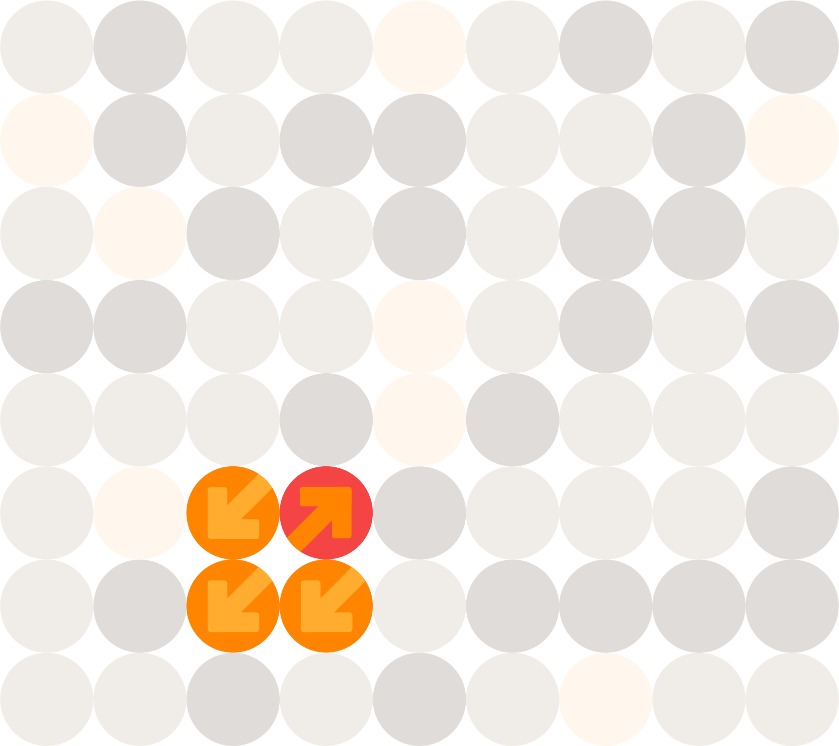
Extortion Attack Group Guide

Power Rankings: Ransomware Malicious Quartile

Q3-2024

halcyon

Table of Contents



Ransom Payments Trending Up in FH-2024

In 2023, a staggering $1 billion in ransom payments was recorded, setting a record largely due to high-profile cyberattacks. Two of the most notable incidents involved Cl0p, a notorious ransomware group that exploited vulnerabilities in a file transfer tool, and BlackCat/ALPHV, which orchestrated a significant attack on Caesars Entertainment's hotel properties. This surge in ransom payments highlights the escalating scale and severity of ransomware attacks targeting organizations across various sectors.

The situation has worsened significantly in 2024. By the end of the first half of the year, ransomware payments reached a staggering $459 million, according to a report by Chainalysis. This figure represents a $10 million increase over the same period in 2023, reflecting a concerning upward trend in ransomware-related extortion. The growing financial impact underscores the heightened capabilities of ransomware groups and the increased pressure on victims to pay.

The situation has worsened significantly in 2024. By the end of the first half of the year, ransomware payments reached a staggering $459 million.

One of the most alarming developments is the spike in ransom demands from some of the most dangerous ransomware groups. In early 2023, the median ransom payment stood at $198,939. However, by mid-2024, this figure skyrocketed to $1.5 million. This sharp increase suggests that ransomware operators have become more adept at infiltrating deeper into targeted networks and exfiltrating sensitive data. By leveraging this stolen information, cybercriminals exert greater pressure on organizations to comply with their demands, often threatening to release critical or damaging data if ransoms are not paid.

Blockchain analysts have also uncovered evidence of a record-breaking ransom payment, with one victim organization paying a colossal $75 million in response to a single attack. This aligns with research from other cybersecurity firms, which reported a median ransom payment of $2.2 million for 49 state and local governments in the first half of 2024. These figures illustrate the increasing financial stakes, especially for public sector entities that may be particularly vulnerable to cyberattacks.

In parallel with the rising costs, the frequency of ransomware attacks has increased by 10% in 2024 compared to the previous year. Despite the rising number of incidents and the growing ransom amounts, there is evidence to suggest that fewer victims are opting to pay. This could be due to a combination of factors, including improved recovery strategies, cybersecurity awareness, and reluctance to fund criminal enterprises. However, even with fewer payments, the overall impact remains severe.

The rise of ransomware as an industry poses an unprecedented threat. The combination of more sophisticated attackers, evolving ransomware variants, and escalating ransom payouts has created a dangerous environment for businesses and governments alike. The financial losses inflicted on organizations are staggering, and these costs are not isolated to the companies targeted–they will ultimately trickle down to consumers through increased costs for goods and services, as well as higher insurance premiums.

Moreover, the true financial toll of ransomware attacks may be significantly underreported. According to FBI estimates, based on intelligence gathered during their infiltration of the Hive ransomware group, only about 20% of ransomware attacks are actually reported to law enforcement. This suggests that the actual economic damage could be much higher–potentially closer to $5 billion when factoring in unreported incidents.

The Change Healthcare ransomware attack resulted in recovery costs exceeding $1 billion, underscoring the immense burden organizations face in the aftermath of such incidents.

It is important to note that this $5 billion estimate only accounts for ransom payments. It does not include the additional costs of recovery, which can be immense. For instance, the Change Healthcare ransomware attack resulted in recovery costs exceeding $1 billion, underscoring the immense burden organizations face in the aftermath of such incidents. These costs go beyond immediate financial outlays and include longer-term consequences like brand damage, potential lawsuits, and regulatory fines–all of which can have lasting impacts on an organization's reputation and financial stability.

Ransomware has evolved into a massive, highly organized industry, with devastating economic consequences. The financial burden affects businesses, governments, and consumers alike, creating a significant drag on the global economy. To curb the growth of this industry, it is essential to make ransomware operations less profitable for attackers. Unfortunately, this remains a distant goal, as cybercriminals continue to exploit weaknesses in cybersecurity defenses.

One of the key strategies employed by ransomware groups is the exploitation of unpatched vulnerabilities and misconfigurations within systems. Threat actors have become increasingly efficient in automating their attacks, allowing them to target a larger number of victims more quickly. The mass exploitation of vulnerabilities such as those found in MoveIT, GoAnywhere, and Citrix Bleed are stark reminders of how many of these attacks could be prevented if organizations prioritized timely patching.

To build resilience against ransomware, organizations must strategically invest in maintaining business continuity and ensuring rapid recovery from attacks. This involves not only securing networks but also developing robust contingency plans to minimize downtime and financial loss. Without these investments, companies will continue to fuel the ever-growing ransomware economy, which thrives on the vulnerabilities of underprepared organizations. In the absence of a comprehensive approach to combating ransomware, the economic toll will continue to rise, with no signs of slowing down.

While we cannot stop ransomware attacks, we can prevent them from being successful.

This is why 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 Q3-2024, which can be reviewed along with earlier reports here: *Power Rankings: Ransomware Malicious Quartile*.

The mass exploitation of vulnerabilities such as those found in MoveIT, GoAnywhere, and Citrix Bleed are stark reminders of how many of these attacks could be prevented if organizations prioritized timely patching.

