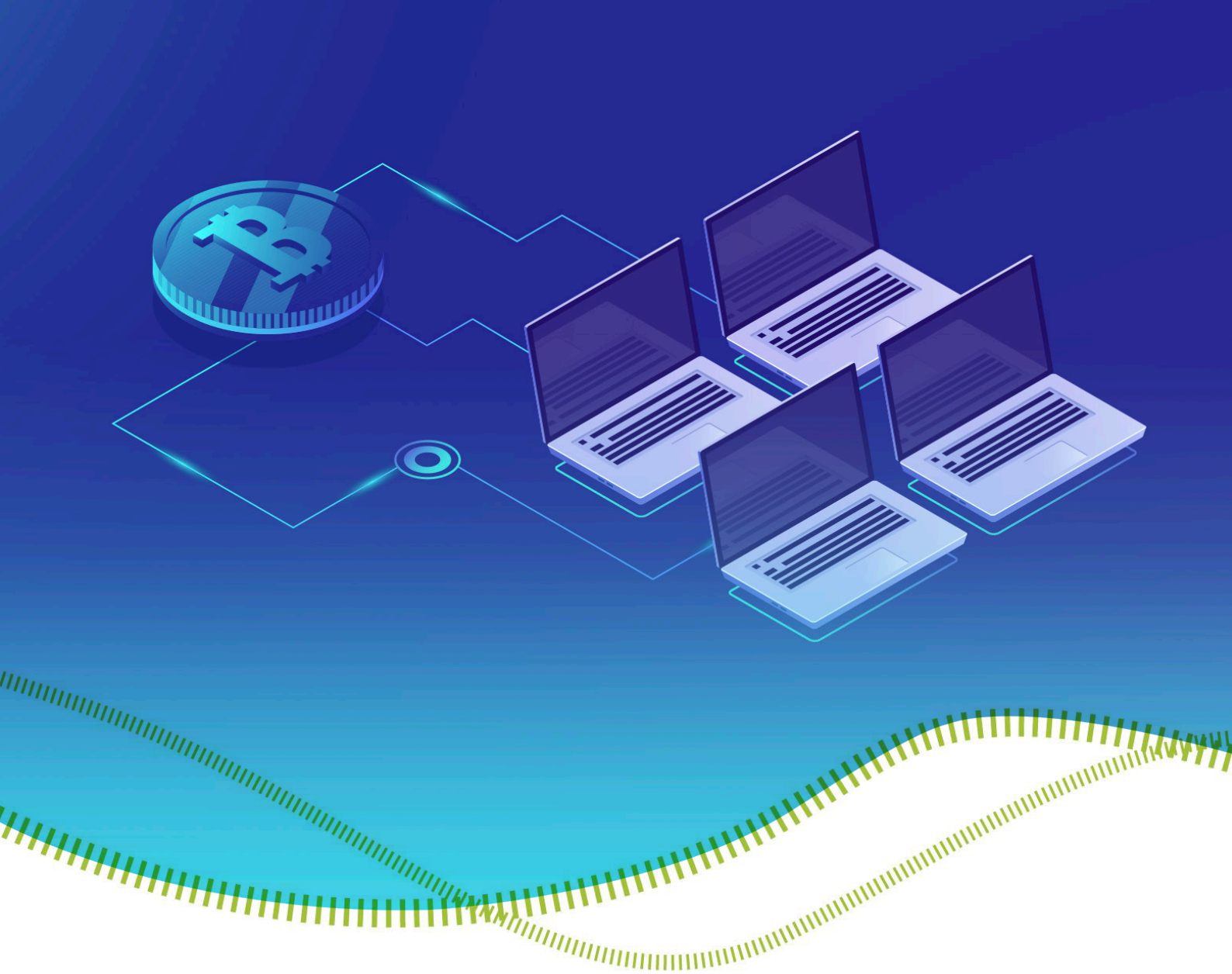


Cryptojacking

What it is, why you should care

CERT.be
The Federal Cyber Emergency Team

The
Federal Cyber
Emergency Team

Table of Contents

1 INTRODUCTION

A while ago, a new phenomenon called *cryptojacking* has appeared. CERT.be sees an uprising of the number of infections and an increasing of their complexity. Detections of coinminers on endpoint computers increase. At this rate CERT.be projects that cryptojacking will become a bigger threat than ransomware.

