**Cryptojacking definition**

Cryptojacking is the unauthorized use of someone else’s computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim’s browser.

[ How much does a cyber attack really cost? [Take a look at the numbers](https://www.csoonline.com/article/3110756/a-deeper-look-at-business-impact-of-a-cyberattack). | Get the latest from CSO by [signing up for our newsletters](http://www.csoonline.com/newsletters/signup.html#tk.cio_fsb). ]

Either way, the cryptomining code then works in the background as unsuspecting victims use their computers normally. The only sign they might notice is slower performance or lags in execution.

**How cryptojacking works**

Hackers have two primary ways to get a victim’s computer to secretly mine cryptocurrencies. One is to trick victims into loading cryptomining code onto their computers. This is done through phishing-like tactics: Victims receive a legitimate-looking email that encourages them to click on a link. The link runs code that places the cryptomining script on the computer. The script then runs in the background as the victim works.

The other method is to inject a script on a website or an ad that is delivered to multiple websites. Once victims visit the website or the infected ad pops up in their browsers, the script automatically executes. No code is stored on the victims’ computers. Whichever method is used, the code runs complex mathematical problems on the victims’ computers and sends the results to a server that the hacker controls.

Hackers often will use both methods to maximize their return. “Attacks use old malware tricks to deliver more reliable and persistent software [to the victims’ computers] as a fall back,” says Alex Vaystikh, CTO and cofounder of SecBI. For example, of 100 devices mining cryptocurrencies for a hacker, 10% might be generating income from code on the victims’ machines, while 90% do so through their web browsers.

Some cryptomining scripts have worming capabilities that allow them to infect other devices and servers on a network. It also makes them harder to find and remove; maintaining persistence on a network is in the cryptojacker's best financial interest.

To increase their ability to spread across a network, cryptomining code might include multiple versions to account for different architectures on the network. In one example described in an [AT&T Alien Labs blog post](https://cybersecurity.att.com/blogs/labs-research/att-alien-labs-analysis-of-an-active-cryptomining-worm), the cryptomining code simply downloads the implants for each architecture until one works.

**[**[**Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!**](https://pluralsight.pxf.io/c/321564/424552/7490?u=https%3A%2F%2Fwww.pluralsight.com%2Fpaths%2Fcertified-information-systems-security-professional-cisspr)**]**

The scripts might also check to see if the device is already infected by competing cryptomining malware. If another cryptominer is detected, the script disables it. A cryptominer might also have a kill prevention mechanism that executes every few minutes, as the AT&T Alien Lab post notes.

Unlike most other types of malware, cryptojacking scripts do no damage to computers or victims’ data. They do steal CPU processing resources. For individual users, slower computer performance might be just an annoyance. Organization with many cryptojacked systems can incur real costs in terms of help desk and IT time spent tracking down performance issues and replacing components or systems in the hope of solving the problem.

**Why cryptojacking is popular**

No one knows for certain how much cryptocurrency is mined through cryptojacking, but there’s no question that the practice is rampant. Browser-based cryptojacking grew fast at first, but seems to be tapering off, likely because of cryptocurrency volatility and the closing of Coinhive, the most popular JavaScript miner that was also used for legitimate cryptomining activity, in March 2019. [The 2020 SonicWall Cyber Threat Report](https://www.sonicwall.com/2020-cyber-threat-report/#threat-report-form) reveals that the volume of cryptojacking attackes fell 78% in the second half of 2019 as a result of the Coinhive closure.

The decline began earlier, however. [Positive Technology's Cybersecurity Threatscape Q1 2019](https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q1/) report shows that cryptomining now accounts for only 7% of all attacks, down from 23% in early 2018. The report suggests that cybercriminals have shifted more to ransomware, which is seen as more profitable.

“Cryptomining is in its infancy. There’s a lot of room for growth and evolution,” says Marc Laliberte, threat analyst at network security solutions provider WatchGuard Technologies.

In January 2018, [researchers discovered the Smominru cryptomining](https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators) botnet, which infected more than a half-million machines, mostly in Russia, India, and Taiwan. The botnet targeted Windows servers to mine Monero, and cybersecurity firm Proofpoint estimated that it had generated as much as $3.6 million in value as of the end of January.

Cryptojacking doesn’t even require significant technical skills. According to the report, [The New Gold Rush Cryptocurrencies Are the New Frontier of Fraud](https://info.digitalshadows.com/TheNewGoldRush-CryptocurrencyResearch-Website.html), from Digital Shadows, cryptojacking kits are available on the [dark web](https://www.csoonline.com/article/3249765/data-breach/a-newcomers-guide-to-the-dark-web.html) for as little as $30.

The simple reason why cryptojacking is becoming more popular with hackers is more money for less risk. “Hackers see cryptojacking as a cheaper, more profitable alternative to ransomware,” says Vaystikh. WIth ransomware, a hacker might get three people to pay for every 100 computers infected, he explains. With cryptojacking, all 100 of those infected machines work for the hacker to mine cryptocurrency. “[The hacker] might make the same as those three ransomware payments, but cryptomining continuously generates money,” he says.

The risk of being caught and identified is also much less than with ransomware. The cryptomining code runs surreptitiously and can go undetected for a long time. Once discovered, it’s very hard to trace back to the source, and the victims have little incentive to do so since nothing was stolen or encrypted. Hackers tend to prefer [anonymous cryptocurrencies like Monero and Zcash](https://www.csoonline.com/article/3252233/cyber-attacks-espionage/new-cryptocurrencies-offer-better-anonymity-new-security-challenges.html) over the more popular Bitcoin because it is harder to track the illegal activity back to them.

**Real-world cryptojacking examples**

Cryptojackers are a clever lot, and they’ve devised a number of schemes to get other peoples’ computers to mine cryptocurrency. Most are not new; cryptomining delivery methods are often derived from those used for other types of malware such as ransomware or adware. "You’re starting to see a lot of the traditional things mal-authors have done in the past," says Travis Farral, director of security strategy at Anomali. "Instead of delivering ransomware or a Trojan, they are retooling that to deliver crypto-mining modules or components."

Here are some real-world examples:

**Spear-fishing PowerGhost steals Windows credentials**

The Cyber Threat Alliance's (CTA's) [The Illicit Cryptocurrency Mining Threat report](https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf) describes PowerGhost, first analyzed by Fortinet, as stealthy malware that can avoid detection in a number of ways. It first uses spear phishing to gain a foothold on a system, and it then steals Windows credentials and leverages Windows Management Instrumentation and the EternalBlue exploit to spread. It then tries to disable antivirus software and competing cryptominers.

**Graboid, a cryptominder worm spread using containers**

In October, Palo Alto Networks released a [report](https://unit42.paloaltonetworks.com/graboid-first-ever-cryptojacking-worm-found-in-images-on-docker-hub/) describing a cryptojacking botnet with self-spreading capabilities. Graboid, as they named it, is the first known cryptomining worm. It spreads by finding Docker Engine deployments that are exposed to the internet without authentication. Palo Alto Networks estimated that Graboid had infected more than 2,000 Docker deployments.

**Malicious Docker Hub accounts mine Monero**

In June 2020, Palo Alto Networks [identified a cryptojacking scheme](https://unit42.paloaltonetworks.com/cryptojacking-docker-images-for-mining-monero/) that used Docker images on the Docker Hub network to deliver cryptomining software to victims' systems. Placing the cryptomining code within a Docker image helps avoid detection. The infected images were accessed more then two million times, and Palo Alto estimates that the cryptojackers realized $36,000 in ill-gotten gains.

**MinerGate variant suspends execution when victim's computer is in use**

According to the CTA report, Palo Alto Networks has analyzed a variant of the MinerGate malware family and found an interesting feature. It can detect mouse movement and suspend mining activities. This avoids tipping off the victim, who might otherwise notice a drop in performance.