Ransomware MQ: Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q3-2024 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 Q3-2024 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

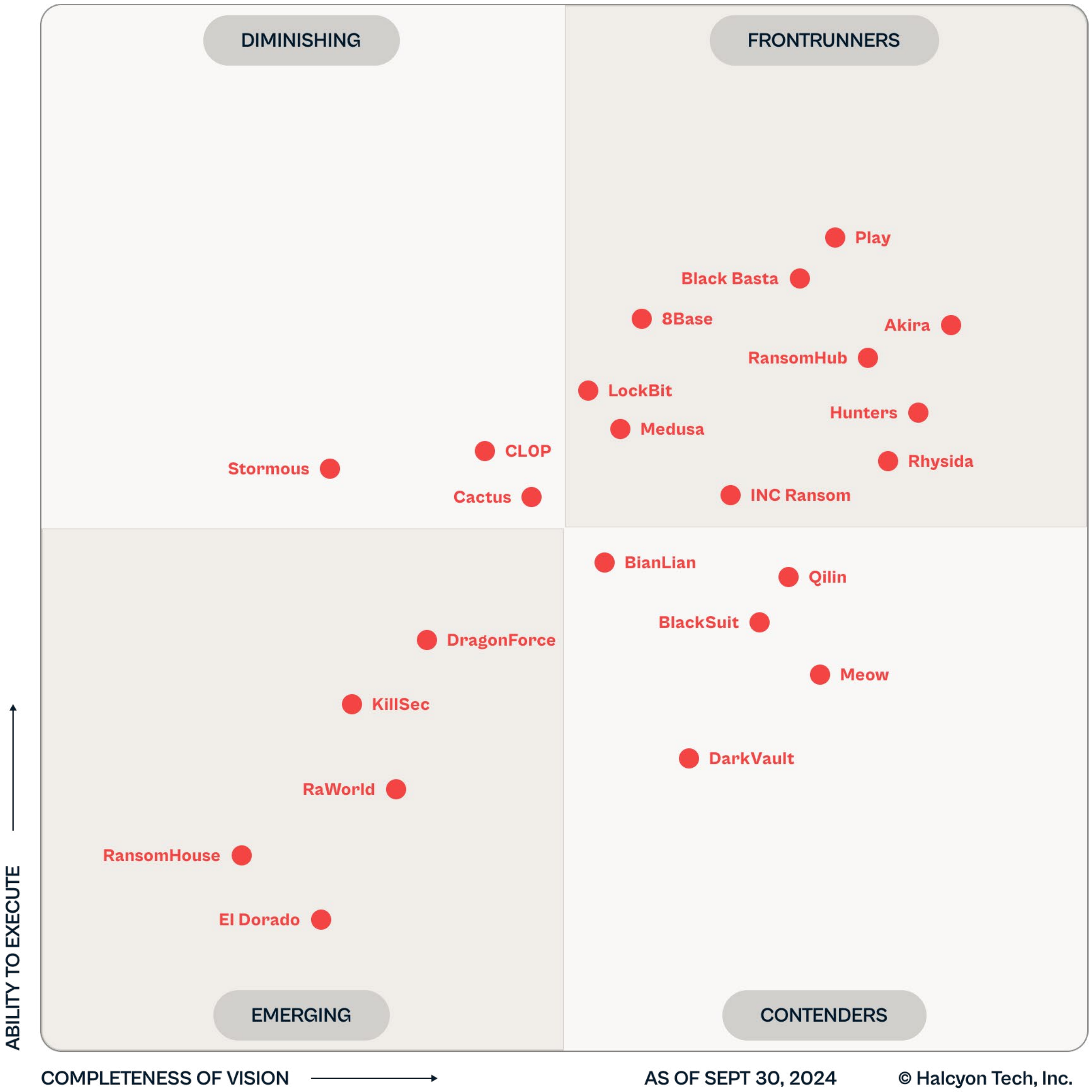
RaaS Platform Development: Attack groups were evaluated on evidence of continued development and improvement of the RaaS platform and TTPs.

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 Q3-2024 Ransomware Malicious Quartile

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



AS OF SEPT 30, 2024

© Halcyon Tech, Inc.

Source: Halcyon (Q3 2024)

Frontrunners

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 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 the first half of 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.

The FBI issued a joint advisory highlighting Play's significant impact, revealing that the group had successfully compromised over 300 organizations.

- **Victims:** 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. 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 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. 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. Their ability to adapt their targets and tactics highlights Play's evolving strategy in maximizing the reach and impact of their operations.

- **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), or stolen credentials from Initial Access Brokers (IABs), to gain initial access to networks. The group also frequently leverages social engineering techniques, such as phishing emails and other deceptive tactics, to bypass security defenses and compromise targets. 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:** 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, a RaaS group that emerged in early 2022, is believed to be an offshoot of the defunct Conti and REvil gangs. The group is known for its sophisticated ransomware that targets both Windows and Linux systems. Black Basta has a 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. 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.

8Base quickly ascended the ranks of active ransomware operators with a high volume of attacks throughout 2023 and the first half of 2024.

- **Attack Volume:** 8Base quickly ascended the ranks of active ransomware operators with a high volume of attacks throughout 2023 and the first half of 2024, making them one of the most active groups.
- **Ransom Demands:** It is unclear how much 8Base typically demands for a ransom.
- **Victims:** 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:** 8Base, which emerged in March 2022, has quickly established itself as a significant threat actor, particularly notable for its surge in activity during the first half of 2024. This rapid growth suggests potential connections to seasoned RaaS operators, possibly linked to RansomHouse, a data extortion group active from late 2022 to early 2023. There are also indications of a possible association with the leaked Babuk builder. 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.
- **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. 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.
- **Victims:** Nissan, Royal College of Physicians and Surgeons, 4LEAF, Park-Rite, Family Day Care Services, The McGregor, Protector Fire Services, QuadraNet Enterprises, Southland Integrated

> Akira's distinctive extortion platform includes a chat feature, which facilitates direct negotiation between victims and attackers–an unusual practice among ransomware groups.

Innovation

- **RaaS Platform Development:** Akira operates a sophisticated RaaS platform written in C++ that targets both Windows and Linux systems. 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. 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 a zero-day vulnerability (CVE-2023-20269) in Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software to conduct brute-force attacks. The group has also been seen leveraging VMware ESXi vulnerabilities to facilitate lateral movement within compromised networks.

- **Targeted Industries:** In the first half of 2024, Akira intensively targeted 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

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.

Strict policy enforcement 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. By the end of Q3, it was responsible for many attacks across various sectors.
- **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, 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 ransomware code is derived from Knight ransomware, which is written in Golang. 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.
- **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. 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

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.

- **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, 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.

> 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.

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

Hunters International

Performance

- **RaaS Platform:** Hunters International, a RaaS group, emerged from the remnants of the defunct Hive ransomware group. 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 the first half of 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, NanoLumens, Integrated Control, Frederick Wildman and Sons, Kablutronik SRL, Caxton and CTP Publishers and Printers, Austal USA.

Building on Hive's advanced infrastructure, Hunters International has adopted a sophisticated platform that leverages both data exfiltration and double extortion tactics.

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. 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.

Medusa

Performance

- **RaaS Platform:** Medusa, a RaaS platform that emerged in the summer of 2021, has rapidly ascended to become one of the most active and formidable ransomware groups. By the second quarter of 2024, Medusa's attack volume had surged significantly, positioning it as one of the top ransomware threats in the landscape. The group 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 in the first half of 2024, but attack volume has begun to decline.
- **Ransom Demands:** Medusa typically demands ransoms in the millions of dollars which can vary depending on the target organization's ability to pay.
- **Victims:** Toyota Financial Services, 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.

By the second quarter of 2024, Medusa's attack volume had surged significantly, positioning it as one of the top ransomware threats in the landscape.

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. To prevent rollback and recovery, Medusa deletes Volume Shadow Copies by abusing the vssadmin command. 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.

  ⚠ **CISA Alert:** CISA Alert aa22-181a

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

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

portal on the Tor network, providing a platform for negotiations and updates. Notable attacks attributed to Rhysida include incidents involving the Chilean military and, more recently, Prospect Medical Holdings. The latter attack severely impacted operations at hundreds of clinics and hospitals across the United States. 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 Q3 2024. However, their attack volume remains modest compared to leading ransomware groups. Rhysida appears to operate as opportunistic attackers.
- **Ransom Demands:** Ransom 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:** 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.

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

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. 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:** Rhysida has been observed targeting the healthcare, education, Government, manufacturing, and tech industries.
- **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.

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 through early 2024.
- **Ransom Demands:** INC instructs victims to log into a Tor portal with a unique user ID provided by the attackers. It is unclear what the average ransom demand is at this point.
- **Victims:** Peruvian Army, 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.

