Identification and analysis of cryptojacking: Performance effects

João Carreiro, *Instituto Superior Técnico – Lisboa*

***Abstract*—Technological evolution, associated with new methodologies and procedures for solving human problems, is usually followed by developments in criminal activities. The arise of blockchain and cryptocurrency confers different possibilities for making payments, anonymizing processes and investments, supporting also a new opportunity for malicious agents to generate illicit ways of earning income. One result of this normalization is cryptojacking, which belongs to the lucrative malware category and means the introduction of malicious code into local programs or online sites, in order to divert processing power from affected devices for unauthorized cryptocurrency mining. For the first time, the incidence of this type of malware has surpassed that of ransomware, making relevant the study of the phenomenon, the understanding of the problem and the analysis of its characteristics. In this respect, the present paper consists in properly instate this malware in the theoretical framework, complemented by a practical part in which experiments were performed, in controlled environment, with different variables and properties, to analyze and measure the effects of cryptojacking on the performance of a computer system. This study concludes that: there are several types of illicit mining scripts running in websites' code; it is possible to assume the presence of cryptojacking through the affected system performance analysis; there is a direct relationship between CPU percentage utilization and malware activation; the temperature recorded after each test is also indicative of unwanted mining activity.**

***Index Terms*—Cryptocurrency; Malware; Cryptojacking; Performance.**

I. Introduction

The significant rise of interest in cryptocurrencies, partly because of the security and anonymity that this type of currency confers in payments, and secondly because their value had increased considerably, made them an asset of choice to investors, replacing some of its alternatives in the risk market.

In this respect and as occurs with almost every field, some cyber criminals have also evolved to keep up with these recent trends, turning cryptojacking, a hard-to-detect type of malware that affects systems connected to the internet, into a natural evolution that derives from recent business opportunities and digital currency mining [28].

Since late 2017, the number of cryptojacking infections, compromising websites by stealing processing power from their visitors, has been rising dramatically, becoming one of the biggest threats reported in 2018, thus signaling its presence in various reports of information security agencies – such as the Cyber Threat Alliance – on pair with private cyber security companies – such as Symantec – and is currently considered a threat at least as significant as the already known ransomware, the last major malware type [13].

To be cost effective (given the inherent energy consumption of the process), mining implies a high processing capacity, which can be achieved individually through cost-effective hardware, or by the community-based alternative, which generally means less suitable equipment, but the integration of a parallel mining system, spread over several machines, combining its processing power and dividing the profits made by the set [22].

II. Related Work

A. Malware

Malicious software, commonly called "malware", designates programs that deliberately fulfill any attacker's negative or harmful intentions [6] and it can be materialized through any computer program that works contrary to the will or interest of a system user or owner.

Over time, there have been many attempts and ways to categorize malware, classifying it according to:

(1) Taxonomy criteria

Including: broadcast means, which subdivides into system-based transmission (requiring human action or activity) and network-based transmission (usually self-replicating); nature of the damage (the malicious effects may occur right after the infection, in the short or long term); and malware intelligence, which can be static (if the infectious program maintains its primary form) or dynamic (when it has dependencies on other programs or reprogramming functions) [24].

Other taxonomic classifications are considered, especially those related to cyberwar, where the following parameters are mentioned: stealth, considered a critical factor for the malware spread ability; monitoring and extraction capacity, ranging from not being able to withdraw any data, to the collection of significant amounts of relevant information, such as access credentials, specific documents, or extensive forensic examination data sets; and destructiveness, also distributed by levels, from the simple performance degrading or file deletion, to software encryption or causing hardware damage [11].

(2) Architecture

Malware affecting computer devices usually falls into four main points: the mechanism of infection, which can range from a random pick to a selected device through physical media, a private network or the Internet; the mechanism of dissemination, including self-propagation upon initial contact with the vulnerable system, embedded propagation through normal communication channels (such as e-mail), or secondary channel propagation, primarily infecting the victim and then transferring and activating the malware; the activation mechanism, which can be automatic (by exploiting system vulnerabilities), manual (e.g., by clicking a link), based on certain human activities (e.g., by inserting a media support or upon authentication), or by scheduled processes; and, finally, the nature of the attack, which can be data theft, partial or complete control of the system affected, file modification or encryption, or even system and components destruction [24].

(3) Detection methods

There are two recognized malware detection techniques: signature-based, represented by the vast majority of antivirus programs and only capable of identifying some of the known malicious agents or those belonging to a predefined rule set; and behaviour-based, assuming that malware can be discovered by observing the harmful effects during the period it is being executed [10].

B. Blockchain and cryptocurrencies

The blockchain, known since 2009 through an article published by someone unknown under the pseudonym of Satoshi Nakamoto [14], works as a database shared by a worldwide computer network (node).

To ensure that copies of the database remain the same, network confirmations are made using records to hold information from all transactions made and new discovered (mined) blocks, keeping digital signatures and checking details through the network to ensure that the exchange is valid. Those blocks, which constitute the network-accepted set of registers, containing a unique code (hash), which allows their integration into the chain and incorporates the code of the previous block to which they are coupled. Lastly, the blockchain, being the part that assembles and interconnects all the registers in a specific order, meaning that authentication of certified third parties is not required to help ensuring their inviolability [18].

Completing this process successfully, which occurs only when a satisfactory hash is found, pays the discovering miner an amount. The new register is then announced to the network and incorporated at the end of the blockchain version saved by each computer. For this reason, it is a well-grounded network and, although theoretically corruptible, in practice it is a very complex process, because existing copies would have to be compromised at a given time, for someone to be able to perform fraudulent transactions or to attempt to perform the same transaction more than once [20].

Also, the network is designed to adjust the mining complexity for the following blocks, in a logic of increasing difficulty and consequently demanding higher computing power [27].

Although the blockchain is designed to provide numerous possibilities for future applications, there are also reports of associated problems, such as lack of regulation, the fact that it may become a lengthy process, or even the associated environmental cost [15].

Since 2009, besides Bitcoin (BTC), other cryptocurrencies emerged and marked their share in the digital investment trading market, highlighting: Litecoin (LTC), Ripple (XRP), Monero (XMR), Stellar (XLM), Ethereum (ETH) and Bitcoin Cash (BCH). The particular cases of XMR (Fig. 1), BTC or ETH, although with quite different absolute amounts, recorded a sudden rise between the final months of 2017 and the beginning of 2018, after which their values decreased again, confirming a volatile value fluctuation.

