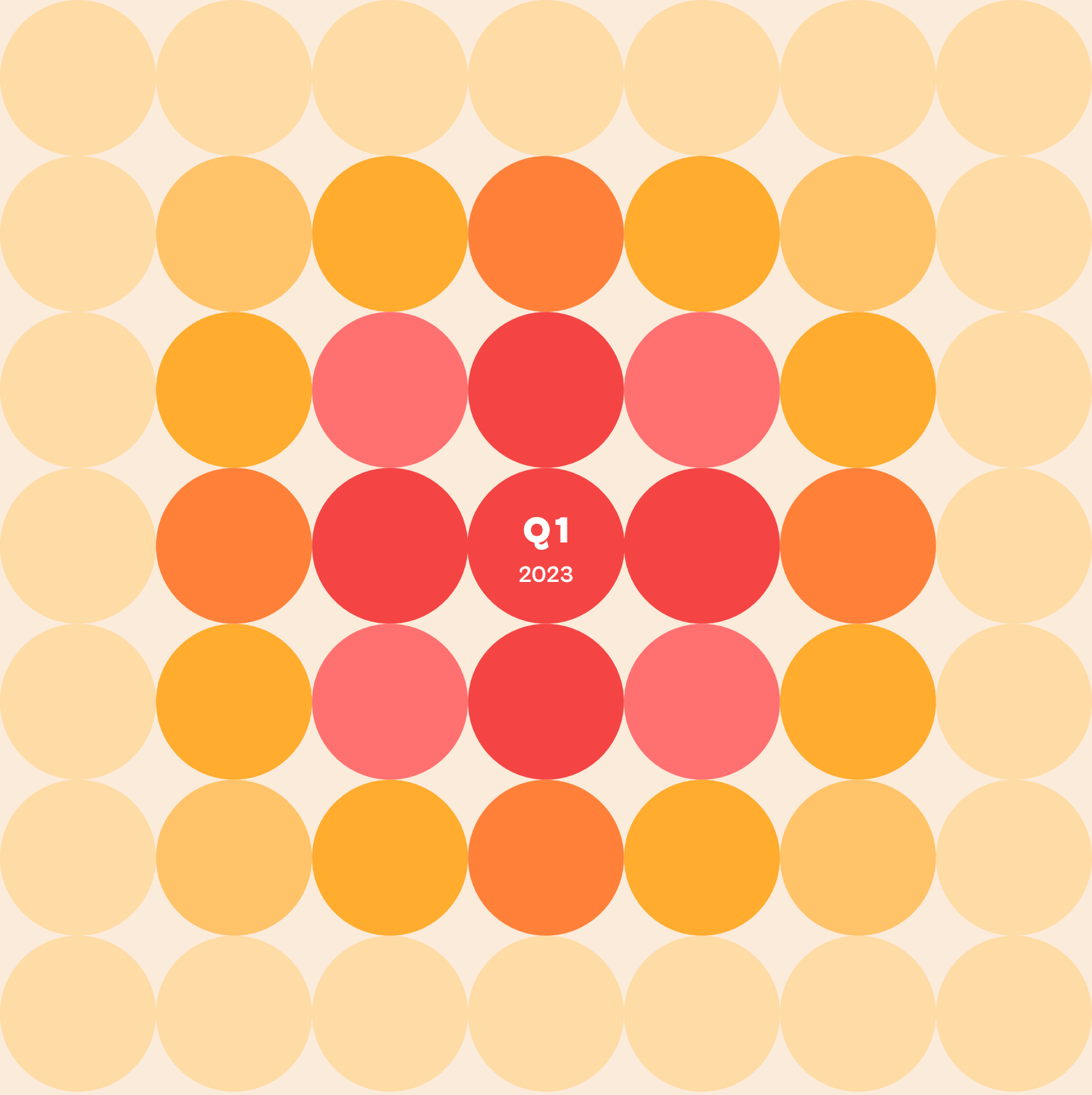


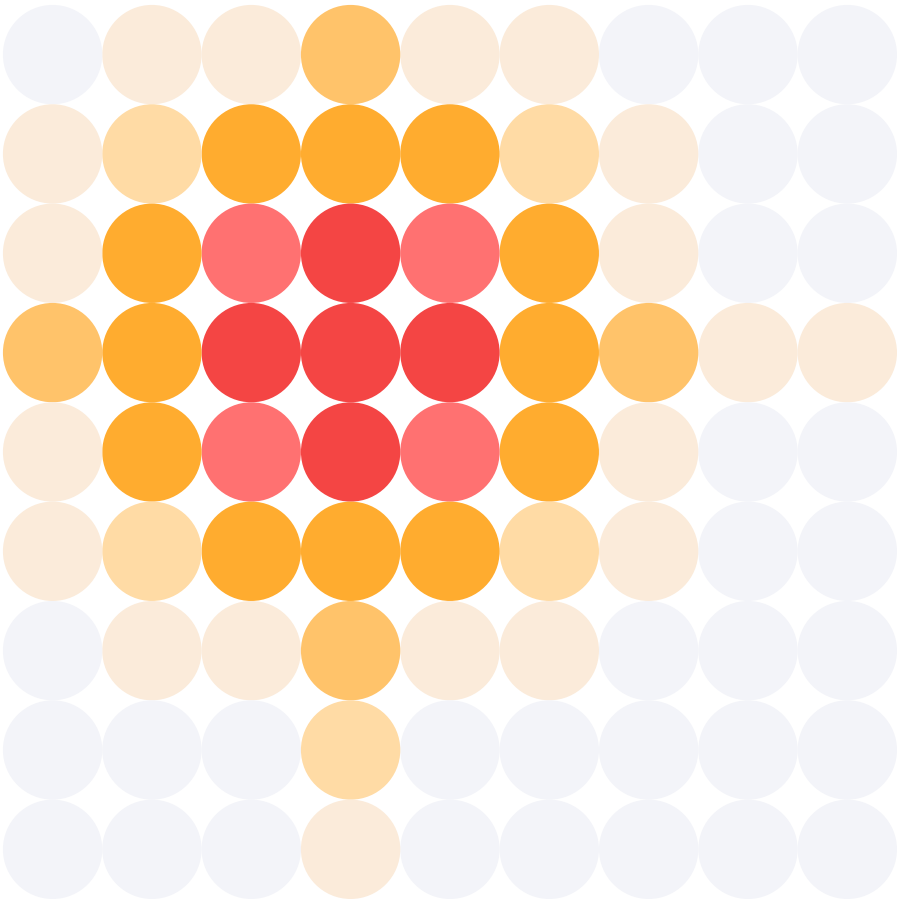
Inside Data Extortion Attacks

Power Rankings: Ransomware Malicious Quartile

Q1-2023

halcyon

Table of Contents



Inside Data Extortion Attacks

Over the course of 2022, 85% of companies were the victim of at least one ransomware attack, and 74% had experienced multiple attacks. Ransomware has fast become the greatest risk to organizations today.

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.

The players change fast in this space as RaaS groups and other ransomware operators rise and fall with law enforcement takedowns or disband and reorganize under different brands.

The Halcyon team of ransomware experts has put together this RaaS power rankings guide as a quick reference guide to the ransomware threat landscape based on data from throughout Q1- 2023 (the 2022 report can be found here).

Ransomware MQ: Evaluation Criteria Definitions

The following are the evaluation criteria for placement on the Q1-2023 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 Q1-2023 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.

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.

Over the course of 2022, 85% of companies were the victim of at least one ransomware attack, and 74% had experienced multiple attacks. Ransomware has fast become the greatest risk to organizations today.

The Q1 2023 Ransomware Malicious Quartile

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

Source: Halcyon (Q1 2023)

Frontrunners

LockBit

Performance

- **RaaS Platform:** LockBit is a RaaS that has been active since 2019 and is enabled with security tool evasion capabilities and an extremely fast encryption speed. LockBit is noted for using a triple extortion model where the victim may also be asked to purchase their sensitive information in addition to paying the ransom demand for decrypting systems. 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 one of the top attack groups in Q1 of 2023, despite being bested in sheer volume by the Cl0p ransomware gang who surged in Q1.
- **Ransom Demands:** LockBit demanded ransoms in excess of $50 million in 2022.

LockBit was by far the most active attack group in 2022 and continued to be one of the top attack groups in Q1 of 2023, despite being bested in sheer volume by the Cl0p ransomware gang who surged in Q1.

Innovation

- **RaaS Platform Development:** The group continues to improve their RaaS platform and introduced LockBit 3.0 in June of 2022. The latest version incorporates advanced anti-analysis features and is 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.
- **Targeted Industries:** LockBit tends to target larger enterprises across any industry vertical with the ability to pay high ransom demands, but also tends to favor Healthcare targets.