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.

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, and AnyDesk to facilitate lateral movement within compromised networks. 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.

- **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.

Contenders

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 less complicated 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 Q2 and Q3 of 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, Griffing & Company, International Biomedical Ltd, Gilbreath, Dow Golub Remels & Gilbreath, Instron, Pelindo, CHU de Rennes, Dekko Window Systems Ltd, CMC Marine.

In early 2023, BianLian shifted away from deploying ransomware payloads, focusing instead on less complicated data exfiltration and extortion attacks.

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.

- **Targeted Industries:** BianLian primarily targets critical infrastructure, financial institutions, healthcare, manufacturing, education, entertainment, and energy sectors by leveraging compromised Remote Desktop Protocol (RDP) credentials.
- **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.

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.
- **Attack Volume:** Qilin's attack volume surged significantly in the first half of 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, 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.

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).

Innovation

- **RaaS Platform Development:** 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. This method is typically implemented after gaining initial network access, often facilitated by phishing campaigns or the use of compromised credentials obtained from previous breaches or dark web markets.
- **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.

BlackSuit

Performance

- **RaaS Platform:** BlackSuit operates as a private ransomware group rather than a traditional RaaS with affiliates. BlackSuit ransomware share similarities with Royal ransomware in terms of code structure and encryption methodology. Both use 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.

Ransom demands for BlackSuit have been observed as high as $18 million, with average demands starting around $2.5 million.

- **Attack Volume:** BlackSuit has quickly gained notoriety for striking a variety of sectors with considerable impact, and activity in 2024 has been 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. Ransom demands for BlackSuit have been observed as high as $18 million, with average demands starting around $2.5 million.
- **Victims:** ZooTampa, Southwest Binding & Laminating, Western Municipal Construction, CDK Global, Kansas City Police Department, Multi-Fill.

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.
- **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.

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.

- **Attack Volume:** Attack volume has increased significantly in 2024.
- **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.

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 software exploits to gain 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.
- **Targeted Industries:** Meow primarily targets the healthcare and education sectors but may be opportunistic in targeting industries with valuable or sensitive information that can be leveraged to compel payment.
- **Economic Model**: Meow appears to be shifting from double extortion to straight data exfiltration for extortion.

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:** By mid-2024, DarkVault had already claimed at least 19 victims. Given its swift expansion and secretive operations, it's anticipated that the group's attack volume will continue to increase, particularly as it focuses on high-value targets in sectors like financial services, where sensitive data is at greater risk.
- **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.

DarkVault engages in various cybercriminal activities such as bomb threats, swatting, doxing, and defacing websites, making them a dangerous and unpredictable entity.

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.

Emerging

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:** DragonForce has been highly active with numerous attacks reported in the first three quarters of 2024. Their attack campaigns are frequent, and their success rate appears substantial given the number of high-profile victims.
- **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:** Seafrigo Group, Ohio Lottery, Yakult Australia, Coca-Cola Singapore.

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.

Innovation

- **RaaS Platform Development:** DragonForce continues to enhance and refine its RaaS platform by integrating advanced features and tactics from the LockBit ransomware. Their use of sophisticated double extortion methods–encrypting data while simultaneously threatening to leak it–demonstrates their ongoing commitment to improving their operational capabilities. 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. By focusing on sectors with critical operations and high-stakes data, DragonForce maximizes its chances of securing significant ransom payments, reinforcing their reputation as a formidable threat.
- **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. 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.

KillSec

Performance

- **RaaS Platform:** KillSec is a RaaS that 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.
- **Attack Volume:** KillSec's attack volume has been on a steady rise since it became more active in late 2023.
- **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.

KillSec is a RaaS that emerged in 2021 as a hacktivist group aligned with the Anonymous movement. Initially known for website defacements and cyber-attacks with ideological motives.

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 distributed denial-of-service (DDoS) tool and an advanced data stealer for gathering sensitive information.
- **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.

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:** In the first three quarters of 2024, RaWorld carried out numerous attacks, with a particular focus on healthcare organizations in Latin America and the financial sector. The group has demonstrated a high success rate in breaching defenses and deploying their ransomware payloads. However, despite their operational effectiveness, RaWorld has not experienced significant growth in scale or attack volume.

RaWorld also employs advanced antivirus evasion techniques, allowing them to remain undetected until the ransomware payload is fully deployed.

- **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:** RaWorld has targeted multiple healthcare organizations in Latin America, along with financial institutions and other businesses in the US and South Korea. Specific victims include several unnamed healthcare providers and financial firms.

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:** RaWorld primarily targets the healthcare and financial sectors, selected for their potential to yield large ransom payments. This strategic focus has proven effective, as demonstrated by their high-profile breaches and the substantial ransom demands that victims have been compelled to pay.

- **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.

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 pale compared to leading threat actors but remain notable with some high-profile attacks in 2024, but the group shows signs they are diminishing.
- **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.

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.

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.

El Dorado

Performance

- **RaaS Platform:** El Dorado, which emerged in March 2024, operates as a RaaS platform designed to target both Linux and Windows systems. 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.

El Dorado strategically targets high-value sectors, such as finance, healthcare, and critical infrastructure, where the financial stakes are high, and disruptions can be costly.

- **Attack Volume:** By June 2024, El Dorado had carried out 16 confirmed attacks, with 13 of these targeting organizations in the United States. However, their activity saw a sharp decline in Q3 of the same year.

- **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:** Victims include companies across various sectors, primarily in the United States. Notable targeted industries included real estate, education, healthcare, professional services, and manufacturing. Specific organizations have not been publicly named, but the distribution indicates a strategic approach to victim selection.

Innovation

- **RaaS Platform Development:** 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 uses the ChaCha20 encryption algorithm for file encryption and RSA-OAEP to secure encryption keys, while also allowing 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 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.

Diminishing

ClOp

Performance

- **RaaS Platform:** In August 2023, ClOp'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, ClOp had virtually disappeared. First observed in 2019, ClOp 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. ClOp 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), and a rare SQL injection zero-day (CVE-2023-34362) used to install a web shell.ClOp'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, ClOp 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:** ClOp 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, ClOp further intensified their operations by exploiting the MOVEit vulnerability (CVE-2023-34362), compromising thousands of organizations globally. However, following this massive wave of attacks, ClOp's activity dramatically declined, and by the latter half of 2024, their attacks had nearly ceased. The rapid shift from aggressive campaigns to near silence suggests a possible reorganization or a strategic pause, though the group's ability to leverage widespread vulnerabilities remains a notable concern.
- **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 ClOp focuses more on the exfiltration of sensitive data.

ClOp 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.

- **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's GoAnywhere MFT server, 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.

- **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

Stormous

Performance

- **RaaS Platform:** Stormous is not a RaaS operation but rather an independent data extortion group that emerged in mid-2021 or early 2022. The group garnered attention after claiming to have exfiltrated 200GB of data from high-profile victims, including Epic Games and the Ministry of Foreign Affairs of Ukraine. Despite the headlines, their actual capabilities remain under question, and the group's claims of large-scale data breaches have not always been verified, leading some to conclude that their operations may be more opportunistic than technically advanced.
- **Attack Volume:** Stormous attack volume had escalated following its partnership with GhostSec, but then declined significantly in 2024.
- **Ransom Demands:** It is unclear how much Stormous demands for ransom payments on average, but the largest observed random demand from the group is $500,000.
- **Victims:** Vietnam Electricity, Duvel Moortgat Brewery, Konika Minolta, Cameron Memorial Community Hospital, Econocom Group, Senior Sistemas, Bandung Institute of Technology, Epson Spain, Interep.

> Despite the headlines, their actual capabilities remain under question, and the group's claims of large-scale data breaches have not always been verified, leading some to conclude that their operations may be more opportunistic.

