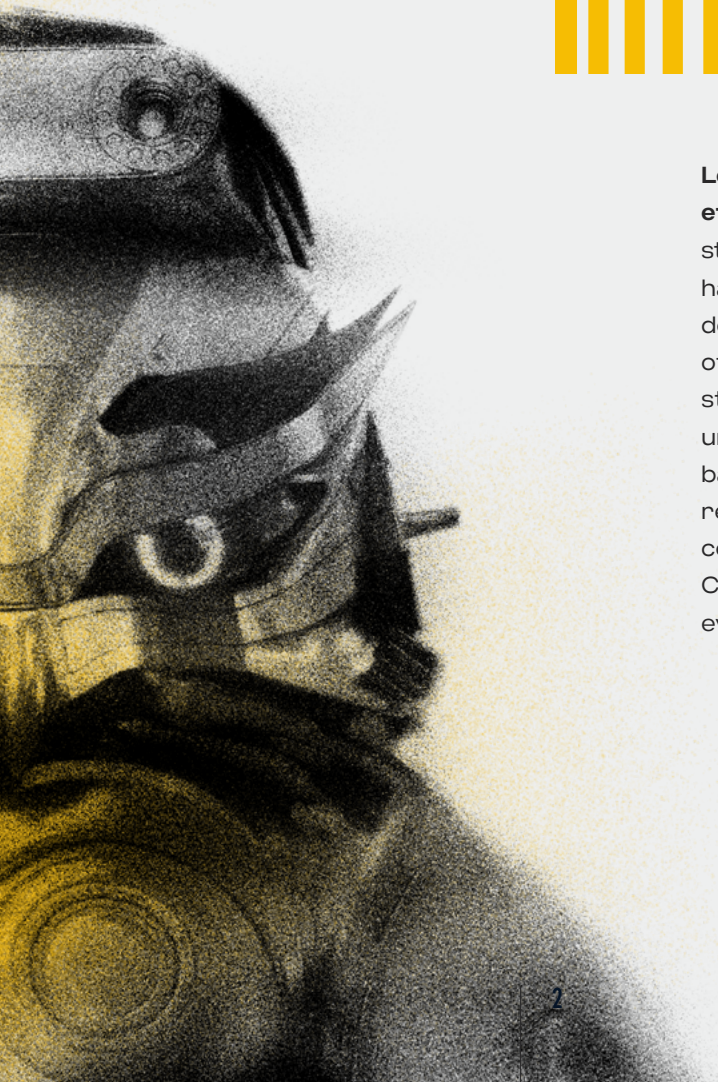
cybereason

Cybereason Vs Ransomware

PREDICTIVE PROTECTION THAT REMAINS UNDEFEATED BY RANSOMWARE

Introduction



Legacy prevention strategies are proving less effective against the threat of modern, multi-stage ransomware. NextGen ransomware has evolved to better evade standard defenses and when deployed as a component of a targeted RansomOps attack, adversaries stand a high chance of success against underprepared environments. A behavior-based approach to prevention, detection and response is required for success against complex ransomware attacks, and Cybereason remains undefeated against every known ransomware family.

Cybereason allows Defenders to detect the preliminary stages of a ransomware attack, fully analyze the scope and scale of the operation, and prevent the execution of the malicious ransomware payload. Learn more about how Cybereason Predictive Ransomware Protection stops any ransomware strain - even those never before seen.

According to the Verizon Data Breach Investigations report, ransomware attacks are on the rise and this medium will be a significant battleground where defenders lock horns with cyber adversaries.

The Cybereason Anti-Ransomware solution applies a **multi-layered approach** that combines intelligence-based, deception, behavioral analytics and machine learning algorithms

Ransomware attacks can put organizations and lives at risk, as witnessed with the continuous onslaught of attacks against the healthcare industry, research organizations, telecommunication centers, financial institutions, critical infrastructure, the public sector, and companies across every industry vertical.