**BadShell uses Windows processes to do its dirty work**

A few months ago, Comodo Cybersecurity found malware on a client's system that used legitimate Windows processes to mine cryptocurrency. Dubbed BadShell it used:

* PowerShell to execute commands--a PowerShell script injects the malware code into an existing running process.
* Task Scheduler to ensure persistence
* Registry to hold the malware's binary code

You can find more details on how BadShell works in [Comodo's Global Threat Report Q2 2018 Edition.](https://www.comodo.com/public/report/global-threat-report-communications.php?track=14303&af=14303)

**Rogue employee commandeers company systems**

At the EmTech Digital conference earlier this year, Darktrace told the [story of a client](https://www.technologyreview.com/s/610636/this-security-firm-found-rogue-crypto-mining-infecting-1000-customers/?utm_source=twitter.com&utm_medium=social&utm_content=2018-03-27&utm_campaign=Technology+Review), a European bank, that was experiencing some unusual traffic patterns on its servers. Night-time processes were running slowly, and the bank’s diagnostic tools didn’t discover anything. Darktrace discovered that new servers were coming online during that time—servers that the bank said didn’t exist. A physical inspection of the data center revealed that a rogue staffer had set up a cryptomining system under the floorboards.

**Serving cryptominers through GitHub**

In March, Avast Software reported that cryptojackers were [using GitHub as a host for cryptomining malware](https://blog.avast.com/greedy-cybercriminals-host-malware-on-github). They find legitimate projects from which they create a forked project. The malware is then hidden in the directory structure of that forked project. Using a phishing scheme, the cryptojackers lure people to download that malware through, for example, a warning to update their Flash player or the promise of an adult content gaming site.

**Exploiting an rTorrent vulnerability**

Cryptojackers have discovered an rTorrent misconfiguration vulnerability that leaves some rTorrent clients accessible without authentication for XML-RPC communication. They scan the internet for exposed clients and then deploy a Monero cryptominer on them. [F5 Networks reported this vulnerability](https://f5.com/labs/articles/threat-intelligence/malware/rtorrent-client-exploited-in-the-wild-to-deploy-monero-crypto-miner) in February, and advises rTorrent users to make sure their clients do not accept outside connections.

**Facexworm: Malicious Chrome extension**

This malware, first discovered by Kaspersky Labs in 2017, is a Google Chrome extension that uses Facebook Messenger to infect users’ computers. Initially Facexworm delivered adware. Earlier this year, [Trend Micro found](https://blog.trendmicro.com/trendlabs-security-intelligence/facexworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/) a variety of Facexworm that targeted cryptocurrency exchanges and was capabile of delivering cryptomining code. It still uses infected Facebook accounts to deliver malicious links, but can also steal web accounts and credentials, which allows it to inject cryptojacking code into those web pages.

**WinstarNssmMiner: Scorched earth policy**

In May, [360 Total Security identified a cryptominer](https://blog.360totalsecurity.com/en/cryptominer-winstarnssmminer-made-fortune-brutally-hijacking-computer/) that spread quickly and proved effective for cryptojackers. Dubbed WinstarNssmMiner, this malware also has a nasty surprise for anyone who tried to remove it: It crashes the victim’s computer. WinstarNssmMiner does this by first launching an svchost.exe process and injecting code into it and setting the spawned process’s attribute to CriticalProcess. Since the computer sees as a critical process, it crashes once the process is removed.

**CoinMiner seeks out and destroys competitors**

Cryptojacking has become prevalent enough that hackers are designing their malware to find and kill already-running cryptominers on systems they infect. CoinMiner is one example.

According to Comodo, CoinMiner checks for the presence of an AMDDriver64 process on Windows systems. Within the CoinMiner malware are two lists, $malwares and $malwares2, which contain the names of processes known to be part of other cryptominers. It then kills those processes.

**Compromised MikroTik routers spread cryptominers**

[Bad Packets reported](https://badpackets.net/200000-mikrotik-routers-worldwide-have-been-compromised-to-inject-cryptojacking-malware/#more-1630) in September last year that it had been monitoring over 80 cryptojacking campaigns that targeted MikroTik routers, providing evidence that hundreds of thousands of devices were compromised. The campaigns exploited a known vulnerability ([CVE-2018-14847)](https://nvd.nist.gov/vuln/detail/CVE-2018-14847) for which MikroTik had provided a patch. Not all owners had applied it, however. Since MikroTik produces carrier-grade routers, the cryptojacking perpetrators had broad access to systems that could be infected.

