Internet Security Threat Report

ISTR

Cryptojacking: A Modern Cash Cow

An ISTR Special Report | Sep 2018

Analyst: Brigid O'Gorman

Contents

Cryptojacking: A Modern Cash Cow

Key points
What you need to know about coin mining
The history of coin mining

Cryptojacking & Cyber Crime

Cryptojacking trends

Case Studies

01 Social scams
02 Attacks on enterprises
03 Software supply chain attack
04 Long arm of the law

The Future of Cryptojacking

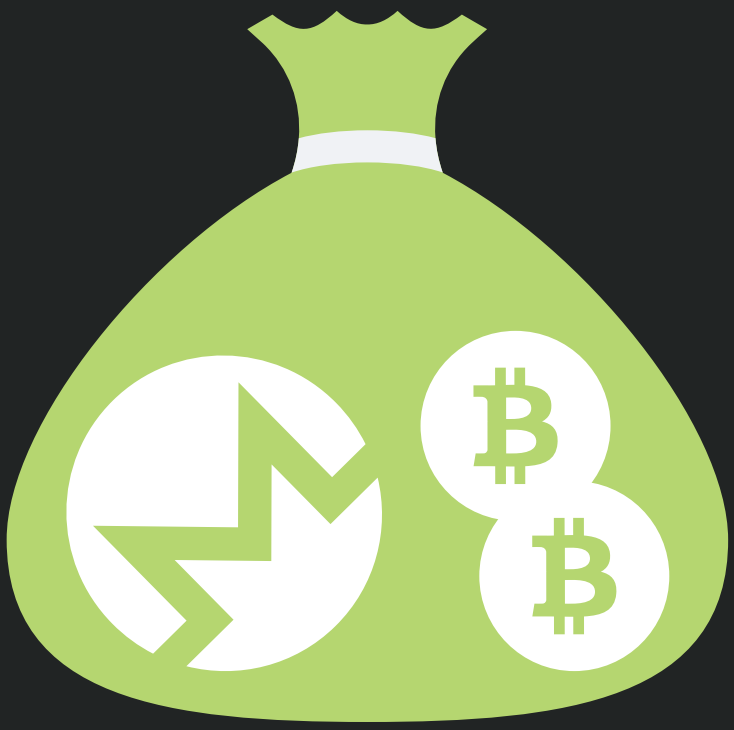
Best Practices

Symantec

Cryptojacking: A Modern Cash Cow

Section

01



In the final quarter of 2017, a surge in cryptojacking placed a firm spotlight on this part of the cyber crime landscape. While incidents of cryptojacking have decreased somewhat from the heights reached at the end of 2017, cryptojacking by opportunistic cyber criminals remains a key concern in the cyber crime landscape.

Key points

- Cryptocurrencies can be mined on personal computers using either file-based miners or browser-based miners. We have seen the greatest surge in activity in the area of browser-based coinminers.
- Cryptojacking activity surged to its peak in December 2017, when more than 8 million cryptojacking events were blocked by Symantec. While we have seen a slight fall in activity in 2018, it is still at an elevated level, with total cryptojacking events blocked in July 2018 totalling just less than 5 million.
- The primary cryptocurrency mined by these cryptojacking miners is Monero.
- Primary effects of cryptojacking include: device slowdown; overheating batteries; increased energy consumption; devices becoming unusable; and reduction in productivity. Cryptojacking in the cloud could also cause additional costs for businesses that are billed based on CPU usage.
- Reasons we saw a surge in cryptojacking in late 2017 include: the launch of the Coinhive service lowering the barriers to entry, and a surge in the value of many cryptocurrencies.

