

Q3
2023

Extortion Attack Group Guide

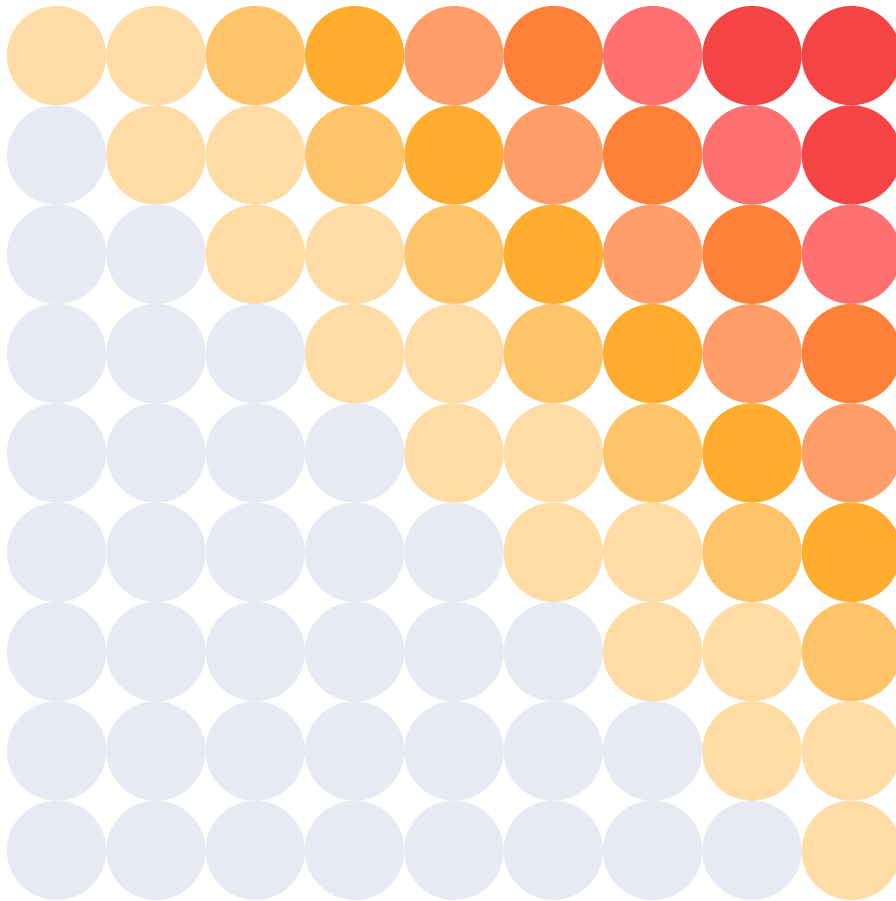
Power Rankings: Ransomware Malicious Quartile Q3-2023





Table of Contents

Power Rankings: Ransomware Malicious Quartile	1
The Data Extortion Attack Threat	3
Ransomware MQ: Evaluation Criteria Definitions	5
The Q3-2023 Ransomware Malicious Quartile	6
Frontrunners	7
ClOp	7
LockBit	8
BlackCat/ALPHV	9
Play	11
BlackBasta	12
8Base	13
Royal	14
Akira	15
Medusa	16
Contenders	18
Cuba	18
Rhysida	19
Snatch	20
BianLian	21
BlackByte	22
Nokoyawa	23
Emerging	25
NoEscape	25
RansomHouse	26
Cactus	27
Stormous	28
Malloxv29	
Qilin	30
Diminishing	31
AvosLocker	31
Vice Society	32
Trigona	33
Q3-2023 Trends	35
Takeaway	37
The Halcyon Mission: Defeat Ransomware	39



The Data Extortion Attack Threat

If the cost of recovering from a ransomware attack does not kill a business, the legal and regulatory fallout certainly could. The annual impact from ransomware attacks in the US alone is estimated to be more than \$20 billion dollars.

On average, ransomware attacks cost more than \$4M to fully remediate, but these estimates do not include potential losses from lawsuits and other tangential costs like damage to the brand, lost revenue, lost production from downed systems, and other collateral damage such as Intellectual property and regulated data loss.



