary's websites and databases, causing widespread damage to public institutions in Argentina. The affected websites remained inaccessible for quite some time.

Initially targeting Latin America, the group expanded its operations to North America, South America, and Europe, going after industries including IT, transportation, construction, government entities, and critical infrastructure.

[According to the FBI](#), Play ransomware was responsible for compromising around 300 organizations globally between June 2022 and October 2023, with some of the breaches impacting critical infrastructure.

The group's leak site reveals that the IT sector was the primary target of Plays' attacks, followed by transportation and other sectors such as construction, materials, and government organizations. Recent victims of Play ransomware include Microchip, RRCA Accounts Management, Credible Group, and Nilorngruppen AB.

In Switzerland, authorities investigated a cyberattack on Xplain, an IT services provider based in Bern. The breach affected various federal and cantonal government entities, including the cantonal police, the Swiss army, customs, and the Federal Office of Police (Fedpol). Play Ransomware

claimed responsibility for the attack and disclosed stolen data from Fedpol and the Federal Office for Customs and Border Security (FOCBS) on a dark web forum.

The ransom note left by the Play ransomware group on victim hosts is notably minimalist, containing only the word "Play" and an email address for contacting the threat actors. This approach differs from typical ransom notes used by other ransomware groups, which often include detailed messages explaining the compromise, the encryption of files, and instructions for paying the ransom.

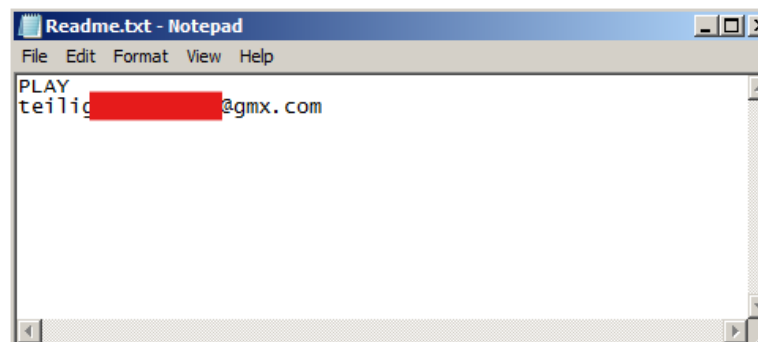


Figure 4. Minimalist Ransom Note of Play

In 2024, Play ransomware activity surged compared to previous years, likely driven by the adoption of a Ransomware-as-a-Service (RaaS) model. This shift enabled the group to broaden its victim base while still profiting from its affiliates' attacks.

Capabilities

Play ransomware gains initial access by exploiting valid accounts **(T1078)** and public-facing application **(T1190)** vulnerabilities, such as those in FortiOS, Citrix, and Microsoft Exchange. The group also uses external-facing services like Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) **(T1133)** to gain entry. Other reports include that spearphishing emails **(T1566)** may also be one of the techniques they employ to gain foothold in the victim's network. Once inside, Play actors employ tools like AdFind to query Active Directory **(T1615)** and Gribba to gather network information **(T1016)** while identifying antivirus software **(T1518.001)**. To evade detection, they use tools such as GMER, IOBit, and PowerTool to disable antivirus defenses **(T1562)** and remove logs **(T1070)**, sometimes leveraging PowerShell scripts **(T1059.001)** for these tasks.

For lateral movement, Play actors utilize command and control tools like Cobalt Strike and SystemBC, along with PsExec for executing commands on remote systems **(T1021)**. They escalate privileges using Mimikatz and WinPEAS to gain domain admin access and search for further escalation paths **(T1082)**. The actors then distribute malicious executables across the network using Group Policy Objects. In the

exfiltration phase, Play ransomware actors compress stolen data into .RAR files with WinRAR and transfer it to actor-controlled accounts using WinSCP **(T1048)**. After exfiltrating the data, they encrypt the files using a hybrid AES-RSA encryption scheme **(T1486)** and rename them with a .play extension.

The main file of the Play ransomware is crafted in a way where analysts would have a difficult time reverse engineering the file. They employ anti-analysis techniques such as string encryption **(T1027.013)**, API hashing **(T1027.007)**, and adding junk code **(T1027.001)**. In both Windows and Linux variants, command line arguments are accepted and would specify which files or directories encrypt.

Play ransomware remains a serious and growing threat to organizations worldwide. As the group adapts and expands its operations, it continues to target critical infrastructure across various industries. With its shift to a Ransomware-as-a-Service model, Play has increased its reach, allowing more attackers to use its tools. The group's use of advanced tactics and double-extortion strategies shows how ransomware threats are evolving, making Play a constant threat to organizations.

8Base

Background

8Base is a financially motivated RaaS affiliate program and data-extortion operation. While the group is known for both encrypting with locker malware and exfiltrating victim data, they primarily focus on the latter - stealing sensitive information for extortion purposes without deploying ransomware. On its data leak site (DLS), the group claims to “exclusively target organizations” that “neglect the privacy and importance of their employees’ and customers’ data.” Active since at least March 2022, 8Base re-emerged under its current branding in early 2023 and became particularly active during the summer of 2023, targeting multiple sectors, especially small to medium-sized businesses in the United States. However, by 2024, their operational tempo slowed, with fewer posts on their DLS. This shift in activity suggests that 8Base is not a newly formed group but rather the continuation of a well-established organization composed of experienced members from the ransomware community. The public profile of 8Base gained significant attention in the spring and summer of 2023 with the launch of their operations. In May 2023, the group transitioned to a multi-extortion model and introduced a “.onion”-based DLS.



