DOI: 10.15611/2023.96.1.05

5 Cryptojacking: Definition, Implementation, Effects and Protection Against That Form of Cyberattack. Is Malicious Cryptomining a Manifestation of the Crisis Behaviour of Individual Miners During Cryptocurrency Rush?

Tomasz Hetmańczuk

WSB Merito University Wroclaw
e-mail: tomasz.hetmanczuk@wroclaw.merito.pl
ORCID: 0000-0002-6948-9428

Cite as: Hetmańczuk, T. (2023). Cryptojacking: Definition, Implementation, Effects and Protection Against That Form of Cyberattack. Is Malicious Cryptomining a Manifestation of the Crisis Behaviour of Individual Miners During Cryptocurrency Rush? In A. Styś (Ed.), *Reactions of Market Entities to Crisis Situations* (pp. 73–96). Wroclaw: Publishing House of Wroclaw University of Economics and Business.

5.1. Cryptojacking: A New Form of Cybercrime

The dynamic progress of information technology observed in recent years and the unlimited possibilities offered by the Internet may also have negative effects in certain situations. New and more sophisticated methods of preying by hackers on ordinary users of the global network are emerging. Generally, it is about making profits illegally, at the expense of unaware owners of computers and other digital devices operating under the supervision of operating systems. One such cybercrime, closely related to cryptocurrency mining, is the so-called cryptojacking, which is also called malicious mining (Gaździcki, 2021). In the opinion of many economists, resorting to cryptojacking by some miners generating virtual currencies may be considered a manifestation of crisis behaviour on their part. It results mainly from economic reasons, focused on "optimizing" costs related to cryptocurrency mining. High prices of equipment used for mining and still rising electricity prices "incline" some cryptocurrency miners to take criminal action, to take advantage of the scale effect and significantly increase their chances of finding another block and attaching it to Blockchain, while "collecting" due remuneration, i.e., block reward expressed in units of a given cryptocurrency.

The economic profitability of mining is largely dependent on the costs of electricity consumed in this high energy-consuming process. Cryptocurrency mining rigs generate huge electricity demand, because they constantly perform billions of complicated calculations per second to find the right string of characters, i.e., hash. The power consumption of such a virtual coin digger, and therefore the cost of electricity, is so high that it can exceed the revenue from mining cryptocurrencies. Hence the constant search, by persons conducting mining activities of virtual currencies, for cheap electricity or "free computing power" from the illegal takeover of other users' hardware resources connected to the Internet. In addition, the crisis behaviour of individual cryptocurrency miners is partly due to the high degree of monopolization of cryptocurrency mining. In this situation, the possibilities to cope with hard competition in the so-called race to find the next block are disproportionately small for individual miners, compared to large installations operated by agreements and associations of cryptocurrency miners.

For obvious reasons, the greatest interest in mining Bitcoin and other cryptocurrencies occurs during periods of speculative bubbles on the market of these virtual assets. Then, attacks in the form of cryptojacking on computers belonging to unaware users are intensified, because the rapidly growing valuation of a given cryptocurrency in fiat money creates space to achieve much higher profits from mining. In such situations, "taking advantage" of cryptojacking, which is *de facto* "free" virtual digging at the expense of others, brings tangible benefits from this criminal practice. The profit and loss account for the miner-hacker does not include then the variable cost item, in the form of electricity consumed, and fixed costs related to the purchase of additional mining equipment, its operation, service and depreciation. To put it simply, if a miner takes the liberty to undertake cryptojacking, the obtained revenues are equal to cryptocurrency mining income.

5.2. The Essence of Cryptojacking

Cryptojacking is an IT term describing the practice of taking over resources and computing power of a computer illegally to mine cryptocurrencies at the expense of the unconscious owner of the equipment. This is done without the consent and knowledge of the user, because the device has been tricked into malicious code, enabling the miner to derive financial benefits from working on the computer network of the victim of cryptojacking. In other words, cryptojacking is a criminal version of mining.

According to the US Cybernetic Security & Infrastructure Agency (CISA) "cryptojacking occurs when cybercriminals use malicious code and effectively take over the computing power of victims' devices and systems, using vulnerabilities in websites, software and operating systems to illegally install cryptocurrency mining software on victims' devices and systems (Cybersecurity and Infrastructure Security Agency [CISA], 2021). This definition by CISA clearly and comprehensively addresses the issue of cryptojacking. It indicates directly who practices cryptojacking, how such a cyberattack is carried out, and what purpose

it serves. On a legal basis, there can be only one interpretation of cryptojacking: it is a form of theft of the computing capacity of devices and their users' systems by illegally installing malware to dig cryptocurrencies. It is worth mentioning that some other definitions of cryptojacking also use this term to determine the form of cryptocurrency theft by cyber criminals that consists in the use of malicious scripts and codes for the illegal takeover of the content of the cryptographic wallet of computer owner.

All criminal activity based on cryptojacking and thief practices of miners-hackers are subordinated to single goal – acquiring "free computing power" to be used for "cost-free" mining of the so-called fossil cryptocurrencies (mineable cryptocurrencies), by creating a special type of mining rig based on the summarized ability to process data from foreign devices, without the legal right to use them.

To this type of robbing, being in fact the illegal takeover of the electronic ability of a digital machine to perform ultra-quick arithmetic operations in a specific unit of time, are exposed desktop computers, laptops, tablets smartphones and servers, as well as other network devices. It does not matter under the supervision of what operating system they work (is it Windows, Linux, MacOS, Android or iOS), the only condition is Internet connection.

In addition, also at risk are devices operating in a system that enables automatic communication and data exchange via networks without human intervention, i.e., the Internet of Things (IoT)[1]. This can be explained as a network of physical objects that are equipped with sensors, special software and other technological solutions enabling connection, data exchange with other devices and systems via the Internet. It is estimated that in 2020 in the world there were over 10 billion devices connected to the IoT infrastructure, covering both ordinary household items (e.g., TV, cameras, refrigerators, washing machines, dryers, etc.), as well as advanced industrial tools (e.g., intelligent digital supply chains, intelligent production, intelligent power networks and smart cities), and by 2025 their number may increase to as much as 31 billion (Lueth, 2020). It is worth noting that in 2017 Symantec, an antivirus software manufacturer, recorded a huge increase in the total number of attacks on devices operating in the IoT system, by as much as 600%. This means that cybercriminals have used and will probably continue to use the network nature of these devices for mass mining of cryptocurrencies.

The most frequently attacked are private user computers and servers in data centres of companies and enterprises operating in various areas of the economy, as well as public organizations and institutions. The dominant motivation for resorting to such immoral and pirate methods by some cryptocurrency miners is the desire to achieve maximum profits from the mining process, with the peculiar method to "optimize" own costs by taking over a specific percentage of computing power of individual devices equipped with processors in combination with the scale effect achieved by mass infection. This mechanism (based on maximizing the number of infected digital devices in the network) is used to compensate in

[1] At present, more and more frequently the term "Intelligence of Things" is used.

some way for the relatively small "output" from the computing power of individual computers belonging to individual Internet users.

Sneaky infection of the potential victim's computer occurs *via* such e-mail that appears to be a reliable message from an allegedly verified sender, but contains the fabricated file (usually in the compressed archive form) or a link to some malicious program. Cybercriminals deliberately use the so-called phishing, i.e., the phenomenon of impersonating other people or institutions that are widely recognized and usually enjoy great social trust (Pieleszek, 2019, pp. 35–48). These include, for example: police, border guards, and other uniformed services, banks, post office, courier companies, prosecutors, courts, notary offices, law firms, brokerage houses, social insurance institutions, insurance companies, tax offices, mobile operators or electricity suppliers. Opening such an attachment by the user is equivalent to installing a virus that constantly "steals" a certain percentage of the computing power of the owner's device. From this moment the threat is already permanent, and cryptocurrency mining activity is resumed after each time the computer is started and the Internet is connected. The whole process takes place in the background of the data processing process by the user's computer, so it is not easy to uncover.

It should be noted that malicious cryptocurrency mining scripts can also be hidden inside advertisements, browser plugins and content management system plugins. In such cases, no other user action is required to infect the computer. All you have to do is visit specific websites or install and enable the plugin, and cryptojacking will be done at its best. Cybercriminals can also use the user's (victim's) cloud computing infrastructure by taking over access rights, i.e., API/SSH keys.

5.3. The Course of Cryptojacking Attack

By using a specially written and fabricated script, hackers gain unauthorized access to the hardware resources of users connected to the Internet. The processor power (CPU) and/or graphics card (GPU) of the victim's computer for such a sneaky attack is "included" into the cryptocurrency mining process. This happens in a camouflaged manner and is difficult to detect by an ordinary computer or smartphone owner. Attackers cynically use the multiplied computing power of virus-infected computers to unaware users. The more victims are "caught" in this hidden net, the faster the efficiency of mining, and competitive advantage over other miners increase.

In fact, the cybercriminal "creates" a special infrastructure infected with malware devices called botnet which it manages in connection with mining at the expense of other users. The theft of "only" a small part of the computing resources of a single digital machine user is a "thoughtful" strategy of cybercriminals from the group of cryptocurrency miners, aimed at making it difficult for computer owners to detect their mining practices and limit the effective elimination of these types of threats.

Cryptojacking itself is constantly evolving. Initially, malware absorbed 100% of the computing power of the affected victim's computer processor. It was a very "effective" method only in the short run, because the user could easily realize that his computer was working incorrectly (huge slowdown in system operation, loud operation of the cooling system, which is accompanied by too frequent switching of fans at higher or maximum speeds). In the case of laptops and smartphones, there was also the effect of excessive heating of the device and "battery drainage". Sooner or later, it must have caused the user's concern and attempts to look for the reasons for this. As a result, cryptojacker was detected relatively quickly and at this point all criminal practices were successfully terminated.

Cryptojacking, which took over almost 100% of computing resources, could cause serious damage to the victim's equipment, speeding up processor wear and tear, and even its damage (smartphones and tablets) together with shortening battery life (laptops and other mobile devices). The rapid deterioration of the parameters of a computer or other device could cause concern to the user and take a number of actions to determine the sources of this incorrect work, which resulted from an effective cryptojacking attack. The second, more sophisticated method of mining using cryptojacking is to modify the malicious code so that the script "provides" cybercriminals with only the planned fraction of the computing power of the victim's computer, with long and unnoticeable operation. The longer such a harmful script remains undetected by the user or antivirus software, the greater the benefits for the hacker and the higher damage to the cryptojacking victim.

Figure 5.1 illustrates the processor's operation on the user's computer on which malware for cryptojacking has been running in the background. The processor idle load is on average 10% of its total performance. At the time of the attack, switching on a script that illegally mines cryptocurrencies, there is a sharp jump in CPU usage (even above 90%). After a short time, it stabilizes at 80–90% of the CPU computing power. The harmful script has been designed so as not to engage 100% processor power, because the user could quickly realize that some process running in the background is excessively consuming its resources. There are also modifications to malware that engage only 30–60% of CPU computing power. In this way, they are more difficult to identify and remain undetectable for a long time. You can defend yourself against such an attack by installing the appropriate browser plugins or using AdBlock – the software blocking ads and java scripts on websites (the vast majority of infections occur when browsing Internet resources). However, this is associated with limiting the comfort of browsing websites (not all options are available and not all information is displayed correctly). Whereas, if you open the attachment attached to e-mail message or run a program downloaded from an illegal source, the only barrier that computer can detect and block such malicious scripts are various anti-virus soft wares. Unfortunately, they are not able to identify correctly all threats related to cryptojacking.

The strategy of cybercriminals using cryptojacking in the process of mining cryptocurrencies is to "hack" to the largest number of devices, not oriented and unaware users, to take profits from the so-called scale effect. This is especially important when the miner-hacker "collects" only a small percentage of computing resources from each device.

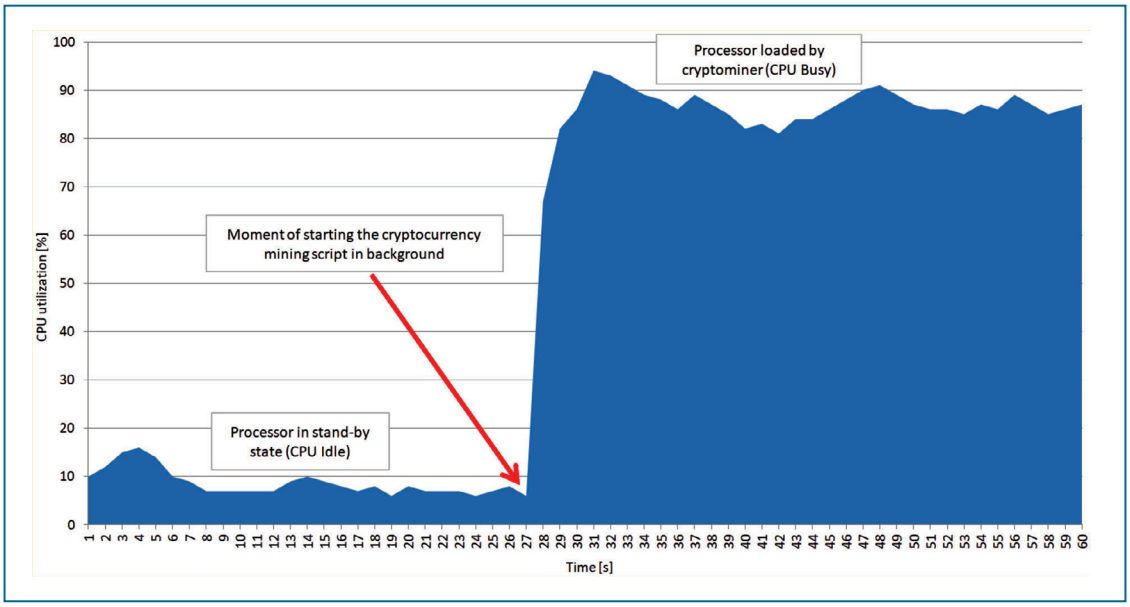


Figure 5.1. Load of the (CPU) processor during its inactivity and at the time of the attack using a malicious cryptocurrency mining script

Source: own study using MS Excel.

Due to this approach, the number of infected computers must go into hundreds, thousands or even millions. Everything is subordinated to the fact that such a cybercriminal can conduct low-cost or often cost-free mining activities.

The first generation of malicious codes used in cryptojacking was based on the so-called thief's call to action (Pieleszek, 2020). This means that the potential victim had to "take the initiative" by opening the attachment in an e-mail, by clicking on the fabricated link, or by downloading and running the file sent from an unknown source. At this point, the operating system was infected by malware, being added as a service and continuously operating in the background. In this simple but insidious way, the hidden cryptominer installed on the victim's computer. It was, in fact, one of the forms of long-used by the cybercriminals phishing[2].