The annual impact from ransomware attacks in the US alone is estimated to be more than \$20 billion dollars.

The financial losses stemming from a ransomware attack can go far beyond incident response and recovery action. Consider [the case of KNP Logistics](#), the UK's largest logistics provider, which declared itself insolvent in September of 2023 following a major ransomware attack that impacted operations and resulted in excessive losses.

Ransomware attacks create liability issues and intellectual property loss for organizations as attackers focus on the exfiltration of sensitive data prior to delivering the ransomware payload, or in some cases opting not to deliver a payload and engage in direct data extortion. We are seeing more [class action lawsuits](#) being filed against victim organizations who suffered data loss in the course of a ransomware attack, and the liability issue is reaching all the way up to company officers and Boards of Directors.

RaaS operators and other data extortion attackers also continue to develop custom tooling and implement novel evasion techniques designed to evade or completely circumvent traditional endpoint protection solutions. Recent reporting indicates ransomware operators have reduced the time to infection after initial compromise from an average 4.5 days to just a matter of hours.

This is because attackers are increasingly taking advantage of unpatched vulnerabilities and misconfigurations by automating aspects of their attack progressions. Automation means ransomware operators can simply hit more victims faster.

For example, hundreds of organizations have been hit by the CIOp ransomware gang this year as they continue to exploit known vulnerabilities in the MoveIT and GoAnywhere software. We also saw signs of automation in attacks exploiting a host of other known, patchable vulnerabilities throughout 2023.

Furthermore, ransomware operators are also expanding their addressable target range with the introduction of Linux variants as well as what is assessed to be the first viable variant targeting macOS being observed in the wild.

The Halcyon team of ransomware experts has put together this extortion group power rankings guide as a quick reference for the extortion threat landscape based on data from throughout Q3-2023, which can be reviewed along with earlier reports here: [Power Rankings: Ransomware Malicious Quartile](#).



The UK's largest logistics provider, which declared itself insolvent in September of 2023 following a major ransomware attack that impacted operations and resulted in excessive losses.



Automation means ransomware operators can simply hit more victims faster. They've reduced the time to infection after initial compromise from an average 4.5 days, to just a matter of hours.



Ransomware MQ: Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q3-2023 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 Q3-2023 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 as well as the percentage of attacks that are known to have been successful.

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

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

Innovation

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

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

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

The Q3-2023 Ransomware Malicious Quartile

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



Source: Halcyon (Q3 2023)

Frontrunners

CIOp

Performance


- **RaaS Platform:** 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. Clop'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 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. CIOp 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 CIOp 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 CIOp 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

Innovation

- **RaaS Platform Development:** CIOp is one of just a handful of known RaaS groups that have developed a Linux version, an indication that CIOp is likely 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



CIOp's unprecedented campaign exploiting the MOVEit vulnerability drove attack levels to a new high, with CIOp assessed to be responsible for about one fifth (21%) of all ransomware attacks in July.



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

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

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 CIOp in Q3. Nonetheless, LockBit is by far the most prolific ransomware operation to date.
- **Ransom Demands:** LockBit has demanded ransoms in excess of \$50 million and hit the world's biggest computer chip maker, Taiwan Semiconductor Manufacturing Company (TSMC), with a \$70 million ransom demand in July.
- **Victims:** 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, with demanded ransoms in excess of \$50 million.



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.
- **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 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.


BlackCat/ALPHV

Performance

- **RaaS Platform:** 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. 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.
- **Attack Volume:** BlackCat/ALPHV became one of the more active RaaS platforms over the course of 2022, and attack volumes in 2023 continue at a steady pace.



New information surfaced claiming the ALPHV/BlackCat ransomware group is responsible for the debilitating cyberattack on MGM Resorts International.

- 
- **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, PWC, Ernst & Young, and Sony, Republic Steel, Coca Cola, Constellation Software, Ring, Five Guys Restaurants

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.
- **Targeted Industries:** BlackCat/ALPHV has a 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.

