

Extortion Attack Group Guide

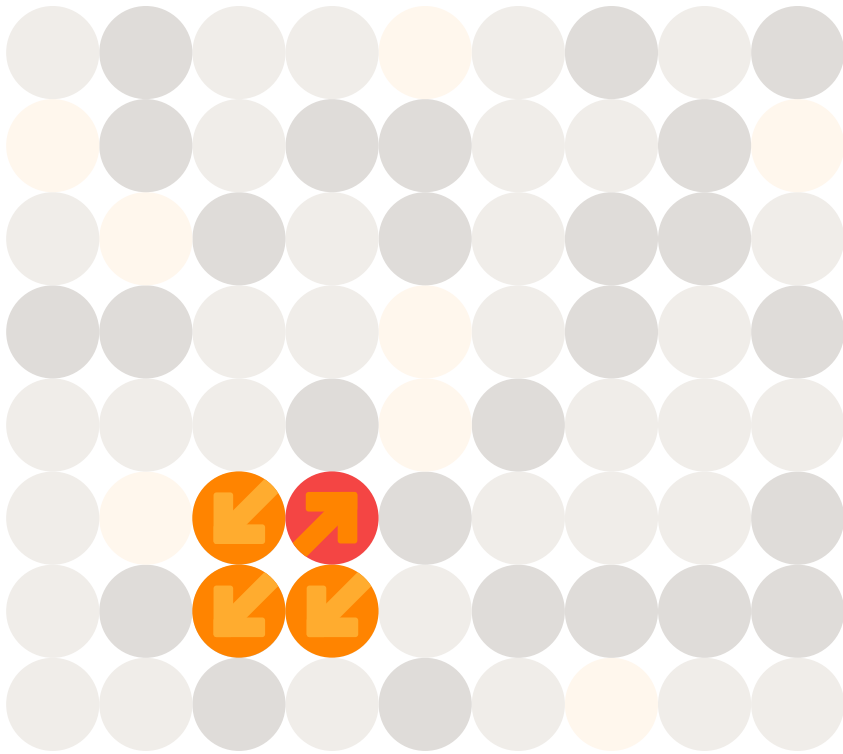
Power Rankings: Ransomware Malicious Quartile Q2-2024





Table of Contents

Ransomware Risk: Perception vs. Reality	3
Ransomware MQ: Evaluation Criteria Definitions	6
The Q2-2024 Ransomware Malicious Quartile.	7
Frontrunners	8
Play	8
Black Basta.	9
8Base.	10
LockBit.	12
Medusa	13
Akira	14
INC Ransom	16
Hunters International	17
RansomHub.	18
BlackSuit	19
BianLian	20
Cactus	21
Contenders	23
Qilin	23
Rhysida.	24
Snatch	25
Emerging	27
DragonForce.	27
RansomHouse	28
RaWorld	29
El Dorado	30
Diminishing	32
Stormous	32
Cuba	33
ClOp.	34
BlackCat/ALPHV	35
Q2-2024 Trends	38
Takeaway	39



Ransomware Risk: Perception vs. Reality

Ransomware attacks continue to plague nearly every major business sector as well as state and local Governments. The relentless pace of attacks brings into question whether organizations fully understand the threat and what steps need to be taken to reduce the risk of costly disruptions.

Halcyon recently conducted a survey published a new study detailing the significant impact on businesses from ransomware and data extortion attacks over the past 24 months. According to the [Ransomware and Data Extortion Business Risk Report \(PDF\)](#), there is a strong disconnect between perception and reality when it comes to prevention and resilience against ransomware and data extortion attacks.

While most respondents feel confident their current security deployments are adequate for both prevention and recovery, the data shows that most attacks are nonetheless successful and victim organizations are struggling to get operations back up and running, which is what is driving up post-attack recovery costs.

The study found that 88% of respondents indicated they were somewhat or very confident their organizations' current security deployments could disrupt an attack before a ransomware payload is delivered. Also, 85% were somewhat or very confident their organizations could quickly resume regular operations following a successful attack. Yet 36% indicated their organizations were infected 5 times or more over the two-year period.

Furthermore, 62% of organizations hit by ransomware reported a major disruption in operations, with 38% saying operations were disrupted for at least two months to more than six months. These findings clearly show that organizations are overly confident in their ability to defend against and quickly recover from ransomware attacks.

Given this disconnect, it's not surprising that the number of ransomware attack victims increased by 71% in 2023 over 2022 levels. The increase was driven by things like more automation, vulnerability exploits, and a 30% increase in the number of identified ransomware operators.

Data exfiltration occurs in nearly every major ransomware attack today, and nearly two-thirds of respondents said that sensitive or regulated data was exfiltrated from their organization. More than half reporting the attackers issued an additional ransom demand to protect the exfiltrated data. Additionally, 58% of victims reported that the loss of sensitive data put their organizations at additional risk of regulatory action and lawsuits.


