eSENTIRE

CASE STUDY

Third Party Serves as Staging Point for Cryptojacking Attack Using Powershell

Attack Types:

Phishing, PowerShell, Zero-Day Exploit

Industry:

Finance

Services:

esENDPOINT™

Financial services are very interconnected with clients, partners and vendors using expansive on-premises and virtual datacenters to send and receive vast amounts of sensitive data daily. Financial services cyber prevention is primarily focused on prevention of fraud and leaks of financial data or personally identifiable information. But, attackers are finding new creative and covert methods to reap financial rewards. Given the compute power required to conduct trades, transactions and interactivity with clients at the speed of modern business, FinTech companies offer unique solutions to improve speed and efficiency. Unfortunately the tradeoff is an ever-expanding sprawl of vendors that can put organizations at risk. For one eSentire client, traditional detection methods were not enough as attackers were able to take advantage of digital grey areas presented by opportunistic vendor risk.

In January 2018, eSentire observed an unknown threat actor attempting to deploy Monero cryptocurrency mining malware to multiple eSentire customers.

This increasingly common type of attack known as “cryptojacking” allows a hacker to leverage the compute power of devices on a personal or corporate network to mine cryptocurrencies, unbeknownst to the victim. Ultimately, this category of attack can lead to poor device performance or potential failure resulting in financial and regulatory repercussions.

Following an investigation from eSentire’s Security Operations Center (SOC) analysts, it was determined that the threat actor was leveraging a previously unknown vulnerability (zero-day exploit) in Kaseya’s Virtual Systems Administrator (VSA) agent as a vector to gain access to the clients’ network. Kaseya is a reputable IT management software vendor used by financial organizations and managed service providers.

From Jan. 19 - 24, eSentire’s SOC analysts leveraged esENDPOINT to observe suspicious PowerShell activity across several customers. Kaseya’s “ageentmon.exe” launched PowerShell with a specific command line and began to download cyroptomining malware from the popular cloud-storage provider Dropbox. The download was performed tactfully in four separate encoded parts plus an initiator script and the execution tasks were scheduled in a staggered manner to avoid detection.

Hackers often use techniques like this to hide among legitimate PowerShell scripts or to purposely confuse an observer with obfuscated commands. eSentire was able to identify this attack, using esENDPOINT’s proprietary machine learning technology code-named BlueSteel to correlate all PowerShell activity on a client’s endpoint with advanced analytics. This proprietary capability alerted eSentire’s SOC analysts on the suspicious activity, triggering the investigation that ultimately uncovered the Kaseya Vulnerability.

Impacted customers were notified and given remediation guidance to reverse the PowerShell commands to stop the mining malware from running.

Kaseya was notified of the vulnerability by eSentire and promptly released a patch to their VSA product for all of their customers.

© 2019 eSentire, Inc. All rights reserved.

ATTACK TIMELINE

2018-01-19
06:46
Client notified of suspicious behavior tracing back to Kaseya agent. Escalated to eSentires Advanced Threat Analytics (ATA) team for deeper investigation.

2018-01-19
09:26
Client replies to alert. The client's MSP advised that the behavior is to be expected.

2018-01-19
09:42
ATA concludes investigation and provides additional evidence of obfuscation and clearly hostile activity.

2018-01-19
12:59
SOC offers to host isolate machines in question and awaits reply as per specific client runbook. Minutes later, the client replies requesting the SOC delay action as they engage their MSP.

2018-01-19
13:50
Further details of the payload, a Monero bitcoin mining malware, shared with the client.

2018-01-19
14:25
Still awaiting answers from their MSP, the client requests remediation recommendations from the SOC.

2018-01-19
14:29
SOC respond with remediation recommendations, advising the infected hosts be re-imaged. eSentire retains raw endpoint data telemetry as evidence.

2018-01-20 - 2018-01- 24
Over the next several days, eSentire continues to work with the client and eventually the MSP. The scale of the breach is ultimately revealed 1,190 systems across the MSP's client base. Due to the scale, the MSP enlists an Incident Response firm for cleanup. eSentire provides all investigation and forensic details to aid in the process. The threat is fully remediated on Jan. 24 and the SOC officially closes the incident. The MSP in question looks to engage eSentire for ongoing Managed Detection and Response services for its network.

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.