Play

Performance

- **RaaS Platform:** Play (aka PlayCrypt) is a RaaS that emerged in the summer of 2022 and is noted for having similarities to Hive and Nokoyawa ransomware strains. Play often compromises unpatched Fortinet SSL VPN vulnerabilities to gain access. Play made headlines with high-profile attacks on the City of Oakland, Argentina's Judiciary and German hotel chain H-Hotels, as well as exfiltrating data from Fedpol and the Federal Office for Customs and Border Security (FOCBS)
- **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

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.



Play made headlines with high-profile attacks on the City of Oakland, Argentina's Judiciary, and the one and only Rackspace.

- **Targeted Industries:** Play ransomware gang has mainly focused attacks in Latin America, especially Brazil, but have attack outside of that region. Play was observed to be running a worldwide campaign targeting managed service providers (MSPs) in August in an attempt 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.

BlackBasta

Performance

- **RaaS Platform:** BlackBasta 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. BlackBasta engages in highly targeted attacks and is assessed to only work with a limited group of highly vetted affiliate attackers.
- **Attack Volume:** BlackBasta 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.
- **Victims:** BionPharma, M&M Industries, Coca-Cola, Yellow Pages Canada, AgCo, Capita, ABB, Merchant Schmidt, Tag Aviation, Blount Fine Foods



BlackBasta maintains a double extortion scheme, and an active leaks website where they post exfiltrated data if a victim organization declines to pay the ransom.

Innovation

- **RaaS Platform Development:** BlackBasta continues to evolve their RaaS platform, with ransomware payloads that can infect systems running both Windows and Linux systems. BlackBasta is particularly adept at exploiting vulnerabilities in VMware ESXi running on enterprise servers. BlackBasta 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, BlackBasta leverages malware strains like Qakbot and exploits

such as PrintNightmare during the infection process. BlackBasta also favors abuse of insecure Remote Desktop Protocol (RDP) deployments, one of the leading infection vectors for ransomware.

- **Targeted Industries:** BlackBasta typically targets manufacturing, transportation, construction and related services, telecommunications, the automotive sector, and healthcare providers.
- **Economic Model:** BlackBasta also employs a double extortion scheme and maintains an active leaks website where they post exfiltrated data if an organization declines to pay the ransom demand.

8Base

Performance

- **RaaS Platform:** The 8Base ransomware gang first emerged in March of 2022 and has quickly become one of the most active groups today, having displayed a "massive spike in activity" in the first half of 2023. The sophistication of the operation suggests they are an offshoot of experienced RaaS operators—most likely Ransomhouse, a data extortion group that first emerged in December of 2021 and was quite active in late 2022 and early 2023. Other researchers see a connection to the leaked Babuk builder. Like most groups today, 8Base engages in data exfiltration for double extortion and employs advanced security evasion techniques including modifying Windows Defender Firewall for bypass.
- **Attack Volume:** 8Base quickly ascended the ranks of active ransomware operators with a high volume of attacks in late spring and throughout the summer of 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



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



of ransomware payloads and loaders in their attacks, most prevalently customized Phobos with SmokeLoader. Attacks also include 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.

- **Targeted Industries:** 8Base targets organizations who provide as well as those 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.

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 despite showing a slight reduction in activity in Q3. 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 Q3 has been below average.
- **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



Royal continues to invest heavily in development expanding their operations and capabilities, to include advanced security evasion and anti-analysis capabilities.



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.

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.



Akira's platform has a chat feature for victims to negotiate directly with the attackers, and it has been observed that Akira informs victims who have paid a ransom of the infection vectors.



- **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

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.

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 in late 2022. Attack volumes have been inconsistent in the first half of 2023 with signs of a resurgence of attack activity in Q3. 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 attacked Philippine Health Insurance Corporation (PhilHealth) in September and leaked approximately 750 gigabytes of sensitive company and customer data.



- **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.

Contenders

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 the first half of 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).
- **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.



Cuba is assessed to be Russian operated and connected to threat actors RomCom and Industrial Spy.



- **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 maintain 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.