The disconnect between perception and reality regarding the actual ransomware threat and perceived risk was underscored by the fact that the Cybersecurity and Infrastructure Security Agency (CISA) alerted nearly 2,000 organizations about known vulnerabilities being exploited by ransomware operators, yet the agency said that only about half took any action on the vulnerabilities despite the warnings.

The fact that hospitals across the nation have to cancel medical procedures and divert ambulances to other facilities, or that our schools are now just as likely to close due to ransomware attacks as they are for inclement weather, are evidence that our collective response to ransomware attacks has been completely inadequate.

Now we must contend with the fact that state and local Governments are regularly seeing critical services disrupted more frequently, even to the degree where officials are forced to declare a state of emergency – something typically reserved for the direst of circumstances.



Data exfiltration occurs in nearly every major ransomware attack today, and nearly two-thirds of respondents said that sensitive or regulated data was exfiltrated from their organization.



Ransomware operators try to elicit as much pain, frustration, and publicity as possible because it translates into revenue. But we cannot discount the dual nature of many of today's ransomware attacks, where the attackers may be serving themselves from a financial perspective but are also furthering a larger geopolitical strategy of an adversarial nation.

This is especially concerning as we move into an already contentious election season. As we approach the fall, we need to prepare for the potential that even a handful of isolated disruptions could cause unwarranted fear, uncertainty, and doubt amongst the public.

There need to be real consequences – not just for those who are orchestrating the attacks and benefitting financially, but also for the nation-states who are benefitting geopolitically. Until there are real consequences on the table, we will see these attackers continue to brazenly act with impunity.

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 Q2- 2024, which can be reviewed along with earlier reports here: [Power Rankings: Ransomware Malicious Quartile](#).



We cannot discount the dual nature of many of today's ransomware attacks, where the attackers may be serving themselves from a financial perspective but are also furthering a larger geopolitical strategy.



Ransomware MQ: Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q2-2024 Ransomware Malicious Quartile. All attack groups evaluated must be a known threat actor group in 2024 with verifiable victims who demanded a ransom payment. Click on the threat actor group name below to see a listing of recent attacks they conducted including targets, industry verticals and other details.

The report is based on available Q2-2024 data. Given the variability between attack groups regarding breadth of targeting, volume of attacks, and overall impact of their attack campaigns, placement on the report is subjective and based on input from ransomware subject matter experts on the following criteria:

Performance

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

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

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

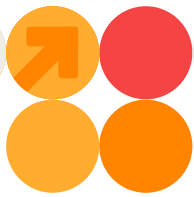
Victims: Sample of victim organizations provided, but attack groups are not ranked on victimology in this report.

Innovation

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

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

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



The Q2-2024 Ransomware Malicious Quartile

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



Source: Halcyon (Q2 2024)

Frontrunners

Play

Performance

- **RaaS Platform:** Play is a RaaS that emerged in the summer of 2022 and has ascended to the top of the threat actors ranking partly by merit, and partly by default as leaders like LockBit and BlackCat/ALPHV have diminished. The group has been one of most prolific threat actors in the RaaS space, and in the second quarter of 2024, it continued its operations with notable effectiveness and innovation. Play is noted for having similarities to the now defunct Hive and Nokoyawa ransomware strains. Play often compromises unpatched Fortinet SSL VPN vulnerabilities to gain initial 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 was one of the top three most prolific ransomware groups for Q1 2024, then they 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 exfiltrated data of those who refuse payment.
- **Victims:** American Nuts, Red River Title, Rackspace, City of Lowell, Geneva Software, Primoteq, Kenya Bureau of Standards, Cambridge Group, AI GoTech, Hill International, CS Cargo City of Oakland, Argentina's Judiciary, H-Hotels, Fedpol, Federal Office for Customs and Border Security (FOCBS).



Play became one of the most prolific threat actors in the RaaS space, and in the second quarter of 2024, and continued its operations with notable effectiveness and innovation.

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 focused attacks on 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 2024 to leverage their remote monitoring and management (RMM) tools to infiltrate customer networks. Recent attacks have targeted construction and manufacturing companies.
- **Economic Model:** Play operates with a well-run business model that includes substantial investment in research and development. The group reinvests in its operational capabilities and affiliate recruitment, maintaining a robust technical support system for its operations. The group employs tactics like the defunct 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.




Black Basta remains one of the most prolific attack groups in 2024 and was observed leveraging unique TTPs for ingress, lateral movement, data exfiltration, and deployment of ransomware payloads.

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. They have been active in exploiting vulnerabilities in ConnectWise (CVE-2024-1709) and using social engineering tactics for initial access. 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, and deployment of ransomware payloads.

- 
- **Ransom Demands:** Ransom demands vary depending on the targeted organization with reports that they can be as high as \$9 million dollars. It is estimated that 35% of the group's victims pay the ransom, enabling Black Basta to exceed \$107 million in ransom revenue from more than 500 victims in less than two years.
 - **Victims:** Southern Water, BionPharma, M&M Industries, coca Cola, Yellow Pages Canada, AgCo, Capita, ABB, Merchant Schmidt, Tag Aviation, Blount Fine Foods.