What you need to know about coin mining

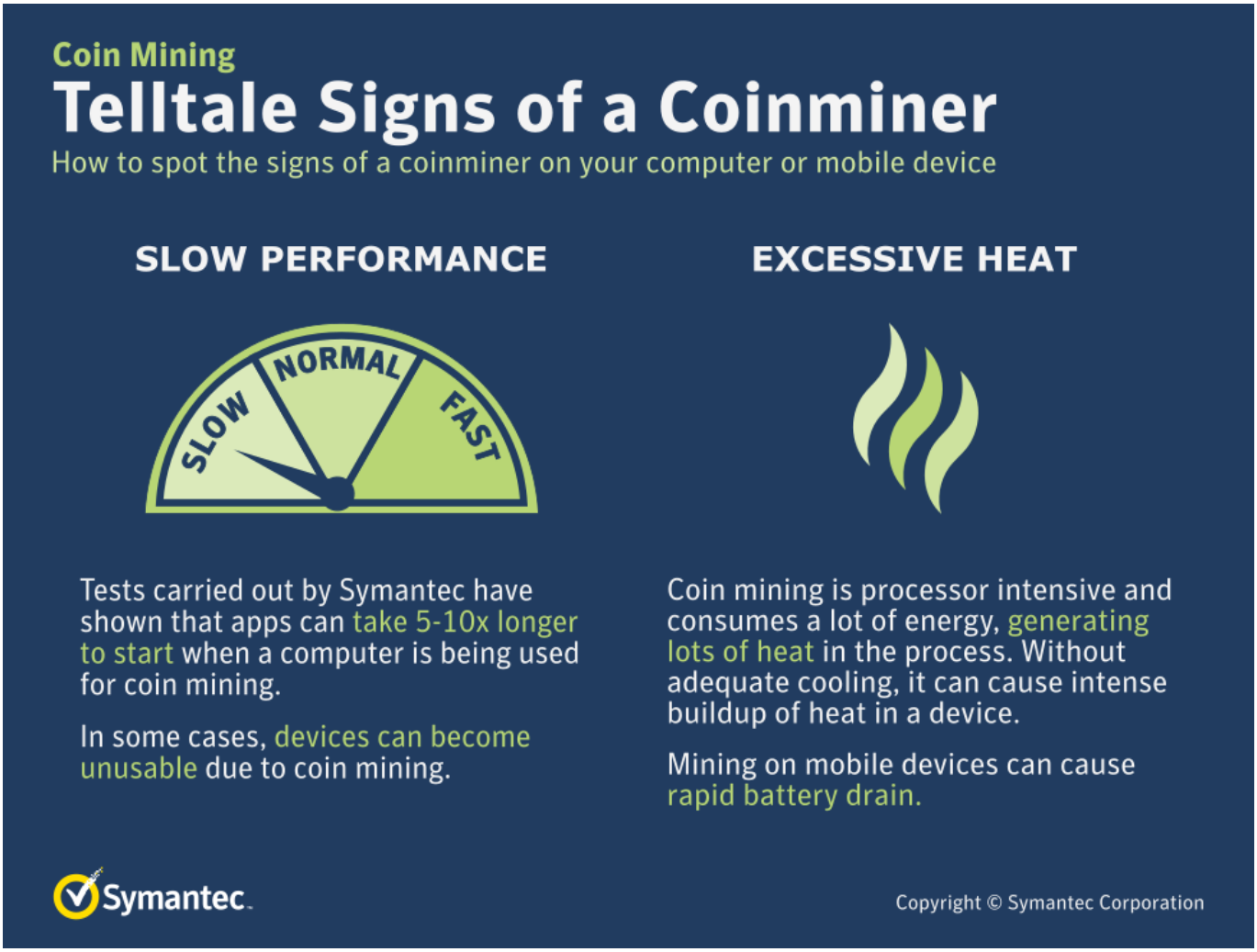
Coinminers are used to mine cryptocurrencies. Cryptocurrencies are digital currencies created using computer programs and computing power and, for the most part, are recorded on the blockchain. The blockchain is a peer-to-peer network that timestamps transactions by hashing them onto an ongoing, hash-based proof of work. This forms a record that cannot be changed without redoing the proof of work. The blockchain was first written about by Satoshi Nakamoto in 2009 and Bitcoin was the first cryptocurrency developed on it, and Bitcoin is still the best known and most highly valued cryptocurrency in existence. However, Bitcoin now requires a lot of processing power, and special equipment, to mine and so is not a viable option for mining on regular computers. Due to its popularity it also now attracts high transaction fees and takes a long time to mine, so it can be difficult to make a profit mining it.

However, other cryptocurrencies have been developed that can more easily be mined using the computing power of regular home computers. Monero is the primary example of this. Monero, unlike Bitcoin, also provides anonymity: it is almost impossible to track Monero transactions.

There are two primary methods of coin mining on personal computers:

- File-based coin mining involves downloading and running an executable file on your computer.
- Browser-based coin mining, which saw the biggest jump in prevalence in 2017, takes place inside a web browser and is implemented using scripting languages.

Coin mining is not illegal, and many people choose to run files or scripts on their computers to carry out coin mining to make money themselves. Many people may not object to some of their computing power being used to mine cryptocurrency when they visit a particular website as it could be a welcome alternative to watching ads or paying for the content in other ways. Websites could create revenue and users of the website would 'pay' by allowing their device's central processing unit (CPU) power to be used to mine cryptocurrency while they are on the website. The problems arise when people aren't aware their computers are being used to mine cryptocurrency, or if cyber criminals surreptitiously install coinminers on victims' computers or Internet of Things (IoT) devices without their knowledge—this is cryptojacking.



The primary impact of cryptojacking is performance related, with its potential impacts for device users including:

- A slowdown in device performance
- Overheating batteries
- Devices becoming unusable

Coin mining also has implications for organizations. Apart from the frustration and reduction in productivity that slow devices cause employees, self-propagating coinminers may require corporate networks to be shut down to facilitate a clean-up. It may also increase businesses' costs due to increased electricity usage. Cryptojacking in the cloud also has additional financial implications for organizations that are being billed based on CPU usage.

The history of coin mining

Cryptojacking surged massively in 2017, but coin mining has been around for quite a while. Browser-based mining dates back to May of 2011 when an innovative service called BitcoinPlus.com was initially launched—not to be confused with another cryptocurrency known as Bitcoin Plus.org. This service used JavaScript code for pooled mining: website owners could sign up to the service and embed scripts into their web pages to make page visitors mine for them. Back in 2011, Bitcoin was still in its infancy, mining difficulty was relatively low, and cryptocurrency prices were even lower.

