



Q1-2025 Extortion Attack Group Guide

Power Rankings: Ransomware Malicious Quartile

Table of Contents

Executive Summary	4
Ransomware MQ: Evaluation Criteria Definitions	5
The Q1-2025 Ransomware Malicious Quartile	6
Frontrunners	7
Akira	7
RansomHub.	8
Lynx.	10
ClOp.	11
INC Ransom	13
Qilin.	14
Medusa	15
SafePay	17
BlackBasta	18
8Base.	19
Play	21
LockBit.	22
Contenders	25
Fog	25
BianLian	26
Hunters International	27
Rhysida.	29
Meow.	30
KillSec	31
Emerging	33
Sarcoma.	33
DragonForce.	34
Cloak	35
Ghost.	37
Arcus Media	38
Diminishing	40
BlackSuit	40
Cactus	41
El Dorado	43
RAWorld.	44
Halcyon Threat Insights	46
Takeaway	49
The Halcyon Mission: Defeat Ransomware	52

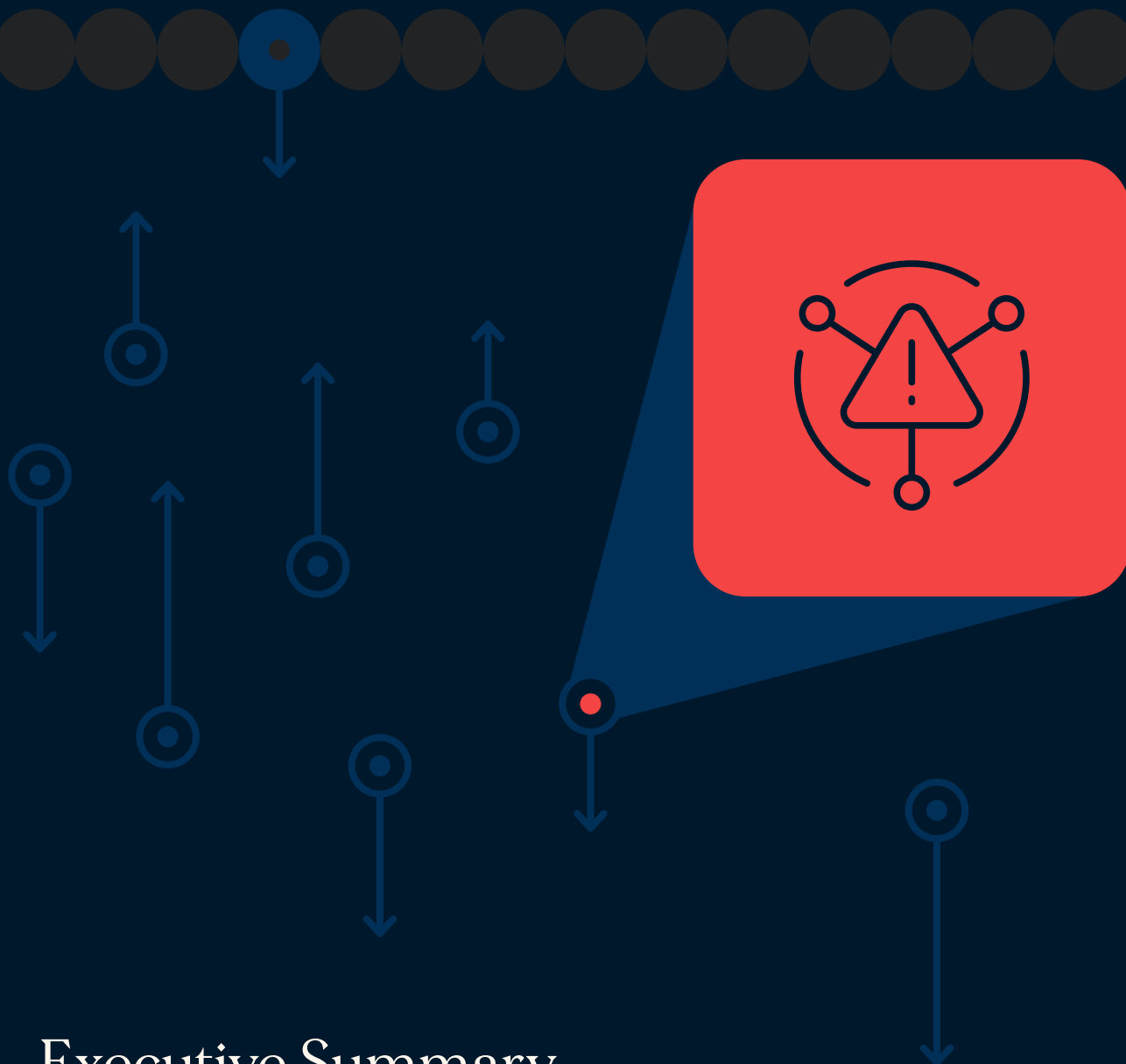


Ransomware has evolved

beyond being a tool for financial gain. For adversarial nations, it serves as a low-cost, high-impact mechanism to disrupt targets while avoiding direct confrontation. Recognizing and addressing this reality is a crucial step in protecting critical systems and ensuring national security in an era of increasingly complex threats.

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 Q1-2025, which can be reviewed along with earlier reports here:

[Power Rankings: Ransomware Malicious Quartile.](#)



Executive Summary

- **Akira** moved to the top spot in Leaders Quartile for attack volume, advanced TTPs.
- **CIOp** moved back into Leaders Quartile based on Cleo exploitation campaign.
- **Lynx and SafePay** were added to Leaders Quartile for attack volume and platform evolution.
- **BlackBasta, 8Base, Play, LockBit** are still in Leaders Quartile but diminished.
- **Hunters International** dropped out of Leaders Quartile to Contenders Quartile.
- **Arcus Media** was added to Emerging Quartile.
- **Fog** moved into Contenders Quartile as operation ramp up.
- **BlackSuit, El Dorado, RAWorld** moved to Diminishing Quartile as operations dwindle.
- **RansomHouse, DarkVault** were removed from report.



Ransomware MQ: Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q1-2025 Ransomware Malicious Quartile. All attack groups evaluated must be a known threat actor group in 2025 with verifiable victims who demanded a ransom payment. Click on the threat actor group name below to see a listing of recent attacks they conducted including targets, industry verticals and other details.

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 Q1-2025 Ransomware Malicious Quartile

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



Source: Halcyon (Q1 2025)

Frontrunners

Akira

Performance


- **RaaS Platform:** The combination of technical advancement and attack volume has put Akira at the top of the ransomware threat actor rankings. Akira emerged in March 2023, and although suspected to be linked to the defunct Conti gang—especially after Conti's code leak in 2022—no definitive connection has been confirmed. After a period focused solely on data theft, Akira resumed encrypting victims' files alongside exfiltration, reviving its double-extortion model. Its extortion platform features a built-in chat function, allowing direct negotiations between victims and attackers—an uncommon tactic. In some cases, Akira has even disclosed infection vectors to ransom-paying victims, deviating from the typical strategy of exploiting the same vulnerabilities repeatedly. While a decrypter was released that worked on earlier or less common Akira samples, it has proven largely ineffective for full recovery. In March 2025, researchers developed a method to decrypt certain Linux-based variants by brute-forcing encryption keys with GPUs. However, publicizing the technique risks prompting Akira to patch the vulnerabilities, potentially eliminating that recovery option.
- **Attack Volume:** As of April 2024, Akira ransomware had amassed approximately \$42 million in ransom payments from over 250 attacks. By November 2024, the group had a surge in activity, publishing data from 35 new victims on its darknet leak site in a single day.
- **Ransom Demands:** Akira ransomware's ransom demands vary significantly, typically ranging from \$200,000 to over \$4 million, depending on the victim's size and sector.

Innovation

- **RaaS Platform Development:** Akira initially developed a Rust-based ransomware variant to target VMware ESXi servers but has since reverted to C++ for both Windows and Linux encryptors. The group typically gains initial access by exploiting VPN credentials and employs advanced attack techniques. Akira ransomware uses PowerShell to delete Windows Shadow Volume Copies, preventing restoration of encrypted data. Akira targets a broad range of file types but avoids critical system files—such as those



In March 2025, Akira was observed leveraging an unsecured webcam to launch an attack on a victim network, circumventing EDR.



with.exe,.dll,.sys,.msi, and.lnk extensions—to maintain system stability and evade detection. They use tools like Mimikatz to extract credentials, disable endpoint detection and response (EDR) software, and perform privilege escalation. In March 2025, Akira was observed leveraging an unsecured webcam to launch an attack on a victim network, circumventing EDR.

Akira affiliates also rely on tools like SoftPerfect network scanner for reconnaissance and use PsExec and Remote Desktop Protocol (RDP) for lateral movement. To further obscure their activities, they utilize Living-off-the-Land Binaries (LOLBins) and commercial off-the-shelf (COTS) tools like PCHunter64. In July 2023, Akira expanded operations by introducing a Linux variant. By August 2023, they were exploiting Cisco VPN zero-day vulnerabilities (CVE-2020-3259 and CVE-2023-20269), and by late 2024, they began exploiting a SonicWall vulnerability (CVE-2024-40766) as well as VMware ESXi flaws to move laterally within compromised networks.

- **Targeted Industries:** Akira's primary focus has been on entities in North America, Europe, and Australia. Notably, the group has attacked sectors including education, finance, manufacturing, and others.
- **Economic Model:** Akira continues to use a double extortion strategy, combining data encryption with data exfiltration. Victims are threatened not only with data loss but also with the public release or sale of stolen information if ransoms go unpaid. The group has leaked large volumes of sensitive data from numerous victims on its leak site, increasing pressure on organizations to meet their demands.

 **CISA Alert:** [CISA Alert aa24-109a](#)

RansomHub

Performance

- **RaaS Platform:** RansomHub, a RaaS platform that emerged in early 2024, has swiftly garnered attention for its high-impact attacks and advanced ransomware deployment techniques. Initially suspected of having connections to LockBit due to similarities in operational style, closer examination reveals that its code bears a strong resemblance to that of the now-defunct Knight group. The platform has distinguished itself by offering affiliates up to 90% of ransom payments, making it highly attractive to potential partners. RansomHub enforces stringent policies within its affiliate network, mandating that affiliates adhere to agreements made with



Once inside, RansomHub deploys tools like Mimikatz for credential harvesting, Angry IP Scanner and Nmap for reconnaissance, and PsExec and RDP for lateral movement.



victims during negotiations. Failure to comply with these agreements can result in permanent bans from the platform. This strict policy underscores RansomHub's commitment to maintaining a structured and reliable operational model, even as it continues to develop its reputation in the ransomware landscape.

- **Attack Volume:** By Q4-2024, RansomHub was the most prolific of the RaaS groups with over 600 confirmed victims, but activity decreased significantly in early 2025.
- **Ransom Demands:** RansomHub's average ransom demands is around \$2.79 million, but that amount likely varies based on the victim's sector and size.

