Cryptojacking spreads across the web

May 8 2018, by Pranshu Bajpai And Richard Enbody

Credit: AI-generated image (disclaimer)

Right now, your computer might be using its memory and processor power – and your electricity – to generate money for someone else, without you ever knowing. It's called "cryptojacking," and it is an offshoot of the rising popularity of cryptocurrencies like bitcoin.

Instead of minting coins or printing paper money, creating new units of cryptocurrencies, which is called "mining," involves performing complex

mathematical calculations. These intentionally difficult calculations securely record transactions among people using the cryptocurrency and provide an objective record of the "order" in which transactions are conducted.

The user who successfully completes each calculation gets a reward in the form of a tiny amount of that cryptocurrency. That helps offset the main costs of mining, which involve buying advanced computer processors and paying for electricity to run them. It is not surprising that enterprising cryptocurrency enthusiasts have found a way to increase their profits, mining currency for themselves by using other people's processing and electrical power.

Our security research group at Michigan State University is presently focused on researching ransomware and cryptojacking – the two biggest threats to user security in 2018. Our preliminary web crawl identified 212 websites involved in cryptojacking.

Types of cryptojacking

There are two forms of cryptojacking; one is like other malware attacks and involves tricking a user into downloading a mining application to their computer. It's far easier, however, just to lure visitors to a webpage that includes a script their web browser software runs or to embed a mining script in a common website. Another variant of this latter approach is to inject cryptomining scripts into ad networks that legitimate websites then unknowingly serve to their visitors.

The mining script can be very small – just a few lines of text that download a small program from a web server, activate it on the user's own browser and tell the program where to credit any mined cryptocurrency. The user's computer and electricity do all the work, and the person who wrote the code gets all the proceeds. The computer's

owner may never even realize what's going on.

Is all cryptocurrency mining bad?

There are legitimate purposes for this sort of embedded cryptocurrency mining – if it is disclosed to users rather than happening secretly. Salon, for example, is asking its visitors to help provide financial support for the site in one of two ways: Either allow the site to display advertising, for which Salon gets paid, or let the site conduct cryptocurrency mining while reading its articles. That's a case when the site is making very clear to users what it's doing, including the effect on their computers' performance, so there is not a problem. More recently, a UNICEF charity allows people to donate their computer's processing power to mine cryptocurrency.

However, many sites do not let users know what is happening, so they are engaging in cryptojacking. Our initial analysis indicates that many sites with cryptojacking software are engaged in other dubious practices: Some of them are classified by internet security firm FortiGuard as "malicious websites," known to be homes for destructive and malicious software. Other cryptojacking sites were classified as "pornography" sites, many of which appeared to be hosting or indexing potentially illegal pornographic content.

The problem is so severe that Google recently announced it would ban all extensions that involved cryptocurrency mining from its Chrome browser – regardless of whether the mining was done openly or in secret.

The longer a person stays on a cryptojacked website, the more cryptocurrency their computer will mine. The most successful cryptojacking efforts are on streaming media sites, because they have lots of visitors who stay a long time. While legitimate streaming websites such as YouTube and Netflix are safe for users, some sites that host

pirated videos are targeting visitors for cryptojacking.

Other sites extend a user's apparent visit time by opening a tiny additional browser window and placing it in a hard-to-spot part of the screen, say, behind the taskbar. So even after a user closes the original window, the site stays connected and continues to mine cryptocurrency.

What harm does cryptojacking do?

The amount of electricity a computer uses depends on what it's doing. Mining is very processor-intensive – and that activity requires more power. So a laptop's battery will drain faster if it's mining, like when it's displaying a 4K video or handling a 3-D rendering.

Similarly, a desktop computer will draw more power from the wall, both to power the processor and to run fans to prevent the machine from overheating. And even with proper cooling, the increased heat can take its own toll over the long term, damaging hardware and slowing down the computer.

This harms not only individuals whose computers are hijacked for cryptocurrency mining, but also universities, companies and other large organizations. A large number of cryptojacked machines across an institution can consume substantial amounts of electricity and damage large numbers of computers.

Protecting against cryptojacking

Users may be able to recognize cryptojacking on their own. Because it involves increasing processor activity, the computer's temperature can climb – and the computer's fan may activate or run more quickly in an attempt to cool things down.

People who are concerned their computers may have been subjected to cryptojacking should run an up-to-date antivirus program. While cryptojacking scripts are not necessarily actual computer viruses, most antivirus software packages also check for other types of malicious software. That usually includes identifying and blocking mining malware and even browser-based mining scripts.

Installing software updates may also help users block attacks that try to download cryptojacking software or other malicious programs to their computers. In addition, browser add-ons that block mining scripts can reduce the likelihood of being cryptojacked by code embedded in websites. Further, users should either turn off or use a strong password to secure remote services such as Microsoft's Remote Desktop Connection or secure shell (SSH) access.

Cryptocurrency mining can be a legitimate source of revenue – but not when done secretly or by hijacking others' computers to do the work and having them pay the resulting financial costs.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation