



Q1
2024

Extortion Attack Group Guide

Power Rankings: Ransomware Malicious Quartile

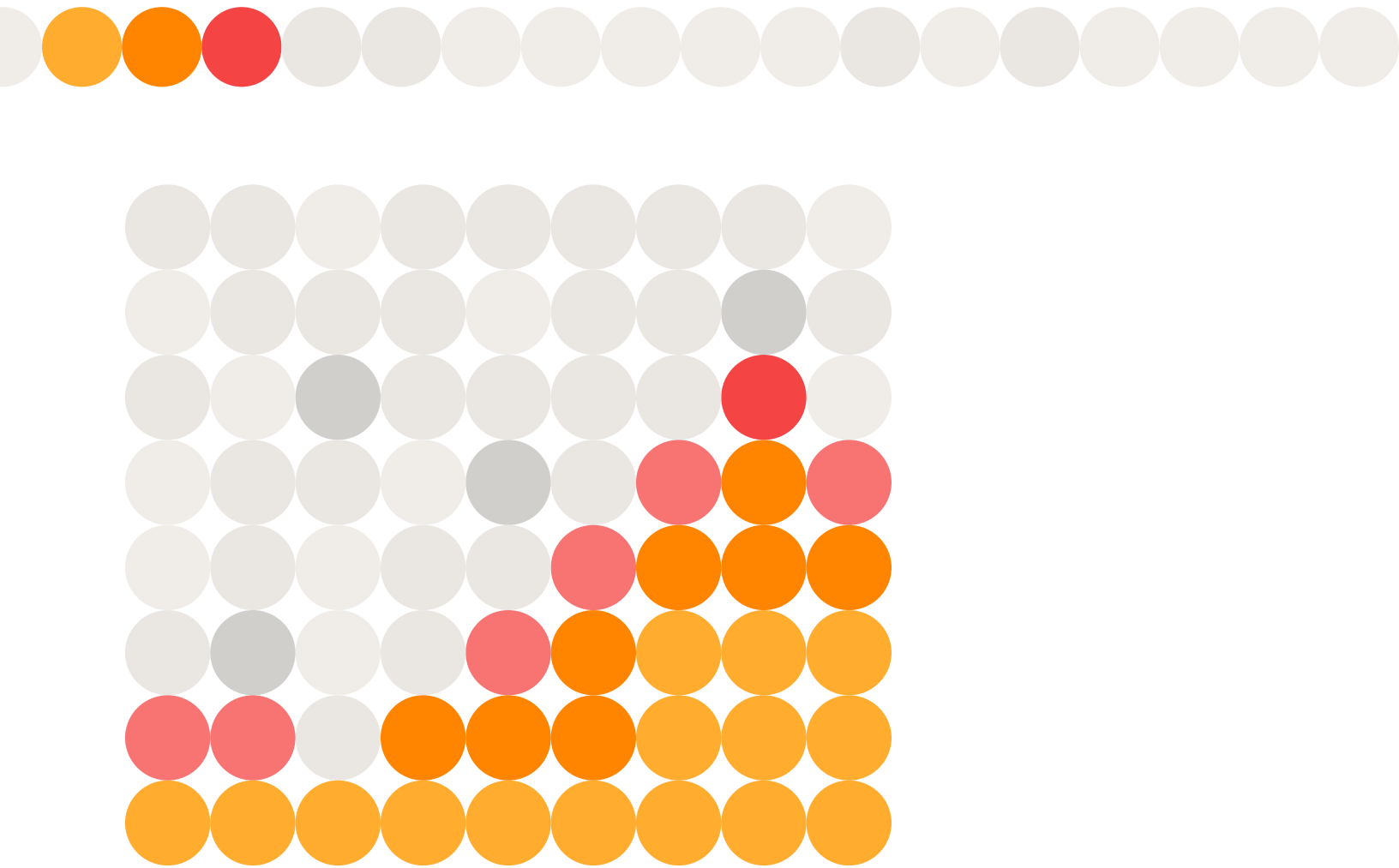
Q1-2024





Table of Contents

Ransomware and Data Extortion Attacks Evolving	3
Ransomware MQ: Evaluation Criteria Definitions	7
The Q1-2024 Ransomware Malicious Quartile	8
Frontrunners	9
Play	9
LockBit	10
Black Basta	12
8Base	13
Akira	14
Medusa	15
Hunters International	16
BianLian	18
Cactus	19
INC Ransom	20
Contenders	22
Qilin	22
Snatch	23
Rhysida	24
BlackSuit	25
Cuba	26
Emerging	28
RansomHub	28
Stormous	29
RansomHouse	30
Diminishing	31
BlackCat/ALPHV	31
NoEscape	32
Knight	34
ClOp	35
Trigona	36
Q1-2024 Trends	38
Takeaway	40



Ransomware and Data Extortion Attacks Evolving

Ransomware attacks in 2023 broke nearly all previous records, with the majority (75%) of organizations reported being targeted by at least one ransomware attack, and 26% reporting they were targeted with ransomware four or more times. All-in-all, the volume of attacks surged in 2023 by 55.5% year-over-year, and a report from Chainalysis revealed that payments to ransomware operators exceeded \$1 billion in 2023, breaking all previous estimations.

But the first quarter of 2024 is telling a bit of a different story, with some research indicating that ransomware attacks may have decreased by 20% or more from levels observed in the last quarter of 2023. Several factors may be at play in prompting the drop in attacks, including law enforcement actions against two of the top ransomware-as-a-service (RaaS) platform providers – LockBit and BlackCat/ALPHV – as well as a push by governments and some security experts to ban ransomware payments.

Other factors may include a decrease in the mass exploitation of patchable vulnerabilities like we saw with the massive MOVEit campaign, and a possible "exit scam" by one of the disrupted ransomware gangs that has undermined trust in the profit-sharing RaaS business model. So, does this mean we are finally getting the upper hand in the fight against ransomware?

It's far too soon to tell, and while we may see significant disruptions in some of the most pervasive operations, these gains are likely short-term. Rather than getting too optimistic that we have found the magic combination of efforts that will result in a sustained decrease in ransomware attacks, it is much more likely that we are simply in the eye of the storm.

Ransomware attacks remain extremely profitable, relatively easy to carry out, and the offenders face little-to-no potential consequences for their activities.

Change Healthcare: Unprecedented Attack

Despite seeing a measurable decrease in the number of attacks in the first quarter of 2024, the impact from ransomware operations had never been more disruptive, as exemplified by the BlackCat/ALPHV attack against healthcare payment processor Change Healthcare that threatened the U.S. healthcare system with near collapse, as providers simply could not get reimbursed for services.

While Change Healthcare is basically a financial company and not a healthcare provider, nonetheless the attack had widespread impact on both healthcare providers and their patients, for example:

- The New Mexico Cancer Center owed \$2 million to its supplier of chemotherapy medication and is concerned the supplier will cut them off
- A therapist in Raleigh-Durham said that they hadn't received payments of nearly \$200,000 for services rendered
- The CEO of Pulse Wellness in Portland said they needed to either sell her home or use credit cards to meet payroll
- A Naperville was hospitalized as he was unable to pay out-of-pocket for medication typically covered by insurance

UnitedHealth, the parent company Change Healthcare, announced in March that it was pouring more than \$2 billion into recovery efforts following what American Hospital Association CEO Rick Pollack described as "the most serious incident of its kind leveled against a U.S. health care organization."



Rather than getting too optimistic that we have found the magic combination of efforts that will result in a sustained decrease in ransomware attacks, it is much more likely that we are simply in the eye of the storm.

The attack was reported in February despite reports that a law enforcement operation back in December may have taken down the ransomware gang's leaks website. The U.S. government had also announced a bounty of as much as \$15 million for information leading to the arrest of BlackCat/ALPHV operators and affiliates.

The takedown attempt apparently failed as the group appeared to have quickly regained control of the websites before claiming attacks on Trans-Northern Pipelines, Prudential Financial, and LoanDepot. This casts doubt on whether law enforcement actions alone are an effective means to disincentivize ransomware attackers.

Despite being in the crosshairs of a major law enforcement takedown BlackCat/ALPHV operators were still able to carry out some really devastating attacks against some big-name companies like Change Healthcare, calling into doubt the effectiveness of these limited law enforcement actions.

What remains to be seen is whether the subsequent exit scam by the ALPHV/BlackCat ransomware gang that cut affiliate attackers out of their share of a purported \$22 million ransom payment from Change Healthcare will do more damage to the RaaS business model than the law enforcement actions. While the long-term impact has yet to play out, rumors of the exit scam no doubt fueled a lot of distrust between affiliates and RaaS providers, and this breakdown of trust will hopefully undermine the ransomware-as-a-service business model.

Proxies and the Dual Nature of Ransomware Attacks

One thing that is not being talked about enough in the media and by policy makers is the very real potential that some ransomware operations may essentially be proxy attacks designed to further the interests of adversarial nations.

For the most part, ransomware operators are out there trying to cause as much pain, publicity and frustration as possible because it translates into illicit dollars in their pockets. That said, we also cannot discount the dual nature of a good portion of today's ransomware attacks, where the attackers may be serving themselves from a financial perspective but are also furthering a larger geopolitical strategy.



