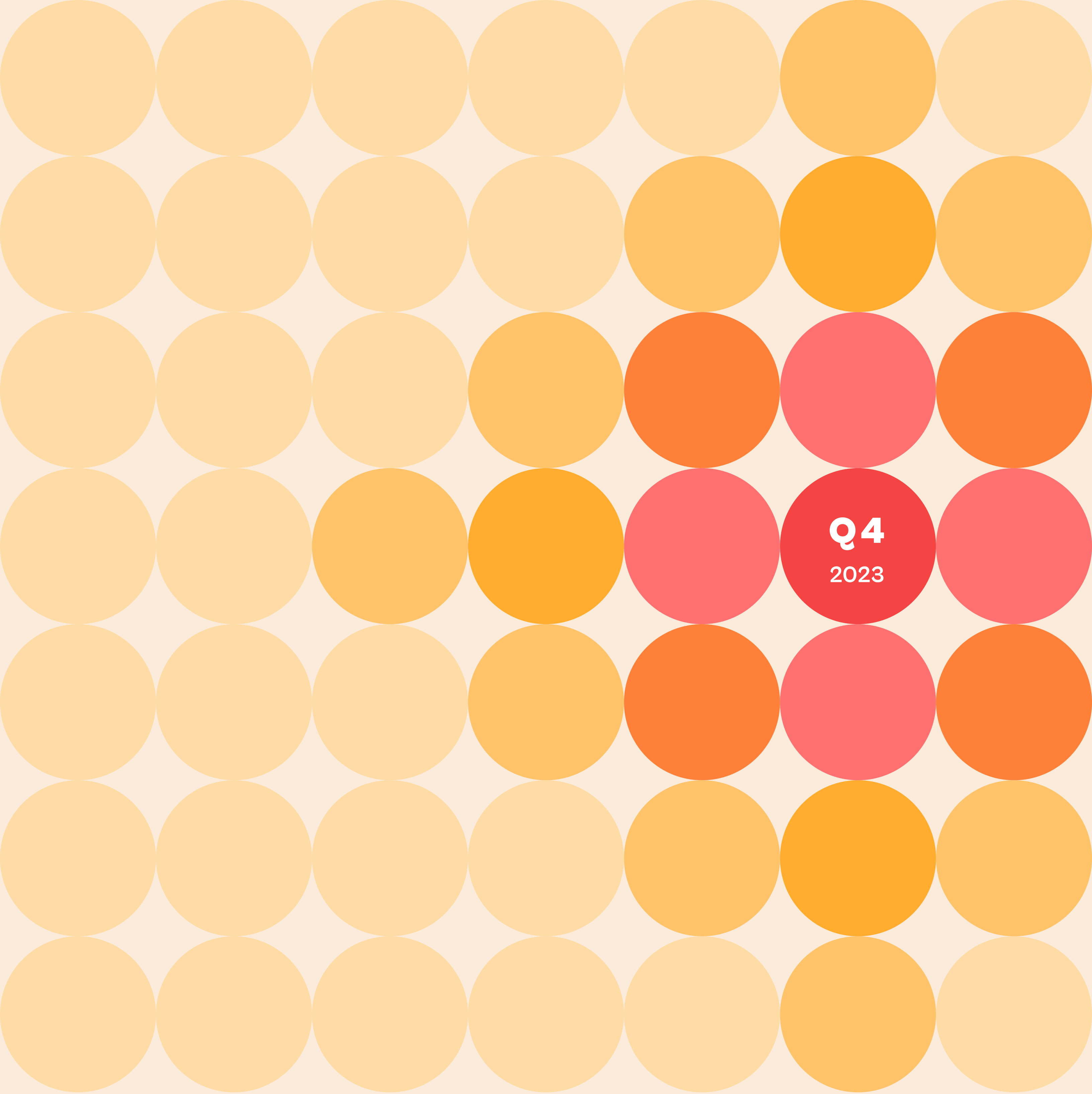


Extortion Attack Group Guide

Power Rankings: Ransomware Malicious Quartile

Q4-2023

halcyon

Table of Contents

Data Extortion Attacks Escalating . . . 3

Ransomware MQ: Evaluation Criteria Definitions . . . 6

The Q4-2023 Ransomware Malicious Quartile . . . 7

Frontrunners . . . 8

- LockBit . . . 8
- Play . . . 9
- 8Base . . . 10
- BlackCat/ALPHV . . . 12
- Black Basta . . . 13
- Medusa . . . 14
- Akira . . . 16
- Cactus . . . 17
- NoEscape . . . 18

Contenders . . . 20

- BianLian . . . 20
- Snatch . . . 21
- Rhysida . . . 22
- Cuba . . . 23
- Qilin . . . 24
- BlackByte . . . 25

Emerging . . . 27

- Knight . . . 27
- INC Ransom . . . 28
- Stormous . . . 29
- RansomHouse . . . 30
- Mallox . . . 30