Some ransomware families can spawn variants that hide in virtual machines, eluding traditional defense techniques. Advances in machine learning detection of ransomware can be effective, but this approach also introduces high-compute processes that consume system resources and negatively impact performance and user experience.

Attackers have found success with ransomware because it can evade traditional alert-centric defenses. In the past, savvy organizations could find comfort in assuring their critical data is backed up off-site so it can be easily restored in the event of a ransomware attack.

Adversaries adapted by introducing a technique we call "double extortion" where the victim's data is not just encrypted and held for ransom, it is also exfiltrated with the threat of being made public should the victim refuse to pay the ransom, effectively undermining the data backup strategy.

The Cybereason Anti-Ransomware solution applies a multi-layered approach that combines intelligence-based deception, behavioral analytics, and machine learning algorithms that reliably block ransomware before any data can be encrypted or compromised, including in attacks leveraging previously unknown, fileless and MBR-based ransomware.

The following provides just a small sample of some of the most nefarious ransomware families plaguing organizations around the world and a demonstration of how Cybereason detects and disrupts the attacks before they escalate to costly and disruptive events.

Cybereason vs. Quantum Locker Ransomware

Quantum Locker is a ransomware strain that was first discovered in July 2021. Since then, the ransomware was observed used in fast ransomware attacks, in some cases even Time-to-Ransom (TTR) of less than 4 hours, leaving defenders little time to react.

The Quantum ransomware is another rebranding of the notorious MountLocker ransomware, which launched back in September 2020. Since then, the ransomware gang has rebranded its operation to various names, including AstroLocker, XingLocker, and now in its current phase, the Quantum Locker.

KEY FINDINGS

Time-to-Ransom (TTR) of less than 4 hours	From initial infection to encryption takes even less than 4 hours, leaving a very short window for defenders to successfully defend against the threat.
High Severity	The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
Human Operated Attack	Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-developed RansomOps attack.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the Quantum Locker ransomware.

WATCH THE VIDEO

Cybereason vs. BlackCat Ransomware

The Cybereason Nocturnus team has been tracking the BlackCat Ransomware (aka ALPHV) since it first emerged in November 2021 BlackCat has been called "2021's most sophisticated ransomware." BlackCat ransomware gained notoriety quickly leaving a trail of destruction behind it, among its recent victims are German oil companies, an Italian luxury fashion brand and a Swiss Aviation company.

Since its recent emergence, BlackCat has attacked various industries, including telecommunication, commercial services, insurance, retail, machinery, pharmaceuticals, transportation, and construction industries. Among the affected regions are Germany, France, Spain, the Philippines, and the Netherlands, with the most victims being located in the US. The operators of the ransomware appear to be from Russian speaking regions. Like many others, BlackCat uses a RaaS model (Ransomware-as-a-service). Affiliates of BlackCat are offered between 80-90% of the ransom payment, and once approved, are given access to a control panel that manages access.

KEY FINDINGS

Sophisticated Ransomware	BlackCat has been called "2021's most sophisticated ransomware
High Severity	The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
Developed in Rust	BlackCat was developed in rust which is unusual for ransomware.
Triple Extortion	The BlackCat operators used double extortion and sometimes triple extortion to make victims pay the ransom.
Shared Infrastructure with LockBit	BlackCat has shared infrastructure, and used similar tools and naming conventions as the LockBit ransomware.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the BlackCat ransomware.

WATCH THE VIDEO

Cybereason vs. Lorenz Ransomware

Lorenz is a ransomware strain observed first in February of 2021, and is believed to be a rebranding of the ".sZ40" ransomware that was discovered in October 2020. Lorenz targets organizations worldwide with customized attacks demanding hundreds of thousands of dollars, and even millions in ransom fee.

The group is targeting victims mostly in English-speaking countries, and according to their website, the group has published stolen data from more than 20 victims, although the estimated number of successful attacks is believed to be higher.

