SOPHOS
Security made simple.

Standing Up to CRYPTOJACKING

Best Practices for Fighting Back

Cryptojacking has recently erupted onto the cybercrime scene, thanks to the surge in value during 2017 of cryptocurrencies such as Bitcoin, Monero, and Ethereum.

Crooks are aggressively targeting laptops, desktops, servers, and even mobile devices. From a single device to entire networks, they infect as many devices as they can to mine for cryptocurrency on, or while using, other people's computers. Simply put, you do the work, pay for the electricity and hardware, and they pocket the rewards.

Read this paper to learn how to fight back! We'll explore the differences between legitimate mining and cryptojacking; how cryptojacking works; the costs of cryptojacking to today's organizations; and practical steps you can take to avoid being a victim of cryptojacking.

A Sophos Whitepaper March 2018

Setting the stage

Cryptomining and cryptojacking are two terms that are commonly used when discussing this topic. Let's start by quickly distinguishing between the two.

Cryptomining is the act of doing all the necessary – and quite frankly very complex – effort required to generate and work with cryptocurrency. It can be both legitimate or malicious, which is determined by several factors, most significantly whether you consciously agree to it.

Cryptojacking is malicious cryptomining. The crooks get code onto your devices without your permission to mine for cryptocurrency using your equipment and your resources. They keep all the proceeds themselves while you get nothing for your hard work.

A common misconception is that the sole purpose of **miners** is to generate cryptocurrency. It's true, this is part of the job. However, they also have another role that is at least equally as important: validating transactions on the blockchain.

To explain **blockchains**, let's use banks as an analogy as cryptocurrency is attempting to replace traditional currency. Usually, banks are in charge of keeping accurate records of transactions. In cooperation with governments, banks ensure that money isn't created out of thin air, and that people don't cheat and spend their money more than once. Blockchains are responsible for the same duties, but also introduce a new way of record-keeping. With a blockchain the entire network, rather than an intermediary or individual, verifies transactions and adds them to the public ledger.

Although a 'trustless' or 'trust-minimizing' monetary system is one of the goals for cryptocurrency, the financial records need to be secured, and the system must ensuring that no one cheats. The miners who work on the blockchain come to a consensus about the transaction history while preventing fraud, notably the double spending of cryptocurrency.

All of this sounds quite complex, and it is. However, there are some basic principles that, once understood, provides you with the ability to understand why cryptojacking has exploded as a trend. Let's start by looking at what it takes to perform legitimate mining and later learn the differences between legitimate and malicious mining.

How to be a cryptominer in four easy steps

Before you can start being a miner for a cryptocurrency, there are a few things you need to consider:

- **Hardware.** Regardless of whether you are a casual miner or you're making mining your full-time profession, your objective is to make money. To mine you need hardware, which clearly has an associated cost. For the casual miner, you may choose to use your gaming or personal machine as it is not being used most of the time.

  If you're more serious, you can spend a considerable amount of money on customized cryptomining hardware. If you're not buying dedicated hardware for mining, the next most efficient way of mining is by chaining together multiple graphics processing units (GPU). This is your traditional graphics card, and miners prefer the high-end kind and they are not cheap. Why a GPU? Because GPUs are efficient at performing the mathematical calculations that are necessary to work on the blockchain.

  The market has already reached the point that it is almost impossible for gamers (not miners) to buy high-end graphics cards because the miners are eating up the supply as soon as it is available. Nvidia has already taken the unprecedented step of asking retailers to stop selling their cards to miners and focus on selling to gamers*. The big question is, if mining is all about making money, how long is it going to take you to recoup your initial investment?

- **Ongoing investment.** Over time all computer equipment gets faster and more efficient. The older your hardware, the slower it becomes in comparison to new hardware. Also, the bigger the hardware, the more electricity it will consume. Ongoing costs associated with running and maintaining your hardware will apply just like in a traditional business, but with cryptomining they can be considerable. The old statement "you need to spend money to make money" is very true here.

- **Pools.** As a single casual miner working on your own you would need to be incredibly lucky to successfully mine just one unit of cryptocurrency. Your chances are slim to none. So, what's the answer? Pool your resources with those from other devices to create a "pool" with the computational power of all combined resources. The chances of successfully mining cryptocurrency increases with the size and computational power of the pool.