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 leveraged 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. Black Basta takes an average of 14% of ransom payments, distributing the remainder among its affiliates.

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 throughout the first half of 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 most active in late 2022 and early 2023. There also may be 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 throughout 2023 and the first half of 2024, making them one of the most active groups.
- **Ransom Demands:** It is unclear how much 8Base typically demands for a ransom.
- **Victims:** GPI Corporate, Lyon Terminal, East Coast Fisheries, Keystone Insurance Services, Spectra Industrial, Kansas Medical Center, Danbury Public Schools, BTU, Advanced Fiberglass Industries, ANL Packaging.



8Base engages in data exfiltration for double extortion and employs advanced security evasion techniques including modifying Windows Defender Firewall for bypass.

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 use a variety of ransomware payloads and loaders in their attacks, most prevalently customized Phobos with SmokeLoader code. 8Base has gained notoriety for its rapid and efficient encryption methods and the appending of a unique “.8base” extension to encrypted files. The group 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 the encryption. 8Base does not appear to be targeting Linux systems yet and is maintaining a focus on Windows. In Q2-2024, 8Base continued using a new variant of the Phobos ransomware payload, typically delivered with SmokeLoader.
- **Targeted Industries:** 8Base primarily targets organizations in the financial, healthcare, and information technology sectors, but about half of the targets are in the business services, manufacturing, and construction sectors.
- **Economic Model:** 8Base does not appear to maintain a RaaS program open to affiliate attackers, appearing to be opportunistic in their choice of victims with a focus on “name and shame” via their leaks site to compel payment of the ransom demand.

LockBit

Performance

- **RaaS Platform:** LockBit operates a RaaS platform 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. In February 2024, an international law enforcement task force called Operation Cronos succeeded in seizing and taking control of the LockBit administration environment. However, LockBit was back online within days. While LockBit continues to be active, it is assessed that they may be falsely reporting some attacks such as the one they claimed against the US Federal Reserve in an effort to maintain credibility with affiliates.
- **Attack Volume:** LockBit was particularly active in May 2024, launching 176 ransomware attacks, which represents a substantial portion of the ransomware activity recorded for that month. LockBit is by far the most prolific ransomware operation to date, but they are showing signs of decline.
- **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 of 2023. The group has extracted substantial ransoms, with reports suggesting cumulative ransom payments reaching into the hundreds of millions, indicating a highly lucrative operation. The ransom demands have varied widely, often reflecting the perceived ability of the victims to pay.
- **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:** The group's ability to continually upgrade their administrative tools and platforms underscores a high degree of maturity in their operations. LockBit continued to innovate their RaaS platform following the release of LockBit 3.0 in June of 2022,



LockBit was particularly active in May 2024, launching 176 ransomware attacks, which represents a substantial portion of the ransomware activity recorded for that month.



and introduced what is considered to be the first iteration of a macOS ransomware variant in April 2023, but the platform has remained relatively unchanged since then. 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, financial services, and government agencies.
- **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.

Medusa

Performance

- **RaaS Platform:** 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 very high in Q2-2024, making them one of the top active ransomware groups. 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.
- **Attack Volume:** Medusa is not the most prolific ransomware group, but it has been one of the more consistent threat groups in the first half of 2024.
- **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:** Toyota Financial Services, Tarrant County Appraisal District, Kansas City Area Transportation Authority, Traverse City Schools, SIMTA, ATI Traduction, EDB, Symposia Organizzazione Congressi S.R.L, Believe Productions, Global Product Sales, ZOUARY & Associés, Neodata, Evasión.

Innovation

- **RaaS Platform Development:** The Medusa RaaS operation 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 has a strategic approach to selecting high-value targets across various industries, effectively increasing the potential ransom payouts. 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.

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. Akira quickly became one of the most active groups and accounts for a significant volume of attacks in 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 growing attack volume, putting them among the leaders when compared to other ransomware operators. They have collected more than \$40 million in ransom for over 250 victims.
- **Ransom Demands:** Ransom demands appear to range between \$200,000 to more than \$4 million.
- **Victims:** Nissan, Royal College of Physicians and Surgeons, 4LEAF, Park-Rite, Family Day Care Services, The McGregor, Protector Fire Services, QuadraNet Enterprises, Southland Integrated

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 2023, 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 2023. Akira has also been observed exploiting VMware ESXi vulnerabilities for lateral movement.
- **Targeted Industries:** Akira targeted heavily in Latin America in June of 2024. The group is focused on the healthcare sector but 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.



Akira is heavily focused on the healthcare sector but has also attacked dozens of organizations across multiple industry verticals including education, finance, and manufacturing.

