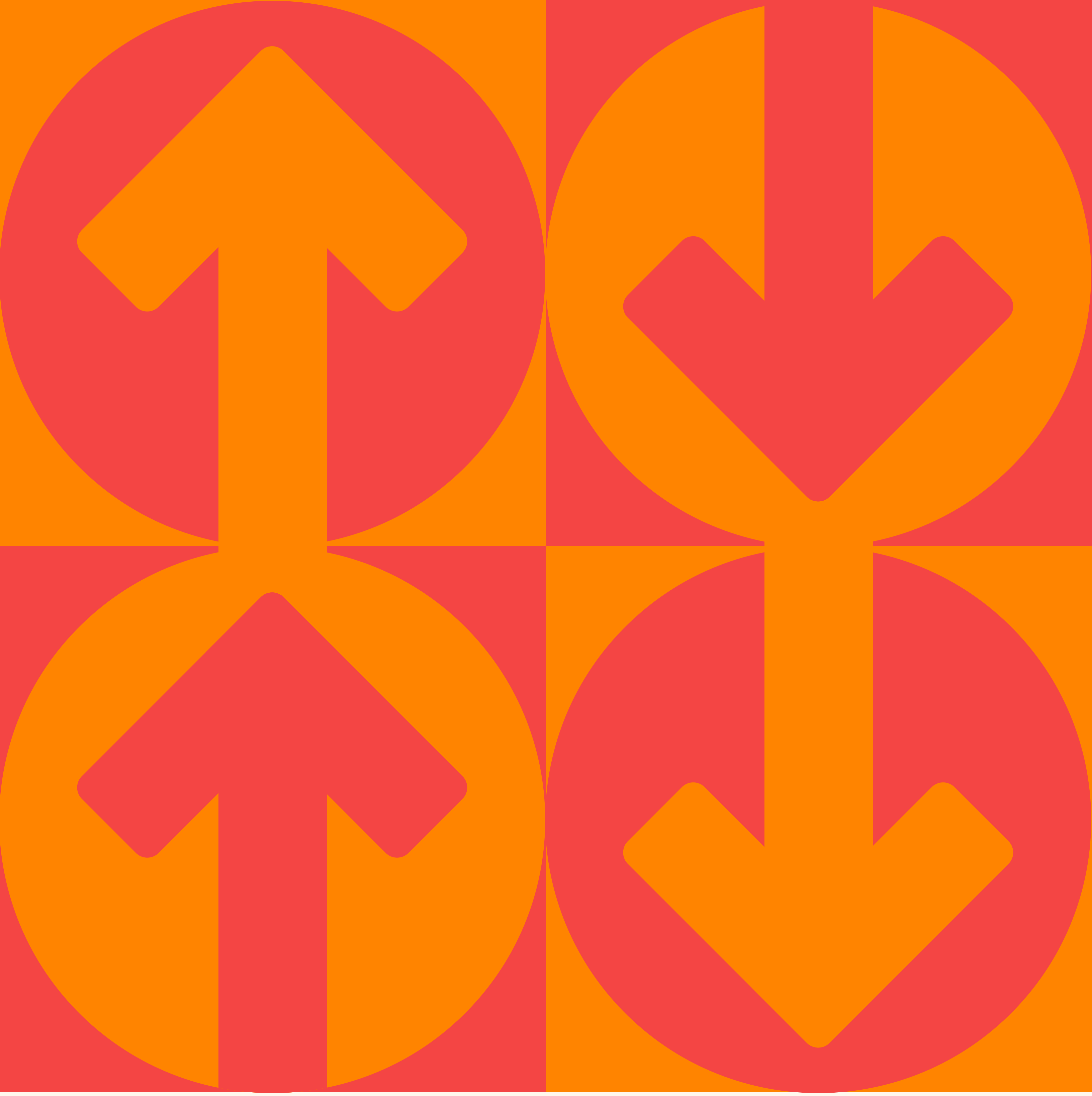


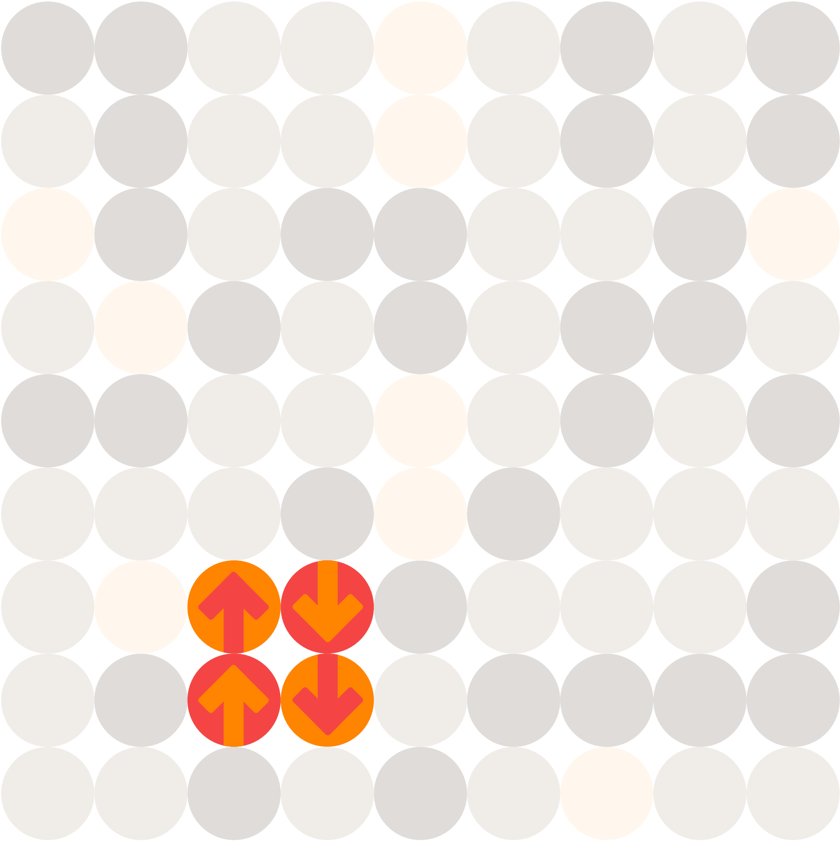
Extortion Attack Group Guide

Power Rankings: Ransomware Malicious Quartile

Q4-2024

halcyon

Table of Contents



Ransomware as a Geopolitical Tool: Russia

Ransomware has become one of the most disruptive cyber threats in recent years, impacting critical systems, endangering lives, and costing billions of dollars. However, framing ransomware attacks as solely financially motivated obscures the reality that some of these incidents serve broader geopolitical purposes.

Specifically, evidence suggests that Russia directs ransomware operators to target sectors like healthcare, energy, and food supply chains, aligning these attacks with its strategic objectives. By undermining public confidence in Western institutions while maintaining plausible deniability, Russia uses ransomware as a tool to further its geopolitical ambitions.

Framing ransomware attacks as solely financially motivated obscures the reality that some of these incidents serve broader geopolitical purposes.

The Stoli Group Incident: Evidence of Strategic Coordination?

The 2024 ransomware attack on the Stoli Group offers a clear example of how ransomware can be used as part of a coordinated strategy. The attack disrupted the company's enterprise resource planning (ERP) systems, delayed financial reporting, and forced manual operations, contributing to a $78 million debt default. Recovery efforts are expected to extend into 2025.

This cyberattack followed a series of actions by the Russian government targeting Stoli, including the seizure of the company's last remaining assets in Russia–two distilleries valued at $100 million–and the designation of Stoli and its founder, Yuri Shefler, as "extremists." These events are part of a long-standing effort by Russia to reclaim vodka trademarks once sold to private entities.

The alignment between the ransomware attack and these state actions suggests more than coincidence. Rather, it appears to be a calculated effort to weaken a company deemed adversarial to Russian interests while advancing domestic objectives. This coordination illustrates how some ransomware attacks can be assessed to be influenced by state priorities.

Evidence of Russian Influence on Ransomware Operations

The Stoli case is just one example of a broader trend linking ransomware operations to Russian interests. A report from Chainalysis revealed that 74% of ransomware revenue went to attackers with ties to Russia in 2021. Such a concentration suggests an ecosystem deeply influenced, if not outright shaped, by Russian state objectives.

Further evidence emerged with the onset of Russia's invasion of Ukraine in 2022. During this period, ransomware attacks against Western targets declined sharply, while attacks against Ukrainian entities increased. This shift indicates that ransomware operators, often seen as independent criminal groups, are responsive to geopolitical developments and may act under the guidance of the Russian government.

Groups like Conti and REvil, known for their connections to Russian intelligence, illustrate how closely intertwined some ransomware operators are with state interests. Ransomware attacks blur the distinction between criminal activity and state-sponsored operations, allowing Russia to pursue its objectives without risking direct attribution.

Ransomware operators, often seen as independent criminal groups, are responsive to geopolitical developments and may act under the guidance of the Russian government.

Ransomware's Role in Targeting Critical Infrastructure

One of the most concerning aspects of this dynamic is the focus on critical infrastructure. Attacks on sectors such as healthcare, energy, and food supply chains go beyond financial extortion. They threaten societal stability, disrupt essential services, and create long-term vulnerabilities.

For instance, ransomware attacks on healthcare systems can delay treatments, compromise patient safety, and strain resources, particularly in already overburdened systems. Attacks on energy providers or food supply chains, meanwhile, can disrupt everyday life, drive up costs, and sow uncertainty. These outcomes align with broader objectives to weaken public confidence in government and institutions.

Despite these broader impacts, ransomware attacks have largely been treated as criminal acts rather than threats to national security. While efforts by the Department of Justice to indict operators and seize funds are important, they have had limited success in deterring future attacks. Operators shielded by state actors, particularly those in Russia, remain beyond the reach of traditional law enforcement.

A Call to Reclassify Ransomware Attacks

To address this evolving threat effectively, it is essential to reframe ransomware attacks targeting critical infrastructure as national security incidents rather than isolated criminal acts. This shift in perspective would enable a more robust response, including:

- **Offensive Cyber Measures:** Disrupting the infrastructure of ransomware operators and their enablers, particularly those operating within adversarial states.
- **Economic Sanctions:** Targeting nations that harbor or sponsor ransomware groups to increase the costs of enabling these activities.
- **International Collaboration:** Strengthening intelligence sharing and coordinated actions among allied nations to counter ransomware operations more effectively.
- **Cyber Deterrence Strategies:** Establishing clear consequences for state-linked ransomware operations, potentially including proportional responses in the cyber or kinetic domains.

Attacks on sectors such as healthcare, energy, and food supply chains go beyond financial extortion. They threaten societal stability, disrupt essential services, and create long-term vulnerabilities.

The Strategic Implications of Ransomware

The volume of ransomware attacks in the US and UK targeting healthcare and food supply chains further shows that a subset of ransomware incidents is not solely financially motivated but are part of a coordinated strategy to advance geopolitical objectives. Recognizing this dual nature of ransomware is essential to developing effective responses.

Treating ransomware attacks targeting critical infrastructure as a purely cybercriminal action misses its broader implications. These attacks are not only about disrupting businesses for financial gain, they are also about eroding societal trust, creating instability, and advancing the strategic goals of states like Russia.

By reclassifying some ransomware attacks as national security threats, policymakers can unlock a wider range of tools to deter and respond to these incidents. Without this change, responses will remain limited in scope and effectiveness, leaving critical infrastructure vulnerable to ongoing exploitation.

Ransomware has evolved beyond being a tool for financial gain. For nations like Russia, it serves as a low-cost, high-impact mechanism to disrupt adversaries 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 Q4-2024, which can be reviewed along with earlier reports here: *Power Rankings: Ransomware Malicious Quartile*.

> These attacks are not only about disrupting businesses for financial gain, they are also about eroding societal trust, creating instability, and advancing the strategic goals of states like Russia.

Ransomware MQ:
Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q4-2024 Ransomware Malicious Quartile. All attack groups evaluated must be a known threat actor group in 2024 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 Q4-2024 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

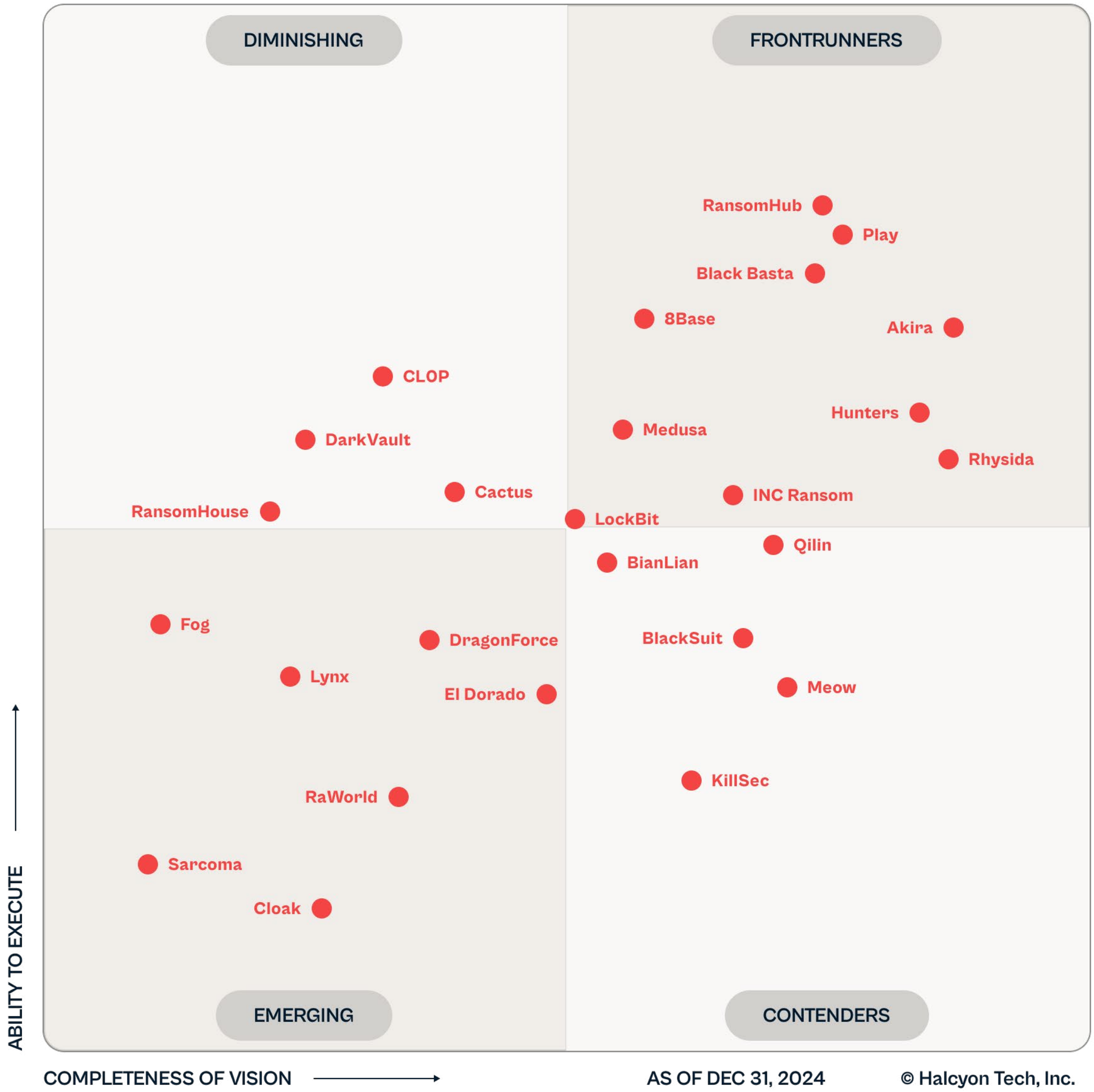
RaaS Platform Development: Attack groups were evaluated on evidence of continued development and improvement of the RaaS platform and TTPs.

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 Q4-2024 Ransomware Malicious Quartile

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



AS OF DEC 31, 2024

Source: Halcyon (Q4 2024)

Frontrunners

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 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:** RansomHub has rapidly grown to become one of the most active ransomware groups since its appearance in early 2024. Attack volume in Q4-2024 places RansomHub as the most prolific of the currently tracked RaaS groups.
- **Ransom Demands:** The group has made substantial ransom demands, evidenced by the $22 million demanded from Change Healthcare. This indicates their focus on targeting large organizations with the capacity to pay significant ransoms.
- **Victims:** Change Healthcare, City of Marietta Georgia, Bologna FC, Aras Group, Kovra, Computan, Scadea Solutions, Christie's Auction House, NRS Healthcare, Frontier Communications.

Innovation

- **RaaS Platform Development:** RansomHub has significantly advanced its RaaS platform by incorporating sophisticated techniques and capitalizing on the decline of other major ransomware groups. The platform has attracted affiliates from these disbanded operations, leveraging their expertise to enhance its own capabilities. RansomHub's code is derived

RansomHub's code is derived from Knight ransomware, which is written in Golang, and they are capable of attacking both Windows and Linux operating systems.

from Knight ransomware, which is written in Golang, and they are capable of attacking both Windows and Linux operating systems. In February 2024, it was reported that the Knight group had put its code up for sale, which likely played a pivotal role in RansomHub's development. This acquisition allowed RansomHub to rapidly integrate advanced features and improve its operational efficiency, positioning itself as a formidable player in the ransomware landscape. RansomHub employs exploitation of unpatched vulnerabilities that include critical flaws such as Citrix NetScaler ADC and NetScaler Gateway (CVE-2023-3519), which allow remote code execution; Fortinet FortiOS and FortiProxy SSL-VPN (CVE-2023-27997), enabling unauthorized access; and Microsoft Netlogon (CVE-2020-1472), or ZeroLogon, which permits attackers to seize control of domain controllers. In addition to exploiting these vulnerabilities, RansomHub uses brute-force attacks to guess weak passwords on services like Remote Desktop Protocol (RDP) and Virtual Private Networks (VPNs), gaining unauthorized access to systems. Once inside, they deploy tools like EDRKillShifter to disable Endpoint Detection and Response (EDR) solutions, ensuring their activities remain undetected. They further use PowerShell and Windows Management Instrumentation (WMI) to execute malicious scripts and commands, create new user accounts or reactivate disabled ones for persistent access, and escalate privileges within the compromised network. To expand their reach, RansomHub employs tools such as Nmap and AngryIPScanner for network reconnaissance and exploits utilities like PsExec and RDP to facilitate lateral movement. Credentials are harvested through tools like Mimikatz, enabling deeper access to systems and expanding the attack's scope. RansomHub encrypts data using algorithms such as Curve25519, ChaCha20 and AES, rendering it inaccessible without a decryption key, and deletes volume shadow copies and backups to obstruct recovery efforts, leaving victims at the mercy of their demands.