The goal of this document is to discuss in-browser mining and *cryptojacking*.

1.1 What are crypto-currencies?

Crypto-currencies are virtual currencies that rely heavily on cryptology in order to function. The first popular one was Bitcoin, which offered a decentralized digital cash system, as an alternative to the classic cash system. Nowadays, a few hundred different crypto-currencies exist, but Bitcoin will be used in this document as an example to illustrate principles.

As the price of some of these crypto-currencies has increased rapidly, crypto mining has gained traction.

1.2 What is mining?

To create a Bitcoin (and thus earn money), a computer has to perform a lot of calculations which need an important amount of resources (CPU). For these calculations, the computer or smartphone is rewarded in Bitcoins. This process is called *mining*.

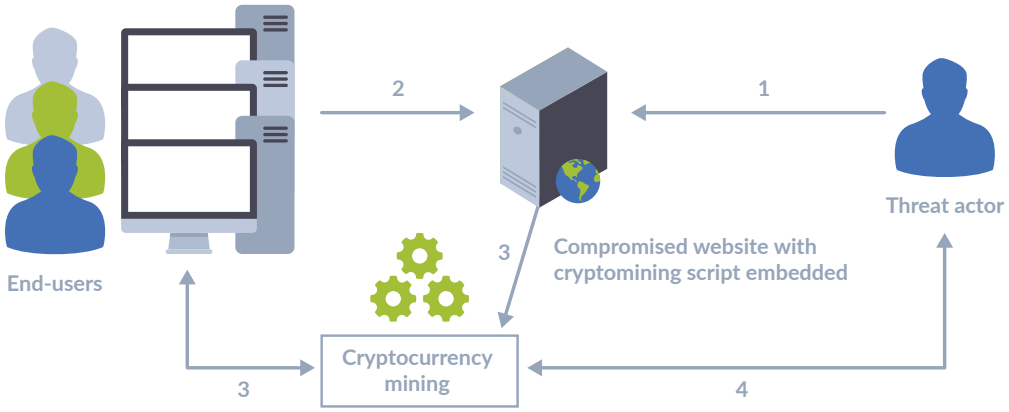
As the amount of calculation needed is really high, the best way to maximize the profits is to have a high number of devices performing these calculation (called a pool of devices).

Because a bigger pool brings larger benefits, some actors on the internet started to include mining programs (called scripts) in their websites. This means that the visitors of the page will mine crypto-currencies for the owner of the website. This happens in the background, so the user might not be aware of it.

If the user gives permission to the website to mine with the user's device, this can be seen as fair compensation for the use of the website and the services behind it.

However, the problem arises when the user is not aware that their browser is mining crypto-currencies.

How cryptojacking works



Steps

1. The threat actor compromises a wesbite
2. Users connect to the compromised website ad the cryptomining script executes
3. Users start unknowinlgy mining cryptocurrency on behalf of the threat actor
4. Uppon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Source: Enisa

2 WHAT IS CRYPTOJACKING?

2.1 What is cryptojacking?

If the user's browser is used to mine crypto-currencies without the user's consent, the user is victim of what is called cryptojacking.

While the crypto-miner is running the user will notice a very high graphics card and/or CPU usage level. The browser could use 40% or more of your available computer power. This means that the computer or smartphone will run slower, the battery will drain faster and the temperature of the device might increase as long as the script is running.

Moreover, an increased workload on the device results in higher electricity bill.