[2] Phishing is a special method of cheating an unconscious and reckless user. It serves, among others, to infect a computer with harmful software, persuade the victim to perform specific actions or extort confidential information. For example, by means of a fabricated website or e-mail, cybercriminals acquire proprietary data that the victim himself voluntarily provides. She is convinced that she logs in to a bank or other website. It is also common practice for hackers to send false e-mails whose content prompts the user to open an attachment in which a harmful code is placed. The essence of phishing is not related to software or the equipment itself, but is based on social engineering and manipulation, where the weakest link is the human factor. Security specialists distinguish 12 basic forms of phishing (for example Clone phishing, Spear phishing, Pharming, Whaling, Email Spoofing, Website Redirect, Typosquatting, Watering Hole and Giveaways) (*Co to jest phishing...*, 2023; *What Is Phishing?*, 2022).

Increasing users' awareness of online security threats, including phishing, "forced" hackers to increase the level of advancement of such an attack. It had to be more sophisticated and reaching more people. This is how the second generation of cryptojacking was initiated, in which the Internet user no longer had been left with the "initiative" (e.g., opening the attachment or downloading and running the file), but all that was needed was to visit an infected website that contained implemented JavaScript malicious code (web-based cryptojacking). Currently, most of the harmful cryptocurrency mining software on third-party devices is launched through scripts embedded in the source code of the website. This process is presented in Figure 5.2. The cryptojacking miner-hacker attack begins by placing a malicious code or script on a website through its "injection", i.e., placing a fabricated ad or using a security vulnerability. When an unconscious user visits such an infected website, the malicious code is executed in his web browser and the computer's operating system is infected. From that moment, the equipment of the victim of such a cyberattack becomes a cryptocurrency mining rig that creates virtual currencies for the benefit of a cybercriminal, and all this is done without the knowledge and consent of the device owner. The block mining reward, i.e., the funds of a given cryptocurrency, goes to the cryptocurrency wallet of a miner-hacker. In this way he used the victim's computing power and did not incur any costs related to mining.

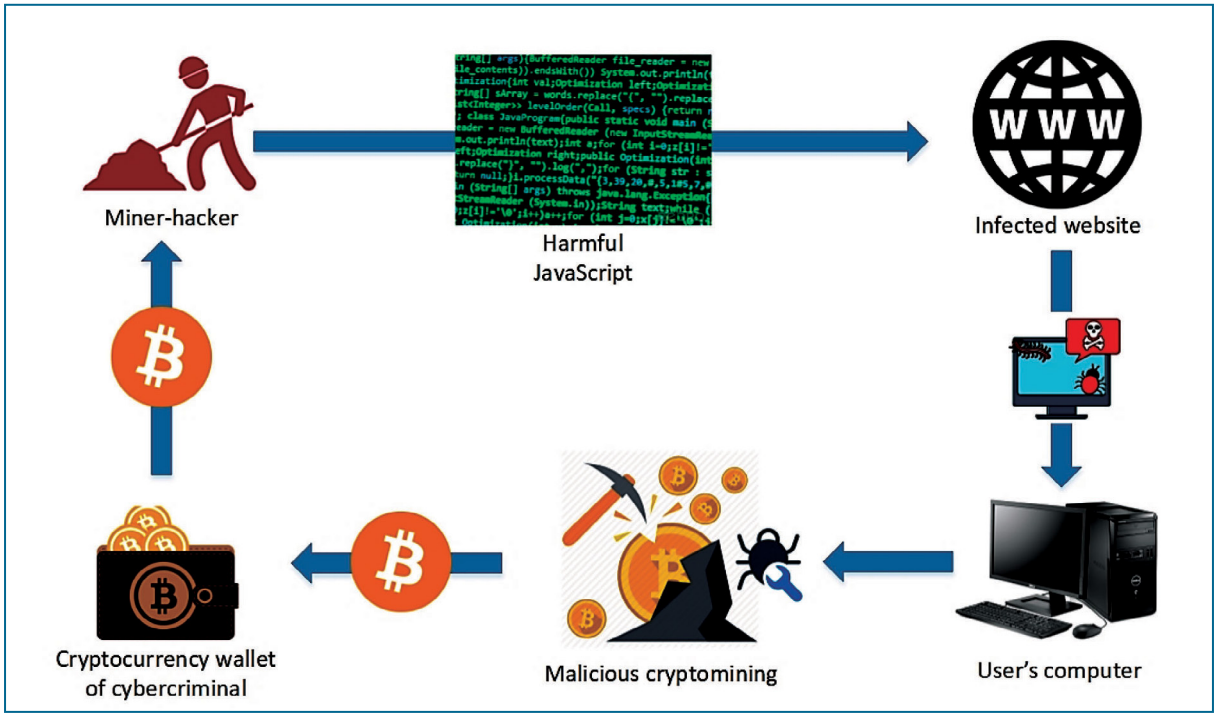


Figure 5.2. A mechanism of cryptojacking action involving placing a malicious script in the source code of a website

Source: own study using MS Visio.

It is worth recalling that Bitcoin mining (or other mineable cryptocurrencies) is the process of creating new BTC units by solving extremely complicated math problems that verify transactions in that virtual currency. When a block is successfully mined, the miner receives a predetermined amount of Bitcoins as a reward.

To sum up, the actions of cybercriminals "practicing" cryptojacking have evolved over time, because they quickly realized that attempts to take over 100% of the computing power of attacked computers can be easily detected, even by an inexperienced user. And then after clearing the browser cache memory or restarting the computer, they lost the cryptojacking victim's computing ability. New versions of this tricky software are more "intelligent" and quite effectively mask their presence. They are primarily focused on the longest possible operation of the infected computer. Therefore, malicious scripts often use only about 1/5 of the processor's computing power so as not to arouse suspicion of the workstation owner. They are constructed in such a way that they make the most of the idle mode (maintenance mode) of the device and then perform the calculations most aggravating the processor. When the user returns to normal operation, they go into "economical" (20–30% CPU load), not to reveal their presence in the operating system and be able to "rob" a victim of its resources and electricity for a very long time, remaining undetected.

5.4. Scale and Examples of Cryptojacking

It is difficult to estimate the scale of cryptocurrency mining using cryptojacking, because official data and statistics are lacking, and the phenomenon itself is still under-explored. It can only be said with certainty that such attacks around the world can be counted in millions. For example, according to the report of November 21, 2017 by Adguard (a company that launches web browser plugins that block unwanted ads and harmful scripts – e.g., AdGuard AdBlocker and Adguard Web Filter), about 33,000 websites were identified that contained a malicious script for mining cryptocurrencies. The analysed sites generated more than a billion entries per month. Adguard was able to determine that within one month there was an increase of as much as 31% in the number of websites that cybercriminals tricked into mining cryptocurrencies (run in-browser mining)[3]. It is estimated that such an increase was caused by one of the largest speculative bubbles on the Bitcoin market that was formed at that time. In turn, the Bad Packets report in February 2018 (Mursch, 2019) already showed over 34,000 pages (34,474), on which hackers secretly launched the most popular cryptocurrency mining script called "CoinHive".

It is worth knowing that cryptojacking does not require any special IT skills (programming, knowledge of the basics of computer networks, or web design). For example, in

[3] "We found cryptojacking scripts on over 33,000 sites with a total traffic of 1 billion monthly visits. The number of sites from Alexa's top 100K list which run in-browser mining grew by 31% over the past month. The overwhelming majority of sites don't bother to warn users or get their consent to mining" (Meshkov, 2022).

