Trinity Cyber

THREAT MITIGATION AND PREVENTION CASE STUDY

AvosLocker Ransomware

Stopping Avos and Their AvosLocker Ransomware Attacks

Avos is a Ransomware-as-a-Service (RaaS) affiliate-based group that is known to target victims across multiple infrastructure sectors including financial services, critical manufacturing, and government facilities. The FBI, U.S. Treasury Financial Crimes Enforcement Network and the Department of the Treasury recently issued a joint advisory on AvosLocker. These ransomware groups often apply "double extortion" by beginning their attack with encrypting files and demanding a ransom to unlock the files. They then threaten to leak the files on the darknet.

Avos RaaS affiliates and attackers are known to target known vulnerabilities as an intrusion vector to deploy AvosLocker ransomware. For example, cybercriminals have targeted vulnerabilities in Log4j, Microsoft Exchange server and Atlassian Confluence Server and Data Center instances for initial access to corporate networks to deploy AvosLocker ransomware. In other cases, AvosLocker has been spread through spam email campaigns.

Trinity Cyber's **TC:Edge** *service, powered by the Trinity Cyber Engine, automatically detects and stops AvosLocker and other ransomware attacks before they begin*.

Traditional Security Products Are Failing

AvosLocker ransomware is a multi-threaded Windows executable written in C++ that runs as a console application and shows a log of actions performed on victim systems. It encrypts files on a victim's server and renames them with the ".avos" extension.

Traditional network security products do not provide adequate protection from AvosLocker ransomware and other cyber attacks. Today's cyber attacks are successful because traditional products cannot examine Internet content deeply or quickly enough with the speed necessary to make a difference inline.

Ransomware gangs and other attackers succeed because their attack methods outmaneuver these products, which were built upon legacy technologies and approaches such as static indicators of compromise. Adversaries often employ obfuscation as part of their attack which enable AvosLocker ransomware and other cyber attacks to go undetected with great success. Ransomware and other attacks are being missed, and organizations are vulnerable. For threats these products do find, an enormous number of false alarms and alerts are produced, straining already overwhelmed security teams.

KEY TAKEAWAYS

- **Detects and prevents AvosLocker ransomware attacks on corporate networks**
- **Defeats initial intrusion attempts and AvosLocker ransomware missed by others**
- **Protects customers *automatically* using contextual, full-session inspection and automated preventive controls**
- **Reduces SOC staff workload**

Stopping AvosLocker Ransomware

Trinity Cyber's **TC:Edge** service line detects, mitigates and prevents AvosLocker as well as a full spectrum of cyber threats. In less than a millisecond, the **TC:Edge** service line can deeply inspect and transform full-session Internet traffic in both directions to expose and mitigate actual threat content or unauthorized traffic inline, automatically. **TC:Edge**'s near-zero False Positive Rate accuracy is *better than 0.03%* and produces almost no false alarms.

A key reason **TC:Edge** prevents AvosLocker and other cyber attacks is that the Trinity Cyber Engine identifies and defeats attacker tactics, techniques and procedures (TTPs). This is critical to defeating and preventing entire classes of ransomware (like AvosLocker), actual malware, command and control (C2), remote code exploits (RCE), drive-by downloads, and in-the-wild malicious threats that are commonly missed by traditional detect-and-respond systems. For AvosLocker attacks, the **TC:Edge** service detects and stops the initial attempts to penetrate the network as well as AvosLocker ransomware in less than a millisecond. On the customer's behalf, **TC:Edge** accurately identifies and removes the malware, preventing the attack, without intervention or action from the customer's security team. This advanced capability dramatically reduces the already-stretched security team's workload. Detailed threat intelligence and metadata as well as the actions taken by Trinity Cyber are immediately available to customers on their portal. In all cases, users, data and infrastructure remain secure and protected because ransomware attacks like AvosLocker are detected, defeated and prevented *automatically*.

Want to learn more? Contact us at info@trinitycyber.com for more information.

Gartner COOL VENDOR 2020