Innovation

- **RaaS Platform Development:** RansomHub targets both Windows and Linux systems, including VMware ESXi servers, and leverages unpatched vulnerabilities such as Citrix NetScaler ADC and Gateway (CVE-2023-3519), Fortinet SSL-VPN (CVE-2023-27997), and Microsoft Netlogon (CVE-2020-1472), also known as ZeroLogon. They also use brute-force attacks on Remote Desktop Protocol (RDP) and VPNs to gain access. Once inside, RansomHub deploys tools like Mimikatz for credential harvesting, Angry IP Scanner and Nmap for reconnaissance, and PsExec and RDP for lateral movement. To avoid detection, they may use EDRKillShifter to disable endpoint defenses. RansomHub encrypts data using Curve25519, ChaCha20, and AES, and deletes volume shadow copies and backups to block recovery. The group also practices double extortion by exfiltrating data and threatening to leak it if the ransom is not paid.
- **Targeted Industries:** RansomHub targets a broad range of industries, including healthcare, manufacturing, professional services, financial services, high technology, and public sector organizations. Their victims vary in size and sector, reflecting an opportunistic strategy focused on exploiting vulnerable, high-value targets regardless of industry.
- **Economic Model:** RansomHub uses double extortion tactics—encrypting victims' data while also exfiltrating sensitive information. If ransom demands go unmet, they threaten to leak the stolen data, adding pressure to force payment. The group offers affiliates up to 90% of ransom proceeds, a high commission that has attracted experienced operators, including former affiliates from groups like BlackCat/ALPHV. These aggressive recruitment efforts, combined with ongoing development, reflect RansomHub's clear focus on growth and long-term sustainability in the ransomware landscape.

 **CISA Alert:** [CISA Alert aa24-242a](#)

Lynx

Performance

- **RaaS Platform:** Lynx ransomware emerged in July 2024, focusing its attacks on the manufacturing and construction sectors. Although the group claims to avoid targeting government, healthcare, and non-profit organizations, its attacks consistently disrupt high-impact industries. Lynx targets Windows environments, encrypting files with the.lynx extension and deleting shadow copies to prevent recovery. While its initial access methods are not well documented, the group is believed to rely on phishing emails and malicious downloads—common techniques used to gain entry into networks.
- **Attack Volume:** Lynx has shown a steady increase in attack volume since its emergence in July 2024, with 96 confirmed victims listed on its data leak site as of Q1-2025.
- **Ransom Demands:** Lynx ransomware's ransom demands remain largely undocumented, but one reported case involved a demand of \$18.1 million following the theft of 30GB of sensitive data. While the average ransomware demand across groups is around \$600,000, Lynx appears to scale its demands based on the size of the target and the data's value.

Innovation

- **RaaS Platform Development:** Unlike typical Ransomware-as-a-Service (RaaS) platforms, Lynx operates as a closed group, with activity carried out by a core team rather than a network of affiliates. Lynx ransomware is specifically designed for Windows environments and shares significant code similarities with INC ransomware, which was written in C++, though its exact programming language has not been explicitly confirmed. It features a range of command-line options that allow attackers to specify target files or directories, terminate processes, encrypt network shares, and adjust system settings. To secure data, Lynx uses advanced encryption techniques, combining AES-128 in CTR mode with Curve25519 Donna algorithms. It also terminates processes and services that could disrupt encryption, leveraging the Windows Service Control Manager and Restart Manager API to handle active files. To block recovery efforts, Lynx deletes or resizes Volume Shadow Copies, effectively disabling standard backup mechanisms.
- **Targeted Industries:** The group has primarily targeted organizations in the United States, with a strong focus on the manufacturing and construction sectors.



Lynx ransomware's ransom demands remain largely undocumented, but one reported case involved a demand of \$18.1 million following the theft of 30GB of sensitive data.

- **Economic Model:** Lynx employs both single and double extortion techniques, encrypting victims' files while also exfiltrating sensitive data to enhance their leverage. Victims who refuse to pay the ransom are listed on Lynx's TOR-hosted leak site, where the stolen data is publicly disclosed, increasing pressure on the affected organizations.

CIOp

Performance

- **RaaS Platform:** First observed in 2019, CIOp is a Ransomware-as-a-Service (RaaS) operation known for its advanced anti-analysis and anti-virtual machine detection capabilities, which help it evade sandbox-based investigations. The group rose to prominence in Q2 2023, becoming the most active ransomware actor during that period by automating the exploitation of file transfer vulnerabilities, including MOVEit Transfer (CVE-2023-34362) and GoAnywhere MFT (CVE-2023-0669). CIOp's large-scale exploitation of the MOVEit flaw alone accounted for roughly 21% of all ransomware incidents in July 2023, contributing to a major global spike in ransomware activity. While the group initially shifted toward data-theft-only extortion tactics in early 2023, it later returned to deploying file-encrypting malware, signaling a renewed embrace of traditional ransomware methods. After a period of limited visibility, CIOp resurfaced in late 2024 and early 2025 through the exploitation of Cleo Integration Cloud vulnerabilities (CVE-2024-50623 and CVE-2024-55956).
- **Attack Volume:** CIOp's attack volume has varied over time, with major spikes linked to mass exploitation campaigns. After peaking in mid-2023 through the MOVEit vulnerability, the group resurfaced in late 2024 and early 2025 by targeting Cleo Integration Cloud, fueling a sharp rise in ransomware activity.
- **Ransom Demands:** CIOp's ransom demands have varied over time, influenced by their targeted attack strategies. In Q2 2023, the group's average ransom demand reached approximately \$2.51 million, contributing to an overall increase in ransomware severity during that period. Additionally, mid-year data from 2023 indicated that CIOp achieved an average payout of \$1,730,486 per victim, underscoring the financial impact of their operations.



After a period of limited visibility, CIOp resurfaced in late 2024 and early 2025 through the exploitation of Cleo Integration Cloud vulnerabilities (CVE-2024-50623 and CVE-2024-55956).



Innovation

- **RaaS Platform Development:** CIOp operates a RaaS and developed a Linux variant of its ransomware in late 2022, expanding its reach beyond Windows environments. Its Windows variant, written in C++, uses RC4 for file encryption and secures keys with RSA 1024-bit encryption. In early 2023, CIOp exploited a vulnerability in Fortra's GoAnywhere MFT (CVE-2023-0669), followed by a major campaign in May 2023 targeting Progress Software's MOVEit Transfer (CVE-2023-34362). This SQL injection flaw enabled mass data theft without encryption, marking a shift to pure extortion tactics. CIOp's MOVEit campaign alone accounted for roughly 21% of ransomware incidents in July 2023. After a quieter period, CIOp resurged in late 2024 by exploiting two zero-day vulnerabilities in Cleo Integration Cloud: CVE-2024-50623, disclosed in October, allowed unauthorized file uploads and downloads; CVE-2024-55956, identified in December, enabled broader unauthorized access. These campaigns highlight CIOp's ongoing ability to adapt its tactics—shifting between encryption and data theft—to exploit vulnerabilities in high-value enterprise systems.
- **Targeted Industries:** CIOp primarily targets large organizations across industries such as finance, healthcare, education, government, and critical infrastructure. The group focuses on high-value victims, often exploiting vulnerabilities in widely used file transfer systems to breach enterprise networks and steal sensitive data.
- **Economic Model:** CIOp's economic strategy centers on large-scale, high-impact breaches, often exploiting file transfer software to steal sensitive data and pressure victims into paying substantial ransoms. While CIOp primarily employs double extortion—combining system encryption with data theft—it has increasingly emphasized data-centric extortion in high-profile campaigns, though full triple extortion methods, such as DDoS attacks, are not consistently used.

 **CISA Alert:** [CISA Alert aa23-158a](#)

INC Ransom

Performance

- **RaaS Platform:** INC Ransom emerged in mid-2023 and has since become an active ransomware threat actor. It remains unclear whether the group operates as a Ransomware-as-a-Service (RaaS) platform with affiliates or functions as a closed internal operation. INC Ransom employs a variety of established tactics, techniques, and procedures, including the use of compromised Remote Desktop Protocol (RDP) credentials for initial access and lateral movement. Initial infections have also been linked to phishing campaigns and the exploitation of known vulnerabilities, such as CVE-2023-3519 in Citrix NetScaler systems. The group demonstrates technical capability in penetrating networks and executing ransomware attacks, often paired with data exfiltration. Uniquely, INC Ransom portrays itself as a "moral agent," claiming its actions serve to reveal cybersecurity weaknesses in victim organizations
- **Attack Volume:** INC Ransom has steadily increased its attack volume since emerging in mid-2023, with a noticeable rise in incidents through late 2023 and early 2024.
- **Ransom Demands:** While exact figures for INC Ransom are unavailable, industry data suggests average ransom demands in 2024 exceeded \$5.2 million, though actual amounts likely vary based on the victim's size and sector.

Innovation

- **RaaS Development:** INC Ransom's structure remains unclear, with no confirmed evidence of a broad affiliate model, suggesting it may operate as a closed internal team. The group uses a wide range of techniques, relying on administrative tools and Living-off-the-Land (LOTL) methods to evade detection, and tools like WMIC, PsExec, and PowerShell are used to deploy ransomware, while applications such as MSPaint and Windows Explorer aid lateral movement. TightVNC and AnyDesk support remote access, and data exfiltration is carried out via MegaSync. The ransomware is written in C++ and uses AES-128 in CTR mode; a Linux variant has also been observed. INC Ransom likely deletes Volume Shadow Copies to hinder recovery. The group's malware has been used by actors like Vanilla Tempest in attacks on U.S. healthcare organizations, with access gained through Gootloader. INC Ransom presents itself as a "moral agent," claiming to expose cybersecurity flaws, though its methods reflect a sophisticated and harmful operation.



INC Ransom's structure remains unclear, with no confirmed evidence of a broad affiliate model, suggesting it may operate as a closed internal team.

- **Targeted Industries:** The group has primarily targeted organizations in North America and Europe, with a focus on sectors such as healthcare, education, and government.
- **Economic Model:** The group employs double extortion tactics by both encrypting victims' data and exfiltrating sensitive information. They operate a leak site where they threaten to publish this data if ransom demands are not met and have followed through on these threats by exposing compromised data when targets refuse to pay.

Qilin

Performance

- **RaaS Platform:** Qilin ransomware, originally known as Agenda, rebranded as a Ransomware-as-a-Service (RaaS) operation in July 2022. Written in both Golang and Rust, Qilin is capable of targeting multiple platforms, including Windows and Linux systems. The use of Rust, known for its security and concurrency performance, enhances Qilin's ability to evade detection and develop cross-platform variants efficiently. Qilin affiliates commonly gain initial access through compromised Remote Desktop Protocol (RDP) credentials, a tactic frequently observed in their campaigns. In the summer of 2024, the group expanded its capabilities by deploying scripts designed to extract credentials stored in Google Chrome browsers across compromised networks. This added credential harvesting functionality highlights the group's ongoing development and adaptation, reinforcing its position as a technically capable and evolving ransomware threat.
- **Attack Volume:** Qilin ransomware has steadily increased its attack volume since mid-2022, with a noticeable surge throughout 2024. By early 2025, the group ranked among the most active ransomware operations, regularly posting new victims to its leak site across various sectors.
- **Ransom Demands:** Qilin's ransom demands typically range from \$50,000 to \$800,000, though in some cases they have issued demands as high as \$50 million. This wide range indicates that Qilin tailors its extortion amounts based on the size of the organization and its perceived ability to pay.