Rhysida

Performance

- **RaaS Platform:** Rhysida is a RaaS that was first observed in May of 2023, and they engage in data exfiltration for double extortion and maintain 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.
- **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, Axiety, Ministry of Finance Kuwait, Prince George's County Public Schools, Ayuntamiento de Arganda City Council, Comune di Ferrara



Rhysida is more recently known for their attack on Prospect Medical Holdings which impacted services at hundreds of clinics and hospitals across the US.

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.

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 in order 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 is on pace to increase 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

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



Snatch tried 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.



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.

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 the latter part of Q3.
- **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



BianLian abandoned the ransomware payload portion of attacks in favor of less complicated data exfiltration and extortion attacks.



Innovation

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

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 they 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 but are on pace to more than double in 2023.
- **Ransom Demands:** Ransom demands from 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 exfiltrates victim data for double extortion and maintain a leaks site to expose or sell victim data. The operators even go so far as to link the auction site in the ransom note.



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 to expose or sell victim data. The operators even go so far as to link the auction site in the ransom note to scare victims.

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 in regard to 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.



Nokoyawa released a variant written in Rust, a secure, cross-platform programming language that makes it easier to evade security controls and target multiple OSes.



- **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.

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.

Emerging

NoEscape

Performance

- **RaaS Platform:** NoEscape – assessed to be a spinoff of the disbanded Avaddon gang—emerged in May of 2023 and operates as a Ransomware-as-a-Service (RaaS) and emerged 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.



Having just recently emerged, NoEscape has rapidly become one of the more prolific attack groups, with attack volume escalating significantly.

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 its 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.

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 hackers 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 then declined in Q3.
- **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

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 is a different kind of threat actor who uniquely "blames" victim organizations for lax security.

Cactus

Performance

- **RaaS Platform:** Cactus ransomware emerged in March of 2023 and 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 quickly amassed a disturbing number of victims in a relatively short time, and attack volumes have escalated in the second and third quarters of 2023.
- **Ransom Demands:** Cactus employs an encrypted messaging platform called TOX chat to conduct negotiations with victims. Ransom demands are assessed to be quite substantial, but an average has not been established.
- **Victims:** 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, AnyDesk, and SuperOps RMM along with deploying Cobalt Strike. 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 generally large-scale commercial organizations across multiple sectors.
- **Economic Model:** As with most extortion gangs today, Cactus engages in data exfiltration by for double extortion by abusing Rclone tool.



Cactus is a new arrival on the RaaS scene but has quickly amassed a disturbing number of victims in a relatively short time, and attack volumes have escalated in the second and third quarters of 2023.

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 modest and 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

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.



Stormous is assessed to have targeted companies whose data was leaked by other threat actors, and some have asserted they are a scam operation.

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 was low but began to accelerate in late 2022 and continued to increase throughout 2023, with activity surging by 174% over 2022 levels.
- **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 Pvt

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.



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.



- **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.

Qilin

Performance

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



Qilin attack volumes are modest but they are putting a lot of resources into developing one of the most generous profit sharing affiliate programs.

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.

Diminishing

AvosLocker

Performance

- **RaaS Platform:** AvosLocker is a threat actor that was first observed in July of 2021, and follows the RaaS model. AvosLocker attacks typically leverage vulnerability exploits and are adept at evading security tools by using polymorphic techniques for payloads and running in Safe Mode.
- **Attack Volume:** While not nearly as prolific as leading threat actors, AvosLocker was more active in 2022 and early 2023, but may be showing signs of a resurgence.
- **Ransom Demands:** AvosLocker began with ransom demands in the hundreds of thousands of dollars but increased those demands into the millions of dollars over time.
- **Victims:** Pacific City Bank, Stratford University, Teladan Prima Agro Indonesia, ALVAC, CASA International, Bluefield University, Entigrity Solutions, Desman Design Management

