What is cryptojacking and how can it infect your computer?

Cryptojackers usually target popular websites which draw audiences numbering in the millions every day. | Photo Credit: Reuters

The transition to a digital economy has rendered financial services more dependent on technology, and the maintenance of a robust framework to protect personal information has acquired greater importance. The already difficult task of keeping pace with hackers trying to access online finances has become even more complicated with the emergence of cryptocurrencies. It has spawned a new breed of hackers – cryptojackers. To understand cryptojackers, however, you need to understand cryptocurrency miners.

Cryptocurrencies like Bitcoin are based on a technology called blockchain, which involves maintaining a digital ledger to publicly record transactions.

A blockchain is reliant on the network of computers that run the software for the cryptocurrency. The computers participate in the relay of information regarding transactions made between holders of the currency. These computers, called nodes, can be operated by anyone who downloads the bitcoin software available for free online. When a transaction is initiated, encrypted details are transmitted among all nodes.

This web of nodes includes those operated by miners, whose objective is to group the outstanding transactions into blocks and then add them to the blockchain, since doing this involves a reward. Adding encrypted transactions to the blockchain is accomplished by the miner's cryptocurrency software solving a complex mathematical puzzle involving the numerical keys to the encryption.

Once a node has hit upon the right combination, it conveys its success to other nodes. Subsequently, other miners drop processing that block and move on to the next. The winning node that registers a transaction by adding it to the blockchain is rewarded in Bitcoin.

Often, the cost of mining becomes prohibitive since high-end machines with substantial computing power are required to solve the puzzle in a timely manner. The electricity required to power the hardware is also considerable, adding to the cost.

Cryptocurrencies are a boon for individuals or corporations which seek financial anonymity. The lack of a central regulatory authority has made it possible for trade in illegal goods to happen through the virtual currencies. However, exchanges that trade bitcoin have witnessed massive fluctuation in prices owing to speculation. The trade in bitcoin remains lucrative.

The valuation of a single bitcoin was 65,693 on January 1, 2017. Its value had peaked at 12,59,942 in December 2017, before conceding gains owing to factors such as governments proposing laws to outlaw cryptocurrencies. Bitcoin was valued at 7,40,376 at the time of writing. This implies that if a lakh of rupees was invested in bitcoin in January 2017, it would have yielded 19.17 lakh at the end of the calendar year.

Another way to have to a piece of the cryptocurrency pie is by leveraging hardware assets to mine for coins. The software for mining cryptocurrencies like bitcoin are open source and are available online. Applications that can be used for the same include Bitcoin Miner (which is available for free download on Windows through the Microsoft Store) and Easy Miner, among others. However, the hardware processing speed required to make mining a feasible are found only in high-end workstations that are powered by GPUs. Hence lone-wolf miners are a rare tribe in the sooty underbelly of the dark web.

The latest threat to computers worldwide is the rise of cryptojacking. The phenomenon is not restricted to the miniscule minority that trades in cryptocurrencies or uses their systems to mine for coins. All users who browse the internet are vulnerable to their systems being ‘cryptojacked’.

To work around the cost overruns that diminish the lustre of mining as a lucrative proposition, attackers have taken to employing malware to force an entry into the computers of remote users, and then using their hardware to mine for coins. This form of distributed computing can be profitable since it eliminates the cost burden of owning a mining rig with hundreds of processors. With more people on the Internet than ever before, there is greater computing power -- be it through desktops, laptops, tablets, or even mobile devices -- that can be maliciously subverted without the knowledge of their owners.

Cryptojackers usually target popular websites which draw audiences numbering in the millions every day. Once the malware patch has been embedded on a website, it infects the web browsers of visitors, slowing down their machines, often causing them to overheat.

Websites and apps which do not seemingly charge a fee for your consuming their content survive on revenue from digital advertising. However, websites like the file-sharing platform Pirate Bay have been found to be employing code which hijacks your system and uses it for mining Monero – a cryptocurrency whose value has almost increased fivefold in the past six months.

Many websites view this as an alternative source of revenue, bypassing intrusive advertisements. In return for content and services, proprietors of websites farm out processors located in disparate geographic locations to mine cryptocurrencies. Coinhive is a tool that allows companies to ‘monetize their digital business with their users’ CPU power.’ The tool patches the JavaScript for the website’s pages, enabling it to stealthily access the hardware of its users without their knowledge.

According to digital security firm *Wandera*, scripts like Coinhive can be embedded on to any app or website, and that users of social media platforms like Facebook, Instagram, and Pinterest are exposed to links containing malicious scripts. The increase in number of mobile devices which are being used to access the internet has also put a large segment of devices running on relatively open environments such as Android at risk of being infected. *Wandera* found that mobile devices that fell prey to cryptojacking websites and apps increased by 287% between October and November 2017.

Apple’s iPhones are also vulnerable to being cryptojacked. *Wandera* researchers found that an iPhone 7 which had a browser tab infected by Coinhive open for two hours, would result in the battery being completely depleted. It was also found that the temperature increased by 20 degrees Celsius from the ambient core temperature when the processor was used for mining at the behest of cryptojackers.

Most of the websites that have been found to use staelth to mine bitcoins on remote systems, use Coinhive. Despite the burgeoning processing power of handheld devices, laptops and desktops possess greater muscle to cruch the numbers required to solve hash functions for mining. Here is a list of applications that could protect your computer from attacks by cryptojackers.

1. NoCoin

It is an extension that can be loaded on web browsers like Google Chrome, Mozilla Firefox, and Opera. In addition to Coinhive, it provides security against other mining software which mine for bitcoin, ethereum, and ripple. However, it also allows users to turn off protection for certain websites. This provision gives users the authority to wilfully trade their processing power for the

services offered by a particular website. NoCoin is an open source tool, the code to which is available on Github.

2. MalwareBytes

Unlike NoCoin, this a software package that acts as a bulwark against a wide variety of malware, and also hackers who try to breach private networks. It is an enterprise software with versions for both personal and professional use. The company boasts that its product detected and quarantined 1,30,000 WannaCry ransomware infections in the first week of its outbreak. Corporate networks are at greater risk to cryptojacking since the the terminals are usually interlinked and possess advanced hardware. MalwareBytes also allows users to remove particular domains or IP addresses from its block list.

3. minerBlock

minerBlock is another anti-mining browser extension that can block cryptojacking attempts by software patches on websites. It maintains a blacklist of compromised websites, and lets users manually add to this list. It is particularly effective in combating code snippets that may be hidden inline in web pages. This extension can block, as well as defuse attacks that have previously breached a system's firewall.

While these tools are not completely infallible, they provide a first line of defence against potential security breaches. Given the dependence of critical personal information on technology, the consequences of voluntarily, or involuntarily letting cryptominers trespass on your computing real estate can be far-reaching.

Virtual reality and machine learning are redefining art, and providing a new canvas for expression of thoughts and ideas

END