Innovation

- **RaaS Platform Development:** Stormous operates without a RaaS platform, focusing primarily on direct data extortion. In 2024, Stormous began collaborating with a smaller threat actor known as GhostSec. This partnership has led to Stormous incorporating the GhostLocker encryptor, developed by GhostSec, into some of their more recent attacks. As part of their evolving tactics, Stormous has also adopted a double extortion strategy, where they not only exfiltrate sensitive data for ransom but also deploy encryption payloads to lock victims' systems, adding further pressure to comply with their demands. This collaboration signals an expansion of Stormous' capabilities, blending their expertise in data extortion with the encryption tools provided by GhostSec to enhance the effectiveness of their attacks.

- **Targeted Industries:** Stormous claims to target Western companies and espouses a lot of rhetoric about the Russian and Ukrainian conflict, but it is not clear if they are hacktivist-oriented or using this to sew confusion.
- **Economic Model**: The exact operational structure of Stormous remains unclear. While they claim to target organizations for political reasons, their activities appear to be more opportunistic, possibly aimed at profiting from the chaotic environment created by the surge in ransomware attacks. It is suspected that Stormous may attempt to exploit the confusion surrounding high-profile attacks by other threat actors, leveraging the disruption to extract ransoms from already-compromised victims. In 2024, Stormous began employing double extortion tactics, combining data theft with ransomware encryption to maximize pressure on their targets. However, despite these efforts, the group seems to be struggling, with signs that their operations may be faltering and their overall impact declining.

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 a growing threat in the ransomware landscape, as they continue to refine their methods to target organizations across various sectors.
- **Attack Volume:** C Cactus ransomware first surfaced in March 2023 and steadily increased its attack volume through early 2024 but have since decreased activity.
- **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.

Cactus primarily gains initial access by exploiting known vulnerabilities in widely used VPN appliances, allowing them to infiltrate targeted networks with relative ease.

- **Victims:** Schneider Electric, SCS SpA, OmniVision Technologies, The Hurley Group, Cornerstone Projects Group, ICOR Global Limited, Cornerstone Projects Group, Societa' Canavesana Servizi.

Innovation

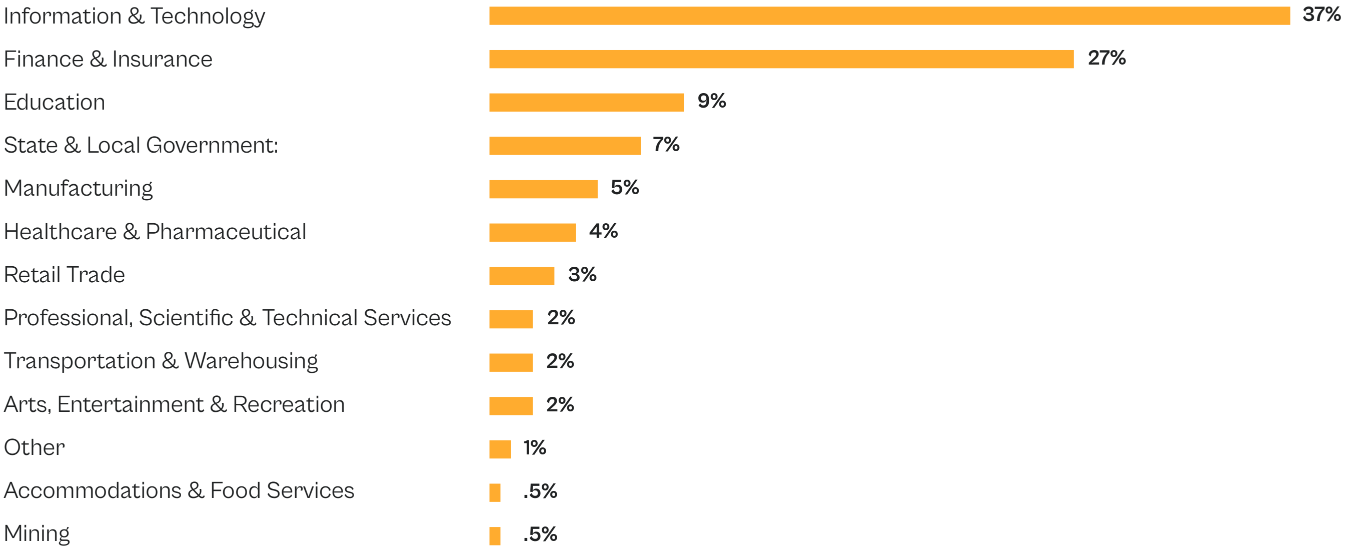
- **RaaS Platform Development:** Cactus ransomware operations rely heavily on Living-off-the-Land (LotL) techniques, which abuse legitimate network tools to avoid detection. These techniques involve the use of trusted tools like Event Viewer, PowerShell, Chisel, Rclone, and Scheduled Tasks to move within targeted networks. 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.
- **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.

Halcyon Threat Insights

Here are the key insights from the Halcyon Threat Research and Intelligence Team findings for July, August, and September of 2024 based on intelligence collected from our customer base:

July 2024

Ransomware Prevented by Industry Vertical



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

Ransomware Precursors Blocked: Trojans

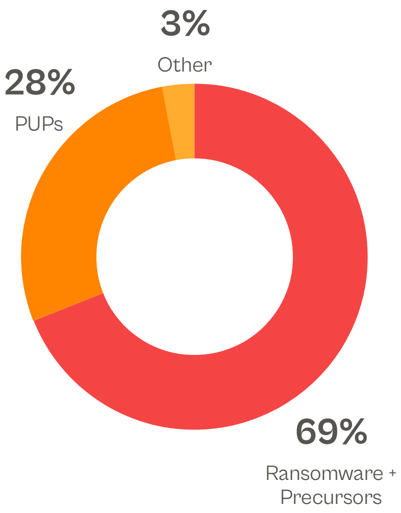
Halcyon detected an array of Trojans that may be precursors to ransomware payloads. It is important to understand that ransomware payloads are the tail-end of an attack, so it is critical to detect precursors prior to infection.

Detecting and blocking trojan activity can prevent attackers from escalating privileges, moving laterally though the network, compromising user credentials, exfiltrating sensitive data and more. Some of the trojans identified in July include:

- **Trojan.chapak/jaik:** Allows remote attackers to gain unauthorized access and control. This Trojan can be used to steal sensitive information, download additional malware and ransomware, or conduct other harmful operations. It often spreads through deceptive methods, such as

July 2024

Threat Types by Category



malicious email attachments, compromised websites, or bundled software downloads. Trojan.Chapak/Jaik poses a serious risk to system security and can lead to data theft, system instability, and further infections.

- **Trojan.msil/msilperseus:** A malicious Trojan written in Microsoft's Intermediate Language (MSIL), targeting systems running on the. NET framework. Once installed, it can execute a range of harmful actions, including stealing sensitive information, logging keystrokes, and downloading additional malware and ransomware. This Trojan often disguises itself as legitimate software to evade detection and can spread through phishing emails, malicious downloads, or compromised websites. Its flexibility and stealth make it particularly dangerous, as it can be customized to perform various malicious activities. Trojan.MSIL/MSILPerseus poses a significant threat to both personal and enterprise security, often leading to severe data breaches and system compromise.

- **Trojan.zeppelin/zapchast:** A highly destructive Trojan that primarily targets Windows systems. Once infiltrated, it typically functions as a backdoor, allowing attackers to gain remote control over the infected device. Known for its adaptability, Zeppelin/Zapchast can be used to deploy ransomware, steal sensitive data, or facilitate further malware infections. It often spreads through phishing campaigns, malicious attachments, or compromised software downloads. The Trojan is designed to evade detection by security tools, making it a significant threat to both individual users and organizations. Its presence on a system can lead to severe data loss, financial damage, and operational disruptions.

- **Trojan.blacklotus/agentb:** A highly advanced and stealthy Trojan designed to infiltrate and compromise systems, often bypassing security measures with ease. It typically acts as a backdoor, providing cybercriminals with remote access and control over the infected device. This Trojan is particularly dangerous due to its ability to evade detection by disabling security features and altering system files. It spreads through phishing emails, malicious links, and compromised software, and can be used to steal sensitive data, deploy additional malware, or launch further attacks. The presence of Trojan.BlackLotus/AgentB on a system can result in significant security breaches and data loss.

