Trinity Cyber

THREAT MITIGATION AND PREVENTION CASE STUDY

Maui Ransomware

Stopping Maui Ransomware

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Treasury (Treasury) recently released a joint Cybersecurity Advisory (CSA) warning North Korean state-sponsored cyber actors are targeting the Healthcare and Public Health sectors for Maui Ransomware attacks. Because these bad actors likely assume healthcare organizations are willing to pay ransoms because of the critical services these organizations provide, the CSA recommends organizations expect these attacks to continue.

According to CISA Alert AA22-187A, Maui Ransomware encrypts servers involved in the delivery of healthcare services—including electronic health records, diagnostics services and imaging services. However, all organizations, independent of sector, are potential targets for Maui ransomware either now or in the future.

Trinity Cyber's **TC:Edge** *service quickly detects and prevents Maui Ransomware attacks to protect customer networks, users and data.*

Maui Ransomware Encrypts Data and Provides No Ransom Note

Maui Ransomware is an encryption binary that is designed for remote manual execution. The remote adversary can use a command-line interface to interact with the malware and identify specific files to encrypt. The Maui Ransomware is known to use a combination of Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) and XOR encryption to encrypt target files. Also, Maui Ransomware often does not provide a ransom note or the steps the victim should take to recover their encrypted data.

Maui Ransomware and a wide variety of other cyber attacks continue to be disruptive. According to the 2022 Verizon Data Breach Report, ransomware attacks increased 13% year over year, a jump greater than the last five years combined. Traditional network security products are failing to provide adequate protection because they cannot examine Internet content deeply or quickly enough with the speed necessary to make a difference inline, and their preventive control capabilities are limited. These products still rely upon legacy technologies and approaches such as static indicators of compromise and signatures. Knowing this, adversaries often employ methods to evade detection, leaving organizations vulnerable. For threats these products do find, an enormous number of alerts are produced, straining security teams that are already overwhelmed with incident response workload, alert fatigue and investigations that are discovered to be false positives almost 50% of the time.

KEY TAKEAWAYS

- **Detects and prevents Maui Ransomware attacks on corporate networks**
- **Prevents malware, exploits and techniques missed by others**
- **Reduces incident response workloads**

Taking Maui Ransomware "Off the Table"

Trinity Cyber took a fundamentally different approach to solving the most important challenges in cybersecurity, and the result is the Trinity Cyber Engine. In less than a millisecond, this revolutionary technology can deeply inspect and transform full session Internet traffic in both directions to expose and mitigate actual threat content or unauthorized traffic inline, automatically. Our fully managed **TC:Edge** service line, built upon the strong foundation of the Trinity Cyber Engine, detects, mitigates and *prevents Maui Ransomware* as well as a full spectrum of other cyber threats. **TC:Edge** provides security teams with highly accurate network prevention against malware delivery, exploit delivery, and other nefarious tactics that ransomware groups deploy.

Unlike others, the **TC:Edge** service is extremely effective at detecting, mitigating and preventing Maui Ransomware and other cyber attacks because the Trinity Cyber Engine identifies and defeats attacker tactics, techniques and procedures (TTPs). This capability is crucial to defeating and preventing entire classes of ransomware (like Maui Ransomware), command and control (C2), remote code exploits (RCE), drive-by downloads, and other threats that often go undetected by traditional security products. For Maui Ransomware attacks, the **TC:Edge** service identifies and removes Maui Ransomware automatically from network traffic. No intervention or action is necessary from the customer's security team, dramatically reducing the already-stretched security team's incident response workload. Detailed threat intelligence and metadata as well as the actions taken by Trinity Cyber are immediately available to customers via the customer portal. Customer users, data and infrastructure remain secure and protected because Maui Ransomware and other cyber attacks are detected, defeated and prevented *automatically*.

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

Gartner COOL VENDOR 2020