Even though it was possible at that time to mine for Bitcoin via BitcoinPlus.com, the reality of the situation was that it was largely a futile exercise. The reward was minuscule compared to the amount of mining power and electricity

required—in June 2011, one bitcoin was worth approximately US$30 (In comparison, in August 2018, one bitcoin was worth approximately $6,000).

Due to this fundamental profitability problem with browser-based mining at the time, it soon died away. However, the idea was once again revived in December 2013 by a group of MIT students with a project called Tidbit—which was ostensibly touted as an alternative way for website owners to raise revenue. However, soon after it started, the New Jersey Division of Consumer Affairs stepped in to investigate the fledgling company on charges of unlawful access to "a person's computer processing power." This resulted in a long drawn out case, which was finally settled in 2015.

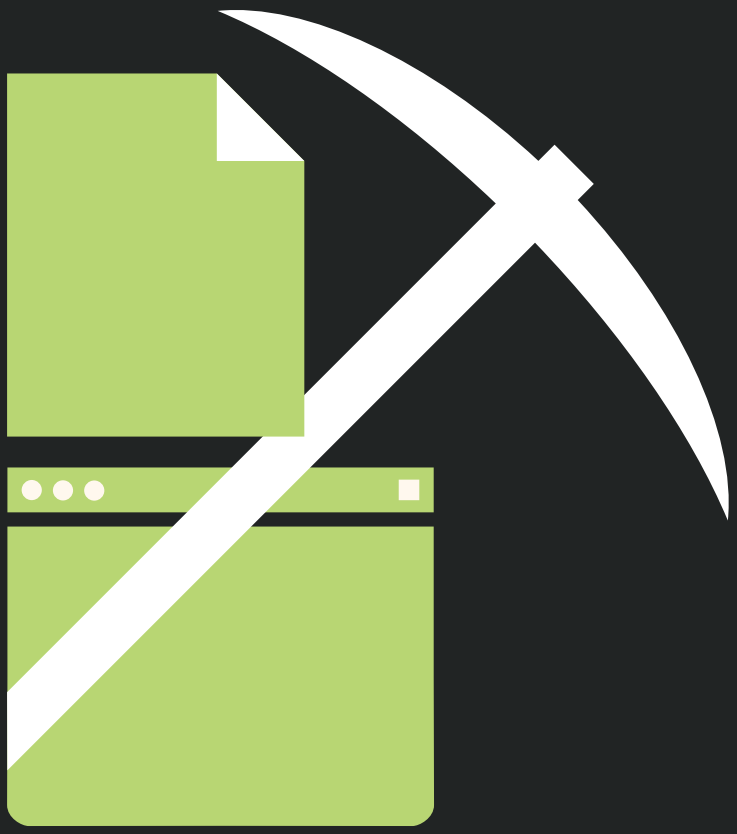
The growing problem of profitability was made even worse by the increasing use of ASIC miners—special machines that could mine Bitcoin much faster. The advent of ASIC miners dragged Bitcoin mining out of the realm of home users and, after the demise of Tidbit, the idea of browser-based JavaScript cryptocurrency mining largely died away once again—until the last quarter of 2017.

The launch of a new service by Coinhive in September 2017 led to a renewed interest in the area of browser-based mining. Coinhive, which like most browser-based miners mines Monero, was marketed as an alternative to ads for websites seeking to generate revenue. It recommends that its users are transparent with site visitors about its presence, but this hasn't stopped unscrupulous operators from using it to carry out cryptojacking with the hope that users won't notice. Since its launch there have been many reports of it being used for cryptojacking without website visitors' knowledge.

Cryptojacking & Cyber Crime

Section

02



Cryptojacking and Cyber Crime

The launch of Coinhive, along with other factors, meant that we witnessed the greatest growth in activity from cyber criminals in the area of browser-based, rather than file-based, cryptojacking. The barrier to entry for browser-based cryptojacking is lower: browser-based cryptojacking does not require the same level of skill as developing an exploit and installing it on victims' computers, which is what would be necessary to carry out file-based activity. The launch of Coinhive—with its ready made scripts—lowered this barrier even further. Cryptojacking via browsers also means that even people whose machines are fully patched are potential victims, if they visit a website that has coin-mining code injected into it. The code will use the power of their device to mine for cryptocurrencies for as long as they have the web page open.

Key reasons for the surge in cryptojacking

- Coinhive lowering barrier to entry
- Surge in the value of cryptocurrencies
- Allows fully patched machines to be targeted
- Cyber criminals can operate without the activity being noticed by victims

Another driving force in the popularity of cryptojacking among cyber criminals was a steep rise in the value of cryptocurrencies towards the end of 2017, which included a surge in the value of Monero, the primary cryptocurrency mined by browser-based coinminers. At the height of the cryptojacking craze at the end of December 2017/start of January 2018, the price of one Monero coin hit more than $350, which is close to 10 times what it was valued at in August 2017. In July 2018 it was hovering at around $130, but it is still worth almost three times what it was valued at in August 2017.

