halcyon

Q2–2025 Extortion Attack Group Guide

Power Rankings: Ransomware Malicious Quartile

Table of Contents

Executive Summary . . . 3

Q2-2025 RMQ Overview . . . 5

Ransomware MQ: Evaluation Criteria Definitions . . . 6

The Q2-2025 Ransomware Malicious Quartile . . . 7

Frontrunners . . . 8
- Akira . . . 8
- Lynx . . . 10
- Medusa . . . 11
- INC Ransom . . . 13
- Qilin . . . 14
- SafePay . . . 16
- DragonForce . . . 17
- Play . . . 19

Contenders . . . 21
- Cactus . . . 21
- Fog . . . 22
- Cloak . . . 24
- BianLian . . . 25
- Sarcoma . . . 27
- Ghost . . . 28
- KillSec . . . 30
- Meow . . . 31

Emerging . . . 34
- Interlock . . . 34
- DevMan . . . 35
- NightSpire . . . 37
- FunkSec . . . 38
- ArcusMedia . . . 39
- RALord (Nova) . . . 41

Diminishing . . . 43
- Cl0p . . . 43
- BlackLock (El Dorado) . . . 45
- LockBit . . . 46
- BlackBasta . . . 48
- RansomHub . . . 50
- Hunters International . . . 52
- Rhysida . . . 54
- 8Base . . . 56

Takeaway . . . 58

halcyon

Executive Summary

Ransomware remains one of the most destructive and costly threats facing organizations today. The financial and operational toll of these attacks continues to escalate, with the average ransom demand reaching $3.5M. Victims are often forced to make high-stakes decisions under extreme pressure, balancing the risk of prolonged downtime, data exposure, and reputational damage against the cost of paying a criminal enterprise.

A recent study underscores the severity of the threat landscape organizations are navigating. While the tactics may evolve, the impact has remained consistently high across industries. Nearly half of targeted organizations ended up paying a ransom, even after negotiations, reflecting the immense leverage attackers hold once systems are encrypted and sensitive data is stolen.

The downstream effects of a ransomware attack extend far beyond the moment of encryption. Organizations can face weeks or months of recovery efforts, disruption to core services, regulatory scrutiny, and lasting damage to brand trust. As we move through 2025, the costs of unpreparedness are clearer than ever. Ransomware is not just a cybersecurity concern–it's a persistent operational and financial threat with enterprise-wide consequences.

The Halcyon team of ransomware experts has put together this extortion group power rankings guide as a quick reference for the extortion threat landscape based on data from throughout Q2-2025, which can be reviewed along with earlier reports here: *Power Rankings: Ransomware Malicious Quartile*.

Halcyon tracked the twenty-nine most active ransomware groups who compromised organizations between April and June 2025, a slight increase from the prior quarter. Since our last report:

Major Movements:

- **New Leader: DragonForce** was the only group added to the Leaders Quartile in Q2, following its expansion into new regions and adoption of advanced techniques like BYOVD.
- **Removed: RansomHouse** and **DarkVault** were removed entirely from the Q2 report due to inactivity.
- **New Additions: DevMan**, **NightSpire**, **FunkSec**, and **RALord (Nova)** were added to the Q2 report as emerging groups show early operational momentum.
- **Former Leaders in Decline:** Once top-tier actors, **Cl0p**, **RansomHub**, **LockBit**, **BlackBasta**, and **8Base** all dropped from the Leaders quartile in Q2–taken down by law enforcement, internal collapse, or fading affiliate trust.

Evolution of Tactics, Techniques, and Procedures:

- **Security Bypass:** DragonForce is now using BYOVD to bypass kernel defenses, while others rely on intermittent encryption to slip past EDR.
- **Virtual Infrastructure Under Siege:** Ransomware crews like **Qilin** and **Medusa** are aggressively targeting VMware ESXi with custom payloads built for virtualized environments.
- **Living Off the Land Remotely:** Threat actors like Sarcoma and others are abusing legitimate RMM tools for stealthy recon and lateral movement, blending in with IT traffic to extend dwell time undetected.
- **Smarter Payloads, Smarter Theft:** Threat actors like **Akira**, **Qilin**, **Arcus Media**, and **DevMan** are consolidating tools, harvesting browser-stored credentials, and deploying modular ransomware frameworks purpose-built for speed, stealth, and disruption.

Q2-2025 RMQ Overview

Only one group has ascended to our top-ranked threats in Frontrunners:

DragonForce

5 Groups In Decline:

- Cl0p
- RansomHub
- LockBit
- BlackBasta
- 8Base

Five former top groups dropped significantly due to law enforcement take downs, internal collapse, or fading trust.

Evasion and Stealth Go Deeper

More groups are clearing logs, self-deleting payloads, Living-Off-The-Land, and figuring out how to become harder to find by blending in or getting around traditional defenses like endpoint detection and response (EDR).

4x

New Groups Added:

- DevMan
- NightSpire
- FunkSec
- RALord/Nova

2x

Groups Removed:

- RansomHouse
- DarkVault

(Removed due to inactivity)

Stronger Account Controls Needed

An observable increase in attacks bypassing MFA shows the need for organizations to prioritize phishing-resistant MFA, like number-matching and hardware tokens, and eliminate authentication t hat relies on voice or text.

Ransomware MQ: Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q2-2025 Ransomware Malicious Quartile. All attack groups evaluated must be a known threat actor group in 2025 with verifiable victims who demanded a ransom payment.

The report is based on available Q1-2025 data. Given the variability between attack groups regarding breadth of targeting, volume of attacks, and overall impact of their attack campaigns, placement on the report is subjective and based on input from ransomware subject matter experts on the following criteria:

Performance

RaaS Platform: Attack groups were evaluated on the relative maturity of the Ransomware-as-a-Service (RaaS) platform to successfully execute an attack, effectiveness in disrupting significant portions of a targeted network, and ability to evade detection until the ransomware payload is executed.

Attack Volume: Attack groups were evaluated on attack campaign volume and the percentage of attacks known to have been successful.

Ransom Demands: Attack groups were evaluated on the dollar value of their ransom demands and an estimation of the income generated from attacks.

Victims: Sample of victim organizations provided, but attack groups are not ranked on victimology in this report.

Innovation

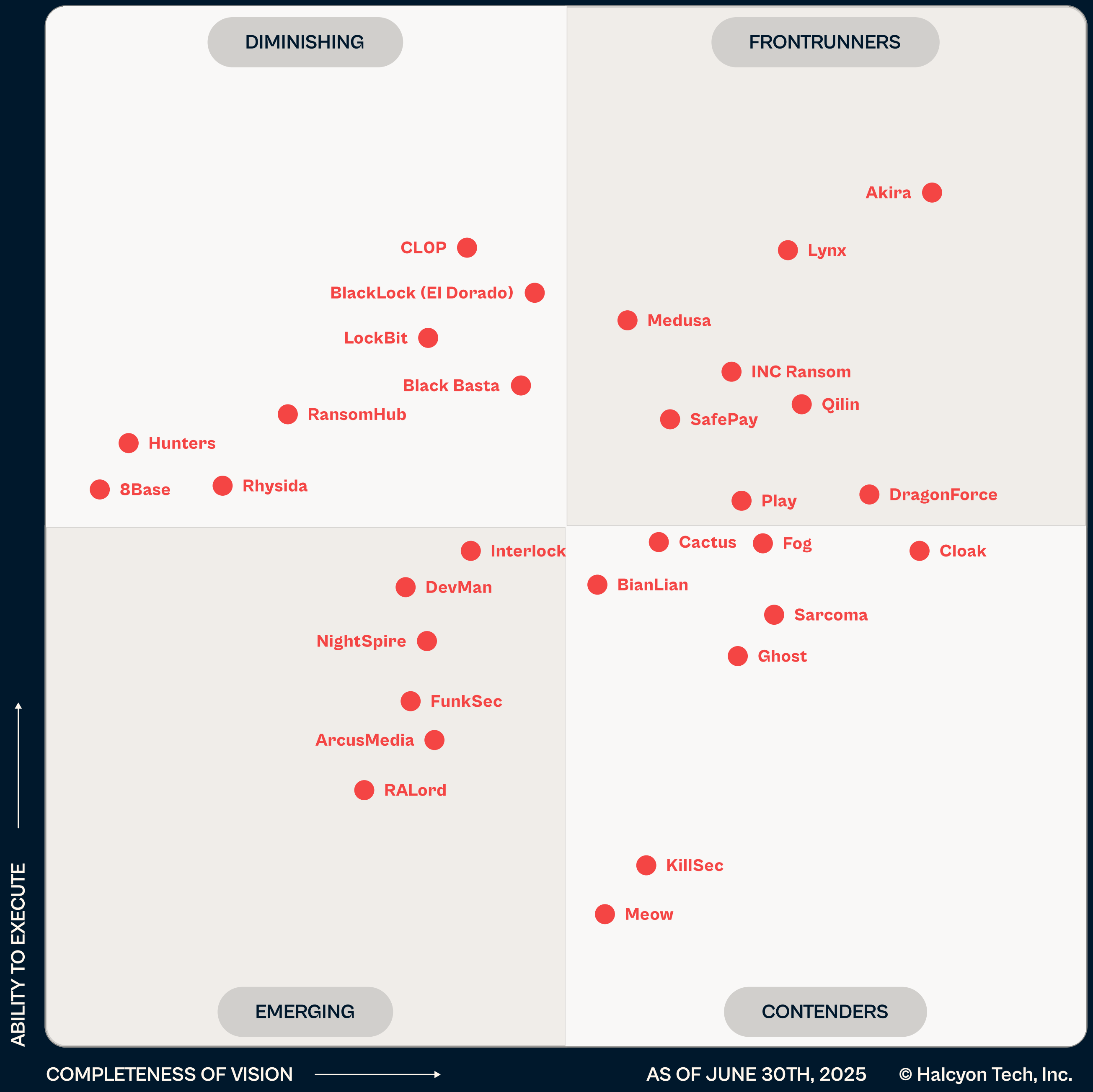
RaaS Platform Development: Attack groups were evaluated on evidence of continued development and improvement of the RaaS platform and TTPs.

Targeted Industries: Attack groups were evaluated on effectiveness of target selection for consistently realizing high dollar ransom demands/payments.

Economic Model: Attack groups were evaluated on an assessment of their business model, estimates on R&D and recruiting efforts, and the availability of technical support services for attack affiliates.

The Q2-2025 Ransomware Malicious Quartile

Figure 1: Top Threat Groups for Ransomware-as-a-Service Ecosystem



AS OF JUNE 30TH, 2025

Source: Halcyon (Q2 2025)

Frontrunners

Akira

Performance

- **RaaS Platform:** The combination of technical advancement and attack volume has put Akira at the top of the ransomware threat landscape. Emerging in March 2023, Akira has been widely speculated to include former members of the defunct Conti gang–especially given its similarities to leaked Conti code–but no definitive links have been established. After briefly pivoting to pure data extortion, Akira returned to its double-extortion model, encrypting files in addition to exfiltrating sensitive data. The group was among the earlier adopters of interactive extortion portals with built-in chat functionality, now a common feature across many RaaS operations. In some rare instances, Akira has disclosed the initial infection vector to victims who paid the ransom–an atypical tactic among ransomware crews. While a decryption tool was released for older samples, it has proven largely ineffective against current variants. In March 2025, researchers uncovered a method for brute-forcing encryption keys on certain Linux variants using GPU acceleration, but this approach remains impractical at scale and risks being neutralized if Akira updates its encryption methods.
- **Attack Volume:** By April 2024, Akira had extorted around $42 million from over 250 victims and ramped up its activity with a major spike in November, leaking data from more than 35 victims in a single day. The group remained highly active into 2025, securing a top-tier position among ransomware operators despite a brief slowdown in April.
- **Ransom Demands:** As of Q2-2025, Akira ransomware's demands continue to vary widely, typically ranging from $200,000 to over $5 million, with pricing influenced by the victim's size, sector, and perceived ability to pay.

Akira uses credential dumping tools like Mimikatz, disables endpoint detection and response (EDR) solutions, and escalates privileges within compromised environments.

Innovation

- **RaaS Platform Development:** Akira ransomware continues to evolve its tooling and tradecraft. While the group initially developed a Rust-based encryptor to target VMware ESXi servers, it has since standardized on C++ variants for both Windows and Linux systems. Akira typically gains initial access by exploiting stolen or brute-forced VPN credentials and regularly employs advanced techniques to evade detection and maintain persistence.

The ransomware uses PowerShell to delete Windows Shadow Volume Copies, making recovery without a decryptor difficult. Akira targets a wide range of file types but avoids critical system extensions–such as .exe, .dll, .sys, .msi, and .lnk–to preserve system stability and reduce the chance of early detection. The group uses credential dumping tools like Mimikatz, disables endpoint detection and response (EDR) solutions, and escalates privileges within compromised environments. In March 2025, Akira was observed exploiting an unsecured webcam to bypass EDR controls–a rare but notable tactic. Akira affiliates rely on tools like SoftPerfect Network Scanner for internal reconnaissance and use PsExec and Remote Desktop Protocol (RDP) to move laterally. To further obscure their activity, they make extensive use of Living-off-the-Land Binaries (LOLBins) and commercial tools like PCHunter64. Since July 2023, Akira has maintained Linux support and expanded its initial access methods, exploiting Cisco VPN zero-days (CVE-2020-3259, CVE-2023-20269) as early as Q3-2023 and later incorporating SonicWall (CVE-2024-40766) and VMware ESXi vulnerabilities by Q4-2024 to facilitate lateral movement across victim networks.

- **Targeted Industries:** Akira remains focused on targets in North America, Europe, and Australia, with some activity extending into South America and Asia. It continues to strike sectors like education, finance, manufacturing, healthcare, and increasingly, mid-sized government and municipal organizations.
- **Economic Model**: Akira continues to rely on a double extortion strategy, combining file encryption with the exfiltration of sensitive data. Victims face threats of both data loss and public exposure, with the group regularly leaking large volumes of stolen information on its darknet site to pressure organizations into paying.

⚠ **CISA Alert:** CISA Alert aa24-109a

Lynx

Performance

- **RaaS Platform:** Lynx ransomware has maintained a steady pace of attacks since first emerging in July 2024, with a continued focus on the manufacturing, construction, and industrial sectors. Despite claims that it avoids government, healthcare, and non-profit targets, the group consistently disrupts high-impact organizations. Lynx primarily targets Windows environments, encrypting files with the .lynx extension and deleting shadow volume copies to hinder recovery. Its initial access methods remain largely undocumented, but available evidence suggests the use of phishing emails, malicious downloads, and potentially compromised RDP credentials to gain entry into victim networks.