According to researchers, Lorenz appears to be the same as ThunderCrypt ransomware observed in May 2017. However, it's not clear if Lorenz was created by the same group or if the group purchased the source code of ThunderCrypt and created its own variant.

Shortly after Lorenz was discovered, the group faced a temporary problem after researchers published a free decryptor (download here). The decryptor was released by the project No More Ransom, a joint project by law enforcement agencies including Europol's European Cybercrime Center.

KEY FINDINGS

Ever Evolving Ransomware	The Lorenz group keeps changing the ransomware capabilities and behavior frequently, making it customized to their victims.
High Severity	The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
Human Operated Attack	Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-developed RansomOps attack.
Interesting Way of Leaking Data	The Lorenz group has a few steps in their leaking data process. From selling it to other threat actors, releasing password-protected RAR archives containing the victim's data, and also selling DBs and access to internal networks.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents Lorenz ransomware.

WATCH THE VIDEO

Cybereason vs. REvil Ransomware

REvil (aka Sodinokibi, Sodin), is a notoriously aggressive and highly evasive threat. Attacks attributed to the REvil gang include a March 2021 attack against Taiwanese multinational electronics corporation Acer where the assailants demanded a record-breaking $50 million ransom. In April, the REvil gang attempted to extort Apple following an attack against one of the tech giant's business partners with threats to increase the ransom demand to $100 million.

Reports indicate that the REvil gang's supply chain attack exploited the Kaseya VSA remote management service to propagate the ransomware to multiple targets. REvil is the same threat actor who hit meatpacking giant JBS with a ransomware attack at the beginning of June, shutting down a good portion of the company's production capabilities.

KEY FINDINGS

Ever Evolving Ransomware	The REvil ransomware gang have been connected to the authors of the prolific GrandCrab ransomware, which was retired in June 2019, but was responsible for 40% of all ransomware infections globally. GandCrab sets a good example for just how impactful REvil may become.
High Severity	The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
Double Extortion	After the ransomware encrypts the target's data and issues the ransom demand for payment in exchange for the decryption key, the threat actors make the additional threat of publishing the exfiltrated data online should the target refuse to make the ransom payment.
Security Bypass	Early iterations of the REvil/Sodinokibi ransomware targeted an AV made by the South Korean security vendor Ahnlab in the infected machine in order to inject its malicious payload to the trusted AV vendor.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents REvil/Sodinokibi ransomware.

WATCH THE VIDEO

Cybereason vs. LockBit2.0 Ransomware

The Cybereason Nocturnus team has been tracking the LockBit ransomware since it first emerged in September 2019 as a ransomware-as-a-service (RaaS). Following the rise of the new LockBit2.0 and the latest events, including the attack against the global IT company Accenture.

There are major improvements in the new version of LockBit2.0, and addition of new features including port scanner, using wake-on-lan to switch on turned off machines, print-out using network printers and automatic distribution in the domain, which puts corporations and small businesses in great danger. LockBit2.0 is "the fastest encryption software all over the world," and they are even sharing a test sample on their website, so everyone who "has any doubts" can check their claim.

KEY FINDINGS

Emerging Threat	In a short amount of time, Lockbit2.0 ransomware caused great damage and made headlines across the world, with over 40 known victims on their website.
High Severity	The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
Group Policy Update to Encrypt Network	LockBit2.0 is the first ransomware to automate the process of executing the ransomware on the entire network with a single command.
Triple Extortion	The group claimed to attack Accenture using DDOS attacks daily. They are also known for exfiltrating data and threatening to make it public if a ransomware demand is not met.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the LockBit2.0 ransomware.

WATCH THE VIDEO

Cybereason vs. Avaddon Ransomware

Avaddon Ransomware has been active since June 2020 and is operating with the Ransomware-as-a-Service (RaaS) and double extortion models, targeting sectors such as healthcare. Avaddon is distributed via malspam campaigns, where the victim is lured to download the malware loader.