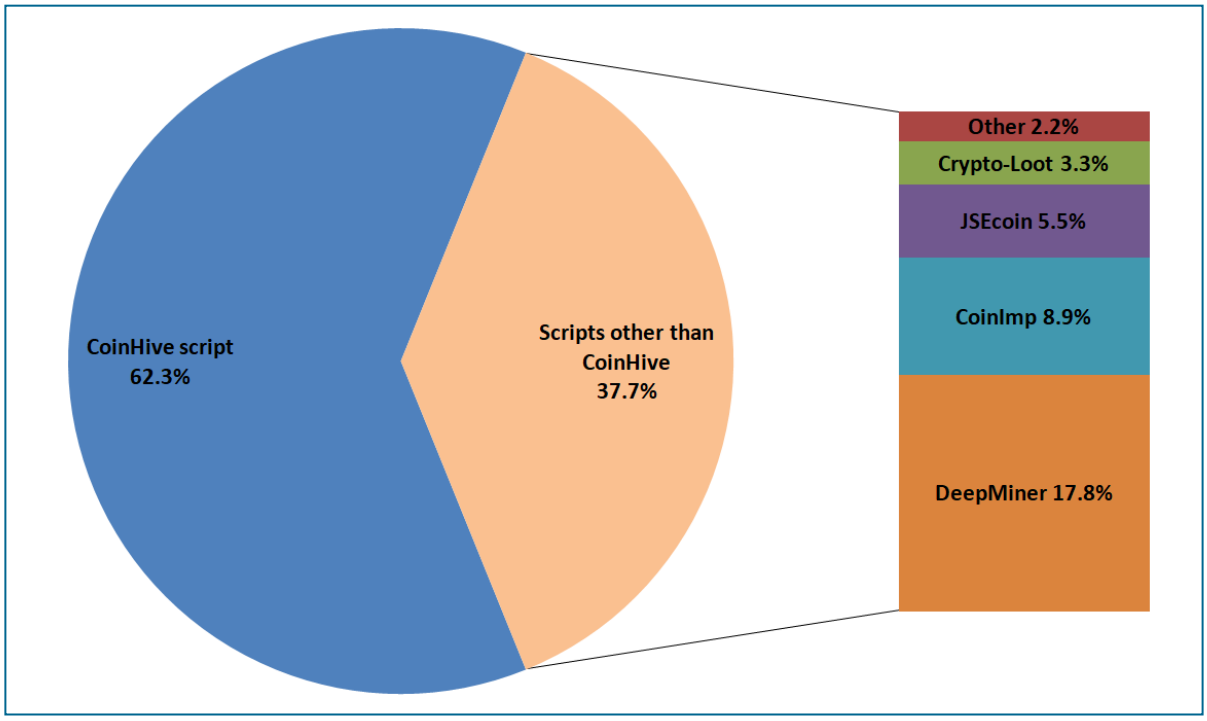
the so-called underground and illegal Internet (Darknet) criminals offer ready-made cryptojacking toolkits for only USD 30. This cost, combined with the prospect of mine a large number of cryptocurrency units, without incurring the cost of purchasing equipment and charges for electricity consumed, makes cryptojacking a very profitable practice. Often, thanks to cryptojacking, hundreds, thousands and even millions of devices dig up non-stop cryptocurrencies. The risk of detecting this malware is relatively small, as such a script can work for a long time imperceptibly (stealth mode). In addition, cybercriminals do not run the risk of prosecution by the relevant services because they do not steal any user data and do not encrypt his hard drive, as is the case with cryptolockers (ransomware). The most famous example in the world of blackmail software was the worm attack "WannaCry", which in May 2017 infected over 300,000 computers in 99 countries. Cybercriminals are increasingly less interested in using ransomware that encrypts users' hard drives to raise funds for "unlocking" access to data carriers. To avoid being targeted and identified by law enforcement, criminals forced a ransom in Bitcoins or other cryptocurrencies. The decline in popularity of malware encryption resulted, among others for two reasons.

First, only a small percentage of users (around 3%) whose hard drives have been encrypted, were willing to pay the ransom. Quite often this was one-time earning for hackers. However, cryptojacking brings income in the long run. In addition, many companies (banks, institutions, corporations, offices and enterprises) regularly back up their data and can easily restore data resources that have been blocked. This means that cyber blackmailers will never receive ransom money from these entities. In addition, companies that create antivirus programs enrich them with additional scanning modules that are able to detect and block such malware. The mechanism for isolating running programs, open attachments and websites in an environment specially separated from the operating system is also very useful. It is called sandbox.

Secondly, people who demand ransom for unlocking user data commit an obvious crime and expose themselves to criminal liability. A hacker intending to use blackmail software must somehow "reveal", by sending a crafted account number, specially prepared mail to contact the victim, etc. This can help law enforcement authorities identify such a criminal operating on the TOR (Darknet) network. In the case of cryptojacking, the miner-hacker basically becomes anonymous all the time and it is difficult to "track down". Unlike most malware software, cryptominer scripts do not cause damage to seized hardware and operating system, but only use the processor and/or graphics card computing power. Cybercriminals stealing computing power of computers of Internet users, to mine Bitcoin or other cryptocurrencies, are primarily guided by fast and high profit ("cost-free" mining). When it comes to the possibility of maintaining almost 100% anonymity, cryptojacking works well for altcoins such as Monero (XMR) and Zcash (ZEC). In the opinion of experts, in the case of Bitcoin one cannot speak of full anonymity, but only pseudo-anonymity.

Figure 5.3 presents the most commonly used scripts that illegally mine cryptocurrencies. The most popular among cybercriminals was the CoinHive script, based on the JavaScript programming language. This was due to its large configuration capabilities and easy imple-

mentation on the website. It did not require particularly deep knowledge of programming and hacking techniques. It was enough for an amateur of illegal mining cryptocurrencies to paste the two-lines code into the source of the page. Such a short script enabled the automatic execution of malicious code in the victim's web browser. The CoinHive script is also compatible with all the most popular web browsers and is relatively easy to implement.



Other (2.2%): Minr, ProjectPoi, CoinNebula, MinerAlt and CoinRail.

Figure 5.3. Structure of Java malicious scripts used by cybercriminals divided into CoinHive and scripts other than CoinHive

Source: own study using MS Excel based on https://badpackets.net.

For the reasons indicated above, CoinHive came first among all malicious codes used for cryptojacking. CoinHive is used by cybercriminals for attacks *web-based cryptojacking* on hacked websites. In other words, it is implemented without the knowledge and consent of website owners. This was done by using vulnerabilities in server or web application configurations. The most frequently attacked in our country were websites of national or local newspapers. This was mainly due to two reasons. First of all, the administrators of these websites did not carefully verify the ads placed on their pages, and indeed such ads written in Java were "carriers" for cryptominers. Secondly, cybercriminals were interested in sites with poor security and at the same time generating heavy traffic (a large number of visitors), as is the case with newspapers and online periodicals. As already mentioned, the

most "popular" among cybercriminals using cryptojacking is JavaScript called CoinHive. It has been identified on over 62% of affected sites that have been dragged into a hidden mining process. Among the group of other scripts, DeepMiner (17.8%) and CoinImp (8.9%) were most commonly used. In June 2018, Check Point Software Technologies revealed that 4 out of 10 detected malicious codes (malware) were so-called cryptominers, i.e., scripts used by hackers for cryptojacking. CoinHive dominated here. In summary, it can be stated that the CoinHive script was the undisputed leader among malware for cryptojacking. Almost every fifth malicious code is DeepMiner, and every tenth is CoinImp, while every twentieth is JSEcoin.