2.2 How to discover?

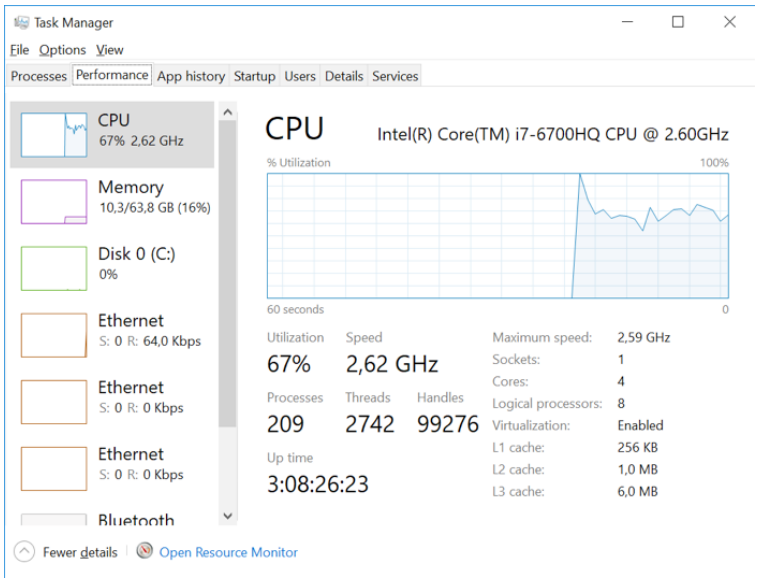
To see if the browser is currently mining crypto-currencies you can use the task manager (windows) or the activity monitor (apple):

2.2.1 Windows task manager

1. Open the task manager by right clicking the task bar and selecting "task manager"
2. Click on "More details"
3. Go to the performance tab, to see your CPU usage

2.2.2 Macintosh activity monitor

1. Hit Command+Spacebar to bring up the Spotlight search field
2. Type in "Activity Monitor"
3. Hit the Return key when "Activity Monitor" populates in the spotlight results
4. You are now in Activity Monitor where you can manage and manipulate tasks



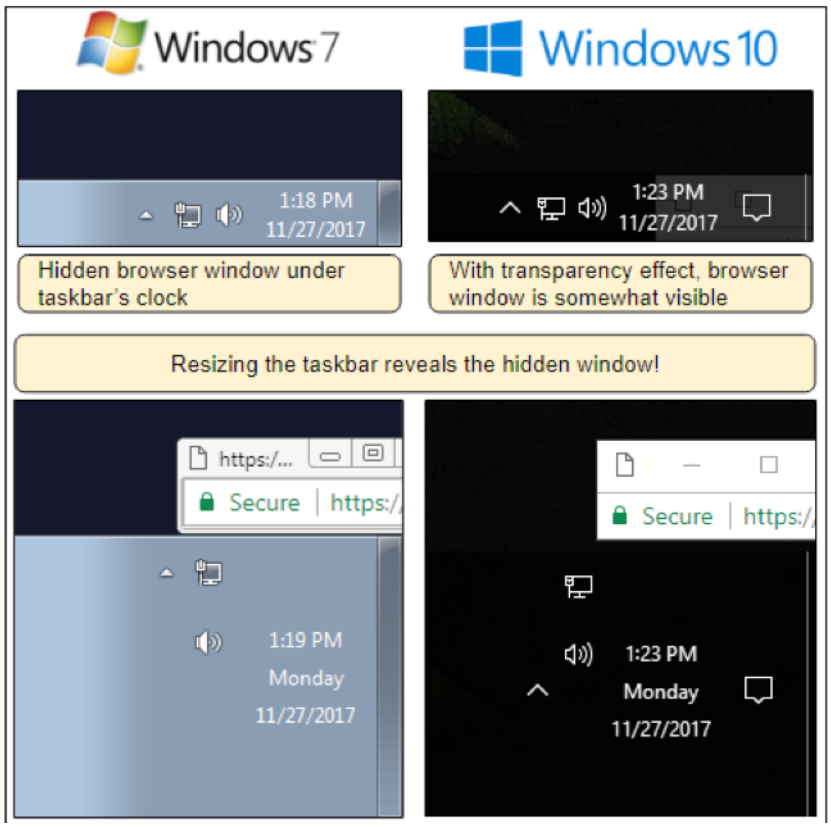
Task manager showing high CPU usage

2.3 How cryptojacking works

Cryptojacking can happen in different ways:

- The script is directly included in the website.
- The script is included in third party advertisement loaded by the website.
- The user installed a browser plugin/extension which injects the script in the websites.
- The user's device got infected with malware that executes crypto mining in the background.

A new version of crypto mining has recently been detected: the website opens a pop-up window that is hidden under the taskbar (see image below). This means that even after leaving the original page, the mining script will continue to use the resources. This allows for the script to run longer, thus maximizing the profits for the script provider.



Hidden Window - Screenshot from blog.malwaresbytes.com

3 HOW TO MITIGATE?

Fortunately, cryptojacking is easy to mitigate.