- **Targeted Industries:** Initially focusing on the healthcare sector, RansomHub's approach indicates very strategic target selection due to the high value and sensitive nature of healthcare data.

- **Economic Model**: RansomHub operates on a RaaS subscription model, indicating a structured revenue-sharing system with its affiliates, similar to other major ransomware groups. Offering up to 90% commission to affiliates, RansomHub has attracted high-profile affiliates from other prominent variants such as LockBit and ALPHV. The group has actively recruited former affiliates from disbanded ransomware operations and maintains a versatile, regularly updated codebase. This suggests a well-funded operation with a clear focus on growth and long-term sustainability.

RansomHub, like many modern ransomware groups, engages in double extortion tactics. They not only encrypt data but also steal sensitive information, which they threaten to leak if the ransom is not paid.

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

Play

Performance

- **RaaS Platform:** Play is a RaaS group that first emerged in the summer of 2022 and quickly gained prominence, due in part to its technical capabilities and the decline of other major players like LockBit and BlackCat/ALPHV. By the second quarter of 2024, Play had established itself as one of the most active and innovative groups in the RaaS space. The group operates with tactics similar to the now-defunct Hive and Nokoyawa ransomware strains, frequently exploiting unpatched Fortinet SSL VPN vulnerabilities to gain initial access to targeted networks. Play may have partnered with the North Korean state-sponsored group Andariel (aka Jumpy Pisces), which would signify a strategic escalation by enhancing Play's capabilities. Play has also exploited major vulnerabilities in Microsoft Exchange (e.g., ProxyNotShell, OWASSRF) and other systems. Play's operations are characterized by their ability to quickly adapt and innovate, making them a formidable force in the ransomware ecosystem. In the first quarter of 2024, the FBI, in partnership with CISA, issued a joint advisory highlighting the Play gang's significant impact, revealing that the group had successfully compromised over 300 organizations since its inception in June 2022. This scale of activity underscores Play's effectiveness in capitalizing on vulnerabilities and their continued rise in the cybercriminal landscape.

- **Attack Volume:** Play was one of the top three most prolific ransomware groups in 2024, breaking a record at the beginning of March 2024 by launching a massive attack that hit 16 victims simultaneously.

- **Ransom Demands:** Specific details about the ransom amounts Play demands remain scarce, but the group has consistently followed through on its threats to leak exfiltrated data from victims who refuse to pay. Play's double extortion model is highly effective, using the stolen data as leverage to increase pressure on organizations, ensuring that even if the encryption is circumvented or backups are restored, the threat of public exposure or sale of sensitive data remains a significant concern. Their strategy of leaking data on dark web forums and dedicated leak sites has cemented their reputation as a group that makes good on its promises, adding to the urgency for victims to comply with their demands.

- **Victims:** Krispy Kreme, Dairy Farmers of Canada, American Nuts, Red River Title, Rackspace, City of Lowell, Geneva Software, Primoteq, Kenya Bureau of Standards, Cambridge Group, AIGoTech, Hill Internationa, CS Cargo City of Oakland, Argentina's Judiciary, H-Hotels, Fedpol, Federal Office for Customs and Border Security (FOCBS).

Innovation

- **RaaS Platform Development:** Play is a continuously evolving RaaS platform, known for its sophisticated use of tools to disable security defenses and maintain persistence in compromised systems. One of Play's primary tools is PowerTool, which it uses to disable antivirus programs and other security monitoring solutions. For persistence, the group employs the SystemBC RAT (Remote Access Trojan), leveraging it alongside legitimate software like Plink and AnyDesk to stay active on targeted systems. Play also utilizes Cobalt Strike for lateral movement once inside a network and employs a variety of advanced techniques to further compromise systems. The group is known for using Mimikatz to harvest credentials and exploiting living-off-the-land binaries (LOLBins) to avoid detection. Play continues to exploit known vulnerabilities in public-facing applications, notably in FortiOS and Microsoft Exchange, to gain initial access to victim networks. To bypass security defenses, Play frequently uses tools such as Process Hacker, GMER, IOBit, and PowerTool, and is known to disable Windows Defender through PowerShell or command scripts. Additionally, Play abuses AdFind to perform command-line queries that help gather critical information from a target's Active Directory. The group was also the first to introduce intermittent encryption techniques, a method designed to evade detection by encrypting files in parts, making it more difficult for defenders to spot the attack early. Play has also developed custom data exfiltration tools to streamline their operations. These include the Grixba information stealer and a Volume Shadow Copy Service (VSS) copying tool, both of which are used to efficiently steal data before encryption begins. The group has been observed exploiting known vulnerabilities, such as ProxyNotShell, OWASSRF, and a remote code execution (RCE) vulnerability in Microsoft Exchange Server, to breach systems. Their use of these advanced techniques and tools highlights Play's commitment to innovation and its

Play is a continuously evolving RaaS platform, known for its sophisticated use of tools to disable security defenses and maintain persistence in compromised systems.

ability to remain a formidable force in the ransomware landscape. Play invests heavily in R&D, uses recruitment to bring in skilled affiliates, and maintains a strong technical support infrastructure.

- **Targeted Industries:** The Play ransomware gang initially concentrated much of its efforts on Latin America, with a particular focus on Brazil, while also expanding its reach to organizations outside the region. Play has intensified its focus on critical infrastructure sectors, including healthcare, government services, and financial institutions. In August 2024, Play initiated a global campaign targeting managed service providers (MSPs), exploiting their remote monitoring and management (RMM) tools to gain access to customer networks. This strategic focus on MSPs allowed the group to amplify the impact of its attacks by infiltrating multiple organizations through a single point of entry. Recent attacks have specifically focused on companies in the construction and manufacturing sectors, reflecting Play's shift toward targeting industries with critical operational processes where disruptions can result in higher ransom demands.

- **Economic Model**: Play ransomware operates with a highly efficient and structured business model, investing significantly in research and development to continuously refine its capabilities. This investment ensures the group remains at the cutting edge of ransomware technology, allowing it to evolve quickly and stay ahead of security defenses. Play reinvests profits into operational enhancements and aggressively recruits skilled affiliates to expand its reach and effectiveness. A well-maintained technical support infrastructure further strengthens its operations, providing affiliates with the tools and guidance needed for successful attacks. Much like the now-defunct Hive and Nokoyawa ransomware groups, Play utilizes double extortion tactics. After infiltrating a victim's network, the group exfiltrates sensitive data and leverages it as an additional layer of pressure. If ransom demands are not met, Play threatens to release the stolen data on their public leak site, adding reputational damage and regulatory penalties to the cost of a breach. This two-pronged approach–encryption and data theft–has proven highly lucrative, making Play one of the more formidable ransomware operations in the current cybercriminal landscape.

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

Black Basta

Performance

- **RaaS Platform:** Black Basta is a RaaS group that first appeared in early 2022, with some cybersecurity researchers speculating that it may be an offshoot of the disbanded Conti and REvil groups. Known for its aggressive tactics and technical proficiency, Black Basta has been actively exploiting vulnerabilities such as ConnectWise (CVE-2024-1709). They have also stolen credentials from Initial Access Brokers (IABs), to gain initial access to networks. Black Basta has adopted sophisticated social engineering methods, including email bombing and impersonation of IT personnel via Microsoft Teams. Black Basta follows a double extortion model, routinely exfiltrating sensitive data from victims to increase the pressure to pay ransoms. This stolen data is often threatened to be published or sold if the victim refuses to meet their demands, amplifying the potential damage and reputational risk for the affected organizations. The group focuses on highly targeted, sophisticated attacks and is believed to work exclusively with a small, carefully vetted group of affiliates, ensuring tighter control over their operations. This selective collaboration model allows Black Basta to maintain a high level of operational security and effectiveness, targeting organizations across various sectors, including finance, healthcare, and manufacturing, where the stakes are high and the potential for large ransom payouts is significant. Their ability to exploit vulnerabilities and use advanced tactics has made Black Basta a prominent player in the ransomware landscape.
- **Attack Volume:** Black Basta remains one of the most prolific attack groups in 2024 and was observed leveraging unique TTPs for ingress, lateral movement, data exfiltration data, and deployment of ransomware payloads.
- **Ransom Demands:** Ransom demands from Black Basta 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.
- **Victims:** BT Conferencing, KMC Global, Southern Water, BionPharma, M&M Industries, coca Cola, Yellow Pages Canada, AgCo, Capita, ABB, Merchant Schmidt, Tag Aviation, Blount Fine Foods.

> Black Basta focuses on highly targeted, sophisticated attacks and is believed to work exclusively with a small, carefully vetted group of affiliates, ensuring tighter control over their operations.

Innovation

- **RaaS Platform Development:** Black Basta is known for its sophisticated ransomware that targets both Windows and Linux systems with notable proficiency in exploiting vulnerabilities in VMware ESXi, a common enterprise server platform. Their ransomware, developed in C++, uses ChaCha20 encryption for data and RSA-4096 for encrypting the encryption key, ensuring rapid and robust encryption across affected networks. The group has been observed using advanced techniques during attacks, including deploying malware strains such as Qakbot and exploiting vulnerabilities like PrintNightmare. They frequently exploit insecure Remote Desktop Protocol (RDP) configurations, which remain a common and effective entry point for ransomware. Black Basta can disable security tools like Windows Defender using batch files with PowerShell commands and Group Policy Objects (GPOs) to disable anti-malware, making their attacks even more difficult to detect and mitigate. The group employs a range of tools to facilitate their attacks, including SystemBC, a remote access trojan used to maintain persistent access, and Cobalt Strike for lateral movement within networks. Black Basta is also known for its meticulous approach to affiliate recruitment, working with a carefully selected group of attackers to execute highly targeted operations.

- **Targeted Industries:** Black Basta typically targets manufacturing, transportation, construction and related services, telecommunications, the automotive sector, and healthcare providers.

- **Economic Model**: Black Basta operates a double extortion scheme, maintaining an active leak site where they publish stolen data if the ransom is not paid. The group typically retains around 14% of the ransom payments, with the rest being distributed among their affiliates.

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

8Base

Performance

- **RaaS Platform:** The 8Base ransomware gang, which emerged in March 2022, has quickly become one of the most active and prominent threat actors in the cyber landscape. Their activity surged significantly in the first half of 2024, establishing them as a major threat. The sophistication of their operations and tactics suggests that they may be an offshoot of experienced RaaS operators, potentially linked to RansomHouse, a data extortion group that surfaced in December 2021 and was highly active in late 2022 and early 2023. There are also indications that 8Base may have connections to the leaked Babuk ransomware builder. 8Base employs double extortion tactics, exfiltrating victim data before deploying ransomware, and is known for using advanced techniques to evade security measures. This includes modifying Windows Defender Firewall settings to bypass protections and enhance their operational effectiveness. The group's rapid growth and sophisticated methods reflect a deep understanding of both ransomware operations and security evasion strategies.

- **Attack Volume:** 8Base quickly ascended the ranks of active ransomware operators with a high volume of attacks throughout 2023 and throughout 2024, making them one of the most active groups.
- **Ransom Demands:** It is unclear how much 8Base typically demands for a ransom, but 8Base ransomware typically issues aggressive ransom demands, combining high monetary requests with threats to publicly release stolen data if victims fail to pay promptly.
- **Victims:** Volkswagen Group, Inno Group, GPI Corporate, Lyon Terminal, East Coast Fisheries, Keystone Insurance Services, Spectra Industrial, Kansas Medical Center, Danbury Public Schools, BTU, Advanced Fiberglass Industries, ANL Packaging.

Innovation

- **RaaS Platform Development:** While 8Base does not maintain a distinct ransomware strain or a public RaaS platform for affiliate recruitment, it is believed to collaborate privately with a select group of vetted affiliates. The group frequently employs a variety of ransomware payloads and loaders, with customized versions of Phobos–often paired with SmokeLoader–being the most prevalent. 8Base is known for its rapid and efficient encryption techniques, typically appending a unique ".8base" extension to encrypted files. They have demonstrated the capability to bypass Windows Defender's Advanced Firewall and routinely erase Volume Shadow Copies (VSS) to hinder data recovery. Although their primary focus remains on Windows systems, with no evidence of targeting Linux environments, they have continued to deploy a new variant of Phobos ransomware, primarily delivered via SmokeLoader. The group employs tools like Mimikatz to harvest credentials, enabling further access and privilege escalation within the compromised network, and leverage tools such as SoftPerfect network scanner to identify potential targets within the network and PsExec and

> 8Base frequently employs a variety of ransomware payloads and loaders, with customized versions of Phobos–often paired with SmokeLoader–being the most prevalent.

Remote Desktop Protocol (RDP) to move laterally across the network. They delete shadow copies to prevent victims from restoring their systems without paying the ransom.

- **Targeted Industries:** 8Base primarily targets organizations in the financial, healthcare, and information technology sectors, but about half of the targets are in the business services, manufacturing, and construction sectors.
- **Economic Model**: 8Base does not appear to maintain a RaaS program open to affiliate attackers, appearing to be opportunistic in their choice of victims with a focus on "name and shame" via their leaks site to compel payment of the ransom demand.

Akira

Performance

- **RaaS Platform:** Akira emerged in March 2023 and quickly gained prominence as one of the most active ransomware groups in 2024. While there are suspicions that Akira may be linked to the infamous Conti gang, especially given the Conti code was leaked in 2022, definitive connections remain unconfirmed. Following a period where they primarily engaged in data theft without encryption, Akira has returned to encrypting victims' files in addition to data exfiltration, reinstating their double-extortion tactics. Akira's distinctive extortion platform includes a chat feature, which facilitates direct negotiation between victims and attackers–an unusual practice among ransomware groups. This feature has sometimes led Akira to disclose specific infection vectors to victims who have paid the ransom, diverging from the common approach of reusing the same vulnerabilities in multiple attacks. Despite the release of a decrypter that was purportedly effective on earlier versions or less common samples of Akira's ransomware, it has proven largely ineffective for full data recovery. The group's innovative approach and high activity levels in 2024 highlight their sophisticated operational capabilities.
- **Attack Volume:** Akira maintains a growing attack volume, putting them among the leaders when compared to other ransomware operators. They have collected more than $50 million in ransom for over 300 victims.
- **Ransom Demands:** Ransom demands appear to range between $200,000 to more than $4 million.

Following a period where they primarily engaged in data theft without encryption, Akira has returned to encrypting victims' files in addition to data exfiltration, reinstating their double-extortion tactics.

- **Victims:** Nissan, MSR Group, Royal College of Physicians and Surgeons, 4LEAF, Park-Rite, Family Day Care Services, The McGregor, Protector Fire Services, QuadraNet Enterprises, Southland Integrated

Innovation

- **RaaS Platform Development:** Akira developed a Rust-based variant specifically designed to attack VMware ESXi servers. After experimenting with Rust-based variants, Akira has reverted to using C++ for both Windows and Linux encryptors. The group is known for exploiting VPN credentials to gain initial access and employs a range of advanced techniques to execute their attacks. Their ransomware modules are specifically designed to delete Windows Shadow Volume Copies using PowerShell, ensuring that backup copies of encrypted files cannot be easily restored. Akira's ransomware encrypts a wide variety of file types, but it intentionally avoids system files with extensions such as .exe, .lnk, .dll, .msi, and .sys to prevent system instability and detection. Akira operators use tools like Mimikatz to extract credentials from compromised systems, enabling further access and privilege escalation and employ tools to disable endpoint detection and response (EDR) solutions. Akira affiliates utilize tools such as SoftPerfect network scanner to identify potential targets within the network and leverage tools like PsExec and Remote Desktop Protocol (RDP) to move laterally across the network. To evade detection, Akira utilizes legitimate Living-off-the-Land Binaries (LOLBins) and commercial off-the-shelf (COTS) tools like PCHunter64, which complicates the identification of their activities. In July 2023, the group expanded their operations with a Linux variant of their ransomware. By August 2023, Akira was observed remotely exploiting zero-day vulnerabilities (CVE-2020-3259 and CVE-2023-20269) in Cisco VPN offerings. In the latter half of 2024, affiliates of Akira have been observed exploiting a vulnerability in SonicWall devices (CVE-2024-40766) to gain initial access. The group has also been seen leveraging VMware ESXi vulnerabilities to facilitate lateral movement within compromised networks.

- **Targeted Industries:** Akira targets organizations in Latin America, with a notable emphasis on the healthcare sector. Despite this regional focus, the group extended its attacks to a diverse array of industries, including education, finance, and manufacturing. Their broad targeting strategy underscores their aim to maximize impact, and ransom yields across multiple sectors.

- **Economic Model**: Akira employs a double extortion strategy, incorporating data exfiltration as a key component of their operations. They not only encrypt victim data but also threaten to expose or sell the stolen information if ransom demands are not met. The group has reportedly leaked gigabytes of stolen data from various victims, amplifying the pressure on targets to comply with their demands.

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

Hunters International

Performance

- **RaaS Platform:** Hunters International is a RaaS group that emerged in October 2023, following the disruption of the Hive ransomware group by law enforcement agencies earlier that year. Building on Hive's advanced infrastructure, Hunters International has adopted a sophisticated platform that leverages both data exfiltration and double extortion tactics. The latest iteration of Hunters International has evolved from its previous methods. Unlike earlier practices where the decryption key was stored separately, the new variant now embeds the key directly within the encrypted file. This approach aligns with more common ransomware practices, streamlining the decryption process while maintaining pressure on victims to comply with ransom demands.
- **Attack Volume:** The attack volume for Hunters International has been substantial, with numerous campaigns launched throughout 2024 targeting a broad range of industries and geographies, indicating a significant operational capacity.
- **Ransom Demands:** The exact figures of their demands have varied widely, adapting to the perceived ability of the victim to pay.
- **Victims:** Toyota Brazil, Jones and Mayer, KMC Controls, Aeris Energy, NanoLumens, Integrated Control, Frederick Wildman and Sons, Kablutronik SRL, Caxton and CTP Publishers and Printers, Austal USA.