Despite being in the crosshairs of a major law enforcement takedown, BlackCat/ALPHV operators were still able to carry out some really devastating attacks against some big-name companies.

The fact that ransomware attacks appear on the surface to merely be cybercriminal activity provides a convenient level of plausible deniability when those attacks also serve the larger geopolitical goals of rogue regimes like Russia, Iran, and North Korea. We know that a good portion of ransomware operators also participate in nation-state sponsored attacks, and there is also a good deal of evidence that there is shared attack infrastructure and tooling between cybercriminals and nation-state operators. [Research by Chainalysis](#) found that 74% of all revenue from ransomware attacks in 2021 went to attackers “highly likely to be affiliated with Russia.” There is little doubt this level of activity is going unnoticed by the Putin regime.

This is why it is imperative that the US government and allied nations who are the targets of these attacks should consider differentiating at least some of the attacks and classify them as terrorist acts – specifically those attacks that target healthcare and other critical infrastructure functions like utilities and elections. [Executive Order 13224](#) seems to be clearly applicable to some ransomware attacks, especially those against healthcare and other critical infrastructure providers:

“For the purpose of the Order, “terrorism” is defined to be an activity that (1) involves a violent act or an act dangerous to human life, property, or infrastructure; and (2) appears to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.”

If we call these attacks what they are—terrorist attacks meant to instill fear and influence geopolitical issues—then we unlock a whole host of options for both offensive cyber and even traditional kinetic military responses as a deterrence. Ransomware attacks against critical infrastructure are a form of terrorism in and of themselves, and the fact that many of the attacks are so closely related to the geopolitical interests of adversarial nations and are providing plausible deniability on the part of nation-state actors means we can no longer address these issues as a criminal matter.



Research by Chainalysis found that 74% of all revenue from ransomware attacks in 2021 went to attackers “highly likely to be affiliated with Russia.”



Ransomware MQ: Evaluation Criteria Definitions

The Halcyon team of ransomware experts has put together this extortion group power rankings guide as a quick reference for the extortion threat landscape based on data from throughout Q4-2023, which can be reviewed along with earlier reports here: [Power Rankings: Ransomware Malicious Quartile](#).

The report is based on available Q1-2024 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 somewhat subjective and based on input from ransomware subject matter experts on the following criteria:

Performance

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

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

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

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

Innovation

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

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

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



The Q1-2024 Ransomware Malicious Quartile

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



Source: Halcyon (Q1 2024)

Frontrunners

Play

Performance

- **RaaS Platform:** Play (aka PlayCrypt) is a RaaS that emerged in the summer of 2022. The group accelerated the pace of attacks in the last half of 2023 to become one of most prolific threat actors in the RaaS space and has notably increased its activities in the first quarter of 2024. Play is noted for having similarities to the Hive and Nokoyawa ransomware strains. Play often compromises unpatched Fortinet SSL VPN vulnerabilities to gain access. In Q1-2024, the FBI issued a joint advisory in partnership with CISA asserting the Play gang had compromised over 300 organizations since emerging in June of 2022.
- **Attack Volume:** Play continued to increase attacks throughout Q1-2024 and is one of the most active ransomware groups today. The group broke a record at the beginning of March 2024—launching a massive attack that hit 16 victims simultaneously.
- **Ransom Demands:** There is little information on how much Play demands for a ransom, but they have made good on their threats to leak the data of those who refuse payment.
- **Victims:** Rackspace, City of Lowell, Geneva Software, Primoteq, Kenya Bureau of Standards, Cambridge Group, AlgoTech, Hill International, CS Cargo, City of Oakland, Argentina's Judiciary, H-Hotels, Fedpol, Federal Office for Customs and Border Security (FOCBS), American Nuts, Red River Title.



In Q1-2024, the FBI issued a joint advisory in partnership with CISA asserting the Play gang had compromised over 300 organizations since emerging in June of 2022.

Innovation

- **RaaS Platform Development:** Play is an evolving RaaS platform known to leverage PowerTool to disable antivirus and other security monitoring solutions and SystemBC RAT for persistence. Play is known to leverage tools like Cobalt Strike for post-compromise lateral movement and SystemBC RAT executables and legitimate tools Plink and AnyDesk to maintain persistence, as well as Mimikatz and living-off-the-land binaries (LOLBins) techniques. Play has been observed leveraging Process Hacker, GMER, IOBit and PowerTool to bypass security solutions as well as PowerShell or command script to disable Windows Defender. Play also

abuses AdFind for command-line queries to collect information from a target's Active Directory. Play first introduced the intermittent encryption technique for improved evasion capabilities. Play also developed two custom data exfiltration tools – the Grixba information stealer and a Volume Shadow Copy Service (VSS) Copying Tool – that improve efficiency in exfiltrating sensitive information on the targeted network. Play has been observed leveraging exploits including ProxyNotShell, OWASSRF and a Microsoft Exchange Server RCE.

- **Targeted Industries:** Play ransomware gang has mainly focused attacks in Latin America, especially Brazil, but have also attacked outside of that region. Play was observed running a worldwide campaign targeting managed service providers (MSPs) in August to leverage their remote monitoring and management (RMM) tools to infiltrate customer networks. Recent attacks have targeted construction and manufacturing companies.
- **Economic Model:** Play employs tactics similar to both the Hive and Nokoyawa ransomware gangs and engages in double extortion by first exfiltrating victim data with the threat to post it on their “leaks” website.


LockBit

Performance

- **RaaS Platform:** LockBit is a RaaS that has been active since 2019 and is highly adept at security tool evasion as well as boasting an extremely fast encryption speed. LockBit is noted for multiple means of extortion where the victim may also be asked to pay a ransom for any sensitive information exfiltrated in the attack in addition to paying a ransom for the encryption key. LockBit employs publicly available file sharing services and a custom tool dubbed Stealbit for data exfiltration.
- **Attack Volume:** LockBit held the title as the leading attack group in the first half of 2023 until overtaken in volume by ClOp in Q3. Nonetheless, LockBit is by far the most prolific ransomware operation to date, and proved they follow through on threats, having exposed a large amount of exfiltrated Boeing data in Q1-2024.
- **Ransom Demands:** LockBit has demanded ransoms of \$50 million or more and hit the world's biggest computer chip maker, Taiwan Semiconductor Manufacturing Company (TSMC), with a \$70 million ransom demand in July.



In February 2024, an international law enforcement task force dubbed Operation Cronos succeeded in seizing and taking control of the LockBit administration environment – however, LockBit was back online within days.

- 
- **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.

Innovation

- **RaaS Platform Development:** In February 2024, an international law enforcement task force dubbed Operation Cronos succeeded in seizing and taking control of the LockBit administration environment. However, LockBit was back online within days. A new variant of LockBit was recently detected in the wild capable of impersonating system administrators and adaptive self-propagation across networks. LockBit continues to innovate their RaaS platform following the release of LockBit 3.0 in June of 2022, and introduced what is considered to be the first iteration of a macOS ransomware variant in April of 2023. The latest versions incorporate advanced anti-analysis features and are a threat to both Windows and Linux systems. LockBit 3.0 is modular and configured with multiple execution options that direct the behavior of the ransomware on the affected systems. LockBit employs a custom Salsa20 algorithm to encrypt files. LockBit takes advantage of remote desktop protocol (RDP) exploitation for most infections, and spreads on the network by way of Group Policy Objects and PsExec using the Server Message Block (SMB) protocol. LockBit appears to also still be supporting the older LockBit 2.0 variant from 2021, where the encryptor used is LockBit 2.0 but the victim is named on the LockBit 3.0 leak site. In Q1-2024, LockBit operators were observed frequently exploiting the Citrix Bleed vulnerability (CVE 2023-4966).
- **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.
- **Economic Model:** LockBit is a very well-run affiliate program and has a great reputation amongst the affiliate (attacker) community for the maturity of the platform as well as for offering high payouts of as much as 75% of the ransom proceeds.

Black Basta

Performance

- **RaaS Platform:** Black Basta is a RaaS that emerged in early 2022 and is assessed by some researchers to be an offshoot of the disbanded Conti and REvil attack groups. The group routinely exfiltrates sensitive data from victims for additional extortion leverage. Black Basta engages in highly targeted attacks and is assessed to only work with a limited group of highly vetted affiliate attackers.
- **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 vary depending on the targeted organization with reports that they can be as high as \$2 million dollars. It is estimated that Black Basta exceeded \$107 million in ransom revenue from more than 90 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.

Innovation

- **RaaS Platform Development:** Black Basta continues to evolve their RaaS platform, with ransomware payloads that can infect systems running both Windows and Linux systems. Black Basta is particularly adept at exploiting vulnerabilities in VMware ESXi running on enterprise servers. Black Basta ransomware is written in C++ and can target both Windows and Linux systems, encrypts data with ChaCha20, and then the encryption key is encrypted with RSA-4096 for rapid encryption of the targeted network. In some cases, Black Basta leverages malware strains like Qakbot and exploits such as PrintNightmare during the infection process. Black Basta also favors abuse of insecure Remote Desktop Protocol (RDP) deployments, one of the leading infection vectors for ransomware.
- **Targeted Industries:** Black Basta typically targets manufacturing, transportation, construction and related services, telecommunications, the automotive sector, and healthcare providers.