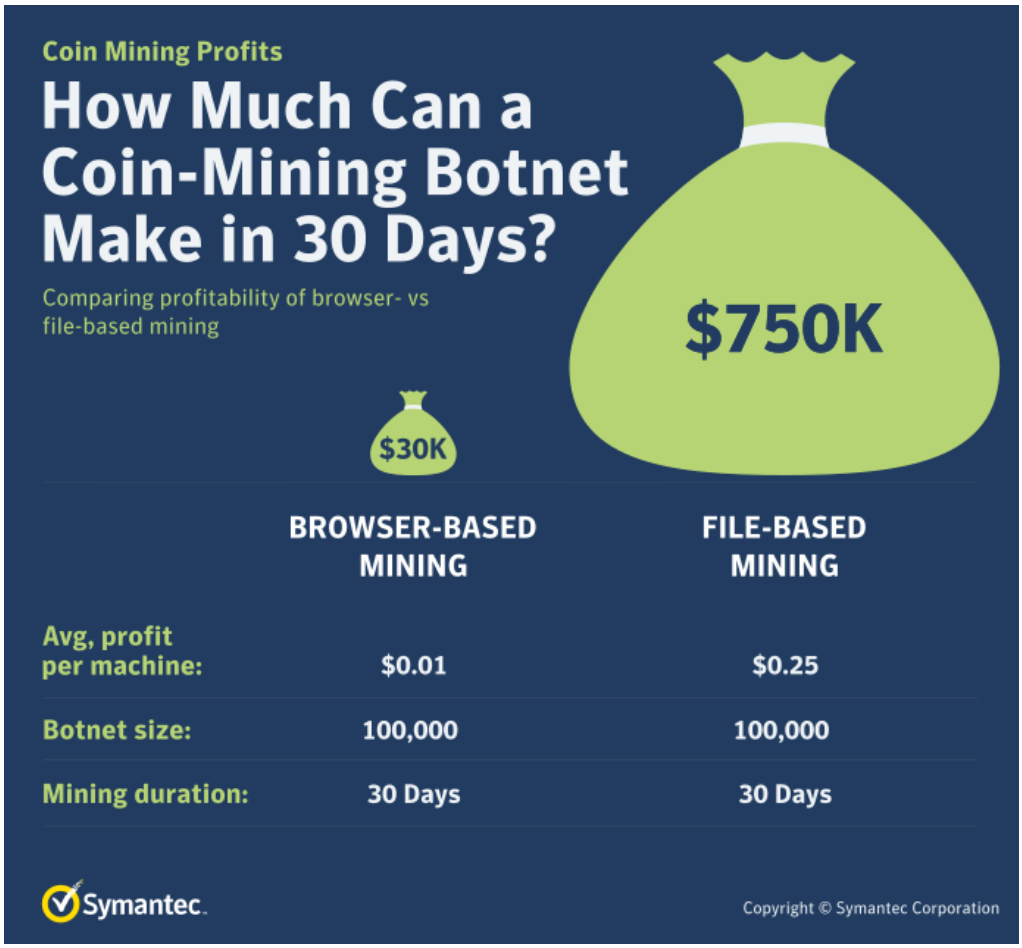
Cryptojacking via browsers also means that even people whose machines are fully patched are potential victims

Figure 1. The fluctuations in the value of Monero from August 2017 to July 2018

Lower barriers to entry plus increasing values, combined with the ability to stay under the radar, made cryptojacking a dream target for cyber criminals, which is why we saw such a surge in activity in this area.

That coinminers can run on people's computers without them immediately being aware that their CPU power is being hijacked is one of the major appeals of cryptojacking for cyber criminals: it is a less disruptive way to make money. Victims won't necessarily immediately realize they are infected, if they ever do. They may notice that their computer is performing more slowly, that their fans are running more often, or that their electricity bill has increased due to their computer using more power, but if the impact is only minor victims may not make the connection to cryptojacking. Cyber criminals can also 'throttle' coinminers so that they only use a certain amount of computing power or use less power if the victim is using their machine to do something that requires a lot of CPU usage, such as playing graphically demanding games. This ability to operate without being noticed can allow cyber criminals to make money without victims even realizing they have something unwanted on their machine or on the website they are visiting. Other threats deployed by cyber criminals, such as ransomware, do not allow them to go unnoticed like this.

However, when it comes to cryptojacking, scale is key for cyber criminals who want to make money. A browser-based coinminer generates roughly one cent per machine in 24 hours of continuous mining; with file-based miners that might increase to between 25 and 50 cents every 24 hours. This return depends a lot on the power of the device and on the value of the currency being mined. But that would mean a botnet of 100,000 bots carrying out browser-based mining, running continuously for 30 days, could make $30,000, or a file-based miner could make $750,000. The potential is there for big results in cryptojacking, but scale is a key part of the equation.