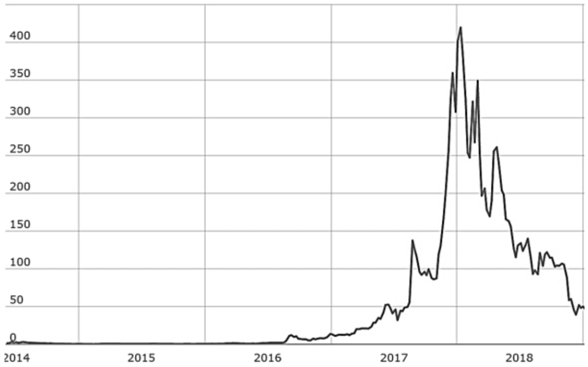

Fig. 1. Monero (XMR) value variation, since its appearance until the end of 2018, in US dollars [29].

This unexpected appreciation and consequent demand for cryptocurrencies, described in Symantec's 2018 Internet Security Threat Report [25, p. 19] as the modern “gold rush”, has led to the occurrence of several unusual situations, such as:

- An increase of investment inside digital currency markets, even replacing some of the conventional investments, especially for youngsters or those people working in technological areas, who considered this a bet with great rewarding potential [1];
- Acceptance of payments (or barters) using BTC, not only to purchase various goods and services, but also for the real estate market [21];
- Dissemination and installation of cryptocurrency exchange machines, in strategic locations of populated cities [23];
- World-wide stock shortages of certain Nvidia and AMD-branded graphics cards, as well as lack of other specific mining equipment (ASICs or mining-rigs) with lucrative mining attributes [9].

C. Cryptojacking

In the quest to keep profiting, cyber criminals turned their attention to a new modality. Experts came to say there are threats that cannot be ignored, focusing particularly on illicit cryptocurrency mining, which is described as "a highly profitable activity, where return (mining gains) cannot be traced back, allowing attackers to be more abstracted from their criminal liability" [3, p. 5], as their actions do not endanger essential resources, are softer in their effects and, therefore, become more difficult to detect.

Other specialists also point at the high profits and rapid growth of mining activities, by comparing the few cryptocurrencies existing in 2013, that together capitalized a total market value of around $1.5 billion, with a contrasting $166 billion spread over more than 1.000 different cryptocurrencies, as registered four years later [12].

In addition, Kaspersky reports that, for the first time, in 2018, malicious cryptocurrency miners surpassed the latest biggest threat to cyberspace – ransomware. The same document indicates that in the first three quarters of 2018, more than five million people were targeted with unwanted mining attacks, mainly due to the use of unlicensed programs, representing a marked increase for this type of attacks, when compared to the same period of the previous year [13].

The next chart (Fig. 2), when associated with the one present in Fig. 1, indicates a positive relation between the great increase of cryptojacking and the appreciation of cryptocurrencies between late 2017 and early 2018.

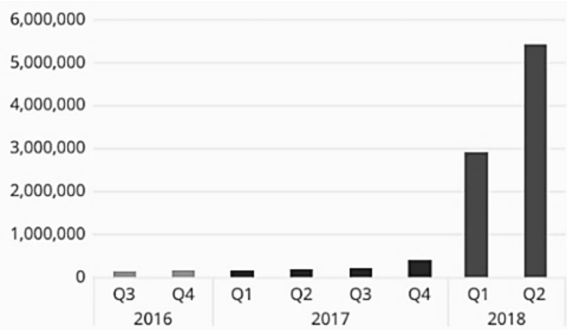

Fig. 2. Total amount of malware related to cryptocurrency mining, between Q3 2016 and Q2 2018 [16].

Moving to its operation modes, there are two possibilities for cryptojacking:

- Machine-based, which acts through software installed locally on the device, including the operating system (OS);
- Browser-based (also known as web-based), activated on simple access to a compromised website.

Although both require an internet connection, the second is more widespread and exploited, especially for its wider potential. Nevertheless, mining software may be distributed and inserted over malicious code inside apparently certified software, through known mailing lists, social networks, using social engineering techniques and others based on the weaknesses of the human factor [2].

According to Rauchberger *et al.* [22], browser-based cryptocurrency mining has existed at least since 2011, referring to a groundbreaking service launched that year, hosted at `www.BitcoinPlus.com`, which emerged because of the low value of BTC at the time. Later, in September 2017, it gave place to CoinHive, a similar service, also consisting of JavaScript code for group mining (in this case, XMR), through mining pools, which allowed users to embed this code into their websites, leading visitors to mine for them.

US-CERT [26] alerts that this kind of malware behaves may differ between being nonpersistent, if unwanted mining occurs only while the users have their browsers specifically open on the affected page, or persistent, if mining activity is maintained even after the victim stops visiting the website triggered it. The same source lists devices that are susceptible to some kind of mining-related attacks, with the most affected being computer systems (computers and servers), but not forgetting network devices (modems and routers), mobile devices (smartphones, tablets, smartwatches, and others subject to the same vulnerabilities) and interconnected IoT devices (smart TVs, printers, cameras, etc.), concluding that virtually any machine with a processor and internet connection can be targeted.

Despite not being easy detecting cryptojacking activities without advanced analysis tools, the following effects are commonly observed:

- Degradation of system performance and increased network traffic, as processing resources may be monopolized by mining and bandwidth may also change slightly;
- Notable rise of the system temperature, due to intensive machine stress, which leads to increased energy consumption (resulting in higher electricity costs), can cause system crashes and incurs in potential risk for physical damage in some hardware components;
- Possible disturbances in normal computational operations;
- Possible financial loss due to program or component failures that may cause the system to be down or intermittently functional.

The European Union Agency for Network and Information Security (ENISA) [7], mentions that several cases of mining abuse have been detected, with particular focus on the first known malicious mining code – CoinHive.

According to the cited agency, browser-based cryptojacking works as shown in the presented scheme (Fig. 3), involving these four steps (as numbered in the figure of the next page), respectively:

1. The malicious actor (threat actor) compromises his own website (or a third-party website);
2. End-users access the compromised website and the script for mining cryptocurrencies is executed;
3. The device that the user has accessed has unknowingly begun to mine cryptocurrencies into the malicious actor's digital wallet;
4. When the compromised device (or pool) mine a "new block" in the blockchain, the malicious agent receives a cryptocurrency value corresponding to this discovery.

