What is Cryptojacking and how to combat this malware?

Cryptojacking is a new way of using criminals to make money with your hardware. When opening a website in your browser, cryptojacking malware can use the CPU to the maximum to exploit cryptocurrency and it is becoming increasingly popular.

Cryptojacking is a new way of using criminals to make money with your hardware. When opening a website in your browser, cryptojacking malware can use the CPU to the maximum in cryptocurrency and it is becoming increasingly popular.

What is Cryptojacking?

Cryptojacking is an attack where attackers will run an electronic digging software on your hardware without your permission. These attackers take electronic money and sell it to make a profit, but you will have problems when using the CPU at a high level and the electricity bill increases rapidly.

Although Bitcoin is the most widely known electronic money, cryptojacking attacks often dig other electronic currencies. Monero is a particularly popular type, as it is designed so that people can dig on the average computer. Monero is also anonymized and is an altcoin (the common name for other cryptocurrency with Bitcoin).

See also: 10 most popular virtual currency, digital money today

Digging electricity by itself involves running complex mathematical equations, using a lot of CPU power. In a typical cryptojacking attack, virtual money digging software will maximize your computer's CPU. So you will see computers work more slowly, use more energy and create more heat. You can hear the fan spinning to cool itself. If you use a laptop, the battery will quickly be depleted. Even on a desktop computer, it will absorb more electricity and increase electricity bills.

Electricity costs are the reason you find it hard to profit if you dig on your computer. But attackers on other people's computers do not have to pay electricity fees but still get a profit.

What device can become a cryptojacking victim?

Any device running the software can be used to dig electronic money. An attacker only needs to make these devices run virtual money digging software that can be profitable.

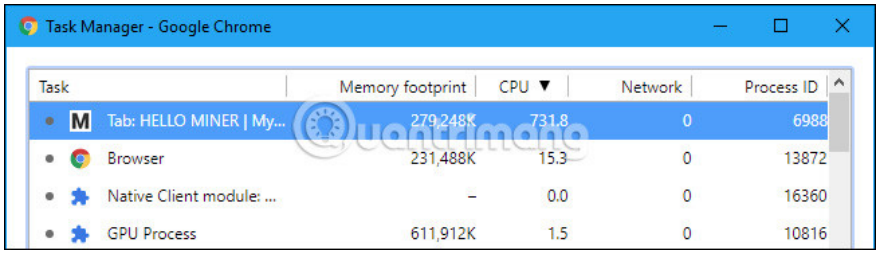
Cryptojacking 'Drive-by' attacks can be done on all devices with browsers such as Windows, Mac, Linux, Chromebook, Android phones, iPhones or iPads. As long as you open the website with the embedded virtual

money digging script on the browser, the attacker can use the CPU to dig electronic money. They will lose access as soon as you close the browser tab or navigate away from that page.

In addition, cryptojacking malware works just like any other malware. If an attacker takes advantage of a security hole or tricks you into installing malware, they can run the virtual money digging script as a background process on your computer, regardless of whether you use a Windows or Mac computer. or Linux. These attackers also try to install electronic digging software into mobile applications, especially Android apps.

In theory, they could even attack a smarthome device with security holes and install electronic digging software on it.

Cryptojacking attack in the browser



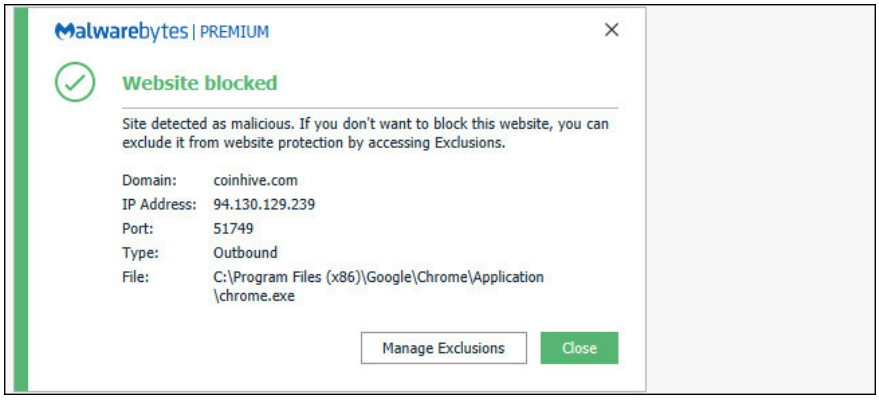
Cryptojacking 'Drive-by' attacks are becoming increasingly popular on the Internet. Websites can contain JavaScript code that runs in your browser and while you open that site, JavaScript code can dig money in the browser, maximizing CPU. When closing the browser tab or navigating away from the site, the process of digging virtual money will stop.

