How-To Geek

How to Detect and Defeat Cryptominers in Your Network

DAVE MCKAY @thegurkha
DEC 28, 2021, 2:46 PM EDT | 5 MIN READ

Chinnapong/Shutterstock

Mining for cryptocurrency isn't illegal. But using a computer or network to do so without permission is. Here's how to tell if someone is cryptojacking your resources for their own benefit.

Cryptocurrencies and the Need to Mine

The virtual tokens that cryptocurrencies use as coins are minted when a large number of very complex mathematical problems have been solved. The computational effort required to solve these problems is enormous.

It’s a collaborative effort, with many computers linked together to form a distributed processing platform called a pool. Solving the mathematical problems—or contributing to their solution—is called mining. Recording transactions made with the cryptocurrency such as purchases and payments also requires mining. The reward for mining is a small amount of the cryptocurrency.

As time goes by it becomes harder to mint new coins. Each cryptocurrency will mint a predetermined number of coins over the life of the currency. As more and more coins are created, and fewer new coins are left to create, the effort required to mine and mint new coins increases. Long gone are the days when it was possible to make money by cryptomining on a small scale. The amount of electricity you use wipes out your small cryptocurrency profit.

Profitable cryptomining requires specialist rigs and even entire farms of machines. The hardware costs must be recouped and the running costs permanently offset, so even then it isn’t all free money. Unless of course, you’re using someone else’s computing resources to perform your mining. Using someone else’s IT resources without permission is a crime, but that’s no deterrent to the cybercriminals.

Using phishing attacks or infected websites they can easily install cryptomining malware without your knowledge, and poach your electrical power and CPU cycles. Another way they cryptomine on your dime is to infect websites so that visitors’ browsers join a cryptomining pool and run JavaScript cryptomining scripts. Whichever method the threat actors employ, it’s called cryptojacking and it lets them make a profit while you face higher utility bills and reduced performance.

Because they try compromise as many computers as possible across as many organizations as possible, their pool of computers becomes large and powerful. That power means they can materially contribute to the mining processes and get rewarded.

RELATED: ***Cryptocurrency Miners Explained: Why You Really Don't***

Want This Junk on Your PC

Large-Scale Mining

Cryptomining has even been used by Advanced Persistent Threat groups and other state-sponsored threat actors. Microsoft has described in a security blog how one state-sponsored cyber-espionage group has added cryptojacking to their usual forms of cybercriminal activity.

They have conducted wide-spread attacks in France and Vietnam, deploying cryptominers to mine the popular cryptocurrency Monero. Mining cryptocurrency on a huge scale like this guarantees it will be profitable.

How To Spot Cryptomining

If you or your users notice a drop in performance of computers or servers, and those machines have a constant high CPU load and fan activity, that might be an indication that cryptojacking is taking place.

Sometimes poorly-written and badly-tested operating system or application patches can have adverse effects that share the same symptoms. But if you're seeing a sudden, widespread number of affected computers and there haven't been any scheduled patches rolled out, its likely to be cryptojacking.

Some of the smarter cryptojacking software limits its CPU load when it notices a certain threshold of legitimate user activity. This makes it harder to spot, but it also introduces a new indicator. If the CPU and fans go higher when nothing or very little is happening on the computer—the exact opposite of what you'd expect—then it is likely to be cryptojacking.

Cryptojacking software can also attempt to blend in by pretending to be a process that belongs to a legitimate application. They can use techniques such as DLL sideloading where a malicious DLL replaces a legitimate DLL. The DLL is called by a *bone fide* application when it launches, or a *doppelgänger* application that has been downloaded behind the scenes.

Once it is called, the fraudulent DLL launches a cryptomining process. If the high CPU load is noticed and investigated, it appears that a legitimate application is misbehaving and performing in an adverse fashion.

With such measures being taken by the malware authors, how can you recognize cryptojacking for what it is, and not mistake it as an errant but "normal" application?

One way is to review logs from network devices such as firewalls, DNS servers, and proxy servers and look for connections to known cryptomining pools. Obtain lists of connections that cryptominers use, and block them. For example, these patterns will block the majority of Monero cryptomining pools:

- *xmr.*
- *pool.com
- *pool.org
- pool.*

The obverse of this tactic is to limit your external connections to known, good endpoints but with a cloud-centric infrastructure that is significantly harder. It's not impossible, but will require constant review and maintenance to make sure legitimate assets are not blocked.

Cloud providers can make changes that impact how they are seen from the outside world. Microsoft helpfully maintain a list of all the Azure IP address ranges, which it updates weekly. Not all cloud providers are so organized or considerate.

Blocking Cryptomining

Most popular browsers support extensions that can block cryptomining in the web browser. Some ad-blockers have the ability to detect and stop JavaScript cryptomining processes from executing.

Microsoft is experimenting with a new feature in their Edge browser, code-named the Super Duper Secure Mode. This shrinks the browser's attack surface hugely by completely turning off the Just in Time compilation within the V8 JavaScript engine.

This slows down performance—on paper at least—but removes a considerable layer of complexity from the browser. Complexity is where bugs slip in. And bugs lead to vulnerabilities that, when exploited, lead to compromised systems. Many testers are reporting no noticeable slow-down in their use of the test release versions of Edge. Your mileage may vary, of course. If you habitually use very intensive web-apps, you'd likely see some sluggishness. But most people would choose security over small performance gains every time.

As Usual…

Prevention is better than cure. Good cyber hygiene starts with education. Make sure your staff can recognize typical phishing attack techniques and tell-tale signs. Make sure they feel comfortable raising concerns and encourage them to report suspicious communications, attachments, or system behaviors.

Always use two-factor or multi-factor authentication where available.

Award network privileges using the principle of least-privilege. Allocate privileges so that individuals have the access and freedom to perform their role and no more.

Implement email filtering to block phishing emails and emails with suspicious characteristics, such as spoofed from addresses. Different systems have different capabilities of course. If your email platform can check links in email body texts before the user can click them, so much the better.

Check your firewall, proxy, and DNS logs and look for inexplicable connections. Automated tools can help with this. Block access to known cryptomining pools.

Prevent the automatic execution of macros and installation processes.

DAVE MCKAY

Dave McKay first used computers when punched paper tape was in vogue, and he has been programming ever since. After over 30 years in the IT industry, he is now a full-time technology journalist. During his career, he has worked as a freelance programmer, manager of an international software development team, an IT services project manager, and, most recently, as a Data Protection Officer. His writing has been published by howtogeek.com, cloudsavvyit.com, itenterpriser.com, and opensource.com. Dave is a Linux evangelist and open source advocate. **READ FULL BIO »**