Innovation

- **RaaS Platform Development:** AvosLocker is written in C++ and has versions for Windows, Linux, and VMware EXSi. It uses the legitimate AnyDesk software to access victim machines and leverages legitimate anti-debugging services for obfuscation. When possible, AvosLocker will delete system restore points, VSS shadow copies, and any backups to thwart recovery efforts. Older versions use RSA AES-256 and ChaCha20 for encryption, while newer versions use Salas20 for file encryption then it encrypts the file encryption keys with RSA AES-256. AvosLocker attacks leverage legitimate open-source tools through living-off-the-land (LotL) tactics for lateral movement including Cobalt Strike and Sliver for C2, Lazagne and Mimikatz for credential theft, tunneling tools such as Chisel and Ligolo, as well as resources like Rclone and FileZilla for data exfiltration that significantly reduce the likelihood of being detected on the targeted network. AvosLocker also abuses remote system administration tools like Splashtop Streamer, Tactical RMM, PuTTY, AnyDesk, PDQ Deploy, and Atera Agent for backdoor access to the network.



AvosLocker is written in C++ and has versions for Windows, Linux, and VMware EXSi. It uses the legitimate AnyDesk software to access victim machines and leverages legitimate anti-debugging services for obfuscation.



- **Targeted Industries:** In the spring of 2022, the FBI issued an alert that AvosLocker ransomware being used in attacks targeting US critical infrastructure.
- **Economic Model:** AvosLocker engages in data exfiltration for double extortion and negotiators may threaten distributed denial-of-service (DDoS) attacks during negotiations.

Vice Society

Performance

- **RaaS Platform:** Vice Society is not a traditional RaaS. The threat group that first emerged in 2021 and has used a variety of ransomware strains including Hello Kitty/Five Hands and Zeppelin before developing a custom ransomware strain that can infect both Windows and Linux systems. Tactics include attempts to compromise data backup solutions and clearing security logs on compromised systems to evade detection. Vice Society has been actively developing custom ransomware dubbed PolyVice and implementing better encryption methods.
- **Attack Volume:** Vice Society is a more recent arrival on the ransomware scene and has been scaling their operations significantly, including a disruptive attack on the second largest school district in the US.
- **Ransom Demands:** Vice Society typically issues ransom demands of more than \$1 million dollars, but evidence suggests they are willing to negotiate for a lower ransom amount.
- **Victims:** San Francisco Bay Area Rapid Transit (BART), Fire Rescue Victoria, Monmouth College, CAFPI, Bogleboo, Hamburg University of Applied Sciences, Lakeland Community College

Innovation

- **RaaS Platform Development:** Vice Society has advanced evasion capabilities and can disable security tools like Windows Defender and evade sandbox analysis. The group is known to exploit vulnerabilities in public-facing applications and websites, exploits like PrintNightmare, or through compromised RDP credentials. Vice Society is known to use DLL side-loading techniques and abuse tools like Cobalt Strike, Mimikatz, SystemBC and PowerShell scripts for remote access to endpoints and



Vice Society is not a traditional RaaS. As a more recent arrival on the scene they've been scaling their operations significantly, including a disruptive attack on the second largest school district in the US, LAUSD.



termination of security software. Vice Society has been observed using Living-off-the-Land (LotL) techniques by way of a custom PowerShell-based tool to automate data exfiltration on targeted networks.

- **Targeted Industries:** Vice Society tends to target the education, healthcare, and manufacturing sectors, but is also noted for attacks like the one that disrupted the rapid transit system in San Francisco.
- **Economic Model:** Vice society uses a double extortion model to compel payment of the ransom demand.

Trigona

Performance

- **RaaS Platform:** Reports indicate hactivists aligned with the Ukrainian Cyber Alliance compromised systems under the control of the Trigona ransomware gang, exfiltrated hundreds of gigabytes of data including source code and potentially decryption keys, and then wiped the servers. Trigona was not a traditional RaaS. The ransomware gang emerged around June of 2022 and operators have been observed scanning for internet-exposed Microsoft SQL servers to exploit via brute-force or dictionary attacks, and they also maintain a Linux version. Trigona is written in Delphi and includes a data wiper feature and has been observed to exfiltrate victim data for double extortion. The attackers will drop malware researchers dubbed CLR Shell to collect system information, to make configuration changes, and to escalate privileges by way of a vulnerability in the Windows Secondary Logon Service.
- **Attack Volume:** Trigona attack volume in 2022 was minimal, but has increased in the first half of 2023, with more than twice the detected attacks in Q1-2023 than in the second half of 2022.
- **Ransom Demands:** It is unclear how much they typically demand for a ransom.
- **Victims:** Amouage, Rolser, Alconex Specialty Products, Alconex, Quest International, FPZ GmbH, Portesa, Feit Electric, Lolaico Impianti, Public Health Management Corporation