- **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 attack proceeds. LockBit is known to employ multiple extortion techniques including data exfiltration to compel payment.

BlackCat/ALPHV

Performance

- **RaaS Platform:** First observed in late 2021, BlackCat/ALPHV is a RaaS that employs 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 can disable security tools and evade analysis and is probably the most advanced ransomware family at present capable of employing different encryption routines, advanced self-propagation, and hinders hypervisors to 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 Q1 2023 continued to increase although it was overtaken by Cl0p in number of attacks in Q1 2023.
- **Ransom Demands:** BlackCat/ALPHV typically demands ransoms in the $400,000 to $3 million range but has exceeded $5 million.

BlackCat/ALPHV can disable security tools and evade analysis and is probably the most advanced ransomware family at present capable of employing different encryption routines, advanced self-propagation, and hinders hypervisors to for obfuscations and anti-analysis.

Innovation

- **RaaS Platform Development:** BlackCat/ALPHV is the first ransomware group using Rust, a secure programming language that offers exceptional performance for concurrent processing. The ransomware 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). It encrypts files with the ChaCha20 or the AES algorithm. BlackCat/ALPHV developers opted for faster over stronger encryption by employing several modes of intermittent encryption and employs a tool called Exmatter for data exfiltration.

- **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. The group achieved a new low by publishing private, compromising clinical photographs of breast cancer patients exfiltrated during an attack. Royal also hit several US municipalities, including an extremely disruptive attack on the City of Dallas.
- **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.

ClOp

Performance

- **RaaS Platform:** ClOp is a RaaS platform first observed in 2019. ClOp has advanced anti-analysis capabilities and anti-virtual machine analysis to prevent investigations in an emulated environment like those commonly used by security tools. ClOp is increasingly using automation to exploit known vulnerabilities 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.
- **Attack Volume:** Attacks by ClOp surged in Q1 of 2023 as the gang leveraged patchable exploits for the GoAnywhere file transfer software to compromise more than 100 victims in a matter of weeks, although it is unknown how well they were able to monetize the attacks. ClOp is likely to be leveraging automation to identify exposed organizations who have not patched against known vulnerability, which is why we are seeing so many new victims.
- **Ransom Demands:** Ransom demands vary depending on the target and average around $3 million dollars but have been reported as to be as high as $20 million. Ransom amounts are likely to continue to grow as ClOp focuses more on the exfiltration of sensitive data.

Attacks by ClOp surged in Q1 of 2023 as the gang leveraged patchable exploits for the GoAnywhere file transfer software to compromise more than 100 victims in a matter of weeks.

Innovation

- **RaaS Platform Development:** ClOp is one of just a handful of RaaS providers that have developed a Linux version, an indication that ClOp is likely actively recruiting new talent to help improve their platform and expand the scope of what and whom they can attack. ClOp's Windows version was written in C++ and encrypts files with RC4 and the encryption keys with RSA 1024-bit.
- **Targeted Industries:** ClOp had previously almost exclusively hit targets in the healthcare sector but has significantly expanded targeting to include most any organization with vulnerable GoAnywhere installations.
- **Economic Model**: ClOp runs an expansive affiliate program and exfiltrates data to be leveraged in triple extortion schemes and has significantly expanded its primary target range beyond the healthcare sector. There are indications that ClOp may be shifting to more of a pure data extortion model, but most victims still suffer the ransomware payload at this point.

Royal

Performance

- **RaaS Platform:** Royal is a RaaS that has been active since September 2022 but has quickly become one of the more concerning ransomware operations. Royal opts for partial encryption for larger files for speed and to evade detection. Royal employs a range of exploitation tactics including using Nsudo, PowerShell, PCHunter, Process Hacker, GMER, or PowerTool, and batch scripts to evade security tools; compromises cloud services; abuses legitimate TLS certificates; deploys CobaltStrike and leverages QakBot, Gozi, and Vidar malware; deletes shadow copies to thwart recovery by way of rollbacks.
- **Attack Volume:** Royal increased attack activity in late 2022 and throughout q1 2023, prompting CISA and the FBI to issue alerts to critical infrastructure providers like the healthcare, communications, and education sectors.
- **Ransom Demands:** According to CISA, Royal ransom demands range between $1 million and $11 million dollars.

Royal increased attack activity in late 2022 and throughout q1 2023, prompting CISA and the FBI to issue alerts to critical infrastructure providers like the healthcare, communications, and education sectors.