The Avaddon Ransomware was discovered in June 2020 and remains a prominent threat. Their first infection vector was spreading phishing emails that lured victims with a supposed image of them, sending it as an email attachment. This in fact was a double extension JavaScript downloader that downloads and executes the Avaddon Ransomware.

KEY FINDINGS

Classic Luring Technique	The Lorenz group keeps changing the ransomware capabilities and behavior frequently, making it customized to their victims.
Active Threat Group	The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
Hybrid Encryption	Avaddon uses a popular hybrid encryption technique by combining AES and RSA keys, typical of other modern ransomware.
Use of Windows Tools	Various legitimate Windows tools are used to delete system backups and shadow copies prior to encryption of the targeted machine.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the Avaddon ransomware.

WATCH THE VIDEO

Cybereason vs. Prometheus Ransomware

Prometheus is a relatively new variant of the Thanos ransomware that is operated independently by the Prometheus group, and was first observed in February of 2021. In just a short period of time, Prometheus caused a lot of damage, and breached over 40 companies.

Like other prominent ransomware groups, such as the DarkSide group, Prometheus follows the RaaS business model and operates as a professional enterprise where it refers to its victims as "customers," and communicates with them using a customer service ticketing system. In addition, Prometheus follows the double extortion trend and hosts a leak site, where it has a "hall of shame" for victims and posts stolen data for sale.

KEY FINDINGS

High Severity	The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
Human Operated Attack	Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-developed attack operation.
Shared Builder	The Prometheus group, as well as other threat actors, used the Thanos builder to build and customize their ransomware.
Group of REvil	The Prometheus ransomware group is branding themselves as part of the REvil group, probably in an attempt to piggyback on the fame of one of the most infamous and successful ransomware groups
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the Prometheus ransomware.

WATCH THE VIDEO

Cybereason vs. Ransom EXX Ransomware

The RansomEXX family, also known as Defray777 and Ransom X, runs as a solely in-memory payload that is not dropped to disk, making it highly evasive. RansomEXX was involved in three major attacks in 2020 against Texas TxDOT in May, against Konica Minolta at the end of July, and against Brazil's court system at the beginning of November.

In addition, last December RansomEXX operators published stolen credentials from Embraer, one of the largest aircraft makers in the world, on its own leaks website as part of the ongoing double extortion trend.

In mid 2020, a Linux variant of RansomEXX emerged. This variant, despite sharing similarities with the Windows variant, is simpler than its predecessor and lacks many features such as disabling security software and command and control communication. There are decryptors for both variants, and the threat actors send paying victims a private key to decode their files.

KEY FINDINGS

Human-Operated Targeted Attacks	RansomEXX is being used as part of a multi-staged human-operated attacks targeting various government-related entities and tech companies. It is being delivered as a secondary payload after the initial compromise of the targeted network.
Disables Security Products	The Windows variant has a functionality that was seen before in other ransomware, disabling various security products for a smooth execution on the infected machine.
Multi-Platform	RansomEXX started solely as a Windows variant, but later a Linux variant was added to the arsenal, sharing similarities with its predecessor.
Fileless Ransomware	RansomEXX is usually delivered as a secondary in-memory payload without ever touching the disk, which makes it harder to detect.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the RansomEXX ransomware.

WATCH THE VIDEO

Cybereason vs. Conti Ransomware

Conti is a relatively new player in the ransomware field. Since first emerging in May 2020, the ransomware operators (aka. the Conti Gang) claim to have over 150 successful attacks, which comes down to millions of dollars in extortion fees. Similar to other ransomware that emerged recently, the Conti gang follows the growing trend of double extortion. They steal sensitive files and information from their victims, and later use it to extort the victims by threatening to publish the data unless the ransom is paid.