**How to prevent cryptojacking**

Follow these steps to minimize the risk of your organization falling prey to cryptojacking:

**Incorporate the cryptojacking threat into your**[**security awareness training**](https://www.csoonline.com/article/2133408/data-protection/network-security-the-7-elements-of-a-successful-security-awareness-program.html)**, focusing on phishing-type attempts to load scripts onto users’ computers.** “Training will help protect you when technical solutions might fail,” says Laliberte. He believes phishing will continue to be the primary method to deliver malware of all types.

Employee training won’t help with auto-executing cryptojacking from visiting legitimate websites. “Training is less effective for cryptojacking because you can’t tell users which websites not to go to,” says Vaystikh.

**Install an ad-blocking or anti-cryptomining extension on web browsers.** Since cryptojacking scripts are often delivered through web ads, installing an ad blocker can be an effective means of stopping them. Some ad blockers like Ad Blocker Plus have some capability to detect cryptomining scripts. Laliberte recommends extensions like [No Coin](https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl?hl=en) and [MinerBlock](https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl?hl=en" \t "_blank), which are designed to detect and block cryptomining scripts.

**Use endpoint protection that is capable of detecting known crypto miners.** Many of the endpoint protection/antivirus software vendors have added crypto miner detection to their products. "Antivirus is one of the good things to have on endpoints to try to protect against cryptomining. If it’s known, there’s a good chance it will be detected," says Farral. Just be aware, he adds, that crypto minor authors are constantly changing their techniques to avoid detection at the endpoint.

**Keep your web filtering tools up to date.** If you identify a web page that is delivering cryptojacking scripts, make sure your users are blocked from accessing it again.

**Maintain browser extensions**. Some attackers are using malicious browser extensions or poisoning legitimate extensions to execute cryptomining scripts.

**Use a mobile device management (MDM) solution to better control what’s on users’ devices.** Bring-your-own-device (BYOD) policies present a challenge to preventing illicit cryptomining. “MDM can go a long way to keep BYOD safer,” says Laliberte. An MDM solution can help manage apps and extensions on users’ devices. MDM solutions tend to be geared toward larger enterprises, and smaller companies often can’t afford them. However, Laliberte notes that mobile devices are not as at risk as desktop computers and servers. Because they tend to have less processing power, they are not as lucrative for the hackers.

None of the above best practices are foolproof. In recognition of that, and the growing prevalence of cryptojacking, cyber risk solution provider Coalition now offers service fraud insurance coverage. According to a [press release](https://www.thecoalition.com/announcements/coalition-introduces-service-fraud-coverage-2018-08-22), it will reimburse organizations for and direct financial losses due to fraudulent use of business services, including cryptomining.

## How to detect cryptojacking

Like ransomware, cryptojacking can affect your organization despite your best efforts to stop it. Detecting it can be difficult, especially if only a few systems are compromised. Don’t count on your existing endpoint protection tools to stop cryptojacking. “Cryptomining code can hide from signature-based detection tools,” says Laliberte. “Desktop antivirus tools won’t see them.” Here’s what will work:

**Train your help desk to look for signs of cryptomining.** Sometimes the first indication is a spike in help desk complaints about slow computer performance, says SecBI’s Vaystikh. That should raise a red flag to investigate further.

Other signals help desk should look for might be overheating systems, which could cause CPU or cooling fan failures, says Laliberte. “Heat [from excessive CPU usage] causes damage and can reduce the lifecycle of devices,” he says. This is especially true of thin mobile devices like tablets and smartphones.

**Deploy a network monitoring solution.** Vaystikh believes cryptojacking is easier to detect in a corporate network than it is at home because most consumer end-point solutions do not detect it. Cryptojacking is easy to detect via network monitoring solutions, and most corporate organizations have network monitoring tools.

However, few organizations with network motoring tools and data have the tools and capabilities to analyze that information for accurate detection. SecBI, for example, develops an artificial intelligence solution to analyze network data and detect cryptojacking and other specific threats.