Innovation

- **RaaS Platform Development:** The Royal RaaS platform has expanded beyond targeting Windows installations to include attacks on systems running Linux and now targets ESXi servers. Evidence indicates they continue 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.
- **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.

Play

Performance

- **RaaS Platform:** Play (aka PlayCrypt) is a RaaS emerged in the summer of 2022 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). Play has similarities to Hive and Nokoyawa ransomware. Play often compromises unpatched Fortinet SSL VPN vulnerabilities to gain access. 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.
- **Attack Volume:** Play continued to increase attacks through the end of 2022 and into Q1 of 2023 and is one of the most active 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.

Play has made 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).

Innovation

- **RaaS Platform Development:** Play is an evolving RaaS platform known to leverage PowerTool to disable antivirus tools and 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 also abuses AdFind for command-line queries to collect information from a target's Active Directory. Play innovated the intermittent encryption technique for improved evasion capabilities.
- **Targeted Industries:** Play ransomware gang has mainly focused attacks in Latin America, especially Brazil, but have attack outside of that region.
- **Economic Model**: Play employs tactics similar to both Hive and Nokoyawa ransomware, and also attempts double extortion by first exfiltrating victim data with the threat to post it on their "leaks" website.

Black Basta

Performance

- **RaaS Platform:** Black Basta is a RaaS that emerged in early 2022 and is assessed by some researchers to be a revival of the Conti and REvil attack groups. The group routinely exfiltrates sensitive data from victims for double extortion. Black Basta engages in highly targeted attacks, and likely only works with a limited group of approved affiliates.
- **Attack Volume:** Considering they just emerged in the spring of 2022, Black Basta quickly became one of the most prolific attack groups moving into 2023. Black Basta was observed leveraging unique TTPs for ingress, lateral movement, data exfiltration data, and deploying ransomware payloads.
- **Ransom Demands:** Ransom demands vary depending on the targeted organization with reports that they can be as high as $2 million dollars.

Considering they just emerged in the spring of 2022, Black Basta quickly became one of the most prolific attack groups moving into 2023. Black Basta was observed leveraging unique TTPs.

Innovation

- **RaaS Platform Development:** The Black Basta RaaS continues to evolve their platform, with ransomware payloads that can infect systems running both Windows and Linux systems by exploiting vulnerabilities in VMware ESXi running on enterprise servers. Black Basta ransomware is written in C++, can target both Windows and Linux systems, encrypts data with ChaCha20 and then the encryption key is encrypted with RSA-4096 for rapid encryption of the targeted network. In some cases, Black Basta leverages malware strains like Qakbot and exploits including PrintNightmare during the infection process. Black Basta also favors abuse of insecure Remote Desktop Protocol (RDP) deployments.
- **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 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.

Contenders

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.

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.

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 though 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 termination of security software.
- **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.

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 increase through the first quarter 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 vanilla, but they do have the ability to bypass security solutions.
- **Attack Volume:** Cuba's attack volume was modest in 2022, but the pace of their attacks appears to have doubled in early 2023.
- **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 target, likely coming down significantly in negotiations.

Cuba's attack volume was modest in 2022, but the pace of their attacks appears to have doubled in early 2023.

Innovation

- **RaaS Platform Development:** Cuba is not the most sophisticated ransomware in the wild. 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.
- **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.

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. 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 shadow copies.
- **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.
- **Ransom Demands:** Medusa typically demands ransoms in the millions of dollars which can vary depending on the target organization's ability to pay.

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 shadow copies.

Innovation

- **RaaS Platform Development:** The Medusa RaaS platform (not to be confused with the operators of the earlier MedusaLocker ransomware typically compromise victim networks through 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.)
- **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, and they are not as generous with their affiliate attackers, only offering as much as 60% of the ransom if paid.

BlackByte

Performance

- **RaaS Platform:** BlackByte is a RaaS that first emerged around July of 2021, and has similarities to LockBit v2.0. with advanced obfuscation capabilities and is assessed to be Russian operated they aborts 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 the volume in 2023.
- **Ransom Demands:** Ransom demands form BlackByte vary by target but have been observed to be in the millions of dollars, with a published $2 million dollar ransom levied against the City of Augusta in 2022.

BlackByte 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.