It is worth knowing that cryptojacking has undergone a kind of evolution. Initially, scripts for capturing computing power of unaware users were placed only on pages with unchecked reputation and widely recognized as harmful (e.g., pages with illegal software, illegal music and movies, such as The Pirate Bay and adult content sites). Over time, however, cybercriminals began to infect sites that generated very high network traffic and were widely recognized as safe. Hackers in Poland even went so far as to install malicious scripts (mainly CoinHive) on pages enjoying high attention and widespread prestige (e.g., YouTube, *Rzeczpospolita*, *Gazeta Wyborcza*, *Gazeta Wrocławska* and other local dailies as well as naszemiasto.pl, parkiet.com, motofakty.pl, muratordom.pl or telemagazyn.pl).

In February 2018, a malicious script used for cryptomining was detected on the *Los Angeles Times* website (O'Donnell, 2019). According to cybersecurity specialists, CoinHive software dedicated to illegal cryptocurrency mining, which was embedded on the *LA Times* (cryptojacking code, was hidden on the interactive page of the kill report – *Homicide Report*), was also implemented on the government websites of Great Britain and the USA. RedLock (RedLock Security Blog. Cloud Threat Defense) reported that the manufacturer of Tesla electric vehicles also fell victim to cryptojacking. Cybercriminals have placed in the corporate cloud environment malicious scripts mining cryptocurrencies.

Currently, the most common form of cryptojacking is the so-called web-based cryptojacking (drive-by cryptomining). Malicious scripts are embedded on the website and when it is opened by the user, it is automatically initiated to mine cryptocurrencies by the browser. The success of such criminal practice depends to a large extent on how cryptominers will be hidden in the source code of the website or in displayed ads on the site.

It is worth recalling that in September 2017 the official CoinHive script appeared (based on the Java programming language), which allowed website owners to earn legally, without having to display intrusive and annoying ads for users. A person visiting such a site was informed about it and had to agree to it. In this way, the user knowingly "provided" a certain percentage of the computing power of his processor and/or graphics card to support the creator who provided the content he created for free. The website owner officially earned by mining cryptocurrencies on the equipment of users visiting his website, and not on ubiquitous advertisements that generated much less revenue and discouraged Internet users from entering such a website. The web administrator had double benefits: his site was higher positioned in search results and earned legal mining income. Over time, the above-

-mentioned script began to be used to illegally take over the computing power of Internet users' equipment. After loading the selected website, the user was no longer asked for permission for use computing power of his computer. He was completely unaware that such a process had already been initiated, and he himself was insidiously manipulated. This was done in two ways. In the first case, the website owner/administrator himself intentionally and thoughtfully placed the mining script on his own website without informing users. Cryptocurrencies mined by this method were pure profit for him. The second option is related to the activities of cybercriminals who illegally placed cryptominers (without the consent and knowledge of the website administrator) in the source code of the page. The site owner did not benefit from it, and hackers took over all the income from cryptojacking. According to Internet cybersecurity experts, the CoinHive script became the biggest threat among malware in the first half of 2018. He even overtook ransomware attacks and Trojans stealing login details for electronic banking. According to the Symantec Internet Security Threat Report, in 2018 the number of ransomware attacks dropped significantly, in contrast, there was a real plague of cryptojacking attacks (Symantec, 2019).

There are really many examples of cryptojacking. Here are some of them related to the use of CoinHive.

December 2017 – malicious CoinHive script was secretly implemented by the owner of the Starbucks chain in Buenos Aires. Customers using the free WiFi network at the company's premises were tricked into mining Monero cryptocurrency on their laptops and smartphones.

January 2018 – on the largest platform offering video streaming, i.e., YouTube, CoinHive was hidden in ads displayed while watching movies.

The turn of July and August 2018 – an attack was carried out on over 200,000 MikroTik routers in Brazil. Each user using wireless networks provided by these routers unknowingly participated in mining cryptocurrencies. The attack using the CoinHive code was intended on a large scale.

The increase in the scale of cryptominers' attacks was associated, among others, with the emerging speculative bubble on the Bitcoin and Ethereum markets. It was the strong economic stimulus that encouraged to intensively mine cryptocurrencies, also using illegal cryptojacking.

Figure 5.4 shows how the use of malware for cryptojacking has changed. In the period from first to third quarter of 2017, the number of uses of this type of software increased moderately. In the fourth quarter of 2017, compared to the previous quarter, attempts to use the malicious code for illegal cryptocurrency mining doubled (100% increase). This was strongly correlated with the speculative bubble formed on Bitcoin (at that time, other mineable cryptocurrencies also followed its trend).

Starting from the first quarter of 2018, there has been a rapid increase in the use of this type of software in taking over the computing power of Internet users. On average, there were 2.5 to 3.8 million new threats related to cryptojacking every quarter. In just two years (2017–2019) almost 16 million different versions of malware software willingly used by cybercriminals to mine cryptocurrencies without the knowledge and consent of computer

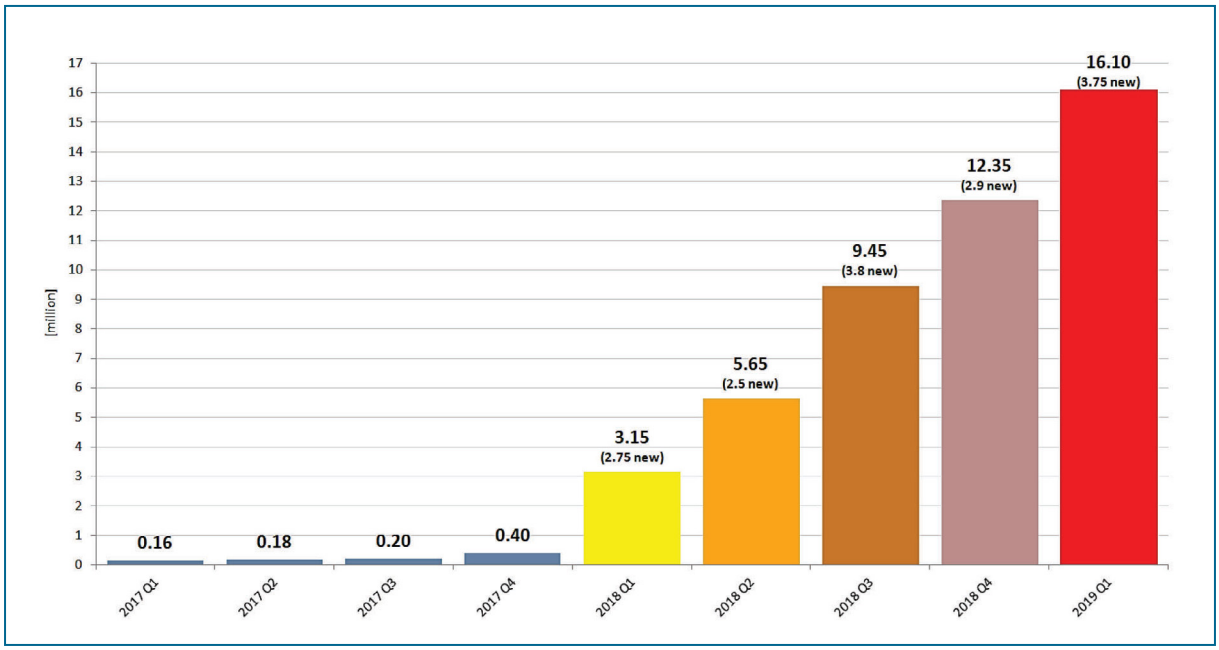


Figure 5.4. Harmful malware used for cryptojacking including new threats/scripts in the period from the first quarter of 2017 to the first quarter of 2019

Source: own calculations using MS Excel based on McAfee Labs Threats Report.

hardware owners or mobile devices. In other words, new threats related to the illegal use of other users' equipment for mining cryptocurrencies increased over hundred times (precisely by 10,062.50%, increase from 0.16 million to 16.10 million).