Black Basta is particularly adept at exploiting vulnerabilities in VMware ESXi running on enterprise servers. Black Basta ransomware is written in C++ and can target both Windows and Linux systems.

- **Economic Model:** Black Basta also employs a double extortion scheme and maintains an active leaks website where they post exfiltrated data if an organization declines to pay the ransom demand.

8Base

Performance

- **RaaS Platform:** The 8Base ransomware gang first emerged in March of 2022 and has quickly become one of the most active groups today, having displayed a “massive spike in activity” in the second half of 2023 that has continued into 2024, making them one of the most significant threats in the wild. The sophistication of the operation suggests they are an offshoot of experienced RaaS operators – most likely Ransomhouse, a data extortion group that first emerged in December of 2021 and was quite active in late 2022 and early 2023. Other researchers see a connection to the leaked Babuk builder. Like most groups today, 8Base engages in data exfiltration for double extortion and employs advanced security evasion techniques including modifying Windows Defender Firewall for bypass.
- **Attack Volume:** 8Base quickly ascended the ranks of active ransomware operators with a high volume of attacks in late spring and throughout 2023, making them one of the most active groups.
- **Ransom Demands:** It is unclear how much 8Base typically demands for a ransom.
- **Victims:** 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 does not appear to have its own signature ransomware strain or maintain an RaaS for recruiting affiliate participation openly, but it is assessed they may service a group of vetted affiliate attackers privately. Like RansomHouse, they appear to use a variety of ransomware payloads and loaders in their attacks, most prevalently customized Phobos with SmokeLoader. 8Base has gained notoriety for its rapid and efficient encryption methods and the appending of a unique “.8base” extension to encrypted files. 8Base has also demonstrated the capability to bypass Windows Defender’s Advanced Firewall. Attacks also included wiping of Volume Shadow Copies (VSS) to prevent rollback of



8Base has demonstrated the capability to bypass Windows Defender’s Advanced Firewall, and attacks include the wiping of Volume Shadow Copies (VSS) to prevent rollback of the encryption.

the encryption. 8Base does not appear to be targeting Linux systems, maintaining a focus on Windows targets. In Q1-2024, 8Base continued using a new variant of the Phobos ransomware payload, typically delivered with SmokeLoader.

- **Targeted Industries:** 8Base primarily targets organizations in the financial 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 first emerged in March 2023, and the group may have links to the notorious Conti gang, although this is difficult to ascertain given the Conti code was leaked in 2022. Despite being a relatively new player, Akira is one of the most active groups and accounts for many ransom incidents in Q1-2024. Interestingly, Akira's extortion platform includes a chat feature for victims to negotiate directly with the attackers, and it has been observed that Akira will inform victims who have paid a ransom of the infection vectors they leveraged to carry out the attack. This is not ransomware "standard procedure" as many ransomware operators have engaged in multiple attacks on the same victim leveraging the same vulnerabilities. A decrypter was released that may have worked on earlier variants or obscure samples of Akira, but its utility has proven to be null for recovery.
- **Attack Volume:** Akira maintains a modest but growing attack volume, putting them in about the middle of the pack when compared to other ransomware operators.
- **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 operates a RaaS written in C++ that is capable of targeting both Windows and Linux systems, typically by exploiting credentials for VPNs.



Innovation

- **RaaS Platform Development:** Akira operates a RaaS written in C++ that is capable of targeting both Windows and Linux systems, typically by exploiting credentials for VPNs. Akira modules will delete Windows Shadow Volume Copies leveraging PowerShell and is designed to encrypt a wide range of file types while avoiding Windows system files with .exe, .lnk, .dll, .msi, and .sys extensions. Akira also abuses legitimate LOLBins/COTS tools like PCHunter64, making detection more difficult. In July, a Linux variant for Akira was detected in the wild, and the group was also observed remotely exploiting a zero-day in Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software (CVE-2023-20269) in brute-force attacks since at least August. Akira has also been observed exploiting VMware ESXi vulnerabilities for lateral movement.
- **Targeted Industries:** The group is heavily focused on the healthcare sector and has also attacked dozens of organizations across multiple industry verticals including education, finance, and manufacturing.
- **Economic Model:** Akira operations include data exfiltration for double extortion with the threat to expose or sell the data should the victim fail to come to terms with the attackers and is assessed to have leaked gigabytes of stolen data from victims.


Medusa

Performance

- **RaaS Platform:** The Medusa is a RaaS that made its debut in the summer of 2021 and has evolved to be one of the more active RaaS platforms. Attack volumes surged activity in the last half of 2023 and the group has been responsible for 11 confirmed attacks in Q1-2024, making them one of the top active ransomware groups. The attackers restart infected machines in safe mode to avoid detection by security software as well preventing recovery by deleting local backups, disabling startup recovery options, and deleting VSS Shadow Copies to thwart encryption rollback.
- **Attack Volume:** Medusa ramped up attacks in the latter part of 2022 and have been one of the more active groups in the first quarter of 2023 but appear to have waned somewhat in the second quarter and slightly increased activity in the third quarter.
- **Ransom Demands:** Medusa typically demands ransoms in the millions of dollars which can vary depending on the target organization's ability to pay.



Medusa restarts infected machines in safe mode to avoid detection by security software as well preventing recovery by deleting local backups, disabling startup recovery options, and deleting VSS Shadow Copies to thwart encryption rollback.

- 
- **Victims:** Kansas City Area Transportation Authority, SIMTA, ATI Traduction, EDB, Symposia Organizzazione Congressi S.R.L, Believe Productions, Global Product Sales, ZOUARY & Associés, Neodata, Evasión.

Innovation

- **RaaS Platform Development:** The Medusa RaaS operation (not to be confused with the operators of the earlier MedusaLocker ransomware) typically compromises victim networks through brute-forcing RDP credentials, malicious email attachments (macros), torrent websites, or malicious ad libraries. Medusa can terminate over 280 Windows services and processes without command line arguments (there may be a Linux version as well, but it is unclear at this time). Medusa encrypts with AES256 algorithm using an encrypted RSA public key. Medusa deletes the Volume Shadow Copies abusing the vssadmin command to thwart rollback efforts. Medusa can disable over 200 services and released a more advanced variant in September with faster encryption speeds and the ability to delete backups to complicate recovery.
- **Targeted Industries:** Medusa targets multiple industry verticals, especially healthcare and pharmaceutical companies, and public sector organizations too.
- **Economic Model:** Medusa also employs a double extortion scheme where some data is exfiltrated prior to encryption, but they are not as generous with their affiliate attackers, only offering as much as 60% of the ransom if paid.

Hunters International

Performance

- **RaaS Platform:** Hunters International operates as a Ransomware-as-a-Service (RaaS), emerging from the remnants of the Hive ransomware group. It utilizes a sophisticated platform that leverages Hive's infrastructure and capabilities, including data exfiltration and double extortion techniques. The new variant of Hunters International reverses an earlier tactic of storing the decryption key in a separate file and adopts the simpler and more common practice of including the key within the encrypted file.



- **Attack Volume:** As a new entrant in the ransomware scene, Hunters International has quickly escalated its attack frequency, targeting a broad range of industries and geographies, indicating a significant operational capacity.
- **Ransom Demands:** The group demands ransoms by employing double extortion tactics; they encrypt the victim's data and additionally threaten to leak it unless the ransom is paid. 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.

Innovation

- **RaaS Platform Development:** Initially casting a wide net, Hunters International appears to be refining its focus on industries that are more likely to pay ransoms, such as healthcare, financial services, and critical infrastructure, given their need for quick recovery and the sensitivity of their data. The group has evolved from Hive's technology, focusing on enhancing the efficiency of their attacks and the reliability of their extortion schemes. They have improved the encryption methods to avoid common decryption techniques and have integrated mechanisms for more effective data exfiltration. The Hunters payload is written in Rust, a secure programming language that offers some advanced capabilities for security tool evasion and has been observed delivering both Windows and Linux variants.
- **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 under a profit-sharing model with its affiliates, similar to other RaaS operations. They offer a portion of the ransom proceeds to affiliates who successfully deploy their ransomware, encouraging widespread dissemination of their malware.



The Hunters payload is written in Rust, a secure programming language that offers some advanced capabilities for security tool evasion and has been observed delivering both Windows and Linux variants.

BianLian

Performance

- **RaaS Platform:** BianLian is not a traditional RaaS. They first emerged in June 2022 as a typical RaaS provider with Golang-based ransomware until a decrypter was released. BianLian successfully attacked several high-profile organizations before a free decryption tool was released to help victims recover files encrypted by ransomware. In early 2023, they appeared to have abandoned the ransomware payload portion of attacks in favor of less complicated data exfiltration and extortion attacks. This shows how successful the double extortion strategy is for ransomware groups, and we will likely see more groups join the likes of BianLian (and Karakurt before them).
- **Attack Volume:** BianLian increased attack volume as they have moved away from deploying ransomware payloads in favor of pure data extortion attacks, making them one of the more prominent groups. Activity waned in Q2 and Q3 of 2023 but surged in Q4 2023 and into early 2024.
- **Ransom Demands:** 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.

Innovation

- **RaaS Platform Development:** The group abandoned the RaaS model in favor of pure data extortion attacks where data is exfiltrated and ransom demand issued, but no ransomware is deployed. BianLian leverages open-source tooling and command-line scripts to engage in credential harvesting and data exfiltration. BianLian has been observed deploying a custom Go-based backdoor for remote access and uses PowerShell and Windows Command Shell to bypass and evade security solutions.
- **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:** Almost exclusively a data extortion attack group now, rarely observed deploying ransomware payloads.



BianLian increased attack volume as they have moved away from deploying ransomware payloads in favor of pure data extortion attacks, making them one of the more prominent groups.

Cactus

Performance

- **RaaS Platform:** Cactus ransomware emerged in March of 2023 and steadily ramped up their attack volume through the beginning of 2024. Cactus is noted for the ability to evade security tools and leverage exploits for known vulnerabilities in common VPN appliances to gain initial access to the networks of targeted organizations. Cactus operators have also been observed running a batch script that unhooks common security tools.
- **Attack Volume:** Cactus is a new arrival on the RaaS scene but has quickly amassed a disturbing number of victims in a relatively short time, and attack volumes have escalated in the second and third quarters of 2023.
- **Ransom Demands:** Cactus employs an encrypted messaging platform called TOX chat to conduct negotiations with victims. Ransom demands are assessed to be quite substantial, but an average has not been established.
- **Victims:** Schneider Electric, SCS SpA, OmniVision Technologies, The Hurley Group, Cornerstone Projects Group, ICOR Global Limited, Cornerstone Projects Group, Societa' Canavesana Servizi.

Innovation

- **RaaS Platform Development:** Cactus operations employ Living-off-the-Land techniques to abuse legitimate network tools like Event Viewer, PowerShell, Chisel, Rclone, Scheduled Tasks and typically drops an SSH backdoor on systems for persistence and for communicating with the C2 servers. Cactus has also been observed leveraging legitimate remote access tools like Splashtop, and SuperOps RMM along with deploying Cobalt Strike. In Q1-2024, Cactus operators were observed abusing Qlik Sense for initial access, as well as ManageEngine UEMS and AnyDesk for remote access and lateral movement on targeted networks. Cactus is unique in that the ransomware payload is encrypted and requires a key to execute to prevent it from being detected by security tools. It is also assessed that Cactus uses a PowerShell script dubbed TotalExec to automate the encryption process in a manner similar to the BlackBasta gang, and that they attempt to dump LSASS credentials for future privilege escalation.



Cactus employs an encrypted messaging platform called TOX chat to conduct negotiations with victims and ransom demands are assessed to be quite substantial.



- **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:** As with most extortion gangs today, Cactus engages in data exfiltration for double extortion by abusing Rclone tool.

INC Ransom

Performance

- **RaaS Platform:** INC Ransom was first observed in the summer of 2023, and it is unclear if they maintain a RaaS affiliate operation or are a closed group. INC uses common TTPs such as leveraging compromised RDP (Remote Desktop Protocol) credentials to gain access and move laterally in a targeted environment. Initial infections have been observed via phishing and exploitation of a vulnerability in Citrix NetScaler (CVE-2023-3519). The group claims to be a “moral agent” and suggests that it is helping victims by exposing their weaknesses.
- **Attack Volume:** INC did not emerge until the second half of 2023, but they appear to be ramping up operations as they refine their code and attack sequences.
- **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, Tylon Corp, Ingo Money, BPG Partners Group, DM Civil, Nicole Miller INC., Pro Metals, Springfield Area Chamber of Commerce, US Federal Labor Relations Authority, Yamaha Philippines.



INC did not emerge until the second half of 2023, but they appear to be ramping up operations as they refine their code and attack sequences.

Innovation

- **RaaS Development:** INC has been observed delivering ransomware using legitimate tools like WMIC and PSEXEC and uses other Living-off-the-Land (LOTL) techniques, abusing applications including MSPaint, WordPad, NotePad, MS Internet Explorer, MS Windows Explorer, and AnyDesk for lateral movement. INC has also been observed abusing tools like Esentutl



for reconnaissance and MegaSync for data exfiltration. INC is written in C++ and uses AES-128 in CTR mode to encrypt files, and it also has a Linux version. It is unclear if INC employs any advanced security tool evasion techniques, and there are indications that they may attempt to delete Volume Shadow Copies (VSS) to hinder encryption rollback attempts.

- **Targeted Industries:** INC targets a wide array of industries, including manufacturing, retail, IT, hospitality, pharma, construction and the public sector.
- **Economic Model:** INC practices double extortion and maintain a leaks site for double extortion, threatening to expose victim. INC has made good on threats to expose sensitive data if a target does not pay the ransom demand.

Contenders

Qilin

Performance

- **RaaS Platform:** Qilin (aka Agenda) is a RaaS operation that first emerged in July of 2022 that is written in the Go and Rust programming languages and is capable of targeting Windows and Linux systems. Rust is a secure, cross-platform programming language that offers exceptional performance for concurrent processing, making it easier to evade security controls and develop variants to target multiple OSs. Qilin operators are known to exploit vulnerable applications including Remote Desktop Protocol (RDP).
- **Attack Volume:** Qilin attack volumes are modest compared to leaders but given they are putting so many resources into developing one of the most generous profit sharing RaaS platforms in the market, combined with the use of advanced programming languages and a versatile attack platform, we are likely to see more from this group.
- **Ransom Demands:** Ransom demands are likely to be in the millions of dollars based on their affiliate profit sharing model which pays a higher percentage for ransoms over \$3 million.
- **Victims:** Big Issue Group, Ditronics Financial Services, Daiwa House, ASIC S.A., Thonburi Energy Storage, SIIIX Corporation, WT Partnership Asia, FSM Solicitors.

Innovation

- **RaaS Platform Development:** The Qilin RaaS offers multiple encryption techniques giving operators several configuration options when conducting the attack.
- **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 operations include data exfiltration for double extortion with the threat to expose or sell the data via their leaks site should the victim fail to come to terms with the attackers. The affiliate program offers an 80% take for ransoms under \$3 million and 85% for those over \$3 million.



With one of the most generous profit sharing RaaS platforms in the market, combined with the use of advanced programming languages and a versatile attack platform, we are likely to see more from this group.

Snatch

Performance

- **RaaS Platform:** Snatch is a RaaS first emerged way back in 2018 but did not become significantly active until 2021. The group hit multiple targets in Q1-2024. Snatch can evade security tools and deletes Volume Shadow Copies to prevent rollbacks and any local Windows backups to thwart recovery, and there has also been a Linux version observed in the wild. Snatch was observed trying to put a new twist on the double extortion gambit: giving cyber insurers details of how they infected victims to nullify coverage if those victims refuse to pay the ransom demand.
- **Attack Volume:** Snatch attack volume has been modest compared to leading ransomware operators but increase about 50% in 2023 compared to 2022 levels.
- **Ransom Demands:** Snatch ransom demands are low compared to leading ransomware operators, ranging from several thousands to tens of thousands of dollars.
- **Victims:** Malabar Gold & Diamonds, Banco Promerica, Cadence Aerospace, Match MG, City of Modesto, Ingenico, Oil India, Department of Defense South Africa, Gaston College, Americana Restaurants, Canadian Nurses Association, Medical Society of the State.



Snatch is written in Go and is somewhat unique in that the ransomware reboots in safe mode to make sure security tools are not running.

Innovation

- **RaaS Platform Development:** Snatch is written in Go and is somewhat unique in that the ransomware reboots in safe mode to make sure security tools are not running. Persistence and privilege escalation are not byproducts of the reboot. Snatch abuses legitimate tools like Process Hacker, Uninstaller, IObit, BCDEDIT, PowerTool, and PsExec. Snatch deletes Volume Shadow Copies to prevent encryption rollbacks. Snatch typically compromises victim networks through brute-forcing RDP credentials and abuses Windows Service Control to execute malicious scripts commands. Snatch reboots in Safe Mode to bypass security and modifies Windows Registry keys to establish persistence. Snatch exfiltrates data to the C2 with Update_Collector.exe malware via port 443 so the exfiltration blends in with normal HTTPS traffic.



- **Targeted Industries:** Snatch targeting varies widely based on their affiliates preferences, including Defense Industrial Base, Food & Agriculture, and Information Technology.
- **Economic Model:** Snatch is one of the more traditional RaaS platforms, where most of the targeting and attack sequence structure is left to the individual affiliates, including whether to exfiltrate data for double extortion. Some threat actors associated with Snatch have claimed they deal only with data and not ransomware deployment.

Rhysida

Performance

- **RaaS Platform:** Rhysida is a RaaS that was first observed in May of 2023, and has become one of the more prevalent threats in early 2024. Rhysida engages in data exfiltration for double extortion and maintains both a leaks site and a victim support portal on TOR. They are thought to be responsible for attacks against the Chilean military and more recently against Prospect Medical Holdings which impacted services at hundreds of clinics and hospitals across the US. In Q1-2024, the FBI and CISA released a joint advisory on Rhysida operations. Also, a decryptor was published by researchers in February 2024, and their activity has slowed down.
- **Attack Volume:** Rhysida has been steadily increasing their attack volume and continuing to expand the targeted industries, but volume is modest compared to leaders. Rhysida appears to be opportunistic attackers with a similar victimology as Vice Society.
- **Ransom Demands:** Ransom demands 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.



In Q1-2024, the FBI and CISA released a joint advisory on Rhysida operations, and a decryptor was published by researchers in February 2024, so their activity has slowed down.

Innovation

- **RaaS Platform Development:** Rhysida appears to have a fairly advanced RaaS offering, with capabilities that include advanced evasion techniques that can bypass antivirus protection, the wiping of Volume Shadow Copies (VSS) to prevent rollback of the encryption, and the ability to modify.



Remote Desktop Protocol (RDP) configuration. Rhysida has been observed deploying Cobalt Strike or similar command-and-control frameworks and abusing PSEXEC for lateral movement, dropping PowerShell scripts, and for payload delivery. Rhysida employs 4096-bit RSA key and AES-CTR for file encryption. Rhysida previously maintained a focus on Windows targets, but recently added Linux variant targeting VMWare ESXi. TTPs are similar to those of Vice Society, which has been less active since Rhysida emerged.

- **Targeted Industries:** Rhysida has been observed targeting the healthcare, education, government, manufacturing, and tech industries.
- **Economic Model:** Rhysida operators purport to be a "cybersecurity team" conducting unauthorized "penetration testing" to ostensibly "help" victim organizations identify potential security issues and secure their networks. The subsequent ransom demand is viewed as "payment" for their services.

BlackSuit

Performance

- **RaaS Platform:** BlackSuit is not a traditional Ransomware-as-a-Service (RaaS); it operates privately without known affiliates. It exhibits technical similarities to the Royal ransomware in its encryption mechanisms and operational tactics. Some sources believe BlackSuit may be a rebranding of Royal (which was a rebranding of Conti).
- **Attack Volume:** Since its emergence in 2023, BlackSuit has quickly gained notoriety for striking a variety of sectors with considerable impact, though specific numbers on attack volume are scarce.
- **Ransom Demands:** Details on typical ransom amounts are not well-documented, but given the pattern of attacks, they are likely significant. BlackSuit reportedly tailors ransom demands to the financial strength of victims to ensure the demand is "reasonable."
- **Victims:** ZooTampa, Southwest Binding & Laminating, Western Municipal Construction.



Unlike many ransomware operations that rely on a network of affiliates, BlackSuit controls its operations tightly, which could be a strategic decision to maintain operational security and maximize profits.



Innovation

- **RaaS Platform Development:** BlackSuit operates with a high level of secrecy, keeping its developments and tactics closely guarded. Unlike many ransomware operations that rely on a network of affiliates, BlackSuit controls its operations tightly, which could be a strategic decision to maintain 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.

Cuba

Performance

- **RaaS Platform:** Cuba is a RaaS that first emerged in 2019, but activity did not really ramp up until 2022, and attacks have continued to steadily increase through 2023 into early 2024. Cuba is assessed to be Russian-operated and connected to threat actors RomCom and Industrial Spy. Cuba is effective but does not really stand out amongst threat actors – their operations are fairly generic, but they do have the ability to bypass multiple security solutions with relative ease. In August, Cuba was observed targeting vulnerability for backup and disaster recovery offering Veeam (CVE-2023-27532).
- **Attack Volume:** Cuba's attack volume more than doubled in 2023 and continued to remain high in early 2024.
- **Ransom Demands:** Cuba operators have demanded some of the highest ransoms ever (in the tens of millions) but it is highly unlikely they have collected anywhere close to their outrageous demands.
- **Victims:** DMS Imaging, Rock County Public Health Department, Mount St. Mary Catholic High School, Phoenicia University, R1 Group, Edgo, Shoes for Crews, CMM, Gihealthcare.



Cuba relies on phishing, exploitable vulnerabilities, and compromised RDP credentials for ingress and lateral movement.



Innovation

- **RaaS Platform Development:** Like most operators, Cuba relies on phishing, exploitable vulnerabilities, and compromised RDP credentials for ingress and lateral movement, and uses the symmetric encryption algorithm ChaCha20 appended with a public RSA key. Cuba leverages PowerShell, Mimikatz, SystemBC and the Cobalt Strike platform. Overall, Cuba is not the most sophisticated ransomware in the wild but appears to be effective, and they have been observed to be improving their toolset with the addition of a custom downloader dubbed BUGHATCH, a security-bypass tool called BURNTCIGAR that terminates processes at the kernel level, the Metasploit array and Cobalt Strike in addition to several LOLBINS including cmd.exe for lateral movement ping.exe for reconnaissance. Recent attacks have used a new variant optimized to minimize unintended system behavior to avoid detection.
- **Targeted Industries:** Cuba selects victims on their ability to pay large ransom demands, targeting larger organizations in financial services, government, healthcare, critical infrastructure, and IT sectors.
- **Economic Model:** Cuba exfiltrates victim data for double-extortion and maintains a leaks site where they publish victim data if the ransom demand is not met. Cuba operators have a decent reputation as far as providing a decryption key to victims who pay the ransom demand.

Emerging

RansomHub

Performance

- **RaaS Platform:** RansomHub operates as a Ransomware-as-a-Service (RaaS) platform, emerging in the cybercrime scene around early 2024. This group has quickly garnered attention due to its impactful attacks and sophisticated approach to ransomware deployment. RansomHub affiliates get to keep as much as 90% of ransom proceeds. The group also claims to enforce strict policies that affiliates must comply with agreements made with victims during negotiations or they will be permanently banned. There is evidence to suggest that RansomHub may be a rebrand or strongly associated with the recently disrupted BlackCat/ALPV RaaS operators.
- **Attack Volume:** While still relatively new, RansomHub has been active, targeting several high-profile victims within a short span, including notable healthcare organizations like Change Healthcare. This rapid onset of activity suggests an aggressive expansion strategy.
- **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.



While still relatively new, RansomHub has been active targeting several high-profile victims within a short span, including notable healthcare organizations like Change Healthcare.

Innovation

- **RaaS Platform Development:** RansomHub has developed its RaaS capabilities, leveraging advanced techniques and benefiting from the dissolution of other ransomware groups. This includes attracting affiliates from other disbanded groups, thereby strengthening their operational capacity.
- **Targeted Industries:** Initially focusing on the healthcare sector, RansomHub's approach indicates a strategic choice likely due to the high value and sensitive nature of healthcare data.

- **Economic Model:** The group operates on a ransomware-as-a-service model, which suggests a structured revenue-sharing system with its affiliates, like other prominent ransomware groups. This model incentivizes the recruitment of skilled affiliates capable of launching significant attacks.

Stormous

Performance

- **RaaS Platform:** Stormous does not maintain a RaaS platform. Stormous emerged in mid-2021 or early 2022 and made headlines claiming to have exfiltrated 200GB of data from victim Epic Games as well as the Ministry of Foreign Affairs of Ukraine. They also were purported to have offered Coca-Cola data for sale. Stormous is assessed to have targeted companies whose data was leaked by other threat actors, and some have asserted they are a scam operation.
- **Attack Volume:** Stormous attack volume has been diminishing and it is assessed that they may not be responsible for some of the attacks they claim.
- **Ransom Demands:** It is unclear how much Stormous demands for ransom payments on average, but it was observed that they were selling what they claimed to be exfiltrated Coca-Cola files for about \$65,000.
- **Victims:** Vietnam Electricity, Duvel Moortgat Brewery, Konika Minolta, Cameron Memorial Community Hospital, Econocom Group, Senior Sistemas, Bandung Institute of Technology, Epson Spain, Interep.

Innovation

- **RaaS Platform Development:** Stormous does not maintain a RaaS platform and focused on straight data extortion. There are indications that Stormous and a lesser threat actor called GhostSec may be collaborating, as it was observed that Stormous has used the GhostLocker encryptor developed by GhostSec in some recent 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 sow confusion.



There are indications that Stormous and a lesser threat actor called GhostSec may be collaborating, as it was observed that Stormous has used the GhostLocker encryptor developed by GhostSec in some recent attacks.



- **Economic Model:** It is still unclear exactly how Stormous operates. They claim politically motivated targeting may be more opportunistic or could be trying to make money from the threat actors' work by leveraging the chaos and confusion around the high volume of ransomware attacks today.

RansomHouse

Performance

- **RaaS Platform:** RansomHouse does not maintain a RaaS platform. RansomHouse is a data extortion group that first emerged in December of 2021 who have some level of political motivation, stating they are “pro-freedom and support the free market” and claim to not work with other hackers or any intelligence agencies. They made headlines in 2022 for attacking chipmaker AMD and exfiltrating 450GB of data. In early 2024, the group began to automate VMware ESXi attacks using a new tool called MrAgent.
- **Attack Volume:** RansomHouse attack volumes pale compared to leading threat actors but have been steadily increasing in late 2022 and the first half of 2023 and continued to decline throughout the second half of 2023.
- **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.



RansomHouse made headlines in 2022 for attacking chipmaker AMD and exfiltrating 450GB of data, and in early 2024 the group began to automate VMware ESXi attacks using a new tool called MrAgent.

Innovation

- **RaaS Development:** RansomHouse does not maintain a RaaS platform.
- **Targeted Industries:** RansomHouse appears to be opportunistic, choosing targets for ease of compromise or for ability to pay. RansomHouse is a different kind of threat actor who uniquely “blames” victim organizations for lax security.
- **Economic Model:** RansomHouse maintains an active leaks site where they engage in “name and shame” to put pressure on victims to pay the ransom demand. RansomHouse exfiltrates victim data for double extortion but is also observed to be actively selling stolen data to other threat actors.

Diminishing

BlackCat/ALPHV

Performance


- **RaaS Platform:** In Q1-2024, the BlackCat/ALPHV gang may have suffered a major disruption by law enforcement, with reports that they took down the operator's websites and developed a decryption tool. However, further reports indicate the gang restored some of their infrastructure after the takedown and despite the disruption. After controversy regarding a \$22 million ransom payment from Change Healthcare and complaints from the access broker of not getting paid his cut, BlackCat announced that the group found a buyer for its source code and is officially shutting down. Other assessments indicate the group may have rebranded as RansomHub, a newer threat actor that has become quite active in Q1-2024. BlackCat/ALPHV was first observed in late 2021 and maintains a well-developed RaaS platform that encrypts by way of an AES algorithm. The code is highly customizable and includes JSON configurations for affiliate customization. BlackCat/ALPHV is adept at disabling security tools and evading analysis and is likely the most advanced ransomware family in the wild.
- **Attack Volume:** BlackCat/ALPHV became one of the more active RaaS platforms over the course of 2022, and attack volume in 2023 continued to increase at a steady pace.
- **Ransom Demands:** BlackCat/ALPHV typically demands ransoms in the \$400,000 to \$3 million range but has exceeded \$5 million. BlackCat/ALPHV recently released an API for their leak site to increase visibility for their attacks and put more pressure on victims to pay the ransom.
- **Victims:** Change Healthcare, MGM Resorts and Casinos, Lehigh Valley Health Network, PWC, Ernst & Young, and Sony, Republic Steel, Coca Cola, Constellation Software, Ring, Five Guys Restaurants, Western Digital, Henry Schein.

Innovation

- **RaaS Platform Development:** BlackCat/ALPHV was the first ransomware developers to employ Rust, a secure programming language that offers exceptional performance for concurrent processing. BlackCat/ALPHV deletes all Volume Shadow Copies using the vssadmin.exe utility and wmic



In Q1-2024, the BlackCat/ALPHV gang may have suffered a major disruption by law enforcement, with reports that they took down the operator's websites and developed a decryption tool.



to thwart rollback attempts and attains privilege escalation by leveraging the CMSTPLUA COM interface and bypasses User Account Control (UAC). BlackCat/ALPHV encrypts files with the ChaCha20 or the AES algorithm, opting for faster encryption versus stronger encryption by employing several modes of intermittent encryption. BlackCat/ALPHV also employs a custom tool called Exmatter for data exfiltration. BlackCat/ALPHV released a new ransomware version called Sphynx in August with improved security evasion capabilities and was observed harvesting One-Time Passwords (OTP) to bypass security tools to drop the Sphynx payload and encrypt Azure cloud storage deployments. Researchers also observed a BlackCat/ALPHV variant that embeds tools like Impacket and RemCom to facilitate lateral movement and remote code execution. In Q1-2024, they added a new tool dubbed Munchkin for propagation to remote machines and were observed abusing stolen credentials to compromise VMs to bypass EDR tools. BlackCat/ALPHV is capable of employing multiple encryption routines, displays advanced self-propagation, and hinders hypervisors for obfuscations and anti-analysis. BlackCat/ALPHV can impact systems running Windows, VMWare ESXi and Linux including Debian, ReadyNAS, Ubuntu, and Synology distributions.

- **Targeted Industries:** BlackCat/ALPHV has wide variability in targeting, but most often focuses on the healthcare, pharmaceutical, financial, manufacturing, legal and professional services industries.
- **Economic Model:** BlackCat/ALPHV also exfiltrates victim data prior to the execution of the ransomware –including from cloud-based deployments – to be leveraged in double extortion schemes to compel payment of the ransom demand. They have one of the more generous RaaS offerings, offering as much as 80-90% cut to affiliates. BlackCat/ALPHV is also noted for putting their leaks website on the public web instead of dark web for increased visibility.

NoEscape

Performance

- **RaaS Platform:** NoEscape was one of the more active threats in 2023, but attacks volume has been diminished in early 2024. Assessed to be a spinoff of the disbanded Avaddon gang. NoEscape emerged in May of 2023 and operates as a Ransomware-as-a-Service (RaaS) with variants for targeting Windows, Linux, and VMware ESXi systems. NoEscape provides affiliates with 24/7 technical support, communications, negotiation assistance, as well as an automated RaaS platform update feature.



NoEscape was one of the more active threats in 2023, but attacks volume has been diminished in early 2024.



- **Attack Volume:** Having just recently emerged, NoEscape has rapidly become one of the more prolific attack groups, with attack volume escalating significantly in the second quarter of 2023.
- **Ransom Demands:** It is unclear how high the typical NoEscape ransom demands tend to be, but it has been observed that profit sharing with affiliates is on par or even more attractive than other groups with ransoms over \$3 million netting 90/10 split with affiliates taking the lion's share.
- **Victims:** University of Hawaii, Mount Holly Nissan, LDLC Asvel, GASMART, KBS Accountants, Seattle Housing Authority, Effigest Capital Services, Korea Petroleum Industrial Co. LTD, Instant Access Co.

Innovation

- **RaaS Platform Development:** NoEscape is written in C++ and is relatively unique in the space in that the developers opted to build the RaaS platform from scratch rather than rely on code re-use from other ransomware variants. NoEscape ransomware payloads target both Windows and Linux systems and support multiple encryption options ranging from extra fast to extra strong encryption and leverages RSA and ChaCHA20 encryption algorithms and may use a single key for all impacted files for faster decryption of a ransom is paid. NoEscape can operate in safe mode to bypass security tools, terminates processes, erase VSS shadow copies and system back-ups to thwart recovery efforts, and abuses Windows Restart Manager to circumvent processes not terminated.
- **Targeted Industries:** NoEscape operations target a wide array of industry verticals with a focus on Education, Professional Services, Manufacturing, Information Technology and Healthcare.
- **Economic Model:** NoEscape offers it's RaaS platform to affiliate attackers and operations typically include data exfiltration or other actions to be leveraged in double extortion schemes such as a denial-of-service option for a hefty additional fee to the affiliate. NoEscape maintains a TOR-based leaks site to name-and-shame victims.

Knigh

Performance

- **RaaS Platform:** Knight is a RaaS platform that emerged in early summer of 2023 as a rebrand of the Cyclops ransomware operations that preceded it. Knight offers affiliates a wide array of builder, toolset, and payload options. Notable is their email phishing campaign using faux TripAdvisor alerts for initial infection.
- **Attack Volume:** The group appears to have gone inactive. The source code for Knight 3.0 ransomware was listed for a sale in February 2024—with conditions that it will sell to a single buyer to preserve the value of the tool.
- **Ransom Demands:** It is unclear what the average ransom demand by Knight is, but reports indicate that they range in the tens-of thousands.
- **Victims:** Agro Baggio, Crace Medical Center, Daiho Industrial, Faieta Motor Company, Mario De Creco, National Health Mission of India, GDL Logistica, Hackett's Printing, US Claims Solutions

Innovation

- **RaaS Development:** Knight emerged as an advanced RaaS offering with a user-friendly UI. Knight also offers both a "full" and "lite" versions to give affiliates more varied payload options. Knight employs static encryption leveraging the HC-256 symmetric algorithm and the SHA512 and Curve25516 algorithms for key management. Knight has been observed terminating a wide range of processes, and leverages malware like Remcos and Qakbot for payload delivery.
- **Targeted Industries:** Thus far, Knight operators and affiliates appear to be opportunistic attackers not focused on any specific industry vertical.
- **Economic Model:** Knight maintains a leaks site and employs double extortion methods, exfiltrating victim data as leverage to compel payment of the ransom demand and appears to have a competitive affiliate program with more than a few platform features for negotiation and collection of ransoms.



Knigh maintains a leaks site and employs double extortion methods, exfiltrating victim data as leverage to compel payment of the ransom demand and appears to have a competitive affiliate program.