Innovation

- **RaaS Platform Development:** The BlackByte RaaS serves up multiple variants of BlackByte ransomware have been observed in the wild, 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.
- **Targeted Industries:** U.S. and global organizations in the energy, agriculture, financial services, and public sectors.
- **Economic Model**: BlackByte exfiltrates victim data for double extortion and maintain a leaks site where expose or sell victim data. The operators even go so far as to link the auction site in the ransom note to scare victims.

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.
- **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 thousand to tens of thousands of dollars.

Innovation

- **RaaS Platform Development:** Snatch is written in Go and is somewhat unique in that the ransomware reboots in safe mode to make sure the security tools are not running. Persistence and privilege escalation are not byproducts of the reboot. Snatch abuses legitimate tools like Process Hacker, Uninstaller, IObit, BCDEDIT, PowerTool, and PsExec. Snatch deletes Volume Shadow Copies to prevent encryption rollbacks.
- **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.

Snatch is written in Go and is somewhat unique in that the ransomware reboots in safe mode to make sure it can evade security tools, delete Volume Shadow Copies to prevent rollbacks and any local Windows backups to thwart recovery.

AvosLocker

Performance

- **RaaS Platform:** AvosLocker is a RaaS 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 became more active in 2022 and are on pace to exceed those attack levels in 2023.
- **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.

AvosLocker attacks typically leverage vulnerability exploits and are adept at evading security tools by using polymorphic techniques for payloads and running in Safe Mode.

Innovation

- **RaaS Platform Development:** AvosLocker is written in C++ and has versions for Windows, Linux, and VMware ESXi. 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 encrypts the file encryption keys with RSA AES-256. AvosLocker leverages the CobaltStrike encoded PowerShell scripts.
- **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.

Emerging

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 decryptor was released. 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). BianLian leverages open-source tooling and command-line scripts to engage in credential harvesting and data exfiltration.
- **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, although still lagging far behind leaders.
- **Ransom Demands:** It is unclear how much BianLian typically requests for a ransom amount, or if they are keen to negotiate the demand down.

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.

Innovation

- **RaaS Platform Development:** BianLian successfully attacked several high-profile organizations before a free decryption tool was released to help victims recover files encrypted by ransomware. 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 has been observed deploying a custom Go-based backdoor for remote access. BianLian 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.

RansomHouse

Performance

- **RaaS Platform:** RansomHouse does not maintain a RaaS platform. RansomHouse is a data extortion group that first emerged in December of 2021. They appear to have some level of political motivation, stating they are "pro-freedom and support the free market" and claim to not work with other hacktivists or any intelligence agencies. They made headlines in 2022 for attacking chip maker 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 early 2023.
- **Ransom Demands:** Ransom demands have been reported to range between $1 million and $11 million.

RansomHouse maintains an active leaks site where they engage in "name and shame" to put pressure on victims to pay the ransom demand.

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.

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.

Innovation

- **RaaS Platform Development:** Stormous does not maintain a RaaS platform.
- **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.

Karakurt

Performance

- **RaaS Platform:** Karakurt does not maintain a RaaS platform. Karakurt practices a unique style of the ransomware model in that they do not encrypt compromised machines or files but instead focus on data exfiltration and demanding a ransom payment with the threat to leak or sell the stolen data.
- **Attack Volume:** While Karakurt maintains a lower volume of attacks than some of their peers, the attacks are extremely effective and yield high ransom payments.
- **Ransom Demands:** Karakurt ransom demands have ranged widely from range from $25,000 to $13,000,000+ with strict payment deadlines.

Karakurt practices a unique style of the ransomware model in that they do not encrypt compromised machines or files but instead focus on data exfiltration and demanding a ransom payment with the threat to leak or sell the stolen data.

Innovation

- **RaaS Platform Development:** Karakurt does not maintain a RaaS platform but has been assessed to be closely related with the defunct Conti ransomware syndicate. They have been observed deploying or abusing tools like Cobalt Strike, Mimikatz, AnyDesk and other tools to elevate privileges and move laterally within a network.
- **Targeted Industries:** Karakurt is opportunistic and does not target specific sectors, industries, or types of victims and has likely automated some target selection based on ease of compromise by way of vulnerability exploits like Log4Shell, outdated VPN appliances, or through stolen VPN and RDP credentials.
- **Economic Model**: Karakurt threat actors attempt to exfiltrate massive quantities of sensitive data and send victims a TOR link and access code where victims negotiate directly with Karakurt actors. Some victims reported Karakurt did not honor the agreement to delete victim information even after a ransom was paid.