Innovation

- **RaaS Platform Development:** Qilin ransomware, originally known as Agenda, introduced an upgraded variant called Qilin.B in fall 2024, as reported by Halcyon researchers. Written in Rust, Qilin.B incorporates advanced



The use of Rust, known for its security and concurrency performance, enhances Qilin's ability to evade detection and develop cross-platform variants efficiently.



encryption methods, using AES-256-CTR for systems with AESNI capabilities and ChaCha20 for others, while securing encryption keys with RSA-4096 and OAEP padding—making decryption without the private key virtually impossible. The variant terminates security-related services, clears Windows Event Logs to obstruct forensic analysis, and deletes itself post-execution to reduce detection and hinder reverse engineering. Qilin.B also deletes Volume Shadow Copies (VSS) to disrupt system backups and block recovery efforts. The Qilin RaaS platform offers flexibility in encryption configuration, supporting AES-256, ChaCha20, and RSA-4096. Its Linux variant was compiled using GCC and leveraging OpenSSL, targets VMware ESXi environments, allowing efficient attacks against virtualized infrastructures. Affiliates have been observed using PowerShell scripts to harvest credentials from Chrome browsers and exploiting known vulnerabilities in software like Fortinet devices and Veeam Backup & Replication. These updates reflect Qilin's growing sophistication, cross-platform capabilities, and strategic use of credential theft and vulnerability exploitation to infiltrate and disrupt enterprise networks.

- **Targeted Industries:** Qilin ransomware targets a wide range of industries, including critical infrastructure, healthcare, education, manufacturing, and government, focusing on mid- to large-sized organizations and exploiting vulnerabilities in widely used IT systems for initial access.
- **Economic Model:** Qilin provides affiliates with customizable ransomware tools in exchange for a share of the ransom payments. Affiliates reportedly receive 80% of payments under \$3 million and 85% for payments exceeding that amount.


Medusa

Performance

- **RaaS Platform:** Medusa, a RaaS platform that emerged in the summer of 2021, quickly became one of the most active and formidable ransomware groups. By the second quarter of 2024, its attack volume had surged, solidifying its place among the top ransomware threats. The group has targeted vulnerabilities like CVE-2023-48788 in Fortinet's FortiClient EMS software and uses a variety of sophisticated techniques to evade detection and complicate recovery efforts. Medusa often restarts infected machines in safe mode to bypass security software and takes steps to prevent data recovery, such as deleting local backups, disabling startup recovery options, and wiping Volume Shadow Copies (VSS).



Medusa operates a RaaS and typically gains initial access to victim networks through methods such as brute-forcing Remote Desktop Protocol (RDP) credentials, exploiting vulnerabilities, or distributing malware via phishing emails and torrents.

- 
- **Attack Volume:** Medusa's attack volume has steadily increased since its emergence in 2021, with a significant surge by Q2 2024, making it one of the most active ransomware groups. By Q1 2025, the group's activity remained high.
 - **Ransom Demands:** Ransom demands from Medusa have varied widely, ranging from \$100,000 to as high as \$15 million, depending on factors such as the size and nature of the targeted organization.

Innovation

- **RaaS Platform Development:** Medusa operates a RaaS and typically gains initial access to victim networks through methods such as brute-forcing Remote Desktop Protocol (RDP) credentials, exploiting vulnerabilities, or distributing malware via phishing emails and torrents. Once inside, it can terminate over 200 Windows services and processes without command-line arguments, utilizing legitimate system tools like PowerShell and RDP for malicious actions, making detection difficult. Medusa uses AES-256 encryption for files and RSA public key encryption for added security, with custom malware like "gaze.exe" deployed to maintain persistence. The ransomware employs credential-harvesting tools like Mimikatz and uses Netscan for network reconnaissance. To prevent recovery, Medusa deletes local backups, disables startup recovery, and wipes Volume Shadow Copies (VSS). In September 2024, Medusa released an updated variant that accelerated encryption speeds and enhanced backup deletion capabilities, further complicating recovery efforts.
- **Targeted Industries:** Medusa employs a strategic approach in selecting high-value targets across various industries to maximize ransom payouts. The group focuses on sectors such as healthcare, pharmaceuticals, and public sector organizations, while targeting a range of other industry verticals.
- **Economic Model:** Medusa primarily targets industries such as healthcare, education, legal, insurance, technology, and manufacturing, focusing on organizations with critical operations. The group has been observed attacking both private and public sector entities, particularly those with high-value data or vulnerabilities in widely used software.

SafePay

Performance

- **RaaS Platform:** SafePay is a Ransomware-as-a-Service (RaaS) group that emerged in November 2024, quickly establishing itself as a significant player in the ransomware landscape. SafePay exhibits unique characteristics that differentiate it from existing ransomware families. While it does not appear to be a direct rebranding of a prior group, analyses suggest that SafePay's operators have incorporated leaked source code from other notorious ransomware families, such as LockBit.
- **Attack Volume:** SafePay has claimed responsibility for multiple attacks in a short period, and it is assessed the group may become a major player in the space.
- **Ransom Demands:** Specific details regarding SafePay's average ransom demands are not publicly disclosed. However, the group employs a double extortion model, combining data encryption with threats to release stolen information unless a ransom is paid.

Innovation

- **RaaS Platform Development:** The SafePay RaaS platform, built on a variant of LockBit from late 2022, demonstrates a high level of sophistication and adaptability. It employs a range of tactics, techniques, and procedures (TTPs), including exploiting known vulnerabilities in widely used software to gain access to victim networks. SafePay encrypts files with the ".safepay" extension and uses ransom notes titled "readme_safepay.txt." The group maintains a strong dark web presence, including a Tor leak site and a site on "The Open Network" (TON) for victim listings and communication. Their toolset includes malware for credential harvesting, such as Mimikatz, and the use of legitimate remote management tools to maintain persistence within compromised networks. SafePay also utilizes double extortion, encrypting data and exfiltrating sensitive information, which they threaten to leak unless a ransom is paid. This combination of encryption, data exfiltration, and persistence tactics allows SafePay to maximize disruption and compel victims to meet their ransom demands.
- **Targeted Industries:** SafePay has targeted organizations across various sectors, including education, technology, healthcare, and transportation.



The SafePay RaaS platform, built on a variant of LockBit from late 2022, demonstrates a high level of sophistication and adaptability.

- **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.

BlackBasta

Performance

- **RaaS Platform:** BlackBasta is a Ransomware-as-a-Service (RaaS) group that emerged in April 2022, quickly establishing itself as one of the most active and formidable players in the ransomware landscape. Although some cybersecurity researchers speculate that BlackBasta may be an offshoot of the disbanded Conti group, there is no definitive proof confirming this connection. The group operates with a high level of sophistication, leveraging a platform based on a variant of LockBit ransomware from late 2022.
- **Attack Volume:** Since its emergence, BlackBasta has seen a significant increase in attack volume, quickly establishing itself as one of the most active ransomware groups. By 2024, the group's activity had surged, with numerous high-profile attacks across various sectors
- **Ransom Demands:** Ransom demands from BlackBasta vary based on the targeted organization, with some reports indicating amounts as high as \$9 million. It is estimated that around 35% of victims pay the ransom, allowing the group to amass over \$107 million in revenue from more than 500 victims in less than two years.

Innovation

- **RaaS Platform Development:** BlackBasta targets both Windows and Linux systems, with particular expertise in exploiting vulnerabilities in enterprise platforms like VMware ESXi. Their ransomware, written in C++, employs ChaCha20 encryption for file encryption and RSA-4096 to encrypt the encryption key, ensuring fast and robust encryption across affected systems. The group utilizes a variety of advanced tactics, techniques, and procedures (TTPs), including exploiting vulnerabilities such as PrintNightmare and leveraging insecure Remote Desktop Protocol (RDP) configurations for initial access. They have also been observed deploying malware strains like Qakbot for credential theft and SystemBC for maintaining persistent access within victim networks. To make detection and mitigation more difficult,



To make detection and mitigation more difficult, BlackBasta disables security tools like Windows Defender using PowerShell commands, batch files, and Group Policy Objects (GPOs) to turn off anti-malware solutions.



BlackBasta disables security tools like Windows Defender using PowerShell commands, batch files, and Group Policy Objects (GPOs) to turn off anti-malware solutions. For lateral movement within compromised networks, they use Cobalt Strike, a widely known tool for post-exploitation. This combination of targeted vulnerability exploitation, custom tooling, and evasion techniques makes BlackBasta a formidable and persistent threat.

- **Targeted Industries:** BlackBasta primarily targets high-value industries such as healthcare, finance, manufacturing, and retail, often focusing on organizations with critical data and large operational footprints. The group has been responsible for attacks on both public and private sector entities worldwide.
- **Economic Model:** Their attacks often involve double extortion, encrypting victim data and threatening to release stolen information unless a ransom is paid. BlackBasta is also known for its meticulous approach to affiliate recruitment, working with a carefully selected group of attackers to execute highly targeted operations.

⚠ **CISA Alert:** [CISA Alert aa24-131a](#)


8Base

Performance

- **RaaS Platform:** The 8Base ransomware group, a Ransomware-as-a-Service (RaaS) operation, emerged in March 2022 and quickly gained attention within the cyber threat landscape. While its surge in activity during the first half of 2024 has not been widely confirmed, the group's tactics and methods have made it a significant player. There has been speculation linking 8Base to other data extortion groups such as RansomHouse, and possible connections to the leaked Babuk ransomware builder, but these claims have not been substantiated by concrete evidence. 8Base is known for its advanced evasion techniques, including modifying Windows Defender Firewall settings to bypass detection, demonstrating the group's deep understanding of both ransomware operations and security evasion strategies. In early 2025, international law enforcement disrupted the group's operations, leading to the arrest of several key members and the seizure of their servers. This action resulted in the shutdown of 8Base's negotiation and data leak sites, effectively crippling the group's activities.



There has been speculation linking 8Base to other data extortion groups such as RansomHouse, and possible connections to the leaked Babuk ransomware builder, but these claims have not been substantiated by concrete evidence.

- 
- **Attack Volume:** By mid-2023, 8Base was responsible for a large portion of ransomware attacks, continuing to escalate its operations and targeting a wide range of industries, before being disrupted by law enforcement in early 2025.
 - **Ransom Demands:** 8Base ransomware typically demands ransoms ranging from \$50,000 to several million dollars, depending on the size and nature of the targeted organization.