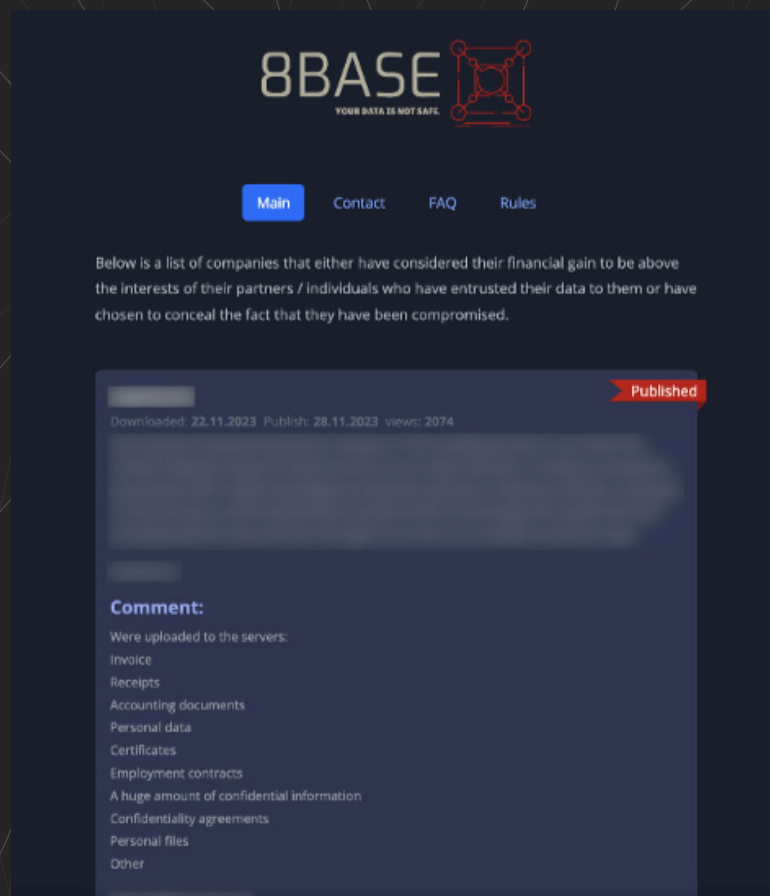


Figure 5: 8Base main DLS page (offline as of 20.12.2024)

By the summer, they expanded their communication channels to include Telegram (<https://t.me/eightbase>) and Twitter/X (<https://x.com/8BASEHOME>). While their Telegram account remained active until December 2023, with one post in December 2024 updating their DLS link, their Twitter/X account ceased activity after December 2023. Historically, the group's DLS was hosted on multiple ".onion" sites, which were all offline as of December 13, 2024. On its DLS, 8Base presents itself as a professional and organized group, offering structured policies and dedicated communication channels, including customer support. The group invites collaboration with like-minded actors while distancing itself from ultra-radical or extremist groups. They also attempt to project an ethical image, claiming not to release morally objectionable data or work with unethical entities.

8Base states that it respects journalism and provides special considerations for journalists—likely a tactic to garner media attention and shape its narrative. Additionally, 8Base claims to assist victims by removing personal data from public leaks and even offering data sets to individuals for potential legal actions. These efforts are framed as serving the public interest. The group lists companies as "Evidence" on their DLS, changing their status to "Disclosed" if no resolution is reached. Their DLS also includes a "Rules" section with operational guidelines and a FAQ that describes them as "honest and simple pentesters." Overall, 8Base's public-facing strategy blends coercion with a semblance of professionalism, aiming to maintain control over the narrative while pursuing financial extortion.

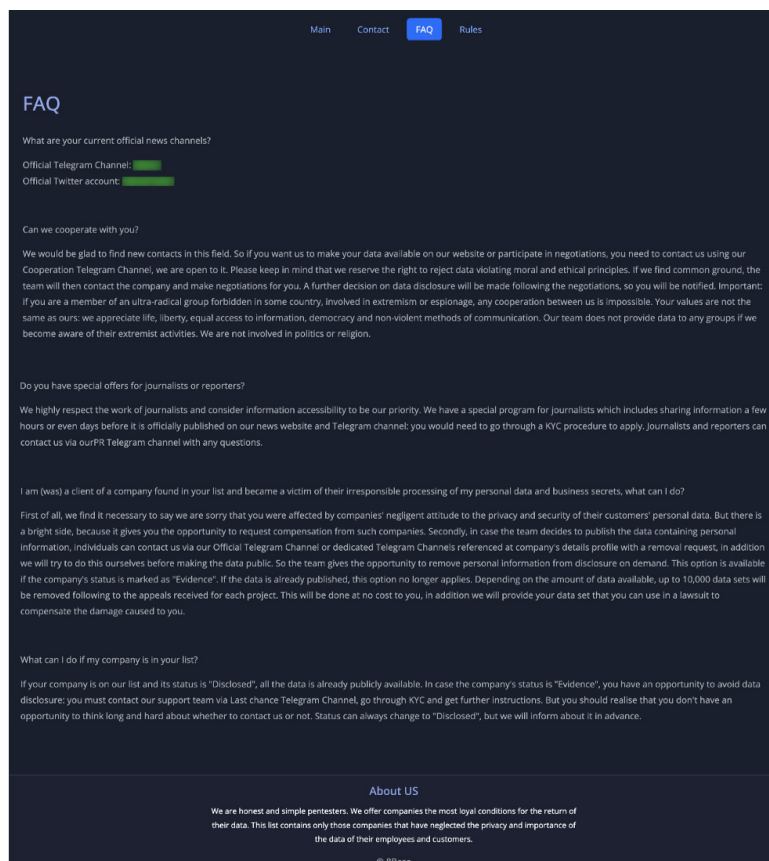


Figure 6. 8Base DLS - FAQ page (offline as of 20.12.2024)