Innovation

- **RaaS Platform Development:** Initially casting a wide net across various sectors, Hunters International has since refined its targeting to focus on industries with high ransom potential. The group now primarily targets healthcare, financial services, and critical infrastructure–sectors where rapid recovery and the handling of sensitive data make organizations more likely to meet ransom demands. Hunters International is known to gain initial access via phishing emails, social engineering, supply chain attacks, and Remote Desktop Protocol (RDP) and utilize tools to disable endpoint detection and response (EDR) solutions. The group employs tools like Mimikatz to harvest credentials, enabling further access and privilege escalation within the compromised network and have been observed creating new domain accounts to establish persistence within the victim's network. Hunters International operators use tools such as SoftPerfect network scanner to identify potential targets within the network and utilize tools like PsExec and Remote Desktop Protocol (RDP) to move laterally across the network while delete shadow copies to prevent victims from restoring their systems. In mid-2024, the group introduced a new Remote Access Trojan (RAT) named SharpRhino, written in C#. Delivered through typosquatting domains impersonating legitimate tools like Angry IP Scanner, SharpRhino establishes persistence and provides attackers with remote access. Leveraging Hive's technology, Hunters International has intensified efforts to improve the efficiency and reliability of its operations. They have advanced their encryption techniques to better counteract common decryption tools and have integrated more sophisticated data exfiltration methods. This evolution underscores their strategic focus on maximizing impact and ensuring that their extortion tactics remain effective against high-value targets.

- **Targeted Industries:** Hunters International has targeted various sectors, including healthcare, finance, and critical infrastructure, with notable attacks on defense contractors and large corporations.

- **Economic Model**: Hunters International operates on a profit-sharing model like other RaaS platforms, offering affiliates a share of the ransom proceeds for successfully deploying their ransomware. This incentivizes the widespread distribution of their malware.

> Hunters International is known to gain initial access via phishing emails, social engineering, supply chain attacks, and Remote Desktop Protocol (RDP) and utilize tools to disable endpoint detection and response (EDR) solutions.

Medusa

Performance

- **RaaS Platform:** Medusa, a RaaS platform that emerged in the summer of 2021, has ascended to become one of the most active and formidable ransomware groups. By the second quarter of 2024, Medusa's attack volumes had surged significantly, positioning it as one of the top ransomware threats in the landscape. The group has been observed targeting a vulnerability in Fortinet's FortiClient EMS software (CVE-2023-48788) and employs a range of sophisticated techniques to evade detection and complicate recovery efforts. Medusa is known for restarting infected machines in safe mode to bypass security software and implementing measures that hinder data recovery. These include deleting local backups, disabling startup recovery options, and wiping Volume Shadow Copies (VSS) to prevent encryption rollback. Such tactics underscore Medusa's focus on maximizing the impact of its attacks and ensuring that victims face severe challenges in recovering their data.
- **Attack Volume:** Medusa is not the most prolific ransomware group, but it has been one of the more consistent threat groups throughout 2024. Medusa has notably intensified its ransomware campaigns late in the year, targeting a diverse range of sectors including healthcare, manufacturing, and education.
- **Ransom Demands:** Medusa typically demands ransoms in the millions of dollars which can vary depending on the target organization's ability to pay. Ransom demands have progressively risen over time, often tailored to the victim's organizational size and data sensitivity, leveraging double-extortion tactics to maximize pressure and payment outcomes.
- **Victims:** Toyota Financial Services, Kela Health, Fancy Foods, Tarrant County Appraisal District, Kansas City Area Transportation Authority, Traverse City Schools, SIMTA, ATI Traduction, EDB, Symposia Organizzazione Congressi S.R.L, Believe Productions, Global Product Sales, ZOUARY & Associés, Neodata, Evasión.

Medusa is known for restarting infected machines in safe mode to bypass security software, deleting local backups, disabling startup recovery options, and wiping Volume Shadow Copies (VSS) to prevent encryption rollback.

Innovation

- **RaaS Platform Development:** The Medusa RaaS operation typically gains access to victim networks through various methods. These include brute-forcing Remote Desktop Protocol (RDP) credentials, deploying malicious email attachments with embedded macros, distributing malware via torrent websites, or leveraging malicious ad libraries. Once inside a network, Medusa demonstrates significant control over system processes. The ransomware can terminate over 280 Windows services and processes without requiring command line arguments, although it is not yet confirmed whether a Linux version exists. Medusa employs AES-256 encryption for file encryption, combined with an RSA public key for additional security. Medusa utilizes advanced tools and techniques, including the deployment of custom malware like 'gaze.exe' and the use of legitimate remote monitoring and management (RMM) tools to establish persistence within victim networks. Medusa extensively uses legitimate system tools and services, such as PowerShell and Remote Desktop Protocol (RDP), to execute malicious commands, making detection more challenging. The group employs tools like Mimikatz to harvest credentials and tools such as Netscan to identify potential targets within the network while deleting shadow copies and backups to prevent victims from restoring their systems. In September 2024, Medusa released an updated variant that further complicates recovery efforts by offering faster encryption speeds and enhanced backup deletion capabilities. This new version continues to disable over 200 services, reinforcing Medusa's strategy of making data recovery as difficult as possible for its victims.

- **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 utilizes a double extortion strategy, exfiltrating data before encryption to increase pressure on victims. However, unlike some other RaaS groups, Medusa is less generous with its affiliates, offering them up to 60% of the ransom proceeds.

Rhysida

Performance

- **RaaS Platform:** Rhysida, a RaaS operation first identified in May 2023, rapidly emerged as a significant threat in early 2024. The group employs sophisticated techniques for network infiltration and persistence, such as exploiting VPN vulnerabilities and leveraging flaws like Zerologon (CVE-2020-1472) to gain initial access. Rhysida operates with a double extortion strategy, exfiltrating sensitive data and threatening its release if ransom demands are not met. The group maintains a leaks site and a victim support portal on the Tor network, providing a platform for negotiations and updates. In February 2024, researchers released a decryptor for Rhysida's ransomware, which temporarily disrupted their operations. However, the group quickly adapted and resumed its activities.
- **Attack Volume:** After a period of low activity in early Q2 2024 following the public release of a decryptor, Rhysida has updated their encryptor and experienced a resurgence in the latter half of 2024. However, their attack volume remains modest compared to leading ransomware groups. Rhysida appears to operate as opportunistic attackers.
- **Ransom Demands:** Ransome demands are based in Bitcoin and have been seen to range from 15 BTC ($775,000) to 60 BTC ($3.7 million) in recent attacks.
- **Victims:** Axis Health, SEATAC Airport, MarineMax, Lurie Children's Hospital, Pierce College at Joint Base Lewis McChord, Ejercito de Chile, Axity, Ministry of Finance Kuwait, Prince George's County Public Schools, Ayuntamiento de Arganda City Council, Comune di Ferrara, Prospect Medical Holdings, Martinique Government.

Rhysida employs sophisticated techniques for network infiltration and persistence, such as exploiting VPN vulnerabilities and leveraging flaws like Zerologon to gain initial access.

Innovation

- **RaaS Platform Development:** Rhysida operates a sophisticated RaaS platform with advanced capabilities designed to evade detection and enhance operational efficiency. Their tactics include bypassing antivirus defenses, deleting Volume Shadow Copies (VSS) to obstruct encryption rollback, and modifying Remote Desktop Protocol (RDP) settings to maintain persistence. The group utilizes Cobalt Strike or similar command-and-control frameworks for managing compromised systems, employs PSExec for lateral movement within networks, and leverages PowerShell scripts to deliver their ransomware payload. Rhysida's ransomware encrypts files using a combination of AES-CTR for encryption and a 4096-bit RSA key for key management. Initially targeting only Windows environments, Rhysida has recently expanded its operations to include a Linux variant aimed at VMware ESXi servers. They use scheduled tasks to establish persistence in compromised hosts, ensuring the ransomware executes upon system startup. Their tactics, techniques, and procedures (TTPs) show notable similarities to those of the Vice Society group, suggesting a possible connection or shared methodology between the two operations.

- **Targeted Industries:** The group targets large organizations across various sectors, including education, healthcare, manufacturing, information technology, and government, primarily in the Middle East, Latin America, and Europe.

- **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

INC Ransom

Performance

- **RaaS Platform:** INC Ransom emerged in the summer of 2023, and it remains uncertain whether they operate as a RaaS platform with affiliates or as a more closed, internal group. The group employs a range of established tactics, techniques, and procedures (TTPs) commonly used in ransomware operations. This includes leveraging compromised Remote Desktop Protocol (RDP) credentials for initial access and lateral movement within victim networks. Their initial infections have been traced back to phishing campaigns and the exploitation of a vulnerability in Citrix NetScaler (CVE-2023-3519). Despite their criminal activities, INC Ransom portrays itself as a "moral agent," claiming to assist victims by exposing vulnerabilities in their cybersecurity defenses. This self-styled justification adds a layer of complexity to their motives, distinguishing them from other ransomware operators.

- **Attack Volume:** INC did not emerge until the second half of 2023, but the cadence of attacks has been increasing throughout 2024.
- **Ransom Demands:** INC instructs victims to log into a Tor portal with a unique user ID provided by the attackers. INC ransomware's ransom demands have consistently escalated over time, leveraging double-extortion tactics with significant financial requirements tailored to the victim's size and the sensitivity of the stolen data.
- **Victims:** Peruvian Army, Alna Bioscience, Quantum Healthcare, NHS Scotland, Xerox, Trylon Corp, BPG Partners Group, DM Civil, Nicole Miller INC., Pro Metals, Springfield Area Chamber of Commerce, US Federal Labor Relations Authority, Yamaha Philippines, Rockford Public Schools.

Innovation

- **Raas Development:** It is currently unclear whether INC Ransom operates as a traditional RaaS with affiliates. INC Ransom has been observed employing a range of techniques to deploy their ransomware, utilizing legitimate tools and Living-off-the-Land (LOTL) methods to avoid detection. They use tools such as WMIC and PsExec for deploying ransomware, which implies they likely employ techniques to bypass traditional security tools. They also exploit common applications like MSPaint, WordPad, Notepad, MS Internet Explorer, MS Windows Explorer to facilitate lateral movement within compromised networks, TightVNC for remote control, and PowerShell scripts to execute commands, making detection more challenging. Threat actor Vanilla Tempest (aka Vice Society) has been observed utilizing INC ransomware in attacks against U.S. healthcare organizations. The collaboration involves initial access facilitated by the Gootloader malware downloader, followed by lateral movement using tools like AnyDesk and the deployment of the INC ransomware payload. For reconnaissance, INC Ransom leverages tools such as Esentutl, and uses MegaSync for data exfiltration, which suggests they are leveraging cloud services to efficiently steal data. The ransomware itself is written in C++ and uses AES-128 encryption in CTR mode to secure files. Additionally, a Linux variant of the ransomware has been reported. While it is not entirely clear whether INC Ransom employs advanced security evasion techniques, there are indications that they may delete Volume Shadow Copies (VSS) to hinder recovery efforts and obstruct encryption rollback. This suggests a level of sophistication in their approach to disrupting victim recovery efforts.

INC exploits common apps like MS Paint, WordPad, Notepad, Internet Explorer, Windows Explorer to facilitate lateral movement, TightVNC for remote control, and PowerShell scripts to execute commands, making detection more challenging.

- **Targeted Industries:** INC targets a wide array of industries, including education, manufacturing, retail, IT, hospitality, pharma, construction, and the public sector.

- **Economic Model**: INC employs double extortion tactics and operates a leak site where they threaten to publish victims' sensitive data if ransom demands are not met. They have followed through on these threats by exposing compromised data when targets refuse to pay.

LockBit

Performance

- **RaaS Platform:** LockBit, a prominent RaaS platform that has been active since 2019, is recognized for its sophisticated evasion techniques and exceptionally rapid encryption speed. The group utilizes multiple extortion strategies, often demanding separate ransoms for decrypting files and for any sensitive data they exfiltrate. For data exfiltration, LockBit employs a mix of publicly available file-sharing services, and a proprietary tool called Stealbit. In February 2024, LockBit's operations faced a significant disruption when an international law enforcement task force, Operation Cronos, temporarily took control of their administrative infrastructure. Despite this setback, the group resumed its activities within days. Although LockBit remains operational, there are suspicions that the group may be overstating its involvement in certain high-profile attacks, such as an alleged breach of the US Federal Reserve, potentially to maintain its reputation and influence among affiliates. In December 2024, the U.S. Department of Justice announced charges against Rostislav Panev, a dual Russian Israeli national, for his role as a developer within the LockBit group. LockBit ransomware, despite significant law enforcement actions, is poised to return with its fourth iteration, LockBit 4.0, set to launch on February 3, 2025.

LockBit ransomware, despite significant law enforcement actions, is poised to return with its fourth iteration, LockBit 4.0, set to launch on February 3, 2025.

- **Attack Volume:** LockBit was especially active in May and June 2024, carrying out over 200 ransomware attacks, which accounted for a significant share of the ransomware incidents reported during that period. While LockBit remains the most prolific ransomware operation to date, there are emerging signs of decline in their activity.

- **Ransom Demands:** LockBit is known for issuing some of the highest ransom demands in the ransomware landscape, with requests reaching up to $50 million or more. Notably, in July 2023, they demanded $70 million from Taiwan Semiconductor Manufacturing Company (TSMC). The group has achieved significant financial success, with total reported ransom payments reaching the hundreds of millions of dollars, underscoring the immense profitability of their operations. LockBit's ransom demands are typically tailored to the victim's perceived ability to pay, reflecting a strategic approach to maximize financial gain from each attack.

- **Victims:** Fulton County, Allegheny Health, Ford Country Americas, Industrial and Commercial Bank of China (ICBS), Alphadyne Asset Management, Boeing, SpaceX, Shakey's Pizza, Banco De Venezuela, GP Global, Kuwait Ministry of Commerce, MCNA Dental, Bank of Brazilia, Endtrust, Bridgestone Americas, Royal Mail.

Innovation

- **RaaS Platform Development:** LockBit's operational maturity is evident in its continuous development and refinement of administrative tools and platforms. After releasing LockBit 3.0 in June 2022, the group made headlines by introducing what is believed to be the first macOS ransomware variant in April 2023. Despite this innovation, there have been few significant changes to the platform since then. LockBit 3.0 is known for its advanced anti-analysis features and supports attacks on both Windows and Linux systems. The ransomware employs a modular design, allowing for various execution modes that dictate its behavior on compromised systems. It utilizes a custom Salsa20 algorithm for file encryption and commonly exploits Remote Desktop Protocol (RDP) to gain initial access. Once inside, it spreads across networks using Group Policy Objects and PsExec through the Server Message Block (SMB) protocol. Interestingly, LockBit continues to support its earlier 2.0 variant, with some victims being encrypted by LockBit 2.0 but listed on the LockBit 3.0 leak site. In Q1 2024, LockBit operators were notably observed exploiting the Citrix Bleed vulnerability (CVE-2023-4966) as part of their attack strategies.

- **Targeted Industries:** LockBit tends to target larger enterprises across any industry vertical with the ability to pay high ransom demands, but also have tended to favor Healthcare organizations, financial services, and government agencies.

- **Economic Model**: LockBit has long been recognized for its highly organized affiliate program, which has earned a strong reputation within the attacker community. The platform is well-regarded for its sophistication and the substantial payouts it offers, with affiliates receiving up to 75% of the ransom proceeds. This attractive payout structure and the platform's maturity made LockBit a popular choice among ransomware operators.

However, recent law enforcement actions, including the notable takedown efforts by Operation Cronos, have reportedly impacted LockBit's affiliate base. There are indications that these legal actions may have led to a significant loss of affiliates, potentially disrupting the group's operations and its ability to execute large-scale attacks as effectively as before.

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

Contenders

Qilin

Performance

- **RaaS Platform:** Qilin initially operated under the name Agenda before rebranding is a RaaS operation that first appeared in July 2022. Qilin is written in Golang and Rust, making it capable of targeting both Windows and Linux systems. Rust, known for its security and cross-platform capabilities, provides excellent performance for concurrent processing, helping Qilin evade security measures and develop variants targeting multiple operating systems. Qilin operators are also known to exploit vulnerabilities in applications like Remote Desktop Protocol (RDP) to gain access to victim networks. In summer of 2024, Qilin was observed deploying scripts to extract credentials stored in Google Chrome browsers across compromised networks.

- **Attack Volume:** Qilin's attack volume surged significantly in 2024, with the group claiming over 150 victims by the third quarter. Notably, Qilin is believed to be behind a major attack on the UK healthcare provider Synnovis, which severely disrupted patient care across the National Health Service (NHS).

- **Ransom Demands:** Ransom demands typically range between $50,000 to $800,000, with affiliates receiving 80-85% of the ransom depending on the amount. Larger payments over $3 million yield a higher percentage cut for affiliates.

- **Victims:** Synnovis, NHS Hospitals, Propak, PetroSpouth, Big Issue Group, Ditronics Financial Services, Daiwa House, ASIC S.A., Thonburi Energy Storage, SIIX Corporation, WT Partnership Asia, FSM Solicitors, Etairos Health, Commonwealth Sign, Casa Santiveri.

Halcyon researchers first observed in fall of 2024 that Qilin upgraded their ransomware variant, known as Qilin.B, incorporating advanced encryption methods that disrupt backup processes and enhance evasion capabilities.

Innovation

- **RaaS Platform Development:** Halcyon researchers first observed in fall of 2024 that Qilin upgraded their ransomware variant, known as Qilin.B, incorporating advanced encryption methods that disrupt backup processes and enhance evasion capabilities. Qilin.B combines AES-256-CTR encryption for systems with AESNI capabilities while retaining Chacha20 for other systems and uses RSA-4096 with OAEP padding to protect encryption keys, making file decryption without the private key or captured seed values impossible. Written in Rust, Qilin.B terminates services associated with security tools, clears Windows Event Logs to hinder forensic analysis, and deletes itself to reduce traces of its presence, making detection and response or attempts to reverse-engineer the payload more difficult. Qilin.B disrupts system backup efforts by deleting volume shadow copies (VSS) which thwarts critical recovery mechanisms. These improvements make detection and mitigation more challenging for targeted organizations. The Qilin RaaS offers multiple encryption techniques, including ChaCha20, AES-256, and RSA-4096, giving operators several configuration options when conducting the attack. The Qilin ransomware is designed to target both Windows and Linux systems, with particular emphasis on Linux environments running on VMware ESXi hypervisors. The Linux variant is compiled using GCC 11, a widely used compiler, and utilizes OpenSSL for securing public key encryption, ensuring robust encryption of sensitive data during attacks. This combination of technologies makes Qilin adaptable and highly effective in targeting virtualized Linux infrastructures. Qilin affiliates have been observed employing credential harvesting techniques, particularly targeting Chrome browser credentials through the use of PowerShell scripts. Qilin continues to exploit well-known vulnerabilities in widely used software, such as Fortinet devices and Veeam Backup & Replication software, to gain initial access to target networks.