The process described can easily be implemented by ordinary users in their domains, as there are several services, such as JSEcoin or CoinImp, which provide all the necessary instructions to integrate their browser-based services. After that, users only need to attract visitors to the website in order to start mining.

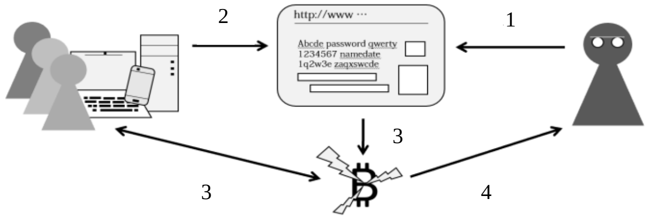

Fig. 3. Browser-based cryptojacking scheme [7].

The code section shown in Fig. 4 has been reproduced using the instructions on the JSEcoin official website and contains the lines of code available for copying, requiring only the user to replace the `<site-key>` parameter with the key that was assigned after his registration. It is particularly interesting to note that, in this case, the script works from an external source (`script src`) and allows the user to set a `throttle:X` limit for the use of processing power from the machines accessing the website. These are two remarkable features that make it harder to detect and mitigate the effects of mining activity.

```
<script
src="https://www.hostingcloud.racing/Adhf.js"></script>
<script>
      var   miner   =   new   Client.Anonymous('<site-key>',
{throttle: 0.5});
      miner.start();
</script>
```

Fig. 4. JavaScript for mining embed into a websites' code [4].

The Cyber Threat Alliance [5] also warns about "recent changes in the sophistication of illicit mining activity", describing it as a multi-level customization to enhance malware capabilities, including the ability to adjust parameters related to the activity, such as limiting the used resources or configuring settings with attributes, e.g. to avoid detection or cease mining when there is evidence that the user is present, through keyboard typing or mouse movement. Unlike unexperienced actors, the more advanced attackers opt for far less detectable parameters, such as using only 20% of the CPU processing power, objectively reducing their mining rate in order to keep their malware active longer on infected machines.

III. Measuring Cryptojacking Effects on Performance

The software analysis process can be performed statically or dynamically. The first is performed without execution, being employed exclusively by the inspection of the source code, by binary representations of the programs or by the mathematical calculation of possible values for the various parameters.

Meanwhile, the less limited dynamic analysis is applied during program execution and can be accomplished in a number of ways, such as: kernel-mode analysis, which allows the researcher to "hide" his scanning activity from malware that only run in user mode, enabling additional system information to be acquired; analysis through emulation of complete components or systems that, depending on the defined parameters, may allow to obtain a sandbox (virtually safe environment that breaks contact with the original system), which is effective for the researcher to analyse effects of running potentially malicious code without the fear of negative impacts on the machine; and virtual machine (VM) analysis, which consents the virtualization of hardware components belonging to a base physical system, in order to simulate an isolated system with the desired privileges and parameters for a given purpose [6].

A. *Methodology*

The practical experiment described in this paper will follow the next steps: creation of four testing environments, with different sets of OS and browser; selection of a sample, composed of a list with 100 websites that were identified as containing cryptojacking scripts in their code; run four tests for each site, one in each environments. Tests consist in verifying if the performance effects caused by opening the selected websites are in accordance with what is expected for an active mining activity.

Considering that is not safe to perform the experiment on a real machine, VMs were created so that performance tests could still be realistic and allowing monitoring to be done from the original machine, as the VMs are defined to access the same processing resources (CPU and GPU) as the primary environment.

In order to fulfil this part of the study and measure the influence of cryptojacking malware on the performance of different systems, it is necessary to select some properties. In this context, it was chosen the same physical machine for testing – a Microsoft Surface Pro (5th generation model), with the following main technical specs [17]:

- OS – Windows 10 Pro;
- Capacity – 256 Gigabytes (GB) Solid State Drive (SSD);
- Processador (CPU) – Intel® Core™ i5-7300U @ 2.60Ghz / 2.71Ghz;
- Graphics (GPU) – Intel® HD Graphics 620 (integrated) with 128MB dedicated memory;
- Memory – 8GB RAM;
- Accessories –Microsoft keyboard with integrated touchpad.

Using this computer, three VMs were created with Oracle VirtualBox (version 5.2.26 128414), to run different OS – Windows, Android and Linux. Due to the specific characteristics and minimum requirements to run each OS, VMs were defined using 3GB of the 8GB RAM available, and different properties were given only regarding the storage capacity and file type of the virtual disks.

To avoid using performance measurement tools that might interact in different ways with the VMs, and also for standardization purposes related to data collection, the native Performance Monitor of Windows 10 was chosen for monitoring utilization percentages for CPU and GPU, as well as for recording the transfer speeds (download plus upload) measured on the network card. To register the temperature of digital thermal sensors, present on the CPU, an online freeware was chosen – CoreTemp (version 1.13).

During tests, the computer had only essential services activated, remained located in the same physical space and was not subject to significant changes in ambient temperature, thus keeping the wanted conditions for the experience. In VMs, only one instance and a browser tab were opened. Monitoring started right after the selected website was loaded, and lasted for three minutes, during which there was no user activity, neither any navigation on the website.

All automatic updates have been turned off, either on the original system or on the VM, in order not to influence the transfer rate measurement. Similarly, for the monitoring tools to return to their default values, to ensure that the temperature returned to normal and to analyse any potential unreported side effects, between each test, it was waited idly for, at least, three minutes.

B. Sample and reference values

To gather the sample for testing, composed by sites allegedly infected with mining malware, two studies were observed: the first conducted by Eskandari *et al*. [8] in December 2017, and the second by Mursch [19] in February 2018. These studies took place with similar experiments to try to find out the current amounts of cryptojacking existing on the internet. Researchers searched for scripts through the site `www.publicwww.com`, which works as a tool for discovering alphanumeric fragments, signatures, key phrases, or words on over 500 million pages using HTML, JavaScript, and CSS.