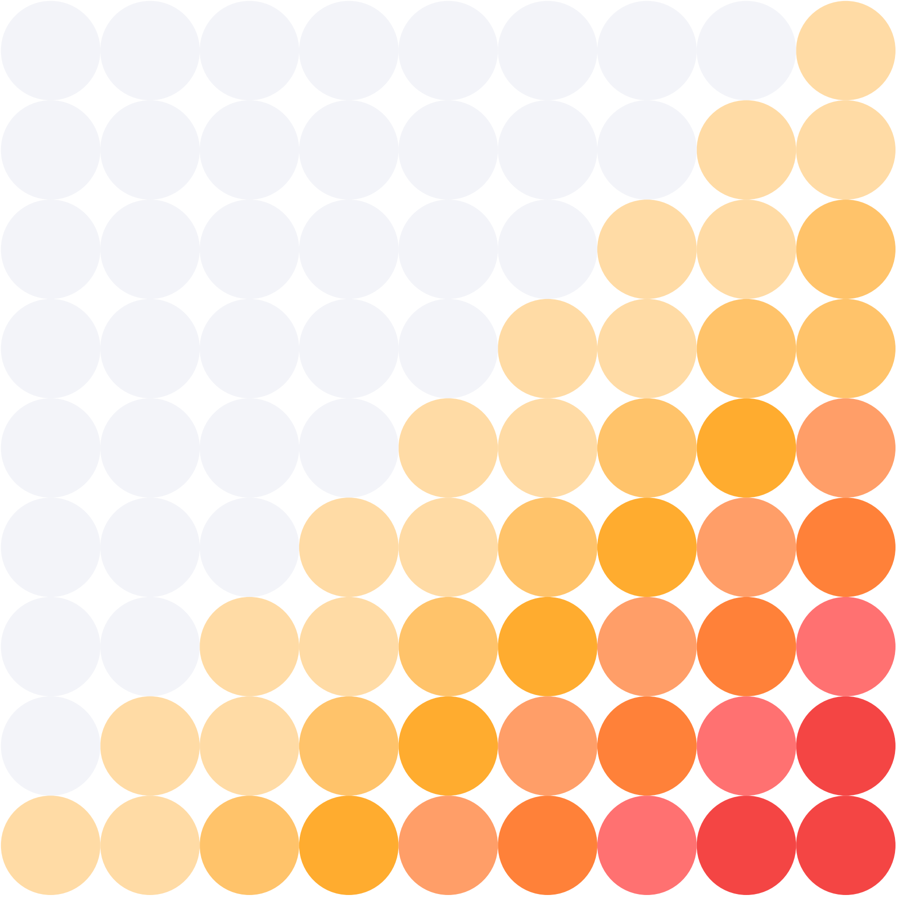
Diminishing . . . 32

- Cl0p . . . 32
- Royal . . . 33
- Ransomed.Vc . . . 34
- Nokoyawa . . . 35

Q4-2023 Trends . . . 37

Takeaway . . . 40

The Halcyon Mission: Defeat Ransomware . . . 43



Data Extortion Attacks Escalating

Ransomware remains one of the most significant threats to organizations of all sizes in all industry verticals. Following a bit of a lull the previous year, the first half of 2023 saw more victims impacted by ransomware attacks than in all of 2022 as threat actors continue to leverage Ransomware-as-a-Service (RaaS) platforms to execute their attacks, The vast majority (75%) of organizations reported being targeted by at least one ransomware attack in 2023, with 26% reporting they were targeted with ransomware four or more times.

Other analysis indicates the volume of attacks surged in 2023 by 55.5% year-over-year with 4,368 cases documented cases. Successful attacks in the U.S. increased by 60% for the healthcare sector, 82% for K-12 schools, and 48% for higher education.

The majority (75%) of organizations reported being targeted by at least one ransomware attack, with 26% reporting they were targeted with ransomware four or more times.

Surprisingly, this do not include the massive number of victims hit with ransomware by way of a vulnerability exploit in the MOVEit managed file transfer software (CVE-2023-34362) the Cl0p ransomware gang leveraged to compromise more than 1000 victims in rapid succession.

While authorities have been making efforts to help organizations address ransomware attacks, efforts to stem the tide of ransomware attacks are hampered by our not truly understanding the magnitude of this growing threat.

Hard numbers on the extent of the ransom crisis are hard to come by, and the problem may be even bigger than we think following a report that revealed over half (61%) of executives say their organizations do not report ransomware attacks.

Over half (61%) of executives say their organizations do not report ransomware attacks.

This lines up with what the FBI reported after spending seven months observing the Hive ransomware gang by infiltrating their operations. The FBI came to the shocking conclusion that only 20% of attacks were being reported to law enforcement.

There is no threat as pervasive as what we see with the explosion in ransomware operators, variants, affiliate threat actors, and total dollar losses to victim organizations, and the potential for an attack to have widespread and very serious repercussions is immanent.

For example, a recent ransomware attack on the Industrial and Commercial Bank of China (ICBC) reportedly disrupted the US Treasuries market, and similar attacks could cripple worldwide financial and banking systems, interfere with international trade, and cause other major disruptions.

The ransomware threat is so pervasive, the UK's Joint Committee on the National Security Strategy (JCNSS) recently warned the nation is at "high risk" of a "catastrophic ransomware attack at any moment."

At some point, these ransomware attacks are going to cross the line from cybercriminal activity to a national security event, especially when we are talking about attacks on critical infrastructure Defense Industrial Base targets.

We know rogue nations tacitly or directly support and/or control these ransomware operators to an extent, and these attacks are starting to look more and more like state-sponsored terrorism, and perhaps we should be addressing them as such.

Ransomware attacks can do more damage to an organization than simply impacting the bottom line, they have the potential to damage brand, increase insurance costs, force budget cuts and layoffs, negatively impact stakeholders and even put victim organizations and their CXOs and BoDs in legal jeopardy.

Recent actions taken against the former CISO for Uber and the more recent cases brought against SolarWinds executives represent a significant sea change regarding where liability lands for security-related decisions.

Today, the C-level and BoDs are increasingly in the crosshairs. We will likely see victims being prosecuted and potentially serving jailtime after a successful ransom attack – especially if sensitive or regulated data was compromised or exfiltrated.

A punitive regulatory stance will only create top-down pressure on CISOs and security teams to be less forthcoming with the C-level and BoD when faced with a security event. Security teams will feel pressure to not report events unless they absolutely must, and this will negatively impact security operations.

Ransomware is a multi-billion-dollar industry that is growing at an astounding pace. If you think your organization is immune, you are headed for an unpleasant surprise. Preparation and prevention before the organization is impacted is always the best course of action.

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 UK's Joint Committee on the National Security Strategy (JCNSS) warned the nation is at "high risk" of a "catastrophic ransomware attack at any moment."