- **Targeted Industries:** Qilin is assessed to be a big game hunter selecting targets for their ability to pay large ransom demands, as well as targeting the healthcare and education sectors.
- **Economic Model**: Qilin employs a double extortion strategy, exfiltrating data and threatening to expose or sell it on their leak site if victims refuse to meet their demands. Their affiliate program offers an 80% share of ransoms below $3 million and 85% for ransoms exceeding $3 million.

BianLian

Performance

- **RaaS Platform:** BianLian is not a traditional RaaS operation. Initially emerging in June 2022 with a Golang-based ransomware, they operated like a typical RaaS provider until a free decryption tool was released, enabling victims to recover their encrypted files. Despite this, BianLian successfully targeted several high-profile organizations. They utilize various hosting providers and a broad range of ports to evade detection. In early 2023, BianLian shifted away from deploying ransomware payloads, focusing instead on simpler data exfiltration and extortion attacks. This shift highlights the effectiveness of double extortion tactics, which have become increasingly popular among ransomware groups. While not the most prolific, BianLian has maintained steady, long-term operations, establishing itself as one of the more successful groups in the cybercrime landscape.
- **Attack Volume:** BianLian has ramped up its attack volume after shifting away from ransomware payloads in favor of pure data extortion attacks, solidifying its position as one of the more prominent groups. While they continue to target new victims weekly, as evidenced by updates on their leak sites, the pace of attacks has slowed in 2024.
- **Ransom Demands:** BianLian focuses primarily on threats of leaking stolen data to compel payment. It is unclear how much BianLian typically requests for a ransom amount, or if they are keen to negotiate the demand down.
- **Victims:** Air Canada, Healthcare Management Systems, L&B Transport, Griffing & Company, International Biomedical Ltd, Gilbreath, Dow Golub Remels & Gilbreath, Instron, Pelindo, CHU de Rennes, Dekko Window Systems Ltd, CMC Marine.

Innovation

- **RaaS Platform Development:** BianLian long ago abandoned the RaaS model, focusing instead on pure data extortion attacks where they exfiltrate data and issue ransom demands without deploying ransomware. The group utilizes open-source tools and command-line scripts for credential harvesting and data exfiltration. They have also been observed deploying a custom Golang-based backdoor for remote access, while using PowerShell and Windows Command Shell to evade and bypass security defenses.

BianLian utilizes open-source tools and command-line scripts for credential harvesting and data exfiltration, deploy a custom Golang-based backdoor for remote access, and leverage PowerShell and Windows Command Shell to evade security defenses.

- **Targeted Industries:** BianLian primarily targeted critical infrastructure, financial institutions, healthcare, manufacturing, education, entertainment, and energy sectors. More recently they have been observed attacking the legal sector.

- **Economic Model**: Now operating almost exclusively as a data extortion group, BianLian is rarely seen deploying ransomware payloads. Their operations are extensive, focusing on data theft, extortion, and employing a range of exfiltration tools to carry out their attacks.

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

BlackSuit

Performance

- **RaaS Platform:** BlackSuit operates as a private ransomware group rather than a traditional RaaS with affiliates. In August 2024, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) confirmed that the Royal ransomware group had rebranded as BlackSuit, affirming observations such as both using OpenSSL's AES encryption with intermittent encryption techniques to speed up the process while evading detection. Some sources suggest that BlackSuit may be a rebranding of Royal, which itself was a rebranding of Conti. The group targets both Windows and Linux systems.

- **Attack Volume:** BlackSuit has quickly gained notoriety for striking a variety of sectors with considerable impact, and activity in 2024 has been consistently high.

- **Ransom Demands:** BlackSuit's focus on large enterprises and critical sectors indicates that their demands are likely significant. The group customizes ransom demands based on the financial capacity of each victim, aiming to make the amount seem "reasonable" and more likely to be paid. BlackSuit has issued ransom demands that combined have exceeded $500 million, with individual demands reaching up to $60 million.

- **Victims:** ZooTampa, SVP Worldwide, Southwest Binding & Laminating, Western Municipal Construction, CDK Global, Kansas City Police Department, Multi-Fill.

BlackSuit utilize tools such as Cobalt Strike for command execution, making detection more challenging and tools to harvest credentials, enabling further access and privilege escalation within the compromised network.

Innovation

- **RaaS Platform Development:** BlackSuit operates with a high degree of secrecy, keeping its tactics and developments well-protected. Unlike many ransomware groups that depend on affiliate networks, BlackSuit maintains strict control over its operations, likely as a strategic move to enhance operational security and maximize profits. They utilize tools such as Cobalt Strike for command execution, making detection more challenging and tools to harvest credentials, enabling further access and privilege escalation within the compromised network. BlackSuit operators use Remote Desktop Protocol (RDP) and PsExec to move laterally within the network and create or modify user accounts to maintain persistence and escalate privileges as well as deleting shadow copies and backups to prevent victims from restoring their systems without paying the ransom.
- **Targeted Industries:** While BlackSuit has attacked a diverse range of sectors, there is a pronounced focus on the education and manufacturing sectors.
- **Economic Model**: Operating independently of a traditional affiliate model, BlackSuit appears to retain all profits from its operations. This approach deviates from the typical RaaS economic model, which often shares profits with a network of affiliate attackers.

⚠ **CISA Alert:** CISA Alert aa23-061a

Meow

Performance

- **RaaS Platform:** Meow (aka MeowLeaks or MeowCorp) ransomware first emerged in 2022 and is assessed to be a spinoff of the Conti gang. Until recently, Meow was a small operation, but they have rapidly escalated attacks as they appear to have shifted tactics to focus more on data exfiltration for extortion without delivering a ransomware payload for encryption, similar to groups like BianLian. In recent months, they have transitioned to a data extortion model, focusing on stealing sensitive information and selling it on their leak site. Associated with the Conti v2 ransomware variant, the group has become notorious for targeting industries in the United States with highly sensitive data, such as healthcare and medical research. A recent surge of claims from Meow has raised questions about the authenticity of their breach announcements. Analysis uncovered a troubling pattern: several of Meow's claimed attacks

Meow has rapidly escalated attacks as they appear to have shifted tactics to focus more on data exfiltration for extortion without delivering a ransomware payload for encryption, similar to groups like BianLian.

match previously confirmed breaches attributed to BlackSuit ransomware throughout this year. This discovery shows the potential role of Meow as a data broker, leveraging existing data from past breaches to bolster their attack claims. While it is common for ransomware groups to recycle data or exaggerate their capabilities, the situation with Meow is notable for being confirmed. Despite these revelations, Meow remains a serious threat, particularly to small and medium-sized businesses (SMBs). Their activity reflects a dangerous evolution in ransomware operations, where groups prioritize publicizing claims to sustain pressure on victims and maintain visibility within the ransomware ecosystem.

- **Attack Volume:** Attack volume has increased significantly in 2024. In August 2024, they accounted for 9% of all global ransomware attacks, positioning them as one of the most active ransomware groups during that period. Meow ransomware's attack volume has surged significantly, particularly following a strategic overhaul in 2024 that shifted focus from traditional encryption-based extortion to data theft and resale.
- **Ransom Demands:** It is unclear how much Meow demands for ransoms. Meow operates under a distinctive business model where victim data is offered with two pricing options. One fee grants access to the data, which can be obtained by either the victim organization or other interested parties. Alternatively, there is a much higher-priced option that offers exclusive access, ensuring that only one buyer obtains the compromised information. This tiered system increases the pressure on victims to pay more for privacy and control over their stolen data. They have been observed selling access to victim data for between $4,000 and $10,000 on the dark web. However, recent attacks have shown significant variation, with some fees as low as a few hundred dollars and others reaching as high as $40,000, depending on the target and the data compromised.
- **Victims:** Superior Court of California, San Francisco Ballet, Karman Inc., Equator Worldwide, Houston Housing authority, Sanglier Limited, Advantage CDC, MaxDream, MacGillivray Law, Community Hospital of Anaconda

Innovation

- **RaaS Platform Development:** Meow initially operated as a typical RaaS platform, encrypting victims' files and appending the "MEOW" extension, most often neglecting to encrypt plain text and ".exe" files. Victims are contacted through email or via Telegram to initiate negotiations for ransom payment. Like other RaaS, Meow uses phishing, exploiting vulnerabilities in

Remote Desktop Protocol (RDP), and compromised software like VMware and Jenkins for unauthorized access. Meow ransomware encrypts with ChaCha20 and RSA-4096, but these payloads are observed less often in the more recent attacks that focus on data extortion. It is unclear if Meow continues to support the RaaS model or engages with affiliate attackers. Meow ransomware targets both Windows and Linux systems, as well as platforms like VMware ESXi. The group has carried out several significant data exfiltration attacks in 2024, notably targeting sectors that handle sensitive personal and financial information.

- **Targeted Industries:** Meow has expanded its victim profile to include organizations across various sectors, such as healthcare, education, and government. Notably, they claimed responsibility for an attack on the Superior Court of California in Sonoma County, highlighting their willingness to target critical public institutions.
- **Economic Model**: Meow appears to be shifting from double extortion to straight data exfiltration for extortion.

KillSec

Performance

- **RaaS Platform:** KillSec emerged in 2021 as a hacktivist group aligned with the Anonymous movement. Initially known for website defacements and cyber-attacks with ideological motives, KillSec later evolved into a more organized cybercriminal group, primarily focusing on ransomware attacks. The group uses various communication channels like Telegram and Tox for negotiations and extortion. KillSec has adopted a RaaS model, enabling affiliates to conduct ransomware attacks using their infrastructure. This approach has expanded their reach and increased the frequency of attacks across various sectors.
- **Attack Volume:** KillSec's attack volume has been on a steady rise since it became more active in late 2023 and remained steady throughout 2024.
- **Ransom Demands:** KillSec's ransom demands typically range from $1,500 to $10,000, with the group often requesting payment in Monero (XMR) cryptocurrency. Monero is favored by some ransomware groups due to its enhanced privacy features, making it more difficult to trace transactions compared to other cryptocurrencies like Bitcoin.

- **Victims:** Italian Chemical Factory, Bradley International Airport, European Parliament, Los Angeles International Airport (LAX), Hartsfield-Jackson Atlanta International Airport (ATL), Romanian Government Institutions, ABC Group, Clubfit Software, MediCheck, Walters Gardens, Ping An Insurance

Innovation

- **RaaS Platform Development:** With the launch of their RaaS platform in June 2024, KillSec has expanded its capabilities. The KillSec RaaS platform enables affiliates, even those with limited technical expertise, to launch ransomware attacks using tools provided by the group. The service offers an advanced locker coded in C++ for encrypting files, along with an intuitive interface accessible via the Tor network. It also includes features such as a denial-of-service (DDoS) tool and an advanced data stealer for gathering sensitive information. The group employs sophisticated methods to infiltrate systems, including phishing attacks, exploiting known vulnerabilities, and using custom malware to maintain persistence within networks. This tactic enhances their ability to compromise targets effectively.
- **Targeted Industries:** KillSec targets a variety of industries, including government, manufacturing, finance, and professional services.
- **Economic Model**: The KillSec RaaS platform is available for a $250 fee, with KillSec retaining a 12% commission from any ransoms collected through its affiliates. KillSec typically engages in double extortion tactics to compel ransom payments.

KillSec offers an advanced locker coded in C++ for encrypting files, along with an intuitive interface accessible via the Tor network, and includes features such as a denial-of-service (DoS) tool and an advanced data stealer for gathering sensitive information.

Emerging

Fog

Performance

- **RaaS Platform:** Fog ransomware, which first emerged in November 2021, primarily targets Windows systems and is recognized as a variant of the STOP/DJVU ransomware family. Renowned for its advanced attack strategies and highly adaptive tactics, Fog has built a reputation for being both persistent and efficient. Once it infiltrates a system, the ransomware encrypts files and appends extensions like ".FOG" or ".FLOCKED" to the affected filenames, rendering them inaccessible. Victims typically find a ransom note left behind, named "readme.txt" or "HELP_YOUR_FILES.HTML," which provides instructions on contacting the attackers to negotiate file recovery. Known for its rapid encryption process, Fog can lock files within hours of deployment, pressuring affected organizations to respond swiftly to minimize operational disruption.
- **Attack Volume:** The attack volume of Fog ransomware has steadily increased since its emergence in May 2024, expanding from targeting U.S. educational institutions to various sectors globally while adopting more sophisticated tactics like double extortion.
- **Ransom Demands:** The average ransom demands by Fog ransomware typically start at a median of $220,000, with actual payments averaging around $100,000.
- **Victims:** Signal Health, Getz Group, Central Pennsylvania Food Bank, Cordogan Clark & Associates, Juice Generation, Complete Recycling Services, Dorner GmbH, Welker, Inc, Conlin's Pharmacy, Jillamy, Lincoln University, Vector Transport

Innovation

- **RaaS Platform Development:** Fog ransomware is infamous for its sophisticated techniques that make recovery exceptionally challenging. It disables Windows Defender, encrypts Virtual Machine Disk (VMDK) files, deletes backups stored in Veeam, and removes Volume Shadow Copies (VSS), effectively crippling traditional recovery options. Fog operators gain initial access to networks by exploiting compromised Virtual Private Network (VPN) credentials and vulnerabilities in VPN gateways, including

Fog ransomware disables Windows Defender, encrypts Virtual Machine Disk (VMDK) files, deletes backups stored in Veeam, and removes Volume Shadow Copies (VSS), effectively crippling traditional recovery options.

SonicWall VPNs, to breach corporate environments. Once inside, the group employs tools such as Cobalt Strike and Mimikatz to escalate privileges, often using methods like pass-the-hash attacks or extracting credentials from user browsers and the NT Directory Service (NTDS.dit). For lateral movement, Fog utilizes PsExec, Metasploit, and Remote Desktop Protocol (RDP), encrypting files across multiple devices to maximize their impact. These coordinated efforts demonstrate Fog's advanced capabilities in infiltrating, spreading, and locking down entire network environments.

- **Targeted Industries:** FOG ransomware has been particularly disruptive in the education and recreation sectors, exploiting compromised VPN credentials to infiltrate systems. In the latter half of 2024, the group increased its focus on financially lucrative sectors, including finance and healthcare, using data exfiltration and double extortion to pressure victims into compliance.
- **Economic Model**: Initially, Fog did not exfiltrate data; however, by July 2024, the group began employing double extortion tactics. The group is known for using double extortion techniques, encrypting data while also threatening to disclose sensitive information if ransom demands are unmet.

DragonForce

Performance

- **RaaS Platform:** DragonForce runs a sophisticated RaaS that emerged in November 2023 and is built using a leaked builder from the infamous LockBit group. This platform enables DragonForce to carry out highly effective attacks, capable of disrupting large segments of targeted networks. Their ability to remain undetected until the ransomware payload is deployed reflects a high level of operational expertise and maturity. DragonForce employs advanced evasion techniques, utilizing encryption and stealth tactics to bypass security defenses, making it difficult for traditional detection methods to intercept their activities prior to execution. This, combined with their use of LockBit's robust framework, allows them to target high-value organizations across various sectors.
- **Attack Volume:** Between August 2023 and August 2024, DragonForce compromised at least 82 victims across various sectors, with a significant number of attacks occurring in the United States, United Kingdom, and Australia.

DragonForce employs advanced evasion techniques, utilizing encryption and stealth tactics to bypass security defenses, making it difficult for traditional detection methods to intercept their activities prior to execution.

- **Ransom Demands:** DragonForce 's ransom demands vary, but they aim for significant amounts. Specific ransom amounts are not always disclosed, but their operations suggest they aim for high-value targets to maximize their demands.
- **Victims:** Ohio Lottery, Yakult Australia, Coca-Cola Singapore, Government of Palau, Aussizz Group, Malone & Co, Watt Carmichael, Westward360, Compression Leasing Services

Innovation

- **RaaS Platform Development:** DragonForce has been observed using ransomware variants based on leaked builders from LockBit 3.0 and ContiV3. This approach allows them to customize and deploy sophisticated ransomware payloads with relative ease. Their use of sophisticated double extortion methods–encrypting data while simultaneously threatening to leak it–demonstrates their ongoing commitment to improving their operational capabilities. They have been observed utilizing tools like Cobalt Strike for lateral movement and Mimikatz for credential harvesting. In addition to adopting LockBit's fast encryption techniques, DragonForce has implemented more advanced data exfiltration and stealth mechanisms, allowing them to evade detection and exert maximum pressure on victims.
- **Targeted Industries:** DragonForce strategically targets high-profile organizations across a range of industries, including logistics, government, manufacturing, and healthcare, which are more likely to pay substantial ransoms. The top targeted sectors include manufacturing, real estate, and transportation.
- **Economic Model**: DragonForce operates a well-structured and highly organized business model, centered around recruiting skilled affiliates and offering comprehensive technical support to ensure the success and efficiency of their attacks. In June 2024, DragonForce launched an affiliate program, offering partners 80% of ransom proceeds and advanced tools for automating attack management. The group invests heavily in research and development, continually enhancing their platform with advanced tools and techniques, which strengthens their operational capabilities. This focus on innovation, coupled with a robust affiliate network, allows DragonForce to quickly adopt new tactics and stay ahead of evolving security defenses. Their ability to rapidly integrate cutting-edge tools, such as custom encryption methods and sophisticated evasion techniques, demonstrates their commitment to maintaining a competitive edge in the

cybercriminal landscape, which bodes well for the longevity and growth of their operations. This strategy not only maximizes their profitability but also helps to build their reputation as a player in the ransomware ecosystem.