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 cybersecurity weaknesses.
- **Attack Volume:** INC did not emerge until the second half of 2023, but the cadence of attacks has been increasing through early 2024.
- **Ransom Demands:** INC instructs victims to log into a Tor portal with a unique user ID provided by the attackers. It is unclear what the average ransom demand is at this point.
- **Victims:** Peruvian Army, NHS Scotland, Xerox, Trylon Corp, BPG Partners Group, DM Civil, Nicole Miller INC., Pro Metals, Springfield Area Chamber of Commerce, US Federal Labor Relations Authority, Yamaha Philippines, Rockford Public Schools.

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 education, manufacturing, retail, IT, hospitality, pharma, construction, and the public sector.



INC has been observed delivering ransomware using legitimate tools like WMIC and PSEXEC and uses other LOTL techniques, abusing applications including MSPaint, WordPad, NotePad, MS Internet Explorer, MS Windows Explorer, and AnyDesk for lateral movement.



- **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.

Hunters International

Performance

- **RaaS Platform:** Hunters International operates as a 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 newest variant of Hunters International reverses an earlier tactic of storing the decryption key in a separate file and adopts the simpler and more customary practice of including the key within the encrypted file.
- **Attack Volume:** The attack volume for Hunters International has been substantial, with numerous campaigns launched throughout Q2-2024 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, Austal USA.

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 attack volume for Hunters International has been substantial, with numerous campaigns launched throughout Q2-2024 targeting a broad range of industries and geographies, indicating a significant operational capacity.



- **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, like other RaaS operations. They offer a portion of the ransom proceeds to affiliates who successfully deploy their ransomware, encouraging widespread dissemination of their malware.

RansomHub

Performance

- **RaaS Platform:** RansomHub operates as a RaaS platform, emerging in the cybercrime scene in early 2024 and was at first suspected of being tied to LockBit, but their code is like the defunct Knight group. 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.
- **Attack Volume:** RansomHub has rapidly grown to become one of the most active ransomware groups since its appearance in early 2024. By the end of Q2, it was responsible for many attacks across various sectors.
- **Ransom Demands:** The group has made substantial ransom demands, evidenced by the \$22 million demanded from Change Healthcare. This indicates their focus on targeting large organizations with the capacity to pay significant ransoms.
- **Victims:** Change Healthcare, Kovra, Computan, Scadea Solutions, Christie's Auction House, NRS Healthcare, Frontier Communications.

Innovation

- **RaaS Platform Development:** RansomHub has 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. RansomHub code is based on the Knight ransomware code, which is written in Golang. It was observed that the Knight group put the code up for sale in February 2024.



RansomHub has invested in recruiting former affiliates from other ransomware groups and maintain a versatile and updated codebase, indicating a well-funded operation with a focus on growth and sustainability.



- **Targeted Industries:** Initially focusing on the healthcare sector, RansomHub's approach indicates very strategic target selection due to the high value and sensitive nature of healthcare data.
- **Economic Model:** The group operates on a RaaS subscription model, which suggests a structured revenue-sharing system with its affiliates, like other prominent ransomware groups. RansomHub has invested in recruiting former affiliates from other ransomware groups and maintain a versatile and updated codebase, indicating a well-funded operation with a focus on growth and sustainability.

BlackSuit

Performance

- **RaaS Platform:** BlackSuit is not a traditional RaaS, but instead 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). BlackSuit targets both Windows and Linux systems.
- **Attack Volume:** BlackSuit has quickly gained notoriety for striking a variety of sectors with considerable impact, and activity in 2024 has been high.
- **Ransom Demands:** Details on typical ransom amounts are not well-documented, but their targeting of large enterprises and critical sectors suggests that their ransom demands are substantial. BlackSuit tailors ransom demands to the financial capabilities of victims to ensure the demand is "reasonable."
- **Victims:** ZooTampa, Southwest Binding & Laminating, Western Municipal Construction, CDK Global, Kansas City Police Department, Multi-Fill.

Innovation

- **RaaS Platform Development:** BlackSuit operates with a high 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.



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.



- **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.

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. They employ diverse hosting providers and use a wide range of ports to complicate detection efforts. In early 2023 they 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 see more groups join the likes of BianLian. While not the most prolific threat, BianLian has maintained steady operations over an extended period of time, making them one of the more successful groups.
- **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. The group has been active with new victims weekly per reports on their leak sites, but the pace of attacks has slowed slightly in Q2-2024.
- **Ransom Demands:** BianLian focuses primarily on threats of leaking stolen data to compel payment. It is unclear how much BianLian typically requests for a ransom amount, or if they are keen to negotiate the demand down.
- **Victims:** Air Canada, Griffing & Company, International Biomedical Ltd, Gilbreath, Dow Golub Remels & Gilbreath, Instron, Pelindo, CHU de Rennes, Dekko Window Systems Ltd, CMC Marine.



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.



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 Golang-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. They manage a comprehensive operation that involves data theft, extortion, and the use of a variety of exfiltration tools.

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 leverages 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 quickly amassed a disturbing number of victims—including nearly 60 high-profile victims—in a brief time, but the pace of attacks has slowed slightly in Q2-2024.
- **Ransom Demands:** Cactus employs an encrypted messaging platform called TOX chat to conduct negotiations with victims. Ransom demands are assessed to be quite substantial, but an average has not been established.
- **Victims:** Schneider Electric, SCS SpA, OmniVision Technologies, The Hurley Group, Cornerstone Projects Group, ICOR Global Limited, Cornerstone Projects Group, Societa' Canavesana Servizi.



Cactus quickly amassed a disturbing number of victims—including nearly 60 high-profile victims—in a brief time, but the pace of attacks has slowed slightly in Q2-2024.



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.
- **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. Cactus' economic model appears robust, incorporating advanced technological tactics and a business model that maximizes profit through the RaaS structure, suggesting considerable investment in R&D and recruitment of affiliates.

Contenders

Qilin

Performance

- **RaaS Platform:** Qilin is a RaaS operation that first emerged in July of 2022 that is written in the Golang 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 volume have increased dramatically. The group has claimed more than 60 victims in the first half of 2024. Qilin is said to be responsible for a devastating attack on healthcare provider Synnovis in the UK that disrupted patient care across the country's National Health Services system.
- **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:** Synnovis, NHS Hospitals, Big Issue Group, Ditronics Financial Services, Daiwa House, ASIC S.A., Thonburi Energy Storage, SIIX Corporation, WT Partnership Asia, FSM Solicitors, Etairos Health, Commonwealth Sign, Casa Santiveri.

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.



Qilin is said to be responsible for a devastating attack on healthcare provider Synnovis in the UK that disrupted patient care across the country's National Health Services system.

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. They utilize advanced techniques such as exploiting VPNs and leveraging vulnerabilities like Zerologon to gain initial access and maintain persistence. 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. A decryptor was published by researchers in February 2024 which slowed operations temporarily, but the group seems to have rebounded.
- **Attack Volume:** Rhysida attack volume increased slightly in Q2-2024, and they continue to expand the targeted industries, but volume is modest compared to leaders. Rhysida appears to be opportunistic attackers.
- **Ransom Demands:** Ransom demands are based in Bitcoin and have been seen to range from 15 BTC (\$775,000) to 60 BTC (\$3.7 million) in recent attacks.
- **Victims:** MarineMax, Lurie Children's Hospital, Pierce College at Joint Base Lewis McChord, Ejercito de Chile, Axiety, Ministry of Finance Kuwait, Prince George's County Public Schools, Ayuntamiento de Arganda City Council, Comune di Ferrara, Prospect Medical Holdings, Martinique Government.

Innovation

- **RaaS Platform Development:** Rhysida appears to have a mature 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 like those of Vice Society, so it is possible Rhysida is a related group.



Rhysida appears to have a mature 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.



- **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.

Snatch

Performance

- **RaaS Platform:** Snatch is a RaaS first emerged back in 2018 but did not become significantly active until 2021. Snatch is a consistent threat that persists but has neither gained a lot of momentum nor diminished over time. 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 has hit several targets in 2024 and their attack volume has been consistent, although nothing comparable to leading attack groups, so they may be trying to keep themselves from drawing too much attention.
- **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, South African National Health Laboratory Service.

Innovation

- **RaaS Platform Development:** Snatch is written in Golang and is 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,



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.



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 has a history of spending up to three months within a victim's network before executing ransomware. They abuse 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.

Emerging

DragonForce

Performance

- **RaaS Platform:** DragonForce operates a sophisticated RaaS platform that utilizes a leaked builder from the notorious LockBit group. This platform allows DragonForce to execute effective attacks that disrupt significant portions of targeted networks. Their ability to evade detection until the ransomware payload is executed demonstrates a high level of maturity in their operations.
- **Attack Volume:** DragonForce has been highly active with numerous attacks reported in Q2-2024. Notable victims include the Seafrigo Group, where 43.01 GB of data was exfiltrated, and the Government of Palau, despite the latter's denial of contact with the attackers. Their attack campaigns are frequent, and their success rate appears substantial given the number of high-profile victims.
- **Ransom Demands:** DragonForce 's ransom demands vary, but they aim for significant amounts. Specific ransom amounts are not always disclosed, but their operations suggest they aim for high-value targets to maximize their demands.
- **Victims:** Seafrigo Group, Ohio Lottery, Yakult Australia, Coca-Cola Singapore.

Innovation

- **RaaS Platform Development:** DragonForce continues to develop and improve its RaaS platform by incorporating advanced features and tactics from the LockBit ransomware. Their use of sophisticated double extortion techniques, combining data encryption with the threat of data leaks, shows ongoing development and enhancement of their operational capabilities.
- **Targeted Industries:** DragonForce effectively selects high-profile targets that are likely to yield high ransom payments. Their targets span various industries, including logistics, Government, manufacturing, and healthcare. This strategic targeting helps them realize significant ransom demands and payments.