Laliberte agrees that network monitoring is your best bet to detect cryptomining activity. “Network perimeter monitoring that reviews all web traffic has a better chance of detecting cryptominers,” he says. Many monitoring solutions drill down that activity to individual users so you can identify which devices are affected.

"If you have good egress filtering on a server where you’re watching for outbound connection initiation, that can be good detection for [cryptomining malware]," says Farral. He warns, though, that cryptominer authors are capable of writing their malware to avoid that detection method.

**Monitor your own websites for crypto-mining code**. Farral warns that crypto jackers are finding ways to place bits of Javascript code on web servers. "The server itself isn't the target, but anyone visiting the website itself [risks infection]," he says. He recommends regularly monitoring for file changes on the web server or changes to the pages themselves.

**Stay abreast of crypto jacking trends.** Delivery methods and the crypto-mining code itself are constantly evolving. Understanding the software and behaviors can help you detect crypto jacking, says Farral. "A savvy organization is going to stay abreast of what’s happening. If you understand the delivery mechanisms for these types of things, you know this particular exploit kit is delivering crypto stuff. Protections against the exploit kit will be protections against being infected by the cryptomining malware," he says.

## How to respond to a cryptojacking attack

**Kill and block website-delivered scripts.** For in-browser JavaScript attacks, the solution is simple once cryptomining is detected: Kill the browser tab running the script. IT should note the website URL that’s the source of the script and update the company’s web filters to block it. Consider deploying anti-cryptomining tools to help prevent future attacks.

**Update and purge browser extensions.** “If an extension infected the browser, closing the tab won’t help,” says Laliberte. “Update all the extensions and remove those not needed or that are infected.”

**Learn and adapt.** Use the experience to better understand how the attacker was able to compromise your systems. Update your user, helpdesk and IT training so they are better able to identify cryptojacking attempts and respond accordingly.

# **How to protect your computer from malicious cryptomining**

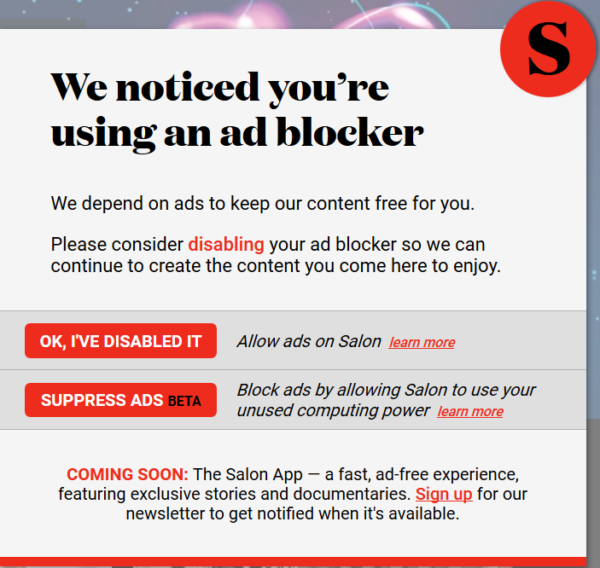
Posted: February 27, 2018 by [Pieter Arntz](https://blog.malwarebytes.com/author/metallicamvp/)  
Last updated: August 16, 2018

Noticing that your computer is running slow? While sometimes a telltale sign of [malware infection](https://www.malwarebytes.com/malware/), these days that seems doubly true. And the reason is: malicious cryptomining. So, what, exactly, is it? We’ll tell you how bad this latest malware phenomenon is for you and your computer, plus what you can do about it.

### Definition

Malicious cryptomining, also sometimes called drive-by mining, is when someone else is using your computer to mine cryptocurrency like Bitcoin or Monero. But instead of cashing in on your own computer’s horsepower, the collected coins go into the other person’s account and not yours. So, essentially, they are stealing your resources to make money.

Cryptomining can sometimes happen with consent, but unfortunately these occasions are rare.