Similarly, for the present experiment, the site `www.publicwww.com` was the primary used platform, performing the initial search for several strings related to various scripts, just like the authors mentioned above did. On this purpose, the search started by inserting the name by which the script is known, repeating the search when more precise expressions were obtained, e.g. the actual parameters of the scripts shown in the points below:

- CoinHive – coinhive.min.js; coinhive.anonymous;
- Crypto-Loot – cryptoloot.pro; crypto-loot.com; cryptoloot.anonymous;
- CoinImp – hostingcould.racing; hashing.win;
- deepMiner – deepminer.anonymous; deepminer.min.js;
- JSEcoin – load.jsecoin.

As a result, Table I aggregates the five types of cryptojacking on which this practical part focuses. Its contents also show the main cryptocurrency mined by each one of them and, in the last columns, the comparing results between the currency value and the number of sites found, in the experiments made Eskandari *et al*. [8] and by Mursch [19], and by the one of the present work.

TABLE I
General results for criptojacking research

Website	Coin	Unit value			Number of sites found		
		2017 [8]	2018 [19]	2019[1]	2017 [8]	2018 [19]	2019[2]
CoinHive	XMR	~260€	~200€	~60€	30611	34474	15385
Crypto-Loot					695	2057	319
CoinImp					317	4119	989
deepMiner					n.a.	2160	2258
JSEcoin	JSE	unk.	unk.	~0.0006€	1131	n.a.	1841

~ – Approximate value; n.a. – Value not available, due to not being considered on that experiment; unk. – Unknown value, due to lack of trusted source.

From the analysis of Table I, is observed that, between comparison among the various results, the number of sites found with evidence of mining malware in their source code peaked in the listing obtained by Mursch's work [19]. This may happen due to some factors, such as:

- Author's searches on Publicwww have been done using different strings, meaning there is a possibility that not all of them will outcome the same number of results;
- The appreciation of Monero (Fig. 1) between late 2017 and early 2018, bringing high increases on mining profitability;
- CoinHive's most recent official service shutdown in March 2019, drastically reducing the number of sites running its script.

The table also shows that the number of sites currently found with deepMiner is similar to those found in 2018, and comparing to 2017 results, the presence of JSEcoin had risen. These results can be explained by the search for sustainable alternatives, bearing in mind known services that were deactivated.

In order to begin the testing phase and measure the effects of cryptojacking, 20 sites where each script type was present (CoinHive, Crypto-Loot, CoinImp, deepMiner and JSEcoin), were randomly chosen from all outputs discovered with Publicwww, totalling a sample of 100 sites. Next, sites that did not opened, at the first attempt, were readily replaced.

In addition to the results obtained above and to expand other author's experiences, the search for the presence of mining malware, in the websites composing the sample, was also verified by two other platforms (`www.notmining.org` and `www.wappalyzer.com`), which allowed to assess whether there were other clues that could indicate that mining elements were present and functioning into websites' code.

As stated, four tests were performed for each of the 100 sites selected (sample), each test running in one of this environments: Windows and Chrome / Windows and Firefox / Android (VM on Windows) and Chrome / Linux (VM on Windows) and Firefox – so that results from the various OS and browsers can be lately compared.

In the end of each test, the values of eight variables were recorded, respectively:

[1] Value of one unit of the corresponding cryptocurrency, in Euros, with source in `https://www.worldcoinindex.com/pt/Moeda`, accessed in 2019/04/30.

[2] Total number of websites where searched strings are present, with source in `https://publicwww.com/websites`, accessed in 2019/04/30.

- $\%CPU_{max}$ – maximum percentage of CPU utilization;
- $\%CPU_{min}$ – minimum percentage of CPU utilization;
- $\%CPU_{m}$ – average percentage of CPU utilization;
- $\%GPU_{max}$ – maximum percentage of GPU utilization;
- $\%GPU_{min}$ – minimum percentage of GPU utilization;
- $\%GPU_{m}$ – average percentage of GPU utilization;
- Tf_c – CPU final temperature, in Celcius degrees;
- v_m – average speed (download and upload) registered by the network card, in Kilobits (Kbit) per second.

Then, in order to obtain some reference values that could be compared with the results of the tests to sample websites, the four tests stated *a priori* were applied to five known and accessible websites, under the same conditions.

Table II aggregates the average values of the four tests performed to these five websites for reference, all them endowed with disparate visuals and multimedia contents, as well as different scripts loaded.

TABLE II
RESULTS FOR TESTING FIVE REFERRAL WEBSITES

N.	%CPU max	%CPU min	%CPU m	%GPU max	%GPU min	%GPU m	Tfc	Vm
R1	15.99	1.33	5.19	1.30	0.26	0.46	38.75	3.49
R2	35.78	**1.89**	6.57	3.97	**0.36**	0.63	41.13	6.60
R3	39.45	0.59	4.91	3.27	0.17	0.33	40.50	17.54
R4	50.96	0.59	**10.65**	**5.78**	0.18	**0.94**	**42.88**	9.87
R5	**58.49**	0.85	5.29	3.34	0.15	0.36	39.75	**34.01**
Av.	40.13	1.05	6.52	3.53	0.22	0.54	40.60	14.30

"Bold" – Higher values registered for each variable; N. – Website assigned number; R1 – www.google.com; R2 – www.facebook.com; R3 – www.youtube.com; R4 – www.ebay.com; R5 – www.sapo.pt; Av. – Average values considering the all the results obtained by testing reference websites.

The values collected by this first benchmarking exemplify a standard for the performance of a computer with a browser opened in a website (homepage only) that does not contain mining malware embedded in its code. The table reveals maximum CPU utilization records between 16% and 58%, minimum CPU utilization between 0% and 7%, average CPU utilization between 5% and 11%, maximum GPU utilization between 1% and 6%, minimum GPU utilization near 0%, average GPU utilization between 0% and 1%, final temperatures of the CPU between 39ºC and 43ºC, and average data transfer speeds between 3 and 34 Kbit/s. These are the values that will later serve for comparison.

C. *Cryptojacking evidence*

The research to prove cryptojacking involved four tests, performed at each one of the 100 sites of the sample (identified across the platforms as mining) and had a total duration of approximately 45 hours. Therefore, a set of 400 tests were ran in the various environments created – 200 tests on Windows, 100 tests on Android, and 100 tests on Linux. As for browsers, Chrome and Firefox were used in Windows, Chrome was used in Android, and Firefox was used in Linux, making it possible a fair comparison between results by OS and by browsers. Throughout this experimental part, a total of 3200 singular results were collected.