- **Trojan.killav/avkill:** Designed to disable or disrupt the functionality of antivirus programs and security software on infected systems. By targeting and terminating processes associated with antivirus tools, it renders the system vulnerable to further attacks. This Trojan often acts as a precursor to more severe malware and ransomware infections, allowing cybercriminals to install additional malicious software undetected. It can be spread through various methods, including email attachments, malicious downloads, or compromised websites, and poses a significant threat to computer security by undermining protective measures.

Ransomware Payloads Blocked:

Halcyon also detected and blocked an array of ransomware payloads that could have significantly disrupted target organizations and their operations:

- **Ransomware.phobos:** A dangerous form of ransomware that typically spreads through compromised Remote Desktop Protocol (RDP) connections, phishing emails, or malicious downloads. The encryption used by Phobos is strong, making data recovery difficult without the decryption key. Phobos primarily targets businesses, leading to significant data loss, operational downtime, and financial harm if backups are not available.

- **Ransomware.hiddentear/msil:** An early open-source ransomware variant written in Microsoft's Intermediate Language (MSIL). Originally created as a proof-of-concept for educational purposes, it has been adapted by malicious actors into a fully functional ransomware threat. This ransomware spreads through phishing emails, malicious downloads, or compromised websites. Its open-source nature has led to numerous variants, making it a persistent threat.

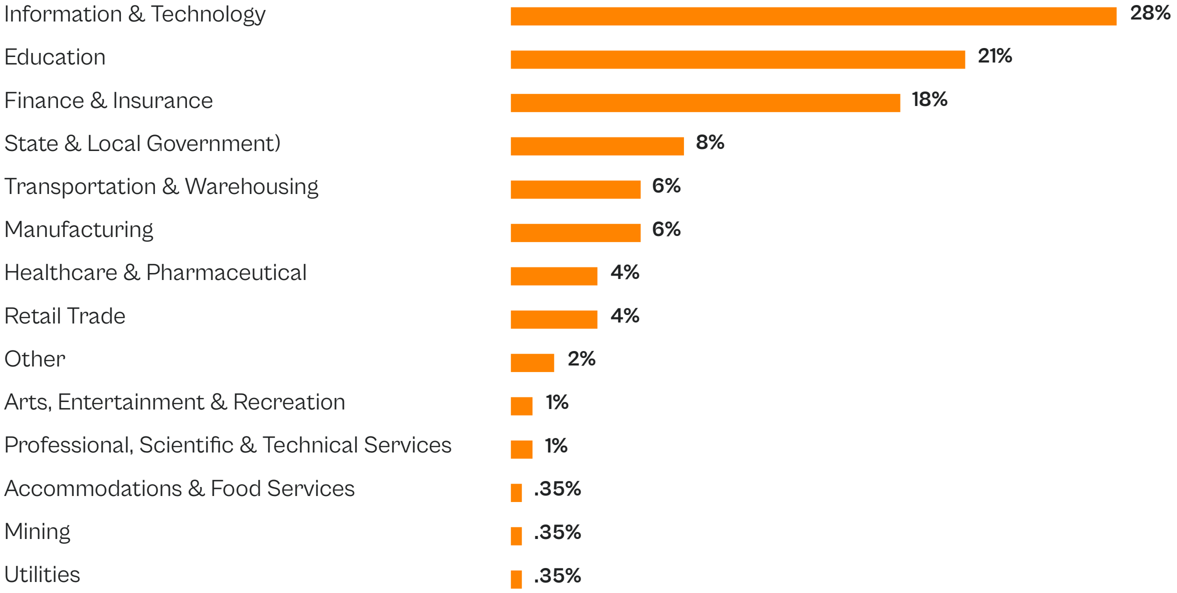
- **Ransomware.akira/ransomx:** An aggressive ransomware variant known for targeting both individual users and organizations. Akira/RansomX is particularly dangerous due to its ability to disable security measures and exfiltrate sensitive data before encryption, which they threaten to leak if the ransom is not paid. This double-extortion tactic makes it a significant threat, leading to severe data loss, operational disruptions, and potential financial and reputational damage for victims.

- **Ransomware.rhysida/ajos:** A highly disruptive form of ransomware that typically spreads through phishing emails, malicious downloads, or vulnerabilities in outdated software. Rhysida/Ajos is particularly dangerous because it often targets businesses and critical infrastructure, leading to significant operational disruptions and financial losses. Its encryption is strong, making recovery difficult without backups or the decryption key.

- **Ransomware.trigona/genie:** A sophisticated ransomware variant that usually spreads through phishing emails, malicious downloads, or exploiting software vulnerabilities. The encryption used is robust, making data recovery nearly impossible without the decryption key. Trigona/Genie is particularly threatening to businesses, as it can lead to severe operational disruptions, data loss, and financial damage.

August 2024

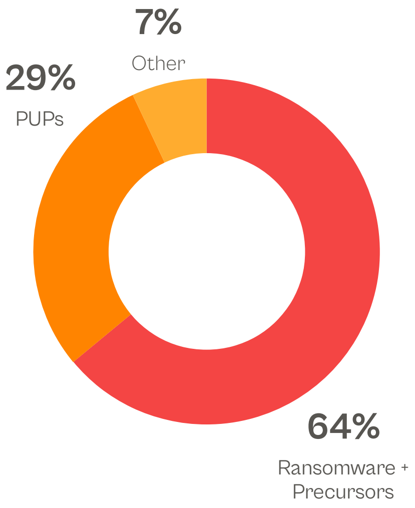
Ransomware Prevented by Industry Vertical



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

August 2024

Threat Types by Category



Ransomware Precursors Blocked: Trojans

Halcyon detected an array of Trojans that may be precursors to ransomware payloads. It is important to understand that ransomware payloads are the tail-end of an attack, so it is critical to detect precursors prior to infection.

Detecting and blocking trojan activity can prevent attackers from escalating privileges, moving laterally though the network, compromising user credentials, exfiltrating sensitive data and more. Some of the trojans identified in August include:

- **Trojan.paradise/msil:** A malicious software that primarily targets systems running Microsoft Intermediate Language (MSIL). It disguises itself as a legitimate program or file to deceive users into installing it. Once executed, it can perform a range of harmful activities, such as stealing sensitive data, allowing remote control of the infected system, downloading additional malware, or disrupting system functionality.

- **Trojan.cosmu/xpiro:** A type of Trojan that is part of the Xpiro malware family and is known for embedding itself deeply within system files, making it difficult to detect and remove. Once active, this Trojan can steal sensitive data, open backdoors for remote attackers, and download additional malicious software. It can also hinder system performance by altering key processes.

- **Trojan.cosmu/xpiro:** A Trojan that integrates itself into system processes and files, making detection and removal challenging. Once installed, it can steal sensitive information, download additional malware, and grant remote access to attackers. This Trojan is also known to disrupt system performance and compromise overall security.

- **Trojan.formbook/razy:** Primarily targets Windows systems and is designed to steal sensitive information, such as login credentials, browser data, and financial details. It can also capture screenshots, log keystrokes, and download additional malware. It operates stealthily, making it difficult for users to detect.

- **Trojan.hesperbot/foreign:** A highly sophisticated banking Trojan designed to steal sensitive financial information from users. Once installed, the Trojan can log keystrokes, capture screenshots, and record online banking activities. It is also capable of creating a remote connection to the infected device, allowing attackers to manipulate transactions and bypass security measures.