Salon.com gave its site visitors the choice to view ads or let them mine your computer

### How bad is it?

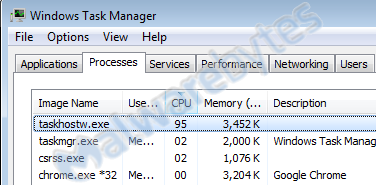
If the duration of the cryptomining is not too prolonged and you are aware of what is going on, then it’s not that big a deal for regular computer users. When you are not aware of the mining activity—which is the majority of the time—it is a theft of resources. This is because cryptomining takes advantage of your computer’s Central Processing Unit (CPU) and Graphics Processing Unit (GPU), running it at higher capacities. Imagine revving your car engine or running your air conditioning while driving up a steep hill.

If cryptomining is too prolonged and running at, or near, the maximum of what your computer can handle, it can potentially slow down every other process, shorten the lifespan of your system, or ultimately brick your machine. And obviously, any malevolent threat actors want to keep using as many of your resources for as long as possible.

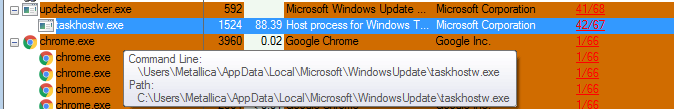
Finding the origin of the high CPU usage can be difficult. Processes might be hiding themselves or masking as something legitimate in order to hinder the user from stopping the abuse. And as a bonus to the cryptominers, when your computer is running at maximum capacity, it will run ultra slow, and therefore be harder to troubleshoot. Besides the theft and the slow, possibly damaged computer, being cryptomined could also make you more vulnerable to other [malware](https://blog.malwarebytes.com/glossary/malware/) by introducing additional vulnerabilities to your system, like in the case of the [Claymore Miner](http://www.tomshardware.com/news/claymore-miner-software-vulnerable-botnet,36356.html).

### Local or website?

When you notice high CPU usage and suspect it might be malicious cryptomining, it is important to know whether it’s being done in your browser or whether your computer itself is infected. So the first thing to do is to identify the process that is gobbling up your resources. Often using the Windows Taskmanager or MacOs’s  Activity Monitor is enough to identify the culprit. But, like in the example below, the process may have the same name as a legitimate Windows file.

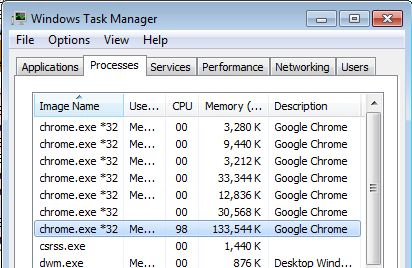


In case of doubt about the legitimacy of the process, it is better to use [Process Explorer](https://blog.malwarebytes.com/101/2016/05/process-explorer-part-2/), which allows you to see the parent process (what started the suspicious process) and the location of the file. In the same example as we used above, Process Explorer shows you the path is different from the legitimate Windows file and the parent process is strange.

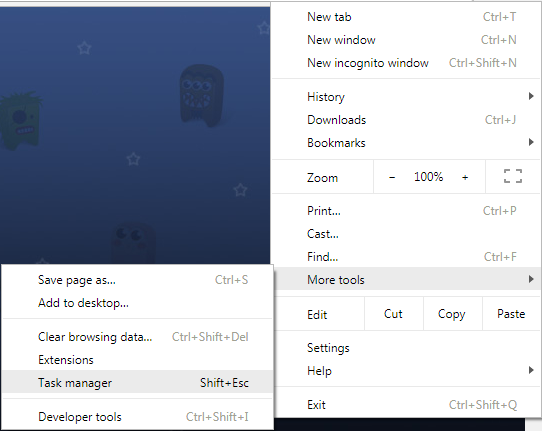


And if you have the [VirusTotal](https://blog.malwarebytes.com/cybercrime/2014/01/process-explorer-now-including-virustotal-support/" \t "_blank) check enabled, you will see that the file itself and the parent are widely detected. (The Chrome detection 1/66 is a false positive by Cylance). Knowing this, you can stop the process to speed up your system and then start working on removing it.