Ransomware MQ: Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q4-2023 Ransomware Malicious Quartile. All attack groups evaluated must be a known threat actor group in 2023 with verifiable victims who demanded a ransom payment. Click on the threat actor group name below to see a listing of recent attacks they conducted including targets, industry verticals and other details.

The report is based on available Q4-2023 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

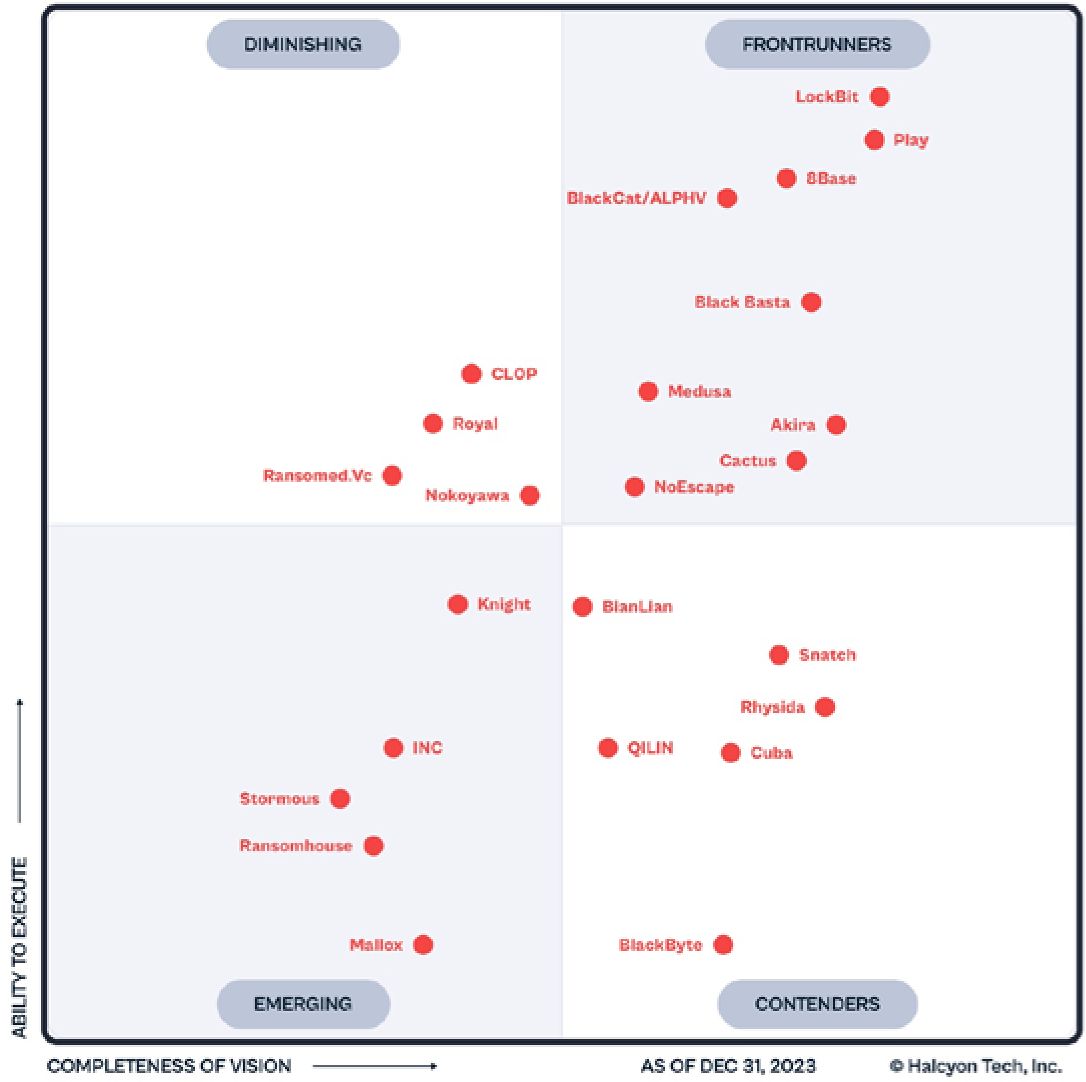
RaaS Platform Development: Attack groups were evaluated on evidence of continued development and improvement of the RaaS platform and TTPs.

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 Q4–2023 Ransomware Malicious Quartile

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



Source: Halcyon (Q4 2023)

Frontrunners

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 was by far the most active attack group in 2022 and continued to be the leading attack group in the first half of 2023 until overtaken in volume by Cl0p 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 Q4-2023.
- **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.
- **Victims:** Boeing, SpaceX, Shakey's Pizza, Banco De Venezuela, GP Global, Kuwait Ministry of Commerce, MCNA Dental, Bank of Brazilia, Endtrust, Bridgestone Americas, Royal Mail.

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 Q4-2023.

Innovation

- **RaaS Platform Development:** 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 Q4-2023, 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 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.

LockBit operators were observed frequently exploiting the Citrix Bleed vulnerability (CVE 2023-4966).

Play

Performance

- **RaaS Platform:** Play (aka PlayCrypt) is a RaaS that emerged in the summer of 2022 and has been accelerating the pace of attacks in the last half of 2023 to become one of most prolific threat actors in the RaaS space. 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 Q4-2023, 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 2023 and is one of the most active ransomware groups today.
- **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 Internationa, CS Cargo, City of Oakland, Argentina's Judiciary, H-Hotels, Fedpol, Federal Office for Customs and Border Security (FOCBS),

Play accelerated the pace of attacks to become one of most prolific threat actors in the RaaS space.

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.
- **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.

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, 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.

8Base first emerged in March of 2022 and has quickly become one of the most active groups with a "massive spike in activity" in 2H–2023.