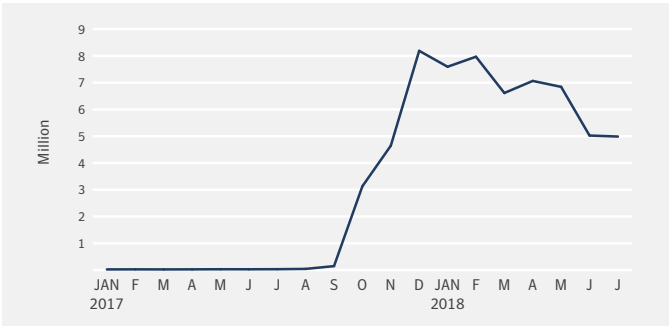
The surge in the profile and value of cryptocurrencies, however, also had a detrimental impact on some people who had invested in them, with numerous coin wallets and exchanges being cleared out by cyber criminals who managed to gain access to them. In this case the anonymity of cryptocurrencies, and lack of regulation in the space, which is a big part of cryptocurrencies' appeal for many people, worked against it as, in most cases, it is impossible to trace where stolen cryptocurrency has gone.

Cryptojacking trends

The surge in activity in cryptojacking was stark. The increase began in October 2017 and hit a peak in December—between the beginning and end of 2017 total cryptojacking activity increased by a staggering 34,000 percent.

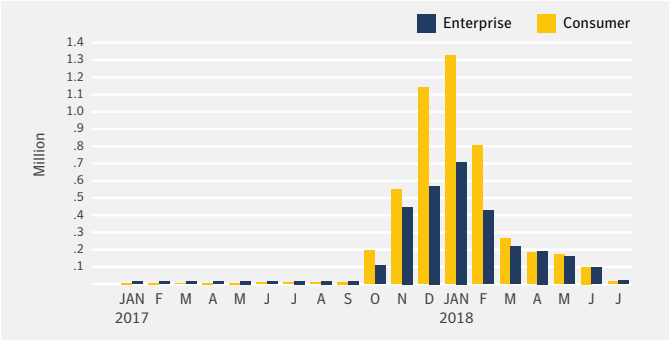
This high level of activity continued into January and February 2018, but activity fell back slightly in March, and fell further in June. However, activity in the space is still extremely strong, with the levels of activity in June on a par with the activity that was taking place last November, and the difference between June 2017 and June 2018, for example, is stark.

Figure 2. All cryptojacking events blocked by Symantec from January 2017 to July 2018



Also interesting is the breakdown of the split between detections on enterprise and consumer machines. When cryptojacking activity was at its height in December, January, and February, these coinminers were being most widely detected on consumer machines—with almost double as many detections of coinminers on consumer machines as enterprise machines in those months. However, since we observed the beginning of a drop in detections in March, detections on consumer and enterprise machines have aligned, with almost the same volume of detections on enterprise machines as consumer machines in the last few months.

Figure 3. Consumer vs enterprise detections of coinminers, January 2017 to July 2018

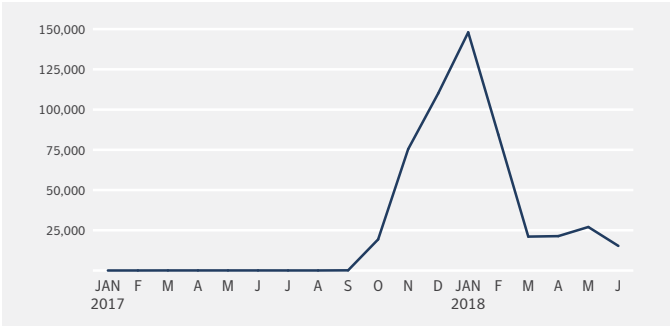


There are a few explanations for this:

- "Fair weather" cryptojacking cyber criminals targeting end-user machines when the value of cryptocurrencies was exceptionally high likely returned to other types of cyber crime once values started to decline
- Some cyber criminals may have simply discontinued their activity once they discovered cryptojacking on end-user machines wasn't as profitable as they thought
- Some cryptojacking cyber criminals are now targeting large corporate networks.

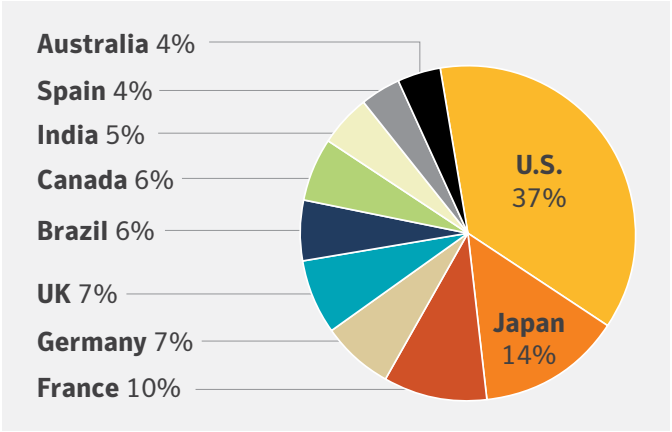
One of the main appeals of browser-based cryptojacking for cyber criminals—that it can take place on even fully patched machines—is highlighted by the fact that Apple Mac operating systems also saw a huge surge in cryptojacking detections towards the end of 2017. We generally see less malicious activity on Macs, so the fact these coinminers could run within browsers and exploit the CPU power of these machines was a big boon to cyber criminals. Cryptojacking detections on Macs reached a peak in January but have fallen back since then.