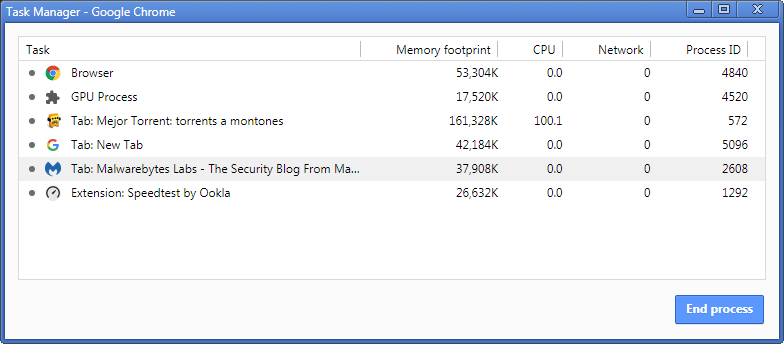
Finding the offender, however, is harder when the process is a browser like in the example below.



Of course, you can simply kill the process and hope it stays away, but knowing which tab/site was responsible does provide you with information that can help you avoid it from happening again. Chrome has a nifty built-in tool to help you with that. It’s called the Chrome Task Manager. You can start it by clicking “More Tools” in the main menu and choosing “Task manager” there.

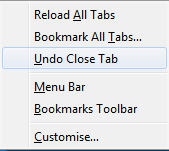


This Task Manager shows the CPU usage of the individual browser tabs and of the extensions, so if one of your extensions included a miner, this will show up in the list as well.



Note that the Chrome Task Manager sometimes shows over 100 CPU usage, so I’m not sure whether it’s a percentage.

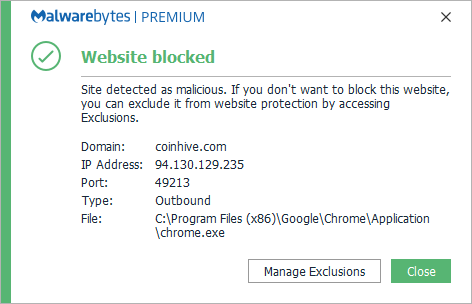
An alternative method that can also be used in other browsers is to disable extensions and close tabs in reverse historical order. If disabling an extension does not help, it’s easy to re-enable it. And if closing a tab does not help, you can use the “Reopen last closed tab” option in browsers that have this option, such as Opera, Chrome, and Firefox.



Firefox’s reopen last closed tab is called “Undo Close Tab”

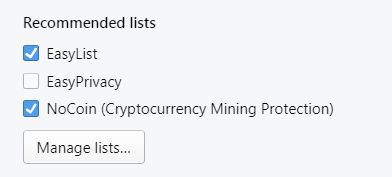
### How to protect against cryptomining

[Malwarebytes](http://www.malwarebytes.com/pricing) stops the installation of many bundlers and Trojans that drop cryptominers on your system. We also block the domains of the most abused scripts and mining pools.



Another option, if you don’t have Malwarebytes, is to block Javascript in the browser that you use to surf the web, but this could also block functionality that you like and need.

If you want more specialized blocking capabilities there are programs like “No Coin” and “MinerBlock” that block mining activities in popular browsers. Both have extensions for Chrome, Firefox, and Opera. [Opera’s latest versions even have NoCoin built in](http://www.zdnet.com/article/opera-just-added-a-bitcoin-mining-blocker-to-its-browser/).



### Summary

Cryptomining can be done locally on the system or in the browser. Knowing the difference can help you remediate the problem, as both methods require different forms of protection. The solutions are almost as popular as the problem, so choose wisely, as there may be frauds out there trying to grab a portion of the market.

# How to stop websites from using your computer to mine Bitcoin (and more)

Some websites may use your computer to mine cryptocurrencies like Bitcoin and Monero. Here's how to stop them.

[](https://www.cnet.com/profiles/caspertek/)

[**Taylor Martin**](https://www.cnet.com/profiles/caspertek/)

Feb. 16, 2018 11:31 a.m. PT

**[6](https://www.cnet.com/how-to/how-to-stop-sites-from-using-your-cpu-to-mine-coins/" \l "comments)**

Mining cryptocurrencies is a great way to earn small amounts of residual income (that could possibly be worth much more in the future). This is becoming an alternative revenue source some websites (and people with more nefarious intentions) are banking on.

