Cybereason vs. REvil Ransomware

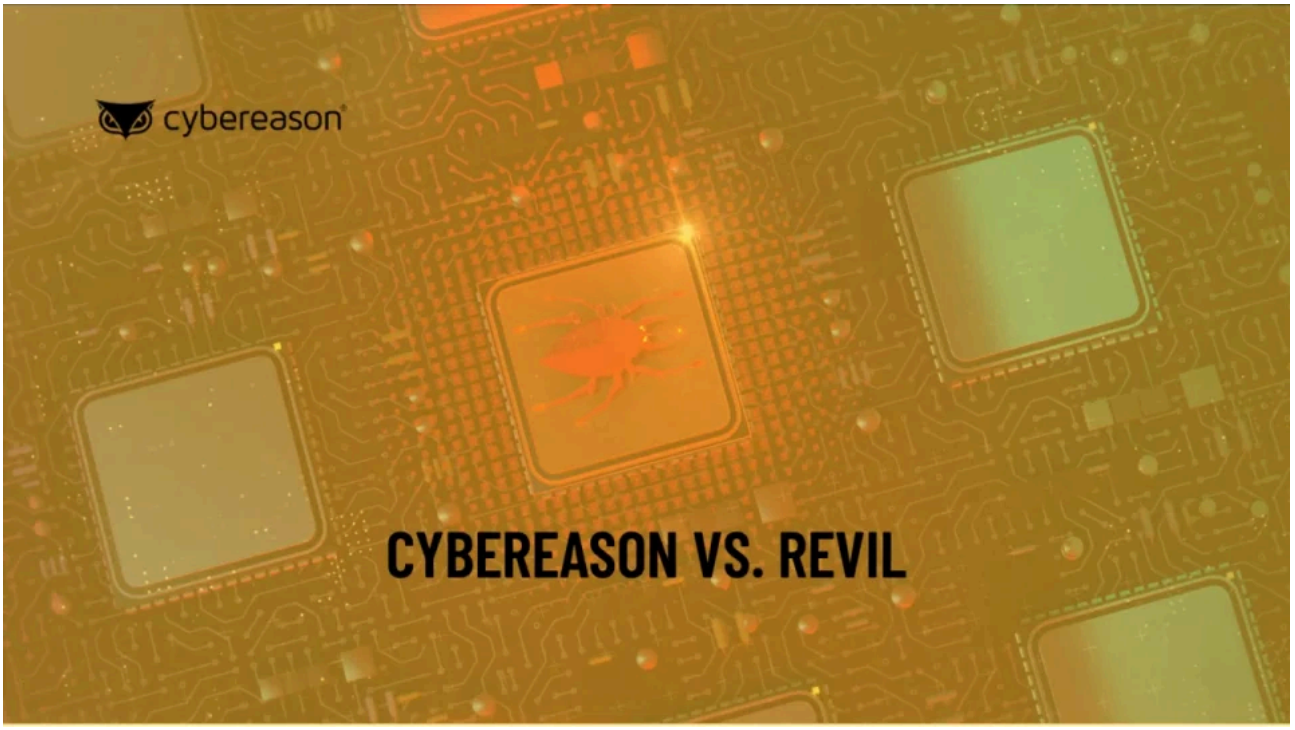
By Cybereason Team

Archived: 2026-04-05 14:29:22 UTC

According to reports, meatpacking giant JBS was hit with a serious attack reportedly involving REvil ransomware, shutting down a good portion of the company's production capabilities and threatening to create supply chain disruptions and sharp cost of goods increases.

Back in April of 2019, the Cybereason Nocturnus team first encountered and analyzed a new type of ransomware dubbed REvil (aka Sodinokibi, Sodin), a notoriously aggressive and highly evasive threat that takes many measures to maintain obfuscation and prevent detection by security tools.

The Cybereason Defense Platform is proven to detect and block REvil ransomware since it emerged in 2019, and continues to allow defenders to protect their organizations from this evolving threat:



The Cybereason Defense Platform Detects and Blocks REvil Ransomware

Tested sample in the video was uploaded to VirusTotal on June 2nd 2021:

SHA-256:

04419b76566142902680b2c44b216905b44a5743502530066e408bac72d20864

Cybereason AI-based NGAV solution prevents the execution of the REVIL ransomware

Cybereason Anti-Ransomware technology detects and blocks REvil

Over time, REvil has become the largest ransomware cartel operating in operation to date. Subsequent 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 a $50 million ransom demand with the additional threats to increase the ransom demand to $100 million and release exfiltrated data from the target should the payment not be made promptly.

The REvil ransomware gang have previously been connected to the same authors of the prolific GandCrab ransomware, which was retired in June 2019. GandCrab was responsible for 40% of all ransomware infections globally. If the association is accurate, GandCrab sets a good example for just how impactful REvil may become.

Much like the DarkSide ransomware gang that struck Colonial Pipeline in early May, the REvil gang follows the double extortion trend, where the threat actors first exfiltrates sensitive information stored on a victim's systems before launching the encryption routine.

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.

This means the target is still faced with the prospect of having to pay the ransom regardless of whether or not they employed data backups as a precautionary measure, and underscores the need to take a prevention-first security posture.

Ransomware Prevention Capabilities are Key

The best ransomware defense for organizations is to focus on preventing a ransomware infection in the first place. Organizations need visibility into the more subtle Indicators of Behavior (IOBs) that allow detection and prevention of a ransomware attack at the earliest stages.

Cybereason delivers fearless ransomware protection via multi-layered prevention, detection and response, including:

- **Anti ransomware prevention and deception:** Cybereason uses a combination of behavioral detections and proprietary deception techniques surface the most complex ransomware threats and end the attack before any critical data can be encrypted.
- **Intelligence-Based Antivirus:** Cybereason blocks known ransomware variants leveraging an ever-growing pool of threat intelligence based on previously detected attacks.
- **NGAV:** Cybereason NGAV is powered by machine learning and recognizes malicious components in code to block unknown ransomware variants prior to execution.

- **Fileless Ransomware Protection:** Cybereason disrupts attacks utilizing fileless and MBR-based ransomware that traditional antivirus tools miss.
- **Endpoint Controls:** Cybereason hardens endpoints against attacks by managing security policies, maintaining device controls, implementing personal firewalls and enforcing whole-disk encryption across a range of device types, both fixed and mobile.
- **Behavioral Document Protection:** Cybereason detects and blocks ransomware hidden in the most common business document formats, including those that leverage malicious macros and other stealthy attack vectors.

Cybereason is dedicated to teaming with defenders to end cyber attacks from endpoints to the enterprise to everywhere - including modern ransomware. Learn more about ransomware defense here or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

About the Author

Cybereason Team

Cybereason is dedicated to partnering with Defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the AI-driven Cybereason XDR Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user and

system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business.

All Posts by Cybereason Team