Figure 4. Endpoint detections of coinminers on Mac computers, January 2017 to July 2018



When we look at the geographic distribution of cryptojacking detections, there does not seem to be a pattern, with the top 10 regions distributed all around the world. Most detections are in the U.S., followed by Japan, and France. This underlines that cryptojacking is a global phenomenon. It is also somewhat unsurprising as, if cyber criminals are embedding these coinminers on a website, they have little control over the geographic locations of those visiting the websites.

Figure 5. Top 10 countries in which cryptojacking activity was blocked, 2017/2018



As we can see from the above statistics, cryptojacking hit the cyber crime landscape at high speed: it was adopted and exploited by cyber criminals so fast that it took a while for both the public and the law to catch up. This allowed cyber criminals to leverage the increased value of cryptocurrencies and the public's interest in them to carry out a variety of scams, some more successful than others. The law, too, has struggled to catch up with this new challenge, though some countries have cracked down harder than others on people engaged in cryptojacking.

Case Studies

Section

03

01 Social scams

As well as turning to cryptojacking, the increasing value and profile of cryptocurrencies also inspired some cyber criminals to try to use social media to make their crypto-currency fortune. The cryptocurrency of choice in these scams seems to mostly be Ethereum, which is one of the other high-profile cryptocurrencies.

These scams are simple and attempt to exploit people's desire to make a quick buck. These scams are primarily carried out on Twitter, and generally follow a similar pattern:

01 Well-known tech/crypto personality sends a tweet.

02 Twitter account impersonating the well-known person comments on the tweet, urging "their" followers to enter an Ether giveaway. However, the rules of the competition generally require individuals to transfer some Ether themselves to enter.

03 This tweet from the fake account is upvoted by bots controlled by the scammer to appear directly beneath the original tweet, so it is seen by more people and seems more legitimate.

04 Any money transferred is never seen by "competition" entrants again.

Among those impersonated in these types of scams were Ethereum founder Vitalik Buterin, and Tesla and SpaceX founder Elon Musk—big names in tech and cryptocurrency seem to be the main targets. It's hard to say how successful these scams have been, but scammers only need a small percentage of them to work to make a profit. These scams have become such an issue that many of those most frequently targeted—including Mr. Buterin—have changed their Twitter handles to include something along the lines of "Not giving away Ether" or "Not doing crypto giveaways." Twitter has recently deleted millions of spammy accounts in an attempt to clean up its platform, but it doesn't seem to have put an end to these scams, as scammers will continue to make new fake accounts to proliferate these scams for as long as they remain profitable. Recent research found at least 15,000 bot accounts engaged in these types of crypto scams over a three-month period.

Quite recently, a scammer impersonating Elon Musk managed to fool some media outlets. In this case, the scammer sent a tweet claiming to be giving away a Tesla Model 3, with several media outlets reporting that Musk was giving away a free car, before numerous people pointed out that the giveaway was a fake.

Another variation of this scam is criminals taking over "verified" Twitter accounts—those with the blue tick—and using them to attempt to carry out similar scams. In a recent case, scammers seized control of the verified Twitter account of a cancelled Fox TV show called *Almost Human*. They then changed the display name (if they had attempted to change the username they would have lost the blue tick) and photo to that of Justin Sun, who is the founder of Chinese blockchain start-up TRON. The account then started tweeting out fake cryptocurrency "giveaway" scams. The account was doing this for several days before it was noticed. Even in this niche space cyber criminals are attempting to innovate, knowing that when people see a blue tick they give a Twitter account more credence. Targeting the account of a cancelled TV show is a smart move, as the account is likely to have many followers, but may not be closely monitored by the company's social media team.

Ethereum founder Vitalik Buterin is frequently targeted by these social media scammers

02 Attacks on enterprises

Symantec researchers recently observed an incident where an enterprise customer was subjected to two waves of attacks that resulted in a Monero coinminer being installed on thousands of machines.

This activity took place in March and April 2018 and particularly targeted the South American offices of a large auto maker. The activity seemed to be either two waves of the same attack or two closely related attacks. The initial infection vector used by the attackers has not been identified, but they did subsequently leverage living-off-the-land tools to spread across the network. They used encoded PowerShell scripts to inject the payloads onto victim machines: the payloads were the Coinreg Monero coinminer (Trojan.Coinreg) and Mimikatz. The attackers obtained valid credentials using Mimikatz, which is a credential-gathering tool, and used them to remotely read and write encrypted payloads to the registry keys of devices on the victim network. It also appears the attacker was uploading stolen information—probably credentials—to the public cloud storage provider Dropbox.

The information linking the two different waves of attacks is that the registry key used to store the payload in the first attack wave matches the XOR decryption key used in PowerShell scripts seen in the second wave.