Trigona

Performance

- **RaaS Platform:** Trigona is not a traditional RaaS. The ransomware gang emerged around June of 2022 and operators have been observed scanning for internet-exposed Microsoft SQL servers to exploit via brute-force or dictionary attacks, and they also maintain a Linux version. 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 is increasing in 2023, with more than twice the detected attacks in Q1-2023 than 2H-2022
- **Ransom Demands:** As Trigona is emerging, it is unclear how much they typically demand for a ransom.

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 sector, healthcare, banking, manufacturing, and retail sectors.
- **Economic Model**: Trigona is written in Delphi and includes a data wiper feature and has been observed to exfiltrate victim data for double extortion. Trigona hosts leaks site that public website versus being hosted on TOR.

Trigona is written in Delphi and includes a data wiper feature and has been observed to exfiltrate victim data for double extortion.

HardBit

Performance

- **RaaS Platform:** HardBit is a RaaS was first observed in October of 2022 and quickly released version 2.0 of their ransomware in November. The HardBit ransomware gang has introduced a new tactic – the effectiveness of which is yet to be seen – where they instruct victims to provide details of their cyber insurance coverage to set the ransom demand.
- **Attack Volume:** Attack volume escalated in late 2022 and continued to increase in Q1-2023.
- **Ransom Demands:** HardBit seeks to determine the level of cyber insurance coverage to set the ransom amount, and typically engages in negotiation with the victim to set the final demand.

Innovation

- **RaaS Platform Development:** HardBit is capable of evading security tools and deletes Volume Shadow Copy Service (VSS) leveraging the Service Control Manager as well as deleting the Windows backup utility catalog to thwart encryption rollbacks. HardBit established persistence and is re-executed when the infected system is rebooted.
- **Targeted Industries:** HardBit appears to be opportunistic in their targeting.
- **Economic Model**: HardBit engages in data exfiltration but there is no evidence yet that they use double extortion tactics on victims as they do not maintain a leaks site, and it is possible they may be selling the information.

Mallox (TargetCompany)

Performance

- **RaaS Platform:** TargetCompany 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 continues to increase in Q1-2023.
- **Ransom Demands:** There is not much info on how much TargetCompany demands for ransoms, but they appear to be relatively low compared to leading threat actors (in the thousands of dollars), but they are a newer group who has only recently started to recruit affiliates and they are constantly improving their malware, so we expect ransom demands to increase.

TargetCompany 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.

Innovation

- **RaaS Platform Development:** TargetCompany 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. TargetCompany has been observed using

advanced TTPs like DLL hijacking that is not common to ransomware attacks. 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 infection where earlier variants targeted vulnerable MS SQL instances. Target only recently appears to be recruiting affiliates for a RaaS platform, so this group is one to watch.

- **Targeted Industries:** Mallox has hit some critical infrastructure IT providers, but appears to be opportunistic, hitting targets mostly located in the US and India.
- **Economic Model**: It is unclear if TargetCompany engages in data exfiltration for double extortion, but they likely will follow other attackers in using this tactic as they develop their RaaS platform.

Diminishing

Lorenz

Performance

- **RaaS Platform:** Lorenz does not maintain a RaaS. They first emerged in 2020 and are assessed to be related to the ThunderCrypt and sZ40 ransomware. Lorenz was notable for the use of backdoors implanted in victim networks to maintain persistence. Lorenz has also been observed acting as an Initial Access Broker (IAB) selling access to victim networks.
- **Attack Volume:** Attack volume is modest compared to leading ransomware threat actors, having increased in 2022 but has significantly decreased in Q1-2023.
- **Ransom Demands:** Lorenz typically demands ransoms in the $500,000 to $700,000 range but have been rumored to exceed $1 million in some cases.

Lorenz was notable for the use of backdoors implanted in victim networks to maintain persistence. Lorenz has also been observed acting as an Initial Access Broker.

Innovation

- **RaaS Platform Development:** Lorenz targeted vulnerabilities in Linux-based MiTel MiVoice Connect to allow remote code execution. Lorenz uses AES encryption with an embedded RSA Public Key and leverages MS BitLocker apparatus by executing on the domain controller. Lorenz uses a reverse shell and abuses a tool called Chisel for tunneling and other living-off-the-land techniques (LotL) for pivoting on the targeted network.
- **Targeted Industries:** Lorenz is opportunistic and is assessed to target based on a victim's ability to pay large ransom demands. Most victims are in the US, China, or Mexico.
- **Economic Model**: Lorenz engages in data exfiltration for double extortion and maintains a leaks site where they threaten to sell victim data if the ransom is not paid. A decryptor was made available in late 2021.