Lynx

Performance

- **RaaS Platform:** Lynx ransomware, a Ransomware-as-a-Service (RaaS) platform that emerged in July 2024, has quickly established itself as a significant threat, executing over 22 attacks primarily within the manufacturing and construction sectors. Specializing in targeting Windows environments, Lynx encrypts files and appends the .lynx extension while also deleting shadow copies to hinder recovery efforts. Although the group claims to avoid targeting government, healthcare, and non-profit organizations, its operational strategy is designed to inflict maximum disruption. Leveraging phishing campaigns and malicious downloads as primary infection vectors, Lynx exploits various entry points to infiltrate and compromise targeted networks effectively.
- **Attack Volume:** The volume of Lynx ransomware attacks has grown steadily since its mid-2024 emergence, escalating in late 2024 with sustained high activity across diverse industries, driven by its adoption of a Ransomware-as-a-Service model.
- **Ransom Demands:** The average ransom demands by Lynx ransomware have reportedly ranged from mid-five to seven figures, showing a gradual increase over time as the group targets larger organizations and refines its double extortion tactics.
- **Victims:** Ascend Analytics, KidKraft Inc., Mark Thomas & Company, Arbitech LLC, Pyle Group, True Blue Environmental, TOC Logistics International, Gortemoller Engineering, Nebraskaland, Siltech Corporation, WIMCO Corp., DZS Inc.

Lynx ransomware has a highly customizable payload, various command-line options that can specify files or directories for encryption, terminates processes, encrypts network shares, and modifies system settings.

Innovation

- **RaaS Platform Development:** Lynx ransomware is written in C++ and specifically designed for the Windows platform, featuring a highly customizable payload. It offers various command-line options that allow attackers to specify files or directories for encryption, terminate processes, encrypt network shares, and modify system settings. The ransomware employs advanced encryption methods, combining AES-128 in CTR mode with Curve25519 Donna algorithms to secure files. To ensure maximum impact, Lynx terminates specific processes and services that might interfere with the encryption process, leveraging the Windows Service Control Manager and the Restart Manager API to handle files that are in use. Additionally, Lynx deletes volume shadow copies, effectively preventing data restoration and amplifying the severity of the attack.

- **Targeted Industries:** Lynx ransomware predominantly targets a diverse range of industry verticals, including finance, energy, architecture, manufacturing, logistics, technology, and professional services, focusing on businesses with high-value data and critical operations.
- **Economic Model**: Lynx utilizes both single and double extortion techniques, encrypting files while exfiltrating sensitive data to enhance its leverage. Victims who refuse to pay are listed on Lynx's TOR-hosted leak site, where stolen data is made publicly available, heightening the pressure on the organization.

El Dorado

Performance

- **RaaS Platform:** El Dorado first emerged in March 2024. Unlike many other ransomware groups, El Dorado has developed a proprietary ransomware builder, showcasing their maturity and innovation by avoiding reliance on previously leaked tools. Their ransomware is written in Golang, providing cross-platform functionality that enables it to encrypt files on both Windows and Linux systems, including VMware ESXi environments. This versatility, combined with their advanced encryption capabilities, highlights the group's technical sophistication, and positions them as a significant threat across various industries and operating systems.
- **Attack Volume:** By fall of 2024, El Dorado had carried out dozens of confirmed attacks, with the majority targeting organizations in the United States. However, their activity saw a sharp decline in Q3 and Q4.
- **Ransom Demands:** Although specific ransom amounts have not been publicly disclosed, El Dorado's use of advanced encryption methods–such as ChaCha20 for file encryption and RSA-OAEP for securing encryption keys–indicates that their demands are likely significant. The group strategically targets high-value sectors, such as finance, healthcare, and critical infrastructure, where the financial stakes are high, and disruptions

can be costly. This focus on industries with substantial resources and a strong incentive to avoid operational downtime suggests that El Dorado stands to generate considerable revenue from their attacks. By leveraging sophisticated encryption and targeting organizations with the capacity to pay large ransoms, the group maximizes their potential earnings.

- **Victims:** Adams Homes, CelPlan, Panzer Solutions, Istituto di Istruzione Superiore, Thunderbird Country Club, City of Pensacola, Tankerska, Baker Triangle, Gough Homes, Sklar Technology Partners, Veterinary Health Center (Kansas State University), TBM Consulting Group, HTE Technologies

Innovation

- **RaaS Platform Development:** The group developed ransomware capable of targeting both Windows and Linux systems, including VMware ESXi hypervisors. Written in Golang for cross-platform capabilities, the ransomware employs ChaCha20 for file encryption and RSA-OAEP for key encryption. It can encrypt files on shared networks using the SMB protocol and is designed to self-delete after execution to evade detection. El Dorado's platform stands out for its continuous development and highly customizable ransomware builder, which is entirely original and does not rely on previously leaked or published tools. This unique builder offers extensive customization options, enabling affiliates to tailor attacks to specific needs. Key features include the ability to target specific directories, bypass local files to avoid detection, and focus on encrypting network shares, maximizing the disruption across enterprise environments. The platform's flexibility makes it a potent tool for attackers, allowing them to optimize ransomware payloads based on the structure and vulnerabilities of their target networks, further enhancing the effectiveness and profitability of their operations. El Dorado encryption algorithm allows affiliates to customize attacks by selecting specific directories, targeting network shares, and skipping file types like DLLs and EXEs to maintain system functionality and maximize disruption.
- **Targeted Industries:** El Dorado strategically focuses on high-value sectors like real estate, healthcare, and education, where the financial impact of operational disruptions is significant, increasing the likelihood of large ransom payments. Their approach reflects a keen understanding of industry-specific vulnerabilities, such as the critical nature of data in healthcare and the reliance on digital infrastructure in education and real estate. By targeting industries where downtime and data loss

El Dorado's platform stands out for its continuous development and highly customizable ransomware builder, which is entirely original and does not rely on previously leaked or published tools.

carry severe consequences, El Dorado maximizes the potential for high payouts, demonstrating both tactical insight and a calculated approach to ransomware deployment.

- **Economic Model**: El Dorado operates with a highly sophisticated business model, actively recruiting affiliates through underground forums such as RAMP, where they offer extensive technical support and customization options for their ransomware.

RaWorld

Performance

- **RaaS Platform:** RaWorld has proven highly effective in executing complex, multistage attacks aimed at disrupting large sections of targeted networks. RaWorld also employs advanced antivirus evasion techniques, allowing them to remain undetected until the ransomware payload is fully deployed. By leveraging tools that disable security measures and exploiting vulnerabilities in network infrastructure, RaWorld maximizes the impact of their attacks, leaving victims with limited options for recovery. Their strategic use of stealth tactics and deep penetration methods underscores a sophisticated operation designed for maximum disruption and financial gain.
- **Attack Volume:** The group's activities have predominantly impacted organizations in the United States, followed by entities in Europe and Southeast Asia, reflecting a broadening geographical scope. However, despite their operational effectiveness, RaWorld has not experienced significant growth in scale or attack volume.
- **Ransom Demands:** RaWorld's ransom demands have varied, but they typically range from several hundred thousand to millions of dollars, depending on the victim's size and industry. Estimates suggest significant income from their operations, given the successful breach of several large organizations. Additionally, RaWorld creates unique ransom notes tailored to each victim, personalizing the extortion process to increase pressure on organizations to pay.
- **Victims:** Specific victims include several unnamed healthcare providers and financial firms, KICO Group, Innomotive Systems, NTrust, Ventana Microsystems, Gulf Energy Maritime, Digital Engineering Inc.

Innovation

- **RaaS Platform Development:** RaWorld has consistently refined its RaaS platform, notably by customizing its ransomware using the leaked Babuk source code. This customization includes the implementation of advanced encryption techniques, making it more difficult for victims to decrypt files without paying the ransom. RaWorld exploits Group Policy Objects (GPOs) to deliver ransomware payloads, using the SYSVOL share path to distribute malicious executables across domain controllers, facilitating rapid propagation throughout the network. Once the malware is positioned, PowerShell is commonly utilized to execute the payloads, reflecting RaWorld's sophisticated approach to privilege escalation and lateral movement within compromised environments. RaWorld uses Safe Mode with Networking to bypass security defenses that are typically disabled in this mode, while also employing registry modifications to further impair protections and disable security measures. More recently, RaWorld has expanded its capabilities by introducing a Linux version of its ransomware, written in Golang, which is not derived from the Babuk code. This new variant demonstrates their commitment to evolving their platform, allowing them to target a broader range of systems and further enhancing their threat capabilities across different operating environments.

- **Targeted Industries:** Initially focusing on the healthcare sector, RA World has expanded its attacks to include manufacturing industries.

- **Economic Model**: RaWorld operates with a well-organized business model, making significant investments in research and development to stay at the forefront of ransomware technology. Their strategy includes actively recruiting affiliates and offering robust technical support to maximize the success of their attacks. RaWorld employs a double extortion model, where they first exfiltrate sensitive data before encrypting it, and then leverage the threat of leaking the stolen information if the ransom is not paid. This approach increases the pressure on victims to comply with their demands, allowing RaWorld to extract larger payouts. The group's focus on innovation and affiliate recruitment demonstrates their commitment to maintaining a profitable and sustainable operation in the ransomware landscape.

RaWorld exploits Group Policy Objects (GPOs) to deliver ransomware payloads, using the SYSVOL share path to distribute malicious executables across domain controllers, facilitating rapid propagation throughout the network.

Sarcoma

Performance

- **RaaS Platform:** Sarcoma ransomware, an aggressive RaaS group that emerged in October 2024, has quickly risen to prominence in the global cybercrime landscape. Despite its recent debut, Sarcoma has gained notoriety for its relentless tactics, high-profile data breaches, and efficient exploitation of vulnerabilities. The group primarily leverages phishing campaigns and vulnerability exploitation to infiltrate networks, making it a rapidly escalating threat. Sarcoma's operations often focus on disrupting supply chains and deploying advanced encryption methods that render data recovery nearly impossible without meeting their ransom demands. Specifically targeting Windows operating systems, Sarcoma exploits vulnerabilities unique to the platform and uses tools such as the Windows Service Control Manager, PowerShell, and Windows APIs to execute its attacks with precision and maximize impact.

- **Attack Volume:** Sarcoma ransomware attack volume has steadily increased since its emergence in late 2024, with a sharp rise in targeted campaigns across diverse industries, leveraging advanced TTPs to maximize disruption and extortion success.

- **Ransom Demands:** Sarcoma ransomware's ransom demands have escalated over time, starting in the mid-five-figure range and growing to high-six or seven figures as the group targets larger organizations and adopts a double extortion model.

- **Victims:** The Plastic Bag Company Pty Ltd, GMG Mining Supplies, Road Distribution Services (RDS), EARTHWORKS Group, Studio Navarra & Marzano, SRS-Stahl GmbH, SunTrust Properties, March Elevator Limited, Zierick Manufacturing Corporation, Pan Gulf Holding, Gedco

Innovation

- **RaaS Platform Development:** Sarcoma ransomware is a highly sophisticated threat actor known for its ability to exploit zero-day vulnerabilities to infiltrate organizational networks. A notable example of this occurred in the attack on Smart Media Group Bulgaria, where Sarcoma leveraged a zero-day vulnerability and utilized Remote Monitoring and Management (RMM) tools to conduct extensive network discovery, identifying and exploiting additional vulnerabilities to deepen its infiltration.

Unlike brute force attacks, Sarcoma employs a diverse and stealthy arsenal of tactics, techniques, and procedures (TTPs) to compromise systems effectively. The group uses a range of Windows-based tools and techniques, including exploiting Remote Desktop Protocol (RDP), executing PowerShell scripts, and leveraging Windows APIs for critical tasks such as terminating processes and deleting shadow copies to prevent recovery. Sarcoma has also been observed employing custom command-line options, allowing them to selectively encrypt specific files, directories, or network shares to maximize their impact. To maintain persistence, Sarcoma modifies Windows Registry keys to ensure the ransomware payload remains active after system reboots and creates scheduled tasks to execute the malicious software periodically. They further enhance their attacks by using tools like Mimikatz to dump credentials or exploiting vulnerable accounts to gain administrative access. Their payloads are encrypted to evade detection by antivirus solutions, and they terminate security-related processes, including endpoint protection services. Sarcoma ensures its encryption is nearly unbreakable by combining AES-256 for file encryption with RSA for secure key exchange. In addition, they delete volume shadow copies (VSS) to eliminate recovery options and use encrypted communication channels to securely connect with their command-and-control (C2) servers, maintaining operational security throughout their attacks. This combination of advanced capabilities and tactical sophistication makes Sarcoma a particularly dangerous ransomware threat.

- **Targeted Industries:** Sarcoma has targeted various sectors worldwide, including healthcare, manufacturing, and finance. While Sarcoma's operations have primarily targeted companies in Australia, New Zealand and Japan, they have begun to expand targeting to other regions.
- **Economic Model**: Sarcoma's attacks typically involve the exfiltration of sensitive data, which they use to coerce victims into compliance without initially stating monetary ransom demands.

Sarcoma uses a range of Windows-based tools and techniques, including exploiting Remote Desktop Protocol (RDP), executing PowerShell scripts, and leveraging Windows APIs for critical tasks such as terminating processes and deleting shadow copies to prevent recovery.

Cloak

Performance

- **RaaS Platform:** The Cloak RaaS group, which first emerged in late 2022, has rapidly established itself as a formidable threat actor in the cybersecurity landscape, executing dozens of attacks across various industries. Cloak's attack strategy involves gaining network access through Initial Access Brokers (IABs) or social engineering techniques, such as phishing, malvertising, exploit kits, and drive-by downloads disguised as legitimate updates like Microsoft Windows installers. Once inside a network, Cloak delivers ransom notes in the form of desktop wallpapers and text files named "readme_for_unlock.txt", while also deleting volume shadow copies to hinder recovery efforts and maximize the attack's impact. Analysts have identified links between Cloak and the Good Day ransomware operation, a variant of the ARCrypter family that first appeared in May 2023. Both groups share a data leak platform, suggesting a potential collaboration or operational overlap in their extortion activities, highlighting Cloak's growing influence and adaptability. Cloak ransomware exhibits a high level of sophistication in its operational tactics. The Cloak payload employs advanced privilege escalation techniques, terminates critical processes, and uses robust encryption algorithms to lock files. Specifically, it utilizes the HC-128 algorithm and secure key generation methods to ensure effective and secure encryption. Cloak's delivery mechanisms seamlessly embed the ransomware payload, making detection more challenging. By targeting security tools, backups, and databases, the ransomware amplifies disruption and complicates recovery efforts. To prolong its impact, Cloak incorporates persistence mechanisms such as registry modifications and user restrictions, ensuring operational downtime. Its use of intermittent encryption, combined with aggressive deletion of recovery tools, exemplifies a modern ransomware strategy designed to exert maximum pressure on victims. Cloak's ability to evade detection, disrupt critical systems, and adapt to evolving countermeasures cements its reputation as a sophisticated and highly effective ransomware operation.

- **Attack Volume:** Cloak ransomware attack volume has steadily increased since its emergence in late 2022, with a significant rise in activity driven by its adoption of RaaS and its focus on leveraging advanced tactics to maximize impact and operational disruption.

- **Ransom Demands:** Cloak ransomware's ransom demands have escalated over time, initially targeting smaller organizations with mid-five-figure amounts and evolving to high-six or seven-figure sums as the group expanded its operations and targeted larger, more lucrative victims. The group boasts an exceptionally high payment rate of 91-96%, highlighting its effectiveness in coercing victims.

Innovation

- **RaaS Platform Development:** The Cloak ransomware group is suspected of acquiring network access through Initial Access Brokers (IABs) while also employing sophisticated social engineering tactics. These include phishing, malvertising, exploit kits, and drive-by downloads disguised as legitimate Microsoft Windows Update installers. Once inside a network, the group deploys a ransomware payload–a variant of ARCrypter believed to be derived from the leaked Babuk ransomware source code. Cloak demonstrates advanced capabilities in privilege escalation, process termination, and system disruption. Delivered via a loader that embeds the ransomware payload, the malware employs sophisticated mechanisms to extract and execute its components. Upon deployment, it terminates processes and services associated with security tools, backups, databases, and essential applications, effectively crippling the victim's ability to recover. It also modifies system settings to hinder user actions and further complicate recovery efforts. Cloak ransomware encrypts files on local drives and network shares using the HC-128 encryption algorithm. Encryption keys are securely generated through a multi-step process: a 32-byte private key is created using CryptGenRandom, and a 32-byte public key is derived with Curve25519_donna. A shared key is then calculated using the private key and a hardcoded public key, followed by a SHA512 hash of the shared key. The first 32 bytes of the hash serve as the HC-128 encryption key, while the remaining 32 bytes act as the initialization vector (IV). To evade detection, Cloak employs advanced techniques such as executing the ransomware payload from virtual hard disks, which can be quickly detached after malicious tasks are completed. The ransomware ensures persistence by modifying registry entries to enable startup execution and restricting user actions, such as logging off or accessing the Task Manager. Additionally, it disrupts critical system utilities and network services to maximize operational downtime. Cloak uses two modes of encryption–full and intermittent–depending on the size of the file being encrypted. Intermittent encryption targets specific chunks of large files to optimize performance while maximizing damage. To increase leverage over victims, the ransomware deletes volume shadow copies

Cloak ransomware encrypts files on local drives and network shares using the HC-128 encryption algorithm where keys are securely generated through a multi-step process that includes 32-byte private key is created using CryptGenRandom, and a 32-byte public key is derived with Curve25519_donna.

using command-line instructions and empties the recycle bin by calling the SHEmptyRecycleBinA function. As part of its anti-debugging strategy, Cloak enables SeDebugPrivilege for its process, respawns itself, and terminates any detected debuggers or performance profiling applications. It also stops services related to antivirus software, backup and restore functions, and database management. Ransom notes are deployed both as desktop wallpapers and as text files to ensure victims are immediately aware of the attack. The strategic combination of intermittent encryption, evasion techniques, and system disruption makes Cloak a sophisticated and highly effective ransomware threat.

- **Targeted Industries:** Cloak primarily targets small to medium-sized businesses in Europe, with Germany as a key focus. The group has extended its operations to countries in Asia and targets various sectors, including healthcare, real estate, construction, IT, food, and manufacturing.
- **Economic Model**: Cloak has been observed recruiting affiliates on underground forums, offering attractive profit-sharing schemes to entice participants providing an above-average 85/15 profit-sharing split, with no upfront payment required to access their platform. Victims who refuse to pay face further consequences, as Cloak publishes their stolen data on its leaks site for double extortion.