Innovation

- **RaaS Platform Development:** 8Base is a ransomware group that operates privately with a select group of vetted affiliates, using customized ransomware payloads such as Phobos, often delivered via SmokeLoader. The group primarily targets Windows systems and employs advanced tactics, techniques, and procedures (TTPs) to evade detection. 8Base bypasses security measures by modifying Windows Defender Firewall settings and erases Volume Shadow Copies (VSS) to obstruct recovery efforts. The group uses AES-256 encryption to lock files and RSA-4096 for key protection, ensuring robust and rapid encryption. 8Base also leverages tools like Mimikatz for credential harvesting, enabling privilege escalation within compromised networks, and PsExec and Remote Desktop Protocol (RDP) for lateral movement. Additionally, 8Base exploits known vulnerabilities, including insecure RDP configurations and specific flaws in widely used software, to gain initial access. By combining strong encryption, effective evasion strategies, and targeted exploits, 8Base maximizes the disruption of its victims' operations while ensuring that data recovery becomes extremely difficult.
- **Targeted Industries:** 8Base primarily targets small and medium-sized businesses across a wide range of industries, including finance, healthcare, manufacturing, and technology.
- **Economic Model:** 8Base employs double extortion tactics, exfiltrating sensitive data before deploying ransomware and threatening to release it if ransom demands are not met. In May 2023, they transitioned to a multi-extortion model, establishing a Tor-based leak site to publish stolen data and significantly increasing their operations.

Play

Performance

- **RaaS Platform:** Play ransomware, a Ransomware-as-a-Service (RaaS) group, first emerged in June 2022 and quickly gained prominence due to its technical proficiency and evolving tactics. By the second quarter of 2024, Play had solidified its position as one of the most active and innovative groups in the ransomware landscape. The group frequently exploits unpatched vulnerabilities, including those in Fortinet SSL VPNs and Microsoft Exchange (e.g., ProxyNotShell, OWASSRF), to gain initial access to networks. Play's operations bear similarities to defunct groups like Hive and Nokoyawa, employing sophisticated techniques for evasion and data exfiltration. In early 2024, the FBI and CISA issued a joint advisory highlighting the group's significant impact, revealing that it had compromised over 300 organizations since its inception.
- **Attack Volume:** Since its emergence in June 2022, Play ransomware has rapidly increased its attack volume, exploiting critical vulnerabilities and compromising over 300 organizations by mid-2024, solidifying its position as a prominent threat.
- **Ransom Demands:** Play ransomware typically demands ransoms ranging from \$100,000 to several million dollars, depending on the size and perceived value of the targeted organization. The group tailors its ransom demands based on the victim's ability to pay.

Innovation

- **RaaS Platform Development:** Play is a continuously evolving Ransomware-as-a-Service (RaaS) group known for its sophisticated use of tools to disable security defenses and maintain persistence. The group utilizes PowerTool to disable antivirus and security monitoring solutions, while employing SystemBC RAT for persistence. Play also uses legitimate software like Plink and AnyDesk to stay active in compromised systems. For lateral movement, they rely on Cobalt Strike, and for credential harvesting, they use Mimikatz. Play exploits vulnerabilities in FortiOS and Microsoft Exchange (e.g., ProxyNotShell and OWASSRF) to gain initial access. To bypass defenses, Play frequently uses tools like Process Hacker, GMER, and IOBit, and disables Windows Defender via PowerShell or command scripts. They introduced intermittent encryption techniques, encrypting files in segments to evade detection. Play also developed custom exfiltration tools, including the Grixba information stealer and a Volume Shadow Copy Service (VSS) copying tool.



Play's operations bear similarities to defunct groups like Hive and Nokoyawa, employing sophisticated techniques for evasion and data exfiltration.



to steal data before encryption. The group employs AES-256 encryption, often paired with RSA-4096 for key protection, ensuring data is locked down quickly and efficiently. Play's innovative TTPs and commitment to R&D make it a formidable threat in the ransomware ecosystem.

- **Targeted Industries:** Play ransomware primarily targets high-value industries, including healthcare, finance, manufacturing, and technology, with a particular focus on organizations with critical data and large operational footprints. The group has been responsible for compromising both public and private sector entities.
- **Economic Model:** Play recruits skilled affiliates and provides technical support to ensure successful attacks. Using double extortion tactics, Play encrypts data and exfiltrates sensitive information, threatening to release it on a public leak site if ransom demands are not met. This two-pronged approach—encryption and data theft—adds reputational damage and regulatory penalties for victims, making Play a highly lucrative and formidable ransomware operation. Play's structured model and investment in innovation contribute to its growing prominence in the cybercriminal landscape.

⚠️ **CISA Alert:** [CISA Alert aa23-352a](#)

LockBit

Performance

- **RaaS Platform:** LockBit, a prominent Ransomware-as-a-Service (RaaS) platform, has been active since 2019 and is known for its sophisticated evasion techniques and rapid encryption speed. The group utilizes a multi-extortion strategy, often demanding separate ransoms for decrypting files and for any sensitive data they exfiltrate. LockBit employs a mix of publicly available file-sharing services and its proprietary tool, Stealbit, for data exfiltration. In February 2024, LockBit's operations were disrupted by Operation Cronos, an international law enforcement effort that temporarily took control of the group's administrative infrastructure, though they resumed activity within days. Despite ongoing law enforcement actions, LockBit remains operational and has continued evolving, with LockBit 4.0 expected to launch in February 2025. In December 2024, Rostislav Panev, a dual Russian-Israeli national and alleged LockBit developer, was charged by the U.S. Department of Justice. There are suspicions that LockBit may overstate its involvement in high-profile attacks, such as the alleged



In early 2025, LockBit announced it would release LockBit 4.0 in February, and the new version introduced even more advanced features to further solidify their position in the ransomware landscape.




breach of the U.S. Federal Reserve, to maintain its reputation and influence among affiliates. However, the group remains one of the most active and sophisticated ransomware operators in the cybercriminal landscape.

- **Attack Volume:** By 2023, LockBit was one of the top ransomware operators, responsible for a significant percentage of global attacks, particularly targeting large enterprises. The group's activity surged in 2024, with hundreds of new victims, despite disruptions like the Operation Cronos takedown. LockBit's continued evolution, including the upcoming LockBit 4.0 release, signals its sustained growth and persistence in the ransomware landscape.
- **Ransom Demands:** LockBit's ransom demands typically range from \$100,000 to several million dollars, depending on the size and value of the targeted organization. The group tailors its ransom requests based on the victim's ability to pay.

Innovation

- **RaaS Platform Development:** LockBit is a highly active Ransomware-as-a-Service (RaaS) group known for continuously refining its tools and tactics. After releasing LockBit 3.0 in June 2022, the group expanded its capabilities with a macOS variant in April 2023, showcasing its technical sophistication. LockBit 3.0 utilizes advanced anti-analysis features, supports attacks on Windows and Linux systems, and employs a modular design that allows affiliates to tailor execution modes. The ransomware uses a custom Salsa20 algorithm for encryption and often exploits Remote Desktop Protocol (RDP) for initial access. Once inside, LockBit spreads using Group Policy Objects and PsExec over SMB. The group has exploited vulnerabilities such as CVE-2023-4966 (Citrix Bleed) to bypass security measures like multi-factor authentication. Despite the introduction of LockBit 3.0, the group continues supporting its LockBit 2.0 variant, with some victims listed on the newer leak site. In early 2025, LockBit announced it would release LockBit 4.0 in February, and the new version introduced even more advanced features to further solidify their position in the ransomware landscape.
- **Targeted Industries:** LockBit primarily targets large organizations across various high-value industries, including finance, healthcare, manufacturing, and government. The group focuses on enterprises in critical infrastructure and those with sensitive data.

- 
- **Economic Model:** LockBit offers affiliates up to 75% of the ransom proceeds, making it an attractive platform for cybercriminals. Its well-established and profitable affiliate program has contributed to its prominence in the ransomware ecosystem, with affiliates targeting large organizations across various sectors. Recent law enforcement actions, such as the takedown efforts under Operation Cronos, have reportedly disrupted LockBit's affiliate base. These efforts may have caused a significant loss of affiliates, potentially impacting the group's ability to conduct large-scale attacks and diminishing its operational effectiveness.

⚠ **CISA Alerts:** [CISA Alert aa23-075a](#) / [CISA Alert aa23-165a](#) / [CISA Alert aa23-325a](#)

Contenders

Fog

Performance

- **RaaS Platform:** Fog ransomware, which first emerged in May 2024, primarily targets Windows systems and is considered a variant of the STOP/DJVU ransomware family. Known for its evolving tactics and strategic sophistication, Fog has gained attention for its aggressive lateral movement and privilege escalation techniques, including the use of pass-the-hash attacks and tools like PsExec. It often gains access through compromised VPN credentials, allowing it to quickly spread across networks. Once inside, the ransomware encrypts files and appends extensions such as ".FOG" or ".FLOCKED", making them inaccessible. Victims typically discover ransom notes named "readme.txt" or "HELP_YOUR_FILES.HTML", which contain instructions for contacting the attackers and negotiating file recovery.
- **Attack Volume:** Fog ransomware, which emerged in early 2024, saw a sharp rise in attack volume throughout the year—initially targeting U.S. educational institutions before expanding to other sectors—ultimately accounting for a significant share of global ransomware incidents by early 2025.
- **Ransom Demands:** Fog ransomware, emerging in early 2024, has been associated with ransom demands ranging from \$50,000 to several million dollars, depending on the targeted organization's size and perceived ability to pay.

Innovation

- **RaaS Platform Development:** Fog does not appear to be a RaaS. The ransomware is known for its advanced and highly disruptive tactics that make recovery extremely difficult. Upon breaching a system, it disables Windows Defender, deletes Volume Shadow Copies (VSS), and removes Veeam backups, undermining most traditional recovery mechanisms. Initial access is typically achieved through compromised VPN credentials, and in some cases, by exploiting vulnerabilities in VPN gateways, including SonicWall appliances. Once inside, Fog operators deploy tools like Cobalt Strike and Mimikatz to escalate privileges—utilizing techniques such as pass-the-hash attacks and extracting credentials from browsers and the NTDS.dit Active Directory database. For lateral movement, they employ PsExec and Remote



Known for its evolving tactics and strategic sophistication, Fog has gained attention for its aggressive lateral movement and privilege escalation techniques, including the use of pass-the-hash attacks and tools like PsExec.



Desktop Protocol (RDP), rapidly propagating across the network to encrypt multiple systems. Fog uses robust encryption algorithms, typically AES-256 for file encryption combined with RSA-2048 to encrypt the AES key, ensuring that files remain inaccessible without the attacker's private key. Though reports suggest Fog may target virtualized environments, including the encryption of VMDK files, this behavior has not been widely confirmed across all incidents. While common adversary frameworks like Metasploit may be used, Fog's activity is more consistently associated with custom scripting and living-off-the-land techniques.

- **Targeted Industries:** Fog ransomware primarily targets sectors such as education, business services, technology, manufacturing, finance, and government. While initially focused on U.S. higher education institutions, its victim profile has broadened to include organizations of varying sizes across multiple industries.
- **Economic Model:** Initially, Fog did not exfiltrate data; however, by July 2024, the group began employing double extortion tactics. Fog ransomware operates under a closed, centralized economic model, where a core group conducts the attacks end-to-end rather than relying on affiliates.