Pools are an important concept to understand for both legitimate and malicious mining operations. When you are running a mining application, are you a member of a legitimate or malicious pool? Obviously, both want their pools to be as big as possible as it increases computational power and the chances of successfully mining cryptocurrency. The big difference is how it pays out. While the legitimate pools will have an agreed method for splitting the proceeds amongst all members, the malicious pools usually only provide the proceeds to a single entity (namely the crook). Different pools have different payment structures and many will payout proportionally compared to how much you worked.

**https://wccftech.com/nvidia-instructs-retailers-stop-selling-miners-sell-gamers/*

Now that you've got your hardware and a basic understanding of pools, you can begin mining. And legitimate mining is really just like working any other kind of job. There are four basic steps to make money from mining cryptocurrencies:

Step 1: Find a job!

This is known as joining a pool. You find a pool that is going to pay you a decent return for what you invest in time, computational power, and ongoing running costs. It's essentially finding out what people are going to pay you for your work.

Step 2: Create a wallet.

After you have a job, you obviously want to be paid. Any proceeds you receive from mining need to go into a wallet. A wallet can be on an exchange, in software (i.e. a file on your device) or secured in hardware. The hardware option is the most secure and recommended option as it is harder to steal.

Step 3: Start working...

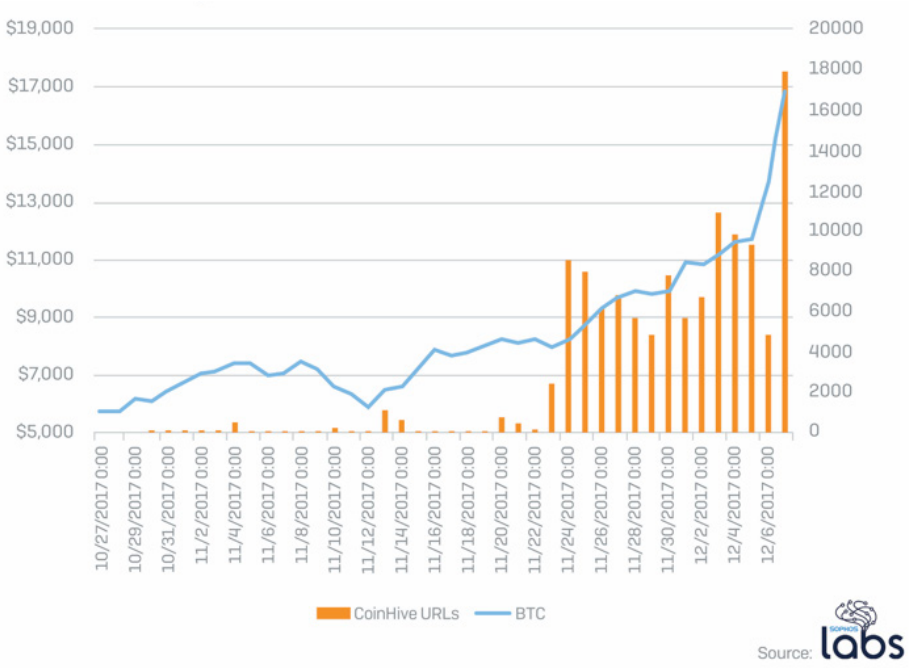
Next step, you need to find the mining program of your choice. There are many different options available depending on the cryptocurrency you are mining, and the specific type of GPU in your device. Then you have to start it. Don't bother sitting and watching it because it's just a command line and you'll grow bored very quickly. It is a "set and forget" type of operation.

Step 4. Get paid.

Now sit back, watch the power bill grow, hope your machine doesn't overheat and cross your fingers that you've joined a legitimate pool and will get paid... Generally, pools have an agreed-upon payment period. Ongoing costs associated with running and maintaining your hardware will apply just like in a traditional business, but with cryptomining they can be considerable, just like a real job. At that point in time they will divide the proceeds from the pool amongst all members of the pool in the agreed-upon fashion.