Like many ransomware operations, 8Base relies on initial access brokers (IABs) to facilitate compromises and is known to purchase already-leaked data. Although 8Base shares similarities with other ransomware gangs, its specific identity, methods, and motivations remain unclear, though its integration into the broader ransomware landscape is evident. Early ransom notes from 8Base resembled those of the Babuk ransomware group, which suggests the use of the Babuk ransomware builder (a tool freely available to various ransomware groups). In September 2023, a duplicate of 8Base's leak site was discovered, allegedly linked to a group called CryptBB. However, 8Base denied any connection, labeling the site as an imitation. In the same month, 8Base inadvertently leaked information about its infrastructure, revealing a link to a private GitLab server named Jcube-group. Data suggests that some of the website's code was written by a [36-year-old programmer residing in the capital city of Moldova](#). 8Base also shares certain characteristics with other ransomware families, such as Phobos and RansomHouse, though no formal ties have been established. For example, a comparison of the ransom notes from 8Base and RansomHouse revealed various similarities, particularly in the welcome page, Terms of Service, and FAQ sections.

However, 8Base differs from RansomHouse in its lack of active recruitment of partners and its more restrained public presence. The design and structure of their DLS sites also differ. When comparing a newer strain of 8Base to Phobos, it was found that 8Base used Phobos in one of its operations, leveraging [SmokeLoader](#) for initial obfuscation, ingress, unpacking, and loading of the ransomware. Additionally, Phobos itself had previously used the file extension “.8base” for encrypted files. The ransom notes from 8Base and Phobos also share similarities, such as the use of the term “phobos” in the top and bottom corners of Phobos’ ransom note, whereas 8Base replaced it with “cartilage” in the top corner. A final link between Phobos and 8Base emerged when [8Base’s DLS temporarily went offline, coinciding with the arrest of a Phobos administrator](#) who was [extradited from South Korea to face cybercrime charges in the U.S.](#) However, [this remains speculative](#) as the DLS quickly came back online with more victim data posted (it is currently offline, though).

Ransomware

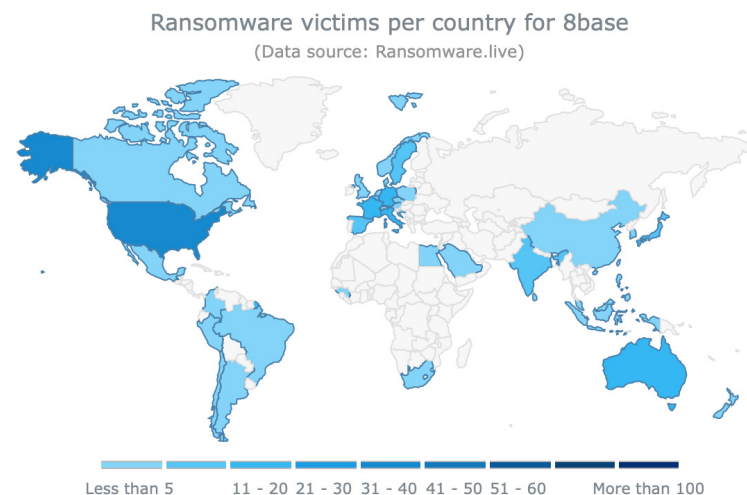
The 8Base group does not use a completely custom-developed ransomware locker. Instead, the attackers have created their own custom modification based on previously leaked ransomware builders, adapting them for their operations. The current version belongs to the Phobos family. The first publicly known 8Base sample, a PE32 file written in C/C++, was [compiled on June 23, 2022](#). However, it went undetected until June 2023, when 8Base’s operations became public. Since its debut, multiple iterations of the lockers have been identified. In November 2023, an update was observed, featuring some minor implementation changes. Despite these adjustments, all 8Base versions follow a consistent pattern of being delivered through the SmokeLoader malware. Upon execution, 8Base locker performs several steps to establish persistence and ensure successful file encryption. It copies itself to multiple locations on the system. It then creates registry keys to enable auto-start upon system reboot, specifically at HKLM and HKCU under the same registry path: SOFTWARE\Microsoft\Windows\CurrentVersion\Run\mtx777.

Additionally, the ransomware modifies registry keys related to internet policy to hinder detection and disable system defenses. To avoid interference, 8Base disables file system redirection using the `Wow64DisableWow64FsRedirection` function. Before encrypting files, 8Base deletes shadow copies and disables system recovery features, preventing victims from recovering their data using built-in Windows tools with commands like `vssadmin delete shadows /all /quiet`, `wmic shadowcopy delete`, `bcdedit /set {default} bootstatuspolicy ignoreallfailures`, `bcdedit /set {default} recoveryenabled no`, and `wbadmin delete catalog -quiet`. It also disables the firewall to prevent detection or interruptions by executing `netsh advfirewall set currentprofile state off` and `netsh firewall set opmode mode=disable`. Once the preparations are complete, 8Base enumerates all local drives and encrypts files with standard data file extensions using AES-256 encryption in CBC mode. It targets attached shares and drive volumes but avoids specific files and folders to prevent damage to the operating system, excluding files like `boot.ini`, `bootfont.bin`, `ntldr`, `ntdetect.com`, `io.sys`, and `recov`, as well as folders like `C:\Windows` and `C:\ProgramData`.