Registry key value:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SasaiKudasai

XOR decryption key:

s@s@ikud@s@123

It's unclear how much money this campaign may have made for the cyber criminals involved.

WannaMine

Another interesting file-based threat we have seen developed by criminals mining cryptocurrencies is WannaMine. WannaMine derives its name from the WannaCry ransomware and coin mining. Unlike WannaCry, which caused havoc around the world in 2017, it doesn't hold computers to ransom. However, it does use the same network spreading capabilities as WannaCry, namely the EternalBlue exploit. WannaMine (MSH.Bluwimps) was first reported on in October 2017, but started to gain widespread attention in February 2018, following reports of devices being rendered unusable due to the malware causing such high CPU usage.

WannaMine uses a combination of living-off-the-land techniques, such as Windows Management Instrumentation (WMI) and PowerShell, and other malware tactics, such as exploits and credential stealers, to maintain persistence and move laterally from computer to computer. Symantec researchers were able to confirm that it uses an exploit against the Oracle WebLogic Server Remote Security Vulnerability (CVE-2017-10271) as an initial infection vector. Our researchers also found that the criminals behind WannaMine are using the open-source exploit tool JexBoss to identify and exploit vulnerable JBoss servers. Since it was discovered in October 2017, WannaMine has infected more than 75,000 devices.

Another similar threat, Smominru (Trojan.Coinminer.B), which also uses EternalBlue and living-off-the-land techniques to spread, has had more success, with its linked wallet containing more than $1.5 million worth of Monero. Our researchers found that one of the files the threat downloads is a legitimate NVIDIA CUDA component. This component (a runtime library) allows the malware to use the CUDA application programming interface (API) of CUDA-enabled graphics processing units (GPUs), and take advantage of the parallel processing power of the GPUs on infected machines and use it for cryptojacking.

03 Software supply chain attack

Software supply chain attacks are something we have talked about extensively, with a chapter on them featuring in this year's ISTR publication. A recent software supply chain attack was interesting for two reasons: its goal was to install a coinminer on victims' computers, and it was also a software supply chain attack within the supply chain.

Researchers recently wrote about a PDF editor program that was using a compromised font package to install a coinminer on users' computers. However, the plot twist was that the program developer's systems were not compromised. The developer of the PDF program downloads its font packages from another software company, and it was this firm that was breached.

During the PDF editor's installation, the program retrieves the font packages as MSI files from the server of a third-party software developer that offers font packages to multiple companies. The hackers managed to compromise the cloud server infrastructure of the font package supplier. The attackers then copied and hosted all the clean and digitally signed MSI files on a replica server under their control. They changed just one of the files, an Asian fonts pack, adding the coinminer code. "Using an unspecified weakness (which does not appear to be MitM or DNS hijack), the attackers were able to influence the download parameters used by the [PDF editor] app. The parameters included a new download link that pointed to the attacker server," the researchers said. Anyone installing the PDF editor would unknowingly install the font packages from the attackers' server, including the malicious package. The PDF editor is installed on computers under SYSTEM privileges, meaning that the coinminer receives full access to the system.

The incident took place between January and March 2018, but only a small number of users were affected.

04 Long arm of the law

As is often the case with developments in cyber crime, the law is struggling to cope with the speed at which they occur.

However, we have seen some court cases involving defendants who have misused coinminers. One of the countries cracking down the hardest in this area so far is Japan. Recently, the first-ever person sentenced for malicious use of the Coinhive library was sentenced to one year in prison in Japan, although the term was suspended for three years so, provided he stays out of trouble for that time, he will not actually have to go to prison. Masato Yasuda (24) reportedly embedded the Coinhive library inside a game cheat tool he later offered for download. Authorities said the tool was downloaded 90 times and that Yasuda made the equivalent of approximately US$45 in Monero from the con.

Japan seems to be keen to clamp down strongly on cryptojacking, with authorities from 10 prefectures having arrested 16 individuals on suspicion of cryptojacking.

In another case, it was reported that an individual was ordered by the Yokohama Summary Court to pay 100,000 yen (US$905) on charges of illegally storing a computer virus after he was found to be using Coinhive on his website. The defendant in the case is arguing, however, that a browser-based coinminer is not a virus as it operates in a similar manner to online advertisements. He is appealing the ruling.

Other criminal cases

While prosecutions related to cryptojacking are relatively new, we have seen prosecutions of people who use cryptocurrencies to carry out money laundering or other illegal activities:

- Included in an indictment against 12 Russian intelligence agents alleged to have hacked Hillary Clinton's presidential campaign is a charge of conspiracy to commit money laundering, as they allegedly used Bitcoin to launder payments.

- In another case, a woman dubbed the "Bitcoin Maven" was sentenced to a year and a day in federal prison for illegally laundering the cryptocurrency. Theresa Tetley, who resided in Southern California, was a former stockbroker who prosecutors said laundered millions of dollars for clients through an unlicensed Bitcoin-for-cash service. She pleaded guilty to money laundering and operating an unlicensed money transmitting business. As well as a prison sentence she was also fined $20,000 and ordered to forfeit 40 bitcoins, about $292,000 in cash, and 25 gold bars.
- Meanwhile in China, cops shut down a World Cup betting ring that was hosting $1.5 billion in cryptocurrency bets. The platform operated on the dark web and used only Bitcoin, Ethereum, and Litecoin. It had been operating for eight months and had 30,000 users worldwide. China does not take a friendly view of cryptocurrencies, attempting to ban many of them, as well as banning initial coin offerings (ICOs).