In 2018, cryptojacking dethroned ransomware (data encryption and ransom demand) as the most popular form of cyberattack. Based on the above analysis, it can be concluded that the huge "popularity" of such solutions in illegal cryptocurrency mining resulted primarily from two factors. First, cybercriminals made profits without incurring any costs associated with the purchase of cryptocurrency mining equipment and charges for electricity consumed. Secondly, the so-called scale effect: taking over the computing power of one or several computers was not important for cryptojacking, but when these numbers went into tens or hundreds of thousands or even millions of Internet users, the profits must have been fabulous, without any own contribution. In other words, cybercriminals mined for free, without taking any risk there. Their calculation was simple: income = profit (because there were no costs associated with mining cryptocurrencies). It can be assumed that if there will be no changes in technology and security in the near future, this dangerous trend will have great progress. At this point, one can put forward the thesis that the existence of cryptojacking is related to the used Proof of Work consensus algorithm, which requires miners to offer some specific amount of work on behalf of the entire network, e.g., Bitcoin. The mining devices used are very energy-consuming. Therefore, the costs of energy consumed may often exceed the revenues from the mining. Until there is a change in the Bitcoin mining

algorithm and other mineable cryptocurrencies to more energy-saving ones such as Proof of Stake and putting them into circulation, the problem of cryptojacking and "free" mining at the expense of other Internet users will remain.

According to estimates contained in the McAfee Labs Threats report, in the first quarter of 2018 there was a rapid, gigantic increase in new malicious scripts mining cryptocurrencies compared to the last quarter of the previous year. This number increased from around 400,000 to 2.9 million (increase by 2.5 million), which means more than 6-fold increase (625%)[4]. It is worth noting that comparing the fourth quarter of 2017 to the third quarter of the same year, the increase in cryptominers was estimated as only 50%. In turn, in the second quarter of 2018, compared to the first quarter, there was a further huge increase in the number of scripts like CoinHive, again by 2.5 million new threats regarding cryptojacking. This meant an increase of 86.21%. In cumulative terms, taking as a basis the fourth quarter of 2017, as many as 5 million completely new and harmful scripts mining cryptocurrencies without the knowledge and consent of users arrived.

Great progression in the growth of new malware dedicated exclusively to illegal cryptocurrency mining, used as part of cryptojacking, is well illustrated by the data for two periods. During one year (from the third quarter of 2017 to the third quarter of 2018) there was over 47-fold increase (4,725%) of the total number of cryptocurrency mining scripts at the expense of unaware Internet users. In the two-year period (first quarter 2017 – first quarter 2019) this increase was gigantic, since it has been estimated to be 10,063%. These numbers can be frightening, but they can also indicate that cryptojacking has become the most "popular" way among cyber criminals for illegal income obtained virtually cost-free. These statistics can also confirm the thesis that ransomware and theft of login data for electronic banking have been overtaken by cryptojacking. The fragment from the original report cited below leaves no doubt that malicious scripts like CoinHive have become "favourite" form of cryptojacking by cybercriminals.

Coin miner malware grew a stunning 629% to more than 2.9 million known samples in Q1 [2018] from almost 400,000 [395 000] samples in Q4 [2017]. This suggests that cybercriminals are warming to the prospect of monetizing infections of user systems without prompting victims to make payments, as is the case with popular ransomware schemes. Compared with well-established cybercrime activities such as data theft and ransomware, cryptojacking is simpler, more straightforward, and less risky. All criminals must do is infect millions of systems and start monetizing the attack by mining for cryptocurrencies on victims' systems. There are no middlemen, there are no fraud schemes, and there are no victims who need to be prompted to pay and who, potentially, may back up their systems in advance and refuse to pay (McAfee, 2018).

It should be recalled that malicious scripts for mining initially appeared on pages with a very dubious reputation offering illegal content (e.g., the most famous page with torrents,

[4] Another producer of antivirus software and cyber security, TrendMicro, published a report in which it informs that according to the analyses, there was a 956% increase in the number of cryptojacking attacks. The study concerned a period of one year, from the first half of 2017 to the first half of 2018 (Trend Micro, 2018, 2019).

i.e., The Pirate Bay). Over time, they were secretly placed on websites of online stores, blogs of famous people and celebrities, and even on the websites of state offices and agencies. It was possible, among others, because the content management software for such pages has not been regularly updated. It is thanks to the gaps in the CMS (Content Management System), that cybercriminals obtained easy and often full access to the source code of the page, on which they placed harmful scripts or hid them into official advertisements presented on these websites. Some hackers even went so far as to create false software updates with implemented malicious code to take control of the computer and its computing power.

Cloud services offered by the global giant Amazon have also been used by cybercriminals to practice cryptomining. Miners-hackers broke into the AWS (Amazon Web Services) of several companies and took advantage of the fact that the administrative console was not protected by any password or the default password was not changed, e.g., "admin". As a result, they obtained the highest level of permissions (this resulted from the reckless approach of the system administrators themselves), which in turn allowed them to take over the gigantic computing power of the Amazon cloud and the offered resources of virtual machines for mining cryptocurrencies, such as Bitcoin, Litecoin or Ethereum (Peterson, 2017).

One of the most famous companies in the world that used Amazon's cloud services and fell victim to cryptojacking was Tesla, founded by Elon Musk, a leading manufacturer of electric and autonomous cars. The hacker attack also led to the disclosure of some proprietary data, including maps, telemetry and vehicle servicing (Browne, 2018). At this point, one should agree with a statement by Kumara, the technical director of RedLock which specializes in monitoring the security and threats of providers of the largest cloud services, such as Microsoft Azure, Google Cloud Platform and Amazon Web Services. "Given the immaturity of cloud security programs today, we anticipate this type of cybercrime [cryptojacking] to increase in scale and velocity" (Liberto, 2019).

In 2018, cybercriminals even used audio description software on official government sites of countries such as Canada, the US and the United Kingdom to bypass security and implement a malicious script that digs cryptocurrencies, called CoinHive. All persons who visited the government websites of these countries were unknowingly used to mine cryptocurrency on their computer equipment. The situation becomes very dangerous when such an attack and the acquisition of computing power of computer systems concerns the management of critical infrastructure of the city, region or even country. An example is the hacking of the European water supply control system (European Water Utility) for cryptomining. This was the first example of cybercriminals' action against the industrial control system, causing perturbations in network management (Largue, 2018). It is worth mentioning that the system worked under the control of Windows XP, whose extended support ended on April 8, 2014. Such an important industrial control system was based on an outdated operating system with many gaps, which is not a very professional approach on the part of administrators.