Diminishing

Cl0p

Performance

- **RaaS Platform:** First observed in 2019, Cl0p operates as a RaaS platform known for its advanced anti-analysis features and anti-virtual machine detection, which helps them evade investigations in emulated environments. Cl0p became the most prolific ransomware group in Q2 2023, largely due to their increased automation in exploiting known vulnerabilities, such as MOVEit Transfer (CVE-2023-34362), GoAnywhere MFT (CVE-2023-0669). Cl0p's large-scale exploitation of the MOVEit vulnerability drove attack levels to unprecedented heights, with the group being responsible for roughly 21% of all ransomware incidents in July 2023. Previously focusing on data extortion since early 2023, Cl0p returned to using encryptors, signaling a potential resurgence. Their ability to exploit vulnerabilities at scale and shift tactics between data extortion and encryption demonstrates their adaptability and technical sophistication, positioning them as a significant force in the ransomware landscape when active.
- **Attack Volume:** Cl0p experienced a surge in attacks throughout 2023, taking advantage of patchable exploits in the GoAnywhere file transfer software to compromise over 100 victims in just a few weeks. This marked a significant escalation in the group's activity. In early summer 2024, Cl0p further intensified their operations by exploiting the MOVEit vulnerability (CVE-2023-34362), compromising thousands of organizations globally. In August 2023, Cl0p's activity dropped sharply, and by September 2023, the group seemed to have gone completely dark, with very few attacks linked to them throughout Q1-2024. By Q2-2024, Cl0p had virtually disappeared. Cl0p's activity dramatically declined, and by the latter half of 2024, their attacks had nearly ceased. In the last part of Q4-2024, Cl0p escalated attacks by exploiting critical vulnerabilities in Cleo's managed file transfer (MFT) software, specifically targeting platforms such as Cleo Harmony, VLTrader, and LexiCom. These attacks have compromised numerous organizations, resulting in a significant number of data breaches. Cl0p has listed 66 affected companies on its dark web portal, pressuring them with a 48-hour ultimatum to meet ransom demands. The stolen data includes confidential business information, personal customer details, and other sensitive records.

In Q4-2024, Cl0p escalated attacks by exploiting critical vulnerabilities in Cleo's managed file transfer (MFT) software, specifically targeting platforms such as Cleo Harmony, VLTrader, and LexiCom, where attacks resulted in a significant number of data breaches.

- **Ransom Demands:** Ransom demands vary depending on the target and average around $3 million dollars but have been reported to be as high as $20 million. Ransom amounts are likely to continue to grow as Cl0p focuses more on the exfiltration of sensitive data.
- **Victims:** Shell, Level8 Solutions, NetScout, AutoZone, Siemens, Allegiant Air, NCR, Virgin Group, Saks Fifth Avenue, US DHS, New York Bar Association.

Innovation

- **RaaS Platform Development:** Cl0p was one of the pioneering RaaS groups to develop a Linux version of its ransomware, signaling the group's effort to recruit new talent and enhance their platform, thereby expanding their range of potential targets. Cl0p's Windows variant, written in C++, employs RC4 for file encryption and uses RSA 1024-bit to secure the encryption keys. In May 2023, Cl0p shifted tactics by exploiting a SQL injection vulnerability (CVE-2023-34362) in Progress Software's MOVEit Transfer, a managed file transfer (MFT) solution. This vulnerability allowed Cl0p to steal sensitive data from victim databases without deploying an encryption payload, focusing entirely on data exfiltration and extortion. Earlier in 2023, Cl0p also exploited a vulnerability in Fortra GoAnywhere MFT servers, further illustrating their strategic use of file transfer system vulnerabilities to breach organizations. These campaigns highlight Cl0p's ability to adapt its methods, emphasizing data theft and extortion as effective tactics alongside traditional ransomware attacks. At the end of Q4-2024, Cl0p was observed leveraging two critical zero-day vulnerabilities in Cleo's software to execute these attacks: CVE-2024-50623, disclosed in October 2024, which enabled unauthorized file uploads and downloads, and CVE-2024-55956, identified in December 2024, which further allowed unauthorized system access.
- **Targeted Industries:** Initially, Cl0p focused almost exclusively on healthcare sector targets, taking advantage of the sensitive nature of medical data and the sector's reliance on uninterrupted operations. However, as the group evolved, they expanded their scope to include a wide range of organizations, particularly those with vulnerable GoAnywhere installations. This broadened targeting included financial services firms, known for their valuable data and deep pockets, as well as government agencies, where disruption could create significant pressure to meet ransom demands. Cl0p's shift toward exploiting vulnerabilities in widely used file transfer solutions allowed them to cast a much wider net, increasing their potential impact across multiple sectors.

- **Economic Model**: Cl0p operated a broad affiliate program, enabling a wide network of attackers to utilize their ransomware platform. The group frequently exfiltrated sensitive data, using it to carry out triple extortion schemes–where they not only demand ransom for decrypting data but also threaten to leak the stolen information and, in some cases, launch additional attacks to pressure victims further. Over time, Cl0p significantly expanded its primary target range beyond the healthcare sector, increasingly focusing on industries such as finance, government, and critical infrastructure. There have been indications that Cl0p may be shifting towards a more data-centric extortion model, where the focus is on leveraging stolen data rather than encrypting systems. However, at this stage, most victims are still subjected to ransomware payloads, combining encryption with data theft to maximize their leverage and potential ransom payments. This hybrid approach allows Cl0p to adapt to different targets while continuing to exploit vulnerabilities across a wide range of sectors.

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

DarkVault

Performance

- **RaaS Platform:** DarkVault is a relatively recent ransomware group, making its debut in late 2023, and has similarities to other major ransomware players, namely LockBit, mimicking their leaks site design. It is unclear if DarkVault is a RaaS. In addition to ransomware attacks, DarkVault engages in various cybercriminal activities such as bomb threats, swatting, doxing, defacing websites, and creating malware. This multi-faceted approach to cybercrime makes them a dangerous and unpredictable entity. Their data leak site is designed to closely resemble that of the notorious LockBit ransomware, leading to speculation that DarkVault could be either a rebranded version of LockBit or attempting to mimic its success. While no definitive proof links DarkVault to LockBit, it's worth noting that many other cybercriminal groups have also adopted LockBit's leaked ransomware builder. As of now, there is no clear evidence indicating whether DarkVault specifically targets both Windows and Linux systems.

- **Attack Volume:** DarkVault attack volumes have decreased dramatically in 2024.

- **Ransom Demands:** DarkVault's ransom demands have been observed to range between $30,000 and $100,000, depending on the target and the data exfiltrated.

In addition to ransomware attacks, DarkVault engages in various cybercriminal activities such as bomb threats, swatting, doxing, defacing websites, and creating malware, which makes them a dangerous and unpredictable entity.

- **Victims:** InThinking, arabot.io, Techguard, Atriline, Q-int, Cosim TI SRL, Glazkov CPA, Bzrastreador, Panda Car Care, PeopleWell Solutions, Sequel Logistics, TaskHound, Lanka Communication Services (Pvt.) Ltd., PT. Oexpress Logistik Indonesia, SalesGig

Innovation

- **RaaS Platform Development:** It remains unclear whether DarkVault operates as a RaaS platform. While certain activities, like leveraging dark web leak sites and emulating the tactics of established ransomware groups such as LockBit, bear similarities to RaaS models, there is no clear evidence that it follows the standard affiliate structure typically seen in these operations.
- **Targeted Industries:** DarkVault often targets industries with valuable or sensitive data, such as e-commerce platforms, healthcare, retail, and finance.
- **Economic Model**: DarkVault uses a double extortion technique, where they not only encrypt victims' systems but also steal sensitive data. If the ransom is not paid, they threaten to release this stolen information publicly.

Cactus

Performance

- **RaaS Platform:** Cactus is known for its ability to evade security tools, using sophisticated methods to bypass defenses. Cactus primarily gains initial access by exploiting known vulnerabilities in widely used VPN appliances, allowing them to infiltrate targeted networks with relative ease. Once inside, Cactus operators have been observed deploying a batch script designed to unhook or disable common security tools, further reducing the likelihood of detection. This combination of vulnerability exploitation and security evasion tactics has made. Cactus has been observed exploiting vulnerabilities in the Qlik business analytics platform, specifically CVE-2023-41266, CVE-2023-41265, and CVE-2023-48365, to gain initial access to target networks. Traditionally focusing on Windows workloads, Cactus has expanded its targets to include virtualization platforms such as VMware ESXi and Microsoft Hyper-V.
- **Attack Volume:** Cactus attack volumes have decreased dramatically in 2024.

- **Ransom Demands:** Cactus employs an encrypted messaging platform called TOX chat to conduct negotiations with victims. Ransom demands are assessed to be quite substantial, but an average has not been established.
- **Victims:** Schneider Electric, SCS SpA, OmniVision Technologies, The Hurley Group, Cornerstone Projects Group, ICOR Global Limited, Cornerstone Projects Group, Societa' Canavesana Servizi.

Innovation

- **RaaS Platform Development:** Cactus ransomware operations rely heavily on Living-off-the-Land (LotL) techniques, which abuse legitimate network tools to avoid detection. These techniques involve the use of trusted tools like Event Viewer, PowerShell, Chisel, Rclone, and Scheduled Tasks to move within targeted networks. Cactus has been observed leveraging legitimate remote management tools like Splashtop, AnyDesk, and SuperOps RMM to maintain persistence within compromised networks. The ransomware employs a unique self-encryption mechanism, requiring a key to decrypt the binary for execution. This approach is likely designed to prevent detection by antivirus software. Additionally, Cactus often drops an SSH backdoor on compromised systems for persistence and to maintain communication with their command-and-control (C2) servers. The group has also been observed leveraging legitimate remote access tools such as Splashtop and SuperOps RMM, alongside the deployment of Cobalt Strike for lateral movement and network compromise. In Q1 2024, Cactus operators expanded their tactics by abusing Qlik Sense for initial access and using ManageEngine UEMS and AnyDesk to facilitate remote access and lateral movement across networks. One of Cactus's unique features is its ransomware payload, which is encrypted and requires a decryption key to execute, making it difficult for security tools to detect during the infiltration phase. Furthermore, it is assessed that Cactus uses a custom PowerShell script known as TotalExec to automate the encryption process, a tactic like that employed by the BlackBasta gang. They have also been observed attempting to dump LSASS credentials to escalate privileges within the network, enhancing their ability to maintain control and further compromise systems. This combination of LotL techniques, advanced persistence mechanisms, and unique payload encryption makes Cactus a formidable and evolving ransomware threat.
- **Targeted Industries:** Cactus has been observed abusing SoftPerfect Network Scanner to do reconnaissance on prospective victims, who are large-scale commercial organizations across multiple sectors.

Cactus has been observed leveraging legitimate remote management tools like Splashtop, AnyDesk, and SuperOps RMM to maintain persistence, and the ransomware employs a unique self-encryption mechanism, requiring a key to decrypt the binary for execution.

- **Economic Model**: Like many modern extortion gangs, Cactus employs data exfiltration as part of a double extortion scheme, frequently abusing the Rclone tool to transfer stolen data to external servers. Their economic model appears strong, blending advanced technological tactics with a well-structured RaaS framework. This model not only allows Cactus to maximize profits by threatening both data encryption and exposure, but it also indicates substantial investment in research and development, as well as in the recruitment and support of affiliates. The RaaS structure enables Cactus to scale their operations efficiently, enlisting skilled affiliates who benefit from their advanced toolset, making the group a significant player in the ransomware landscape.

RansomHouse

Performance

- **RaaS Platform:** RansomHouse transitioned into a RaaS platform shortly after its launch in December 2021, evolving from a primary focus on data extortion to offering affiliates the infrastructure and tools for conducting ransomware attacks. RansomHouse's shift to a RaaS platform is highlighted by their deployment of tools like MrAgent for automating attacks on platforms such as VMware ESXi. They claim not to collaborate with hacktivist groups or intelligence agencies, positioning themselves as independent operators. RansomHouse gained significant attention in 2022 with their attack on chipmaker AMD, where they exfiltrated 450GB of sensitive data.

- **Attack Volume:** RansomHouse attack volumes have decreased dramatically in 2024.

- **Ransom Demands:** Ransom demands have been reported to range between $1 million and $11 million.

- **Victims:** Advanced Micro Devices, Indonesia Power, AMD, Mission Community Hospital, Van Oirschot, Hawkins Delafield Wood, SMB Solutions, United Urology Group.

In early 2024, RansomHouse introduced MrAgent, a tool designed to automate ransomware deployment across VMware ESXi hypervisors by identifying host systems, disabling firewalls, and simultaneously encrypting multiple virtual machines, while receiving configurations from a command and control (C2) server to schedule encryption events.

Innovation

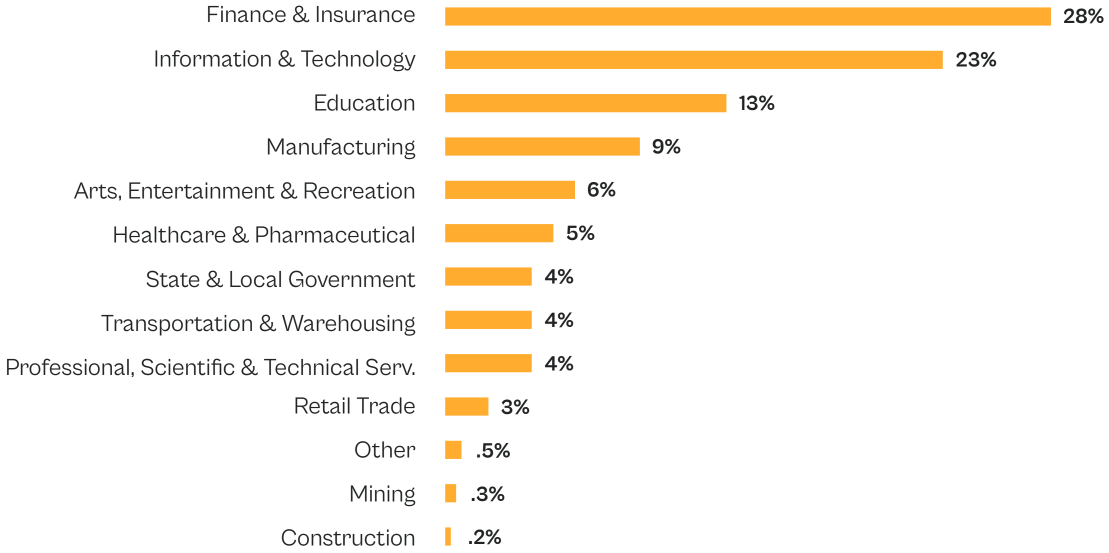
- **Raas Development:** In early 2024, RansomHouse introduced MrAgent, a tool designed to automate ransomware deployment across VMware ESXi hypervisors by identifying host systems, disabling firewalls, and simultaneously encrypting multiple virtual machines, while receiving configurations from a command and control (C2) server to schedule encryption events and execute commands to evade detection. Their strategic focus on exfiltration in addition to encryption allows them to pressure victims with the threat of public data leaks, increasing the likelihood of ransom payments.
- **Targeted Industries:** In 2023 and 2024, RansomHouse expanded its operations beyond Italy, increasingly targeting U.S. organizations, particularly in the technology, industrials, and healthcare sectors, which house critical infrastructure. The group selects victims opportunistically, based on ease of compromise or financial capability, and uniquely frames its attacks because of the victims' poor security practices, publicly blaming them for negligence.
- **Economic Model**: RansomHouse operates an active leak site where they employ a "name and shame" tactic, publicly exposing victims to increase pressure for ransom payments. In addition to using double extortion by exfiltrating sensitive data, RansomHouse is also known to sell stolen data to other threat actors, further monetizing their attacks and expanding their revenue streams beyond ransom demands.

Halcyon Threat Insights: October

Here are the key insights from the Halcyon Threat Research and Intelligence Team findings for October 2024 based on intelligence collected from our customer base:

October 2024

Ransomware Prevented by Industry Vertical



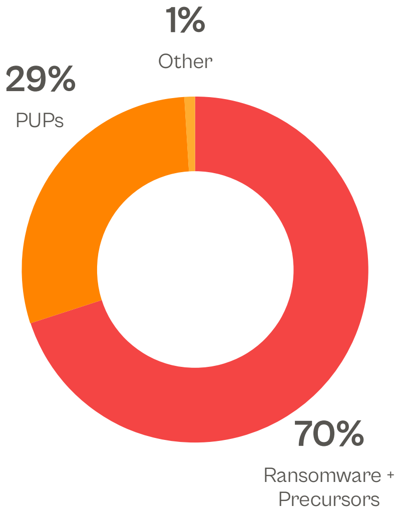
The Finance, IT and Education sectors were the most targeted industry verticals in October 2024

Ransomware Precursors Blocked

trojan.mimikatz/genericfca: A malicious trojan variant associated with the well-known Mimikatz tool, which is often used in cybersecurity attacks for credential theft and lateral movement within networks. Mimikatz itself is an open-source tool initially developed for educational purposes to demonstrate vulnerabilities in Windows' authentication systems. However, threat actors frequently abuse its functionalities to extract sensitive information, such as login credentials and stored passwords, from targeted systems. Once installed on a system, it leverages advanced techniques to bypass antivirus defenses and gain access to the system's memory, where it retrieves plaintext credentials from processes like LSASS (Local Security Authority Subsystem Service). This variant poses a high risk in corporate environments, as it enables attackers to escalate privileges and access sensitive resources, facilitating further exploitation.

