cybereason | EBOOK

CYBEREASON VS RANSOMWARE

Undefeated in the Fight Against Ransomware

TABLE OF CONTENTS

INTRO

Traditional prevention strategies are proving less effective against the threat of modern, multi-stage ransomware. Next-gen ransomware has evolved to better evade standard defenses and when deployed as a component of a targeted 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 ransomware attacks. **Cybereason delivers fearless ransomware protection: confident, comprehensive, low-touch protection delivered by a field proven solution that security teams can rely on.**

Unfortunately - ransomware attacks are here to stay. This new tactic of cyber adversaries is quickly becoming a go-to method to create digital compromise, and according to the Verizon Data Breach Investigations report, "ransomware is a problem that's continuing to get bigger."

As defenders lock horns with attackers, a defense strategy for modern, multistage ransomware attacks will be a critical dynamic to address in 2021. (source)

Ransomware is prevalent.

Cybercrime has increased 600% since the start of the global pandemic, with ransomware being a preferred weapon. Ransomware kits are widely available on the dark web and have a lower bar of entry for use and deployment by malicious actors. Since 2016, at least 4,000 ransomware attacks have taken according to the FBI.

Ransomware is multistage.

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 device performance and user experience.

Ransomware has consequences.

Ransomware attacks put organizations and lives at risk with attacks against hospitals, research organizations working on COVID-19 vaccines, telecommunication centers, financial institutions, public sector agencies and private sector companies across every industry vertical. Ransomware comes with both tangible and intangible costs.

Cybereason reverses the adversary advantage and fully protects against modern, multistage ransomware attacks.

WATCH THE VIDEO

Cybereason vs REvil Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents REvil ransomware.

REvil (aka Sodinokibi, Sodin), 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 assainlants 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.

- **Connection to GandCrab 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.

WATCH THE VIDEO

Cybereason vs LockBit2.0 Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents 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 featuresincluding 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 corporates 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.

- **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 claims to attack Accenture, one of its victims, using DDOS attacks daily in addition to being known for exfiltrating data with threat to make public if a ransomware demand is not met.

WATCH THE VIDEO

Cybereason vs Avaddon Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents Avaddon ransomware.

Avaddon Ransomware 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 being lured to download the malware loader.

The Avaddon Ransomware was discovered in June 2020, and remains a prominent threat ever since. Their first infection vector was spreading phishing emails that were luring victims with a supposedly 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.

- **Classic Luring Technique:** To lure the victim, the Avaddon loader is sent as a double extension attachment in phishing emails, tricking the victim into thinking an image of them was leaked online and sent to them.
- **Active Threat Group:** Since its discovery in June 2020, Avaddon is still an active threat, marking almost a year of activity.
- **Hybrid Encryption:** Avaddon uses a popular hybrid encryption technique by combining AES and RSA keys, typical to 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.

WATCH THE VIDEO

Cybereason vs Prometheus Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents 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.

- **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:** Prometheus ransomware 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.

WATCH THE VIDEO

Cybereason vs DarkSide Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents DarkSide ransomware.

Darkside Ransomware is a relatively new ransomware strain that made its first appearance in August 2020 and made headlines in May when it disrupted operations of the Colonial Pipeline. DarkSide follows the RaaS (ransomware-as-a-service) model, and according to the group, it is equipped with the fastest encryption speed on the market, and even includes Windows and Linux versions.

In an effort to grow and expand their operations, the group has started an affiliate program for potential users. Like many other ransomware variants, DarkSide follows the double extortion trend, which means the threat actors not only encrypt the user's data, but first exfiltrate the data and threaten to make it public if the ransom demand is not paid.

- **Emerging Threat:** In a short amount of time, the DarkSide group has established a reputation for being a very "professional" and "organized" group that has potentially generated millions of dollars in profits from the ransomware.
- **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.
- **Aiming Towards the DC:** The DarkSide group is targeting domain controllers (DCs), which puts targets and the whole network environment at great risk.
- **Detected and Prevented:** The Cybereason Defense Platform fully detects and prevents the DarkSide ransomware.

WATCH THE VIDEO

Cybereason vs. RansomEXX

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents the RansomEXX ransomware.

RansomEXX Ransomware, 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 of 2020, against Konica Minolta in the end of July, and against Brazil's court system in the beginning of November.

- **Component of Human-Operated Attacks:** RansomEXX is being used as a part of multi-staged human-operated attacks targeting various government related entities and tech companies. It is being delivered as a secondary payload after 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.

WATCH THE VIDEO

Cybereason vs Conti Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents Conti ransomware.

Conti Ransomware is a relatively new variant that has proven alarmingly effective. Since first emerging in May 2020, the Conti ransomware operators claim over 150 successful attacks, which equates to millions of dollars in extortion fees. Similar to other ransomware variants that have 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.

- **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 operators have released three versions of the ransomware, improving the malware through each iteration.
- **Spreads rapidly 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.

WATCH THE VIDEO

Cybereason vs Clop Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents Clop ransomware.