Conti is a very destructive threat. Besides the double extortion that puts information and reputation at risk, the Conti operators equip it with a spreading capability, which means that Conti not only encrypts the files on the infected host but also spreads via SMB and encrypts files on different hosts, potentially compromising the entire network. The rapid encryption routine takes just a few seconds to minutes due to its use of multithreading, which also makes it very difficult to stop once the encryption routine starts.

Another major factor that contributes to the popularity of Conti is the collaboration with the TrickBot Gang. Conti is sold as a Ransomware-as-a-Service in underground forums to exclusive buyers and partners such as the TrickBot gang, which replaced Ryuk and adopted Conti as their new ransomware of choice.

In addition to the sophisticated capabilities and the collaboration with the TrickBot gang, the increased number of Conti attacks against big companies such as Advantech, which was extorted for $13.8M, and other attacks against big North American based companies, contributed to Conti making its way into the news this year. With a rapid development cycle that keeps the malware up-to-date and equipped with advanced capabilities, along with the promotion done by the TrickBot gang, it is no wonder why Conti is referred to as the successor of Ryuk.

KEY FINDINGS

Low-and-Slow	Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-fledged hacking operation.
Rapid Development Cycle	In just a few months, the Conti gang has released 3 versions of the ransomware, improving the malware each version.
Spreading across the network	Conti is not satisfied with causing damage to just the infected machine. Instead, it spreads in the network via SMB and encrypts files on remote machines as well.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the Conti ransomware.

WATCH THE VIDEO

Cybereason vs. ClOp Ransomware

The Cybereason Nocturnus team has been tracking the activity of the ClOp ransomware, a variant of CryptoMix ransomware. The name "clop" comes from Russian or Bulgarian, and means "bug."

In 2019, the TA505 threat actor started delivering ClOp as their final payload. TA505 is a well-known sophisticated cybercrime threat actor, attacking various sectors for financial gain. In 2019, the TA505 group changed their main strategy into encrypting assets in a corporate network and demanding a Bitcoin ransom for the decryption key.

More recently, ClOp attacked AG, a large German software company. They breached AG's internal network and demanded more than $20 million ransom. In another case, the group attacked a South Korean retailer, demanding a $40 million ransom and threatening to leak two million cards.

KEY FINDINGS

Evolving Threat	TA505 has evolved its attack tactics, delivering ClOp ransomware as the final payload on as many systems as possible in order to pressure the victim to pay the ransom. Nonpaying ClOp victims' data is being published on the ClOp leaks site.
Multi-Staged Attack	Before deploying ClOp, two prior payloads are deployed to allow the attackers to move laterally within the compromised network before downloading and deploying the ClOp ransomware.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the ClOp ransomware.

WATCH THE VIDEO

Cybereason vs. Ryuk Ransomware

Ryuk ransomware has been infecting victims since around 2018, and is believed to be based on the source code of Hermes ransomware, which was sold on an internet hacking forum back in 2017. Since its inception, Ryuk has been used to target large organizations to great effect, having accumulated as much as $61.26 million (as of Feb 2020) in ransom payments according to federal investigations.

In March of 2020, the threat actors temporarily stopped deploying Ryuk, and a new ransomware called Conti was introduced. Researchers found that the code bases were similar, implying this could be the successor to Ryuk. However, in September 2020 Ryuk made a swift return, and with Conti infections still happening alongside it, the evidence pointed to Conti not being a successor so much as a new, different strain of malware.

Shortly after the start of Ryuk's hiatus, a new malware called BazarLoader was observed being delivered by TrickBot. Currently, evidence suggests that Ryuk, Conti and BazarLoader are used by the same threat actor. Ryuk ransomware is most often seen as the final payload in a larger targeted attack against a corporation, and since its return in September, it has been mainly via TrickBot or BazarLoader infections.