The difference between legitimate and malicious mining

The basic difference is intent. Legitimate and malicious mining are the same in almost every sense except who gets paid and whether the person who owns the device performing the mining willingly chooses to participate. It's easy to understand the concept of the crooks wanting you to do the hard work and they take all the proceeds. That's why cryptojacking has exploded with the growth in the value of cryptocurrencies in the market. Crooks see an opportunity to make "free money" off the back of your hard work. And how do they achieve this? They manage to get cryptomining code onto your device, and without your permission and knowledge, immediately set your device working as a part of their malicious pool.



As previously stated, they want their pool to be as large as possible to increase the chance of them successfully mining cryptocurrency. The more they mine, the more they make. So, they set to work in an attempt to infect as many devices as possible and enslave them into the cryptojacking trade.

The many faces of cryptojacking

Malicious JavaScript miners

Malicious JavaScript miners are the quick and easy way for crooks to enslave a large number of devices. The logic is pretty simple: what do most people do on a regular basis? They browse the web.

By turning every browser that goes to a website into a worker the crooks can very quickly add lots of devices to a malicious mining pool. If you're a cryptojacker, it's brilliant: someone else does the work, you use their resources, and you get all the proceeds for yourself.

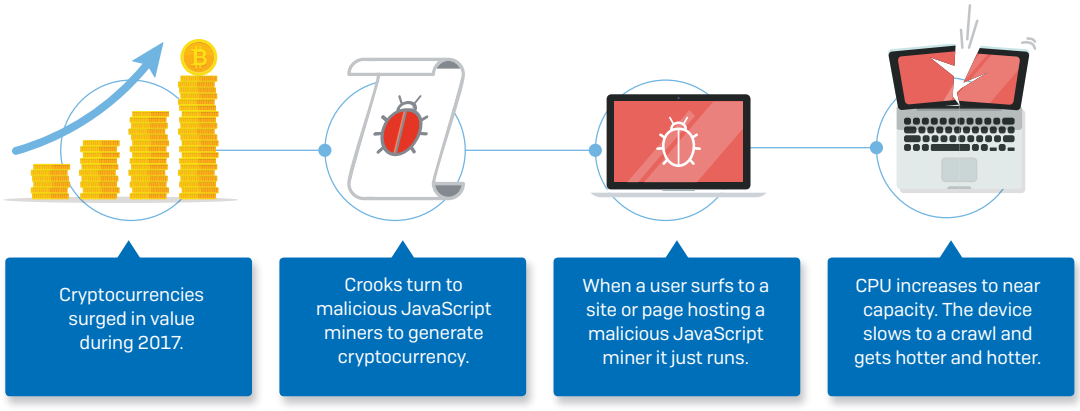
Now, ask yourself how many devices have a browser that can run JavaScript? It's a mind-bendingly large number. Every laptop, desktop, mobile device (phone and tablet), servers, and other devices are the potential victims. And as the crooks have access to a large number of compromised websites, the chances that they will get devices with a browser running the JavaScript miner are very high.

JavaScript miners are transient miners, as your browser may only perform the mining tasks for a short period of time. The mining stops when you close the browser or the tab that is viewing the infected website, so it is in theory easy to stop. However, how often do you actually close your browser, or is it always running the background?

When a user surfs to a site or page hosting a malicious JavaScript miner, they are not asked for permission to run the JavaScript miner – it just runs. Around this time the CPU on the device will increase to near maximum capacity and the device will slow to a crawl. **The more a processor works, the more electricity it consumes, the hotter it gets.** Mobile devices can rise to "cooking temperatures" and mining can drain a battery quickly, even leading to battery expansion and device destruction.

Some of these JavaScript miners are smart and have the ability to limit their CPU usage, enabling them to remain hidden for longer. The longer they can hide and execute, the more work they perform for the crooks and their malicious pool. Even though a mobile device is not the most efficient miner, the crooks will take every piece of computational power they can grab!

Some JavaScript miners are smart enough to know that they are on a mobile device and only really go into full blown mining when they are attached to power and stays relatively dormant when operating on the battery. That way the user doesn't notice a suspiciously large drop in battery performance – again so they can remain unnoticed for longer. Also, most people don't pay attention to their phones if they have them plugged in and charging. This works better on a mobile device because people don't close the browser on their mobile device – they mainly have it in the background as they swap to different apps.



The grey zone of cryptominers

The grey zone is where a legitimate website uses JavaScript miners as 'payment' for people visiting their site.