Trigona is not a traditional RaaS Group. Trigona is written in Delphi and includes a data wiper feature that has been observed to exfiltrate victim data for double extortion.



Innovation

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



Q3-2023 Trends

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

General

- **Ransomware Unabated:** Ransomware operators are set to have the second most profitable year according to the Department of Homeland Security's 2024 Homeland Threat Assessment report
- **Reporting Issues:** The majority of executives surveyed (61%) indicate they did not report a major ransomware attack to authorities
- **Insurance Claims Spike:** Reports indicate a 12% spike in cyber insurance claims related to ransomware attacks over the first six months of 2023
- **Botnet Takedown:** The FBI and the Justice Department spearheaded a multinational operation that disrupted the massive Qakbot botnet operation that has driven millions in losses from ransomware attacks

Organizational Risk

- **Existential Threat:** The risk to organizations from ransomware attacks grows, as KNP Logistics—the UK's largest logistics provider—declared itself insolvent following a major ransomware attack that affected key systems, processes and resulted in the loss of financial information
- **Third-Party Risks:** DHS suspects sensitive security information compromised in a ransomware attack on government contractor Johnson Controls
- **Insurance Struggles:** Cyber insurance carriers are struggling to provide effective coverage in an evolving ransomware threat landscape where operations are more commonly focused on data theft and extortion and don't always include a ransomware payload
- **Mandatory SEC Reporting:** The SEC will soon be requiring publicly traded companies to disclose cyberattacks within four business days if they are deemed material to current and prospective shareholders
- **Confidence Wanes:** Fully 93% of survey respondents believe the threat of ransomware attacks increased in 2023, and 67% lacked confidence their organization could recover data and critical business processes in the event of an attack



The UK's largest logistics provider—declared itself insolvent following a major ransomware attack that affected key systems, processes and resulted in the loss of financial information.



Tooling

- **Rust Ransomware:** More ransomware variants written in Rust continue to emerge which allow for advanced evasion capabilities by disabling security tools and evading sandbox analysis
- **More Zero-Days:** Ransomware gangs are more often leveraging zero-day exploits typically seen in nation-state operations in attacks
- **Linux Threat:** More ransomware gangs are developing Linux versions, but not much attention has been paid to what this trend means for the ransomware threat landscape
- **Cloud Risk:** BlackCat/ALPHV has been observed harvesting One-Time Passwords (OTP) to bypass security tools to drop the recently released Sphynx variant to encrypt Azure cloud storage deployments
- **CIoP Rampage:** The ClOp ransomware gang's unprecedented campaign exploiting a known vulnerability in the MOVEit file sharing program drove attacks levels to a new high in July



Takeaway

Ransomware poses an existential threat to organizations of all sizes in any vertical. Ransomware attacks continue to be extremely lucrative, with ransom demands and recovery costs bleeding victim organizations for millions of dollars.

Ransomware-as-a-Service (RaaS) and other operators are implementing novel evasion techniques into their payloads specifically designed to evade or completely circumvent traditional endpoint protection solutions.

In many cases, there has been documented overlap between nation-state attack elements and those of cybercriminal ransomware gangs. Today's ransomware attacks are more complex and difficult to defend against than ever before.

Attackers are getting more efficient at exploiting vulnerabilities, and this trend is likely to continue as threat actors automate aspects of their attack sequences. We see evidence of this automation in the hundreds of organizations that have been hit by just one ransomware group exploiting one patchable vulnerability in early 2023.