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:** 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. Attacks also included wiping of Volume Shadow Copies (VSS) to prevent rollback of the encryption. 8Base does not appear to be targeting Linux systems, maintaining a focus on Windows targets. In Q4-2023, 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.

BlackCat/ALPHV

Performance

- **RaaS Platform:** In Q4-2023, 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. Further reports indicate the gang restored some of their infrastructure after the takedown. While the operations may have been stifled, BlackCat/ALPHV still remains a top threat. 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:** 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.

BlackCat/ALPHV may have been disrupted by law enforcement, who took down their websites and developed a decryption tool, but the gang restored some of their infrastructure, so BlackCat/ALPHV still remains a top threat.

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 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 Q4-2023, 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.

BlackCat/ALPHV added a new tool dubbed Munchkin for propagation to remote machines and were observed abusing stolen credentials to compromise VMs and bypass EDR tools.

- **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.

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 has quickly become one of the most prolific attack groups in 2023 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:** 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.
- **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.

It is estimated that Black Basta exceeded $107 million in ransom revenue from more than 90 victims in less than two years.

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 were inconsistent in the first half of 2023 with a resurgence of attack activity in the last half of 2023. 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.

Medusa has evolved to be one of the more active RaaS platforms, where attack volume was inconsistent before a resurgence of activity in the last half of 2023.

- **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.
- **Victims:** 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 through 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.

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

> Akira maintains a modest but growing attack volume, putting them in about the middle of the pack when compared to other ransomware operators.

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 has 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.

Cactus

Performance

- **RaaS Platform:** Cactus ransomware emerged in March of 2023 and have been steadily ramping up their attack volume through the end of 2023. Cactus is noted for the ability to evade security tools and leverages exploits for known vulnerabilities in common VPN appliances to gain initial access to the networks of targeted organizations. Cactus operators also have been observed running a batch script that unhooks common security tools.
- **Attack Volume:** Cactus is a new arrival on the RaaS scene but has quicky 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:** 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 Q4-2023, 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

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.

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.

- **Targeted Industries:** Cactus has been observed abusing SoftPerfect Network Scanner to do reconnaissance on prospective victims, who are generally 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.

NoEscape

Performance

- **RaaS Platform:** NoEscape was one of the more active threats in Q4-2023. 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 both 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.
- **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:** Mount Holly Nissan, LDLC Asvel, GASMART, KBS Accountants, Seattle Housing Authority, Effigest Capital Services, Korea Petroleum Industrial Co. LTD, Instant Access Co.

Assessed to be a spinoff of the disbanded Avaddon gang, NoEscape was one of the more active threats in Q4-2023.

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, erases 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 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.

Contenders

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 appear 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 volumes as they have moved away from deploying ransomware payloads in favor of pure data extortion attacks, making them one of the more prominent groups in Q1-2023, then activity dipped in Q2 and early Q3 with signs of a resurgence in Q4.
- **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.

BianLian was one of the first gangs to abandon the RaaS model in favor of pure data extortion attacks where data is exfiltrated and ransom demand issued, but no ransomware is deployed.

- **Targeted Industries:** BianLian primarily targets 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.

Snatch

Performance

- **RaaS Platform:** Snatch is a RaaS first emerged way back in 2018 but did not become significantly active until 2021. Snatch can evade security tools and deletes Volume Shadow Copies to prevent rollbacks and any local Windows backups to thwart recovery. 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 increased about 50% in 2023 compared to 2022 levels.
- **Ransom Demands:** Snatch ransom demands are relatively low compared to leading ransomware operators, ranging from several thousands to tens of thousands of dollars.
- **Victims:** 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 attack volume has been modest compared to leading ransomware operators but increased about 50% in 2023 compared to 2022 levels.

Innovation

- **RaaS Platform Development:** Snatch is written in Go and is somewhat unique in that the ransomware reboots in safe mode to make sure the 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.
- **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.

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 the latter half of 2023. 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 Q4-2023, the FBI and CISA released a joint advisory on Rhysida operations.
- **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:** It remains unclear how much Rhysida operators typically demand for a ransom payment at this time.
- **Victims:** 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.

Rhysida has been steadily increasing their attack volume and continuing to expand the targeted industries, but volume is modest compared to leaders.

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.

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. 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).

> Cuba is a RaaS that emerged in 2019, but activity did not really ramp up until 2022, and attacks have continued to steadily increase through 2023.

- **Attack Volume:** Cuba's attack volume appears to have more than doubled in 2023 over 2022 levels.
- **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:** Rock County Public Health Department, Mount St. Mary Catholic High School, Phoenicia University, R1 Group, Edgo, Shoes for Crews, CMM, GIhealthcare.

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.
- **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.

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.

Some Qilin variants are written in Rust, which offers exceptional performance for concurrent processing, making it easier to evade security controls and develop variants to target multiple OSs.

- **Victims:** Ditronics Financial Services, Daiwa House, ASIC S.A., Thonburi Energy Storage, SIIX 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.

BlackByte

Performance

- **RaaS Platform:** BlackByte is a RaaS that first emerged around July of 2021, and has similarities to LockBit v2.0 with regard to advanced obfuscation capabilities. BlackByte is assessed to be Russian operated given they abort attacks on Cyrillic language systems. They made headlines when the attacked the San Francisco 49ers and the City of Augusta, but it was their targeting of critical infrastructure targets that earned them an alert from CISA and the FBI in 2022.
- **Attack Volume:** BlackByte attack volumes were modest in 2022 compared to leading ransomware operators and were on pace to more than double in 2023.
- **Ransom Demands:** Ransom demands form BlackByte vary by target but have been observed to be in the millions of dollars, with a published $2 million dollar ransom levied against the City of Augusta in 2022.
- **Victims:** Yamaha Corporation of America, San Francisco 49ers, Hotel Xcaret, D-Link, City of Augusta, United Service Union, NV GEBE, Brett Martin, Wagner-CAT.