[Salon.com](https://www.salon.com/about/faq-what-happens-when-i-choose-to-suppress-ads-on-salon/), for example, is giving readers the option to opt out of advertisements in exchange for letting the site use their CPUs to mine Monero, a cryptocurrency that's easier to mine than [Bitcoin](https://www.cnet.com/tags/bitcoin/) and has a current market cap of $4.6 billion.

Of course, where there's room for a legitimate way to earn money, corruption is soon to follow.

Anti-malware software firm [Malwarebytes](https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/) and IT security company [ESET](https://www.welivesecurity.com/2017/09/14/cryptocurrency-web-mining-union-profit/) both warned of sneaky uses of JavaScript files that use the CPU of visitors to mine cryptocurrencies without their knowledge (or explicit permission). This can come in the form of malicious software that is installed on a user's computer, an undetected JavaScript file that mines in the background or a pop-under window that can continue to mine coins even after the browser is closed.

If you're not sure how to determine if your computer is being used to mine coins without your knowledge, make sure to [read our article](https://www.cnet.com/news/find-out-if-websites-are-mining-bitcoin-cryptocurrency/) on detecting coin mining. And if it is, how can you put a stop to it? Here are four ways to stop your computer from mining coins without your permission.



**Watch this:**Cryptojacking: The hot new hacker trick for easy money

 1:43

## Should you block coin mining?

Whether you should allow websites to use your computer to mine coins is entirely up to you. In most cases, it's entirely harmless. But the trouble is how ethical it is for a company to use your computer for something other than what you intended.

When a website is upfront about coin mining, there is no harm in supporting its content or service by allowing it to harness your computing power. It's a great trade-off if you're not a fan of advertisements.

That said, mining can affect the performance (and battery life) of your computer and (marginally) increase your power bill. As long as you understand this and give consent, there is no issue. It's when websites decide to do it in the background, without your knowledge, that it becomes unethical.

## How to stop sites from mining coins with your CPU

Assuming your computer doesn't have a malicious coin mining program installed, there are a number of ways to block coin mining while you browse.

### Disable JavaScript on specific sites

If you suspect a website is using your computer to mine cryptocurrencies without your permission, you can simply block JavaScript altogether.

The problem, however, is that this is a very aggressive way to block mining and will break many websites. Facebook, for instance, will not load without JavaScript enabled.

### Coin mining blockers

If you don't want to use an ad blocker or just want to specifically block coin mining, there are a handful of extensions available

* No Coin ([Chrome](https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl?utm_source=chrome-ntp-icon), [Firefox](https://addons.mozilla.org/en-US/firefox/addon/no-coin/), [Opera](https://addons.opera.com/en/extensions/details/no-coin/?display=en))
* minerBlock ([Chrome](https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl?utm_source=chrome-ntp-icon), [Firefox](https://addons.mozilla.org/en-US/firefox/addon/minerblock-origin/), [Opera](https://addons.opera.com/en/extensions/details/minerblock/?display=en))
* Anti Miner ([Chrome](https://chrome.google.com/webstore/detail/anti-miner-no-1-coin-mine/ibhpgkhoicjhklmbhdoeikeggbeejonj?utm_source=chrome-ntp-icon))
* Coin-Hive Blocker ([Chrome](https://chrome.google.com/webstore/detail/coin-hive-blocker/ccagdbjcbhmcdcbbknfebhhdbolnfimo?hl=en))

These extensions work by blacklisting known domains and mining scripts. They're regularly updated and are among the best hands-off approaches to block mining. On the flip side, if you want to support a website by allowing it to mine, you can whitelist it.

### Anti-malware software

While browsers haven't yet adapted to blocking cryptocurrency miners (or at least making them an opt-in option), some anti-malware software has. Malwarebytes, for example, offers cryptocurrency miner blocking in [its premium subscription](https://www.malwarebytes.com/premium/).