- **Attack Volume:** Lynx has continued its upward trajectory in attack volume, with over 130 confirmed victims listed on its data leak site–up from 96 at the end of Q1-2025. The sustained growth underscores the group's expanding operational footprint and rising impact across targeted sectors.

- **Ransom Demands:** Lynx ransomware's ransom demands remain largely undocumented, but one confirmed case involved a demand of $18.1 million following the theft of 30GB of sensitive data. While most ransomware demands across groups average around $600,000, Lynx appears to tailor its demands to the victim's size, industry, and the perceived value of the stolen data.

Innovation

- **RaaS Platform Development:** Lynx continues to operate as a closed ransomware group rather than a Ransomware-as-a-Service (RaaS) platform, with all activity believed to be conducted by a core internal team. Designed specifically for Windows environments, Lynx shares notable code similarities with INC ransomware, primarily developed in C/C++. The malware supports a range of command-line options that allow operators to target specific files or directories, terminate processes, encrypt network shares, and modify system settings. It employs strong encryption, combining AES-128 in CTR mode with Curve25519 Donna for key exchange. To ensure effective encryption, Lynx terminates interfering processes and services using the Windows Service Control Manager and Restart Manager API. It also deletes or manipulates Volume Shadow Copies to disable native recovery options and increase pressure on victims to pay.

Lynx ransomware supports a range of command-line options that allow operators to target specific files or directories, terminate processes, encrypt network shares, and modify system settings.

- **Targeted Industries:** Lynx has primarily targeted organizations in the United States, maintaining a strong focus on the manufacturing and construction sectors, while also expanding into engineering, logistics, and industrial services.

- **Economic Model**: Lynx continues to use both single and double extortion tactics, encrypting victim files and exfiltrating sensitive data to maximize pressure. Victims who decline to pay are named on the group's TOR-hosted leak site, where portions of the stolen data are published to coerce payment and amplify reputational damage. Lynx operates a selective RaaS model that offers affiliates up to 80% of ransom payments, supporting them with a full-featured platform for managing attacks and extortion.

Medusa

Performance

- **RaaS Platform:** Medusa remains one of the most aggressive and persistent Ransomware-as-a-Service (RaaS) operations since its emergence in mid-2021, consistently ranking among the top active threat groups. Following a major surge in attack volume through Q2-2024, Medusa has maintained its momentum by exploiting vulnerabilities such as CVE-2023-48788 in Fortinet's FortiClient EMS and deploying advanced evasion tactics, including rebooting systems into safe mode to bypass endpoint defenses. The group now also targets ESXi environments, expanding its reach into virtualized infrastructure. Medusa continues to sabotage recovery efforts by deleting local backups, disabling startup recovery options, and wiping Volume Shadow Copies (VSS), making data restoration virtually impossible without access to a decryptor.

- **Attack Volume:** Medusa has maintained steady growth since its 2021 emergence, with a major surge by Q2-2024 that pushed it into the top tier of active ransomware groups. Its activity remained high through Q1 and into Q2-2025, confirming its status as a persistent threat.

- **Ransom Demands:** Medusa's ransom demands continue to vary significantly, typically ranging from $100,000 to $15 million, depending on the victim's size, industry, and the sensitivity of the exfiltrated data.

Medusa remains one of the most aggressive and persistent Ransomware-as-a-Service (RaaS) operations since its emergence in mid-2021, consistently ranking among the top active threat groups.

Innovation

- **RaaS Platform Development:** Medusa continues to operate as a RaaS platform, gaining initial access through brute-forced RDP credentials, exploited vulnerabilities, phishing emails, and malicious torrents. Once inside, it can terminate over 200 Windows services and processes without needing command-line arguments, using native tools like PowerShell and RDP to evade detection. Medusa encrypts files with AES-256 and secures keys using RSA public key encryption, while deploying custom malware like gaze.exe for persistence. It leverages Mimikatz for credential harvesting and Netscan for reconnaissance, and aggressively blocks recovery by deleting local backups, disabling startup recovery, and wiping Volume Shadow Copies (VSS). In September 2024, the group released an updated variant that significantly increased encryption speed and improved backup destruction, making recovery even more difficult.

- **Targeted Industries:** Medusa continues to take a strategic approach in selecting high-value targets, prioritizing sectors like healthcare, pharmaceuticals, and government while also expanding into education, manufacturing, and technology.

- **Economic Model**: Medusa continues to operate as a RaaS platform offering affiliates up to 80% of ransom payments, which has fueled its sustained activity across high-value sectors. The group employs double extortion by encrypting files and exfiltrating data and has been observed using triple extortion tactics–demanding additional payments for full decryption or to delay data leaks. Victim data is published on its Tor-hosted leak site, often with added pressure tactics like daily leak countdowns or pay-to-delay options.

⚠ **CISA Alert:** CISA Alert aa25-071a

INC Ransom

Performance

- **RaaS Platform:** INC Ransom remains an active and technically capable ransomware group that first emerged in mid-2023. While it has not publicly advertised itself as a Ransomware-as-a-Service (RaaS), some indicators–such as variation in tactics across incidents–suggest possible affiliate involvement, though this remains unconfirmed. The group continues to use established techniques for initial access, including compromised RDP credentials, phishing campaigns, and exploitation of known vulnerabilities like CVE-2023-3519 in Citrix NetScaler systems. Once inside, INC combines data encryption with exfiltration, leveraging double extortion to pressure victims. Notably, the group brands itself as a "moral agent," claiming its attacks are intended to expose security flaws–an attempt to frame its operations as ethical hacking, despite the financial motivations and real-world harm caused.
- **Attack Volume:** INC has continued to escalate its attack volume since emerging in mid-2023, with a marked increase through late 2023 and early 2024, followed by sustained activity and growing visibility into mid-2025.
- **Ransom Demands:** Exact ransom figures for INC remain unconfirmed, but industry estimates indicate that average demands in 2024 exceeded $5.2 million, with actual amounts varying widely depending on the victim's size, sector, and the sensitivity of exfiltrated data.

Innovation

- **Raas Development:** INC continues to use a broad set of techniques to evade detection, relying heavily on administrative tools and Living-off-the-Land (LOTL) methods, including WMIC, PsExec, and PowerShell for deployment, while even benign tools like MSPaint and Windows Explorer have been leveraged during lateral movement. TightVNC and AnyDesk facilitate remote access, and MegaSync is used for data exfiltration. The ransomware is written in C++ and uses AES-128 in CTR mode for encryption; a Linux variant has also been observed in the wild. INC likely deletes Volume Shadow Copies to block recovery, and its tooling has been linked to attacks involving Vanilla Tempest, including intrusions into U.S. healthcare organizations via Gootloader. While the group continues to frame itself as a "moral agent" exposing security flaws, its tactics demonstrate a deliberate and sophisticated operation designed for maximum disruption and extortion.

INC deletes Volume Shadow Copies to block recovery, and its tooling has been linked to attacks involving Vanilla Tempest, including intrusions into U.S. healthcare organizations via Gootloader.

- **Targeted Industries:** INC continues to primarily target organizations in North America and Europe, with a strong focus on sectors such as healthcare, education, government, and critical infrastructure, including energy and public services.

- **Economic Model**: INC Ransom continues to use double extortion tactics, encrypting victim systems while exfiltrating sensitive data to increase leverage. Victims who refuse to pay are listed on the group's leak site, where INC has repeatedly followed through on threats by publishing stolen data. While the group's public persona and tactics mirror those of larger RaaS operations, there is still no confirmed evidence of a broad affiliate model or profit-sharing structure suggesting INC may function as a closed team or a tightly vetted operation with limited external involvement.

Qilin

Performance

- **RaaS Platform:** Qilin ransomware (originally known as Agenda) continues to operate as a Ransomware-as-a-Service (RaaS) group after rebranding in July 2022. Developed in both Golang and Rust, Qilin supports cross-platform functionality and targets both Windows and Linux environments, with Rust-based variants enhancing stealth and detection evasion. Affiliates typically gain initial access through compromised Remote Desktop Protocol (RDP) credentials, and in 2024, Qilin expanded its capabilities by deploying scripts to extract stored credentials from Google Chrome across victim networks. This ongoing development reflects a sustained focus on credential harvesting, lateral movement, and technical adaptability, solidifying Qilin's reputation as a persistent and evolving ransomware operation.

- **Attack Volume:** Qilin ransomware has continued to scale its attack volume, building on the significant surge observed throughout 2024. By early 2025, it ranked among the most active ransomware groups, consistently posting new victims across sectors such as healthcare, education, manufacturing, and government on its leak site.

- **Ransom Demands:** Qilin's ransom demands typically range from $50,000 to $1 million, though demands have reached as high as $50 million in select high-stakes cases. This broad range reflects a tailored extortion strategy, with demands adjusted based on the victim's size, sector, and the sensitivity of the data exfiltrated.

Developed in both Golang and Rust, Qilin supports cross-platform functionality and targets both Windows and Linux environments, with Rust-based variants enhancing stealth and detection evasion.

Innovation

- **RaaS Platform Development:** Qilin ransomware continues to evolve through its upgraded variant, Qilin.B, first identified by Halcyon researchers in fall 2024. Written in Rust, Qilin.B features advanced encryption capabilities, using AES-256-CTR for systems with AES-NI support and ChaCha20 for others, with RSA-4096 and OAEP padding to secure keys—making decryption without the private key effectively impossible. The variant terminates security services, deletes Windows Event Logs to hinder forensic analysis, and removes itself after execution to evade detection and reverse engineering. It also deletes Volume Shadow Copies (VSS) to block recovery. The Qilin RaaS platform offers affiliates customizable encryption configurations, supporting AES-256, ChaCha20, and RSA-4096. Its Linux variant, compiled with GCC and OpenSSL, specifically targets VMware ESXi environments for efficient disruption of virtualized infrastructures. Qilin affiliates have been observed using PowerShell scripts to extract credentials stored in Chrome and exploiting vulnerabilities in widely deployed systems such as Fortinet devices and Veeam Backup & Replication. These capabilities underscore Qilin's growing technical sophistication, expanding cross-platform reach, and strategic focus on credential theft and vulnerability exploitation to maximize impact.

- **Targeted Industries:** Qilin ransomware continues to target a broad range of industries—including critical infrastructure, healthcare, education, manufacturing, and government—prioritizing mid- to large-sized organizations. The group frequently exploits known vulnerabilities in widely deployed IT systems to gain initial access, often combining these exploits with credential theft to deepen network compromise.

- **Economic Model**: Qilin operates a well-established RaaS model offering affiliates 80% of ransoms under $3 million and up to 85% for larger payouts. Qilin supports a double extortion strategy to pressure victims with public exposure threats via its TOR-hosted leak site.

SafePay

Performance

- **RaaS Platform:** SafePay remains one of the most rapidly emerging Ransomware-as-a-Service (RaaS) groups since its debut in November 2024, quickly gaining traction through frequent victim postings and aggressive extortion tactics. While not a confirmed rebrand of any known operation, SafePay exhibits distinct characteristics that set it apart from other ransomware families, including indicators that its developers have incorporated elements of leaked source code from groups like LockBit. The group has shown signs of technical maturity and operational discipline unusual for a newcomer, suggesting that experienced actors may be behind the operation. Its consistent activity and growing visibility have positioned SafePay as a rising threat within the ransomware ecosystem.

- **Attack Volume:** SafePay has claimed responsibility for a growing number of attacks in a short timeframe, steadily increasing its presence on leak sites and in incident reporting. Based on its rapid operational tempo and expanding victim profile, the group is now widely assessed as an emerging major player in the ransomware landscape.

- **Ransom Demands:** Specific figures for SafePay's average ransom demands remain undisclosed, but available evidence suggests the group targets mid- to large-sized organizations with sizable extortion expectations.

The combination of exploit-driven access, stealthy lateral movement, and aggressive extortion tactics has positioned SafePay as a fast-moving and increasingly dangerous ransomware operation.

Innovation

- **RaaS Platform Development:** SafePay code is based on a modified variant of LockBit code from late 2022 and continues to demonstrate a high level of technical sophistication and operational adaptability. SafePay operators and affiliates use a wide range of TTPs, including exploiting known vulnerabilities in popular enterprise software to gain initial access, leveraging legitimate remote management tools for persistence, and deploying credential-harvesting malware such as Mimikatz during post-exploitation. Files are encrypted with the ".safepay" extension, and ransom notes are dropped as "readme_safepay.txt." The group maintains a strong presence across both Tor and The Open Network (TON), using these platforms to communicate with victims and leak stolen data. SafePay consistently uses a double extortion strategy by encrypting critical systems while exfiltrating sensitive data to maximize leverage through public exposure threats and prolonged operational disruption. This combination of exploit-driven access, stealthy lateral movement, and aggressive extortion tactics has positioned SafePay as a fast-moving and increasingly dangerous ransomware operation.

- **Targeted Industries:** SafePay has targeted organizations across a wide range of sectors, including education, technology, healthcare, transportation, and manufacturing, with a focus on mid-sized to large enterprises.
- **Economic Model**: SafePay has been observed using double extortion tactics, encrypting victim data, and threatening to release it publicly unless the ransom is paid. By allowing affiliates to carry out attacks under its banner, SafePay maximizes its reach and impact, enabling the group to leverage the actions of external actors while maintaining operational control.

DragonForce

Performance

- **RaaS Platform:** DragonForce has established itself as a sophisticated Ransomware-as-a-Service (RaaS) operation since emerging in August 2023, leveraging a dual-codebase built from leaked LockBit 3.0 and customized Conti builders. This hybrid approach reflects the group's technical adaptability and deliberate reuse of battle-tested ransomware frameworks to accelerate development and increase reliability. DragonForce quickly gained traction in the cybercrime ecosystem, carrying out high-impact attacks across sectors such as manufacturing, transportation, real estate, and retail. Its sustained leak site activity and growing victim count have solidified its reputation as one of the more aggressive and strategically disruptive ransomware groups in operation today.
- **Attack Volume:** DragonForce ransomware has shown a steady increase in attack volume since its emergence in August 2023. By August 2024, the group had claimed 82 victims across a range of industries, and by early 2025, it had expanded its operations into the Middle East–most notably targeting organizations in Saudi Arabia and the broader Gulf region.
- **Ransom Demands:** Specific figures on DragonForce ransomware's average ransom demands remain undisclosed, but available evidence suggests the group consistently targets high-value organizations, likely seeking multi-million-dollar payouts in line with large-scale double extortion operations.

DragonForce has adopted a range of advanced tactics including clearing Windows event logs, disabling endpoint security tools, and using BYOVD techniques to bypass kernel-level defenses.

