Crossing the Digital Divide (v146)

Crypto Jack

by Joseph Feigon

for the Observer

What is cryptojacking?

Cryptojacking is a scheme to use people’s devices (computers, smartphones, tablets, or even servers), without their consent or knowledge, to secretly mine cryptocurrency on the victim’s dime. Instead of building a dedicated cryptomining computer, hackers use cryptojacking to steal computing resources from their victims’ devices. When you add all these resources up, hackers are able to compete against sophisticated cryptomining operations without the costly overhead.

If you’re a victim of cryptojacking, you may not notice. Most cryptojacking software is designed to stay hidden from the user, but that doesn’t mean it’s not taking its toll. This theft of your computing resources slows down other processes, increases your electricity bills, and shortens the life of your device. Depending on how subtle the attack is, you may notice certain red flags. If your PC or Mac slows down or uses its cooling fan more than normal, you may have reason to suspect cryptojacking.

The motivation behind cryptojacking is simple: money. Mining cryptocurrencies can be very lucrative, but turning a profit is now next to impossible without the means to cover large costs. To someone with limited resources and questionable morals, cryptojacking is an effective, inexpensive way to mine valuable coins.

How does cryptojacking work?

Cryptojackers have more than one way to enslave your computer. One method works like classic malware. You click on a malicious link in an email and it loads cryptomining code directly onto your computer. Once your computer is infected, the cryptojacker starts working around the clock to mine cryptocurrency while staying hidden in the background. Because it resides on your PC, it’s local—a persistent threat that has infected the computer itself.

An alternative cryptojacking approach is sometimes called drive-by cryptomining. Similar to malicious advertising exploits, the scheme involves embedding a piece of JavaScript code into a Web page. After that, it performs cryptocurrency mining on user machines that visit the page.

How do I protect myself from cryptojacking?

Whether you’ve been cryptojacked locally on your system, or through the browser, it can be difficult to manually detect the intrusion after the fact. Likewise, 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 you from stopping the abuse. As a bonus to the cryptojackers, when your computer is running at maximum capacity, it will run ultra slow, and therefore be harder to troubleshoot. As with all other malware precautions, it’s much better to install security before you become a victim.

One obvious option is to block JavaScript in the browser that you use to surf the web. Although that interrupts the drive-by cryptojacking, this could likewise block you from using functions that you like and need. There are also specialized programs, such as “No Coin” and “MinerBlock,” which block mining activities in popular browsers. Both have extensions for Chrome, Firefox, and Opera. Opera’s latest versions even have NoCoin built in.

Control those things you can, and keep the surprises to a minimum.