ClOp

Performance


- **RaaS Platform:** Attacks by ClOp operators and affiliates fell dramatically in August of 2023, then the group appeared to have gone dark altogether in September with few attacks attributed to them throughout Q1-2024. ClOp is a RaaS platform first observed in 2019 that displays advanced anti-analysis capabilities and anti-virtual machine analysis to prevent investigations in an emulated environment. ClOp became the most prolific attack group in Q2-2023 by increasingly using automation to exploit known vulnerabilities in the MOVEit (CVE-2023-34362) and GoAnywhere (CVE-2023-0669) software offerings to infiltrate targets, as well as a SQL injection zero-day vulnerability (CVE-2023-34362) that installs a web shell—a rarity amongst ransomware operators. ClOp's unprecedented campaign exploiting the MOVEit vulnerability drove attacks levels to a new high, with ClOp assessed to be responsible for about one-fifth (21%) of all ransomware attacks in July.
- **Attack Volume:** Attacks by ClOp surged in Q1 of 2023 as the gang leveraged patchable exploits for the GoAnywhere file transfer software to compromise more than 100 victims in a matter of weeks. ClOp proceeded to compromise hundreds of organizations leveraging the MOVEit vulnerability in early summer, although it is unknown how well they were able to monetize these attacks. In some instances, it was observed that ClOp did not proceed with detonating a ransomware payload, opting instead for direct extortion leveraging the exfiltrated data.
- **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.
- **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:** ClOp is one of just a handful of known RaaS groups that have developed a Linux version, an indication that ClOp is likely actively recruiting new talent to help improve their platform and expand their addressable target range. ClOp's Windows version was written in C++ and encrypts files with RC4 and the encryption keys with RSA 1024-bit. In



Attacks by ClOp operators and affiliates fell dramatically in August of 2023, then the group appeared to have gone dark altogether in September with few attacks attributed to them throughout Q1-2024.



May of 2023, CIOp began exploiting SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution called MOVEit Transfer which was leveraged to steal data from victim databases. The campaign exploiting MOVEit appears to have been focused on data exfiltration and extortion without delivering an encryption payload. CIOp attackers also exploited a Fortra GoAnywhere MFT server vulnerability at the beginning of 2023.

- **Targeted Industries:** Early on, CIOp had previously almost exclusively hit targets in the healthcare sector but has significantly expanded targeting to include most any organization with vulnerable GoAnywhere installations.
- **Economic Model:** CIOp runs an expansive affiliate program and exfiltrates data to be leveraged in triple extortion schemes, and it has also significantly expanded its primary target range beyond the healthcare sector. There are indications that CIOp may be shifting to more of a pure data extortion model, but most victims still get hit with the ransomware payload at this point.

Trigona

Performance

- **RaaS Platform:** Trigona has resurfaced in early 2024 following reports that hackers aligned with the Ukrainian Cyber Alliance had compromised systems under the control of the Trigona ransomware gang, exfiltrated hundreds of gigabytes of data including source code and potentially decryption keys, and then wiped the servers. Trigona is not a traditional RaaS. The ransomware gang emerged around June of 2022 and operators have been observed scanning for internet-exposed Microsoft SQL servers to exploit via brute-force or dictionary attacks, and they also maintain a Linux version. Trigona is written in Delphi and includes a data wiper feature and has been observed to exfiltrate victim data for double extortion. The attackers will drop malware researchers dubbed CLR Shell to collect system information, to make configuration changes, and to escalate privileges by way of a vulnerability in the Windows Secondary Logon Service.
- **Attack Volume:** Trigona's attack volume in 2022 was minimal, but has increased in the first half of 2023, with more than twice the detected attacks in Q1-2023 than in the second half of 2022.



Trigona has resurfaced in early 2024 following reports that hackers aligned with the Ukrainian Cyber Alliance had compromised systems under the control of the Trigona ransomware gang.



- **Ransom Demands:** It is unclear how much they typically demand for a ransom.
- **Victims:** Claro, Vision Plast, Fertility North, Premier Facility Management, PT Samuels Sekuritas Indonesia, Amouage, Rolser, Alconex Specialty Products, Alconex, Quest International, FPZ GmbH, Portesa, Feit Electric, Lolaico Impianti, Public Health Management Corporation.

Innovation

- **RaaS Platform Development:** There are multiple Trigona versions detected in the wild targeting both Windows and Linux systems. Trigona TTPs have some overlap with BlackCat/ALPHV but are considered much less technically savvy. They employ a 4,112-bit RSA and 256-bit AES encryption in OFB mode which is buggy and complicated to decrypt, but they do have a reputation for reliably providing the decryption sequence to victims who pay the ransom demand. Trigona abuses legitimate programs including AteraAgent, Splash Top, ScreenConnect, AnyDesk, LogMeln and TeamViewer.
- **Targeted Industries:** Trigona may be opportunistic, but most attacks seem to focus on companies in the technology, healthcare, banking, manufacturing, and retail sectors.
- **Economic Model:** Trigona hosts leaks site that public website versus being hosted on TOR.



Q1-2024 Trends

Some interesting trends emerged in the first quarter of 2024...

Automation and Exploits

- Threat actors were observed targeting improperly configured Microsoft SQL (MSSQL) servers in a massive campaign designed to deliver Mimic ransomware, with attacks detected in the European Union, the United States, and Latin America: [Bleeping Computer](#)
- Ransomware operators have been observed leveraging remote access tool TeamViewer by way of exposed or brute-forced credentials to compromise networks and deploy payloads developed with the LockBit builder: [Bleeping Computer](#)
- Exploit that takes advantage of a high severity bug in the Fortra GoAnywhere MFT software could allow attackers administrative permissions on a targeted device: [The Hacker News](#)
- The LockBit ransomware gang continued to exploit a known vulnerability in the Citrix NetScaler web application delivery control (ADC) and the NetScaler Gateway appliance: [SC Magazine](#)
- Threat actors were observed conducting automated scans for vulnerable aiohttp Python libraries that could allow unauthorized access to files on targeted systems when symlinks are not present: [Bleeping Computer](#)
- LockBit Threatened to release exfiltrated Fulton County documents that “contain a lot of interesting things and Donald Trump’s court cases that could affect the upcoming US election”: [Business Insider](#)
- The Rhysida ransomware gang claimed they sold sensitive data exfiltrated in a February attack on Lurie Children’s Hospital after putting it up for sale for \$3.4 million: [The Record](#)
- Ransomware operators almost always target data backups in attacks and organizations with compromised backups were almost twice as likely to pay the ransom (67% versus 36%): [TechRadar](#)
- Ransomware operators threatened individual patients whose data had been exposed in a ransomware attack with swatting, a harassment tactic that involves calling in bomb threats or other false threats to law enforcement: [The Register](#)

Data Exfiltration

- Threat actors claimed to have exfiltrated 27 TB of confidential data from Johnson Controls International which “holds classified/sensitive contracts for DHS that depict the physical security of many (Department of Homeland Security) facilities”: [Bleeping Computer](#)
- According to a new FBI Internet Crime Complaint Center’s (IC3) latest report, of the 16 industries designated as critical U.S. infrastructure, healthcare suffered more ransomware attacks than any other sector: [Axios](#)
- American Hospital Association CEO Rick Pollack said the attack on Change Healthcare is “the most serious incident of its kind leveled against a U.S. health care organization”: [NBC News](#)
- UnitedHealth, parent company Change Healthcare, is pouring \$2 billion into recovery efforts as healthcare providers are in a serious financial crisis highlighting the impact of attacks on critical infrastructure: [SC Media](#)



LEO Actions

- The United States posted a bounty of up to \$10 million for information leading to the identification of the Hive ransomware operation, despite the group being inactive following an LEO infiltration and takedown in 2022: [Reuters](#)
- Authorities disrupted LockBit's infrastructure in February, but the group claims to still be active: [Bleeping Computer](#)
- Following an LEO takedown attempt, BlackCat/ALPHV appears to have voluntarily shut down operations in order to cheat affiliates out of a cut of the purported \$22 million ransom payment from Change Healthcare: [BleepingComputer](#)

Regulators, Liability and Lawsuits

- The US Department of Health & Human Services (HHS) Office for Civil Rights (OCR) is investigating medical payments giant Change Healthcare to see if Change Healthcare was in compliance with the Health Insurance

Portability and Accountability Act (HIPAA) Privacy and Security and Breach Notification Rules: [Infosecurity Magazine](#)

- Healthcare providers are increasingly facing lawsuits for failing to safeguard sensitive patient data and inadequately addressing ransomware attacks: [Bloomberg Law](#)
- Research indicates that filings made thus far under the new SEC four-day reporting requirement set are "not compliant with the new SEC cybersecurity incident disclosure rules": [Forbes](#)
- Law firm Mastagni Holstedt a filed lawsuit against managed service provider (MSP) LanTech LLC and data backup provider Acronis for more than \$1 million in damages alleging the companies failed to protect the firm from a disruptive ransomware attack: [MSSP Alert](#)
- US Fertility (USF) settled a class action lawsuit for \$5.75 million following a 2020 ransomware attack that included the exfiltration of sensitive data for nearly 900,000 people: [Health IT Security](#)



Takeaway

Ransomware attacks pose a significant threat to organizations of all sizes and industries. By fostering a culture of cybersecurity, investing in the right technologies and personnel, and developing comprehensive incident response and business continuity plans, organizations can minimize the impact of ransomware attacks and maintain a strong security posture.

As well, in understanding and addressing the unique challenges that ransomware presents, stakeholders can work together to protect their organizations and maintain the trust of their customers and employees.

Financial losses, operational disruptions, data exfiltration, reputational damage, legal consequences, and the evolving threat landscape are all factors that demand attention.

To protect your business, invest in robust cybersecurity measures, engage in ongoing employee training, and cultivate a culture of cybersecurity awareness. Collaborate with legal counsel to navigate the legal and regulatory landscape and develop a crisis communication plan to address reputational damage.