DragonForce continues to develop and improve its RaaS platform by incorporating advanced features and tactics from the LockBit ransomware.



- **Economic Model:** DragonForce operates a well-structured business model, focusing on recruiting affiliates and providing technical support to maximize the efficiency and impact of their attacks. Their use of advanced tools and continued R&D investments underscore a robust economic model designed to sustain and grow their operations. The group's ability to rapidly incorporate new tactics and tools highlights their commitment to maintaining a competitive edge in the cybercriminal landscape.

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 custom tool.
- **Attack Volume:** RansomHouse attack volumes pale compared to leading threat actors but remain notable with some high-profile attacks in 2024, although the group shows signs they could be diminishing.
- **Ransom Demands:** Ransom demands have been reported to range between \$1 million and \$11 million.
- **Victims:** Advanced Micro Devices, Indonesia Power, AMD, Mission Community Hospital, Van Oirschot, Hawkins Delafield Wood, SMB Solutions, United Urology Group.

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.



RansomHouse attack volumes pale compared to leading threat actors but remain notable with some high-profile attacks in 2024, although the group shows signs they could be diminishing.

RaWorld

Performance

- **RaaS Platform:** RaWorld has demonstrated effectiveness in executing attacks through multistage processes designed to disrupt significant portions of targeted networks and employs tactics like exploiting Group Policy Objects (GPOs) and using antivirus evasion measures to evade detection until the ransomware payload is executed.
- **Attack Volume:** During Q2-2024, RaWorld was involved in numerous attacks, particularly targeting healthcare organizations in Latin America and the financial sector. The group has shown a high success rate in breaching defenses and executing their ransomware payload.
- **Ransom Demands:** RaWorld's ransom demands have varied, but they typically range from several hundred thousand to millions of dollars, depending on the victim's size and industry. Estimates suggest significant income from their operations, given the successful breach of several large organizations.
- **Victims:** In Q2-2024, RaWorld targeted multiple healthcare organizations in Latin America, along with financial institutions and other businesses in the US and South Korea. Specific victims include several unnamed healthcare providers and financial firms.

Innovation

- **RaaS Platform Development:** RaWorld has shown continuous improvement in their RaaS platform, including customizing ransomware using the leaked Babuk source code. This customization involves sophisticated encryption techniques and the use of unique ransom notes tailored to each victim. RAWorld more recently added a Linux version that is not based on the Babuk code but is instead written in Golang.
- **Targeted Industries:** The group's primary targets have been in the healthcare and financial sectors, chosen for their high potential for significant ransom payments. The effectiveness of their target selection is evident in their high-profile breaches and the substantial ransom demands met by victims.



RaWorld has demonstrated effectiveness in executing attacks through multistage processes designed to disrupt significant portions of targeted networks and employs tactics like exploiting Group Policy Objects (GPOs) and using antivirus evasion measures.



- **Economic Model:** RaWorld operates with a well-structured business model that includes substantial investments in research and development, recruiting affiliates, and providing technical support. The group's economic model also involves double extortion tactics, where they steal data before encrypting it and threaten to leak the data if the ransom is not paid.

El Dorado

Performance

- **RaaS Platform:** El Dorado, emerging in March 2024, operates as a RaaS platform targeting both Linux and Windows systems. The group has developed a sophisticated ransomware builder that does not rely on previously leaked ransomware tools, which demonstrates their maturity and innovation. The ransomware uses Golang for cross-platform capabilities, allowing it to encrypt files on both Windows and Linux including VMware ESXi environments.
- **Attack Volume:** By June 2024, El Dorado had executed 16 known attacks, with a significant concentration in the United States, where 13 of these incidents occurred.
- **Ransom Demands:** While specific ransom demand amounts are not detailed, the use of sophisticated encryption methods (ChaCha20 for file encryption and RSA-OAEP for key encryption) and targeted attacks on high-value sectors suggest high ransom demands. The group's focus on industries that can afford to pay large sums implies substantial potential income from their operations.
- **Victims:** Victims in Q2-2024 included companies across various sectors, primarily in the United States. Notable targeted industries included real estate, education, healthcare, professional services, and manufacturing. Specific organizations have not been publicly named, but the distribution indicates a strategic approach to victim selection.

Innovation

- **RaaS Platform Development:** El Dorado's platform is noted for its continuous development and customization options. The ransomware builder is unique and does not rely on previously published sources. It allows for extensive customization, including targeting specific directories, skipping local files, and focusing on network shares.



El Dorado has developed a sophisticated ransomware builder that does not rely on previously leaked ransomware tools, which demonstrates their maturity and innovation.



- **Targeted Industries:** El Dorado effectively targets high-value sectors such as real estate, healthcare, and education, maximizing the potential for high ransom payments. This strategic targeting demonstrates a deep understanding of industry vulnerabilities and the potential monetary impact of ransomware attacks.
- **Economic Model:** El Dorado operates with a sophisticated business model, recruiting affiliates through forums like RAMP and providing technical support and customization options. The use of Golang for cross-platform capabilities and the availability of both Windows and Linux encryptors indicate significant investment in R&D. The group's approach includes leveraging existing system tools for lateral movement and encryption, enhancing their evasion tactics and operational effectiveness.

Diminishing

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. 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 had escalated following its partnership with GhostSec, but declined significantly in 2024.
- **Ransom Demands:** It is unclear how much Stormous demands for ransom payments on average, but the largest observed random demand from the group is \$500,000.
- **Victims:** Vietnam Electricity, Duvel Moortgat Brewery, Konika Minolta, Cameron Memorial Community Hospital, Econocom Group, Senior Sistemas, Bandung Institute of Technology, Epson Spain, Interep.

Innovation

- **RaaS Platform Development:** Stormous does not maintain a RaaS platform and focuses on straight data extortion. Stormous and a lesser threat actor called GhostSec began collaborating, in 2024 and it was observed that Stormous has used the GhostLocker encryptor developed by GhostSec in some recent attacks, as well as engaging in double 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 sow 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. In 2024 they began to engage in double extortion, but the franchise looks to be failing.



Stormous and a lesser threat actor called GhostSec began collaborating, in 2024 and it was observed that Stormous has used the GhostLocker encryptor developed by GhostSec in some recent attacks.

Cuba

Performance

- **RaaS Platform:** Cuba is a RaaS that first emerged in 2019, but activity did not really ramp up until 2022, and attacks had continued to steadily increase into early 2024 but dropped off dramatically in Q2-2024. 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 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 spiked in late 2023 but has tapered off in the first half of 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 anything close to their outrageous demands.
- **Victims:** DMS Imaging, Rock County Public Health Department, Mount St. Mary Catholic High School, Phoenicia University, R1 Group, 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. Recent attacks have used a new variant optimized to minimize unintended system behavior to avoid detection.



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.



- **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.

CIOp

Performance

- **RaaS Platform:** Attacks by CIOp operators and affiliates fell dramatically in August 2023, then the group appeared to have gone dark altogether in September 2023 with few attacks attributed to them throughout the rest of Q1-2024. In Q2-2024, CIOp has all but disappeared. CIOp 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. CIOp 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. CIOp's unprecedented campaign exploiting the MOVEit vulnerability drove attacks levels to a new high, with CIOp assessed to be responsible for about one-fifth (21%) of all ransomware attacks in July.
- **Attack Volume:** Attacks by CIOp surged in 2023 as the gang leveraged patchable exploits for the GoAnywhere file transfer software to compromise more than 100 victims in a matter of weeks. CIOp proceeded to compromise thousands of organizations leveraging the MOVEit vulnerability in early summer 2023 but attacks have all but ceased in Q2-2024.
- **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 CIOp 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.



CIOp proceeded to compromise thousands of organizations leveraging the MOVEit vulnerability in early summer 2023 but attacks have all but ceased in Q2-2024.



Innovation

- **RaaS Platform Development:** CIOp was one of the first RaaS groups that developed a Linux version, an indication that CIOp had been actively recruiting new talent to help improve their platform and expand their addressable target range. CIOp's Windows version was written in C++ and encrypts files with RC4 and the encryption keys with RSA 1024-bit. In 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 exclusively hit targets in the healthcare sector before significantly expanding targeting to include most any organization with vulnerable GoAnywhere installations, particularly in financial services and Government agencies.
- **Economic Model:** CIOp ran 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 were 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.


BlackCat/ALPHV

Performance

- **RaaS Platform:** The Justice Department and FBI actively targeted BlackCat/ALPHV through disruptions and decryption tools to mitigate the impact of their attacks. In Q1-2024, the BlackCat/ALPHV gang suffered a major disruption by law enforcement, with reports that they took down the operator's websites and developed a decryption tool. However, 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. 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



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.



includes JSON configurations for affiliate customization. BlackCat/ALPHV is adept at disabling security tools and evading analysis and is 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, but the franchise folded in early 2024.
- **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 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 had 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.



Q2-2024 Trends

Some interesting trends emerged in the first quarter of 2024:

Legal and Regulatory Liability

- **Vendors Sued:** A recently filed lawsuit by law firm Mastagni Holstedt against managed service provider (MSP) LanTech LLC and data backup provider Acronis seeks more than \$1 million in damages, alleging the companies failed to protect the firm from a disruptive ransomware attack: [MSSP Alert](#)
- **Victims Sued:** US Fertility (USF), which provides IT services to more than 200 physicians at multiple fertility clinics, has 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](#)
- **Revictimized:** The US Department of Health & Human (HHS) Services Office for Civil Rights (OCR) recently opened an investigating into medical payments giant Change Healthcare to enforce rules designed to safeguard the Protected Healthcare Information (PHI) of patients: [Infosecurity Magazine](#)
- **C-Level Liability:** Nearly two-dozen state Attorney's General have petitioned the CEO of UnitedHealth Group over concerns following the devastating ransomware attack on subsidiary Change Healthcare that occurred in February: [PDF](#)
- **Data Extortion:** Group Health Cooperative of South-Central Wisconsin (GHC-SCW), a non-profit healthcare service provider, disclosed that documents containing the private health information (PHI) of over 500,000 individuals were exfiltrated in a January ransomware attack: [Bleeping Computer](#)