BianLian

Performance

- **RaaS Platform:** BianLian is not a traditional Ransomware-as-a-Service (RaaS) operation. The group emerged in June 2022 with a Golang-based ransomware and initially conducted full-spectrum attacks but was never structured as a public affiliate model. In early 2023, after a free decryptor was released, BianLian abandoned file encryption and pivoted to a pure extortion strategy—exfiltrating sensitive data and threatening to leak it unless paid. They leverage a mix of legitimate remote access tools, varied hosting providers, and multiple network ports to evade detection and maintain access. This strategic shift highlights the growing success of data theft-driven extortion, even without ransomware payloads. While not the most prolific group, BianLian has remained active and effective, targeting healthcare, critical infrastructure, and professional services sectors.
- **Attack Volume:** Since adopting this data-theft-only model, the group has maintained a consistent tempo of attacks, frequently targeting U.S.-based organizations in sectors like healthcare, education, and critical infrastructure.



While not the most prolific group, BianLian has remained active and effective, targeting healthcare, critical infrastructure, and professional services sectors.

- **Ransom Demands:** BianLian ransomware's ransom demands have varied over time and across different incidents. Early reports indicated that demands ranged between \$100,000 and \$350,000. However, more recent data suggests that the group's ransom demands have increased significantly, with averages reported around \$3 million.

Innovation

- **RaaS Platform Development:** BianLian never operated as a traditional Ransomware-as-a-Service (RaaS) group and now focuses entirely on data extortion attacks without deploying encryption payloads. After initially using a Golang-based ransomware in 2022, the group pivoted in early 2023 to pure extortion following the release of a public decryptor. BianLian exfiltrates sensitive data and demands payment under the threat of public disclosure. They rely heavily on open-source tools and command-line scripts for credential harvesting and data extraction, often using Rclone to move stolen files. For persistence and remote access, they deploy a custom backdoor written in Go, while leveraging PowerShell and Windows Command Shell to evade security tools through living-off-the-land techniques.
- **Targeted Industries:** BianLian primarily targets organizations in healthcare, education, government, legal services, and critical infrastructure, with a strong focus on U.S.-based entities. Their victim selection suggests a preference for sectors that handle sensitive data and are under pressure to avoid public disclosure, increasing the likelihood of ransom payment.
- **Economic Model:** BianLian operates under a self-managed economic model, meaning the group handles all aspects of the attack lifecycle internally—from initial access to data theft, extortion, and negotiation—without relying on affiliates or partners.

⚠ **CISA Alert:** [CISA Alert aa23-136a](#)

Hunters International

Performance

- **RaaS Platform:** Hunters International is a Ransomware-as-a-Service (RaaS) group that emerged in October 2023, shortly after the Hive ransomware group was dismantled by law enforcement. Though they deny being a direct rebrand, Hunters International's codebase shows clear links to Hive, suggesting a technical lineage. The group operates a sophisticated platform



Notably, Hunters International now embeds the decryption key directly within each encrypted file, streamlining recovery for victims who pay—an evolution from previous approaches that stored keys separately.



using double extortion tactics, combining data exfiltration with file encryption to pressure victims. Notably, the ransomware now embeds the decryption key directly within each encrypted file, streamlining recovery for victims who pay—an evolution from previous approaches that stored keys separately. Since its debut, Hunters International has launched frequent attacks, averaging nearly one per day by late 2024, and has targeted a broad array of industries across multiple countries. This sustained activity, paired with their technical agility, underscores the group's growing prominence in the ransomware landscape.

- **Ransom Demands:** While exact figures are unavailable, Hunters International's ransom demands likely align with or exceed the 2024 industry average of \$2.73 million, given their focus on high-value targets.

Innovation

- **RaaS Platform Development:** Initially broad in its targeting, the group has since refined its focus to sectors with high ransom potential, primarily healthcare, financial services, and critical infrastructure, where data sensitivity and downtime costs are high. Their access methods include phishing, social engineering, supply chain compromises, and exploitation of Remote Desktop Protocol (RDP). To evade detection, they disable Endpoint Detection and Response (EDR) tools and use PowerShell and Windows Command Shell. Hunters International employs Mimikatz for credential harvesting, creates new domain accounts for persistence, and uses tools like SoftPerfect Network Scanner to identify internal assets. Lateral movement is facilitated through PsExec and RDP, while shadow copies are deleted to block system restoration. In mid-2024, the group introduced a new C#-based Remote Access Trojan (RAT) called SharpRhino, delivered via typosquatted domains mimicking tools like Angry IP Scanner. SharpRhino enables stealthy, persistent remote access. Hunters International has also improved its encryption techniques and adopted more advanced data exfiltration, underscoring its strategic focus on maximizing extortion pressure and operational efficiency.
- **Targeted Industries:** Hunters International favors high-value targets in sectors like healthcare, financial services, critical infrastructure, education, and manufacturing, particularly in North America and Europe.
- **Economic Model:** Hunters International operates under a RaaS model, and leverages data exfiltration for double extortion.

Rhysida

Performance

- **RaaS Platform:** Rhysida is a Ransomware-as-a-Service (RaaS) operation first identified in May 2023 that quickly rose to prominence by early 2024. The group employs a double extortion strategy, exfiltrating sensitive data and threatening public leaks if victims do not comply with ransom demands. Rhysida maintains a leak site on the Tor network to expose non-paying victims, but there is limited evidence of a formal victim support portal. For initial access, the group typically uses phishing emails and legitimate administrative tools like Cobalt Strike for persistence and lateral movement. While vulnerabilities such as ZeroLogon (CVE-2020-1472) and compromised VPNs are common across ransomware actors, Rhysida's direct use of these has not been definitively confirmed. In February 2024, researchers released a free decryptor exploiting a flaw in Rhysida's encryption process, briefly disrupting their operations. However, the group quickly adapted, resuming attacks and reinforcing its presence in the ransomware landscape. Rhysida's tactics, technical agility, and rapid resurgence demonstrate its capability to remain a persistent threat despite temporary setbacks.
- **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 regarding Rhysida ransomware's average ransom demands are not widely disclosed. However, in November 2023, Rhysida demanded 20 Bitcoin (approximately \$740,000 at that time) from one victim.

Innovation

- **RaaS Platform Development:** Rhysida deletes Volume Shadow Copies (VSS) to prevent recovery and uses Cobalt Strike or similar command-and-control tools for managing compromised systems. PSEXEC is deployed for lateral movement, while PowerShell scripts deliver ransomware payloads. Rhysida also uses scheduled tasks to maintain persistence across reboots. Rhysida's encryption process combines AES-256 in CTR mode for file encryption and RSA-4096 for secure key management, ensuring victims cannot recover data without the private key. Initially targeting Windows environments, Rhysida has expanded its arsenal to include a Linux variant aimed at VMware ESXi servers, reflecting a growing trend among ransomware groups targeting



Rhysida's encryption process combines AES-256 in CTR mode for file encryption and RSA-4096 for secure key management, ensuring victims cannot recover data without the private key.



virtual infrastructure. Although specifics on exploited vulnerabilities remain limited, the group often gains access through phishing and misconfigured or exposed remote services. Tactically, Rhysida's methods show notable overlap with the Vice Society group, raising the possibility of shared tooling or personnel. Despite a brief disruption in February 2024 due to a publicly released decryptor, the group quickly adapted and remains an active and evolving threat across multiple sectors.

- **Targeted Industries:** Rhysida primarily targets sectors such as healthcare, education, government, and critical infrastructure, focusing on organizations where data sensitivity and operational urgency increase the likelihood of ransom payment.
- **Economic Model:** Rhysida operators claim to be a "cybersecurity team" performing unauthorized "penetration testing" to supposedly "assist" victim organizations in identifying security vulnerabilities and strengthening their networks. They present the subsequent ransom demand as "payment" for their services.

⚠ **CISA Alert:** [CISA Alert aa23-319a](#)

Meow

Performance

- **RaaS Platform:** Meow ransomware (also known as MeowLeaks or MeowCorp) emerged in late 2022 and is believed to be a spinoff of the Conti gang, based on reused code. Initially a low-profile operation, Meow has recently shifted to a data extortion-only model, stealing sensitive information and posting it on its leak site without deploying encryption malware—similar to groups like BianLian. The group primarily targets U.S.-based sectors with high-value data, particularly healthcare and medical research. However, a recent surge in claimed breaches has raised doubts about their authenticity, as several incidents attributed to Meow match known attacks by BlackSuit ransomware. This overlap suggests Meow may sometimes act as a data broker or exaggerate claims to boost visibility and pressure victims. Despite this, Meow remains a credible threat, especially to small and medium-sized businesses (SMBs), and reflects a broader trend toward extortion-driven ransomware operations.
- **Attack Volume:** Meow ransomware began with low attack volume in late 2022 but has significantly increased activity throughout 2024, frequently posting new victims on its leak site as it intensifies its focus on data extortion.



Meow has recently shifted to a data extortion-only model, stealing sensitive information and posting it on its leak site without deploying encryption malware—similar to groups like BianLian.

- **Ransom Demands:** Specific data on Meow ransomware's average ransom demands is limited, but at least one documented case in 2024 showed a demand as low as \$7,000, significantly below the industry average of \$3.7 million.

Innovation

- **RaaS Platform Development:** Meow initially used a hybrid encryption scheme, combining ChaCha20 for file encryption and RSA-4096 for key management before shifting to more data extortion attacks. Initial access is commonly achieved through phishing, exploitation of Remote Desktop Protocol (RDP) vulnerabilities, and compromises of widely used platforms like VMware and Jenkins. For lateral movement and execution, Meow operators employ living-off-the-land techniques and open-source tools, though their tooling remains less documented than that of other groups. In 2024, Meow transitioned to a data extortion-only model, abandoning ransomware payloads in favor of stealing sensitive information and using public leak site exposure to pressure victims. It remains unclear whether Meow continues to operate as a RaaS or functions as a closed group. Recent attacks target both Windows and Linux systems, including VMware ESXi, with an increasing focus on organizations handling financial and personal data, particularly among small and mid-sized businesses.
- **Targeted Industries:** Meow ransomware primarily targets organizations handling sensitive financial and personal data, with a focus on sectors like healthcare, financial services, professional services, and education, particularly among small and mid-sized businesses.
- **Economic Model:** Meow appears to be shifting from double extortion to straight data exfiltration for extortion.

KillSec

Performance

- **RaaS Platform:** KillSec emerged in late 2023 as a hacktivist group initially aligned with the Anonymous movement, known for website defacements and ideologically motivated cyberattacks. Over time, the group evolved into a more structured cybercriminal entity, shifting focus toward ransomware operations. In June 2024, KillSec adopted a Ransomware-as-a-Service (RaaS) model, enabling affiliates to conduct attacks using their infrastructure, which significantly expanded their reach and increased the volume of



KillSec's transition from hacktivism to financially driven cybercrime highlights their tactical pivot and growing sophistication in the ransomware ecosystem.



targeted incidents. The group communicates with victims primarily through Telegram and Tox, using these platforms for extortion, negotiation, and public threat dissemination. KillSec's transition from hacktivism to financially driven cybercrime highlights their tactical pivot and growing sophistication in the ransomware ecosystem.

- **Attack Volume:** KillSec's attack volume has increased notably since adopting a Ransomware-as-a-Service model in mid-2024, with a growing number of incidents reported across diverse sectors.
- **Ransom Demands:** Specific data on KillSec ransomware's average ransom demands is currently unavailable. However, in the first half of 2024, the average ransom demand across various ransomware groups exceeded \$5.2 million.