Ransomware Payloads Blocked

Halcyon also detected and blocked an array of ransomware payloads that could have significantly disrupted target organizations and their operations:

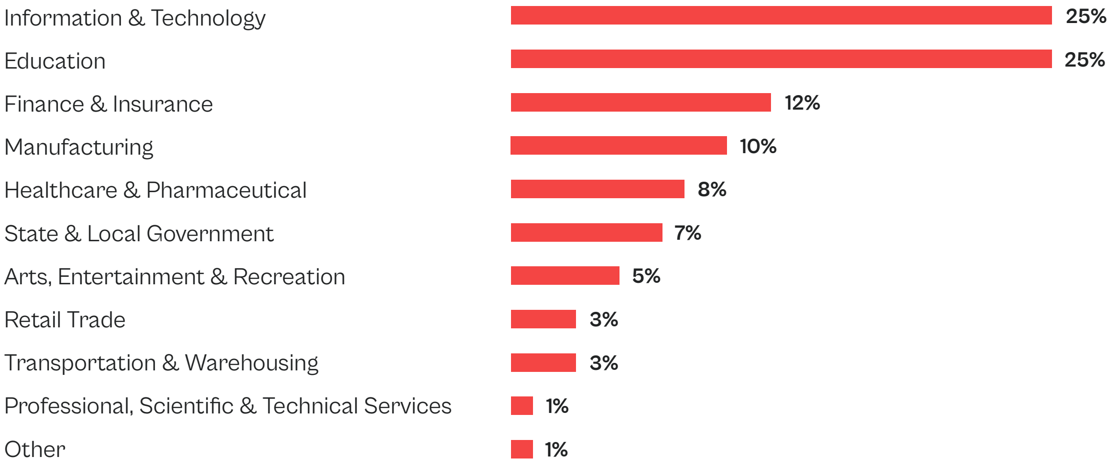
- **Ransomware.agenda/qilincrypt:** Known for its flexibility, this ransomware allows attackers to customize the ransom note, encryption techniques, and attack approach to suit specific targets. It often spreads through phishing campaigns or by exploiting vulnerabilities in software. QilinCrypt poses a serious risk to business operations, leading to financial loss, data breaches, and potential long-term disruption.

- **Ransomware.lockbit/blackmatter:** A highly advanced strain of ransomware combining features from both LockBit and BlackMatter ransomware families that targets businesses and critical infrastructure. It spreads through phishing attacks, exploited software vulnerabilities, or remote desktop protocol (RDP) weaknesses. This ransomware variant is known for its fast encryption speed, ability to evade detection, and the attackers' use of double extortion tactics–threatening to release stolen data if the ransom is not paid.

- **Ransomware.darkrace/imps:** An aggressive ransomware variant that is distributed through phishing emails, malicious downloads, or exploiting system vulnerabilities. DarkRace/IMPS is particularly dangerous due to its ability to spread quickly within networks and evade traditional security measures. In addition to encryption, it may also exfiltrate sensitive data, using double extortion tactics to pressure victims by threatening to leak stolen information.
- **Ransomware.phobos/crysis:** A highly destructive ransomware variant that primarily targets small and medium-sized businesses and spreads through weak remote desktop protocols (RDP), phishing attacks, and malicious downloads. Once inside a system, it encrypts a wide range of file types, appending a unique extension and leaving behind a ransom note with instructions for payment. Phobos/Crysis is known for its robust encryption methods and lack of decryption options without paying the ransom, leaving victims with little recourse.
- **Ransomware.maze/ranpack:** Maze, also known as RanPack, is a ransomware strain that emerged around 2019. Maze typically targets large organizations, and its attacks have affected sectors such as healthcare, finance, and manufacturing. The ransomware is often delivered through phishing emails, exploiting vulnerabilities in outdated software.

September 2024

Ransomware Prevented by Industry Vertical



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

Ransomware Precursors: Trojans

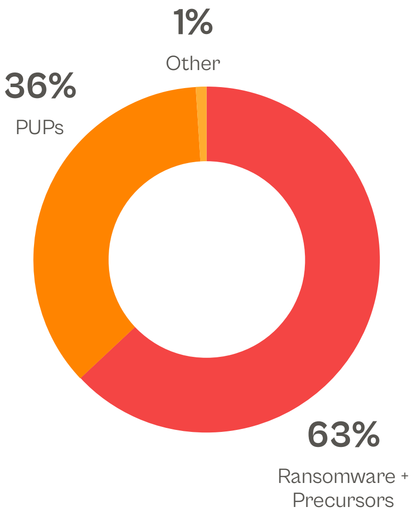
Halcyon detected an array of Trojans that may be precursors to ransomware payloads. It is important to understand that ransomware payloads are the tail-end of an attack, so it is critical to detect precursors prior to infection.

Detecting and blocking trojan activity can prevent attackers from escalating privileges, moving laterally though the network, compromising user credentials, exfiltrating sensitive data and more. Some of the trojans identified in September include:

- **Trojan.msil/reverserat:** A remote access trojan (RAT) written in the Microsoft Intermediate Language (MSIL), targeting Windows-based systems. It enables attackers to remotely control compromised machines, exfiltrate data, and execute malicious commands. Distributed through phishing emails, malicious links, or exploited software vulnerabilities, this trojan is known for its flexibility and stealth. It can capture keystrokes, take screenshots, manipulate files, and deploy additional payloads, posing a severe threat to both personal and enterprise environments. Its advanced evasion techniques make it challenging to detect and remove.

September 2024

Threat Types by Category



- **Trojan.knight/tedy:** Primarily targets Windows systems, exploiting vulnerabilities to gain unauthorized access and execute malicious payloads. Trojan. Knight/Tedy is designed to bypass detection mechanisms, making it difficult to identify and remove. Operates as a backdoor, allowing attackers to remotely control the compromised system, steal sensitive data, or deploy additional malware like ransomware payloads.
- **Trojan.keygen/barys:** Disguises itself as a key generator for pirated software but secretly infects systems with malware. Often spread through file-sharing platforms and suspicious downloads and tricks users into executing it by promising free access to licensed software. Designed to steal sensitive information, install additional malware like ransomware, or create backdoors for remote access, bypassing system security. It poses a significant risk by modifying system files, evading detection, and operating without user knowledge.
- **Trojan.xbrtrh/bplat:** A highly evasive malware variant designed to infiltrate systems and execute malicious activities undetected. It primarily targets Windows-based environments, exploiting system vulnerabilities to establish persistent control. Once inside, it can disable security features, modify system configurations, and download additional malicious payloads. Often used by cybercriminals to facilitate data theft, execute financial fraud, or serve as a backdoor for further exploitation. Obfuscation techniques and the ability to hide in legitimate processes make it difficult to detect and remove.
- **Trojan.acll/bbsw:** A stealthy and highly adaptable malware that often masquerades as legitimate software or uses deceptive tactics, such as bundled downloads, to bypass security defenses. It establishes a backdoor for attackers to remotely control the compromised system, allowing them to manipulate files, execute commands, or deploy additional malicious payloads. It can also collect sensitive information, monitor user activities, and disable security tools, making it a potent threat for both individuals and organizations.

Ransomware Payloads

Halcyon also detected and blocked an array of ransomware payloads that could have significantly disrupted target organizations and their operations:

- **Ransomware.tedy/encoder:** A destructive ransomware variant that spreads through phishing emails, malicious attachments, or software vulnerabilities. It can also disable recovery options and delete backups to make file restoration difficult. It is part of a broader family of ransomware known for its disruptive impact and sophisticated attack strategies. This variant typically leverages advanced encryption algorithms, such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman), making it virtually impossible to decrypt files without the decryption key.

- **Ransomware.crysis/crusis:**A highly dangerous ransomware strain that spreads through phishing emails, malicious attachments, and weak Remote Desktop Protocol (RDP) settings. It scans the system for files to encrypt, using strong encryption algorithms like AES-256 and RSA-2048, making decryption nearly impossible without the attacker's key. Crysis/Crusis is particularly harmful due to its ability to disable antivirus programs, delete shadow copies, and encrypt files on network drives.