Since it was not possible to find studies with standard results for this kind of tests and since, if existing and active, mining scripts can be defined within less detectable parameters, some reasonable values were considered to assess whether, or not, the websites in the sample actually contained mining malware, based on the two variables most commonly referred by authors – CPU utilization and temperature reached.

According to this, reference websites (which do not contain mining scripts) and sample websites (which allegedly contained mining indicators) were divided into four categories, two of them considered negative results for cryptojacking, and the other two, within the results considered positive.

For the websites of the sample, the division is based on the results obtained by the four tests performed to each one of them, in order to separate cases where the presence of mining is considered unlikely (which does not mean that mining not existed, but that it was not verified by results), from other cases where exist possible mining activity (for manifesting in the performance of few tests performed), and for last, the cases in which this mining activity was clearly noticeable (for manifesting in the performance of most of the tests performed).

Therefore, within the sites that were designated as "positive", the only difference marked for classification within "indicted" or "verified" categories was the number of tests (out of the four) that showed results that explicitly fit mining activity.

In the given assumptions, the results are now divided as "negative" or "positive" for cryptojacking. Given the 420 tests performed on a total of 105 selected sites, categorization is based on the following criteria:

- Negative Results:
  - **Referral** – websites selected for reference and comparison (not part of the sample), as they were considered legitimate, disparate, and do not contain mining scripts in their source code;
  - **Free** – websites from sample, appearing to be cryptojacking free, because their tests did not trigger mining activity, being their general results very similar to those of the referral websites.
- Positive results:
  - **Indicted** – websites from sample, that appear to have active mining activity, falling into this category all those which, in one or two of the four tests performed, resulted in an average CPU utilization of 20% (or more) and/or generated a final CPU temperature of 50ºC (or higher);
  - **Verified** – websites from sample, that have notorious mining activity, falling into this category all of which, in at least three of the four tests performed, yielded an average CPU utilization of 20% (or higher) and/or generated a final CPU temperature of 50ºC (or higher).

Consequently, there are three categories used for comparison of results – referral websites (negative), referenced sites (positive) and proven sites (positive), with a special focus on the latter two of them.

The following three illustrations show typical performance charts obtained during testing these categories.

🟥 – Average % of CPU utilization. 🟩 – v_m in bytes/s (scale 1–0.0001)
🟦 – Average % of GPU utilization. 🟨 – T_f in Celsius degrees.

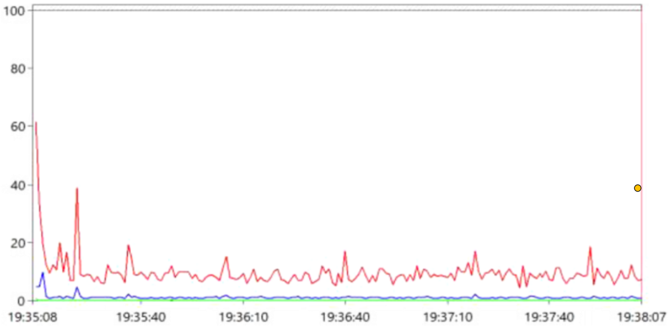

Fig. 5. Results obtained for `www.facebook.com` (Referral), running Chrome on Android, for 3 minutes.

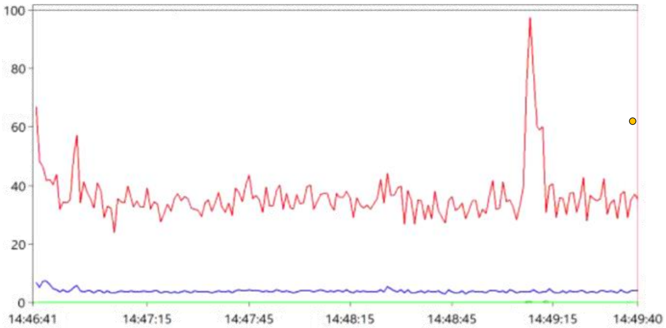

Fig. 6. Results obtained for `https://108clip.com` (Indicted), running Chrome on Android, for 3 minutes.

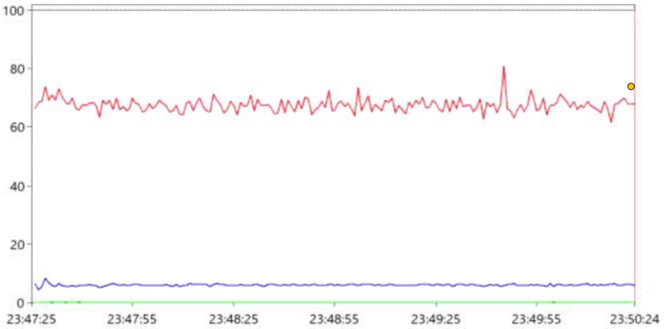

Fig. 7. Results obtained for `https://coinmarketcal.com` (Verified), running Chrome on Android, for 3 minutes.

D. Analysis of results

To better verify the differences between results obtained, when dividing the sites by the categories mentioned above, Fig. 8, 9, 10 and 11 show boxplot charts containing various data pertinent to the study, which include:

- Minimum and maximum values, indicated by the extremes of the vertical line;
- Atypical results (outliers) that, because of their discrepancy with other values, are outside the dispersion limits, represented by a small circle;
- A box with the main dispersion limits, bringing together the values between the first and third quartile, which represent the range of highest concentration of records;
- The average, marked with the horizontal line inside the scatter boundary box, and the median, represented by an "x".

Explicitly, Fig. 8 shows that Referral websites have the lowest dispersion for the average percentages of CPU utilization, concentrating the results up to 10%, although there are two higher outliers. On Indicted websites, the spread is broader, containing results between 5% and 60%. Still, most registrations are in between 12% and 34%.

For Verified websites, there is a greater spread of records, but the scatter box is between 23% and 52%, meaning that, by comparison, the value corresponding to the first quartile is very similar to the average of the Indicted category.