With the increasing use of adBlockers many sites are no longer making as much advertising money as they would like, so they are giving people a choice: either disable the adBlocker and get all those annoying and persistent ads, or agree to allowing the website to turn your device into a cryptomining slave. The ethical aspects of this seemingly innocent act are not discussed in this whitepaper; however, in the opinion of Sophos, it falls between the categories of legitimate and malicious, but definitely more towards the malicious side.

Native Code Attacks

Native code attacks are nothing new and native code cryptominers are a particularly nasty example of an infection. The crooks will initially infect and exploit your devices using traditional malware means and then secretly install cryptomining software and set your device to work.

Cryptojacking malware can be incredibly persistent. Remember that the longer your device acts as a member of the crook's malicious pool the more money they can potentially make. They are similar to their ransomware cousins because they use the same type of exploits and infection mechanisms to not only initially infect a device, but laterally move across the network and infect as many devices as possible. Namely, they use the EternalBlue and Mimikatz exploits. But unlike their ransomware cousins, which are "in your face," cryptojacking malware will remain hidden as long as possible.

But they get worse. They will also remove any other mining software they find because they want all your resources to themselves. If they want to mine as efficiently as possible it's not smart to share the resources they've just stolen with someone else. They will also download the most efficient miner for the device they've just infected. That means determining if it is a 32- or 64-bit system and the operating system that it is running. The most common variants found here run on Windows, macOS, and Linux.

If that's not enough, they also install a Remote Access Trojan (RAT). That means the crooks can not only run invisibly on your device, they also have complete control. They can delete and modify files, upload and download files, and install other malware. Realizing that you have cryptojacking malware on one or more devices is a concern. The mining software may be the least of your problems as you don't know how they got in, what else they have done, or what other devices they have infected with cryptojacking or other malware.

The longer cryptomining malware can stay hidden, the more processing power the crooks can steal from you and the more cryptocurrency they can make.

Native Code Attacks on Mobile Devices

In addition to the native code attacks on Windows, macOS, and Linux, SophosLabs has also seen an increased presence of mining functionality in native mobile apps, primarily on Android devices. This can happen in one of two ways:

1. The mobile app explicitly includes mining code
2. Popular apps have been modified to include mining code and have been downloaded from non-standard app stores

The basic concept is the same: get mining code onto a device and enslave the device mining cryptocurrency for the crooks. Obviously native apps on mobile devices perform significantly better than JavaScript in a mobile browser. Thankfully with standard mobile management technology it is relatively easy for an IT administrator to block both types of mobile apps.

The business implications of cryptojacking

Cryptojacking might sounds relatively harmless at first – it doesn't need to read your personal data, or even to access to your file system. However, the downsides are still very significant:

1. **Unbudgeted operating expenses** from powering computers to work for someone else.
2. **Opportunity costs** because legitimate works gets slowed down. You think your computer is slow now, wait until you get cryptomining software on it!
3. **Security risks** from who-knows-what untrusted programs and network connections.
4. **Reputational and regulatory costs** of reporting, investigating and explaining the cryptomining activity.
5. **Ethical concerns** of allowing employees to mine using your resources.

Those risks are real, and you need to decide if your business can afford to ignore these risks. Your business needs to form an opinion on what is your policy on cryptomining. While the view on cryptojacking is simple – it should never be allowed – the view on legitimate mining varies from business to business.

Some companies will allow legitimate mining on company resources. Others will not. Again, there is an ethical component of allowing employees to use company resources, including the hardware, electricity, and ongoing running costs to perform legitimate cryptomining. You can also ask yourself: does this make the employee the bad guy?

Expanding the discussion on legitimate vs. malicious mining

Of course, not all cryptomining is cryptojacking; some is legitimate. However, from an IT perspective, it can be almost impossible to distinguish between them. For example, it's possible for a crook to turn a legitimate mining program into a malicious one simply by changing a config file. The owner won't notice that their resources have been "stolen" until they don't get paid. Also, how can you block malicious cryptojacking versus legitimate mining if they look the same?

This quote from Joe Levy, CTO at Sophos, reflects the subtlety of the situation and the Sophos position:

"In the absence of a reliable way to differentiate between consensual and non-consensual mining, the bad apples ruin the good ones."

