Trinity Cyber

THREAT MITIGATION AND PREVENTION CASE STUDY

Unauthorized Active Cryptomining

Unauthorized Cryptomining on the Corporate Network

Traditional network security products are inadequate to detect, mitigate and prevent modern threats. Their lack of visibility and preventive capabilities also leave enterprises vulnerable to unauthorized traffic such as cryptomining, as Trinity Cyber recently highlighted for a biotechnology customer.

Shortly after Trinity Cyber's **TC:Edge** managed service was initiated, the patented Trinity Cyber Engine technology detected and mitigated active Ethereum mining executing on the corporate network. These cryptomining activities had been present for some time but had evaded detection by the customer's existing security products. However, the Trinity Cyber Engine and its deep, comprehensive inspection and automated preventive controls discovered and stopped the cryptomining activities automatically.

Trinity Cyber Delivers While Others Fail

As part of the **TC:Edge** service, the Trinity Cyber Engine detected an open source Linux download of HiveOS, a platform that allows users to set up, mine and control mining processes. In addition, corresponding TCP traffic in the form of the Stratum protocol (supports pooled cryptomining) was also detected on the corporate network on the same day. This traffic was of two varieties: web traffic that reported the status of mining periodically back to a server and a raw TCP stream that received and verified mining jobs on the blockchain.

Although cryptomining activities had been present and were executing actively on the corporate network, the existing security infrastructure did not identify or send alerts on the ongoing activity. In contrast, the **TC:Edge** service, built upon the Trinity Cyber Engine and its superior deep, contextual and full-session inspection, detected this traffic almost immediately. In addition, its automated preventive controls stopped the unauthorized cryptomining traffic automatically on the customer's behalf.

As a result of Trinity Cyber's rapid engagement with the customer, the cryptomining devices and the responsible personnel were quickly identified. The devices were removed from the network, and no subsequent cryptomining activities were detected on the network.

KEY TAKEAWAYS

- **Prevented unauthorized cryptomining traffic executing on the corporate network**
- **Identified unauthorized cryptomining traffic consistently missed by existing security products**
- **Protected corporate network with automated preventive control to stop the unauthorized cryptomining activities, not just issue alerts**
- **Expanded network visibility**
- **Reduced SOC staff workload**

Dramatically Reducing Cyber Risk

Modern ransomware, malware, exploits, and unauthorized traffic such as cryptomining are surprisingly successful at avoiding detection by traditional cybersecurity products. They are ineffective because their reliance on indicators limits their ability to expose and prevent modern threats. For the threats these products do detect, very large numbers of false positives and alerts are generated, triggering significant incident response workload and increasing strain on already overloaded SOC resources.

Trinity Cyber has a better way that addresses these challenges and reduces cyber risk. In less than a millisecond, the patented Trinity Cyber Engine can deeply *inspect and transform full-session Internet traffic in both directions to expose and mitigate actual threat content or unauthorized traffic inline,* not the simple indicators of threat. Our near-zero False Positive Rate accuracy is industry-leading and produces almost no false alarms. The Trinity Cyber Engine's new, automated preventive controls are tuned to defeat attacker tactics, techniques and procedures (TTPs), which is vital to defeating and preventing modern cyber threats. Our fully managed service lines remove work from our customers and protect them from unauthorized network traffic (like cryptomining), entire classes of actual malware, command and control (C2), remote exploits, drive-by downloads, and in-the-wild malicious threats that are commonly missed by traditional detect-and-respond systems.

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

Gartner COOL VENDOR 2020