Innovation

- **RaaS Platform Development:** DragonForce has adopted a range of advanced tactics, including clearing Windows event logs, disabling endpoint security tools, and using the "Bring Your Own Vulnerable Driver" (BYOVD) technique to bypass kernel-level defenses. The group has been observed using Living-off-the-Land Binaries (LOLBins) and custom tooling to evade detection, and while tools like Cobalt Strike and Mimikatz are commonly associated with similar operations, their direct use by DragonForce has not yet been publicly confirmed. Encryption methods likely include AES-256 for file encryption and RSA for key exchange, aligning with standards seen in other mature ransomware families. Combined with aggressive data exfiltration and precision targeting, these tactics reflect DragonForce's growing technical sophistication and ability to execute high-impact attacks across critical industries.

- **Targeted Industries:** The group has expanded its targeting across a range of industries, including manufacturing, transportation, real estate, and critical infrastructure, and continues to attract attention for its operational discipline and high-impact attacks.

- **Economic Model**: DragonForce continues to operate under a Ransomware-as-a-Service (RaaS) model, partnering with affiliates who conduct attacks in exchange for a revenue share–typically 70% to the affiliate and 30% to the operator, though higher shares may be offered for large payouts. The group consistently uses double extortion tactics, exfiltrating sensitive data prior to encryption and leveraging its dark web leak site to pressure victims into payment by threatening public exposure.

Play

Performance

- **RaaS Platform:** Play ransomware remains an established Ransomware-as-a-Service (RaaS) operation, though its overall activity appears to have slowed slightly following sustained law enforcement pressure and heightened defensive awareness. First emerging in June 2022, Play quickly rose to prominence by exploiting unpatched vulnerabilities–particularly in Fortinet SSL VPNs and Microsoft Exchange servers (e.g., ProxyNotShell, OWASSRF)–to gain initial access. The group's tooling includes variants tailored for both Windows and Linux environments, enabling broader reach across enterprise infrastructure. Play's operations have drawn comparisons to defunct ransomware outfits like Hive and Nokoyawa, reflecting a shared emphasis on stealth, persistence, and data exfiltration.

- **Attack Volume:** Play ransomware has compromised more than 350 organizations since its emergence, according to updated industry reporting and law enforcement data. Although its attack volume has declined relative to peak activity in 2023 and early 2024, Play remains an active threat.

- **Ransom Demands:** Play ransomware continues to issue ransom demands typically ranging from $100,000 to over $5 million, adjusting the amount based on the size, sector, and perceived financial capacity of the targeted organization. The group consistently tailors its demands to maximize leverage, often factoring in the sensitivity of exfiltrated data and the urgency of operational recovery.

For exfiltration, Play uses custom tooling such as the Grixba information stealer and a Volume Shadow Copy Service (VSS) copier to extract data before encryption.

Innovation

- **RaaS Platform Development:** Play ransomware continues to demonstrate a high level of technical sophistication, leveraging a broad set of tools and techniques to disable defenses, persist in compromised environments, and execute rapid, damaging attacks. The group uses PowerTool to terminate antivirus and monitoring processes, and maintains access with SystemBC RAT, while tools like Plink and AnyDesk enable stealthy remote control. For lateral movement, Play frequently deploys Cobalt Strike and uses Mimikatz for credential harvesting. Initial access is often achieved through exploitation of known vulnerabilities, including FortiOS flaws and Microsoft Exchange vulnerabilities like ProxyNotShell and OWASSRF. To evade detection, Play disables Windows Defender using PowerShell or scripts and employs offensive tools like Process Hacker, GMER, and IOBit. The group has adopted intermittent encryption, encrypting partial file content to speed up attacks and reduce visibility. For exfiltration, Play uses custom tooling such as the Grixba information stealer and a Volume Shadow Copy Service (VSS) copier to extract data before encryption. Encryption is handled using AES-256, with keys protected via RSA-4096, reflecting a continued investment in effective, efficient attack methods.

- **Targeted Industries:** Play ransomware continues to target high-value industries such as healthcare, finance, manufacturing, technology, and government, with a focus on organizations that manage sensitive data or rely on uninterrupted operations. The group has compromised both public and private sector entities globally.
- **Economic Model**: Play continues operating a structured RaaS model, recruiting skilled affiliates–who typically earn around 70% of each ransom payment while Play retains approximately 30%. The group leverages double extortion by encrypting victim data and exfiltrating sensitive information, threatening to leak it via its public leak site to intensify pressure. This combination of impactful disruption, reputational leverage, and consistent affiliate support has helped Play maintain its status as a lucrative and technically adept ransomware operation.

⚠ **CISA Alert:** CISA Alert aa23-352a

Contenders

Cactus

Performance

- **RaaS Platform:** Cactus ransomware continues to operate as a technically advanced and highly active threat group, first identified in early 2023. While it is not formally associated with a known Ransomware-as-a-Service (RaaS) model, Cactus is believed to function as a closed operation, displaying a level of precision and consistency that points to experienced operators. Initially focused on Windows-based targets, Cactus has since expanded to include virtualization platforms such as VMware ESXi and Microsoft Hyper-V, reflecting a deliberate shift toward broader enterprise infrastructure. The group has also been observed targeting business intelligence platforms like Qlik Sense, signaling a clear intent to compromise high-value environments with sensitive data. Though no confirmed links to legacy ransomware groups have been established, Cactus exhibits behaviors and strategic patterns characteristic of veteran actors in the ransomware ecosystem.

One of Cactus's more distinctive techniques involves encrypting its own ransomware binary, requiring a decryption key at runtime—making detection and analysis significantly more difficult.

- **Attack Volume:** Cactus ransomware has steadily grown in prominence since its emergence in early 2023, evolving from a lesser-known threat into a consistent presence in enterprise-focused ransomware activity. Its operations have expanded in both scope and scale, with a noticeable increase in victim disclosures and a sustained focus on high-value targets across critical industries.

- **Ransom Demands:** Specific figures for Cactus ransomware's average ransom demands remain undisclosed, but industry assessments suggest demands typically range from several hundred thousand to over $5 million, depending on the victim's size, sector, and the sensitivity of the compromised data.

Innovation

- **RaaS Platform Development:** Cactus ransomware continues to use a range of advanced tactics, techniques, and procedures (TTPs) to evade detection and maintain persistence within victim environments. Initial access is typically gained by exploiting vulnerabilities in VPN appliances and enterprise platforms, including Qlik Sense flaws (CVE-2023-41265, CVE-2023-41266, CVE-2023-48365). Once inside, Cactus operators abuse Living-off-the-Land (LotL) techniques using tools such as PowerShell, Scheduled Tasks, Rclone for exfiltration, and Chisel for tunneling traffic. The group frequently relies on legitimate remote access software like Splashtop, AnyDesk, and SuperOps RMM to preserve access and blend into normal administrative activity. One of Cactus's more distinctive techniques involves encrypting its own ransomware binary, requiring a decryption key at runtime–making detection and analysis significantly more difficult. Additional tactics include deleting shadow volume copies to obstruct recovery, dumping LSASS credentials to escalate privileges, and in some cases deploying SSH backdoors to enable continued access post-encryption.

- **Targeted Industries:** Cactus ransomware continues to target a broad range of industries–including manufacturing, healthcare, finance, legal services, and IT–across North America, Europe, and increasingly, regions of Asia and the Middle East. The group consistently focuses on mid- to large-sized enterprises with complex infrastructures and high-value data.
- **Economic Model**: Cactus continues to operate as a closed, private ransomware group rather than a public RaaS platform, with no verified affiliate model or revenue-sharing structure observed to date. The group consistently employs double extortion tactics–exfiltrating sensitive data prior to encryption and threatening to leak it publicly if ransom demands are not met. This centralized approach enables Cactus operators to maintain full control over the attack lifecycle, victim negotiations, and ransom proceeds, allowing them to maximize profits while minimizing operational exposure and risk of insider leaks.

Fog

Performance

- **RaaS Platform:** Fog ransomware remains an active and rapidly evolving threat since its emergence in May 2024. Initially identified as a variant of the STOP/DJVU family, Fog has since demonstrated unique characteristics that set it apart, signaling the work of a more capable and strategically driven group. The ransomware primarily targets Windows environments and is known for its fast-moving attacks and ability to spread across enterprise networks. Encrypted files are typically marked with extensions such as ".FOG" or ".FLOCKED," and ransom notes–commonly titled "readme.txt" or "HELP_YOUR_FILES.HTML"–provide instructions for contacting the attackers.

After gaining initial access–typically through compromised VPN credentials or by exploiting vulnerabilities in VPN gateways–Fog disables Windows Defender, deletes Volume Shadow Copies, and removes Veeam backup data to eliminate recovery options.

- **Attack Volume:** Fog ransomware has continued its rapid growth following its emergence in early 2024, with a sharp increase in attack volume over the past year. While initially focused on a narrow set of victims, the group quickly broadened its scope and now accounts for a significant share of global ransomware incidents heading into mid-2025.

- **Ransom Demands:** Fog ransomware has been linked to ransom demands ranging from $50,000 to over $3 million, with amounts tailored based on the victim organization's size, industry, and the sensitivity of exfiltrated data.

Innovation

- **RaaS Platform Development:** Fog ransomware does not appear to operate as a Ransomware-as-a-Service (RaaS) and is instead attributed to a closed, technically capable group employing highly disruptive tactics that make recovery exceptionally difficult. After gaining initial access–typically through compromised VPN credentials or by exploiting vulnerabilities in VPN gateways such as SonicWall appliances–Fog disables Windows Defender, deletes Volume Shadow Copies (VSS), and removes Veeam backup data to eliminate recovery options. The group uses tools like Cobalt Strike and Mimikatz for privilege escalation, employing techniques such as pass-the-hash attacks and credential extraction from browsers and NTDS.dit. For lateral movement, Fog relies on PsExec and Remote Desktop Protocol (RDP) to propagate rapidly across networks. Encryption is carried out using AES-256 for files, with symmetric keys encrypted using RSA-2048, rendering decryption without the attacker's key virtually impossible. While Fog has reportedly encrypted VMDK files in some incidents, more recent activity suggests the group has developed functionality to target ESXi environments more deliberately, including dedicated routines for encrypting virtualized infrastructure. Though tools like Metasploit may appear in its broader arsenal, Fog's operations tend to favor custom scripts and extensive use of living-off-the-land techniques, reflecting a high degree of stealth, adaptability, and situational awareness.

- **Targeted Industries:** Fog ransomware has expanded its targeting beyond its initial focus on U.S. higher education institutions to include organizations of various sizes across a wide range of sectors, including business services, technology, manufacturing, finance, and government. This broadened victim profile reflects the group's growing reach and strategic shift toward maximizing impact across diverse industries.

- **Economic Model**: Fog ransomware has fully adopted double extortion tactics, exfiltrating sensitive data before encryption and threatening to leak it if ransom demands are not met–a shift that began in July 2024. The group operates under a closed, centralized model with no known affiliate structure or revenue sharing, indicating that a core internal team executes attacks from initial access through extortion and negotiation. This approach allows Fog to maintain tight operational control, reduce risk exposure, and maximize ransom proceeds.

Cloak

Performance

- **RaaS Platform:** Cloak ransomware has continued to expand its presence since emerging in late 2022, becoming a notable force within the Ransomware-as-a-Service (RaaS) ecosystem. The group initially gained momentum through a series of frequent and high impact attacks and has since demonstrated increasing sophistication and operational consistency. Cloak shares infrastructure, such as a common data leak platform, with the Good Day ransomware group, a variant of the ARCrypter family that appeared in mid-2023. This overlap suggests collaboration, shared operators, or use of the same backend systems, underscoring Cloak's adaptability, and its integration within the broader ransomware landscape.

- **Attack Volume:** Cloak ransomware has steadily expanded its operations since its emergence in late 2022, evolving into a persistent threat within the ransomware ecosystem. After fluctuating throughout 2024, the group saw a renewed surge in attack volume in early 2025, signaling a clear escalation in both activity and operational reach.

- **Ransom Demands:** Specific ransom figures for Cloak remain unconfirmed, but trends across the broader ransomware ecosystem in 2024 indicate that average payments frequently reached into the seven-figure range. Cloak's overall success rate in securing payments is still unclear, as no verified data has been publicly disclosed regarding how often its victims comply with ransom demands.

Cloak's use of virtual hard disk (VHD) delivery, stealthy execution, and destructive behaviors–such as selective file wiping–highlight its growing technical sophistication and threat potential.

Innovation

- **RaaS Platform Development:** Cloak ransomware has continued to evolve into a technically advanced threat, with code and tooling linked to leaked Babuk source material. Cloak typically gains initial access through Initial Access Brokers (IABs) or social engineering tactics, including phishing emails and malicious installers disguised as legitimate Windows updates. It uses embedded loaders to deliver its payload, which leverages privilege escalation, process termination, and anti-debugging techniques to evade detection. Cloak encrypts files using the HC-128 algorithm, with encryption keys generated through a multi-step process involving CryptGenRandom, Curve25519, and SHA512 hashing for secure key handling and IV generation. The ransomware supports both full and intermittent encryption modes to optimize performance and impact. Persistence is achieved via registry modifications, and recovery is obstructed by deleting volume shadow copies and disabling key system services. Cloak's use of virtual hard disk (VHD) delivery, stealthy execution, and destructive behaviors–such as selective file wiping–highlight its growing sophistication and threat potential.

- **Targeted Industries:** Cloak ransomware continues to target a wide range of industries–including manufacturing, healthcare, education, government, and professional services–across North America, Europe, and Asia. This broad targeting pattern reflects a globally opportunistic strategy aimed at exploiting vulnerable organizations across diverse sectors and regions.
- **Economic Model**: Cloak operates under a Ransomware-as-a-Service (RaaS) model, allowing affiliates to execute attacks using its tooling in exchange for a share of the ransom–typically a 70/30 split in favor of the affiliate. The group consistently employs double extortion tactics, encrypting victim data while exfiltrating sensitive information and threatening to publish it on a leak site if ransom demands are not met. This structure enables Cloak to scale operations while attracting experienced affiliates, reinforcing its position within the competitive RaaS ecosystem.

BianLian

Performance

- **RaaS Platform:** BianLian continues to operate as a non-traditional ransomware group, having never adopted a public Ransomware-as-a-Service (RaaS) model. First observed in June 2022 with a Golang-based ransomware, the group initially carried out full-spectrum attacks involving file encryption. However, following the release of a free decryptor in early 2023, BianLian pivoted to a pure extortion model–focusing solely on data exfiltration and threatening to publish stolen information unless a ransom is paid. This shift reflects a broader trend toward data-centric extortion that bypasses the need for encryption. While not among the most prolific threat actors, BianLian has remained active and persistent, sustaining operations against high-value targets.