BlackByte serves up multiple variants including versions written in Go, C, and .NET, and the operators have exploited ProxyShell vulnerabilities for ingress while leveraging tools like Cobalt Strike and WinRAR.

Innovation

- **RaaS Platform Development:** Interestingly, the BlackByte RaaS serves up multiple variants of ransomware including versions written in Go, C, and .NET. Operators have exploited ProxyShell vulnerabilities for ingress, and leverage tools like Cobalt Strike and WinRAR. BlackByte uses its own custom exfiltration tool called Exbyte. BlackByte capabilities include bypassing security tools, process hollowing, and modification of Windows Firewall, VSS, as well as registry key values. BlackByte deploys Cobalt Strike beacons, abuses vulnerable drivers to evade security, and deploys custom backdoors to exfiltrate victim data.

- **Targeted Industries:** U.S. and global organizations in the energy, agriculture, financial services, and public sectors.

- **Economic Model**: BlackByte exfiltrates victim data for double extortion and maintain a leaks site where expose or sell victim data. The operators even go so far as to link the auction site in the ransom note to scare victims.

Emerging

Knight

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:** Attack volumes have been moderate compared to leaders, but with the prospect that there may be Linux and macOS versions as well as Windows, we may see attacks volumes begin to increase in Q1-2024.

- **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.

Knight is a RaaS platform that emerged in early summer of 2023 and as a rebrand of the Cyclops ransomware operations that preceded it.

Innovation

- **Raas Development:** Knight emerged as a fairly 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.

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).
- **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:** Xerox, Trylon 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 uses common TTPs such as leveraging compromised RDP credentials to gain access and move laterally in a targeted environment.

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.

INC has been observed abusing tools like Esentutl for reconnaissance and MegaSync for data exfiltration.

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 Coca-exfiltrated Cola files for about $65,000.
- **Victims:** Konika Minolta, Cameron Memorial Community Hospital, Econocom Group, Senior Sistemas, Bandung Institute of Technology, Epson Spain, Interep.

Stormous attack volume has been diminishing, and is assessed that they may not be responsible for some of the attacks they claim.

Innovation

- **RaaS Platform Development:** Stormous does not maintain a RaaS platform and focuses on straight data extortion.
- **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**: 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 appear to have some level of political motivation, stating they are “pro-freedom and support the free market” and claim to not work with other hacktivists or any intelligence agencies. They made headlines in 2022 for attacking chipmaker AMD and exfiltrating 450GB of data.
- **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 (AMD), Indonesia Power, Mission Community Hospital, Van Oirschot, Hawkins Delafield Wood, SMB Solutions.

RansomHouse extortion demands have been reported to range between $1 million and $11 million.

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.

Mallox

Performance

- **RaaS Platform:** Mallox is an emerging RaaS that first emerged in October of 2021 using a ransomware variant dubbed “tohnichi” for its file extension. The group then introduced a variant that appended files with “.mallox” which resulted in most researchers calling the group “Mallox.” Mallox was notable for its swift encryption speed, ability to bypass security tools like Windows Defender, and deletion of Shadow Copies to thwart encryption rollback.

- **Attack Volume:** Mallox attack volume accelerated, with activity surging by 174% over 2022 levels, but attack volume subsided in Q4-2023.
- **Ransom Demands:** There is not much information on how much Mallox demands for ransoms, but they appear to be relatively low compared to leading threat actors (in the thousands of dollars). Mallox is a newer group who has only recently started to recruit affiliates and are assessed to be improving their TTPs and payloads, so we expect ransom demands may increase.
- **Victims:** PT Garuda Indonesia, Measuresoft, DUHOCAAU, Kirkholm Maskiningeniører, Bozovich, Ban Leong Technologies Ltd, AddWeb Solution Private Limited.

Mallox attack volume accelerated, with activity surging by 174% over 2022 levels, but attack volume subsided in Q4-2023.

Innovation

- **RaaS Platform Development:** Mallox has been observed using advanced TTPs like DLL hijacking that is not common to ransomware attacks. Mallox employs a unique delivery method for the ransomware payload that does not require a loader, but instead uses a batch script to inject into the "MSBuild.exe" process in memory to evade detection. Mallox uses the Chacha20 algorithm for encryption. In 2023 they began using a variant that appends with ".xollam" which leverages malicious OneNote file attachments for exploitation of insecure MS-SQL servers to infiltrate networks. Mallox was observed exploiting two remote code execution vulnerabilities (CVE-2020-0618 and CVE-2019-1068) where earlier variants targeted vulnerable MS SQL instances to deliver the payload.
- **Targeted Industries:** Mallox has hit some critical infrastructure IT providers, but appears to be opportunistic, hitting targets mostly located in the US and India.
- **Economic Model**: Mallox only recently appears to be recruiting affiliates for a RaaS platform, so this group is one to watch. It is unclear if they engage in data exfiltration for double extortion, but they likely will follow other attackers in using this tactic as they develop their RaaS platform.

Diminishing

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 the rest of Q4-2023. ClOp is a RaaS platform first observed in 2019 which 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:** Level8 Solutions, NetScout, AutoZone, Siemens, Allegiant Air, NCR, Virgin Group, Saks Fifth Avenue, US DHS, New York Bar Association.

Once a leading threat, ClOp attacks fell dramatically in August then appeared to have ceased in September, with few attacks attributed to them throughout the rest of Q4-2023.

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 May of 2023, ClOp 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. ClOp attackers also exploited a Fortra GoAnywhere MFT server vulnerability at the beginning of 2023.
- **Targeted Industries:** Early on, ClOp 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**: ClOp runs an expansive affiliate program and exfiltrates data to be leveraged in triple extortion schemes and has significantly expanded its primary target range beyond the healthcare sector. There are indications that ClOp may be shifting to more of a pure data extortion model, but most victims still get hit with the ransomware payload at this point.