The ransomware also terminates processes associated with databases and applications to avoid conflicts during encryption, such as `sqlservr.exe`, `mysqld.exe`, `oracle.exe`, `excel.exe`, `winword.exe`, and `powerpnt.exe`. 8Base employs a size-based encryption strategy: files smaller than 1.5MB are fully encrypted, while larger files are partially encrypted to enhance speed. Once encrypted, files are renamed with the victim's unique ID, the attacker's email address, and the ".8base" extension. 8Base drops ransom notes in two formats: `info.hta` and `info.txt` in the affected directories. The notes inform victims that their files have been encrypted due to a "computer security issue" and instruct them to contact the attackers via email at `support@rexdata.pro` or through Tox messenger. Victims are required to include their unique ID in the subject of the message. The note warns against renaming encrypted files or using third-party decryption tools, as this may lead to permanent data loss. Victims are offered to decrypt up to three files (under 4MB and without sensitive data) for free as a demonstration. Ransom payment is primarily demanded in Bitcoin, with the price typically depending on how quickly the victim responds and collaborates.

Victimology

8Base has developed a broad and varied victim profile, with its targeting strategy appearing opportunistic, affecting organizations across multiple industries and regions. Data from their DLS and public statistics reveal that the group has targeted over 400 organizations, with nearly twice as many posts in 2023 compared to 2024. In May 2023 alone, 8Base published data from 67 victims compromised between April 2022 and May 2023. This surge in activity and the large number of victims positioned them as a prominent player in the ransomware landscape during the summer of 2023. According to their DLS, the group primarily focused on companies in the United States, Brazil, and the United Kingdom, while avoiding attacks on CIS or ex-CIS (Commonwealth of Independent States) countries.



The majority of their victims are small to medium-sized businesses, particularly in professional services such as accounting, law, business services, and legal consulting. Other heavily targeted sectors include manufacturing, construction, finance, insurance, and healthcare. Among their most recent high-profile alleged victims was Volkswagen, [although the company stated that its IT infrastructure remained unaffected](#).

Capabilities

The 8Base group has a distinctive approach to ransomware deployment, following a multi-faceted attack chain. Initial access is often achieved through phishing emails (T1566), with the malware typically downloaded from domains associated with the SystemBC (T1090). In some instances, a batch file (T1059.003) is used to disable Windows Defender (T1562.001) and allowlist the malware path through WMIC (T1047). Once initial access is gained, the attackers proceed to the credential access stage, using tools like Mimikatz (S0002), LaZagne (S0349), WebBrowserPassView, VNCPassView, PasswordFox, and ProcDump to extract passwords and other sensitive data (T1003). These tools facilitate the capture of valuable credentials, further enabling the attackers' infiltration of the network. To evade detection, 8Base deploys various techniques, including executing the custom bat files to disable Windows Defender (T1562.001, T1587.001), deleting shadow copies (T1490), disabling Windows event logs (T1562.002), and bypassing sandboxes such as Cuckoo (T1497.001). Notably, SmokeLoader (T1588.001) is used to decrypt and deliver the ransomware payload, while other tools like PCHunter, GMER, and Process Hacker (T1588.002) assist in evading security software and terminating processes that might interfere with the attack. Lateral movement is commonly achieved using PsExec (S0029) to propagate the batch file and ransomware binary across the compromised network. Privilege escalation is often accomplished by modifying registry entries (T1112) to bypass User Access Control (UAC) and elevate privileges. For example, attackers may add registry keys that disable UAC and reduce security prompts, granting full administrative control.

They also use IFEO (Image File Execution Options) registry keys (T1546.012) to attach cmd.exe to accessibility programs like HelpPane.exe, utilman.exe, Magnify.exe, and sethc.exe, which are accessible from the lock screen (T1546.008). As part of defense evasion, 8Base uses SmokeLoader to unpack and execute the malicious payload in memory. The ransomware also disables or modifies the system firewall with commands such as netsh advfirewall set currentprofile state off and netsh firewall set opmode mode=disable to prevent detection and interference from security tools (T1562.004). Additionally, the malware clears Windows event logs using wevtutil.exe (T1070.001) and executes file discovery commands to identify files for encryption. The ransomware scans for specific file extensions and directories (T1083) to avoid encrypting critical system files, while also gathering information about the victim's OS version, volume serial number, and system configuration to tailor the encryption process (T1082).

During the encryption phase, 8Base terminates processes that could interfere with encryption (T1489), such as common applications and security software. It also deletes files and directories that could be useful for system recovery or forensic analysis (T1485). To ensure persistence, the malware creates registry entries for autorun and drops copies of itself in the user's Startup folder (T1547.001). After encrypting the files (T1486), 8Base operators often rely on RClone (S1040) to exfiltrate data from the system (T1567).

Hunters International

Background

Hunters International, a financially motivated cybercriminal group operating under the RaaS model, emerged in early October 2023, shortly after another RaaS - the Hive ransomware group, was dismantled in a coordinated law enforcement operation earlier that year. While speculation about ties to Hive persists, Hunters International still denies any direct affiliation, claiming it independently acquired Hive's source code and infrastructure.