BianLian continues to operate outside the traditional Ransomware-as-a-Service (RaaS) model and now exclusively conducts data extortion attacks, forging file encryption entirely.

- **Attack Volume:** BianLian has maintained a steady attack volume since shifting to a data-theft-only extortion model in early 2023. While not among the most prolific groups, it has remained consistently active, regularly posting new victims to its leak site and sustaining a persistent presence in the ransomware ecosystem.

- **Ransom Demands:** BianLian ransom demands have continued to vary by target, but recent trends show a significant increase compared to earlier activity. While initial demands ranged from $100,000 to $350,000, more recent incidents have seen average demands climb to around $3 million, reflecting the group's focus on high-value data theft and enterprise-scale extortion.

Innovation

- **RaaS Platform Development:** BianLian continues to operate outside the traditional Ransomware-as-a-Service (RaaS) model and now exclusively conducts data extortion attacks, forgoing file encryption entirely. The group originally deployed a Golang-based ransomware in 2022 but pivoted to a pure extortion strategy in early 2023 after the release of a free decryptor. BianLian exfiltrates sensitive data and threatens public exposure to coerce payment. Their toolset is heavily reliant on open-source utilities and native system functions, using command-line scripts for credential harvesting and Rclone to exfiltrate data. For persistence and remote access, BianLian deploys a custom backdoor written in Go, and leverages PowerShell and Windows Command Shell for lateral movement and defense evasion–favoring living-off-the-land techniques to minimize detection and maintain a low profile across compromised networks.

- **Targeted Industries:** BianLian continues to primarily target U.S.-based organizations, with a focus on sectors that manage highly sensitive data and face significant consequences from public exposure–such as healthcare, education, legal services, government, and critical infrastructure. The group's victim selection strategy reflects a calculated effort to pressure organizations that are more likely to pay to prevent reputational damage and regulatory fallout.

- **Economic Model**: BianLian operates under a self-managed economic model, executing the full attack lifecycle in-house–including initial access, data exfiltration, extortion, and ransom negotiation–without the use of affiliates or revenue-sharing arrangements. The group relies exclusively on a double extortion strategy, stealing sensitive data and threatening to publish it if payment is not made. This centralized approach allows BianLian to maintain tight operational control, minimize risk exposure, and retain 100% of ransom proceeds.

⚠ **CISA Alert:** CISA Alert aa23-136a

Sarcoma

Performance

- **RaaS Platform:** Sarcoma ransomware has rapidly established itself as a significant threat actor since first being identified in October 2024. Despite its recent emergence, the group has gained attention for executing aggressive and high-impact attacks, often resulting in major data breaches and operational disruption. Sarcoma's campaigns have demonstrated a clear strategic intent, with a particular emphasis on targeting critical points in supply chains to maximize downstream consequences. While full technical attribution is still evolving, Sarcoma's expanding footprint and consistent victim disclosures indicate a growing level of coordination, scale, and threat maturity within the ransomware ecosystem.
- **Attack Volume:** Sarcoma ransomware has maintained a sharp upward trajectory since launching in October 2024, when it carried out 31 attacks in its first month and reached 58 total by year-end. Its activity has continued to climb steadily through 2025, marked by increasingly frequent victim disclosures, rising ransom demands, and a clear shift toward high-value, enterprise-scale targets.
- **Ransom Demands:** Sarcoma's ransom demands have steadily escalated since its debut, initially starting in the mid-five-figure range. By early 2025, demands commonly reached the high six figures and, in cases involving large enterprises, have exceeded $1 million.

Sarcoma's campaigns have demonstrated a clear strategic intent, with a particular emphasis on targeting critical points in supply chains to maximize downstream consequences.

Innovation

- **RaaS Platform Development:** Sarcoma ransomware has demonstrated increasing technical sophistication, particularly through its use of remote monitoring and management (RMM) tools to conduct internal reconnaissance, escalate privileges, and expand access across compromised networks. In a confirmed attack on Smart Media Group Bulgaria, Sarcoma leveraged RMM software to identify vulnerabilities and pivot laterally, highlighting the group's ability to weaponize legitimate administrative tools for malicious purposes. While there have been unverified reports of zero-day exploitation, most observed intrusions rely on known vulnerabilities and misconfigurations. Sarcoma's tactics include disabling security services, deleting Volume Shadow Copies (VSS) to block recovery, and deploying encrypted payloads to avoid detection during execution. The ransomware uses AES-256 for file encryption, with RSA key exchange to securely lock decryption keys, making recovery nearly impossible without the attacker's private key. Although tools like PowerShell and Mimikatz are often used by comparable groups, there is currently no confirmed evidence that Sarcoma consistently relies on them, suggesting the use of alternative or custom tooling in its operations.

- **Targeted Industries:** Sarcoma ransomware continues to target a broad spectrum of industries—including manufacturing, logistics, legal services, accounting, and industrial supply—demonstrating a wide-ranging and opportunistic attack strategy. With confirmed victims across North America, Europe, Asia, and Africa, the group has established itself as a global threat, frequently focusing on organizations that manage sensitive data or play key roles in critical operational and supply chain functions.
- **Economic Model**: Sarcoma operates as a Ransomware-as-a-Service (RaaS) group, working with affiliates who conduct attacks in exchange for a share of ransom payments—typically following a 70/30 revenue split, with affiliates receiving the larger share. The group consistently employs double extortion tactics, exfiltrating sensitive data before encrypting systems and threatening to publish the stolen information on its dark web leak site if victims refuse to pay. This model allows Sarcoma to scale its operations quickly while maintaining pressure on victims through both operational disruption and reputational risk.

Ghost

Performance

- **RaaS Platform:** Ghost ransomware (aka GhostLocker) has continued to evolve following its initial release in October 2023 by GhostSec, a threat actor originally rooted in hacktivist operations associated with Anonymous. The launch of GhostLocker marked a clear transition from ideological hacking to financially motivated cybercrime. Originally built in Python, the ransomware was redeveloped into GhostLocker 2.0 using Golang by January 2024, improving its performance, scalability, and cross-platform compatibility. GhostLocker is part of a broader alliance known as "The Five Families," which includes GhostSec, Stormous, SiegedSec, ThreatSec, and others—a

Marketed as enterprise-grade ransomware, GhostLocker includes a web-based builder offering customization options such as anti-detection features, automated data exfiltration, multiple persistence mechanisms, and a WatchDog process to maintain execution.

collaborative model that reflects the increasing professionalization and strategic coordination among cybercriminal groups. In early 2024, GhostSec and Stormous jointly launched the STMX_GhostLocker Ransomware-as-a-Service (RaaS) platform, expanding their operational reach and further blurring the line between hacktivism and profit-driven ransomware activity. Ghost's trajectory highlights how threat actors with activist roots are adapting to the monetized ransomware ecosystem through shared infrastructure, rebranding, and tactical alliances.

- **Attack Volume:** Ghost ransomware has steadily increased its attack volume since launching GhostLocker in October 2023, building on earlier hacktivist roots. Now active in over 70 countries, the group's operations surged through late 2024 and into 2025, driven in part by its STMX_GhostLocker RaaS platform and collaborations with allied threat groups.

- **Ransom Demands:** Specific ransom demand figures for GhostLocker remain undisclosed, but based on broader ransomware trends, average demands across the ecosystem reached approximately $5.2 million in early 2024. GhostLocker is believed to tailor its demands based on the victim's size, industry, and data sensitivity, in line with other financially motivated groups.

Innovation

- **RaaS Platform Development:** As of Q2-2025, GhostLocker has evolved significantly from its initial release, reflecting growing technical maturity and commercialization. The original version, developed in Python, was packaged using tools like PyInstaller and Nuitka, and relied on dropping files and spawning child processes for encryption. In January 2024, GhostLocker 2.0 was released in Golang, enhancing detection evasion, execution speed, and cross-platform compatibility–supporting Windows, Linux, and VMware environments. The ransomware uses the Fernet symmetric encryption algorithm, which is built on AES-128 in CBC mode with PKCS7 padding. Marketed as enterprise-grade ransomware, GhostLocker includes a web-based builder offering customization options such as anti-detection features, automated data exfiltration, multiple persistence mechanisms, and a WatchDog process to maintain execution.

- **Targeted Industries:** GhostLocker ransomware has targeted a broad range of industries–including technology, education, healthcare, manufacturing, and critical infrastructure–across multiple regions, with confirmed activity in the Middle East, Africa, Asia, Europe, and the Americas.

- **Economic Model**: GhostLocker continues to operate as a Ransomware-as-a-Service (RaaS) platform, offering affiliates access to a web-based builder and control panel for customizing payloads, configuring encryption options, and managing victims. Affiliates typically pay an upfront fee ranging from $999 to $1,200 USD, with referral discounts and tiered incentives that resemble a pyramid-style recruitment model. The platform supports double extortion tactics–exfiltrating sensitive data before encryption and threatening to publish it on leak sites if ransoms go unpaid. While exact affiliate revenue shares have not been publicly confirmed, the structure appears to favor affiliates, with GhostSec and its partners retaining a smaller percentage for providing infrastructure and support.

KillSec

Performance

- **RaaS Platform:** KillSec has solidified its position as a hybrid threat actor, having transitioned from its origins as an Anonymous-aligned hacktivist group into a financially motivated ransomware operation. Initially known for website defacements and ideological attacks, KillSec shifted toward profit-driven cybercrime throughout 2024, adopting a Ransomware-as-a-Service (RaaS) model in June of that year. This move enabled affiliates to carry out attacks using KillSec's infrastructure and tooling, leading to a marked increase in both operational scale and global visibility. The group communicates with victims primarily through encrypted messaging platforms like Telegram and Tox, using them for extortion, negotiation, and public shaming. KillSec's evolution from hacktivism to structured ransomware activity reflects its growing tactical maturity and its integration into the broader cybercriminal ecosystem.

- **Attack Volume:** KillSec's attack volume has risen steadily since adopting a Ransomware-as-a-Service model in mid-2024, with a noticeable uptick in reported incidents across a wide range of sectors. The group's shift to a scalable affiliate-driven model has significantly expanded its operational footprint and increased the frequency of attacks globally.

- **Ransom Demands:** Specific figures for KillSec ransomware's average ransom demands remain unavailable. However, based on broader ransomware trends, average demands across the ecosystem exceeded $5.2 million in the first half of 2024, and KillSec is believed to tailor its demands based on the size and perceived value of each victim.

Designed for accessibility, the KillSec platform enables affiliates–including those with limited technical expertise–to execute ransomware campaigns using pre-built tools and infrastructure.

Innovation

- **RaaS Platform Development:** KillSec has significantly expanded its capabilities and reach through its Ransomware-as-a-Service (RaaS) platform launched in June 2024. Designed for accessibility, the platform enables affiliates–including those with limited technical expertise–to execute ransomware campaigns using pre-built tools and infrastructure. The offering includes a sophisticated file encryption locker written in C++, along with a Tor-based control panel that allows affiliates to anonymously manage attacks, victims, and payments. In addition to ransomware functionality, KillSec's RaaS package includes a denial-of-service (DDoS) tool, and an advanced data stealer used to exfiltrate credentials, documents, and browser-stored data for use in double extortion schemes. For initial access, the group leverages a mix of phishing campaigns, exploitation of known vulnerabilities, and deployment of custom malware to establish persistence and expand footholds within targeted networks.
- **Targeted Industries:** KillSec primarily targets organizations in government, manufacturing, finance, and professional services, focusing on victims likely to possess sensitive data and limited tolerance for operational disruption.
- **Economic Model**: KillSec operates under a Ransomware-as-a-Service (RaaS) model, supplying affiliates with ready-to-use ransomware payloads, infrastructure, and support in exchange for a share of ransom payments–typically following a 70/30 or 80/20 split favoring affiliates. The group employs a double extortion strategy, exfiltrating sensitive data prior to encryption and threatening to publish it if victims refuse to pay. This dual-pressure approach, combined with a low barrier to entry for affiliates, has helped KillSec rapidly expand its reach and increase its impact across a wide range of sectors.

Meow

Performance

- **RaaS Platform:** Meow ransomware (aka MeowLeaks or MeowCorp) continues to operate as a data extortion-focused threat actor that first emerged in late 2022. Believed to be a spinoff of the Conti gang due to code similarities, Meow initially operated with limited visibility but has since transitioned to a pure extortion model, stealing sensitive data and publishing it on its leak site without deploying file-encrypting malware. This mirrors tactics used by other data-focused groups like BianLian. Meow primarily targets U.S.-based organizations with valuable data, particularly in healthcare

Meow ransomware has fully transitioned into a data extortion-only operation, abandoning its earlier use of file-encrypting malware in favor of stealing sensitive information and leveraging public leak site exposure to coerce payment.

and medical research, though its broader victim base includes small and mid-sized businesses. A recent spike in claimed breaches–some overlapping with known BlackSuit incidents–has raised questions about the group's authenticity in certain cases, suggesting it may function as a data broker or amplify false claims to increase pressure on victims. Despite these credibility concerns, Meow remains an active and potentially damaging actor within the evolving landscape of extortion-centric ransomware operations.

- **Attack Volume:** Meow ransomware has significantly expanded its activity since its low volume start in late 2022. Throughout 2024 and into 2025, the group has intensified its focus on data extortion, frequently posting new victims to its leak site and demonstrating a marked increase in both operational tempo and public visibility.

- **Ransom Demands:** Specific data on Meow ransomware's average ransom demands remains limited, but available evidence suggests the group often targets smaller organizations with relatively modest demands. In at least one confirmed 2024 case, Meow issued a ransom demand as low as $7,000–significantly below the industry average of $3.7 million–indicating a volume-based or opportunistic extortion strategy aimed at maximizing payout likelihood from resource-constrained victims.

Innovation

- **RaaS Platform Development:** Meow ransomware has fully transitioned into a data extortion-only operation, abandoning its earlier use of file-encrypting malware in favor of stealing sensitive information and leveraging public leak site exposure to coerce payment. In its initial phase, Meow employed a hybrid encryption scheme using ChaCha20 for file encryption and RSA-4096 for key management, but by 2024, the group shifted entirely to exfiltration-based tactics. Initial access is typically achieved through phishing campaigns, exploitation of Remote Desktop Protocol (RDP) vulnerabilities, and compromises of widely used platforms such as VMware and Jenkins. Once inside, Meow operators use living-off-the-land techniques and a range of open-source tools for lateral movement and execution, though their tooling remains less well-documented compared to larger ransomware groups. Recent attacks have affected both Windows and Linux systems, including VMware ESXi environments, with a growing emphasis on organizations handling sensitive financial or personal data–particularly among small and mid-sized businesses.