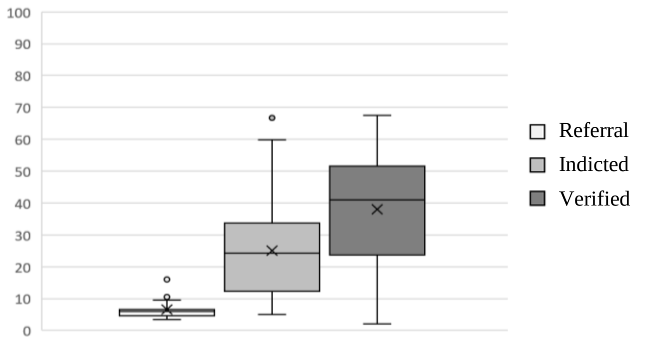

Fig. 8. Comparative Boxplot of %CPUm values, by website category.

As for the temperatures recorded at the end of each test, it can be seen from the boxplot in Fig. 9 that, once again, the results for the Referral tests have reduced dispersion and are concentrated around 40ºC. In turn, the final temperature recorded on the sites of the category Indicted, is spread between 39ºC and 73ºC, with greater agglomeration between 50ºC and 60ºC. For the Verified websites, the average value of 65ºC and the tendentially higher values stand out from the other categories.

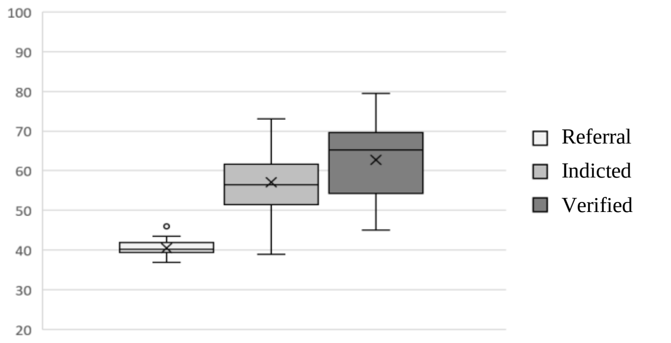

Fig. 9. Comparative Boxplot of Tfc values, by website category.

In contrast to the previous two graphs, which show significant differences between results of Referral websites and the rest, the following boxplots, about the average GPU percentage utilization results and average data transfer speeds, do not attest those variances between the categories defined.

In both cases, it is visible a weak, widespread and similar dispersion of values between the various categories, even accompanied by several outliers. These statistics may indicate that the two variables under consideration are not good indicators of the presence of cryptojacking, since quite similar values were obtained comparing Referral websites (free from malware) with Indicted or Verified categories of the sample, which were considered positive for mining infection.

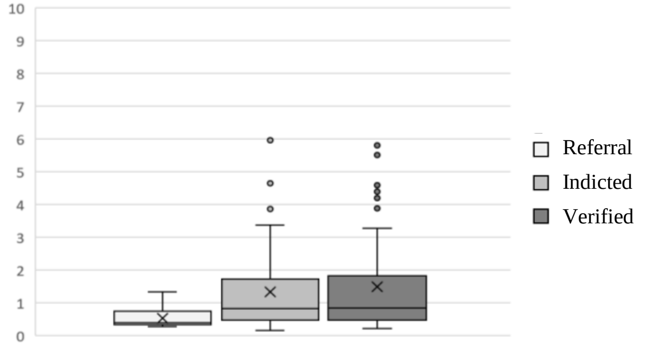

Fig. 10. Comparative Boxplot of %GPUm values, by website category.

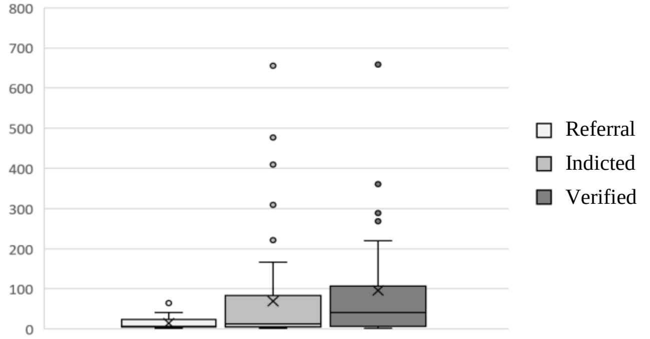

Fig. 11. Comparative Boxplot of vm values, by website category.

To complement the graphical comparisons above displayed and to prove that variables $\%GPU_m$ and v_m were not relevant to identify cryptojacking within this study, sample standard deviation (*s*) was calculated to determine whether the recorded values tend to be close to the average values. Thus, Table III contains the values of the standard deviation for each variable, considering Referral, Indicted, and Verified websites.

The table clears that GPU records are highly consistent, since values do not deviate considerably from the average. As for final temperature results, deviation is very small for the Referral websites and approaches 8ºC for both the positive categories.

On the other hand, regarding the average transfer speed, deviation notes that there were quite discrepant values influencing the average, particularly for the Indicted and Verified categories.

TABLE III
STANDARD DEVIATION APPLIED TO RESULTS OF DEFINED CATEGORIES

Website Category	*s* %CPU max	*s* %CPU min	*s* %CPU m	*s* %GPU max	*s* %GPU min	*s* %GPU m	*s* Tfc	*s* Vm
Referral	20.15	1.09	2.90	2.39	0.14	0.30	2.13	16.13
Indicted	19.33	16.54	15.66	4.69	1.14	1.33	7.92	129.25
Verified	15.80	19.37	16.36	4.83	1.04	1.48	8.82	173.90

For a last clarification on the relevance of data collected, it was also calculated, for tests within the positive website categories, the Pearson correlation coefficient between the average percentage of CPU utilization (clearly associated with mining) and its final temperature, giving a result of p=0.69, which indicates a moderate positive relationship, implying that, when the CPU register increases, the temperature tends to rise.

On the other hand, the correlation between the average percentage of CPU utilization and the average transfer speed, p= -0.06, meaning that there is no plausible relation between these variables in the context of the tests performed.

Taking in account the previous statements, it is pertinent to observe the final temperature recorded, and it seems not reliable to use the average transfer rate values to evaluate the presence of cryptojacking malwares.

E. Statistics

Remind that, from the total of 400 tests completed on the sample (100 websites) – 200 were performed on Windows, 100 on Android, and 100 on Linux. Concerning to browsers – 200 tests took place using Chrome and the remaining 200 using Firefox.

As stated in the initial part of this chapter (p. 6), parameters were defined for framing websites with positive results in two categories (Indicted and Verified), based on the number of tests that reached certain minimum values.