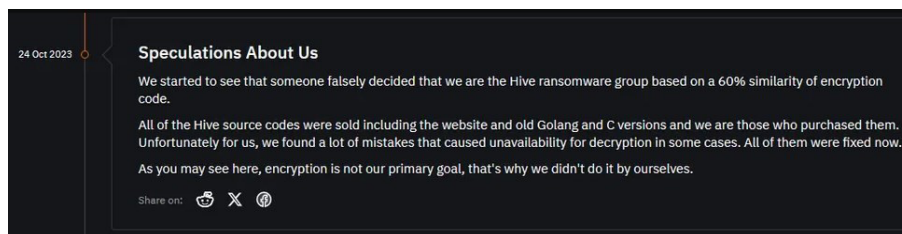


Figure 7. Hunters International denies Hive affiliation via its DLS (online as of 20.12.2024)



Initially emphasizing data exfiltration, Hunters International adopted a dual extortion approach by late October 2023, combining data theft with file encryption. However, their primary focus remains on data exfiltration, with all reported victims experiencing data theft, though not all had their files encrypted. This approach categorizes them more as a data extortion entity than a traditional ransomware group. Despite launching with a mature toolkit, the group has struggled to establish a robust reputation and attract high-caliber affiliates within the cybercriminal ecosystem as of late 2024.

The group's operations are centered on TOR-based domains, including a primary data leak site (DLS) (as of December 2024 available at `hunters55rdxciehogzvw7vgyv6nt37t bwax2reroyzxhou7my5ejyid[.onion]`) and several onion-based mirrors (for reliability and anti-DDoS purposes). These platforms enable victims to access leaked information, negotiate in a chatroom, test free decryption of up to five files, and receive payment instructions.

The screenshot displays the main interface of the Hunters International Data Leak Site (DLS). On the left, a sidebar contains navigation options: 'Companies' (selected), 'News', a 'World Clock' showing times for various cities, 'Visitors' statistics (8,577 last 24 hours, 60,822 last 7 days, 267,749 last month), and a 'Public Visitor' section. The main content area is divided into two primary sections. The 'Companies' section lists several entities with their respective details: ICBC (London) (United Kingdom, Revenue \$250M, 500 employees, 7/7 disclosures), Trev Deeley Motorcycles (Canada, Revenue \$21.7M, 131 employees, 0/1 disclosures), Microvision (United States of America, Revenue \$9M, 340 employees), and Astaphans (United States of America, Revenue \$5.3M, 25 employees). The 'Disclosures' section on the right lists three categories: 'Forecast' (Published 17 Sep, 37.5 MB, 20 files, 1,288 views), 'KYC' (Published 19 Sep, 53 GB, 51,249 files, 1,501 views), and 'Financial Crime' (Published 20 Sep, 3.1 GB, 1,241 files, 589 views). Each disclosure entry includes a 'View' button and a thumbnail image. At the bottom right, there is a 'Share on' section with social media icons for Telegram, Twitter, Facebook, and LinkedIn.

Figure 8. Main page of Hunters International DLS (online as of 20.12.2024)

During 2024, the group briefly hosted clear web domains—huntersinternational[.]net, huntersinternational[.]su, and huntersinternational[.]org—but these were decommissioned by December 2024.

Hunters International claims it acquired Hive's source code in mid-October 2023, addressing bugs that had previously hindered file decryption. Despite their claims, no concrete evidence supports a direct transaction or collaboration with the original Hive group. It remains plausible that the group comprises former Hive affiliates or actors who purchased the code before Hive's disruption in early 2023 (Hive infrastructure dismantled in January 2023 by a coalition including the FBI and Europol, had extorted over \$100 million from more than 1,500 victims worldwide. The [operation was marked by a seven-month FBI undercover effort](#), which culminated in the seizure of Hive's infrastructure. This action allowed authorities to distribute decryption keys to over 300 victims, averting approximately \$130 million in potential ransom payments. Additionally, the takedown led to several arrests in [Ukraine](#) and [France](#)). Regardless, they have leveraged this foundation to prioritize data theft as a core tactic in their extortion model.

Ransomware

Hunters International's ransomware locker, [first reported in late October 2023](#), is a Rust-based encryption tool that marks encrypted files with the ".LOCKED" or ".locked" extensions by default and leaves ransom notes titled "Contact Us.txt" or "READ ME NOW!.txt" (depending on the variant). These notes direct victims to a login-protected .onion chat portal, where login credentials are provided for negotiation access. Unlike earlier Hive ransomware variants, which stored decryption keys separately, Hunters International embeds the decryption key within each encrypted file, following a simpler and more commonly observed ransomware design.

Upon its emergence, [researchers noted that 60% of Hunters International's initial codebase overlapped with Hive](#), leading to speculation of a rebrand. Hunters International quickly denied any formal affiliation with Hive, describing itself as an independent "startup RaaS" that purchased Hive's code and infrastructure to launch its own operations. Leveraging this foundation, the group implemented several key improvements, including:

- Correcting decryption flaws in Hive's encryption logic that occasionally rendered files irrecoverable.
- Streamlining command-line options and improving encryption key management.
- Transitioning from earlier Hive versions written in C and Golang to the Rust programming language, which offers increased resistance to reverse engineering, robust cryptographic capabilities, and efficient encryption.
- Introducing options for customization, such as file extension choices, Volume Shadow Copy deletion, and minimum file size specifications for encryption.
- Modifying encryption algorithms, replacing Hive's ChaCha20-Poly1305 cipher with a combination of AES for file encryption and RSA OAEP for key encryption.

These changes reflect a broader trend in ransomware development, with Rust increasingly adopted by other groups like BlackCat, Luna, Agenda, and RansomExx.

Hunters International's ransomware targets both Windows and Linux environments, searching all available drives, including network drives, using the WIN32 API function `GetLogicalDriveStringsW`. It selectively excludes certain files, folders, and extensions from encryption, such as critical system files (e.g., `boot.ini`, `ntldr`), specific directories (e.g., `Windows`, `System Volume Information`), and non-essential extensions (e.g., `.exe`, `.dll`). If no command-line arguments are passed, the ransomware terminates. Key arguments include:

- `-c` for adding victim login credentials to the ransom note (e.g., `-c username:password`).
- `-a` (or `--attach`) for enabling logs.
- `-A` (or `--no-aggressive`) for disabling data recovery prevention.
- `-E` (or `--no-extension`) for omitting file extensions on encrypted files.
- `-m` (or `--min-size`) to set a minimum file size for encryption (e.g., `-m 1024`).