KEY FINDINGS

Evolving Threat	One of the reasons behind Ryuk's unfortunate success is the threat actor's capacity to evolve their tactics, techniques and procedures (TTPs).
Multi-Staged Attack	Since early 2019, the TrickBot information stealer trojan has been a more or less constant partner-in-crime, with many campaigns also including other malware, frameworks and tools. Some early campaigns utilized the EMPIRE framework, and in later campaigns Cybereason observed Emotet downloading TrickBot deploying Ryuk.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents Ryuk ransomware.

WATCH THE VIDEO

Cybereason vs. Egregor Ransomware

Egregor is a newly identified ransomware variant that was first discovered in September 2020, and has recently been identified in several sophisticated attacks on organizations worldwide, including the gaming industry giants Crytek and Ubisoft.

Similar to the Maze ransomware, Egregor's operators run an extortion ransomware operation, where the data is stolen and stored on the attacker's servers before it is encrypted on the users machine. Egregor is probably the most aggressive ransomware family in terms of negotiation with the victims. Its operators give only 72 hours to contact them. If the ransom is not paid, the data is released to the public via the attacker's website, "Egregor News."

Egregor is believed to be a relative of another ransomware called Sekhmet that emerged in March 2020, which shares a lot of similarities with Egregor and also some similarities with Maze.

Egregor is still quite a mystery when it comes to how it is delivered in the attack and who is behind the campaign. Not much is known at this point, but speculation includes theories that Egregor is the "heir to Maze," after that threat actor announced they were shutting down their operations in late October 2020. This assumption is supported by the close similarities between the two - and of course the timing.

KEY FINDINGS

Emerging Threat	In a short amount of time, Egregor ransomware caused great damage and made headlines across the world.
Multi-Staged Attack	Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-fledged hacking operation.
Infection Vector via Commodity Malware	The infection seems to start with commodity malware. Based on a preliminary reconnaissance of data sent to the C2 servers, the operators can choose to escalate to an interactive hacking operation, which ultimately causes a mass ransomware infection.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the Egregor ransomware.

WATCH THE VIDEO

Cybereason vs. MedusaLocker Ransomware

MedusaLocker ransomware first emerged in September 2019, infecting and encrypting Windows machines around the world. There have been reports of MedusaLocker attacks across multiple industries, especially the healthcare industry which suffered a great deal of ransomware attacks during the COVID-19 pandemic.

To maximize the chances of successful encryption of the files on the compromised machine, MedusaLocker restarts the machine in safe mode before execution. This method is used to avoid security tools that might not run when the computer starts in safe mode.

To make it even more dangerous, MedusaLocker uses a combination of AES and RSA-2048, making the procedure of brute forcing the encryption practically impossible. Recently, there have been reports stating that AKO, a variant of MedusaLocker, added an element of double extortion, threatening to release stolen files publicly.

KEY FINDINGS

Encrypting Mapped Drives	MedusaLocker encrypts shared network drives of adjacent machines on the network.
Selective Encryption	MedusaLocker avoids encrypting executable files, most likely to avoid rendering the targeted system unusable for paying the ransom.
Double Extortion	The ransom note left by new MedusaLocker variants contains threats to publicly reveal stolen data if payments are not made.
Detected and Prevented	The AI-Driven Cybereason Defense Platform fully detects and prevents the MedusaLocker ransomware.

WATCH THE VIDEO

Contact a Cybereason Defender to Learn More

The Cybereason team is available to provide additional details on how our industry-leading solutions can deliver unparalleled prevention, detection and response capabilities - most notably the anti-ransomware capabilities modern organizations require to assure they do not fall prey to costly and disruptive ransomware attacks.

The Cybereason team is here to provide more information on products and services, contain an ongoing incident and more.

Talk to a Cybereason Defender today.

ABOUT CYBEREASON

Cybereason is the champion for today's cyber defenders providing future-ready attack protection that unifies security from the endpoint, to across the enterprise. The Cybereason XDR Platform combines the industry's top-rated detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a MalOp (malicious operation). The result: defenders can end cyber attacks from endpoints to everywhere.