The following graphic figure present additional statistical information dividing the 119 tests that yielded positive results, by OS and browsers.

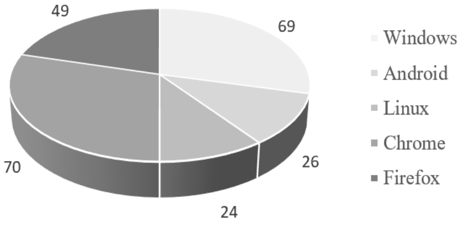

Fig. 16. Number of positive tests (Indicted/Verified), by OS and browser.

Below, two tables show other detailed statistical information. Table IV, which shows the positive results for each OS and brower used, exhibits that for the Indicted category, the quantity of results obtained using Chrome on Windows was far superior than using the same browser on Android. As for Verified category, the number of results was similar throughout OS and browser.

The total positive percentage is also similar for all tests made in Android, Linux and Firefox through Windows, although within the first group of tests realized in Chrome on Windows, 44% of the websites accused mining activity, against near 25% for the remaining.

TABLE IV
RESULTS FOR CRYPTOJACKING ON THE SAMPLE, BY BROWSER AND OS

Browser	OS	Sample	Indicted	Verified	Total positive %
Chrome	W	100	27	17	44%
	A	100	9	17	26%
Firefox	W	100	11	14	25%
	L	100	8	16	24%

W – Windows; A – Android; L – Linux;

Consecutively, the information in Table V provides the detailed results based on the script used, allowing to conclude that JSEcoin is the script that contained most results for the category Indicted and in total amount of positives, while CoinImp has the most websites belonging to Verified.

TABLE V
RESULTS FOR CRYPTOJACKING ON THE SAMPLE, BY SCRIPT TYPE

Type	Sample	Indicted	Verified	Total positive	Total positive %
CoinHive	20	9	1	11	55%
Crypto-Loot	20	8	1	9	45%
CoinImp	20	4	8	12	60%
deepMiner	20	6	5	11	55%
JSEcoin	20	13	3	16	80%

Regarding the websites testing for cryptojacking, 80% returned positive while using JSEcoin and 60% while using CoinImp. Only Cryto-Loot did not overcome half of the websites it tested as being infected, with a 45% total positive rate. CoinImp results were peculiar, since the script had the minimum number of websites Indicted for cryptojacking.

F. *Distinct behaviors*

Finishing the analysis of results, some of the observations obtained during the tests are worth mentioning and should be further analyzed, since they showed some distinctive particularities and behaviors, with emphasis on the cases described below:

- Some sample websites belonged to companies, news agencies or government departments, such as a website[3] registered to "Instituto Nacional de Salud Agrícola Integral", which belongs to Venezuelan Government. In this case it was not possible to confirm through tests the presence of mining, although it is worth mentioning that this website fits to the sample for containing the CoinImp script. This data reinforces the notion that, when there are fragilities within systems and websites, these can be exploited by harmful agents, who take advantage of these weaknesses to introduce mining scripts which will be undetected by the websites' owners. These agents then profit from what users deem as viable/safe/legitimate;
- Another interesting case occurred when websites presented an initial loading period showing inconsistent resource usage, but without reaching alarming levels. After two minutes, a clear mining activity is registered, apparently programmed to consume roughly 50% of the system's processing power. These noteworthy results manifest the importance of a wide testing time amount. If a shorter test was made, the mining activity would not have been detected. The way the script works is specially deceiving for users, since it not only makes it difficult to detect mining activity by only using half of the processing power, but also has a delayed activation time, or an activation linked to minimal profit, reducing the ability of the user to see a cause-effect relation between opening the website and the slowing down of the system;
- Taking into account the graph shown in Fig. 17, some websites started CPU usage through a certain period of time, to then drop it to reduced values. A few websites kept reduced CPU usage values throughout the remain duration of the test, apparently showing that they were no longer mining, even considering that was the case at first. Other set of websites, such as this example, raised their rates again after some time passed. These cases were also considered to be related to harmful agents using mining rentability settings.

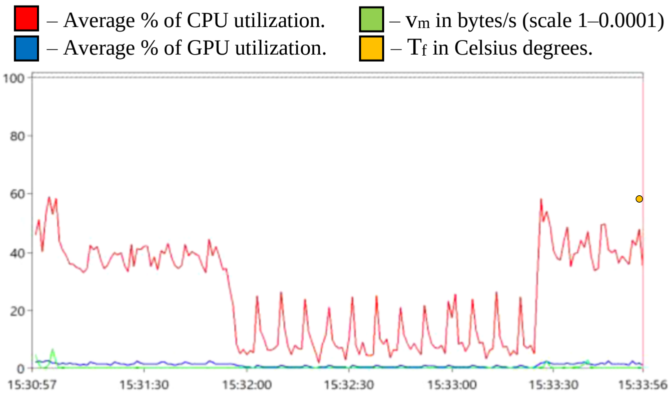

Fig. 17. Results obtained for `http://legendaoficial.net` (Indicted), running Firefox on Linux, for 3 minutes.

IV. CONCLUSION

Have being studied the cryptojacking malware phenomenon, first by theory and then through practical experimentation, it is now relevant to mention its most important achievements.

The set of contents presented in this paper concludes with the following:

- Crypto mining malwares peaked between 2017 and 2018, coinciding with a strong appreciation of some cryptocurrencies;

[3] URL: `insai.gob.ve`.

- The value of cryptocurrencies and the change of mining complexity are two factors associated with the evolution and spread of cryptojacking;
- There are types of mining malwares that work differently depending on the particulars of the affected OS and browser, making it clear that the lower the performance effects, the harder it will be to detect mining activities;
- Cryptojacking attacks can be detected by analyzing the performance of the affected system, since for mining activities to be effective and profitable, the way CPU performance is affected presents recognizable patterns;
- In addition to the performance effects mentioned by most authors, such as increased CPU or GPU utilization, it has also been found by this study that the temperature achieved by the system, which proved a moderate positive correlation with the utilization of CPU, is relevant for mining activity research, as some performance measurement mechanisms can be fooled by some scripts;
- No connection could be proven between the average network transfer speed (download and upload) of a system and the presence of mining activity.

ACKNOWLEDGMENT

I would like to express gratitude to my dissertation Adviser, Prof. Dr. Miguel Correia (IST – Lisboa) for all the general support, the sharing of wisdom, and the assistance carried out during the research.