- **Targeted Industries:** Meow ransomware primarily targets organizations handling sensitive financial and personal data, focusing on sectors like healthcare, financial services, professional services, and education–especially among small and mid-sized businesses more vulnerable to data exposure pressure.
- **Economic Model**: It remains unclear whether Meow operates as a RaaS platform or a closed, centralized group, as no confirmed affiliate structure or revenue-sharing details have been disclosed. The group's shift away from encryption and its opportunistic targeting–particularly of small and mid-sized organizations–suggest a streamlined, self-managed extortion model focused on speed, visibility, and lower barriers to victim coercion.

Emerging

Interlock

Performance

- **RaaS Platform:** Interlock emerged in late 2023 as a closed affiliate ransomware operation that blends custom malware development with aggressive extortion tactics. While not linked to any legacy ransomware groups, Interlock exhibits technical and strategic similarities to operations like BlackCat and LockBit, including selective encryption, recovery targeting, and the use of a modular toolset. The group operates under strict affiliate controls that require referrals and vetting, allowing Interlock to maintain operational discipline and reduce exposure. Interlock ransomware is deployed through custom obfuscated loaders, typically delivered using PowerShell or scripts that allow stealthy execution across both Windows and Linux systems. The group disables recovery infrastructure, deletes shadow copies, and establishes persistence through registry edits and scheduled tasks. Unlike many RaaS platforms, Interlock favors fast-moving intrusions and destructive payloads that maximize downtime for the victims.

- **Attack Volume:** Since its launch, Interlock has been linked to more than 80 confirmed ransomware incidents, with a steady operational tempo that has increased throughout 2024 and into 2025. Victim disclosures and leak site activity suggest Interlock has scaled quickly without compromising control over affiliate behavior or technical consistency.

- **Ransom Demands:** Interlock's ransom demands vary based on the victim's sector, size, and perceived urgency. Demands typically range from several hundred thousand dollars to multiple millions, with pressure tactics escalating based on victim response time and level of engagement.

Interlock ransomware is deployed through custom obfuscated loaders, typically delivered using PowerShell or scripts that allow stealthy execution across both Windows and Linux systems.

Innovation

- **RaaS Platform Development:** Interlock's ransomware platform uses AES encryption with RSA-wrapped keys and supports selective file encryption to balance impact and speed. The group regularly uses credential harvesting tools such as Mimikatz and deploys anti-debugging and process injection techniques to evade detection. Recovery tools are neutralized early in the attack chain, and endpoint protections are routinely disabled. Interlock uses custom-built payloads and commodity tools in tandem with Living-off-the-

Land Binaries (LOLBins), enabling flexibility across hybrid environments. Affiliates often gain initial access via credentials purchased from Initial Access Brokers or obtained through phishing. Once inside, Interlock operators conduct internal reconnaissance using tools such as PowerShell scripts and built-in network discovery commands. Lateral movement is achieved through RDP, PsExec, and abuse of native administrative utilities. The group has also deployed customized versions of existing tools to maintain persistence, avoid triggering security controls, and ensure access after reboots.

- **Targeted Industries:** Interlock targets a broad range of sectors including professional services, manufacturing, education, retail, and healthcare. The group has consistently attacked victims across North America, Europe, and Asia, with opportunistic targeting that prioritizes organizations holding sensitive data or operating under tight availability requirements.
- **Economic Model**: Interlock employs a standard double extortion model, encrypting files while exfiltrating sensitive data to increase leverage during negotiations. Affiliates receive approximately 70–80% of ransom payments, while the Interlock core operators maintain the infrastructure and tools in exchange for a share of the proceeds. Victims who refuse to pay are listed on Interlock's leak site, where stolen files are made publicly accessible in stages.

⚠ **CISA Alert:** CISA Alert aa25-203a

DevMan

Performance

- **RaaS Platform:** DevMan is a ransomware group first identified in early 2025 and is currently considered a non-public, closed operation rather than a Ransomware-as-a-Service (RaaS) platform. The group does not appear to work with affiliates and instead conducts attacks directly using a proprietary toolset. DevMan has been observed targeting Windows environments, with early samples indicating cross-platform development is underway, including limited functionality aimed at Linux and VMware ESXi systems. The group uses a data-extortion-first approach, though encryption is still employed in a majority of confirmed cases, suggesting DevMan operates with a hybrid model rather than as a pure data extortion crew.
- **Attack Volume:** Since emerging in Q1-2025, DevMan has maintained a low-to-moderate but rising attack tempo, with approximately 40–50 confirmed victims posted to its leak site as of Q2-2025.

DevMan uses custom info-stealer components embedded in payloads, indicating dual-use campaigns that combine ransomware deployment with credential harvesting operations.

- **Ransom Demands:** DevMan's ransom demands have varied significantly based on victim profile, with observed demands ranging from $100,000 to $1.5 million. While not as aggressive as top-tier actors, the group has shown a capacity to scale its demands based on data sensitivity and organizational size.

Innovation

- **RaaS Platform Development:** Though not a public RaaS, DevMan demonstrates a technically sophisticated and evolving toolset. Initial access is typically gained through phishing emails, brute-force attacks on Remote Desktop Protocol (RDP), or exploited vulnerabilities in edge-facing services. Once inside, DevMan operators use PowerShell and cmd-based scripts to deploy payloads and disable security tools. Volume Shadow Copies (VSS) are deleted to block system recovery. The group has been observed using DragonForce encryptors to carry out file encryption, employing AES-256 for data encryption and RSA-2048 to secure the encryption keys. DevMan has also deployed Mimikatz for credential theft and uses SoftPerfect Network Scanner for internal reconnaissance. Lateral movement is typically conducted using PsExec or RDP, and the group favors lightweight, in-memory execution to reduce detection. Analysts have also identified custom info-stealer components embedded in DevMan payloads, indicating dual-use campaigns that combine ransomware deployment with credential harvesting operations.

- **Targeted Industries:** DevMan primarily targets small to mid-sized enterprises across sectors including manufacturing, professional services, construction, and healthcare. Victim telemetry indicates a focus on North America and Western Europe, with a growing presence in Latin America. The group appears opportunistic, prioritizing ease of access over specific industry verticals.

- **Economic Model**: DevMan operates as a closed threat group, not as a RaaS, and retains full control of the attack lifecycle from initial access to negotiation. It employs a double extortion model, combining encryption with the exfiltration of sensitive data, which is then used to pressure victims via its leak site. The group has not been observed offering affiliate access or revenue sharing, further reinforcing its status as a self-contained operation.

NightSpire

Performance

- **RaaS Platform:** NightSpire is an emerging ransomware group first observed in early 2025. While early reporting speculated that it may be affiliated with or inspired by elements of older RaaS groups, NightSpire currently operates as a closed group and does not function as a public Ransomware-as-a-Service (RaaS) platform. The group carries out attacks internally without offering access to outside affiliates. NightSpire ransomware is designed to target Windows-based systems, with artifacts suggesting ongoing development toward Linux and ESXi compatibility, though widespread cross-platform deployment has not yet been confirmed. NightSpire combines file encryption with data theft, using a classic double extortion model, and maintains a dedicated Tor-based leak site to pressure non-paying victims.
- **Attack Volume:** NightSpire remains low-volume but consistent, with approximately 25–30 confirmed victims posted to its leak site since its debut. The group has maintained a targeted campaign approach, prioritizing stealth and control over volume.
- **Ransom Demands:** NightSpire ransom demands typically fall between $150,000 and $2 million, depending on the victim's size and the sensitivity of the exfiltrated data.

Innovation

- **RaaS Platform Development:** NightSpire demonstrates moderate but advancing technical sophistication. Initial access methods include phishing emails with malicious attachments, compromised RDP credentials, and exploitation of vulnerable web applications. Once inside, operators use PowerShell scripts, Windows Command Shell, and batch files to deploy payloads and disable endpoint protections. The ransomware uses AES-256 for file encryption and RSA-2048 for key encryption. Volume Shadow Copies are deleted to prevent recovery, and the group uses Mimikatz for credential harvesting. Lateral movement is achieved using PsExec, with RDP and WMI used to pivot between hosts. NightSpire also deploys open-source network scanning tools like Advanced IP Scanner and uses custom obfuscation routines to hinder detection and sandbox analysis. Persistence is maintained via registry keys and scheduled tasks, and in several incidents, the ransomware was launched from temporary directories using renamed processes to further evade endpoint detection.

NightSpire deploys open-source network scanning tools like Advanced IP Scanner and uses custom obfuscation routines to hinder detection and sandbox analysis.

- **Targeted Industries:** NightSpire primarily targets professional services, real estate, healthcare, and regional manufacturing firms, with most incidents concentrated in North America and parts of Western Europe. Victim selection suggests a focus on mid-market organizations with under-resourced security programs and high-value datasets.

- **Economic Model**: NightSpire operates as a closed operation, handling all stages of attack execution and negotiation without external affiliates. It employs a double extortion model, exfiltrating sensitive data before deploying ransomware and threatening to publish the stolen files if the ransom is not paid. All known operations are run internally, and no evidence of revenue sharing or public recruitment has been observed, indicating that NightSpire is a self-contained threat actor focused on control and operational security.

FunkSec

Performance

- **RaaS Platform:** FunkSec is a recently emerged ransomware group, first identified in early 2025, and appears to be operating as a closed group rather than a public Ransomware-as-a-Service (RaaS) platform. The group does not advertise affiliate recruitment and handles all aspects of attack execution internally. FunkSec ransomware is currently designed for Windows environments, with limited evidence suggesting early experimentation with Linux-targeting capabilities, though these remain unconfirmed in active campaigns.

- **Attack Volume:** FunkSec has displayed low but rising attack volume, with approximately 20–25 victims posted to its leak site since its emergence. The group's operational tempo is gradually increasing, and their targeting has shown signs of becoming more selective and impactful.

- **Ransom Demands:** FunkSec's ransom demands typically range from $75,000 to $1 million, with variation based on the victim's size, data sensitivity, and operational footprint. In some cases, the group has offered discounted payments for quick resolution, suggesting a willingness to negotiate for faster monetization rather than pursuing maximum possible payouts.

FunkSec makes use of off-the-shelf reconnaissance tools, including Advanced IP Scanner, and hides its payloads with basic obfuscation and renamed executables to bypass signature-based defenses.

Innovation

- **RaaS Platform Development:** FunkSec is not a traditional RaaS platform and does not appear to engage in affiliate-based campaigns. Initial access methods include phishing emails, malicious Microsoft Office documents, and brute-forced RDP endpoints. After gaining access, the group uses PowerShell and batch scripts to disable security solutions and deploy its payload. Encryption is executed using AES-256, with RSA-2048 securing the encryption keys. The ransomware deletes Volume Shadow Copies and disables Windows recovery features to block restoration. Credential theft is achieved using Mimikatz, and lateral movement is conducted through RDP, WMI, and PsExec. FunkSec also makes use of off-the-shelf reconnaissance tools, including Advanced IP Scanner, and hides its payloads with basic obfuscation and renamed executables to bypass signature-based defenses.

- **Targeted Industries:** FunkSec has primarily focused on small to mid-sized organizations in professional services, regional finance, IT services, and logistics, with attacks concentrated in North America and parts of Central Europe.

- **Economic Model**: FunkSec operates a self-managed, closed economic model, with no known public affiliate recruitment or revenue sharing. All observed campaigns have been executed internally by the core operators. The group uses double extortion tactics, exfiltrating sensitive data before encryption and threatening to leak it via their Tor-based site if payment is not made. FunkSec's model favors agility and direct control over scale, likely allowing for faster negotiation cycles and tighter operational security.

ArcusMedia

Performance

- **RaaS Platform:** Arcus Media has quickly established itself as a technically advanced Ransomware-as-a-Service (RaaS) operation since its emergence in May 2024. Gaining early notoriety through a wave of high-impact attacks, the group distinguishes itself by deploying custom-built malware rather than relying on leaked or recycled code–indicating a high level of in-house development capability. Arcus Media operates a closed affiliate model, requiring referrals and vetting to join, which helps maintain operational security and limit exposure. Within months of its debut, the group was linked to over 50 confirmed attacks, reflecting both scale and coordination. Though not directly associated with any major legacy ransomware brands,

Arcus Media disables security tools, halts recovery services, deletes shadow copies to block restoration, and establishes persistence via registry changes and scheduled tasks, enabling Arcus Media to maintain control across system reboots.

Arcus Media's structure and approach—particularly its calculated targeting, selective encryption, and recovery sabotage—mirror the playbooks of past groups like REvil and DarkSide.

- **Attack Volume:** Arcus Media has continued its rapid rise in attack volume, solidifying its reputation as a high-frequency threat actor. Since its emergence in May 2024, the group has been linked to more than 75 ransomware incidents, reflecting a fast-growing operational tempo and the expansion of its tightly controlled affiliate network.

- **Ransom Demands:** Specific figures for Arcus Media's average ransom demands remain undisclosed. However, early incident reporting suggests the group tailors its demands based on victim size and sector, with some cases involving demands ranging from several hundred thousand to multiple millions of dollars.

Innovation

- **RaaS Platform Development:** Arcus Media continues to demonstrate a high level of technical sophistication through its use of advanced tactics, techniques, and procedures (TTPs). Initial access is typically achieved via phishing campaigns or through compromised credentials acquired from Initial Access Brokers. Once inside, the group deploys its custom-built ransomware using obfuscated scripts and loaders, enabling stealthy execution and flexible delivery. The ransomware performs selective file encryption using the AES algorithm, with RSA employed for secure key exchange—ensuring efficiency while maximizing operational disruption. Arcus Media uses tools such as Mimikatz for credential harvesting and privilege escalation, while employing process injection and anti-debugging techniques to evade endpoint detection. The malware disables security software, terminates recovery-related services, and deletes shadow copies to prevent system restoration. Persistence is established through registry modifications and scheduled tasks, allowing the ransomware to survive reboots and maintain control over infected systems. The group's modular architecture and adaptive toolset reflect a mature, evolving framework built to deliver fast, damaging, and hard-to-recover-from attacks.

- **Targeted Industries:** Arcus Media continues to target a wide range of industries—including business services, retail, media, healthcare, and manufacturing—demonstrating an opportunistic strategy aimed at organizations with valuable or sensitive data. Its attacks have been observed across North America, Europe, and parts of Asia, indicating a growing global reach and a focus on regions with high concentrations of data-rich enterprises.

- **Economic Model**: Arcus Media operates under a controlled Ransomware-as-a-Service (RaaS) model, working with a selectively vetted group of affiliates who receive approximately 70% of ransom payments, while the core operation retains the remaining 30%. The group employs consistent double extortion tactics, stealing sensitive data prior to encryption and threatening public disclosure via its leak site to increase pressure on victims. This structured economic model, combined with its use of custom tooling and high-impact targeting, has positioned Arcus Media as a rapidly growing and increasingly organized player in the ransomware ecosystem.