Defeating Ransomware: Metrics for Cyber Resilience

When considering cyber resilience and how to effectively assess and organizations posture, we must take into account that the threat landscape is continuously evolving, presenting formidable challenges to organizations striving to safeguard their assets and maintain operational continuity. Amidst this dynamic environment, the focus needs to emphasize not only the prevention of cyber threats but also the ability to swiftly detect, respond to, and recover from potential breaches.

Achieving cyber resilience requires more than just robust cybersecurity measures; it demands a comprehensive understanding of an organization's

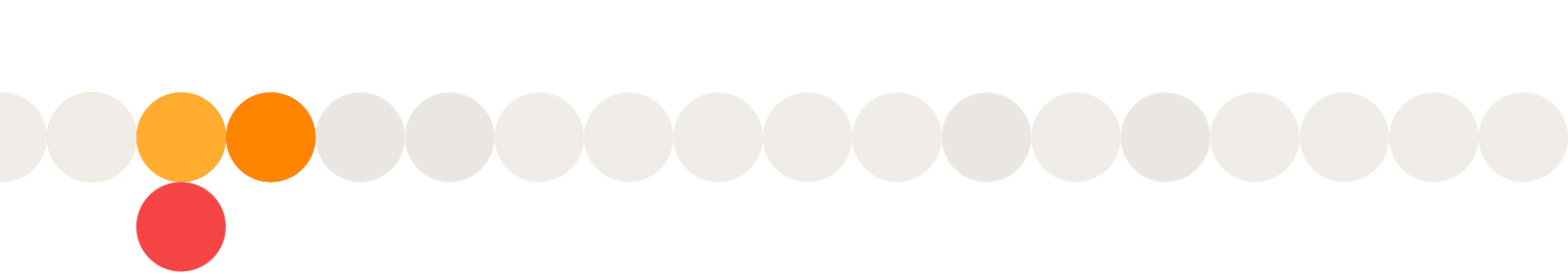
preparedness to withstand and rebound from cyber incidents. Central to this endeavor is the strategic selection and diligent monitoring of key performance indicators (KPIs) and metrics tailored to assess cyber resilience effectively.

Here are some of the essential metrics that can assist in bolstering cyber resilience:

Mean Time to Detect (MTTD): This measures how long it takes for an organization to detect a cyber threat or incident. A lower MTTD indicates better detection capabilities. MTTD is a key indicator that can be used to determine whether an organization is properly prepared to respond to threats in a timely manner. Lowering the MTTD can help contain the lateral movement within an organization and is an effective way to reduce the potential impact spread in a breach.

Mean Time to Respond (MTTR): This measures how long it takes for an organization to respond to a cyber threat or incident once it has been detected. A lower MTTR indicates faster response capabilities. Once an incident has been detected how quickly is an organization able to respond to the event, in order to effectively lower this metric, consider the outcomes of tabletop exercises and implementation of lesson learned during incidents that should provide indications of area for improvement in the response.

Incident Response Plan Effectiveness: Assess the effectiveness of the incident response plan by measuring how well it is followed during a cyber incident, including factors like containment time, communication effectiveness, and coordination among response teams. In order to have an effective cyber resilience strategy it is key that an organizations response plans are effective and followed, if the plan is not being followed it can lead to an increase in the time required to respond and effectively mitigate the



issue. Evaluate whether the plan needs to be changed to address changes in the threat landscape, risk themselves, or the organization response.

Cybersecurity Training and Awareness: Measure the effectiveness of cybersecurity training programs by tracking metrics such as employee awareness levels, completion rates of training modules, and performance in simulated phishing exercises. At the end of the day cyber incidents often have at least some if not a major human component. Evaluate the effectiveness of the training you are providing and the way it is provided. Often organizations provide a "one size fits all" approach to cyber training and awareness, this unfortunately misses the mark, a successful approach for a developer will not address the same needs for the CFO.

Cybersecurity Hygiene: Track metrics related to cybersecurity hygiene practices, such as the frequency of system patching, vulnerability scanning results, and compliance with security policies and standards. Hygiene should be table stakes for any organization trying to increase their cyber resilience, however this is often not the case. Create a prioritized approach to address the hygiene issue. Avoid the pitfall of chasing the next new cyber solution until you have a successful approach to address your organization's cyber hygiene.

Cyber Risk Exposure: Quantify cyber risk exposure by assessing the organization's risk posture based on factors such as asset criticality, vulnerability severity, and threat likelihood. If you don't have a valid way to measure your exposure, then you have little ability to identify where to prioritize your resources and increase your resilience.

Third-Party Risk Management: Track metrics related to third-party cyber risk, including the number of third-party assessments conducted, the level of compliance with security requirements, and any incidents or breaches involving third-party vendors. In today's interconnected world it's impossible to have any perspective on the resilience of your organization if you can understand the risk that your third-party relationships and connections are introducing into the ecosystem you operate in.

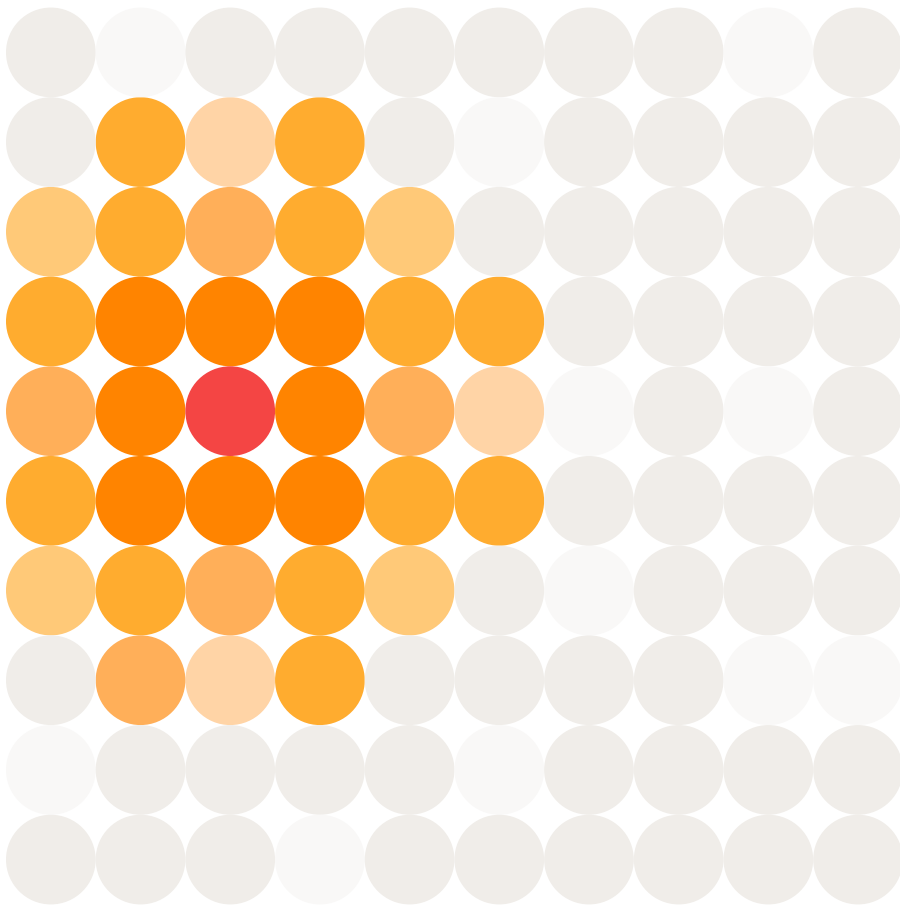
Security Controls Effectiveness: Assess the effectiveness of security controls by monitoring metrics such as intrusion detection/prevention system (IDS/IPS) alerts, firewall rule effectiveness, and malware detection rates. Are your controls effective? Should you be investing in other areas with potentially better ROI? Measuring whether you have implemented the right controls and are delivering the right results is important to consider.

Backup and Recovery Metrics: Measure the effectiveness of backup and recovery processes by assessing metrics such as backup success rates, recovery time objectives (RTO), and recovery point objectives (RPO). In an incident, can you get the data back? How long will recovery take? Does it match the desired recovery window? This should be tested and confirmed that the expectation meets real world results.

Business Continuity and Disaster Recovery (BCDR) Metrics: Measure the organization's ability to maintain operations during and after a cyber incident by tracking metrics such as recovery time objectives (RTOs), recovery point objectives (RPOs), and the success rate of BCDR exercises.

Effective cyber resilience requires a holistic approach that incorporates proactive measures, rapid detection, efficient response, and robust recovery mechanisms. By monitoring and optimizing these key metrics, organizations can enhance their ability to withstand and recover from cyber threats, safeguarding their operations and maintaining business continuity.

Lastly, think about how often the plan is tested and confirm disaster recovery planning. Sometime this is outside of cyber, but it's important to confirm that your plans can be implemented in a true DR scenario and services remain available.



The Halcyon Mission: Defeat Ransomware

Halcyon is the cyber resilience platform that Global 2000 companies rely upon to defeat ransomware-as-a-service attacks. With the fastest endpoint recovery capabilities and multiple layers of resiliency that includes bypass and evasion protection, key capture and automated decryption and data extortion prevention, the Halcyon Anti-Ransomware Platform reverses the impact of ransomware attacks in just minutes. 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.