V. REFERENCES

[1] Arnold, A.: 30% Of Millennials Would Rather Invest In Cryptocurrency (2018), https://www.forbes.com/sites/andrewarnold/2018/01/07/30-of-millennials-invest-in-cryptocurrency-here-are-3-tips-to-help-you-do-it-smarter, accessed in 2018/12/07.

[2] Bissaliyev, M., Nyussupov, A. e Mussiraliyeva, S.: Enterprise Security Assessment Framework for Cryptocurrency Mining Based on Monero. Journal of Mathematics, Mechanics and Computer Science, 98, 67-76 (2018).

[3] Cisco: Cybersecurity Special Report – Small and Mighty – How Small and Midmarket Busineses Can Fortify Their Defenses Against Today's Threats. Cisco Systems (2018a).

[4] CoinImp: Documentation of Monero JavaScript Mining (2019), https://www.coinimp.com/documentation, accessed in 2019/03/27.

[5] Cyber Threat Alliance: The Illicit Cryptocurrency Mining Threat (2018), https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf, accessed in 2019/09/27.

[6] Egele, M., Scholte, T., Kirda, E., e Kruegel, C.: A Survey on Automated Dynamic Malware-Analysis Techniques and Tools. ACM Computing Surveys, Vol. 44, No. 2, Article 6, 2-42 (2012).

[7] European Union Agency for Network and Information Security (ENISA): Cryptojacking – Cryptomining in the browser (2017), https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser, accessed in 2019/01/18.

[8] Eskandari, S., Leoutsarakos, A., Mursch, T., Clark, J.: A First Look at Browser-Based Cryptojacking. IEEE Security & Privacy on the Blockchain (2018).

[9] Evangelho, J.: Nvidia CEO – "We're Not Anywhere Near" Meeting GPU Demand (2018), https://www.forbes.com/sites/jasonevangelho/2018/03/27/nvidia-ceo-were-not-anywhere-near-meeting-gpu-demand, accessed in 2018/11/27.

[10] Galal, H., Mahdy, Y. e Atiea, M.: Behavior-based features model for malware detection. Journal of Computer Virology an Hacking Techniques, ISSN 2274-2042, Vol. 2, Issue-8, 54-56 (2015).

[11] Hurley, J. e Chen, J.: Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018). National Defense University Washington DC, USA (2018).

[12] Lau, H.: Browser-Based Cryptocurrency Mining Makes Unexpected Return from the Dead (2017), https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency, accessed in 2019/01/23.

[13] Lopatin, E.: Kaspersky Security Bulletin 2018 – Story of the year – Miners (2018), https://securelist.com/kaspersky-security-bulletin-2018-story-of-the-year-miners/89096, accessed in 2018/12/23.

[14] Marr, B.: A Very Brief History Of Blockchain Technology Everyone Should Read (2018), https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#4d7cc2a37bc4, accessed in 2019/01/16.

[15] Marr, B.: The 5 Big Problems With Blockchain Everyone Should Be Aware Of (2018a), https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#59da16a31670, accessed in 2019/01/16.

[16] McAfee: Threat Report – Don't Join Blockchain Revolution Without Ensuring Security. McAfee Labs Threats Report (2018).

[17] Microsoft: Surface Pro (5.ª Geração) – Especificações Técnicas (2019), https://www.microsoft.com/pt-pt/p/surface-pro-5ª-geracao/8NKT9WTTRBJK, accessed in 2019/03/16.

[18] Murray, M.: A Reuteurs Visual Guide – Blockchain explained (2017), http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html, accessed in 2018/12/18.

[19] Mursch, T.: How to find cryptojacking malware (2018). https://badpackets.net/how-to-find-cryptojacking-malware, accessed in 2019/04/14.

[20] Peck, M.: Blockchains – How They Work and Why They'll Change the World (2017), https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world, accessed in 17/03/2019.

[21] Pinheiro, A., D'Espiney, J. e Barroso, R.: Venda de casas em bitcoins já chegou a Portugal (2018), https://www.dn.pt/dinheiro/interior/venda-de-casas-em-bitcoins--ja-chegou-a-portugal-9029355.html, accessed in 2018/11/27.

[22] Rauchberger, J., Schrittwieser, S., Dam, T., Luh, R., Buhov, D., Pötzelsberger, G. e Kim, H.: The Other Side of the Coin: A Framework for Detecting and Analyzing Web-based Cryptocurrency Mining Campaigns. ARES 2018 – International Conference on Availability, Reliability and Security, 1-10 (2018).

[23] SAPO TEK: Máquina de criptomoedas chegou a Braga e pode estar a caminho de outras cidades (2018), https://tek.sapo.pt/noticias/computadores/artigos/maquina-de-criptomoedas-chegou-a-braga-e-pode-estar-a-caminho-de-outras-cidades, accessed in 2018/11/26.

[24] Suleiman, B. e Husain, R.: Study of Computer Malware and Its Taxonomy. International Journal of Engineering and Applied Sciences, ISSN 2394-3661, Vol. 2, Issue-8, 54-56 (2015).

[25] Symantec: 2018 Internet Security Threat Report [ISTR], Vol. 23 (2018), https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf, accessed in 2019/01/04.

[26] United States Computer Emergency Readiness Team (US-CERT): Security Tip – Defending Against Illicit Cryptocurrency Mining Activity (2018), https://www.us-cert.gov/ncas/tips/ST18-002, accessed in 2019/01/18.

[27] Xie, M.: Bitcoin Mining Is More Popular And More Destructive Than Ever (2018), https://www.forbes.com/sites/forbestechcouncil/2018/05/24/bitcoin-mining-is-more-popular-and-more-destructive-than-ever/#5186db4d4f1f, accessed in 2018/12/20.

[28] Wolfson, R.: Cryptojacking On The Rise: WebCobra Malware Uses Victims' Computers To Mine Cryptocurrency (2018), https://www.forbes.com/sites/rachelwolfson/2018/11/13/cryptojacking-on-the-rise-webcobra-malware-uses-victims-computers-to-mine-cryptocurrency, accessed in 2018/11/29.

[29] WorldCoinIndex: Monero Gráficos (2019b), https://www.worldcoinindex.com/pt/Moeda/monero, accessed in 2019/01/18.