A Closer Look at the Cryptojacking

Original:
https://www.btcc.com/en-US/academy/crypto-basics/a-closer-look-at-the-cryptojacking

With the increasing complexity of hacker attacks, Cryptojacking has become very common in recent times. Read this guide to learn what Cryptojacking is and how to detect it.

Cryptojacking is a form of network attack on the Internet. In this attack, hackers use the processing power of unsuspecting individuals to mine cryptocurrencies for their personal use and acquisition.

It can also be said to be unauthorized use of computing systems or tablets and mobile phones to mine crypto assets, such as Bitcoin, Ethereum, monero and others. In short, hackers of cryptocurrency hijacking often use the victim's system to perform all necessary updates required by the blockchain, which will lead to the mining of new tokens. Then the hacker takes away these new tokens (profits), and the victim bears the brunt of the cost of mining, the possible wear and tear of his system, and the high cost of power, mainly to power the system.

What is Cryptocurrency Mining?

We know that the real currency is printed and distributed by the central government of each country. But what about cryptocurrency? Since there is no central government to print and distribute these assets, because it is a virtual currency, where does it come from? This is a million questions that have puzzled many people.

Well, the answer is that these assets are created through a process called mining. Mining is a detailed, expensive and sometimes rewarding process, adding transaction records to the public account book of past transactions, commonly known as blockchain.

Cryptocurrency mining is carried out by a group of specialized computers that can churn out high hash rates. A higher hash rate will greatly increase your chances of solving the mathematical problems involved in creating a new Bitcoin.

Those involved in the process of creating these digital assets are called miners. For example, the emergence of new Bitcoin is almost the same as the underground mining of products such as gold. This is why it was decided to call the process of acquiring new coins mining.

Miners generally serve the cryptocurrency community by confirming legal transactions and helping the community effectively curb dual consumption, that is, miners in the community confirm each transaction to ensure that community members do not spend money that has been spent elsewhere.

Honest Transactions

In essence, miners can be compared to auditors. Their only responsibility is to ensure that users of cryptocurrency are honest in their transactions with other users. Therefore, once the miner can verify a certain number of transactions, he will receive a certain amount of asset reward.

For Bitcoin, the leading crypto asset, this number is 1MB. However, it is worth noting that not everyone who verifies a transaction will be rewarded. Why? The answer is that if a miner wants to get a reward, he needs to be the first person to get the closest correct answer to a mathematical question on the Internet. Broadly speaking, this arduous process is called proof of work.

This means that every miner needs hard work and a bit of luck to get the first 64 bit hexadecimal number, commonly known as the “hash value”. This hash value must be less than or equal to the target hash value at any time. Simply put, this is a guessing job that requires some luck.

Miners randomly generate as many “nonces” as possible by using their computers and guess the hash value as quickly as possible. Nonce, also known as a one-time number, is the key to generating a hash value less than or equal to the target. Then, the miner will be granted credit for completing the block and get a certain amount of Bitcoin.

For these reasons, miners often spend a lot of money to buy a ton of good computing power, so that they have a very high “hash rate”, which can be measured by megahash per second (MH / s), gigahash per second (GH / s) and terahash per second (th / s). This is quite a lot of hash values in a few seconds.

In short, miners help ensure the security of cryptocurrency networks. As we said earlier, miners help to forge new coins into circulation; Without them, there would be no new digital assets in circulation.

How Does Secret Hijacking Work?

One fact is that there are quite a number of ways for hackers to penetrate computer systems. One common approach is through the use of classic malware.

In this case, the target victim unknowingly clicks on a malicious link, which may be in his email, or even in a corner of the Internet, and it begins to uninstall an crypto mining code on your system. Once this code is started on your device, hackers start working around the clock to mine cryptocurrency assets through your device. On the contrary, the victims knew nothing about the

mining activities being carried out by the hackers.

This type of attack has infected your device itself, sometimes referred to as a local attack.Another way Cryptojacking works is through a method called “bypass method”. In this form, malicious threats have been embedded in JavaScript code on a web page. Therefore, any user accessing such web pages will unknowingly let their devices mine cryptocurrencies for these hackers.

Some websites have disclosed that they may use your equipment for mining activities in some cases. Most of these websites believe that they use your device to mine cryptocurrency assets, and you can access any free content they may have on the website, which is a fair deal. An example is a free game website, which knows that an ordinary user will spend quite a long time on their website.

The website may use its players’ devices (laptops, PCs, mobile phones, etc.) to mine cryptocurrencies when playing their games on the website. However, after these users close their tags or leave the website, the device is no longer vulnerable to hackers. The system allows the victim’s devices to continue to be used to mine crypto assets after leaving the website.

Examples of Cryptocurrency Hijacking Attacks

In 2018, a Spanish cyber security company reported that a cryptocurrency hijacking script called wannamine had become widely popular around the world. According to the company, hackers are exploiting monero, one of the most popular privacy coins.

The exploitation of this digital asset is relatively easy because it depends on CPU rather than GPU or ASICs. Another notable attack was reported by the governments of the United Kingdom, the United Kingdom and Canada. According to them, an Cryptojacking attack took advantage of text to voice software embedded in some of these government websites. Then, the hackers inserted a malicious coinhive script into the software, which allowed them to exploit the browser of website visitors to mine monero.

How to Detect and Prevent Cryptocurrency Hijacking

To be honest, detecting Cryptojacking attacks can be a difficult task. It’s almost impossible to find because it’s always hidden or appears as a basic activity of your device. Unsuspecting users are often confused by this gimmick.

However, in any case, a device hijacked by crypto will show the following signs.

- Your device fan will start running faster than usual to prevent it from heating up. A password

hijacking script will usually make your device work overtime, so in order to meet this new workload, your fan will be strengthened to prevent any danger.
- Your device will start to feel much hotter than usual.
- Your device is starting to perform below its best.
- Other signs may include that your device's battery is consuming faster than usual, or the electricity bill is high.

In order to prevent this form of attack, there are some noteworthy actions that can be carried out. Some of them are.

- People can start using browser extensions to stop Cryptojacking scripts flooding the Internet.
- Internet advertising is a common feature of the world wide web. One feature of the network is that some scripts are embedded in these websites, so blocking these advertising websites can protect people from attackers.

We mentioned how the illegal cryptocurrency mining script is embedded in JavaScript. Another way to prevent cryptocurrency hijacking is to disable JavaScript when accessing the Internet. This will help protect users from any such attacks.

Conclusion

Recently, due to the increasing complexity of hacker attacks on unsuspecting Internet users, Cryptojacking has become very common.

Accordingly, while most victims of these malicious attacks may not know that they are being used for the benefit of others, the wear and tear and bill levels caused by the attacks begin to drag them down with little or no time.

Cryptocurrency mining can be a laborious, time-consuming and very expensive operation; By using cryptocurrency to hijack software, hackers can subvert this and still find ways to make profits from unsuspecting victims.