Innovation

- **RaaS Platform Development:** With the launch of its Ransomware-as-a-Service (RaaS) platform in June 2024, KillSec significantly expanded its operational capabilities and reach. The platform is designed to be user-friendly, allowing even affiliates with limited technical skills to launch ransomware attacks using tools provided by the group. It features an advanced file encryption locker coded in C++ and an intuitive control panel accessible via the Tor network, enabling anonymous management of attacks. KillSec's RaaS offering also includes a denial-of-service (DDoS) tool and an advanced data stealer to collect sensitive information for further extortion. For initial access, the group employs a range of tactics including phishing campaigns, exploitation of known vulnerabilities, and deployment of custom malware to establish persistence within compromised systems. These capabilities reflect KillSec's evolution from a hacktivist collective into a technically capable cybercriminal enterprise, increasingly effective at compromising and extorting victims across multiple sectors.
- **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) economic model, providing affiliates with ransomware tools and infrastructure in exchange for a cut of ransom payments. The group also employs a double extortion strategy.

Emerging

Sarcoma

Performance

- **RaaS Platform:** Sarcoma ransomware, a rapidly emerging RaaS group first identified in October 2024, has quickly risen to prominence in the global cybercrime landscape. Despite its recent debut, the group is already known for aggressive attacks, significant data breaches, and a strategic focus on disrupting supply chains. Sarcoma typically gains initial access through phishing and vulnerability exploitation, enabling swift and damaging intrusions across various sectors. While technical details of its methods remain under investigation, its growing impact and operational reach have made it a serious and escalating threat within the ransomware ecosystem.
- **Attack Volume:** Sarcoma ransomware launched in October 2024 with 31 attacks in its first month and continued gaining momentum, reaching 58 total attacks by the end of the year. Its activity has steadily increased into 2025, with rising ransom demands and a growing focus on high-value targets.
- **Ransom Demands:** Sarcoma's ransom demands have steadily increased since its debut, starting in the mid-five-figure range. By early 2025, demands have escalated to high-six and even seven figures, particularly in attacks targeting large enterprises.

Innovation

- **RaaS Platform Development:** Sarcoma ransomware is a sophisticated threat actor known for leveraging remote monitoring and management (RMM) tools to conduct in-depth network discovery and escalate access through known vulnerabilities. In at least one confirmed incident, Sarcoma used RMM tools during its attack on Smart Media Group Bulgaria, identifying and exploiting weak points to expand its footprint. While some reports suggest the use of zero-day vulnerabilities, this remains unconfirmed. Sarcoma's tactics include disabling security processes, deleting volume shadow copies (VSS), and using encrypted payloads to evade detection. The group reportedly employs AES-256 encryption for file locking, combined with RSA for secure key exchange, making recovery nearly impossible without payment. Although tools like



While technical details of Sarcoma's methods remain under investigation, its growing impact and operational reach have made it a serious and escalating threat within the ransomware ecosystem.



PowerShell, Mimikatz, and custom command-line options are commonly used by similar ransomware groups, there is currently no public confirmation that Sarcoma consistently uses them.

- **Targeted Industries:** Sarcoma ransomware targets a wide range of industries—including manufacturing, logistics, legal, accounting, and industrial supply—highlighting its broad, opportunistic approach. With victims across North America, Europe, Asia, and Africa, the group poses a global threat to organizations handling sensitive data or supporting critical operations.
- **Economic Model:** Sarcoma operates as a ransomware-as-a-service (RaaS) group, partnering with affiliates who carry out attacks in exchange for a share of the ransom, typically splitting profits 70/30 in favor of the affiliate. The group engages in double extortion, exfiltrating sensitive data before encryption and threatening to leak it on their dark web site if victims do not pay.

DragonForce

Performance

- **RaaS Platform:** DragonForce is a sophisticated Ransomware-as-a-Service (RaaS) operation that emerged in August 2023, leveraging malware variants built from leaked LockBit 3.0 and customized Conti builders. This dual-codebase approach reflects the group's evolving capabilities and strategic reuse of proven ransomware frameworks. DragonForce quickly gained traction within the cybercrime ecosystem, conducting targeted attacks against organizations across industries such as manufacturing, transportation, and real estate. The group employs advanced evasion techniques and log-wiping mechanisms to disable security tools and complicate forensic analysis.
- **Attack Volume:** DragonForce ransomware, emerging in August 2023, has demonstrated a notable increase in attack volume over time. Between its inception and August 2024, the group targeted 82 victims across various industries. By February 2025, DragonForce had expanded its operations to the Middle East, notably targeting organizations in Saudi Arabia.
- **Ransom Demands:** Specific information about DragonForce ransomware's average ransom demands is not publicly available, but their operations suggest they aim for high-value targets to maximize their demands.



DragonForce has adopted advanced tactics such as clearing event logs and disabling security tools, often using the “Bring Your Own Vulnerable Driver” (BYOVD) method to bypass defenses.

Innovation

- **RaaS Platform Development:** DragonForce has adopted advanced tactics such as clearing event logs and disabling security tools, often using the “Bring Your Own Vulnerable Driver” (BYOVD) method to bypass defenses. While tools like Cobalt Strike and Mimikatz are common in similar attacks, their direct use by DragonForce has not been publicly confirmed. The group likely employs AES-256 encryption for data locking combined with RSA for key exchange—standard among modern ransomware families. Their use of stealth, paired with data exfiltration and aggressive encryption, highlights an evolving threat actor capable of targeting high-value systems across multiple industries with increasing precision and operational maturity.
- **Targeted Industries:** DragonForce ransomware targets a broad range of industries—including manufacturing, transportation, logistics, real estate, construction, and professional services—highlighting its opportunistic approach to maximizing disruption and ransom potential.
- **Economic Model:** DragonForce operates under a ransomware-as-a-service (RaaS) model, partnering with affiliates who execute attacks in exchange for a revenue share, typically around 70% to the affiliate and 30% to the operator. The group employs double extortion tactics, exfiltrating sensitive data before encryption and threatening to leak it to pressure victims into payment.


Cloak

Performance

- **RaaS Platform:** The Cloak ransomware group emerged in late 2022 and has rapidly evolved into a prominent player in the ransomware-as-a-service (RaaS) ecosystem. Initially gaining traction through frequent and impactful attacks across diverse industries, Cloak has demonstrated a clear trajectory of growth and sophistication. Analysts have observed operational links between Cloak and the Good Day ransomware group, a variant of the ARCrypter family that surfaced in mid-2023, with both groups sharing a common data leak platform. This overlap suggests potential collaboration or shared infrastructure, highlighting Cloak's adaptability and integration within the broader ransomware landscape.



Analysts have observed operational links between Cloak and the Good Day ransomware group, a variant of the ARCrypter family that surfaced in mid-2023, with both groups sharing a common data leak platform.

- 
- **Attack Volume:** Cloak ransomware rapidly expanded its operations after emerging, with activity linked to the Good Day group by mid-2023, suggesting shared infrastructure or collaboration. After fluctuating throughout 2024, the group's attack volume surged again in early 2025, signaling a renewed escalation in its operations.
 - **Ransom Demands:** While specific figures for Cloak have not been confirmed, average ransomware payments across the ecosystem rose significantly in 2024, often reaching seven figures. The group's effectiveness in coercing payment remains unclear, as no verified data on Cloak's ransom success rate is publicly available.

Innovation

- **RaaS Platform Development:** Cloak ransomware, associated with the Good Day variant of the ARCrypter family, has been linked to ransomware strains built from leaked Babuk source code. According to Halcyon analysis, Cloak gains initial access via Initial Access Brokers (IABs) or social engineering methods such as phishing and malicious installers disguised as Microsoft Windows updates. It uses embedded loaders to deliver its payload, which employs privilege escalation, process termination, and anti-debugging techniques to evade detection. Cloak encrypts files using the HC-128 algorithm, with keys generated through a multi-step process involving CryptGenRandom, Curve25519, and SHA512 hashing for secure encryption and IV creation. The ransomware supports full and intermittent encryption modes to optimize performance while maximizing disruption. Cloak achieves persistence through registry modifications and hinders recovery by deleting volume shadow copies and disabling critical system services. Its use of virtual hard disk (VHD) delivery, stealth techniques, and data destruction tactics underscores its sophistication and growing threat profile.
- **Targeted Industries:** Cloak ransomware targets industries such as manufacturing, healthcare, education, government, and professional services across North America, Europe, and Asia, reflecting a broad and opportunistic global attack strategy.
- **Economic Model:** Cloak operates under a ransomware-as-a-service (RaaS) model, enabling affiliates to deploy its payloads in exchange for a share of ransom payments—typically a 70/30 split favoring affiliates. The group uses double extortion tactics.

Ghost

Performance


- **RaaS Platform:** Ghost ransomware, known as GhostLocker, was introduced in October 2023 by GhostSec, a hacktivist group originally linked to Anonymous. The launch marked a strategic shift for GhostSec from ideological operations to financially motivated cybercrime. GhostLocker was initially developed in Python and later re-engineered into GhostLocker 2.0 using Golang by January 2024, enhancing its capabilities and cross-platform functionality. The ransomware is part of a broader collaboration among several threat groups, including Stormous, SiegedSec, and ThreatSec—collectively known as “The Five Families.” These alliances signal a growing trend of cooperation among cybercriminal collectives. In early 2024, GhostSec and Stormous expanded their efforts with a joint RaaS platform called STMX_GhostLocker. The emergence and development of Ghost ransomware reflects the increasing professionalization and coordination within the cybercriminal landscape, particularly among actors with origins in hacktivist movements.
- **Attack Volume:** Beginning in early 2021, the Ghost ransomware group initiated attacks by exploiting unpatched, internet-facing services, leading to widespread compromises across more than 70 countries.
- **Ransom Demands:** While specific figures for GhostLocker are unavailable, average ransom demands across ransomware attacks reached approximately \$5.2 million in early 2024

Innovation

- **RaaS Platform Development:** Ghost was initially developed in Python and packaged using tools like PyInstaller and Nuitka, with early versions dropping files and creating child processes for encryption. In January 2024, GhostLocker 2.0 was released in Golang, enhancing evasion and cross-platform support for Windows, Linux, and VMware. It uses the Fernet symmetric encryption algorithm, based on AES-128 in CBC mode with PKCS7 padding. Marketed as enterprise-grade ransomware, Ghost includes a web-based builder with customizable options and features like anti-detection, automated exfiltration, multiple persistence methods, and a WatchDog process. GhostSec developed it in collaboration with groups such as SiegedSec, ThreatSec, Stormous, and BlackForums, collectively known as “The Five Families.” In February 2024, GhostSec and Stormous launched the STMX_GhostLocker RaaS platform.



The emergence and development of Ghost ransomware reflects the increasing professionalization and coordination within the cybercriminal landscape, particularly among actors with origins in hacktivist movements.

- 
- **Targeted Industries:** Ghost ransomware has targeted industries including technology, education, healthcare, manufacturing, and critical infrastructure across regions such as the Middle East, Africa, Asia, and parts of Europe and the Americas.
 - **Economic Model:** Ghost operates as a Ransomware-as-a-Service (RaaS), offering affiliates a web-based builder and management portal for customizing ransomware payloads. Affiliates pay an initial fee ranging from \$999 to \$1,200 USD, with referral discounts available, creating a pyramid-like structure. The platform supports double extortion tactics, involving data exfiltration prior to encryption, thereby pressuring victims to pay by threatening data exposure. Specific details on affiliate revenue shares remain undisclosed.