RALord (Nova)

Performance

- **RaaS Platform:** RALord (Nova) is an emerging ransomware operation first observed in early 2025, currently believed to operate as a closed group, with no evidence suggesting a public Ransomware-as-a-Service (RaaS) structure. The group does not appear to recruit affiliates and instead conducts all stages of the attack lifecycle internally. RALord (Nova) ransomware is designed for Windows-based environments, and while references to Linux payload development have surfaced in underground forums, no Linux variant has been observed in active campaigns to date.

- **Attack Volume:** RALord (Nova) attack volume is relatively low, with fewer than 20 confirmed victims posted since its emergence. The group appears to be in the early stages of development and refinement, with attacks showing growing consistency but of a limited scale.

- **Ransom Demands:** Their ransom demands generally fall between $50,000 and $750,000, with pricing adjusted based on the victim's size, data sensitivity, and operational impact. The group has shown a tendency to offer "early payment" discounts and has used staged threats (e.g., data samples posted in phases) to escalate pressure on victims during negotiations.

RALord (Nova) routinely deletes Volume Shadow Copies and disables System Restore to block recovery, while using Mimikatz for credential harvesting, PsExec and WMI for lateral movement, and deploying tools like SoftPerfect for internal reconnaissance.

Innovation

- **RaaS Platform Development:** RALord (Nova) does not operate a RaaS model and does not advertise affiliate access. Initial access is typically achieved through phishing emails, malicious document attachments, or RDP brute force attacks. Once inside, the group deploys its ransomware payload via PowerShell scripts, often preceded by the disabling of security tools using batch commands and registry edits. RALord (Nova) uses AES-

256 encryption for files and RSA-2048 for securing encryption keys. The ransomware routinely deletes Volume Shadow Copies and disables System Restore to prevent recovery. Credential harvesting is conducted using Mimikatz, and lateral movement is achieved using PsExec and WMI, with evidence of network scanning tools like SoftPerfect deployed for internal reconnaissance. Persistence is typically achieved via scheduled tasks and autorun registry keys.

- **Targeted Industries:** RALord (Nova) primarily targets small to mid-sized organizations across sectors such as legal services, small finance firms, education, and regional healthcare, with activity concentrated in North America and parts of Eastern Europe. The group appears opportunistic, favoring targets with exposed services or weaker security postures over specific industry verticals.
- **Economic Model**: RALord (Nova) operates a self-contained economic model, executing attacks end-to-end without affiliate involvement. The group uses a double extortion approach, stealing sensitive data before encryption and threatening to publish it if victims do not pay. All proceeds appear to be retained by the core operators, and no evidence of profit-sharing or RaaS infrastructure has been observed. This tightly controlled model allows them to maintain operational secrecy but limits its scale compared to open affiliate-based groups.

Diminishing

Cl0p

Performance

- **RaaS Platform:** Cl0p appears to be a diminishing force in the ransomware ecosystem, following a sharp rise to prominence in mid-2023. First observed in 2019, Cl0p built a reputation for advanced evasion techniques, including anti-analysis and anti-VM capabilities, and gained global attention through large-scale exploitation of file transfer vulnerabilities–most notably MOVEit Transfer (CVE-2023-34362) and GoAnywhere MFT (CVE-2023-0669). At its peak in July 2023, Cl0p was responsible for an estimated 21% of all ransomware activity, driven by automated mass exploitation. Although the group shifted to a data-theft-only model in early 2023, it briefly returned to deploying file-encrypting malware before fading from visibility. A short-lived resurgence in late 2024 and early 2025–fueled by the exploitation of Cleo Integration Cloud vulnerabilities (CVE-2024-50623 and CVE-2024-55956)–has since cooled, and Cl0p's overall activity has declined significantly, suggesting the group may be in retreat or transitioning out of sustained operations.

- **Attack Volume:** Cl0p's attack volume continued to decline following a brief resurgence in late 2024 and early 2025 driven by the exploitation of Cleo Integration Cloud vulnerabilities. While the group previously saw major spikes linked to mass exploitation campaigns–most notably during the MOVEit incident in mid-2023–its activity has since diminished significantly, with few confirmed attacks in recent months.

- **Ransom Demands:** Cl0p ransom demands have historically varied based on the scope and profile of each attack, often reflecting the group's preference for large-scale, high-value targets. During its peak in Q2 2023, Cl0p's average ransom demand reached approximately $2.51 million, with mid-year data indicating average payouts of around $1.73 million per victim–highlighting the group's significant financial impact at the time. However, since its brief resurgence in late 2024, there have been fewer confirmed ransom negotiations, and no updated payout data has been publicly disclosed, aligning with the group's overall decline in activity.

Cl0p's economic model remains focused on large-scale, high-impact breaches, typically involving the exploitation of enterprise file transfer software to steal sensitive data and demand substantial ransoms.

Innovation

- **RaaS Platform Development:** Cl0p continues to operate as a Ransomware-as-a-Service (RaaS) group, though its activity has diminished following a brief resurgence in late 2024. The group expanded its technical capabilities in late 2022 by developing a Linux variant of its ransomware, broadening its reach beyond Windows environments. Its Windows payload, written in C++, uses RC4 for file encryption and secures encryption keys with 1024-bit RSA. In early 2023, Cl0p began exploiting Fortra's GoAnywhere MFT vulnerability (CVE-2023-0669), followed by a highly impactful campaign targeting Progress Software's MOVEit Transfer (CVE-2023-34362), a SQL injection flaw that enabled mass data exfiltration without encryption. This MOVEit campaign marked a significant tactical shift toward pure data theft and accounted for approximately 21% of all ransomware incidents in July 2023. After a period of reduced visibility, Cl0p resurfaced in late 2024 by exploiting two zero-day vulnerabilities in the Cleo Integration Cloud. The first, CVE-2024-50623, disclosed in October, allowed unauthorized file uploads and downloads, while the second, CVE-2024-55956, discovered in December, enabled broader unauthorized system access. These campaigns reinforced Cl0p's specialization in exploiting enterprise-grade file transfer platforms and demonstrated its continued ability to pivot between encryption-based ransomware and data-theft extortion depending on the target and opportunity.

- **Targeted Industries:** Cl0p primarily targets large organizations in sectors like finance, healthcare, education, government, and critical infrastructure. The group focuses on high-value victims, often breaching networks by exploiting file transfer system vulnerabilities, though recent activity has declined.

- **Economic Model**: Cl0p's economic model remains focused on large-scale, high-impact breaches, typically involving the exploitation of enterprise file transfer software to steal sensitive data and demand substantial ransoms. The group primarily uses double extortion tactics—combining data theft with encryption—but has increasingly emphasized data-centric extortion, particularly in high-profile campaigns like MOVEit. While Cl0p is believed to operate as a RaaS at times, it appears to rely on a small, tightly controlled group of trusted affiliates rather than a broad open model. Revenue-sharing details are not publicly confirmed, but Cl0p's preference for precision-targeted campaigns suggests a selective affiliate structure aimed at maximizing payout and minimizing operational risk.

⚠ **CISA Alert:** CISA Alert aa23-158a

BlackLock (El Dorado)

Performance

- **RaaS Platform:** BlackLock (El Dorado) has faded significantly from prominence following a brief but technically notable emergence in March 2024. Positioned early on as an advanced and independent operation, El Dorado distinguished itself by developing its own proprietary ransomware builder rather than relying on leaked or recycled code, signaling a clear intent to operate outside the shadow of legacy groups like LockBit or Conti. The group launched with a closed affiliate program and a strong focus on cross-platform compatibility and encryption strength, indicating a structured and experienced team behind the scenes. However, momentum stalled in late Q1 2025 after researchers exploited a vulnerability in El Dorado's dark web leak site, exposing its infrastructure and dealing a serious blow to its credibility and operational security. Since then, BlackLock activity has declined sharply, and the group is now considered to be in decline, with little evidence of continued high-impact operations.

- **Attack Volume:** BlackLock (El Dorado) saw a brief surge in activity after its March 2024 debut, targeting multiple sectors. However, following a major infrastructure compromise in early 2025, its attack volume has dropped sharply, and the group is now considered a diminishing threat.

- **Ransom Demands:** Specific figures for BlackLock (El Dorado) average ransom demands remain undisclosed but based on its focus on enterprise targets and industry norms, demands are likely in the high six- to seven-figure range.

Developed from a proprietary builder–entirely independent of leaked codebases–BlackLock's tooling offers extensive customization and operational flexibility, allowing attackers to tailor payloads to specific environments.

Innovation

- **RaaS Platform Development:** As of Q2-2025, BlackLock (El Dorado) ransomware remains technically advanced despite a sharp decline in activity. Written in Golang, it offers cross-platform capabilities to target Windows, Linux, and VMware ESXi environments. The ransomware uses the ChaCha20 algorithm for file encryption, paired with RSA-OAEP for secure key exchange, providing strong cryptographic integrity. It can encrypt files across SMB network shares, allowing it to disrupt shared storage and enterprise infrastructure. The malware supports custom configurations, enabling operators to define target directories, exclude critical file types like DLLs and EXEs, and prioritize network-based resources. Upon execution, it self-deletes to hinder forensic analysis and limit post-incident investigation. Developed from a proprietary builder–entirely independent of leaked codebases–

BlackLock's tooling offers extensive customization and operational flexibility, allowing attackers to tailor payloads to specific environments. Despite its sophistication, the group's recent inactivity suggests these capabilities are currently underutilized or abandoned.

- **Targeted Industries:** BlackLock (El Dorado) ransomware has primarily targeted industries such as manufacturing, IT services, healthcare, and professional services across North America, Europe, and Asia. While its past activity reflected a global, enterprise-focused strategy, recent inactivity indicates a significant decline in operational reach.
- **Economic Model**: BlackLock (El Dorado) operates under a Ransomware-as-a-Service (RaaS) model, providing a proprietary builder to a small group of vetted affiliates. Affiliates reportedly retained up to 70% of ransom payments, with the remainder going to the core operators. The group consistently used double extortion tactics–exfiltrating sensitive data before encrypting systems and threatening to publish the stolen information if ransoms were not paid. However, following a major infrastructure compromise and a sharp decline in activity, the sustainability of this model appears in question, and the operation is now considered to be in decline.

LockBit

Performance

- **RaaS Platform:** LockBit–once the most prolific Ransomware-as-a-Service (RaaS) platform since its launch in 2019–is now showing clear signs of decline following sustained law enforcement pressure and internal disruption. Known for its advanced evasion capabilities, rapid encryption speed, and aggressive multi-extortion tactics, LockBit gained notoriety for demanding separate ransoms for file decryption and the suppression of leaked data, often exfiltrated using both public file-sharing services and its proprietary tool, Stealbit. However, the group's dominance has been seriously undermined since Operation Cronos in February 2024, when international law enforcement seized large portions of LockBit's infrastructure, temporarily disabling its leak site and admin panel. Although operations resumed within days, the takedown revealed critical weaknesses in the group's backend systems and sowed distrust among affiliates. Further blows came in December 2024, when U.S. authorities charged alleged developer Rostislav Panev, fueling speculation that LockBit's leadership structure had been compromised. Despite announcements of a forthcoming "LockBit 4.0" update, the group has struggled to maintain momentum, with fewer verified

Despite announcements of a forthcoming "LockBit 4.0" update, the group has struggled to maintain momentum, with fewer verified attacks and increased skepticism surrounding its claims–such as the widely disputed allegation of breaching the U.S. Federal Reserve.

attacks and increased skepticism surrounding its claims–such as the widely disputed allegation of breaching the U.S. Federal Reserve. LockBit remains technically capable, but its credibility, affiliate loyalty, and overall activity appear to be fading, marking it as a diminishing force in the ransomware ecosystem.

- **Attack Volume:** LockBit's attack volume has dropped significantly from its peak. While it remained highly active through early 2024–despite disruptions like Operation Cronos–the number of confirmed incidents has since declined sharply. With fewer verified attacks and growing skepticism around its victim claims, LockBit appears to be losing momentum, even as it promotes the upcoming release of LockBit 4.0.

- **Ransom Demands:** LockBit ransom demands typically range from $100,000 to over $5 million, depending on the victim's size, sector, and perceived ability to pay. The group continues to tailor its demands strategically, often adjusting based on the sensitivity of stolen data and the organization's financial profile.

Innovation

- **RaaS Platform Development:** LockBit remains technically sophisticated despite its declining activity, continuing to refine its tooling across multiple platforms. Following the release of LockBit 3.0 in June 2022, the group expanded its capabilities with a macOS variant in April 2023–one of the first serious attempts by a major ransomware group to target Apple systems. LockBit 3.0 features advanced anti-analysis techniques, a modular architecture for customized execution, and support for attacks on Windows, Linux, and VMware ESXi systems. The ransomware uses a customized Salsa20 encryption algorithm and commonly gains initial access through Remote Desktop Protocol (RDP) exploitation or compromised credentials. Once inside a network, LockBit spreads laterally using Group Policy Objects (GPO) and PsExec over SMB, enabling rapid deployment across enterprise environments. The group has also exploited vulnerabilities such as CVE-2023-4966 (Citrix Bleed) to bypass multi-factor authentication and expand access. While LockBit 3.0 remains the most widely used variant, some affiliates still deploy LockBit 2.0, and victims from both versions continue to be listed on LockBit's leak site. Although the group announced LockBit 4.0 for release in February 2025, as of Q2 there is limited public evidence of its deployment at scale–raising questions about its current operational capacity amid falling attack volume and increased law enforcement scrutiny.

- **Targeted Industries:** LockBit continues to primarily target large organizations in high-value industries such as finance, healthcare, manufacturing, and government. Its focus remains on enterprises that manage critical infrastructure or sensitive data—though recent activity suggests a narrowing scope amid declining operational momentum.

- **Economic Model**: As of Q2-2025, LockBit continues to operate under a Ransomware-as-a-Service (RaaS) model, offering affiliates up to 75% of ransom proceeds—one of the most competitive profit-sharing structures in the ransomware ecosystem. This generous model helped fuel LockBit's rise, attracting skilled affiliates and enabling widespread, large-scale attacks across high-value sectors. The group relies heavily on double extortion tactics, encrypting systems while exfiltrating sensitive data to pressure victims into payment through public leak threats. However, recent law enforcement actions—particularly Operation Cronos—have severely disrupted LockBit's infrastructure and reportedly led to a significant loss of affiliates. This attrition has likely undermined the group's ability to maintain previous attack volumes, contributing to its ongoing decline in operational reach and effectiveness.