- **Risk of Exposure:** A threat group known as ShinyHunters apparently published a 1.3TB database of compromised Ticketmaster customer data on the relaunched BreachForums criminal forum and is asking for a \$500,000 ransom: [Tech Radar](#)

Dual Nature of Ransomware

- **Plausible Deniability:** FBI says ongoing Chinese campaign known as Volt Typhoon has successfully gained access to numerous American companies in telecommunications, energy, water and other critical sectors, with 23 pipeline operators targeted – China says it's ransomware gangs: [Reuters](#)
- **Voting Systems at Risk:** Georgia's Coffee County was forced the county to sever the connection to the state's voter registration system out of precaution following a ransomware attack after CISA (Cybersecurity and Infrastructure Security Agency) notified the county of the attack in mid-April: [CNN](#)
- **In Crisis:** An attack on the Ascension hospital system has forced staff to depend on manual paper-and-pen systems in the treatment of patients in an environment described by one nurse as "pure and utter chaos from the second you walk into the door": [WKRN](#)
- **Lives at Risk:** Medical procedures have been canceled at multiple London hospitals and a critical emergency declared in the aftermath of a ransomware attack against pathology services provider Synnovis: [Reuters](#)
- **Increasing Attacks:** At least 44 ransomware attacks targeting healthcare organizations in April following disclosure of a \$22M payout in the Change Healthcare attack, more victims from that sector than they have ever previously tracked in a single month: [Wired](#)



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, and potential legal consequences stemming from ransomware attacks 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.


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, 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. 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 do not 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 is 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.

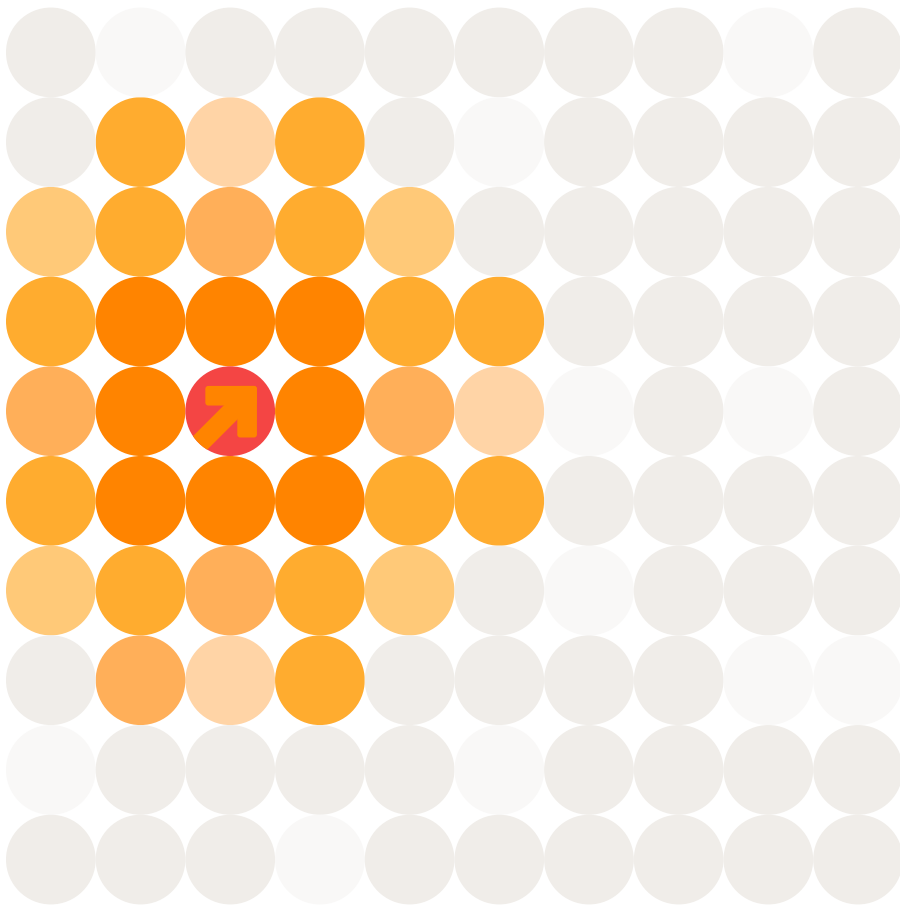
Security Controls Effectiveness: Assess the effectiveness of security controls by monitoring metrics such as intrusion detection/prevention system (IDS/IPS) alerts, firewall rule effectiveness, and malware detection rates. Are your controls effective? Should you be investing in other areas with potentially 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 comprehensive 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 is 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 and Resilience 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.