The Future of Cryptojacking

Section

04

The Future of Cryptojacking

The sustainability of this huge growth in cryptojacking is something we pondered in the ISTR. We said then that "The longevity of this activity very much depends on the future value of these cryptocurrencies." This seems to have been borne out, with the drop in cryptojacking activity coinciding with the decreasing value of Monero.

Questions have been asked recently as to whether cryptojacking has reached its peak, and if we are likely to see cyber criminals returning to other threats, such as ransomware and financial Trojans. The answer to this is probably a partial yes. The drop in activity indicates that some cyber criminals have stopped cryptojacking, or at the very least reduced the effort they were putting into it. A few factors may have contributed to this decrease in activity:

- The drop in value of cryptocurrencies
- The level of scale required to make a decent profit
- Security companies such as Symantec introducing better detections for these coinminers as the threat increased

However, cryptojacking is far from dropping off cyber criminals' radar. In July 2018, a massive campaign targeted more than 200,000 MiKroTik routers and altered the traffic passing through the routers in order to inject a copy of the Coinhive library inside all the pages served through the router—allowing them to infect a huge amount of web traffic. This shows that while overall activity may have decreased, cyber criminals are still innovating in this space.

The increased profile of coin mining and cryptocurrencies also means they have come to the attention of law enforcement and officials. "The Future of Digital Currency" was recently discussed by the House Financial Service Committee in the U.S. Congress, with one of the participants—Representative Brad Sherman—suggesting that "We should prohibit U.S. persons from buying or mining cryptocurrencies."

It is unlikely the U.S. would implement such an outright ban, although other countries, including China and India, have implemented laws cracking down on cryptocurrency trading. However, it is likely that regulations and scrutiny in the area of cryptocurrencies will continue to increase.

Such factors may discourage the wide adoption of cryptojacking by cyber criminals that was observed late in 2017, but cryptojacking is still one of the main threats we are seeing in the cyber security landscape. Once some groups of cyber criminals find they are still able to make money in this area it is likely to be something that will continue to cause headaches for internet users for some time to come.

The sustainability of this huge growth in cryptojacking is something we pondered in the ISTR. We said then that "The longevity of this activity very much depends on the future value of these cryptocurrencies." This seems to have been borne out, with the drop in cryptojacking activity coinciding with the decreasing value of Monero.

Best Practices

Section

05

Best Practices

- Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single point failures in any specific technology or protection method. This includes deployment of endpoint, email, and web gateway protection technologies as well as firewalls and vulnerability assessment solutions. Always keep these security solutions up to date with the latest protection capabilities.
- Educate anyone using your device or network and urge them to exercise caution around emails from unfamiliar sources and around opening attachments that haven't been solicited, which may contain file-based coin-mining malware.
- Consider installing ad-blocking or anti-coin-mining extensions on web browsers for an extra layer of protection against potentially unwanted applications (PUAs).
- Only visit websites that you trust and watch out for any small print on the website that may indicate it is running a coinminer.
- Be wary of clicking on ads for unfamiliar websites and when downloading apps to your phone. Mobile phones can be used for mining cryptocurrency too. Use the same caution when downloading browser extensions.
- Educate employees about the signs that indicate their computer may have a coinminer and instruct them to inform IT immediately if they think there may be a coinminer on a device that is on the company network.
- Monitor battery usage on your device and, if you notice a suspicious spike in usage, scan it for the presence of any file-based miners. If that fails to show anything then take note of the websites you had open when the spike in battery usage occurred.
- Install the latest patches on your devices, use strong passwords and enable two-factor authentication.
- Ensure your router, and all IoT devices, are fully patched and the firmware is up to date.
- Monitor network logs (IPS logs, DNS logs, firewall logs) for suspicious outgoing connections to mining-related IP addresses. Block these addresses at the corporate firewall and consider suspicious any computer that continues to access those addresses.
- Lock down RDP access and frequently replace all user passwords—especially users with admin access—with new, strong passwords.
- Run a recent release of PowerShell (5 or higher) and configure it to log detailed activity.
- Secure your computers' built-in Windows Management Instrumentation (WMI). Attackers, including those seeking to mine coins, increasingly abuse this technology. Administrators should consider creating Group Policy Objects (GPO) or firewall rules to prevent unauthorized remote WMI actions, and perhaps control access by user accounts.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

More Information

Symantec Worldwide: http://www.symantec.com

ISTR and Symantec Intelligence Resources: https://www.symantec.com/security-center/threat-report

Symantec Security Center: https://www.symantec.com/security-center

Norton Security Center: https://us.norton.com/security-center

Symantec

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

Symantec.com

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

09/18