Virtually anyone can become a victim of cryptojacking. In July 2018, it turned out that on the Steam platform, which is ranked as the largest digital distribution of computer games,

a game with hidden malicious code was available. We are talking here about the game "Abstractism" which without the knowledge and consent of people playing it secretly mined cryptocurrencies. That PC game has been prepared and issued only to unauthorized use of the computing power of computers users (processors and graphics cards). The game has been designed in such a way as to encourage users to use it as long as possible. The more time the player spent on this game, the more virtual items he received (like weapons, points or experience) for use in other games. In other words, the longer the player was connected to the Internet and logged into the game, the rarer and more valuable items he could receive. For example, the first of them was available to him after 15 minutes, the second one after 30 minutes, and the third only after an hour of continuous gameplay (Gurwin, 2018). It was rightly assumed that it could be a camouflaged cryptocurrency mining rig. The excuse of the producer, Okalo Union, was quite naive. The company claimed that the high consumption of the processor and graphics card is the result of starting the game at the highest graphic settings. These were ridiculous arguments, because the game was very simple and only two--dimensional, and in addition in the black-white version. Therefore, it could not absorb such computer resources in any way. Suspicions have been confirmed; the game mined the cryptocurrency in the background, previously installing the so-called Trojan horse, which transformed player's computer into an efficient cryptomining machine. The owner of the Steam platform, Valve, has removed "Abstractism" from its gaming catalogue. This is an example that even on such a well-known and valued service as Steam, you could fall victim to cryptojacking (Radulovic, 2018; Tomczyk, 2018a).

Experts on cybersecurity have shown that it is possible to illegally mine cryptocurrencies through the hidden use of JavaScript even in an Excel spreadsheet. Of course, with no permission to perform the relevant calculations and without obtaining the consent of the user who started such a fabricated file (Tomczyk, 2018b). In this way, virtually anyone can fall victim to cryptojacking, because the Office programs package is very popular, and a large number of users download data from various sources in CSV or XLS/XLSX format.

5.5. Effects of Cryptojacking

The effect of hidden cryptojacking resulting from taking over computing power is – from the exploitation and technical side – deterioration of computer's operation. Among others this includes increased processor load, increasing fan switching frequency and multiplied operation at higher speeds than usual, repeated system suspension, heating the case of the entire device and its loud operation, which does not occur under normal conditions of use. A device that has been infected with malware for cryptojacking can also switch off without reason, automatically restart repeatedly, or often display so-called Blue Screen of Death (BSoD). This is a symptom of a serious error of the system or running application, due to the consumption of excessive computing power and preventing other system operations. The

increasing number of episodes with the emerging BSoD is caused by excessive overloading of computer resources, which may result from its inclusion in the mining process, when cryptominer is active in the background.

In the case of infected smartphones and tablets, malware used for cryptojacking occurs with strong overheating of batteries in these devices during their network operation. As a result of miners/hackers cryptojacking – the equipment's life is significantly reduced. This entails financial consequences for users who are forced to purchase new devices much earlier than would appear from their normal life cycle.

In other words, the destructive effect of cryptojacking on the user's computer on which cryptocurrency malware has been insidiously installed, will manifest itself in the best case with a decrease in its performance and interference in smooth operation and technical perturbations, and in the worst one – total and irreversible damage/destruction of the device.

Seemingly, this criminal practice (cryptojacking) may seem harmless to the user or the attacked institution. Taking over the computing power of a computer, server or mobile device using a malicious script, however, has many negative effects. On the one hand, cryptojacking reduces the performance of the equipment in use, and on the other – generates higher expenses for its owner. It is about spending on electricity consumed and maintenance services, or the purchase of new computer components that have been worn out prematurely as a result of cryptomining.

5.6. Cryptojacking as a Criminal Act

Among all cybercrimes cryptojacking (also known as cryptomining) has been gaining importance since 2017, and its intensity is strongly correlated with fluctuations in cryptocurrency rates expressed in fiat money, and connected with the creation and bursting of price bubbles. It was at the end of 2017 that one of the largest speculative bubbles on the Bitcoin market was growing rapidly, counting from his debut on the web in 2009, and thus mass of miners grew, including miners-hackers using cryptojacking to mine new BTC units. The effect of cryptojacking is the perfidious and hidden theft of some computing resources of network users, leading to slowing down the operation of the devices they use and contributing to a significant reduction in their actual service life, which, as a consequence, is reflected in higher electricity bills and undesirable shortening of the equipment replacement period due to excessive exploitation and increasing failure due to continuous overload and overheating of computer components.

Cryptojacking still does not pose a high risk to the hacker performing such an attack, while it is relatively easy to implement on the victim's computer, and at the same time not easy to identify by a user robbed of part of the computing capacity of his central unit. It should be emphasized that detecting the operation of a cryptominer is not easy for the average owner of a computer connected to the Internet, because malware has the possibility of so-called mimicry, consisting in similarity to other installed programs. A kind of chameleon

effect works here. In addition, the tracking and detection of the perpetrator by the relevant services and law enforcement bodies is relatively difficult.

It is worth noting that in Poland cryptojacking exhausts the features of computer fraud, so it is a criminal act, in accordance with the wording of art. 287 § 1 of the Polish Criminal Code.

Who, in order to achieve a financial gain or cause damage to another person, without authorization, influences the automatic processing, collection or transfer of IT data or changes, removes or introduces a new record of IT data, is punishable by imprisonment from 3 to 5 months (Ustawa z dnia 6 czerwca 1997, Art. 287 § 1).

Unfortunately, in practice the detectability of this type of crime is extremely low, and the criminalization of such a criminal act is so far unique. By January 2021, courts in Poland had only imposed a prison sentence against one cryptojacker. It can be assumed, without a high probability of making a mistake, that there were quite numerous cases of cryptojacking in our country's territory, because constant and massive attempts to steal computing power from foreign computers are a common phenomenon on the network. It is estimated, however, that most such attacks affect individual computer users in countries such as India, Japan, Taiwan, the United States of America and Australia.

The law attorneys Friedman Nemecek & Long L.L.C.[5] from Cleveland, the state of Ohio, present the following interpretation of cryptojacking with an indication that this is a federal crime in the US: "Cryptojacking involves using part of someone's computing power without their knowledge or consent to gain monetary benefits. Under federal law, this act is a fraud and suspects in cryptojacking may be brought to justice" (Friedman & Nemecek, 2022). According to the information of this lawyer's office referring to the prosecutor, at the end of 2021 two people were accused of financial fraud related to cryptojacking. The US Attorney's Office for the Eastern District of Missouri in the collected evidence showed that two accused Iranian citizens were acting to the detriment of the interests of a technology company from the city of Saint Charles, Missouri. They were accused of deliberately misleading the cloud service provider to launch five additional servers working for and at the expense of the entity. Two cybercriminals, by obtaining unauthorized access to the official account of this company, which is used to manage access to the Microsoft Azure cloud, placed an order on its behalf to extend the existing cloud service capabilities. According to prosecutors, "Jeloudar and Safaei 'fraudulently' gained access to a cloud services account used by a tech company in St Charles, Missouri" (*Two Iranian*…, 2021). The contracted increased cloud computing power was to be used to mine Monero cryptocurrency for cyber criminals. The crime was only revealed when the cloud service provider issued an invoice for a dizzying USD 760,000.

By misrepresenting themselves through the victim company's account, the defendants fraudulently authorized the cloud service provider to build and install at least five new

[5] "A Limited Liability Company [LLC] is a hybrid between corporation and partnership structures in the United States whereby business owners are given liability protection and pass-through taxation. This means that owners of an LLC are not personally liable for the company's debts and obtain certain tax advantages. Furthermore, owners of an LLC are called 'members' rather than partners or shareholders" (*Limited Liability*…, n.d.).

computer servers in the cloud. The purpose of the new servers was to run and operate software programs to generate cryptocurrency (Kovacs, 2021).

It is worth mentioning that in the US financial fraudsters are punishable by up to 20 years imprisonment and/or a fine.