Clop Ransomware is a variant of CryptoMix ransomware, with the name "clop" coming from the Russian or Bulgarian word for "bug". In 2019, the TA505 threat actor started delivering Clop as their final payload. TA505 is a well-known and 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.

- **Clop is an evolving threat.** TA505 have evolved their 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 - non-paying 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.

WATCH THE VIDEO

Cybereason vs Ryuk Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents Ryuk ransomware.

In 2020, Ryuk Ransomware was the most profitable strain, making it a likely favorite for attacks in 2021. 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.

Ryuk ransomware is most often seen as the final payload in a larger targeted attack against a corporation.

- **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).
- **Multiple Payloads:** 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.

WATCH THE VIDEO

Cybereason vs Egregor Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents Egregor ransomware.

Egregor Ransomware is a newly identified variant that was first discovered in September of 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 one of the most aggressive ransomware families in terms of negotiation with the victims, demonstrated by the operator's demands to initiate contact within 72 hours. If the ransom is not paid, the data is released to the public via the attacker's website, "Egregor News."

- **New and emerging Threat:** In a short amount of time, Egregor ransomware caused a great deal of damage and made headlines across the world.
- **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.
- **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.

WATCH THE VIDEO

Cybereason vs NetWalker Ransomware

DETECTED AND PREVENTED:

The Cybereason Defense Platform fully detects and prevents NetWalker ransomware.

NetWalker Ransomware has been one of the most notorious families over the course of the past year, targeting organizations in the US and Europe including several healthcare organizations, despite several known threat actors publicly claiming to abstain from targeting such organizations due to COVID-19.

NetWalker operators have adopted the recent popular trend among ransomware purveyors: double extortion. In addition to demanding a ransom for the encrypted files, the group behind NetWalker steals sensitive data and files from its victims. The group extorts the victims by threatening to leak the stolen data unless ransom is paid. This technique renders the practice of data backups all but moot in combating the impact from ransomware attacks. Other known ransomware groups that leverage the double extortion paradigm are Maze, REvil, and DoppelPaymer.

- **Encrypting Mapped Drives:** NetWalker encrypts shared network drives of adjacent machines on the network.
- **Double Extortion Operations:** The threat actor behind NetWalker threatens to publicly reveal stolen data if payments are not made.
- **Worldwide Threat:** NetWalker was employed in attacks across a variety of industries around the world, which caused great damage to many organizations.

WATCH THE VIDEO

Cybereason vs MedusaLocker Ransomware

DETECTED AND PREVENTED:

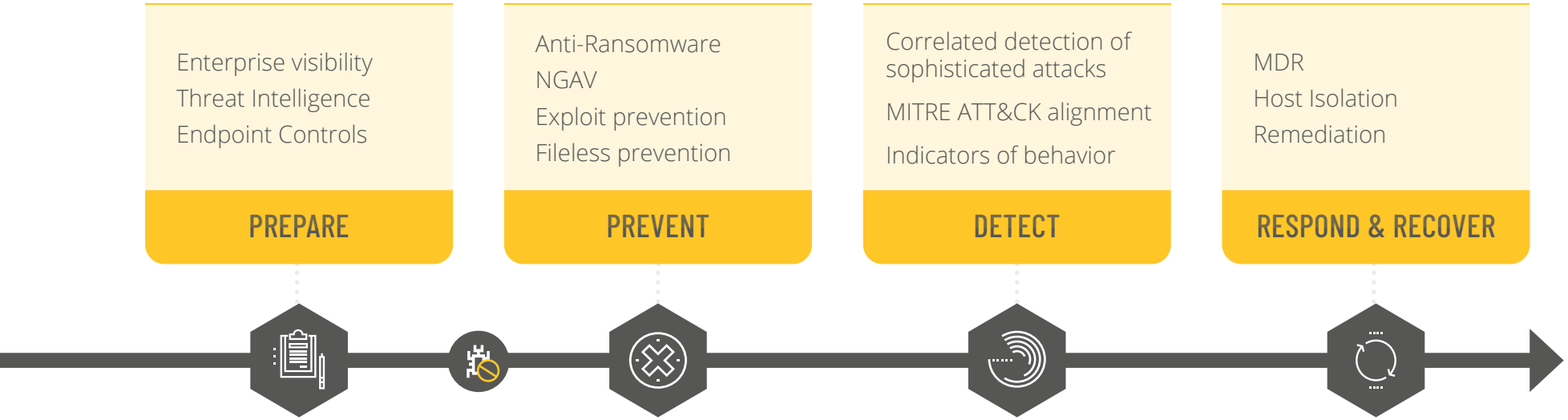
The Cybereason Defense Platform fully detects and prevents MedusaLocker ransomware.

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.

In order 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.

- **Encrypted 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.

Fearless protection against modern and multistage ransomware.



Let's continue the conversation.

Cybereason is the champion for today's cyber defenders providing future-ready attack protection that unifies security from the endpoint, to the enterprise, to everywhere the battle moves. The Cybereason Defense 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).

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 to mitigate future cyber risk.

The result: defenders can end cyber attacks from endpoints to everywhere.

Learn more about fearless ransomware protection today →