Given the security, reputational, and regulatory issues that in-house cryptomining poses to a business, and the difficulty in distinguishing between legitimate vs. malicious mining, Sophos strongly advises that that your default position should be to stop it.

Fighting back against cryptojacking

When it comes to stopping cryptojacking there is no silver bullet. Just like protecting yourself against ransomware, you need to take a layered approach to protection.

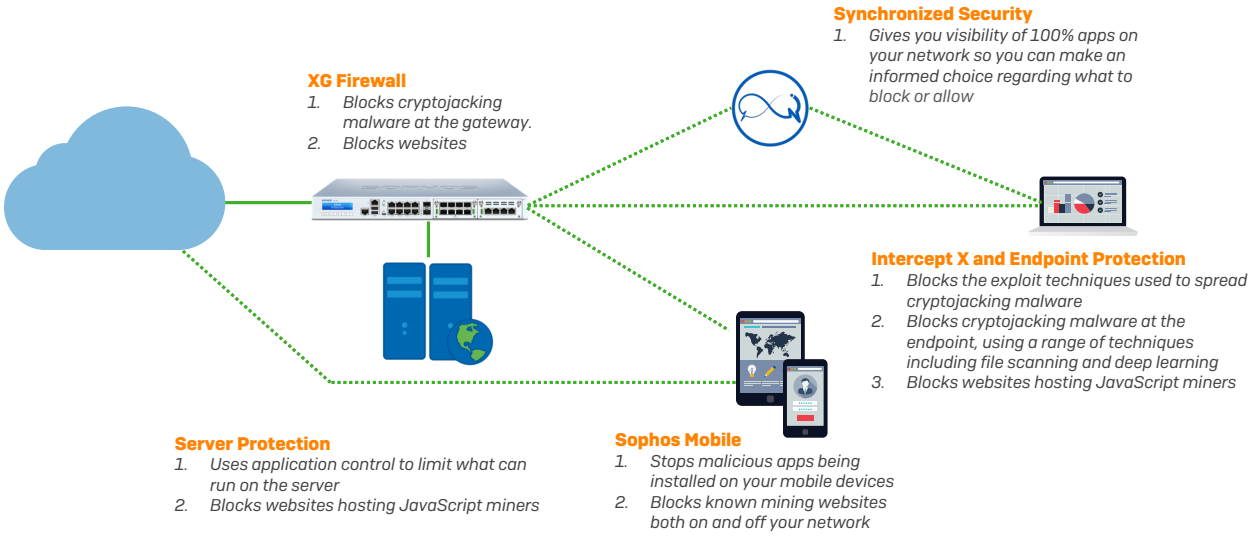
1. **Block websites hosting JavaScript miners** both at the gateway and the endpoints
2. **Stop cryptomining malware** at every point in the attack chain
3. **Prevent cryptomining apps** from running on your network

We also recommend that you:

- Keep your devices patched to minimize the risk of exploit-related attacks
- Use mobile management technology to ensure that native mobile apps aren't present on your mobile phones nor tablets
- Educate your team:
  - Cryptomining is **not** an acceptable use of company resources or power
  - Explain traditional attack vectors of malware such as phishing and how they can protect themselves
- Maintain a strong password policy
- Keep an eye out for the tell-tale signs that you've been cryptojacked:
  - Slow network
  - Soaring electricity bill
  - Spike in CPU consumption

How Sophos can help

Sophos offers a range of technologies to protect you at every point in the attack chain.



Try for yourself, for free at www.sophos.com/freetrials.

- **Sophos Central** gives you Intercept X, Endpoint, Server, and Mobile protection, all managed through a single, intuitive console.
- **Sophos XG Firewall**, our NSS Labs-recommended appliance. You can run it in-line with your current appliance and see the difference.

Further reading

For more information on cryptomining from Sophos threat experts, check out the Sophos Naked Security blog at https://nakedsecurity.sophos.com/.

Sophos customers can also visit the Knowledge Base for information on how to block and authorize JavaScript cryptominers in Sophos products.

- Block JavaScript Cryptominers
- Authorize JavaScript Cryptominers
- SophosLabs whitepaper on cryptomining on mobile devices.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2018-02-28 WP-NA (MP)