Crypto-jacking - Cryptocurrency-mining malware: the Peeled Onion

2018 Data Breach Digest

verizon

The situation

As in previous years, 2017 saw significant interest in cryptocurrencies or crypto-jacking, both the classic Bitcoin and newer alternatives. Unsurprisingly, with the meteoric rise in Bitcoin value interest hasn't been limited to investors. In 2017, the VTRAC | Investigative Response Team has investigated several cybersecurity incidents involving attackers whose motivation has been financial gain through cryptocurrency mining malware.

This variety of malware uses the processing power (e.g. CPU or graphics card) of the infected system to mine cryptocurrency, which could then be used like traditional cash to purchase items or directly exchanged for legal tender. While mining is a legitimate process in the cryptocurrency lifecycle, using someone else's system in an unauthorized manner is not.

While Bitcoin is the most widely known cryptocurrency, there are hundreds of alternative cryptocurrencies sometimes better suited for mining through malware. This is due to their relative anonymity or ease of being mined on ordinary systems. In 2017, we investigated only a few cases of malware mining for Bitcoin while the majority of cases involved Monero or Zcash.

In one such "non-Bitcoin" case, a customer who had observed a significant number of alerts originating from their firewalls called upon us. The firewalls were blocking suspicious outbound traffic to The Onion Router (Tor) network and in doing so, triggering alerts. Our customer believed they had the situation under control because the firewalls were blocking the traffic. They asked us to determine the cause of the traffic, verify they had things under control, and verify there were no indications of data exfiltration or lateral movement in their network.

Response tip

Be vigilant for anomalous activity, such as sharp increases in system CPU usage or network egress / ingress traffic volumes; monitor firewall and network appliance logs for anomalous activity.

Why are cryptocurrencies so attractive to cybercriminals?

- Money talks: To the tech savvy attacker, cryptocurrency is as good as cash. It's used to directly make purchases, particularly when buying illegal goods, such as stolen identity information, hacking tools or drugs on the DarkNet
- Easy to exchange: If the perpetrator isn't interested in spending cryptocurrency directly then it's simple to cash-in cryptocurrency for traditional cash at many exchanges
- Easy to transfer: Cryptocurrencies can easily be transferred around the world without the delays or bureaucracy associated with traditional wire transfers and banks
- Comfort in anonymity: While Bitcoin (by design) is inherently traceable, there are services to facilitate the laundering of Bitcoin (for a modest fee) which make it attractive to attackers. More recently alternative cryptocurrencies, such as Monero have been developed with privacy and anonymity built in by design, making them attractive to attackers
- Lucrative return: Unlike ransomware attacks with most victims not paying the ransom, cryptocurrency mining has a more promising return rate

Response tip

Block access to command and control (C2) servers at the firewall level; deploy Group Policy Objects (GPOs) to block known malicious executable files and disable macros.

Investigative response

Prior to engaging us, the customer had obtained full packet captures (FPCs) of network traffic and captured a physical memory dump from a system generating the suspicious outbound traffic. We dove into the network FPCs and the memory dump, and soon provided actionable intelligence to identify other potentially compromised systems on the network. This actionable intelligence – indicators of compromise (IoCs) – included system names, IP addresses, malware file hashes / file names and malicious process names.

A review of the active network connections immediately revealed that while the majority of traffic was blocked by the firewall, there were successful connections to resources in the Tor network. This was due to the firewall filtering being based on IP address blacklisting, which didn't encompass all Tor addresses used by the malware. It was also observed that further network connections were being made to a mining pool associated with the Monero cryptocurrency. All malicious network activity was identified as originating from the Microsoft "powershell.exe" process (a command line shell and scripting tool) running on the sample system and other systems found to be infected.

Meanwhile, in reviewing the FPCs our VTRAC | Applied Intelligence (a.k.a. Network Forensics) team confirmed the malware used a propagation method similar to that of well-known ransomware instances. The method leveraged leaked hacking tools by the hacking group "The Shadow Brokers." An examination of an image of the sample system confirmed it wasn't patched against a known vulnerability (CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability) that made the propagation possible. This was contrary to our customer's belief they were properly secured.