October 2024

Threat Types by Category



trojan.cobaltstrike/lazy: A malicious trojan variant linked to the commercial penetration testing tool Cobalt Strike, which has been increasingly weaponized by threat actors for sophisticated cyberattacks. Originally designed to help security professionals simulate real-world attacks, Cobalt Strike has unfortunately become a powerful tool for malicious activity. In particular, the "Lazy" variant of this trojan exploits the tool's extensive post-exploitation features, making it ideal for advanced persistent threat (APT) operations and other targeted cyberattacks. Once deployed, it provides attackers with command-and-control (C2) capabilities, allowing them to establish persistent access, perform lateral movement, and exfiltrate sensitive data. The "Lazy" variant often focuses on evading detection, utilizing techniques such as process injection, fileless payloads, and obfuscation to bypass endpoint defenses and traditional antivirus solutions.

trojan.injexa/dridex: A sophisticated banking trojan designed to steal sensitive financial information and enable further malicious activities within infected systems. Originating from the Dridex malware family, which is known for targeting banking and financial services, this variant, Injexa/Dridex, is particularly dangerous due to its ability to deploy modular payloads, adapt to various environments, and evade detection with advanced obfuscation techniques. Once a user unknowingly executes the malware, Injexa/Dridex installs itself and establishes a command-and-control (C2) connection with a remote server controlled by the attackers. From there, it can log keystrokes, capture screenshots, and steal credentials or other valuable data. The trojan also enables attackers to inject malicious code into web pages viewed by the victim, making it highly effective in stealing online banking credentials.

trojan.marte/volt: A malware variant that leverages remote access trojan (RAT) capabilities to infiltrate systems, exfiltrate data, and establish persistent backdoors within target environments. Emerging as a threat in both personal and enterprise environments, Marte/Volt is particularly concerning due to its stealth and adaptability, enabling cybercriminals to perform a range of malicious activities remotely. Once deployed, this trojan establishes a covert connection with a command-and-control (C2) server, allowing attackers to take control of infected machines. Once activated, the trojan can monitor user activity, capture keystrokes, access sensitive files, and, in some cases, even control webcams and microphones. The Marte/Volt variant is often equipped with sophisticated obfuscation techniques, making it difficult for standard antivirus software to detect and neutralize.

trojan.remcos/craexxe: A potent remote access trojan (RAT) that provides attackers with unauthorized access and control over infected devices, enabling extensive data theft, surveillance, and manipulation of system processes. Originally marketed as a legitimate tool for IT professionals, Remcos (Remote Control & Surveillance) has been co-opted by cybercriminals for malicious purposes. The Craexxe variant is particularly insidious due to its focus on stealth and versatility, making it a preferred tool in both targeted and broad-based attacks. Once activated, it installs itself deeply within the system, establishing a command-and-control (C2) connection with the attacker. This connection allows the attacker to execute commands remotely, monitor user activity, capture keystrokes, and exfiltrate sensitive information. Craexxe's advanced obfuscation and anti-analysis techniques enable it to bypass many traditional antivirus defenses, making detection and removal challenging.

Ransomware Payloads Blocked

trojan.wannacry/wanna: A notorious ransomware that gained global attention in May 2017 when it rapidly infected hundreds of thousands of systems across numerous industries. The WannaCry payload exploits vulnerabilities in the Windows operating system, particularly the EternalBlue exploit, which was leaked from a cache of NSA hacking tools. The worm-like behavior of WannaCry allows it to propagate automatically across networks, making it exceptionally contagious. Once executed, WannaCry begins by scanning for unpatched or vulnerable Windows systems, then encrypts files with extensions typically associated with essential user data, such as documents, images, and archives. WannaCry can cause significant operational disruptions, data loss, and financial damage, especially in large organizations.

ransomware.lockbit/lockbit2: A fast-spreading ransomware strain targeting organizations across various industries worldwide. Known for its speed, adaptability, and automated processes, LockBit 2.0 has become one of the most prolific ransomware variants, typically leveraging the RaaS model. LockBit 2.0 works by infiltrating systems, often through phishing emails, vulnerable software, or weak Remote Desktop Protocol (RDP) connections, and then quickly encrypting data files. The ransomware's advanced encryption algorithm makes it nearly impossible to decrypt data without the attacker-provided key. LockBit 2.0 also includes advanced evasion techniques to bypass endpoint detection and response (EDR) solutions, making it especially challenging to detect and contain. Additionally, it employs a "double extortion" method, in which attackers threaten to leak sensitive data if the ransom isn't paid.

ransomware.sodinokibi/revil: A sophisticated ransomware strain responsible for high-profile attacks across numerous industries. Known for its advanced techniques and aggressive tactics, REvil operates on a RaaS model, which has enabled REvil to spread widely and impact organizations of all sizes, making it one of the most formidable ransomware threats to date. Once executed, REvil makes decryption without the attackers' key nearly impossible. Additionally, REvil employs a "double extortion" strategy: attackers not only demand a ransom for decrypting the files but also threaten to leak sensitive information publicly if the ransom isn't paid, increasing pressure on victims.

trojan.zeppelin/zapchast: A ransomware variant that targets enterprise networks and individuals, primarily focusing on organizations in healthcare, technology, and education sectors. Part of the Zeppelin ransomware family, Zapchas is notorious for its stealth and adaptability, which allows attackers to launch highly targeted and destructive attacks. This ransomware is often deployed in "big-game hunting" attacks, where cybercriminals aim for high-value targets to maximize their ransom demands. Once inside a network, it spreads to other systems and encrypts critical files, disrupting operations and causing significant downtime. This variant is known for its customization capabilities, allowing attackers to tailor the ransom note, encryption methodology, and demands based on the specific victim, which heightens the pressure to pay the ransom.

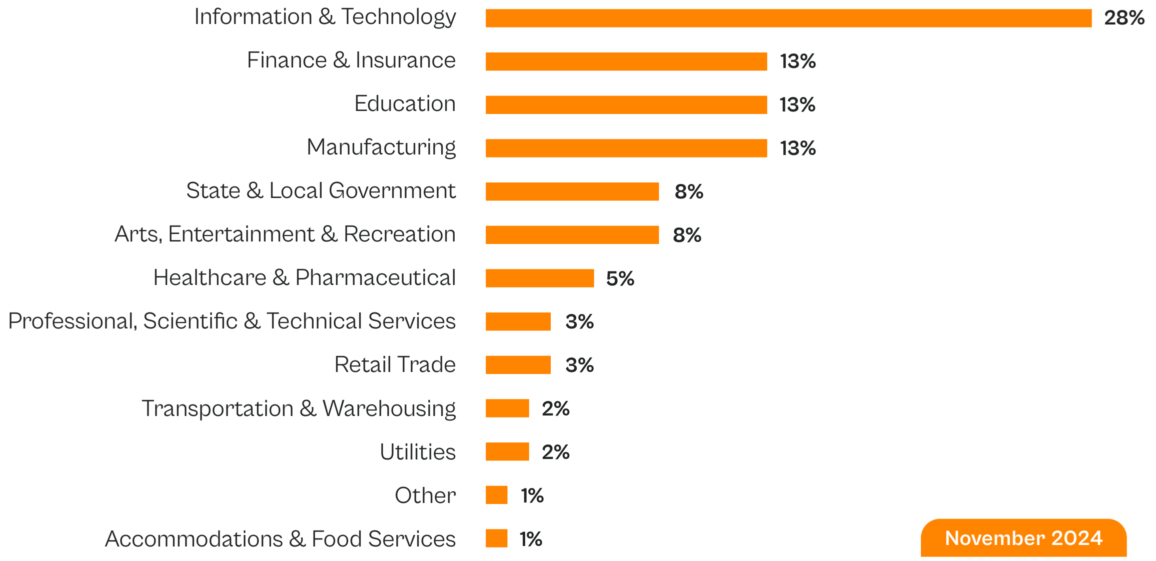
trojan.xorist/cryptotorlocker2015: A ransomware variant that is part of the Xorist ransomware family, CryptoTorLocker2015 is typically spread through malicious email attachments, compromised websites, or bundled with other software, often disguising itself as legitimate files to trick users into opening it. Upon execution, the ransomware searches for valuable file types such as documents, images, and databases. This variant of Xorist is known for its relatively straightforward tactics, but it can still cause significant disruption, especially for users without backups or security protections in place.

Halcyon Threat Insights: November

The IT, Finance, and Education sectors were the most targeted industry verticals in November 2024.

November 2024

Threats Prevented by Industry Vertical



Threat Types by Category

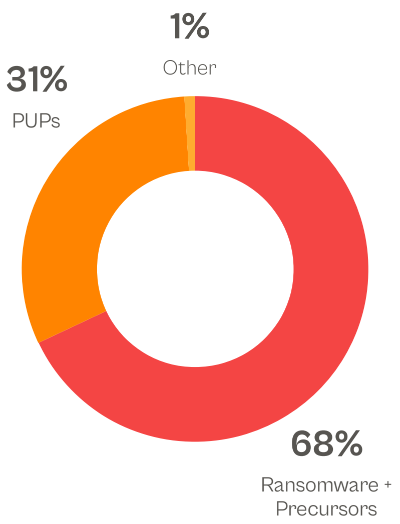
Halcyon detected and blocked a wide variety of threats that were missed by other security layers in our client's environments that are often precursors to the delivery of the ransomware payload.

Ransomware Precursors Blocked

Trojan.weelsof/mikey: The primary functions of this Trojan include data theft, system manipulation, and unauthorized remote access. It may harvest sensitive information such as login credentials, banking details, or personal files, which can be exploited for financial gain or identity theft. Additionally, it can download and install other malware, such as ransomware or spyware, further compromising the system. It often disables security software and system defenses, making detection and removal challenging. In some cases, it may display fake warnings or lock the system entirely, demanding payment for restoration–actions characteristic of ransomware-like behavior.

November 2024

Threat Types by Category



Trojan.cosmu/xpiro: Once installed, it establishes itself deeply within the operating system, infecting executable files and spreading across the network to compromise other connected devices. Its primary objectives include stealing sensitive information, such as login credentials, financial data, and personal files. Additionally, it often creates backdoors, granting attackers unauthorized access to the infected system. These backdoors can be used to deploy other forms of malware, such as ransomware, keyloggers, or botnets. A distinguishing feature is its polymorphic nature, allowing it to change its code structure dynamically to avoid detection. This makes it particularly challenging to remove and a persistent threat even to well-secured environments.

Trojan.clipbanker/zusy: A type of Trojan malware designed to manipulate clipboard data, primarily targeting cryptocurrency transactions and other financial activities. The Trojan's primary function is to monitor and intercept clipboard activity. When a user copies sensitive information, such as cryptocurrency wallet addresses or banking details, it replaces the copied content with an attacker-controlled value. For example, if a user attempts to send cryptocurrency to a specific wallet, the Trojan substitutes the intended address with the attacker's address, diverting the funds without the user's awareness. In addition to its clipboard manipulation capabilities, it may include spyware functionalities to harvest sensitive information, such as login credentials, or even serve as a delivery mechanism for additional malware.

Trojan.sasfis/processhijack: Once installed, it hijacks legitimate system processes to mask its activity, blending into the operating system's normal operations. This tactic allows it to evade detection by security tools and remain active for extended periods. The Trojan is often used to download and execute additional payloads, including spyware, ransomware, or other forms of malware. It can also steal sensitive information such as login credentials, banking details, or personal files, which can then be exploited or sold on the dark web. In addition, the Trojan may weaken system defenses by disabling antivirus programs or altering system configurations, further exposing the system to subsequent attacks.

Trojan.apbcw/r002c0xcp24: Once installed, it establishes a foothold in the operating system by disguising itself as a legitimate process or system file. Its primary objectives include data theft, surveillance, and system compromise. It may harvest sensitive information such as passwords, financial data, or personal documents. Additionally, it can serve as a gateway for other malware, such as ransomware, spyware, or botnet components. This Trojan is also known for its ability to disable or bypass security software, making removal more challenging. It may create backdoors to provide attackers with persistent remote access, allowing them to control the infected system, monitor user activity, or deploy further attacks.

Ransomware Payloads Blocked

Trojan.diskwriter/lfbzh: A highly destructive ransomware wiper designed to manipulate or overwrite disk data on compromised systems. It can overwrite, delete, or encrypt critical files, rendering them unusable. In some cases, it may modify the system's master boot record (MBR) or partition tables, leading to complete system failure or preventing the operating system from booting. These actions often serve as a precursor to further malicious activities, such as ransomware attacks or data theft. It may also create backdoors, enabling attackers to remotely access the system for surveillance, data exfiltration, or further malware deployment. Its ability to disable security defenses and evade detection makes it particularly challenging to counter.

Trojan.rook/abysslocker: This payload establishes a foothold in the infected system by exploiting system vulnerabilities or misconfigurations. It can evade detection by masquerading as legitimate processes and employing obfuscation techniques. In addition to ransomware functionality, this Trojan often installs backdoors, granting attackers persistent remote access to the compromised system. These backdoors can be used for further data theft, espionage, or additional malware deployment. The impact of this ransomware can be devastating to an organization, resulting in data loss, operational disruption, financial impact, regulatory actions, legal liability and brand damage.

Ransomware.msil/msilperseus: A ransomware strain developed using the Microsoft Intermediate Language (MSIL), a code format utilized in .NET applications. Known for its aggressive encryption capabilities and stealthy delivery mechanisms, this ransomware is a significant threat to individuals and organizations. It targets a wide range of file types, including documents, images, databases, and backups. A defining characteristic is its ability to evade detection by antivirus software through advanced obfuscation and polymorphic techniques, making it challenging to identify and remove. In some cases, it also disables system recovery options and deletes shadow copies to prevent victims from restoring their files.

Ransomware.incransom/imps: Its stealthy nature and aggressive encryption mechanisms make it a significant threat to individuals, businesses, and organizations. Once executed, it can scan the victim's system for valuable files, including documents, images, videos, and databases. Using strong encryption algorithms, it locks these files, rendering them inaccessible. A defining characteristic of IncRansom/IMPS is its ability to evade detection through advanced obfuscation techniques and its capability to disable security defenses such as antivirus software or firewalls. Additionally, it may delete backups or shadow copies to prevent file recovery without paying the ransom.

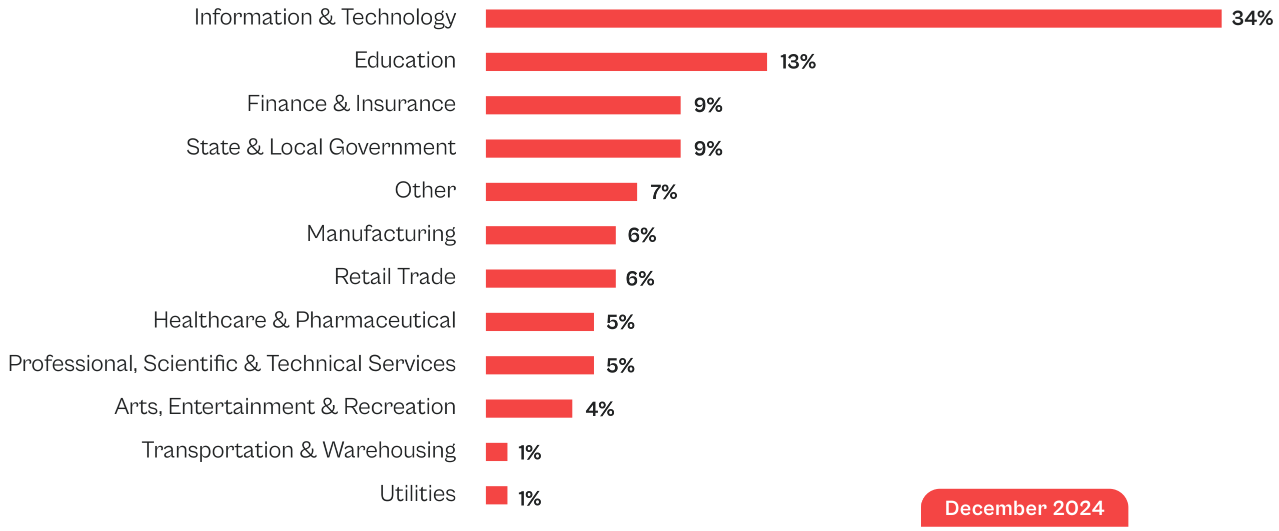
Ransomware.embargo/barys: Upon infection, it scans the system for valuable files, including documents, databases, images, and backups. It uses robust encryption algorithms to lock these files, making them inaccessible to the user. A notable feature of Embargo/Barys is its ability to evade detection using advanced obfuscation techniques and by disabling security defenses such as antivirus software and firewalls. It may also delete shadow copies and backups to prevent victims from recovering their files independently.

Halcyon Threat Insights: December

The IT, Education, and Finance sectors were the most targeted industry verticals in December 2024.

December 2024

Ransomware Prevented by Industry Vertical

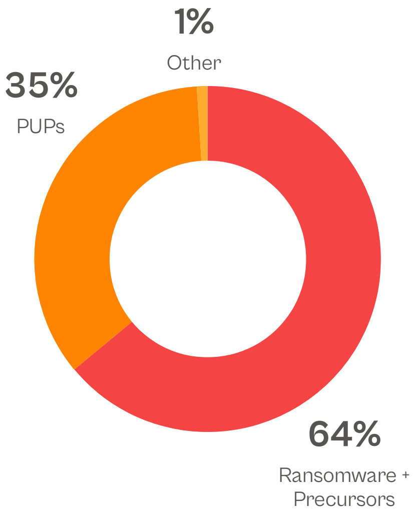


Ransomware Precursors Blocked

Trojan/Backstab.killav: A type of malware specifically designed to disable antivirus (AV) and security solutions on a targeted system which allows attackers to deploy additional malware, such as ransomware, spyware, or keyloggers, without triggering detection or prevention protocols. It typically works by terminating processes associated with antivirus software, modifying system registry entries to disable startup protections, or exploiting vulnerabilities within the AV software itself. In some cases, it uses privilege escalation techniques to bypass administrative controls and ensure persistence. Advanced variants may also block updates to security software, rendering systems defenseless against emerging threats. Once active, it prepares the system for deeper compromise by erasing logs, masking malicious activity, and opening pathways for lateral movement within a network.

December 2024

Threat Types by Category



Trojan.Emotetu/Buecsvii: A sophisticated and highly modular Trojan that has evolved into one of the most dangerous malware strains in the cyber threat landscape. Originally designed to steal financial credentials, this Trojan now serves as a multi-functional malware loader, enabling distribution of additional payloads such as ransomware, spyware, and other Trojans. Once executed, it establishes persistence on the infected system, connects to a command-and-control (C2) server, and downloads additional modules tailored to the attacker's objectives. These modules may include data exfiltration, credential theft, or lateral movement tools to expand the infection within a network. What sets it apart is its ability to adapt and evade detection through advanced obfuscation techniques, such as polymorphic code and encrypted communication with its C2 servers.

Trojan.Sirefef/Zeroaccess: A highly stealthy Trojan that is primarily known for its ability to establish a botnet, distribute other malware, and conduct click fraud or cryptocurrency mining. It operates by exploiting vulnerabilities in systems to gain unauthorized access and establish persistence. Once installed, it often modifies the Master Boot Record (MBR) or system drivers, making it difficult to detect and remove. The Trojan uses a peer-to-peer (P2P) communication protocol, allowing infected systems to function as part of a decentralized botnet that can evade traditional command-and-control (C2) server takedowns. Once active, it performs a variety of malicious tasks, such as downloading additional payloads, redirecting web traffic for click fraud, or utilizing system resources for cryptocurrency mining, which can severely degrade system performance.