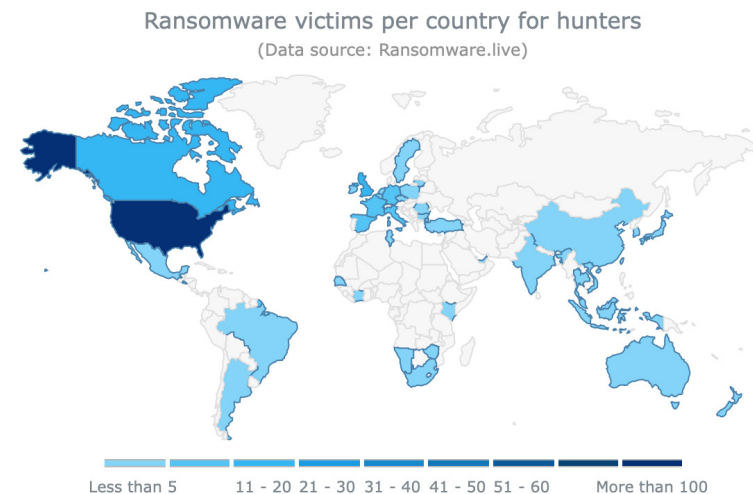
If the `-A` parameter is not specified, the ransomware executes commands to hinder recovery and terminates processes related to backups, databases, and common applications. These commands include:

- Deleting Volume Shadow Copies (`vssadmin.exe delete shadows /all /quiet`).
- Removing backup catalogs (`wbadmin.exe delete catalog`).
- Disabling recovery and boot failure policies (`bcdedit.exe /set {default} recoveryenabled No`).

Hunters International prioritizes data exfiltration over encryption, diverging from Hive's strategy of using stolen data as secondary leverage. This shift reflects the group's understanding of data as a monetizable asset, either through ransom payments or resale opportunities. [Bitdefender's analysis](#) of 2023 sample highlighted encryption routines that embedded AES keys within each encrypted file, separated by 16 null bytes (`0x00`). In some variants, the ransomware also exhausted system memory by writing random data to buffer files, further disrupting recovery efforts. The group's professional organization and ongoing code updates suggest that Hunters International is poised to remain a significant player in the ransomware landscape.

Victimology

The group communicates primarily in Russian and English, refraining from attacks on CIS (Commonwealth of Independent States) countries, a behavior often associated with CIS or ex-CIS-based actors. Like many other RaaS operations, Hunters International is a highly opportunistic group with no specific focus on regions or industries, enabling them to cast a wide net and target victims globally (240+ DLS posts as of December 2024, with 250+ historically known to be posted in total). While the United States and Canada appear to be the primary targets based on DLS data, their attacks have also extended to countries such as the UK, Germany, Mexico, Brazil, New Zealand, Japan, Namibia, China, and India, demonstrating their global reach and strategic focus on maximizing ransom potential.



This broad targeting approach has led the group to exploit vulnerabilities in organizations across a range of sectors, including healthcare, automotive, manufacturing, logistics, finance, education, and food. Hunters International adopts a non-discriminatory stance, attacking any entity they identify as vulnerable. Whether targeting critical infrastructure like energy providers, healthcare institutions, educational facilities, research organizations, or even cultural entities such as zoos, the group demonstrates a willingness to target a diverse array of victims. One notable attack attributed to Hunters International [targeted a U.S.-based plastic surgery clinic](#), resulting in the theft of data from approximately 248,000 files, including patient names and addresses.

Capabilities

The Hunters International group and its affiliates employ a range of TTPs to execute their operations, with reliance on the abuse of legitimate tools and customized malware. One of the group's patterns is also using 7Zip to compress stolen data before exfiltration (T1074, T1560.001). In maintaining access to compromised systems, this cluster known to use AnyDesk (T1219), leveraging it for remote access as part of their persistence strategy. For system configuration changes, they also known to use bcdedit, a Windows command-line tool for managing boot settings (T1562.009). By altering boot settings, the group prevents system recovery (T1490). One of the group's more recent tactics involves the use of a custom RAT - SharpRhino developed in C# (T1587.001). Identified in August 2024, and initially distributed via malvertising campaigns (T1583.008), the malware masqueraded as legitimate network scanning software, such as Angry IP Scanner (T1018), to lure victims. Early versions placed malicious files in the C:\ProgramData\Microsoft\LogConverter directory, but subsequent updates modified its persistence mechanisms, with later versions installing malicious files in WindowsUpdater or LogUpdateWindows folder under C:\ProgramData\Microsoft. The malware was specifically designed to exfiltrate data and deploy the group's lockers (T1041). SharpRhino facilitates C2 communications by creating directories and using batch files executed via LOLBins to decrypt and inject .NET payloads into memory

(T1055). It also features keylogging capabilities (T1056.001) and generates unique machine IDs, which supports further persistence and evasion of detection. SharpRhino's encryption capabilities have evolved over time, incorporating RC4 decryption (T1573.001) and base64 encoding (T1132.001) for secure communication with C2 servers. In September 2024, the RAT was observed using a valid certificate (T1587.002) to sign its payloads. The malware's design, persistence mechanisms, and use of signed certificates align it with other tools in the ThunderShell / SMOKEDHAM (S0649) malware family.