3.1 The internet user

- Consider using an ad-blocker or an anti-virus as many of them already prevent these scripts from running.
- Only install browser extensions/plugins that you trust and that are distributed by a trusted app store (Google Play, Microsoft store , etc).
- Regularly check installed extensions and remove those that are no longer needed. The more extensions installed, the greater the risk of malicious behavior or a vulnerability to emerge, so keep them to a minimum.
- Disable unnecessary browser extensions.
- If the computer or smartphone is slower or hotter than usual, or the web browser is unresponsive, restart the web browser.
- Advanced users can disable JavaScript by default and only allow trusted websites to run JavaScript
- Check on a regularly basis if your browser is still clean with tools like : https://cryptojackingtest.com
- Inform CERT.be by sending an email to cert@cert.be. This helps us in monitoring cyber security in Belgium.
- Since you're victim you can file a complaint at your local police station.

3.2 The website owner

If you notice complains from users concerning crypto mining or a slower-than-usual platform, make sure you are not distributing mining scripts unwillingly. Moreover, it is illegal in Belgium without user consent and has a maximum sentence of up to 5 years of jail (for the first offence).

3.3 The system administrator

- Block ingress and egress traffic to TCP and UDP ports 3333, 5555, 7777, 8000, and 14444 at your demarcation point, if there is not an existing business purpose.
- Disable or remove software, ports, protocols, and services that are not in use.
- Black list the domain names published on : http://iplists.firehol.org/

4 LEGAL AND ILLEGAL USE OF CRYPTO MINING

It's important to distinguish the legal use of a crypto miner and the illegal use of crypto mining, which is defined as *cryptojacking*. The subtle difference is the agreement and transparancy of the mining process to the user who is mining the cryptocurrency.

Crypto mining: crypto mining is for example a legitimate new business where companies and individuals dedicate a considerable amount of CPU power to crypto mining, an intensive process of computing and solving complicated mathematical problems in order to earn a Proof of Work, which verifies the next block in the chain.

Cryptojacking: Cryptojacking is a form of cyber-attack in which a hacker hijacks a target's processing power in order to mine cryptocurrency on the hacker's behalf. The user is not aware and didn't give his consent to the attacker.

The basis for the punishment are determined by committing these infringements are defined in the Belgian Penal Law under:

- **Article 504quater criminal code – IT Fraud**

  §1. The person who obtains, for themself or for others, with fraudulent intent, an unlawful economic benefit by entering, modifying or annulling the data in an IT system, which have been saved, processed or transmitted by an IT system, or by modifying by any technological means the possible use of the data in an IT system.

- **Article 550ter criminal code - Hacking**

  §1. Any person who, knowing they are not authorized to do so, directly or indirectly enters, alters, erases or changes information in an IT system, or by using any other technological means alters the possible use of data in an IT system.

  §3. Any person who, as a result of committing an offence referred to in §1, totally or partially hinders the correct functioning of the concerned IT system or of any other IT system, is sentenced to an imprisonment of one year to five years and to a fine of twenty-six EUR to one hundred thousand BEF or to only one of these punishments.

https://www.symantec.com/about/newsroom/press-releases/2018/symantec_0321_01
https://bittrex.com/home/markets
https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/
https://bitcoin.org/bitcoin.pdf

5 CONTACT

The Federal Cyber Emergency Team
Wetstraat 16
1000 Brussels
info@cert.be

The Federal Cyber Emergency Team
Wetstraat 18
1000 Brussels
info@cert.be

About CERT.be

She federal cyber emergency team (CERT.be) is the operational arm of the Centre for Cyber Security Belgium (CCB) which helps the government, emergency services and companies to prevent, coordinate and provide assistance in the event of cyber incidents.
www.cert.be

About the Centre for Cyber Security Belgium

The Centre for Cyber Security Belgium (CCB) is the national centre dealing with cyber security issues in Belgium. The CCB aims to monitor, coordinate and supervise the implementation of Belgium's strategy on cyber security. By optimising exchanges of information, the general public, companies, the government and critical sectors can be adequately protected.
www.ccb.belgium.be

Responsible editor

Centre for Cyber Security Belgium, Miguel De Bruycker, rue de la Loi 18, 1000 Brussels