Royal

Performance

- **RaaS Platform:** Royal is a RaaS that has been active since September 2022 but has quickly become one of the more concerning ransomware operations, then displayed a significant reduction in activity throughout the second half of 2023. Royal deletes shadow copies to thwart recovery by way of rollbacks, and opts for partial encryption for larger files for speed and to evade detection. Royal famously attacked the City of Dallas, disrupting emergency services and other critical operations, and ultimately costing the municipality upwards of $10 million dollars to recover from the attack.
- **Attack Volume:** Royal increased attack activity in late 2022 and throughout the first half of 2023, prompting CISA and the FBI to issue alerts to critical infrastructure providers like the healthcare, communications, and education sectors, but activity in Q4 was below average.

Royal quickly became one of the more concerning ransomware operations, then displayed a significant reduction in activity throughout the second half of 2023.

- **Ransom Demands:** Royal ransom demands range between $1 million and $11 million dollars.
- **Victims:** City of Dallas, Unisco, Curry County, Clarke County Hospital, Penncrest School District, ZooTampa, Silverstone Formula One Circuit, Reventics LLC.

Innovation

- **RaaS Platform Development:** The Royal RaaS platform has expanded beyond targeting Windows installations to include attacks on systems running Linux and now targets VMWare ESXi servers. Assessments indicate Royal continues to invest heavily in development, expanding their operations and capabilities. The RaaS platform includes advanced security evasion and anti-analysis capabilities. The platform previously employed an encryptor from BlackCat/ALPHV but shifted to using a new encryption module dubbed Zeon. Royal also employs a range of exploitation tactics including using Nsudo, PowerShell, PCHunter, Process Hacker, GMER, or PowerTool, and batch scripts to evade security tools. Royal has been observed compromising cloud services, abusing legitimate TLS certificates, deploying CobaltStrike, and leveraging QakBot prior to the botnet's takedown. Royal has also been observed employing Goz and Vidar malware variants.
- **Targeted Industries:** Royal tends to target critical infrastructure sectors including the Manufacturing, Communications, Healthcare, and Education sectors, with a focus on small to medium-sized organizations.
- **Economic Model**: Royal typically does not include a specific ransom demand in the post-infection ransom note, but instead requires victims to directly negotiate terms through an Onion URL via the Tor browser.

Ransomed.Vc

Performance

- **RaaS Platform:** The story of Ransomed.Vc is illustrative of the rapid pace at which the ransomware threat landscape changes. The group was a startup RaaS that first emerged in late summer of 2023, but their tenure was short-lived. While they appeared to have come onto the scene in force, there were indications the group was more bluster than actual action, with several purported victims denying having been breached. In November, it

Ransomed.Vc illustrates the rapid threat landscape changes, having emerged in late summer, but by November it was reported that several gang members may have been arrested.

was reported that several gang members may have been arrested, and their infrastructure seemed to have been the target of a Denial-of-Service (DoS) attack.

- **Attack Volume:** Attack volume appeared to be substantial at first, but the actual number of attacks has been disputed.
- **Ransom Demands:** It is unclear what the average ransom demand from Ransomed.Vc is, but the amount set in the NTT Docomo is reported to have been more than $1 million dollars.
- **Victims:** Sony Corp, TransUnion, NTT Docomo, the State of Hawaii, Optimity, JHooker, A1 Data, I&G Broker House.

Innovation

- **Raas Development:** Not much is known about the Ransomed.Vc RaaS platform, but there appears to be a connection to the Everest and Stormous ransomware gangs. They were observed actively recruiting affiliates attackers, but then someone claiming to be associated with the gang was offering the platform for sale via Telegram following reports that some of the gang had been arrested, claiming the assets were worth as much as $10 million dollars. With groups like these, it is assumed the operators will simply regroup, retool, rebrand, and continue operations.
- **Targeted Industries:** With only a few dozen victims, it is unclear what industries Ransomed.Vc focused on targeting.
- **Economic Model**: Ransomed.Vc maintains a leaks site and employs double extortion methods, exfiltrating victim data as leverage to compel payment of the ransom demand and has made good on threats to expose and offer for sale sensitive exfiltrated data if the ransom is not paid. Ransomed.Vc is noted for employing a unique twist on the double extortion scheme by threatening to report victims for GDPR violations to EU authorities if the ransom demand is not met.

Nokoyawa

Performance

- **RaaS Platform:** Nokoyawa is a RaaS that emerged in February 2022 targeting Windows systems and has similarities to Karma and Nemty ransomware. It has been assessed that Nokoyawa operators may have intentionally forked with two different programming languages in an effort to evade detection. Nokoyawa is notable for being one of the first attack groups to burn a Windows zero-day vulnerability in attacks, exploiting a privilege escalation flaw (CVE-2023-28252) impacting the Windows Common Log File System (CLFS). It is highly unusual to see ransomware gangs using zero-day exploits targeting vulnerabilities in Windows, as these exploits are highly valuable to nation-state sponsored espionage operations, so unusual to see them leveraged in cybercrime.

- **Attack Volume:** Nokoyawa attack volume was modest compared to leaders, but their innovation is noted regarding the development of a Rust-based variant and the use of zero-day exploits and other advanced TTPs. Attack volume slowed for this threat actor in the second and third quarters.
- **Ransom Demands:** It is unclear how much the average Nokoyawa ransom is, but at least one IcedID attack that distributed Nokoyawa ransomware ended with a $200,000 ransom demand.
- **Victims:** Nexon Asia Pacific, AT&S, Roman Catholic Diocese of Albany, Pea River Electric Cooperative, Studio Domaine LLC.

Nokoyawa is notable for being one of the first attack groups to burn a Windows zero-day vulnerability in attacks, exploiting a privilege escalation flaw (CVE-2023-28252).

Innovation

- **RaaS Platform Development:** Nokoyawa has a robust RaaS offering originally written in C with several variants now in the wild, including Nevada ransomware that is written in Rust (similar to BlackCat/ALPHV) that can also target 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. Nokoyawa employs asymmetric Elliptic Curve Cryptography leveraging the Tiny-ECDH open-source library and a Salsa20 symmetric key. Nokoyawa employs Cobalt Strike and custom loaders to evade security solutions and appears to include portions of the leaked Babuk source code.
- **Targeted Industries:** Nokoyawa typically targets the healthcare, retail, energy, manufacturing, healthcare, and government sectors.
- **Economic Model**: Nokoyawa 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.

Q4–2023 Trends

Some interesting trends emerged in the fourth quarter of 2023...

Record Setting Year

- The vast majority (75%) of organizations reported being targeted by at least one ransomware attack in 2023, with 26% reporting they were targeted with ransomware four or more times: InfoSecurity Magazine
- The first half of 2023 saw more victims impacted by ransomware attacks than in the entirety of 2022: Security Magazine
- The volume of ransomware attacks surged in 2023 by 55.5% year-over-year from 2022 levels, with 4,368 cases documented cases: The Hacker News
- Ransomware attacks in the U.S. increased by 60% for the healthcare sector, 82% for K-12 schools, and 48% for higher education institutions: Data Breach Today

Liability for C-Level and Boards

- SEC implements rules requiring public companies to disclose "material cyberattacks" within four business days: Bleeping Computer
- SEC announced enforcement actions against SolarWinds and the company's CISO alleging fraud and internal control failures for known security risks: SEC
- Ransomware attack that exposed the PHI of 2.5 million McLaren Health Care patients could result in multiple federal class action lawsuits for failure to protect patient records: BankInfoSecurity

The Stakes are High

- A ransomware attack on the Industrial and Commercial Bank of China (ICBC) reportedly disrupted the US Treasury market: Financial Times
- CISA warned an Iran-linked threat actor is "actively targeting and compromising" multiple U.S. water treatment facilities: NPR
- The UK's Joint Committee on the National Security Strategy (JCNSS) warned that is a "high risk" the nation will experience a "catastrophic ransomware attack at any moment": The Record
- Ransomware attacks are causing psychological trauma for incident responders and business owners: The Record
- MGM's SEC 8-K filing revealed the company lost $100 million following a highly publicized ransomware attack in early September: DarkReading
- Ransomware and data extortion claims have been increasing every year, surging 40% in 2019 and almost 80% in 2022, with 2023 also trending higher: Insurance Journal

Attackers Improving

- Ransomware operators have reduced the time to infection after initial compromise from an average 4.5 days to a matter of a few hours: The Record
- We are seeing a steady increase in the number of zero-day vulnerabilities being exploited by ransomware operators employing automated scans looking for vulnerable applications: CyberWarZone

Vulnerability Exploits Rule

- LockBit is exploiting the Citrix Bleed vulnerability (CVE-2023-4966) that impacts the Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances: CISA
- HelloKitty observed exploiting critical vulnerability in Apache ActiveMQ service (CVE-2023-46604) that could allow remote code execution and arbitrary shell commands: The Hacker News
- SysAid advised customers to update following Cl0p's exploitation of a zero-day (CVE-2023-47246) in the SysAid IT support software: https://documentation.sysaid.com/docs/latest-version-installation-files
- Ransomware operators were observed targeting misconfigured MSSQL servers in a massive campaign designed to deliver Mimic ransomware: Bleeping Computer

Healthcare in the Crosshairs

- 68% said ransomware attacks resulted in a disruption to patient care, 43% said data exfiltration during the attack also negatively impacted patient care, 46% noting increased mortality rates and 38% noting more complications in medical procedures following a ransomware attack: HelpNet Security
- Attack ion Prospect Medical Holdings forced suspension emergency services, cancelled medical procedures, downed billing systems and caused ambulances to be diverted: WSHU
- Attack shut down dozens of Akumin medical centers causing appointments to be cancelled and making it impossible for doctors to view images for diagnosis and treatment: WUSF
- Two hospital emergency rooms in New Jersey were forced to divert ambulances following a disruptive ransomware attack: ABC7NY
- 800,000 patients had their data exposed and the attackers are extorting individual patients for a $50 ransom to avoid having personal health information (PHI) exposed online: The Record
- Ransomware operators are threatening patients whose data has been exposed with swatting, a harassment tactic that involves calling in false threats to law enforcement: The Register
- Ransomware attacks against U.S. healthcare providers cost nearly $80 billion over the past seven years, with 539 reported attacks impacting 10,000 hospitals and clinics with over 52 million records compromised: InfoSecurity Magazine
- Akumin Imaging filed for Chapter 11 bankruptcy protection amidst a "ransomware incident" that patients unable to schedule appointments: First Coast News

Push to Ban Ransom Payments

- Biden administration leads a multinational coalition of 50 nations who [propose banning ransom payments: The Record
- Calls for ban on ransom payments increase as threat actors carry out more complex, targeted attacks against specific industries and organizations: The Register

Takeaway

While the lessons learned from ransomware and data extortion attacks in Q4-2023 are numerous, beyond the increasing volume and complexity of attacks the real story here is the toll these attacks are taking on people.

It's no surprise that ransomware attacks are causing psychological trauma for incident responders and business owners, as the potential consequences of a successful attack can mean millions in losses – something that represents an existential risk, especially for smaller organizations.

This is particularly true for CISOs who have long endured the "brunt of the blame" for successful attacks regardless of their efforts to get more funding to improve the security posture of the company. But it is also becoming clear that regulatory and legal liability is rapidly moving up the chain to threaten the C-Suite and Boards of Directors.

Until recently, while ransomware attacks were very disruptive to organizations, at the end of the day everyone went home. Most CISOs know that they can only expect to keep a job for a few years, as there has always been volatility for the position. But until now, everyone still went home.