This mass exploitation wave is also evidence that ransomware gangs are increasingly leveraging automation to identify and target exposed organizations who have not patched against known vulnerabilities, which is why we are seeing so many new victims.

The annual impact from ransomware attacks in the US alone is estimated to be more than \$20 billion dollars. This figure does not include additional incident response costs, tangential costs, damage to the brand, lost revenue, lost production from downed systems, and other collateral damage.

And the above figures did not even include the ransom payment, the long-term damage to an organizations' brand (loss of consumer trust), increased cyber insurance premiums, legal fees, or lost revenue which can far exceed remediation costs – and we have not even gotten to the potential impact from data exfiltration.



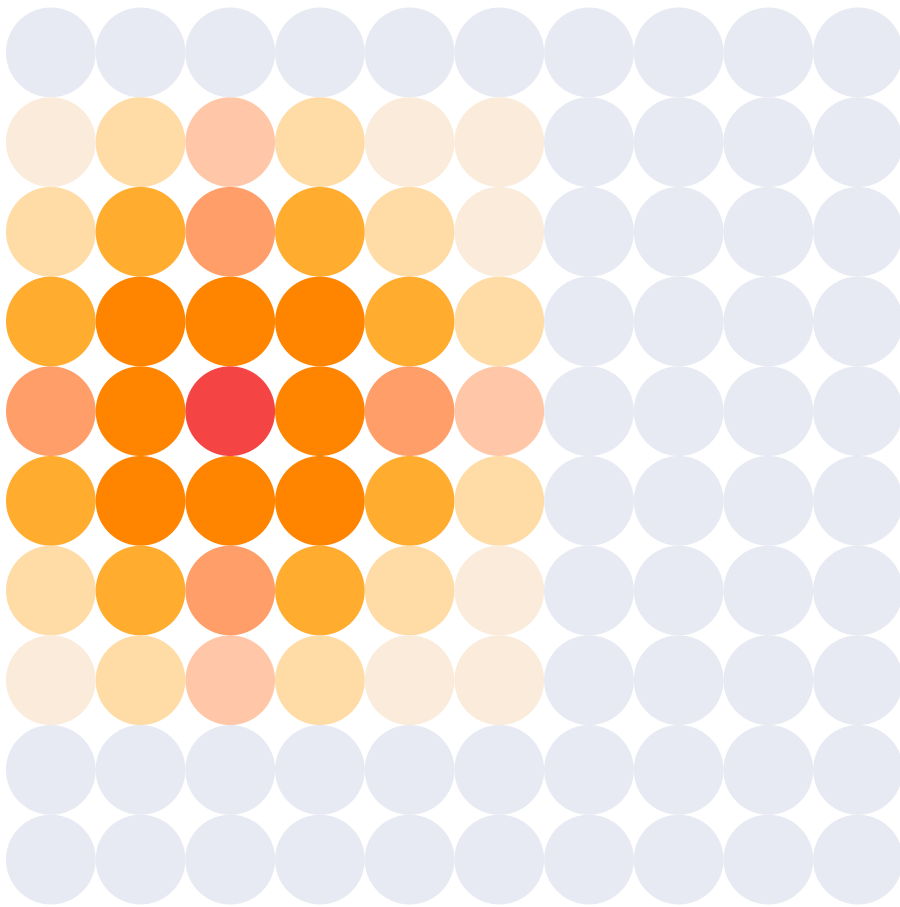
Attackers are getting more efficient at exploiting vulnerabilities, and this trend is likely to continue as threat actors automate aspects of their attack sequences.



These days, ransomware operators do not brick your systems and ask for a ransom payment, they first steal sensitive data to use as leverage by threatening to leak it publicly. For many organizations this exposure of customer data has regulatory implications and can lead to lawsuits and fines.

Additionally, sensitive data on corporate transactions, R&D, patents, etc. can end up in the attackers' hands and be sold to the highest bidder on dark web forums or end up in the hands of a competitor.

While larger organizations may be able to absorb these costs, this potentially represents an existential threat to smaller companies and their employees' jobs. If your organization is not prioritizing anti-ransomware defenses, you should really be asking why not.



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.**