⚠ **CISA Alerts:**
CISA Alert aa23-075a / CISA Alert aa23-165a / CISA Alert aa23-325a

BlackBasta

Performance

- **RaaS Platform:** As of Q2-2025, BlackBasta remains a technically capable but increasingly diminished Ransomware-as-a-Service (RaaS) operation that first emerged in April 2022. It rapidly became one of the most active ransomware groups through 2022 and 2023, gaining a reputation for targeting large enterprises with precision and speed. While some researchers have suggested links to the defunct Conti group, no conclusive evidence has confirmed this affiliation. BlackBasta's platform is based on a customized variant of LockBit ransomware dating back to late 2022, reflecting a strong technical foundation. However, the group's visibility and attack volume have declined significantly in recent months, suggesting a potential loss of affiliate support, strategic retreat, or internal disruption.

- **Attack Volume:** BlackBasta's attack volume has declined significantly after peaking in 2023 and early 2024. Once among the most active ransomware groups, recent months have seen fewer confirmed incidents and reduced visibility, indicating a drop in momentum and possible affiliate attrition.

The coordinated use of custom ransomware, targeted vulnerability exploitation, credential theft, persistence tooling, and evasion techniques positioned BlackBasta as a technically advanced and persistent threat actor—despite a recent decline in activity.

- **Ransom Demands:** BlackBasta's ransom demands continue to vary depending on the victim's size and industry, with some reported demands reaching up to $9 million. Estimates suggest that approximately 35% of victims have paid, enabling the group to generate over $107 million in ransom revenue from more than 500 confirmed attacks within its first two years of operation.

Innovation

- **RaaS Platform Development:** BlackBasta continues to exhibit a high level of technical proficiency through a wide range of advanced tactics, techniques, and procedures (TTPs). The group targets both Windows and Linux systems, with expertise in exploiting enterprise platforms such as VMware ESXi. Its ransomware, written in C++, uses the ChaCha20 algorithm for file encryption and RSA-4096 for encrypting the symmetric key–resulting in fast, efficient, and secure encryption across large environments. Initial access is often achieved by exploiting known vulnerabilities, including PrintNightmare (CVE-2021-34527), as well as through poorly secured or misconfigured Remote Desktop Protocol (RDP) services. Once inside the network, BlackBasta has been observed deploying Qakbot, a banking Trojan and credential stealer, to harvest login information, and SystemBC, a proxy malware used to maintain persistence and mask command-and-control traffic. The group also disables endpoint protections such as Windows Defender using PowerShell commands, batch scripts, and Group Policy Objects (GPOs) to suppress alerts and prevent remediation efforts. For lateral movement and post-exploitation, BlackBasta relies on Cobalt Strike, a widely used red-teaming tool repurposed by many threat actors to maintain control and execute payloads across networks. This coordinated use of custom ransomware, targeted vulnerability exploitation, credential theft, persistence tooling, and evasion techniques positions BlackBasta as a technically advanced and persistent threat actor–despite a recent decline in activity.

- **Targeted Industries:** BlackBasta continues to primarily target high-value industries including healthcare, finance, manufacturing, and retail, with a focus on organizations that manage sensitive data and have large, distributed operational infrastructures. The group has conducted attacks against both public and private sector entities across multiple regions, though recent activity suggests a decline in scale and frequency.

- **Economic Model**: BlackBasta continues to operate under a Ransomware-as-a-Service (RaaS) model, employing a double extortion strategy that involves both encrypting victim data and exfiltrating sensitive information to pressure victims into paying. The group is known for its selective and disciplined affiliate recruitment process, working with a vetted group of experienced operators to carry out highly targeted, high-impact attacks. Affiliates reportedly receive up to 80% of ransom proceeds, with the core BlackBasta team retaining the remainder. This tightly controlled economic model has enabled the group to maintain operational security and effectiveness, though a decline in recent attack volume suggests possible affiliate attrition or internal disruption.

⚠ **CISA Alert:** CISA Alert aa24-131a

RansomHub

Performance

- **RaaS Platform:** RansomHub is showing signs of decline after a brief period of high activity and visibility following its emergence in early 2024. Initially drawing attention for its advanced ransomware deployment and generous affiliate terms–offering up to 90% of ransom payments–RansomHub quickly positioned itself as a competitive RaaS platform. While early comparisons were made to LockBit, its codebase more closely resembles that of the now-defunct Knight group, suggesting a possible rebranding or code inheritance. RansomHub initially distinguished itself by enforcing strict affiliate policies, requiring compliance with victim negotiation agreements and threatening bans for violations–an attempt to maintain credibility and control. However, in recent months, the group's attack volume has dropped significantly, with fewer confirmed incidents and less affiliate chatter in underground forums. This decline suggests diminishing momentum, potential affiliate attrition, and waning influence in the broader ransomware ecosystem.

- **Attack Volume:** RansomHub's attack volume has declined sharply following its peak in Q4-2024, when it was the most prolific RaaS group with over 600 confirmed victims. Despite its rapid rise, activity dropped significantly in early 2025, with fewer new victims posted and a noticeable slowdown in affiliate-driven campaigns.

- **Ransom Demands:** RansomHub's average ransom demand is estimated to be around $2.79 million, though actual amounts vary depending on the victim's industry, size, and the sensitivity of the stolen data. This variability reflects the group's tailored extortion approach, aligning ransom demands with each victim's perceived ability to pay.

Once inside, RansomHub uses tools like Mimikatz for credential harvesting, Angry IP Scanner and Nmap for network reconnaissance, PsExec and RDP for lateral movement, and deploys EDRKillShifter to bypass endpoint detection and response (EDR) solutions.

Innovation

- **RaaS Platform Development:** RansomHub continues to demonstrate advanced technical capabilities, targeting both Windows and Linux systems, including VMware ESXi environments. The group frequently exploits unpatched vulnerabilities such as CVE-2023-3519 (Citrix NetScaler ADC and Gateway), CVE-2023-27997 (Fortinet SSL-VPN), and CVE-2020-1472 (Netlogon, aka ZeroLogon) to gain initial access. In addition, they conduct brute-force attacks on Remote Desktop Protocol (RDP) and VPN services to infiltrate poorly secured networks. Once inside, RansomHub uses tools like Mimikatz for credential harvesting, Angry IP Scanner and Nmap for network reconnaissance, and PsExec and RDP for lateral movement. To evade detection and disable defenses, they may deploy EDRKillShifter, a known tool for bypassing endpoint detection and response (EDR) solutions. The ransomware encrypts data using a combination of Curve25519, ChaCha20, and AES encryption algorithms, and systematically deletes Volume Shadow Copies and other backups to prevent data recovery. RansomHub also employs double extortion tactics, exfiltrating sensitive data and threatening to leak it publicly if the ransom is not paid–further increasing pressure on victims to comply.

- **Targeted Industries:** RansomHub continues to target a wide range of industries, including healthcare, manufacturing, professional services, financial services, high technology, and the public sector. The group adopts an opportunistic approach, focusing on vulnerable, high-value targets across various sectors and organization sizes, prioritizing potential impact and payout over industry specificity.

- **Economic Model**: RansomHub operates as a Ransomware-as-a-Service (RaaS) platform that uses double extortion tactics–encrypting victims' data while exfiltrating sensitive information and threatening public leaks if the ransom is not paid. The group offers affiliates up to 90% of ransom proceeds, one of the highest payout rates in the ransomware ecosystem, which has helped attract seasoned operators, including former affiliates from dismantled groups like BlackCat/ALPHV. This generous commission structure, combined with aggressive recruitment and continued development, positioned RansomHub as a major player in late 2024. However, recent declines in activity suggest the operation may now be losing momentum, with affiliate attrition and law enforcement pressure possibly undermining its long-term sustainability.

⚠ **CISA Alert:** CISA Alert aa24-242a

Hunters International

Performance

- **RaaS Platform:** Hunters International is showing signs of decline following a period of sustained activity after its October 2023 debut. Widely believed to be the technical successor to the dismantled Hive ransomware group–despite public denials–the group's codebase shares clear lineage with Hive, indicating a continuation of its tools and techniques. Initially, Hunters International gained traction through a high-frequency campaign cadence and a sophisticated double extortion model, which included embedding decryption keys directly within encrypted files–a notable evolution intended to streamline recovery for paying victims. However, by mid-2025, the attack volume has tapered off significantly, and the group's presence on leak sites and in incident reporting has diminished. This decline in activity may be attributed to affiliate loss, increased law enforcement pressure, or competition from more active RaaS platforms. As a result, Hunters International is now viewed as a diminishing threat–one that launched with momentum but is increasingly fading from the ransomware landscape.

- **Ransom Demands:** Specific figures for Hunters International's ransom demands remain undisclosed, but available evidence suggests they likely align with or exceed the 2024 industry average of $2.73 million. The group's focus on high-value targets and use of double extortion tactics support the assumption that demands are tailored to extract maximum leverage based on the victim's size and sector.

Hunters International introduced a custom C#-based Remote Access Trojan (RAT) known as SharpRhino, distributed through typosquatted domains mimicking legitimate tools like Angry IP Scanner. SharpRhino provides stealthy, persistent remote access, enabling deeper control over compromised environments.

Innovation

- **RaaS Platform Development:** Hunters International continues to demonstrate a technically capable and methodical approach to ransomware operations, though its activity has declined in recent months. Initially broad in scope, the group has since refined its targeting to high-ransom-potential sectors such as healthcare, financial services, and critical infrastructure, where data sensitivity and operational disruption can create maximum leverage. Initial access is gained through a variety of vectors, including phishing campaigns, social engineering, supply chain compromises, and the exploitation of Remote Desktop Protocol (RDP). Once inside, Hunters International disables Endpoint Detection and Response (EDR) solutions using batch scripts and administrative tools, while leveraging PowerShell and Windows Command Shell to execute payloads and maintain stealth. The group uses Mimikatz for credential harvesting and creates new domain accounts for persistence. Tools like SoftPerfect Network Scanner are deployed to map internal assets, and PsExec and RDP are commonly used for lateral movement. System recovery is obstructed by deleting Volume Shadow Copies, making restoration without a decryptor nearly impossible. In mid-2024, Hunters International introduced a custom C#-based Remote Access Trojan (RAT) known as SharpRhino, distributed through typosquatted domains mimicking legitimate tools like Angry IP Scanner. SharpRhino provides stealthy, persistent remote access, enabling deeper control over compromised environments. The group has also enhanced its encryption routines and adopted more sophisticated data exfiltration methods, reinforcing its double extortion strategy and emphasizing a focus on efficiency, stealth, and sustained pressure on victims.

- **Targeted Industries:** Hunters International continues to favor high-value targets in sectors such as healthcare, financial services, critical infrastructure, education, and manufacturing, with a primary focus on organizations based in North America and Europe.

- **Economic Model**: Hunters International operates under a Ransomware-as-a-Service (RaaS) model, leveraging double extortion tactics that combine data encryption with the exfiltration of sensitive information to pressure victims into payment. Affiliates are offered a competitive revenue share–reportedly up to 80% of ransom proceeds–making the platform attractive to experienced operators. This model enabled rapid expansion following the group's debut in late 2023. However, recent declines in attack volume suggest the operation may be losing affiliates or facing internal challenges, diminishing its position in the ransomware ecosystem.

Rhysida

Performance

- **RaaS Platform:** Rhysida is a Ransomware-as-a-Service (RaaS) operation that first emerged in May 2023 and quickly gained notoriety through a series of high-impact double extortion attacks. The group exfiltrates sensitive data and threatens to publish it via its Tor-based leak site if ransom demands are not met, though it notably lacks a full-featured victim support portal common among more mature RaaS operations. Rhysida gained traction by early 2024, targeting organizations across healthcare, education, and government sectors. In February 2024, researchers released a free decryptor that exploited a flaw in the group's encryption process, briefly disrupting its operations. However, Rhysida responded swiftly by updating its tooling and resuming attacks, demonstrating technical agility and resilience. While its exact origins remain unclear, Rhysida's continued activity and ability to recover from setbacks have solidified its presence as a persistent—though now increasingly diminished—player in the ransomware landscape. Recent months have seen reduced activity, suggesting a possible drop in affiliate engagement or strategic pivot, contributing to its fading prominence.

- **Attack Volume:** Rhysida has maintained a steady attack tempo, averaging 3 to 19 victims per month and listing around 140 victims by September 2024, even rebounding quickly after a brief disruption caused by a decryptor release.

- **Ransom Demands:** Specific figures for Rhysida ransomware's average ransom demands remain limited, but available data points suggest mid-to-high six-figure demands. In one confirmed case from November 2023, Rhysida demanded 20 Bitcoin—valued at approximately $740,000 at the time—highlighting the group's targeting of victims with the capacity to pay substantial ransoms.

Rhysida tried to maintain a steady attack tempo, averaging 3 to 19 victims per month and listing around 140 victims by September 2024, but attacks have decreased significantly after a disruption caused by a decryptor release.

Innovation

- **RaaS Platform Development:** Rhysida continues to exhibit a technically capable and adaptive ransomware operation, though its activity has declined in recent months. The group uses Cobalt Strike and similar command-and-control frameworks to manage compromised systems, often deploying PowerShell scripts to deliver ransomware payloads and PSExec for lateral movement. Scheduled tasks are created to maintain persistence across reboots, and Volume Shadow Copies (VSS) are deleted to prevent recovery. Rhysida's encryption scheme combines AES-256 in CTR mode for file encryption with RSA-4096 for secure key management, making recovery without the private key virtually impossible. Initially focused on Windows environments, Rhysida has since expanded its capabilities with a Linux variant targeting VMware ESXi servers, aligning with a broader trend among ransomware groups prioritizing virtual infrastructure. While confirmed exploitation of specific vulnerabilities remains sparse, Rhysida typically gains access via phishing campaigns and exposed or misconfigured remote services. The group's TTPs show considerable overlap with those used by Vice Society, suggesting possible shared tooling or operational links. Despite a temporary disruption in February 2024 following the release of a free decryptor, Rhysida quickly adapted its tooling and resumed activity–demonstrating resilience and operational maturity, though more recently showing signs of diminished momentum.

- **Targeted Industries:** Rhysida continues to primarily target sectors such as healthcare, education, government, and critical infrastructure–focusing on organizations where data sensitivity, regulatory pressure, and operational urgency create strong incentives to pay.
- **Economic Model**: Rhysida continues to operate under a Ransomware-as-a-Service (RaaS) model and employs double extortion tactics–encrypting victim data and exfiltrating sensitive information to pressure victims into paying. The group typically threatens to leak stolen data via its Tor-based leak site if demands are not met. While exact affiliate share percentages have not been publicly confirmed, Rhysida's structured operations suggest an active affiliate model with a competitive payout structure to attract experienced partners. Notably, Rhysida positions itself as a rogue "cybersecurity team," claiming that its attacks are unauthorized "penetration tests" intended to help victims identify security gaps. Ransom demands are framed as "compensation" for these unsolicited services–an attempt to obscure criminal intent and soften the perception of extortion. Despite this narrative, Rhysida's tactics and infrastructure clearly align with traditional financially motivated ransomware operations.