Arcus Media

Performance

- **RaaS Platform:** Arcus Media is a ransomware-as-a-service (RaaS) group that emerged in May 2024, rapidly gaining prominence through a series of high-impact attacks. Unlike many newer groups, Arcus Media uses custom-built malware rather than reusing leaked code, signaling a high level of technical sophistication. The group operates a closed affiliate program requiring referrals and vetting, aiming to maintain operational security. Arcus Media has been linked to over 50 attacks within a short span, targeting industries such as business services, retail, and media. Their selective encryption methods, recovery disruption tactics, and focus on disabling critical processes reflect a calculated strategy to maximize leverage over victims. While not directly tied to major legacy groups, Arcus Media's model and tactics resemble those of REvil and DarkSide, marking its rapid evolution in the ransomware ecosystem.
- **Attack Volume:** Arcus Media has shown a rapid increase in attack volume, quickly establishing itself as a high-frequency threat actor. Within just a few months, the group was linked to dozens of ransomware incidents, reflecting a fast-growing operational tempo and expanding affiliate network.
- **Ransom Demands:** Specific information regarding Arcus Media's average ransom demands is not publicly available.



Arcus Media's tooling and modular delivery mechanisms reflect a mature and adaptable malware framework designed for stealth, disruption, and maximum leverage over victims.



Innovation

- **RaaS Platform Development:** Arcus Media employs a range of advanced tactics, techniques, and procedures (TTPs) to infiltrate and disrupt target environments. Initial access is typically gained through phishing emails or compromised credentials, often purchased via Initial Access Brokers. The group uses obfuscated scripts and loaders to deploy its custom ransomware payload, which features selective file encryption to balance speed and impact. Arcus Media uses the AES encryption algorithm for file locking, paired with RSA for secure key exchange—standard among modern ransomware variants. For privilege escalation and credential harvesting, tools like Mimikatz are deployed, while endpoint detection evasion is achieved through process injection and anti-debugging techniques. The ransomware also disables security software, terminates recovery services, and deletes shadow copies to prevent restoration. Persistence is maintained via registry modifications and scheduled tasks. Arcus Media's tooling and modular delivery mechanisms reflect a mature and adaptable malware framework designed for stealth, disruption, and maximum leverage over victims.
- **Targeted Industries:** Arcus Media targets a broad range of industries, including business services, retail, media, healthcare, and manufacturing, reflecting an opportunistic approach focused on organizations with valuable or sensitive data. Geographically, its attacks have been observed across North America, Europe, and parts of Asia.
- **Economic Model:** Arcus Media operates under a ransomware-as-a-service (RaaS) model, partnering with a vetted group of affiliates who carry out attacks in exchange for a revenue split—typically 70% to the affiliate and 30% to the operator. The group uses double extortion tactics, exfiltrating sensitive data before encrypting files and threatening public leaks.

Diminishing

BlackSuit

Performance


- **RaaS Platform:** BlackSuit is a private ransomware group that does not operate as a traditional ransomware-as-a-service (RaaS), instead maintaining centralized control over its operations. In August 2024, the FBI and CISA assessed that BlackSuit is a rebranding of the Royal ransomware group, based on observed overlaps in tooling, encryption methods, and tactics including the use intermittent encryption techniques. Royal itself was previously linked to members of the now-defunct Conti group, suggesting a lineage of operators migrating across multiple ransomware brands. BlackSuit continues to target both Windows and Linux environments, including VMware ESXi systems, indicating its capacity to disrupt diverse enterprise infrastructures.
- **Attack Volume:** Since mid-2023, BlackSuit ransomware has steadily increased its attack volume, continuing the operational momentum of the Royal group under a new identity.
- **Ransom Demands:** Specific figures for BlackSuit's average ransom demands have not been publicly disclosed, but based on patterns from Royal and similar groups, demands likely range from several hundred thousand to multi-million dollars, depending on the victim's size and sector.

Innovation

- **RaaS Platform Development:** BlackSuit ransomware employs a range of advanced tactics, techniques, and procedures (TTPs) to infiltrate and disrupt victim environments. Initial access is typically gained through phishing or exploitation of exposed services, followed by lateral movement using tools such as Remote Desktop Protocol (RDP) and PsExec. The group often creates or modifies user accounts to maintain persistence and escalate privileges. Once inside, BlackSuit deletes volume shadow copies and disables backup systems to prevent recovery. While specific tooling is not always confirmed, its tactics align with those seen in similar operations, including the likely use of credential dumping and command execution frameworks. BlackSuit encrypts data using AES via OpenSSL libraries and employs intermittent encryption to speed up operations while evading detection.



BlackSuit deletes volume shadow copies and disables backup systems to prevent recovery, and its tactics align with those seen in similar operations, including the likely use of credential dumping and command execution frameworks.



Its tight operational control—carried over from its predecessor, Royal—indicates a high level of discipline and intent to avoid detection and maximize impact across both Windows and Linux environments, including VMware ESXi systems.

- **Targeted Industries:** BlackSuit targets a wide range of industries—including healthcare, education, government, and critical infrastructure—across North America, Europe, and parts of Asia, reflecting a broad and globally oriented attack strategy.
- **Economic Model:** BlackSuit operates as a closed, centralized ransomware group rather than a public RaaS, keeping control within a core team rather than using affiliates. The group employs double extortion tactics, exfiltrating sensitive data before encryption and threatening to leak it if the ransom is not paid. By avoiding affiliate partnerships, BlackSuit likely retains full ransom profits while reducing the risk of operational exposure.

⚠ **CISA Alert:** [CISA Alert aa23-061a](#)


Cactus

Performance

- **RaaS Platform:** Cactus ransomware first emerged in early 2023 and has quickly evolved into a notable threat within the cybercriminal landscape. Although not directly linked to a larger ransomware-as-a-service (RaaS) group, Cactus appears to operate as a private entity, showing signs of technical maturity and deliberate expansion over time. Cactus initially focused on targeting Windows-based systems but has since broadened its scope to include virtualization platforms such as VMware ESXi and Microsoft Hyper-V, reflecting its growing capabilities and adaptability. Cactus has also been observed exploiting vulnerabilities in widely used business platforms like Qlik Sense, indicating a shift toward targeting enterprise environments with higher-value data. While no confirmed affiliation with legacy ransomware groups has been established, Cactus demonstrates techniques and strategic behavior consistent with other advanced operations, suggesting its operators may have prior experience in the ransomware ecosystem.
- **Attack Volume:** Since its emergence in early 2023, Cactus ransomware has steadily increased its attack volume, evolving from a relatively unknown threat to a consistent presence in enterprise-targeted ransomware incidents. Over time, its operations have expanded in scope and scale.



Cactus initially focused on targeting Windows-based systems but has since broadened its scope to include virtualization platforms such as VMware ESXi and Microsoft Hyper-V, reflecting its growing capabilities and adaptability.

- 
- **Ransom Demands:** Specific figures for Cactus ransomware's average ransom demands have not been publicly disclosed, but based on observed activity and industry norms, demands are estimated to range from several hundred thousand to multiple millions of dollars.

Innovation

- **RaaS Platform Development:** Cactus ransomware employs a range of advanced tactics to evade detection and maintain persistence within targeted networks. It gains initial access by exploiting known vulnerabilities in VPN appliances and enterprise platforms, notably Qlik Sense (CVE-2023-41265, CVE-2023-41266, CVE-2023-48365). Once inside, Cactus abuses Living-off-the-Land (LotL) techniques, leveraging tools like PowerShell, Scheduled Tasks, Rclone, and Chisel for lateral movement and data exfiltration. Operators have been observed using legitimate remote access tools such as Splashtop, AnyDesk, and SuperOps RMM to maintain access and evade security monitoring. Cactus employs a unique tactic of encrypting its own ransomware binary, requiring a decryption key at runtime to execute—making it difficult for security tools to detect. The ransomware also deletes shadow copies, dumps LSASS credentials for privilege escalation, and may deploy SSH backdoors for continued access.
- **Targeted Industries:** Cactus ransomware targets a wide range of industries—including manufacturing, healthcare, IT services, and finance—across North America, Europe, and parts of Asia.
- **Economic Model:** Cactus operates as a private ransomware group rather than a public RaaS, maintaining tight control over its operations without known affiliate involvement. It uses double extortion tactics, exfiltrating sensitive data before encrypting systems and threatening to publish the stolen information if the ransom is not paid. This centralized model allows Cactus operators to retain full control over negotiations and ransom proceeds, maximizing profits while reducing exposure.

El Dorado

Performance

- **RaaS Platform:** El Dorado ransomware, also known as Eldorado, first emerged in March 2024, positioning itself as a distinct and technically mature operation within the cybercriminal ecosystem. Unlike many newer groups that rely on repurposed or leaked ransomware code, Eldorado developed its own proprietary builder from the ground up, signaling both innovation and a deliberate effort to establish independence. The group announced its arrival through underground forums, launching a closed affiliate program that suggested a structured and selective approach to expansion. While there is no confirmed direct link to legacy ransomware families such as LockBit or Conti, Eldorado's operational model and rapid development trajectory indicate that its core operators may possess prior experience in organized ransomware activity. The group's early emphasis on cross-platform capabilities and encryption strength further reflects a calculated evolution, designed to compete with more established threat actors.
- **Attack Volume:** El Dorado has shown a steady increase in attack volume, quickly progressing from initial activity to consistent targeting of organizations across multiple sectors.
- **Ransom Demands:** Specific figures for El Dorado's average ransom demands have not been publicly disclosed but based on industry trends and the group's focus on enterprise targets, demands are likely in the high six- to seven-figure range.

Innovation

- **RaaS Platform Development:** El Dorado ransomware is written in Golang, giving it cross-platform capabilities to target Windows, Linux, and VMware ESXi systems. It uses the ChaCha20 algorithm for file encryption and RSA-OAEP for secure key exchange, ensuring strong cryptographic protection. The ransomware can encrypt files over SMB shares, enabling it to impact networked environments and shared storage. It supports custom configurations, allowing operators to specify directories, skip critical file types like DLLs and EXEs, and focuses on network shares to maximize disruption. After execution, the ransomware is designed to self-delete, reducing forensic visibility. El Dorado's proprietary builder, developed independently of leaked codebases, offers extensive customization and operational flexibility. This tooling enables attackers to tailor payloads based on target infrastructure, enhancing stealth and impact.



Unlike many newer groups that rely on repurposed or leaked ransomware code, Eldorado developed its own proprietary builder from the ground up, signaling both innovation and a deliberate effort to establish independence.

- **Targeted Industries:** El Dorado ransomware targets industries such as manufacturing, IT services, healthcare, and professional services across North America, Europe, and Asia, reflecting a global, enterprise-focused attack strategy.
- **Economic Model:** El Dorado operates under a ransomware-as-a-service (RaaS) model, offering a proprietary builder to a limited set of affiliates who conduct attacks in exchange for a profit share—typically favoring affiliates with up to 70% of the ransom. The group employs double extortion tactics.