To further its objectives, the group also conducts spear-phishing campaigns (T1566.001, T1566.002) and exploits vulnerabilities in RDP (T1190, T1133, T1078) for initial access. In addition to SharpRhino, the group relies on various other tools and utilities to support its operations, many of which are LOLBins. These include VssAdmin, used to delete shadow copies in Windows, preventing data recovery, and wbadmin, which is employed to delete system backups (T1490). The WMIC utility is also used to interact with WMI for executing backup deletions and terminating processes (T1047). They also modify boot policies and use LOLBins such as Microsoft.NodejsTools.PressAnyKey.exe (T1127) to execute malicious scripts, evading detection methods and further supporting persistence.



Qilin

Background

Qilin ransomware is a sophisticated cyber threat group that has emerged as a significant player in the ransomware landscape. The operation was initially launched under the name [“Agenda” in July 2022](#). However, by September of the same year, it rebranded as “Qilin” and continues to operate under this name to this day. The name may be inspired by the mythical Chinese creature “Qilin” (Chinese: 麒麟), which symbolizes strength and adaptability. Despite this reference, the group is believed to be of Russian origin.

Qilin is a Ransomware-as-a-Service (RaaS), which means that cybercriminals external to the core Qilin team (also known as ransomware affiliates) are invited to perform ransomware attacks using the Qilin RaaS platform. The Qilin RaaS will handle payload generation, the publication of stolen data, and ransom negotiations.

The Qilin RaaS operators are also tracked as Water Galura ([Trend Micro](#)) and GOLD FEATHER ([Secureworks](#)). Qilin is advertised on the exclusive Russian-speaking forum RAMP (short for Ransom Anon Market Place), where acquiring an account can cost up to \$500 in BTC. The forum profile “Haise” joined RAMP on 29 May 2022 and advertised Qilin on 13 February 2023. Affiliates that use the RaaS platform can receive up to 80% if the ransom is paid by the victim (if the ransom paid is 3 million USD or less). And for ransoms over 3 million USD an affiliate’s cut can rise to 85%.

Victimology

In October 2022, the first victim of Qilin was posted to their Tor Data Leak Site (DLS). However, there are reports of Qilin ransomware being deployed as early as June 2022. Currently, Qilin’s DLS contains data from 234 companies.

Qilin’s victims are globally dispersed, with the group targeting organizations across various countries and industries. Its targets span sectors such as education, healthcare, and critical services. Geographical regions affected include Argentina, Australia, Brazil, Canada, Colombia, France, Germany, Japan, New Zealand, Serbia, Thailand, the Netherlands, the UAE, the UK, and the US, among others.

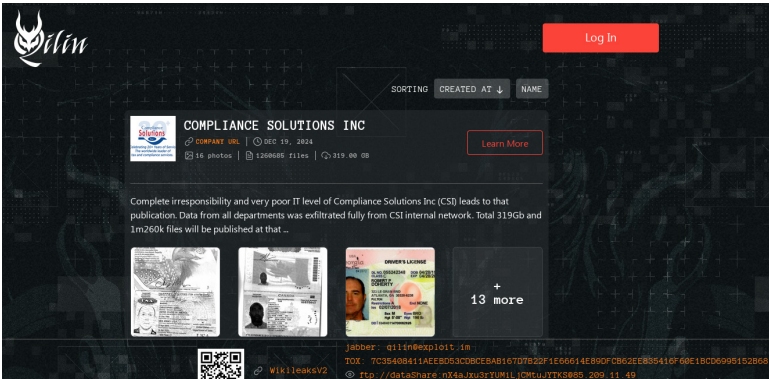


Figure 9. TOR Data Leak Site of Qilin Ransomware

From Q2 2023, the number of Qilin victims began to steadily be listed at a rate of around five victims per month. Since the start of 2024, the number of Qilin victims has noticeably increased.

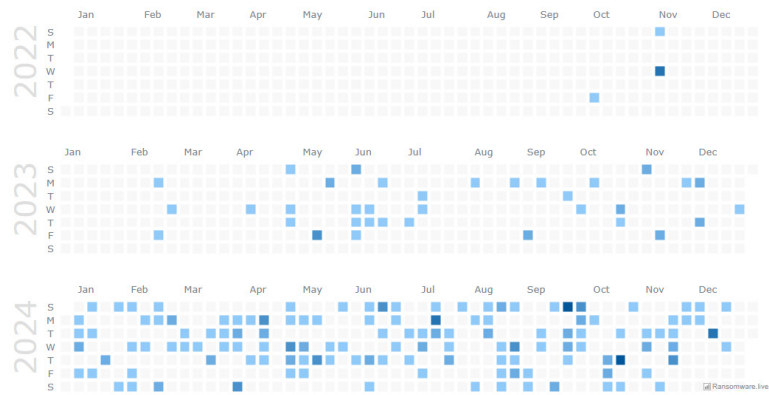


Figure 10. Distribution of Qilin Victim Posts Over Time (Source: Ransomware.live)

The group's approach appears to be opportunistic rather than highly targeted. According to a trusted third party's monitoring of the Qilin DLS, healthcare victims accounted for just over 7% of the more than 100 victims listed on the DLS. The most frequently targeted industries included manufacturing, legal and professional services, and financial services.

As a common activity within the Russian-speaking cybercriminal underground, the operators of Qilin declared in a RAMP forum post: "We do not work in the CIS countries". This statement signifies that they prohibit their affiliates from deploying Qilin ransomware or extorting victims in countries that are part of the Commonwealth of Independent States (CIS), which consists of former Soviet Union (USSR) member states.

In mid-2023, Qilin affiliates were demanding ransoms ranging from \$25,000 to \$600,000. Notably, a real estate development company in Thailand reportedly paid \$600,000 following 20 days of negotiations.