⚠ **CISA Alert:** CISA Alert aa23-319a

8Base

Performance

- **RaaS Platform:** The 8Base ransomware group–originally emerging in March 2022 as a Ransomware-as-a-Service (RaaS) operation–is now considered a diminishing threat following a major law enforcement disruption in early 2025. Known for its aggressive extortion tactics and sophisticated evasion techniques, 8Base had gained prominence for manipulating Windows Defender Firewall settings and other stealth methods to bypass security controls. Despite speculation linking the group to RansomHouse or the leaked Babuk ransomware builder, no definitive technical overlap has been confirmed. Although the group saw a spike in activity during the first half of 2024, the impact of that surge remains loosely documented. In early 2025, coordinated international law enforcement efforts led to the arrest of several key members and the seizure of 8Base's infrastructure, including its negotiation and leak sites. These takedowns effectively crippled the group's operations, resulting in a sharp and sustained decline in activity. Once viewed as a significant player in the data extortion ecosystem, 8Base is now widely regarded as a diminishing presence with little indication of recovery or continued activity.

In early 2025, coordinated international law enforcement efforts led to the arrest of several key 8Base members and the seizure of their infrastructure, including negotiation and leak sites.

- **Attack Volume:** 8Base's attack volume has sharply declined following a major law enforcement disruption in early 2025. After accounting for a significant share of global ransomware activity by mid-2023, the group's operations have effectively ceased, with no recent victim postings or confirmed attacks observed.

- **Ransom Demands:** 8Base ransomware demands typically range from $50,000 to several million dollars, tailored to the size, industry, and perceived ability of the targeted organization to pay.

Innovation

- **RaaS Platform Development:** 8Base ransomware remains technically sophisticated despite its recent operational decline, having employed a range of advanced TTPs during its peak activity. The group operated privately with a small, vetted set of affiliates and deployed customized ransomware payloads–frequently based on Phobos–often delivered via SmokeLoader. Targeting primarily Windows systems, 8Base used strong encryption methods, combining AES-256 for file encryption with RSA-4096 for secure key protection, ensuring fast and irreversible data locking. To gain initial access, 8Base exploited exposed Remote Desktop Protocol (RDP) configurations and leveraged known vulnerabilities in widely used software. Once inside, the group used Mimikatz to harvest credentials and escalate privileges and relied on PsExec and RDP for lateral movement. To evade detection, 8Base disabled security controls by modifying Windows Defender Firewall settings and deleted Volume Shadow Copies (VSS) to block recovery. These TTPs, combined with highly disruptive encryption and stealthy delivery mechanisms, made 8Base a formidable actor during its active period. However, following the law enforcement takedown of its infrastructure in early 2025, these operations have largely ceased, and no new campaigns have been confirmed.

- **Targeted Industries:** 8Base primarily targeted small and medium-sized businesses across diverse industries, including finance, healthcare, manufacturing, and technology. This broad targeting strategy reflected an opportunistic approach.
- **Economic Model**: 8Base operated under a private, closed affiliate model and employed double extortion tactics–exfiltrating sensitive data before deploying ransomware and threatening public leaks to pressure victims into paying. In May 2023, the group expanded to a multi-extortion strategy by launching a Tor-based leak site, allowing them to publish stolen data and amplify extortion pressure. Affiliates were selectively recruited and are believed to have received a majority share of ransom proceeds, though exact percentages were never publicly confirmed. This model fueled a sharp rise in activity through mid-2024, but operations have since collapsed following law enforcement takedowns and infrastructure seizures in early 2025.

Takeaway

Organizations must realize they are in this fight alone and should urgently prioritize both prevention and resilience measures. Organizations must also ensure they are prepared to respond swiftly and effectively when–not if–an attack occurs. The stakes have never been higher, and waiting for systemic intervention is no longer an option.

Developing a comprehensive incident response plan and regularly testing recovery procedures are essential steps to mitigating the potential damage. Here are some of the essential metrics that can assist in bolstering cyber resilience:

Mean Time to Detect (MTTD): MTTD is a critical metric that measures the average time it takes an organization to identify a potential cyber threat or incident. A lower MTTD reflects stronger detection capabilities, indicating that an organization can quickly recognize abnormal activities or indicators of compromise (IoCs). Monitoring MTTD provides insights into the effectiveness of security monitoring systems, such as Security Information and Event Management (SIEM) solutions, and highlights the efficiency of security teams. Reducing MTTD helps contain cyber threats before they can propagate within the organization, thereby limiting the lateral movement of attackers and minimizing the overall damage from a breach. For organizations aiming to enhance their cybersecurity posture, a key objective should be the continuous refinement of tools, processes, and personnel training to lower MTTD, improving real-time detection capabilities.

Mean Time to Respond (MTTR): MTTR measures the average time an organization takes to respond to a detected cyber threat or incident. A lower MTTR reflects the organization's ability to swiftly neutralize or mitigate security threats, reducing potential impacts on business operations. Once an incident is detected, response teams must act quickly to contain the threat, remediate vulnerabilities, and restore affected systems. Efficient response strategies can be developed through regular testing, such as running incident response tabletop exercises and reviewing lessons learned from past events. By analyzing these exercises, organizations can identify areas for improvement and refine their incident response protocols, ultimately enhancing response times and decreasing MTTR.

Incident Response Plan Effectiveness: The incident response plan effectiveness of any organization is determined by how well the plan is executed during an actual cyber event. Key indicators include how quickly the threat is contained, how efficiently internal and external communications are handled, and the level of coordination between security, IT, and leadership teams. Regular assessments of the response plan ensure it remains relevant to the evolving threat landscape, addresses new vulnerabilities, and adapts to organizational changes. If the plan is not followed properly during an incident, it can lead to delays in response, exacerbating the potential impact of the attack. To ensure continuous improvement, organizations should regularly test their plans, update them based on new risks, and measure their effectiveness during real-world scenarios and simulations.

Cybersecurity Training and Awareness: Effective cybersecurity training programs play a pivotal role in reducing the human element in cyber incidents. These programs should be tailored to different roles within the organization, recognizing that the cybersecurity needs of a software developer differ from those of a financial executive. Metrics such as employee completion rates for training modules, performance in simulated phishing exercises, and overall awareness levels should be tracked to measure effectiveness. Training should not be a "one-size-fits-all" solution; instead, it should be designed to address the specific responsibilities and risks associated with each role. A well-designed, role-based training program can significantly enhance the organization's human defense layer, reducing the risk of human error in cyber incidents.

Cybersecurity Hygiene: Cyber hygiene refers to the routine practices that help maintain the security and health of an organization's systems and networks. This includes regular patch management, continuous vulnerability scanning, and adherence to security policies. Proper hygiene is foundational to an organization's cybersecurity resilience, yet many organizations struggle to implement it consistently. Prioritizing cybersecurity hygiene–such as ensuring critical systems are regularly patched and reducing misconfigurations–helps prevent common attack vectors. Organizations should avoid getting distracted by the latest cybersecurity technologies until they have established a robust cyber hygiene framework, which serves as the first line of defense against many types of attacks.

Cyber Risk Exposure: Cyber risk exposure quantifies the organization's potential vulnerability to cyber threats, considering factors such as the criticality of assets, the severity of vulnerabilities, and the likelihood of specific threats materializing. Without a clear understanding of risk exposure, organizations cannot effectively allocate resources to protect their most critical systems and data. Regular risk assessments should identify high-value assets, evaluate the current security posture, and prioritize mitigation strategies based on the most pressing risks. This allows organizations to focus on areas where their cybersecurity investments will have the greatest impact, enhancing their overall resilience to attacks.

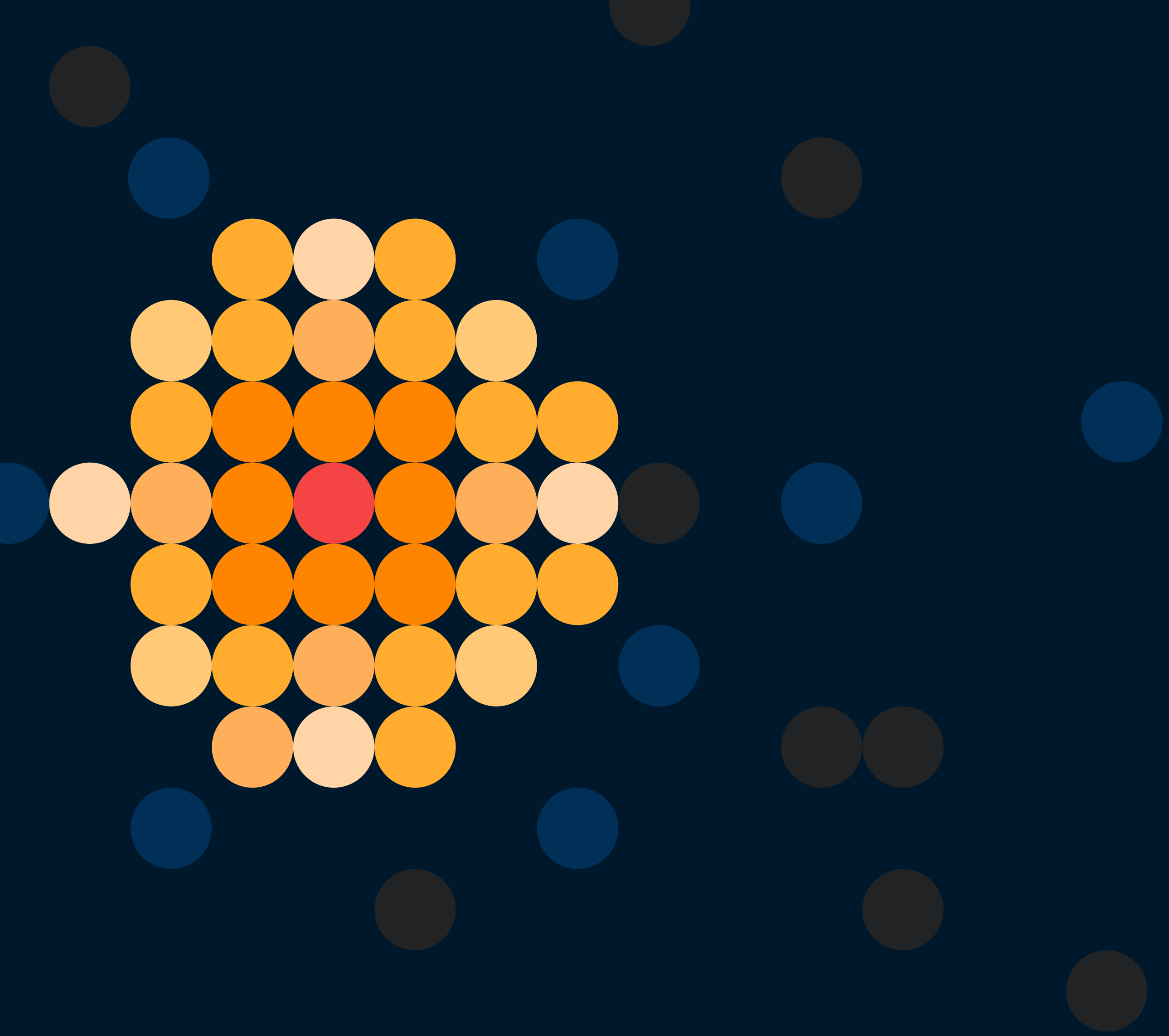
Third-Party Risk Management: In today's interconnected digital environment, managing third-party risk is essential. Organizations often rely on vendors, suppliers, and partners who may introduce additional cyber risks. Tracking third-party risk involves monitoring the number of risk assessments conducted on vendors, their compliance with security requirements, and any security incidents that involve these third parties. A strong third-party risk management program ensures that all external partners follow security best practices, minimizing the chances that vulnerabilities introduced through third-party connections will affect the organization. Continuous monitoring and reassessment of vendor security posture are critical for maintaining a secure ecosystem.

Security Controls Effectiveness: Security controls, such as firewalls, intrusion detection systems (IDS), and malware detection tools, must be regularly assessed for effectiveness. Metrics like the number of alerts from IDS/IPS systems, firewall rule efficacy, and the success rate of malware detection provide valuable insights into whether the controls are adequately protecting the organization. Regularly evaluating the return on investment (ROI) of these controls helps ensure resources are directed toward solutions that provide the most robust protection. Security teams should continuously monitor and adjust their controls based on threat intelligence and the evolving threat landscape to maintain optimal defense capabilities.

Backup and Recovery Metrics: Backup and recovery processes are essential for ensuring that critical data can be restored in the event of an incident. Metrics such as backup success rates, Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO) help organizations assess their ability to recover from cyberattacks, data corruption, or system failures. Regular testing of backup systems is essential to confirm that recovery times align with business continuity expectations. This ensures that, during an actual event, data recovery is quick, complete, and meets the organization's operational requirements.

Business Continuity and Disaster Recovery (BCDR) Metrics: Measuring an organization's business continuity and disaster recovery capabilities is critical for maintaining operations during and after a cyber incident. Metrics such as RTOs, RPOs, and the success of BCDR exercises are essential indicators of readiness. Regular testing ensures that plans are not only theoretically sound but can be executed effectively in real-world scenarios. Ensuring that services remain available, even under adverse conditions, requires comprehensive testing, including worst-case scenario simulations. Disaster recovery planning must also integrate with overall business continuity strategies to ensure seamless operations across all departments during a crisis.

By monitoring and optimizing these critical metrics, organizations can improve their resilience to cyber threats. An effective cybersecurity strategy integrates rapid detection, efficient response, and robust recovery protocols, ensuring the organization can continue to operate and recover swiftly from incidents. Regular testing and updating of plans are essential to maintain preparedness in an ever-changing threat landscape.



The Halcyon Mission: Defeat Ransomware

Halcyon is the only cybersecurity company that eliminates the business impact of ransomware. Modern enterprises rely on Halcyon to prevent ransomware attacks, eradicating cybercriminals' ability to encrypt systems, steal data, and extort companies. Backed by an industry-leading warranty, the Halcyon Anti-Ransomware Platform drastically reduces downtime, enabling organizations to quickly and easily recover from attacks without paying ransoms or relying on backups. For more information on how Halcyon efficiently and effectively defeats ransomware attacks, visit halcyon.ai and schedule a personal demo today with one of our ransomware experts.

halcyon