RAWorld

Performance

- **RaaS Platform:** RAWorld ransomware emerged in early 2024 as a rapidly evolving threat actor within the cybercrime landscape. While the group does not appear to be directly linked to any major legacy ransomware families, its level of coordination and attack sophistication suggests that its operators may have prior experience in organized cybercriminal activity. RAWorld initially demonstrated a clear trajectory of growth, expanding its targeting scope and refining its attack strategies to maximize impact, but recently attack activity declined. The group's rise aligns with broader trends in ransomware development, including a shift toward more centralized, technically advanced operations that do not rely on traditional affiliate structures.
- **Attack Volume:** Since its emergence in early 2024, RAWorld has shown a steady increase in attack volume, transitioning from sporadic incidents to more frequent and coordinated campaigns.
- **Ransom Demands:** While specific figures for RAWorld's average ransom demands have not been publicly disclosed, the group is believed to follow broader industry trends, with demands likely ranging from several hundred thousand to several million dollars.

Innovation

- **RaaS Platform Development:** RAWorld ransomware employs a highly customized variant based on the leaked Babuk source code for its Windows payload, incorporating ChaCha20 encryption with RSA key wrapping to ensure strong data encryption. It propagates across networks by exploiting Group Policy Objects (GPOs), distributing payloads via the SYSVOL share on domain controllers. Execution is commonly performed using PowerShell,



RAWorld initially demonstrated a clear trajectory of growth, expanding its targeting scope and refining its attack strategies to maximize impact, but recently attack activity declined.



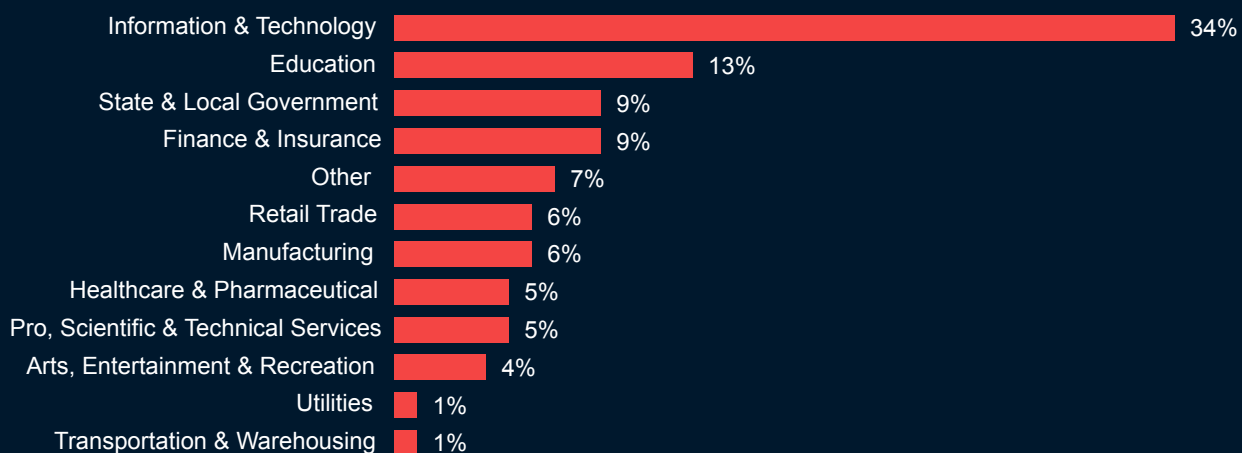
while registry modifications are applied to disable security tools and impair system defenses. RAWorld also forces infected systems to reboot into Safe Mode with Networking, bypassing many endpoint protections that are inactive in that mode. To enhance platform reach, the group has developed a separate Linux variant written in Golang—independent of the Babuk codebase—expanding its targeting to VMware ESXi and Linux environments. This evolution reflects RAWorld's increasing technical sophistication, as it leverages native Windows tools, script-based automation, and cross-platform payloads to maximize impact, persistence, and evasion within enterprise networks.

- **Targeted Industries:** RAWorld targets industries such as manufacturing, healthcare, education, government, and technology across North America, Europe, and parts of Asia.
- **Economic Model:** RAWorld operates as a ransomware-as-a-service (RaaS) group, offering its platform to affiliates in exchange for a profit share—typically around 70% for affiliates and 30% for operators. The group uses double extortion tactics, exfiltrating sensitive data before encryption and threatening to leak it if the ransom is not paid.

Halcyon Threat Insights: January

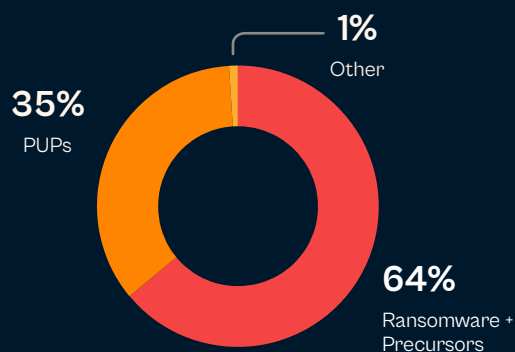
Here are the key insights from the Halcyon RISE Team findings for January 2025 based on intelligence collected from our customer base.

Threats Prevented by Industry Vertical



Threat Types by Category

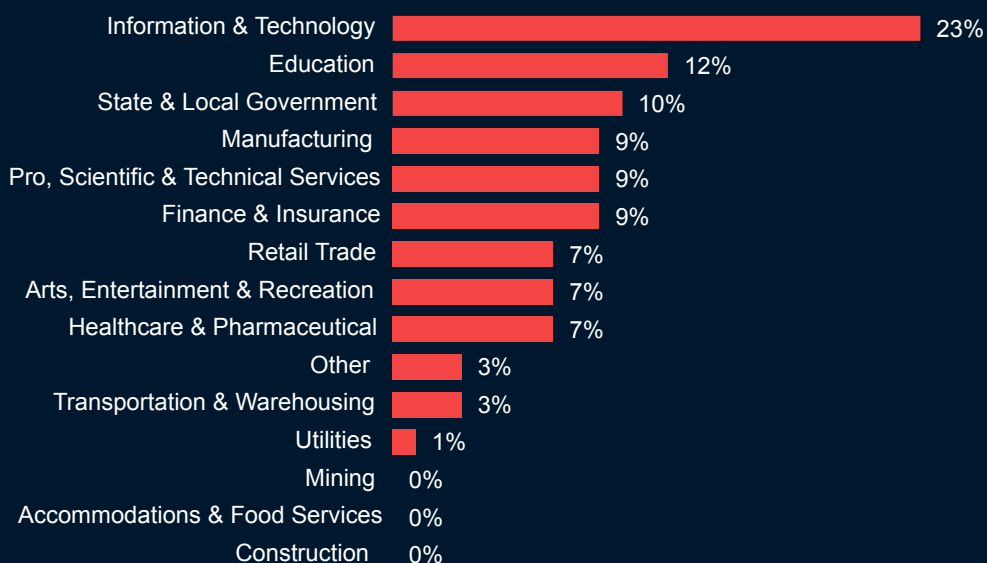
Halcyon detected and blocked a wide variety of threats that were missed by other security layers in our client's environments that are often precursors to the delivery of the ransomware payload.



Halcyon Threat Insights: February

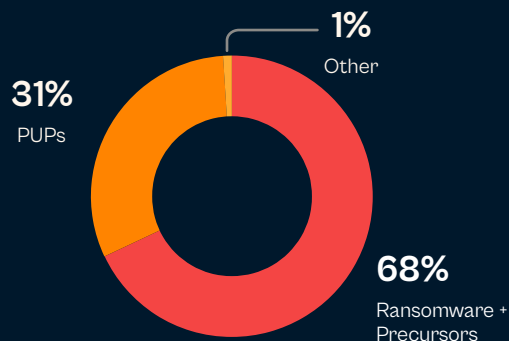
Here are the key insights from the Halcyon RISE Team findings for February 2025 based on intelligence collected from our customer base.

Threats Prevented by Industry Vertical



Threat Types by Category

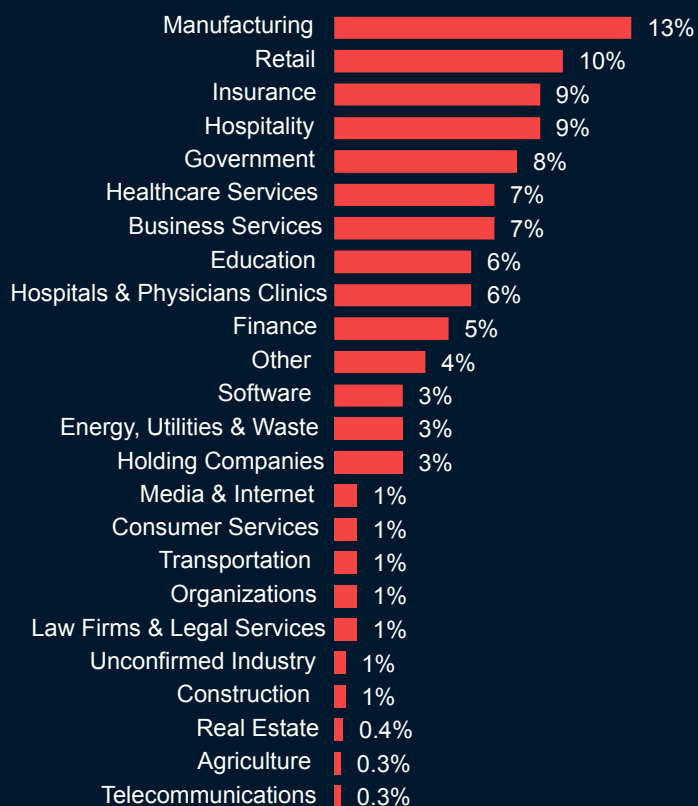
Halcyon detected and blocked a wide variety of threats that were missed by other security layers in our client's environments that are often precursors to the delivery of the ransomware payload.



Halcyon Threat Insights: March

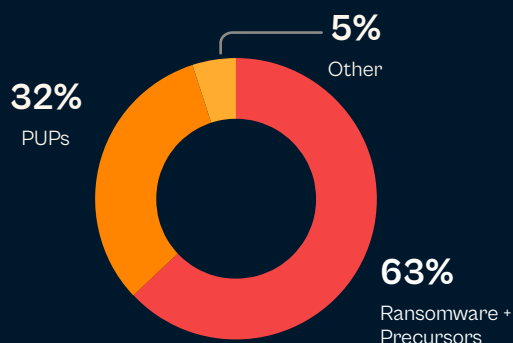
Here are the key insights from the Halcyon RISE Team findings for March 2025 based on intelligence collected from our customer base.

Threats Prevented by Industry Vertical



Threat Types by Category

Halcyon detected and blocked a wide variety of threats that were missed by other security layers in our client's environments that are often precursors to the delivery of the ransomware payload.





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 effectiveness of an organization's plan is measured by its execution during a real 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.

A decorative graphic in the top left corner consisting of a grid of colored dots in shades of orange, yellow, and blue, with a single red dot in the center. The background is dark blue with scattered dots in various colors.

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.