Capabilities

There are multiple variants of Qilin ransomware written in different programming languages. The ransomware was originally developed using the Go programming language (also known as Golang), which is favored by threat actors for its efficiency and cross-platform compatibility. However, researchers have recently identified updated versions of the ransomware written in Rust. While Qilin primarily targets Windows machines, a Linux variant was discovered in December 2023, specifically targeting VMware ESXi servers.

The Qilin ransomware operator gains initial access to victims primarily through phishing **(T1566)** and spear-phishing emails. The threat actors are also known to leverage stolen credentials **(T1078)** to access public-facing Citrix servers **(T1133)** as an entry point. However, it remains unclear how these credentials are obtained. Possible explanations include prior intrusions by an Initial Access Broker (IAB) or the use of logs from infostealer malware. Additionally, the threat actors exploit well-known vulnerabilities in Fortinet devices **(T1190)**. Evidence suggests they may move laterally from a FortiGate firewall, via its SSL VPN service, to a failover server. There are also indications of brute-force attempts targeting VPN devices **(T1110.003)**.

Once initial access is established, Qilin operators have been observed using Nmap and Nping for internal network enumeration **(T1046)** and leveraging Remote Desktop Protocol (RDP) **(T1021.001)** with valid credentials **(T1078)** for lateral movement. The threat actors also employ a combination of Cobalt Strike and remote monitoring and management (RMM) tools **(T1219)**. To disable endpoint detection and response (EDR) systems **(T1562.001)**, Qilin affiliates utilize the bring-your-own-vulnerable-driver (BYOVD) technique, relying on publicly available tools like Spyboy's Terminator and YDark, which are designed for kernel manipulation **(T1068)**. Additionally, Qilin affiliates have been observed using PCHunter and PowerTool as part of their toolset. **(T1588.002)**

Qilin operators have reportedly modified Group Policy Objects (GPOs) **(T1484.001)** to execute a PowerShell script **(T1059.001)** on all machines connected to the compromised domain network. This script, launched via a batch file included in the GPO, is designed to collect credentials stored in Google Chrome **(T1552.001)**. Early versions of Qilin would also change the default user's password and enable automatic login with the new credentials. The ransomware is capable of rebooting the victim's machine in safe mode

(T1562.009), allowing it to bypass protection systems before initiating its encryption routine. The Rust-based variant of Qilin ransomware has been observed propagating across VMware vCenter and ESXi servers, as well as via PsExec **(T1021.002)**, a Windows Sysinternals tool. This propagation is achieved through a custom PowerShell script embedded in the ransomware binary. Another notable capability of Qilin ransomware is its use of intermittent encryption **(T1486)**, which is reportedly intended to evade detection by security solutions. In the backup management console, Qilin ransomware manually performs actions such as deleting tape backups, disabling scheduled backup jobs, and deleting backup jobs **(T1490)**. Additionally, Qilin ransomware further disrupts backup operations by deleting volume shadow copies.

In October 2024, a new variant of Qilin ransomware, dubbed Qilin.B, was observed. Qilin.B is an advanced version of the Qilin ransomware family, built on previous iterations with enhanced encryption capabilities. It terminates services **(T1489)** associated with security tools, clears Windows Event Logs **(T1070.001)** to hinder forensic analysis, and deletes itself **(T1070.004)** to reduce traces of its presence, making detection more difficult.

References

Play

- <https://socradar.io/dark-web-profile-play-ransomware/>
- <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/play-ransomware-group-detection-and-protection/>
- https://www.trendmicro.com/en_ph/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
- https://www.trendmicro.com/en_ph/research/24/g/new-play-ransomware-linux-variant-targets-esxi-shows-ties-with-p.html
- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a>
- <https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/>
- <https://chuongdong.com/reverse%20engineering/2022/09/03/PLAYRansomware/>
- <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/analyzing-play-and-lockbit-the-top-ransomware-threats-facing-retailers/>
- <https://www.hhs.gov/sites/default/files/baza-r-call-campaigns-analyst-note.pdf>

8Base

- <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-8base>
- <https://malpedia.caad.fkie.fraunhofer.de/details/win.8base>
- <https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html>
- <https://www.fortinet.com/blog/threat-research/ransomware-roundup-8base>
- <https://socradar.io/dark-web-profile-8base-ransomware/>
- <https://www.hhs.gov/sites/default/files/8base-ransomware-analyst-note.pdf>

Hunters International

- <https://netenrich.com/blog/hunters-international-group-dls-identity-exposure>
- <https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-hunters-international-ransomware>
- <https://socradar.io/dark-web-profile-hunters-international/>
- https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf
- <https://blackpointcyber.com/wp-content/uploads/2024/10/Hunters-International.pdf>
- <https://www.ransomlook.io/group/hunters>

Qlin

- https://www.trendmicro.com/en_gb/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html
- https://www.trendmicro.com/en_gb/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html
- https://www.trendmicro.com/en_gb/ciso/24/f/synnovis-cyberattack-highlights-vulnerability-of-nhs-supply-chains.html
- https://www.trendmicro.com/en_gb/research/22/l/agenda-ransomware-uses-rust-to-target-more-vital-industries.html
- <https://www.secureworks.com/research/threat-profiles/gold-feather>
- <https://www.group-ib.com/blog/qilin-ransomware/>
- <https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/>
- <https://socradar.io/dark-web-profile-qilin-agenda-ransomware/>
- <https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf>

For all of Trustwave SpiderLabs' research on the Energy and Utilities sector, [please see the full series here](#).



Trustwave
SpiderLabs