CoinHive is the first virtual money digging script, attracting the attention of the community, especially when they integrate into The Pirate Bay. However, there are other virtual money digging scripts other than CoinHive and they are increasingly integrated into the website.

In some cases, the attacker negotiates with a legitimate website and adds another cryptographic code to it. These guys make money when people visit that website. In other cases, website owners add their own virtual money digging script to make a profit.

This script works on any device with a web browser. It is often used to attack Windows, Mac and Linux desktops with more hardware resources than phones. But even when you view the web page on Safari on iPhone or Chrome on an Android phone, the site may also contain a virtual money digging script that runs on it, although the digging process is slower but the site can do it. .

How to prevent Cryptojacking in the browser



You should run security software that automatically blocks e-digging software on your browser. For example, Malwarebytes automatically blocks CoinHive and other electronic digging scripts, preventing them from running inside your browser. Windows Defender antivirus software integrated on Windows 10 cannot block all virtual money digers in the browser. Check your security software companies to see if they block virtual money digging scripts.

Although security software can protect you, you should also install browser extensions that provide a blacklist of virtual money digging scripts.

See also: 5 super fast ways to stop digging virtual money on web browsers

On iPhone, iPad or Android devices, the website using electronic digging software will stop when you navigate away from the browser application or change the tab. This operating system does not allow them to use multiple CPUs in the background.

On Windows, Mac, Linux or Chromebook computers, as long as you open the tab in the background, it can also use the CPU. However, if you have software that blocks these scripts, you won't need to worry anymore.

Cryptojacking malware

Cryptojacking malware is also becoming increasingly popular. Ransomware earns money on your computer, encrypts files for ransom and then asks you to pay with electronic money to unlock these files. Cryptojacking malware ignores this and hides in the background, quietly digging virtual money on your device and then sending it to the attackers. If you do not notice that your computer is running slow or the process uses 100% of the CPU, you do not even recognize malware on your device.

See also: 7 types of ransomware you didn't expect

Just like other types of malware, an attacker must find a vulnerability or trick you into installing their software to attack the computer. These attackers also try to install virtual money digging software into software that looks legitimate. Google has had to remove the Android app with software to dig virtual money from Google Play Store and Apple has done the same on Mac Apple Store.

This type of malware can infect any device from a desktop computer to a phone (if it can reach Apple Store and Google Play Store) and even on some smart home devices with losses. security vulnerability.

How to avoid Cryptojacking malware

Cryptojacking malware is like any other malware. To protect the device from being attacked by this malware, be sure to install the latest security updates, review it carefully before installing anything, and only install it on a legitimate source. trust.

On Windows computers, you should run anti-malware software to block electronic digging software like Malwarebytes, it also has a Mac version. If you suspect that your computer is infected with malware, you should perform a computer scan with your favorite anti-malware software. And the good news is that you can run Malwarebytes with an antivirus application.

On Android devices, you should only download software from Google Play Store. If you sideload the application from outside the Play Store, you may download malware to your device. Although some electronic digging software may trick Google into being in Google Play Store, Google may remove these malicious software from your device after finding them. If you install the application outside of Play Store, Google cannot protect you.

You can also monitor Task Manager (in Windows) or Activity Monitor (on a Mac) if you think a Windows or Mac computer is slow or hot. Look for the CPU usage processes on it and do a site search to see if it's legitimate. Of course, background operating system processes also use a lot of special CPUs on Windows.

Although many "greedy" electronic digging software uses all the CPU power they have, some virtual money digging scripts only use 50% of the computer's CPU power instead of 100% like other software. This makes the computer run better but also makes it difficult for users to detect them. Even if you don't see 100% CPU usage, your computer or browser may still be infected with electronic digging software.

See more:

1. 6 best Bitcoin digging software for Windows, Mac, Linux
2. Summary of popular network attacks today
3. 7 measures to enhance security for e-wallets you should not ignore