RagnarLocker

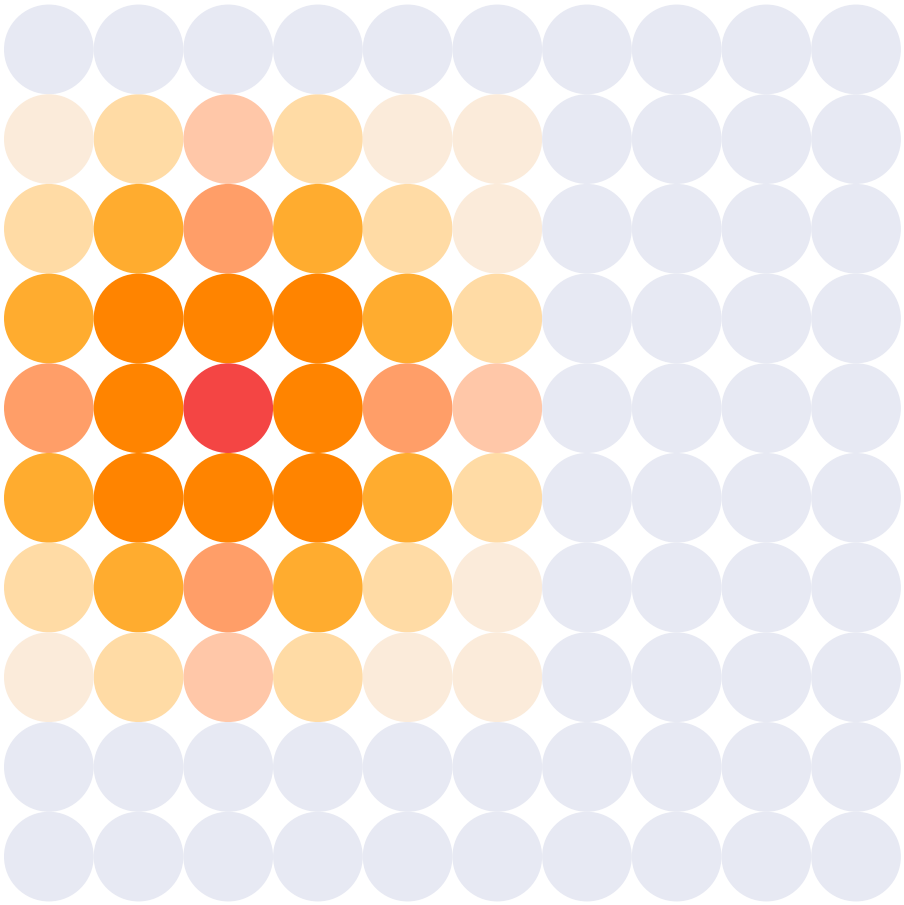
Performance

- **RaaS Platform:** RagnarLocker is not a traditional RaaS. They first emerged in December of 2019 and were assessed to be related to or working in cooperation with Maze and MountLocker operators. RagnarLocker typically compromises victim networks through vulnerable Remote Desktop Protocol (RDP) software, a common ransomware technique.
- **Attack Volume:** RagnarLocker was increasingly active in 2022, but attack volume has dripped off significantly in Q1-2023.
- **Ransom Demands:** RagnarLocker ransom demands vary and have been observed to exceed $10 million.

RagnarLocker ransom demands vary and have been observed to exceed $10 million.

Innovation

- **RaaS Platform Development:** Ragnar Locker has both Windows and Linux versions that actively detect and bypass security tools on the targeted network, as well as scanning for virtual-based machines, and any remote management solutions. IT encrypts with a custom Salsa20 algorithm and has been observed terminating services that managed service providers (MSPs) to remotely protect and manage customer networks.
- **Targeted Industries:** RagnarLocker is opportunistic and is assessed to target based on a victim's ability to pay large ransom demands, focusing on the manufacturing, energy, financial services, government, and information technology sectors.
- **Economic Model**: RagnarLocker engages in data exfiltration for double extortion and maintains a leaks site called "Wall of Shame." RagnarLocker will delete VSS Shadow Copies to thwart encryption rollback.



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**.

halcyon