- **Trojan.lockbit/blackmatter:** A dangerous ransomware hybrid that combines features from both LockBit and BlackMatter ransomware families, targeting businesses and critical infrastructure. In addition to encryption, it can exfiltrate sensitive data, increasing pressure on victims by threatening to leak information if demands are not met. It spreads through phishing emails, malicious attachments, and exploiting known vulnerabilities in outdated software.

- **Trojan.tedy/lockbit:** Known for its rapid propagation and strong encryption algorithms, this ransomware often spreads through phishing emails, malicious attachments, or exploits in vulnerable software. The payload not only locks down files but may also exfiltrate sensitive information, increasing the pressure on victims to comply with ransom demands.

- **Ransomware.blackbasta/basta:** Known for its use of double-extortion tactics, where it not only encrypts data but also exfiltrates sensitive information, threatening to leak it if the ransom is not paid. The ransomware spreads through phishing emails, compromised RDP access, and known software vulnerabilities. Its rapid adoption and targeted attacks have made Black Basta a prominent threat in the cybercriminal landscape.

Halcyon Attacks Lookout

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

July 2024	August 2024	September 2024
Alleged Attacks Posted to Leaks Websites: 393	**Alleged Attacks Posted to Leaks Websites:** 470	**Alleged Attacks Posted to Leaks Websites:** 387
Confirmed Attacks Posted to Our Database: 342	**Confirmed Attacks Posted to Our Database:** 396	**Confirmed Attacks Posted to Our Database:** 337
Top 5 Industries Targeted: • Manufacturing: 59 attacks • Healthcare: 48 attacks • Business Services: 38 attacks • Construction: 32 attacks • Education: 21 attacks	**Top 5 Industries Targeted:** • Manufacturing: 79 attacks • Business Services: 49 attacks • Construction: 45 attacks • Healthcare: 32 attacks • Retail: 25 attacks	**Top 5 Industries Targeted:** • Manufacturing: 63 attacks • Business Services: 40 attacks • Construction: 35 attacks • Healthcare: 17 attacks • Education: 15 attacks
Most Active Groups: • RansomHub: 36 attacks • LockBit: 32 attacks • Hunters International: 25 attacks • Akira: 25 attacks • Play: 19 attacks	**Most Active Groups:** • RansomHub: 68 attacks • Meow: 35 attacks • Play: 25 attacks • LockBit: 22 attacks • BianLian: 18 attacks	**Most Active Groups:** • RansomHub: 69 attacks • Play: 42 attacks • Medusa: 20 attacks • Qilin: 18 attacks • Meow: 15 attacks

Q3-2024 Trends

Some interesting trends emerged in the third quarter of 2024:

Crisis Deepens

- **Clay County in Indiana Issues Disaster Declaration Following Ransomware Attack:** Clay County, Indiana Emergency Management Agency officials issued a disaster declaration following a disruptive ransomware attack on county networks which has halted operations at the Clay County Courthouse and Clay County Probation/ Community Corrections facilities.
- **Ransomware Payouts: "Firmly on Track for the Worst Year on Record":** Over $459 million was exported in the first half of the year, marking a $10 million increase from the previous year, signaling a worsening trend.
- **Dark Angels Ransomware Gang Nets Record $75M Ransom Payment:** The ransomware operation Dark Angels has reportedly set a new record by receiving a $75 million ransom payment from an unnamed Fortune 50 company.

Ransom Debate Continues

- **CISA Director Says Ransom Payment Ban Unlikely:** The Director of CISA said it is unlikely the U.S. government would issue a formal ban on ransom payments to ransomware operators despite the fact that such a ban would diminish the financial incentives for further attacks.
- **Ransomware: Majority of Victims Who Paid Ransom Suffered Multiple Attacks**: 74% of respondents who faced ransomware attacks in the last 12 months were hit multiple times, with some enduring multiple attacks in the span of a single week.
- **They Paid the Ransom Demand but the Decryptor Doesn't Work – Surprised?:** For some victims of the Hazard ransomware, paying the ransom only made things worse. After paying to receive a decryptor, they found it did not work.

Data Exfiltration Focus

- **Over 2.7 Billion Records from National Public Data Exposed in Breach:** The leaked data consists of two text files totaling 277GB, containing unencrypted records, though it is unclear if it covers every individual in the US.
- **Medical Records for 791K Exposed in Ransomware Attack on Lurie Children's Hospital:** The Rhysida ransomware group, which took credit for the attack on Lurie Children's, has claimed that the 600 Gb of data stolen from the hospital has been sold on the black market because the hospital refused to pay the ransom demand.
- **RansomHub Publishes Exfiltrated Florida Health Department Data:** Ransomware threat actors RansomHub have claimed to have published 100 gigabytes of exfiltrated data belonging to the Florida Department of Health asserting that the agency failed to pay a ransom demand following an attack.
- **RansomHub Exfiltrated Sensitive Data from Planned Parenthood of Montana:** Planned Parenthood of Montana announced it was the target of a cybersecurity attack in late August 2024

- **Sensitive Data of One Million NHS Patients Exposed Online After Ransomware Attack:** Analysis estimates that over 900,000 people may be affected by the attack, which involved data published by the Qilin ransomware gang in June.
- **Hunters International Hits ICBC and Exfiltrates 6.6TB of Sensitive Data:** The cyberattack was orchestrated by a group known as Hunters International, who claim to have stolen 5.2 million files, totaling 6.6 terabytes of sensitive data.
- **Hunters International Ransomware Operators Threaten to Publish US Marshals Data:** The Hunters International ransomware group is threatening to leak 386 GB of data from the U.S. Marshals Service (USMS), claiming it includes "Top Secret" documents, gang files, and information from the 2022 drug enforcement operation.

Legal and Regulatory Repercussions

- **Lurie Children's Hospital Named in Class Action Lawsuit Following Ransomware Attack:** The lawsuit claims Lurie Children's failed to implement reasonable and appropriate cybersecurity measures and did not comply with industry standards for cybersecurity.
- **CDK Global Named in Multiple Lawsuits Following Ransomware Attack:** The lawsuits allege CDK failed to adequately protect customer data, exposing tens of thousands of individuals' personal information, including Social Security numbers and financial details.
- **Judge Dismisses Most of SEC Case Against SolarWinds and CISO:** The SEC accused SolarWinds of downplaying its cybersecurity issues and the attack's severity while hiding customer warnings about malicious activity.
- **NCPA, Providers in 22 States Sue Change Healthcare/Optum/UHG Over Ransomware Attack:** The National Community Pharmacists Association (NCPA) and over three dozen healthcare providers from 22 U.S. states have filed a lawsuit against Change Healthcare, Optum, and UnitedHealth Group following a severe ransomware attack in February 2024.
- **IT Services Provider in UK Fined Over NHS Ransomware Attack:** The ICO provisionally found that the company had failed to protect the personal information of nearly 83,000 individuals, including sensitive data.
- **Exposed Employee PII in Ransomware Attack Spurs Class Action Lawsuit for City of Columbus:** The international ransomware group Rhysida claims responsibility for the attack, asserting that they stole 6.5 TB of data, including passwords, logins, and access to city cameras.
- **Enzo Biochem Fined $4.5M for Poor Security Following Ransomware Attack:** The biotech company has been ordered to pay $4.5 million to the attorneys general of New York, New Jersey, and Connecticut following a 2023 ransomware attack that compromised the data of over 2.4 million people.
- **Lehigh Valley Health Network to Pay $65M Judgement After Ransomware Attack:** The class-action lawsuit, filed in March 2023, accused LVHN of failing to safeguard patient data.