We then analyzed firewall logs to identify any other systems beaconing out to the Tor network and requiring remediation. We assisted the customer with a remediation plan that involved providing samples of the malware to their anti-virus vendor, patching vulnerable systems, eradicating the malware and rebuilding key systems based upon legacy operating systems.

Response tip

Perform malware analysis to understand malware functionality for detection and response, and mitigation and prevention.

What types of cryptocurrency-related attacks are there?

- Cryptocurrency mining: As detailed in this article, the objective of many attackers is to directly mine cryptocurrencies for illicit profit
- Crypto-malware/ransomware attacks: Prevalent for the past few years, this attack commonly leads to files being rendered useless to its legitimate owner through encryption; the decryption key is provided by the attacker only when a ransom is paid in cryptocurrency
- Cryptocurrency wallet theft: Cryptocurrencies are commonly stored in wallet files, either on an individual system or online wallet service. These wallets contain private keys controlling the cryptocurrency and are attractive targets for cybercriminals. Malware targeting wallet files for theft and phishing attacks to gain online wallet service credentials is on the rise
- Cryptocurrency wallet service/broker distributed denial of service (DoS) attacks: These DDoS attacks prevent users from using their cryptocurrency wallet (e.g., as Bitcoin prices fall, it was time to sell as fast as possible)

Lessons learned

During the investigation, it was discovered that hundreds of systems within the network hadn't been patched with the latest Microsoft Windows patches. Prompt and proper patching could have averted this incident.

On this occasion the malware targeted cryptocurrency mining, but more malicious software could've leveraged the same vulnerabilities and made a more significant impact on business.

Mitigation and prevention

- Conduct regular security assessments; evaluate defensive architecture design based on sandboxing, web browser separation, and virtualization for select activities
- Establish a vulnerability patch management program; apply security patches soon; confirm patching succeeded
- Employ enterprise and host-based anti-virus solutions with up-to-date signatures to detect and eradicate threats as they arise
- For critical systems and servers, deploy File Integrity Management (FIM) and Application White Listing (AWL) solutions; add Intrusion Prevention System (IPS) rules; disallow internet browsing
- Block and/or alert on internet connections to cryptocurrency mining pools; include Tor networks, unless a valid business reason not to do so
- To the extent possible, remove local admin; force standard user use for web browsing activity and force escalation for privileged user use in other context

Detection and response

- Be vigilant for anomalous activity, such as sharp increases in system CPU usage or network egress / ingress traffic volumes; monitor firewall and network appliance logs for anomalous activity
- Block access to command and control (C2) servers at the firewall level; deploy Group Policy Objects (GPOs) to block known malicious executable files and disable macros
- Perform malware analysis to understand malware functionality for detection and response, and mitigation and prevention
- Conduct periodic threat hunting activities across the network to locate and identify any undetected cyber threat activity evading traditional cybersecurity tools
- Create an Incident Response Playbook for cryptocurrency related scenarios; train incident responders on response efficient and effective activities.

What can malware analysis tell me about cryptocurrency-mining malware?

In performing malware analysis to understand its functionality, consider conducting these activities:

- Identify any kill-switches and/or configuration files; determine their impact on malware functionalities
- Evaluate blocking malicious remote servers (not just C2) used at firewall and proxy servers
- Evaluate blacklisting malicious domain names at Domain Name System (DNS) level
- Create additional detection rules; perform threat hunting using network Intrusion Detection System (nIDS) / host Intrusion Detection System (hIDS) signature, including YARA rules, file hashes, etc.
- Identify any self-propagation mechanisms; take corrective measures (e.g., reporting to vendor, patching vulnerabilities)
- Eradicate any persistence mechanisms
- Determine encryption mechanism used and possible way to recover encrypted files