Trojan.Hesperbot/Foreign: An advanced Trojan designed to steal sensitive financial information and facilitate unauthorized access to online banking accounts. Known for its sophisticated features and stealthy behavior, it establishes persistence on the infected system, often using rootkit components to avoid detection and is equipped with a wide array of malicious capabilities, including keylogging, screen capturing, video recording, and form grabbing, allowing attackers to collect login credentials and other sensitive data. One of its standout features is the ability to inject malicious code into legitimate banking sessions, redirecting victims to fake login pages or prompting them to download additional malware, enabling attackers to bypass multi-factor authentication (MFA) and compromise accounts even on secure platforms. The modular design and encrypted communication with its command-and-control (C2) servers make it highly adaptable and difficult to detect.

Trojan.Mediyes/Rootkit: A stealthy and highly dangerous piece of malware designed to infiltrate systems, establish deep persistence, and enable attackers to carry out a variety of malicious activities while evading detection. Combining the capabilities of a Trojan and a rootkit, Mediyes can remain hidden within an infected system while providing attackers with backdoor access and control. Once executed, it installs itself at the kernel level, modifying system processes and critical files to mask its presence, and its functionality allows it to intercept and manipulate system calls, effectively hiding files, processes, and network activities from both users and security tools. The Trojan component of Mediyes facilitates data theft, including capturing sensitive information like credentials and payment details. It can also enable attackers to inject malicious code into web traffic, redirecting victims to phishing sites or facilitating click fraud and may serve as a downloader for additional malware payloads, amplifying its impact.

Ransomware Payloads Blocked

Trojan.lockbit/fragtor: A highly sophisticated and destructive ransomware variant associated woith the LockBit ransomware group known for its rapid encryption speed and evolving techniques. Once executed, the payload disables security tools, terminates processes, and encrypts files on infected systems, appending a unique extension to the encrypted files. What sets LockBit/Fragtor apart is its advanced capabilities, including anti-analysis mechanisms such as code obfuscation, sandbox evasion, and self-destruction features. It often spreads laterally within networks by exploiting weak credentials, unprotected RDP (Remote Desktop Protocol) connections, or privilege escalation techniques. The Trojan's modular design allows attackers to customize payloads, making it adaptable to various attack scenarios.

Trojan.phobos/zusy: A dangerous and highly adaptable ransomware associated with ransomware campaigns and financial theft observed in various attack campaigns targeting a wide range of industries. Once executed, it establishes persistence on the infected system, encrypts critical files, and appends a unique extension. In addition to ransomware capabilities, some variants include information-stealing functions, such as capturing credentials, browser data, and payment details. It uses sophisticated evasion techniques, such as code obfuscation and sandbox detection to avoid detection by antivirus software, and disables system restore points, making recovery more challenging.

Ransomware.lockbit/blackmatter: A sophisticated and highly destructive ransomware strain known for its efficiency, stealth, and adaptability, it combines features from both the LockBit and BlackMatter ransomware families, making it a formidable threat. Once inside, the ransomware spreads laterally, exploiting privilege escalation and weak network segmentation to gain control of critical infrastructure and encrypts files rapidly. A defining feature is its ability to disable security solutions, delete backups, and evade detection using advanced obfuscation techniques. It often exfiltrates data before encryption, enabling attackers to threaten victims with data leaks if ransom demands are not met–known as double extortion.

Ransomware.akira/dacic: A potent ransomware strain associated with the Akira ransomware group known for its aggressive tactics and evolving techniques that scans the network for critical assets, disables security tools, and encrypts files with strong encryption algorithms, appending a distinct extension to the affected files. Its advanced capabilities include data exfiltration before encryption, making victims susceptible to data exposure even if backups are available, and its stealth features, such as process obfuscation and evasion of antivirus tools, allow it to bypass traditional security measures.

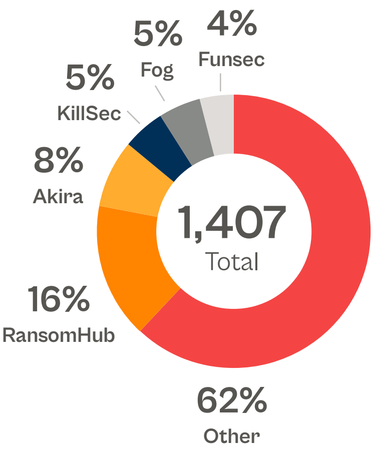
Ransomware.incransom/imps: A ransomware variant known for its stealthy infection methods and aggressive extortion tactics associated with the INC ransomware group. Once it infiltrates a system, it encrypts files using strong encryption algorithms, rendering them inaccessible. A unique feature is its ability to disable security defenses and delete shadow copies, making file recovery difficult without backups. Some versions also include double extortion tactics, where attackers exfiltrate sensitive data before encryption and threaten to publish or sell it if the ransom is not paid.

Halcyon Attacks Lookout

Halcyon provides timely news and analysis on the ransomware economy and tracks hundreds of ransomware attacks every month on our *Halcyon Attacks Lookout* website, including details on the attackers, victims, industry verticals, geolocations impacted and more.

Here's what we tracked for the Q4-2024 period:

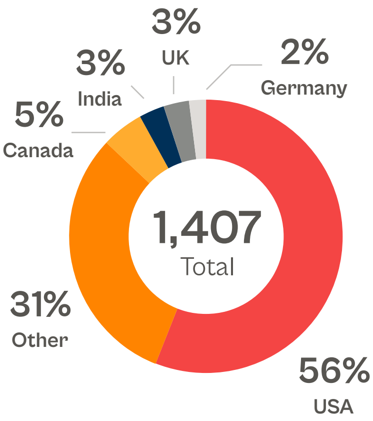
Total Attacks By Group



Top 5 Threat Groups:

- **RansomHub:** 220
- **Akira:** 116
- **Play:** 76
- **Fog:** 66
- **Funksec:** 60
- (**Other:** 869)

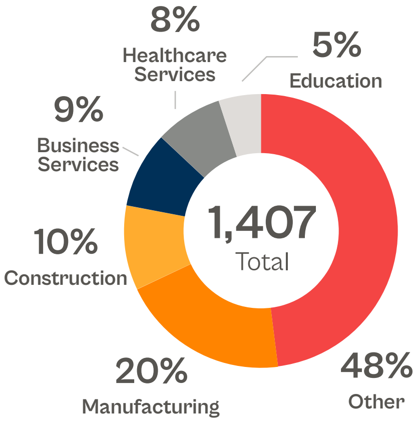
Attacks Per Country



Top 5 Countries:

- **USA:** 768
- **Canada:** 69
- **India:** 49
- **UK:** 47
- **Germany:** 43
- (**Other:** 431)

Most Targeted Industries



Top 5 Industries:

- **Manufacturing:** 280
- **Construction:** 133
- **Business Services:** 131
- **Healthcare Services:** 119
- **Education:** 75
- (**Other:** 669)

Q4-2024 Trends

Some interesting trends emerged in the final quarter of 2024:

Ransomware at Scale:

- **H1-2024: Ransomware Attacks Increased 68% in Severity:** According to Coalition's 2024 Cyber Claims Report: Mid-Year Update, while the frequency of ransomware attacks slightly decreased in early 2024, their severity intensified.
- **Ransomware Attack on Blue Yonder Disrupts Supply Chain:** The attack disrupted its private cloud services, affecting several key clients, including UK grocery chains and Fortune 500 companies.
- **Losses from Change Healthcare Ransomware Attack Approach $3B:** UnitedHealth Group (UHG) has revised its estimate of the costs related to the cyberattack on its Change Healthcare IT services, raising the figure to nearly $2.9 billion for fiscal year 2024.
- **Number of Ransomware Operations Disrupted in 2024: Nearly Zero:** From coordinated takedowns to high-profile arrests, authorities managed to dismantle infrastructure, disrupt operations, and hold critical players accountable. However, the overall ransomware landscape continues to grow in both scale and impact.

Advancing TTPs:

- **Latest Qilin.B Ransomware Features Better Evasion and Stronger Encryption:** This strain employs AES-256-CTR encryption with AESNI support for faster performance on modern CPUs, while using ChaCha20 for older systems. It also utilizes RSA-4096 to secure encryption keys, making decryption nearly impossible without the private key.
- **New LockBit4 Ransomware Payload May Emerge in 2025:** LockBit ransomware, despite significant law enforcement actions earlier this year, is poised to return with its fourth iteration, LockBit 4.0, set to launch on February 3, 2025, according to the gang's alleged leader, "LockBitSupp," who announced the comeback via a dark web post.
- **ClOp Ransomware Group Embarks on Extensive Cleo Exploit Campaign:** ClOp, which claimed responsibility for the Cleo attacks in mid-December, announced on its Tor-based website that victims are being contacted with proof of data theft and offered a final chance to pay a ransom before their names are revealed.
- **Akira Develops Rust-Based Ransomware to Target ESXi Servers:** The Akira ransomware gang have developed a Rust variant to target VMware ESXi servers, marking a significant evolution in their technical architecture by transitioning from C++ to Rust for its new ESXi encryptor variant.
- **Black Basta Leveraging Microsoft Teams for Social Engineering:** Black Basta has shifted tactics from email-based phishing to impersonating IT help desk staff on Microsoft Teams for initial infection.

Threats to Critical Infrastructure:

- **TSA Proposes Cybersecurity Mandates for Rail, Airlines and Pipelines:** The Transportation Security Administration (TSA) has issued proposed cybersecurity regulations aimed at solidifying and expanding emergency directives first implemented after the 2021 Colonial Pipeline ransomware attack.

- **Cyberattack Disrupts American Water - Largest Water Utility in the US:** American Water, which serves over 14 million people across 14 states and operates on 18 military installations, said it discovered the unauthorized activity and took immediate action, including pausing its billing systems.

- **Ransomware and Data Exfiltration Attacks Put Energy Sector at Risk:** The attack on ENGlobal Corporation, and the recent confirmation by Schneider Electric of a ransomware attack that resulted in the breach of 40 GB of sensitive data, highlight a growing national security concern about the cascading risks posed by cyberattacks on critical suppliers to the energy sector.

Ransomware Fallout:

- **MOVEit Exploit Fallout: Massive Data Leak from Amazon, McDonald's and 1000+ Companies:** Notable impacted companies include Amazon (2.8 million records), MetLife (585,000 records), and HSBC (280,000 records), among others, revealing the scope of compromised employee information.

- **UMC Struggles to Recover from Extensive Ransomware Attack:** UMC acknowledged that there is still work to be done, particularly with restoring more patient-facing systems and internal programs crucial for patient care.

- **Ransomware Attacks - The New Snow Day for Schools:** CISA issued a stark warning about the rising threat of ransomware attacks targeting the education sector and updated its cybersecurity guidelines for K-12 organizations.

Takeaway

The war on ransomware escalated in 2024 as international law enforcement agencies ramped up their efforts, delivering key blows to some of the most notorious cybercriminal networks.

From coordinated takedowns to high-profile arrests, authorities managed to dismantle infrastructure, disrupt operations, and hold critical players accountable. However, while these actions mark significant progress, the overall ransomware landscape continues to grow in both scale and impact.

Despite a small handful of high-profile arrests, ransomware operators remain as adaptive and resilient as ever, leveraging cutting-edge innovation to maintain their dominance.

Attackers are increasingly sophisticated, employing advanced encryption techniques, exploiting zero-day vulnerabilities, and diversifying their extortion methods to maximize profits. As a result, ransomware attacks are not only rising in frequency but also causing greater harm to victim organizations, their customers, and the broader economy.

The ripple effects of these attacks extend far beyond the initial breach. Victim organizations face skyrocketing costs for incident response, legal fees, and regulatory compliance as governments worldwide impose stricter reporting requirements and penalties.

Meanwhile, downstream organizations–those reliant on the impacted entities–suffer from supply chain disruptions, loss of revenue, and reputational damage. The economic toll is staggering, with recovery efforts often stretching into months and costing millions.

The following represent the only significant law enforcement actions against ransomware operators over the course of 2024, and when measured against the number and severity of reported attacks during the year, they don't even represent a drop in the proverbial bucket:

LockBit Targeted in "Operation Cronos": In February, a joint law enforcement operation known as "Operation Cronos" set its sights on the prolific LockBit ransomware group. Authorities in Ukraine, Poland, and the United States executed simultaneous actions, taking control of key darknet infrastructure and arresting several affiliates. Most notably, the operation resulted in the release of a decryptor for LockBit 3.0, providing a lifeline for victims to recover their encrypted data without succumbing to ransom demands. While Operation Cronos disrupted LockBit's momentum, its decentralized affiliate structure poses challenges for long-term suppression.

Operation Endgame Disrupts Botnets Fueling Ransomware: In May of 2024, Europol escalated efforts further with "Operation Endgame" targeting the foundational infrastructure supporting ransomware campaigns. Four suspects were arrested across Ukraine and Armenia, and over 100 servers were seized or disrupted. The operation zeroed in on malware loaders and botnets–IcedID, Smokeloader, SystemBC, Pikabot, and Bumblebee–which have long served as the first stage in deploying ransomware payloads. Europol temporarily weakened ransomware groups' ability to scale attacks, but the longterm impact was negligible.

Ransomware Cartel Leader Arrested in Spain: In August, Spanish authorities, working alongside global partners, apprehended the suspected leader of the Ransom Cartel in Estepona, Málaga. The individual allegedly orchestrated a sprawling cybercrime operation specializing in ransomware and malvertising, with annual fraud estimates reaching $34 million. The Ransom Cartel is believed to share operational ties with former REvil/Sodinokibi affiliates, leveraging similar tools and tactics. This arrest highlights the enduring trend of threat actors pivoting and rebranding after major takedowns to continue operations under new banners.

Phobos Ransomware Operator Indicted in the U.S.: In November, U.S. authorities indicted Evgenii Ptitsyn, a 42-year-old Russian national linked to the Phobos ransomware operation. Operating under pseudonyms like "derxan" and "zimmermanx", Ptitsyn is accused of designing and distributing Phobos on darknet forums. Phobos primarily targets small-to-midsize businesses (SMBs), exploiting weaker cybersecurity defenses to maximize success. To date, Phobos operators have victimized over 1,000 entities globally, extorting more than $16 million. Despite Ptitsyn's indictment, Phobos remains a persistent threat, with its affiliate-driven model ensuring continued proliferation.

Let's Face it, We Are on Our Own

The harsh reality is that organizations have been left to fend for themselves against sophisticated adversaries who operate with the support and safe harbor of rogue states. There is simply no way that we can expect a local hospital or small regional utility to withstand an attack while every day we see large, well-resourced victims fall prey to ransomware operators.

The ransomware economy has ballooned into a multi-billion-dollar industry, relentlessly targeting critical infrastructure like healthcare systems and key supply chain providers with impunity. The number of arrests – or lack thereof – underscores the fact that we as a nation have no idea how to combat these attacks.

Government responses are wholly inadequate, being limited to simply offering more guidelines, frameworks, and the occasional arrest—none of which stems the tide of these attacks. Relying on the criminal justice system as deterrence is naive at best, and in hindsight will more likely be seen as negligent.

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

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

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

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

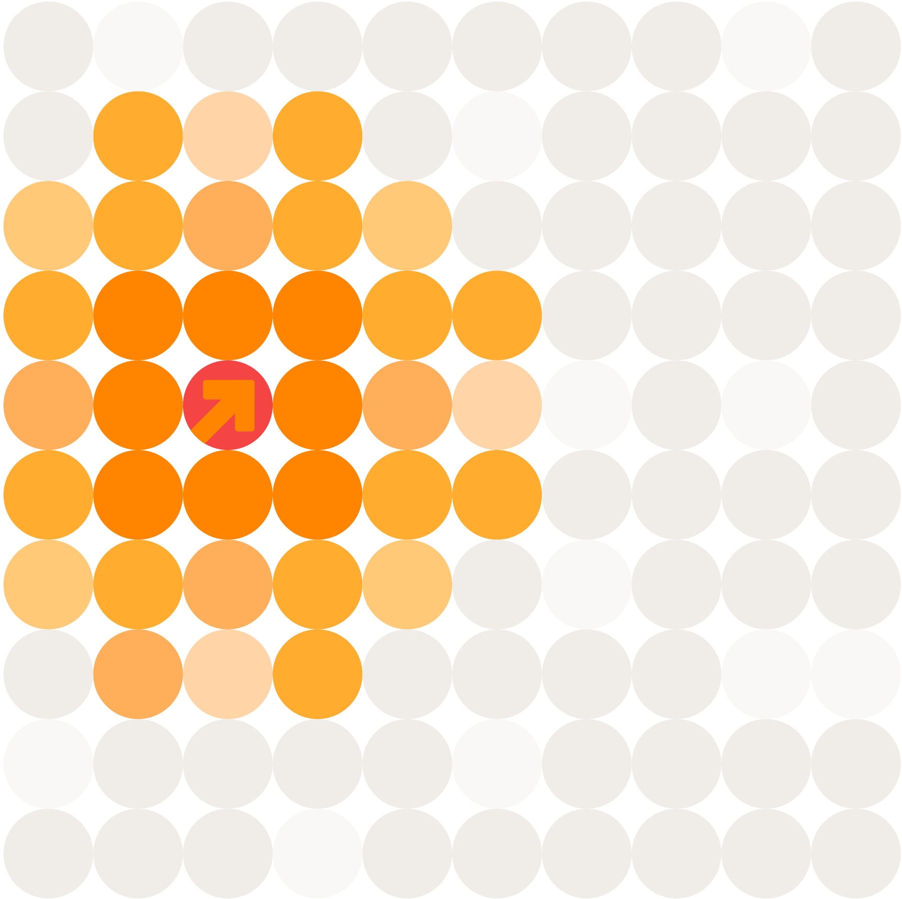
Third-Party Risk Management: In today's interconnected digital environment, managing third-party risk is essential. Organizations often rely on vendors, suppliers, and partners who may introduce additional cyber risks. Tracking third-party risk involves monitoring the number of risk assessments conducted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

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

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

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

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



The Halcyon Mission: Defeat Ransomware

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

halcyon