Evolving TTPs

- **North Korean Operations Highlight Espionage and Ransomware Attack Overlap:** A North Korea-linked threat actor, APT45, known for its cyber espionage operations, has expanded into financially motivated attacks involving ransomware, distinguishing it from other North Korean hacking groups.
- **Play Ransomware Debuts Linux Variant that Targets VMware ESXi:** The Play ransomware gang is the latest to develop a dedicated Linux locker for encrypting VMware ESXi virtual machines.
- **Qilin Ransomware TTPs Include Harvesting VPN Credentials in Chrome:** In a recent Qilin ransomware attack observed in July 2024, threat actors stole credentials stored in Google Chrome browsers on compromised endpoints.
- **New Cicada Ransomware Variant Targets VMware ESXi:** Analysis suggests that this new ransomware shares significant similarities with the ALPHV/BlackCat ransomware, indicating a potential rebranding or a fork by former ALPHV developers.
- **CISA and FBI Alert on Iranian Ransomware Attacks Against US Infrastructure:** These actors, known by various names including Pioneer Kitten, UNC757, Parisite, Rubidium, and Lemon Sandstorm, have been targeting both U.S. and foreign organizations across multiple sectors.
- **New RansomHub TTPs Include TDSSKiller and LaZagne for Disabling EDR:** This new method, recently uncovered by researchers, involves combining two well-known tools: Kaspersky's TDSSKiller, a legitimate rootkit removal tool, and LaZagne, a credential-harvesting utility.
- **Kransom Ransomware Attack Leverages DLL Side-Loading and Valid Certificates:** This sophisticated malware leverages DLL side-loading techniques to deploy its payload, utilizing a legitimate digital certificate issued by COGNOSPHERE PTE. LTD., adding an extra layer of credibility to its malicious activities.
- **Mallox Ransomware Operators Develop Linux Variant with Leaked Kryptina Code:** An affiliate of the Mallox ransomware group, also known as TargetCompany, has been observed using a modified version of the Kryptina ransomware to target Linux systems.

Takeaway

Ransomware attacks have become one of the most devastating threats to modern businesses, often bringing operations to a complete standstill. When critical systems and sensitive data are seized, an organization can find its daily processes crippled.

The impact goes beyond the immediate disruption; lost revenue, missed opportunities, and long-term damage to the company's reputation are just the beginning.

For many businesses, especially smaller ones, the downtime caused by ransomware can be catastrophic, forcing temporary or even permanent closures, with lasting repercussions that may be impossible to recover from. Larger corporations may have the resources and resiliency to endure such disruption. However, for small and medium-sized enterprises (SMEs), the consequences can be existential.

Unlike bigger companies, SMEs often lack the financial reserves or technical capability to spend weeks recovering their systems. A prolonged shutdown could spell the end of operations, as they struggle to absorb the cost of getting back online and repairing the damage.

Ransom demands vary widely, ranging from thousands to tens of millions of dollars, depending on the size and sector of the targeted company. However, the ransom is only part of the financial impact. The costs associated with incident response–hiring specialized cybersecurity teams, consulting legal experts, and dealing with potential regulatory fines–can quickly escalate.

Moreover, these figures do not encompass the full scope of the damage. Beyond the immediate financial hit, there are tangential costs that can be even more severe. These include long-term brand damage, eroded consumer trust, and increased cyber insurance premiums. Legal fees and ongoing litigation can further stretch an organization's resources. Revenue lost due to system downtime can sometimes exceed the direct costs of remediation. Unlike tangible losses, these are difficult to predict or budget for, leaving many companies vulnerable to financial ruin.

Ransomware attacks also pose significant risks in terms of intellectual property (IP) and regulated data. Once attackers gain access to a company's systems, they do not merely lock files–they often steal the data, threatening to leak it publicly unless the ransom is paid. For many organizations, particularly those dealing with sensitive customer information, this kind of exposure brings regulatory implications. Failure to adequately protect customer data can lead to lawsuits, regulatory fines, and irreparable reputational damage.

The theft of proprietary business data–such as patents, trade secrets, or confidential transaction information–can be just as damaging. Attackers frequently sell such information on dark web forums, where the highest bidder could gain access to a company's most valuable assets.

Data exfiltration–removing sensitive data from a company's systems before encrypting them–has become a common tactic in ransomware attacks. This significantly increases the pressure on the victim to pay the ransom. Even if an organization is prepared to recover from the initial attack, the fact that sensitive data has been stolen puts them at ongoing legal and financial risk.

Regulatory obligations to report data breaches vary by jurisdiction and industry, but failure to do so in a timely manner can result in hefty fines and legal consequences. In some cases, companies may face class action lawsuits, particularly when customer data has been compromised.

Paying the ransom is far from a guaranteed solution. Cybersecurity experts widely advise against it, as it not only funds criminal enterprises but also does not guarantee the recovery of encrypted data. The bad news is that attackers may still choose to sell or expose stolen data even after receiving payment. As a result, organizations are left facing both immediate and long-term challenges, with no assurance of a positive outcome even if they comply with the attackers' demands.

Ransomware operators have also evolved their tactics to maximize the financial impact. Increasingly, attackers exploit opportunities to extract multiple payments from a single attack, targeting not just the initial victim but also their partners, vendors, and customers. Exfiltrated data can be leveraged to extort these third parties, widening the attack's financial and reputational damage.

Organizations must prioritize both prevention and resilience. This includes implementing strong encryption protocols, access controls, and continuous employee training to minimize the likelihood of an attack. Yet, prevention alone is not enough–organizations must also be prepared to respond swiftly and effectively when an attack occurs.

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.

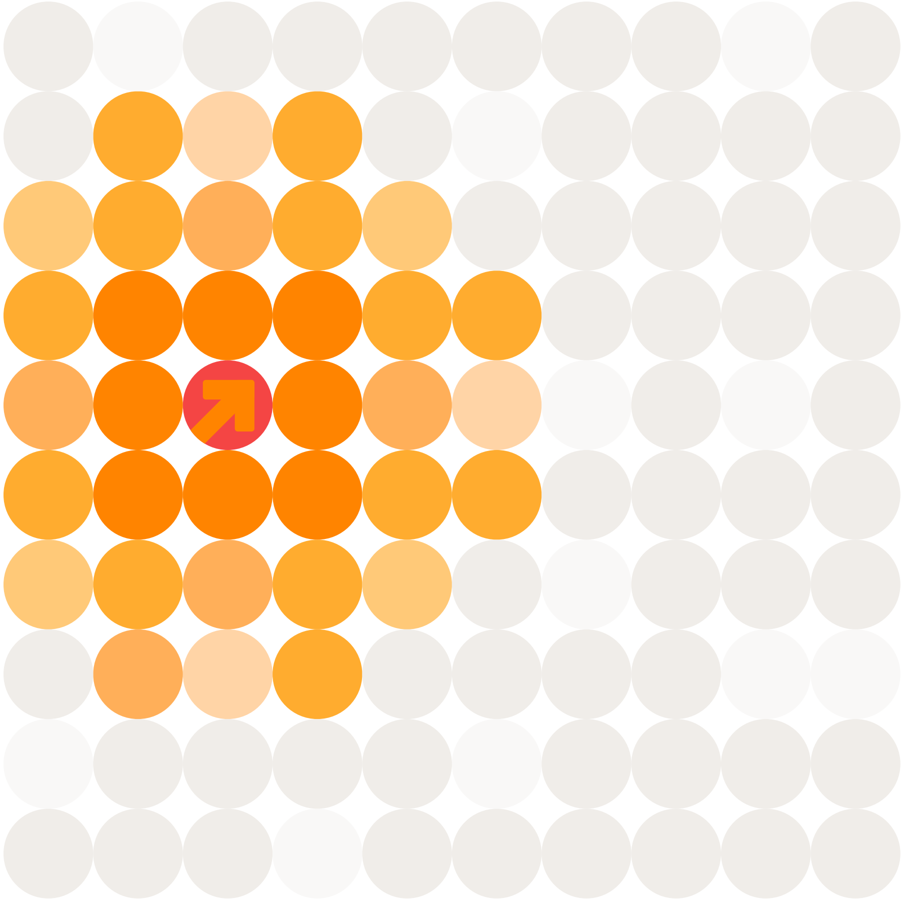
- **Third-Party Risk Management**: In today's interconnected digital environment, managing third-party risk is essential. Organizations often rely on vendors, suppliers, and partners who may introduce additional cyber risks. Tracking third-party risk involves monitoring the number of risk assessments 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.