That may no longer be the case. When you look at the legal actions taken against the former CISO for Uber and the more recent cases brought against SolarWinds executives including the CISO, we are witnessing a significant sea change regarding where liability lands for security-related decisions.

Executives and Boards of Directors are increasingly at risk of being prosecuted and potentially serving jailtime following a successful ransomware attack – especially if sensitive or regulated data was compromised or exfiltrated in the attack.

Why? The government is failing to protect organizations from ransomware attacks, which makes them look ineffective, and the government does not like to look inept, so they know they must do something.

So, what do they do? They re-victimize the victims of these attacks so they can pat themselves on the back and say they are addressing the problem. They are making the problem worse for the victims.

Take the recently enacted reporting rule implemented by the Securities and Exchange Commission (SEC) last December. The new rules require publicly traded companies to disclose a "material" security event within four days or face regulatory actions.

While more visibility and accountability regarding security-related events at public companies is a good thing on its face, we need to be careful to not confuse disclosing information about a cyberattack with actually informing investors as to why an attack should be considered in their investment decisions.

Forensic investigations are difficult, and they take time – a lot of time. The disclosure rule set by the SEC has the potential to create a situation where an attack is disclosed but the details are murky because it could be weeks or months before the organization can adequately assess the information the SEC is requiring be reported.

The company's leadership would then be in a position where they trickle out incomplete information over time as the investigation progresses, and simply end up dying by a thousand cuts.

Remember what happened to Okta when they tried to be timely and transparent about a breach event? Their stock was hammered, and the CEO was heavily criticized for how they handled the disclosures.

The inability to provide concrete answers immediately will likely create confusion and anxiety for investors and attempts to be forthright and transparent will result in contradictory or escalating disclosures, creating more legal liability for the organization and its leadership.

And there are more issues that can arise, as there is also the potential impact that the regulatory actions against victim organizations and their leadership will have on security culture within an organization.

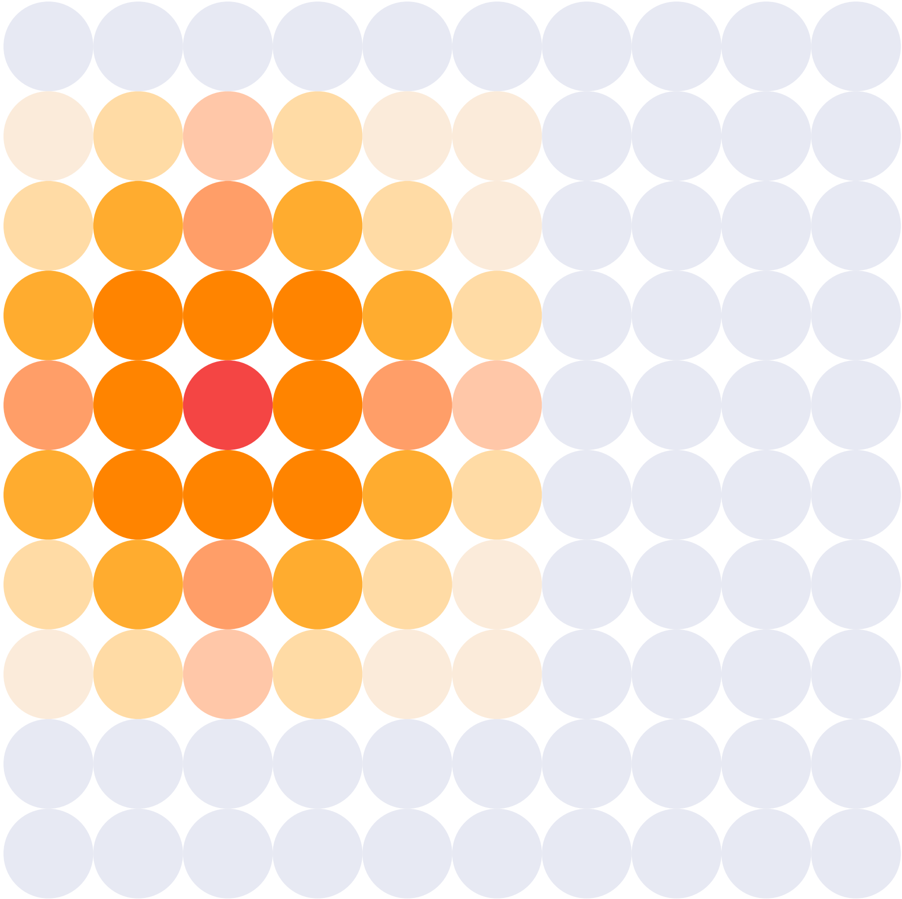
A punitive regulatory stance by the government will likely create top-down pressure on CISOs and security teams to be less forthcoming with the C-level and BoD when faced with a security event. It is not hard to see that security teams will feel pressure to not report events to leadership unless they absolutely must, and this has the potential to negatively impact security operations.

All these factors add up to one thing: organizations who were already struggling to defend themselves against the threat from ransomware and data extortion attacks now also must contend with being re-victimized by an overzealous legal and regulatory landscape.

And while the C-Level and BoD are increasingly at risk of legal and regulatory actions, it is most definitely the CISO or equivalent who is at most risk of getting thrown under the bus following a successful attack.

In this environment, it is likely that we may see CISOs and/or security team leaders potentially face jail time following an attack, and this risk could also extend to executives and Boards.

This trend will do little to help improve security and has the potential to do the exact opposite, putting more organizations and people at risk.



The Halcyon Mission: Defeat Ransomware

Halcyon.ai is the leading anti-ransomware company. Global 2000 companies rely on the Halcyon platform to fill endpoint protection gaps and defeat ransomware with minimal business disruption through built-in bypass and evasion protection, key material capture, automated decryption, and data exfiltration and extortion prevention – talk to a Halcyon expert today to find out more.

halcyon