It should also be mentioned that the European Union Agency for Cybersecurity (ENISA) is of the opinion that cryptojacking is an illegal activity, but such attacks are not of great interest to law enforcement authorities, and their cases are rarely reported by injured users, mainly due to the relatively small negative direct consequences (European Union Agency for Cybersecurity [ENISA], 2020a). The ENISA report confirmed that in 2019 the most commonly used malware by cybercriminals was cryptojacking (over 64 million cases in 2019) (ENISA, 2020b). Infection of the internal network of companies and organizations of this type with malware causes financial losses of these entities or increases the costs of operating IT systems (increased electricity consumption and IT costs, as well as a decrease in the efficiency of the attacked equipment, and thus a reduction in employee productivity).

In summary, cryptojacking is an illegal method of mining cryptocurrencies. This crime is not about directly stealing other people's virtual funds. In practice, the Internet user who is the target of the attack does not need to have cryptocurrencies at all for crypto-jacking to occur. A cryptojacking attack describes the unauthorized use of a person's computing power to mine virtual currencies. This is done by insidiously infecting a computer or other devices connected to the Internet with malware.

5.7. Possibilities of defence against cryptojacking

It is worth emphasizing that Internet users are not completely defenceless against cryptojacking. To protect from it relatively easily. Some basic rules must be observed. First, under no circumstances open suspicious links to unknown pages (i.e., redirecting) and open files (especially with the EXE, ZIP or RAR extension) sent *via* e-mail or downloaded from unknown and uncertain sources. A good habit is to regularly and systematically update your operating system and software to "fix" security vulnerabilities. In addition, it is recommended to install a web reputation rating plugin in your browser that suggests which pages are secure and which may contain malicious scripts (Pieleszek, 2019, pp. 49–56). One should not forget about having commercial antivirus software. Free antivirus programs are not effective enough to detect and block malicious code that is a cryptojacking medium. Cybersecurity specialists also suggest adding an extension to your browser that blocks ads (AdBlock) and Java scripts on websites and thus prevents the launch of illegal cryptomining (e.g., No Coin, NoMiner or minerBlock).

It should also be pointed out that human aspect is always the weakest security link and this is also confirmed in the case of cryptojacking. It is the user who usually performs the action, e.g., opening an attachment or clicking on a link or advertisement that runs the

mining script. Therefore, the system should be regularly scanned for the presence of cryptocurrency mining code and backed up data.

Protection against cryptojacking is really possible, but you need user involvement. There are plugins (addons) for web browsers like Firefox or Chrome, that are blocking the display of ads on the page (with hidden cryptominers) and the execution of Java scripts (like Ad Blocker Plus). However, such an add-on had to be installed on the user's own initiative, and configured accordingly. Many of them either disregarded the problem or did not have adequate knowledge of this threat and could not be properly secured. The first browser that had a built-in and integrated mechanism for detecting and blocking cryptocurrency mining scripts on websites was Opera. It was enough to select only the "No Coin" function in the settings. It should be added that later there was an automatic regular update of the cryptojacking script list.

It is worth emphasizing once again that in the face of cryptojacking attacks, users are not completely helpless and powerless. They should use common sense, not perform unthinkingly certain operations and activities. In a word, you must follow the elementary rules of using the Internet. In the case of malware hidden in files, do not open attachments sent *via* e-mail from unverified senders, in particular executable files with EXE extension and packed files with ZIP or RAR extensions. When browsing the Internet resources, you should examine the reputation of the pages you visit using special plugins that are added to your web browser. Downloading illegal content from unknown sources, including pirate software, may expose you to infecting your operating system with a malicious code. In addition, do not mindlessly click on the links redirecting to a given website, in particular in the so-called shortened links. The last element of defence against cryptominers is installing a dedicated plug-in blocking ads and Java scripts. This plugin should be added to every web browser used. Unfortunately, this involves incorrect display of some websites and forms. In other words, the comfort of browsing websites is reduced, but this is at the expense of security.

Confirmation of the importance of security is the systematic and regular update of the operating system and installed programs is the Trend Micro report published on June 10, 2019. The security bulletin highlights the new threat of insidious installation of illegal cryptocurrency mining software. Cybercriminals are increasingly using vulnerabilities in operating systems, programs and services to gain unauthorized access to a computer or server to implement malicious code. It should be emphasized that each software provider periodically issues patches that remove detected vulnerabilities. Unfortunately, not all users decide to update their software, especially the Windows operating system, which may seem logical and rational. It has often happened that the official update issued by Microsoft worsened the functioning of the system instead of increasing its performance and functionality. Paradoxically, the official patch to remove vulnerabilities in Oracle WebLogic has made it easier for hackers to penetrate systems and install cryptojacking software. They used security certificates, behind which scripts that illegally mine cryptocurrencies were

hidden. In this way, they outsmarted antivirus and malware detection programs because they do not scan certificates for encrypted connections (https).

The idea of using certificate files to hide malware is not a new one [...]. By using certificate files for obfuscation purposes, a piece of malware can possibly evade detection since the downloaded file is in a certificate file format which is seen as normal – especially when establishing HTTPS connections (Vicente, Triunfante & Gelera, 2019).

In addition, other issue of broadly understood security should not be underestimated. Cryptojacking can contribute to increased infiltration of operating systems, ranging from home computers (PCs) to servers of large corporations and government agencies. This is a very dangerous trend that will promote the intensification of data leaking, including business data, as well as sensitive data and strategic data important for the functioning of countries.

5.8. Conclusions

With the development of cryptocurrency mining carried out in the online environment, and significantly driven by the mechanism of creating speculative bubbles on the market of these virtual assets in combination with the highly rooted FOMO syndrome (Fear of Missing Out) among investors eager for quick and huge profits, a completely new form of cybercrime has appeared on the web. On the IT level, it consists in planned, intentional and insidious infection by miners/hackers with a malicious code of devices equipped with processors and connected to the network, and then on taking over their computing power for their own purposes – so mining cryptocurrencies for free. Such criminal activity is referred to as cryptojacking, also called malicious mining (malicious cryptomining) (Behan, 2022, pp. 649–656). This is a relatively new type of computer attacks launched by cybercriminals on the equipment of ordinary users, including not only personal computers, but also servers, smartphones and tablets.

Miners/hackers can for a long time operate other people's devices connected to the Internet in order to achieve their own financial benefits, without the knowledge and consent of users. Cryptojacking can affect both individuals, companies or public institutions, and be used for unconscious work of entire groups of computers or related devices cooperating via the network. Infected computers and servers lose their performance by slowing down the work of a company or organization or institution. Systems and programs may not work as smoothly as the user needs, and which is directly due to the technical specification of the equipment and its configuration. In addition, as a result of infection, devices consume much more energy, which due to a large number of them can be a serious financial problem for the entity conducting business activity.

It should be emphasized once again that cryptojacking is a type of cybercrime, where the miner/hacker secretly uses the victim's computing power to generate cryptocurrencies. This usually happens when the victim unknowingly installs a program containing malicious scripts that allow the cybercriminal to access the computer or other device connected to the

Internet. Cryptojacking may seem like a harmless crime, because the only thing "stolen" is just some fraction of the power from the data processing potential of the attacked user's computer. However, the use of someone else's computing capacity for this criminal purpose takes place without the victim's knowledge or consent, only for the benefit of a cybercriminal who illegally mines cryptocurrencies and earns money on it. In these circumstances, revenue means pure income for the miner/hacker, as he does not bear the costs associated with the creation of mineable cryptocurrencies (purchase of equipment and operating costs, including electricity costs). Considering the large number of infected devices and the possibility of obtaining a total gigantic computing power, creating conditions for generating cost-free huge amounts of virtual currencies based on the so-called Proof of Work consensus algorithm, miners/hackers see cryptojacking as a lucrative crime that is easy to commit, while being difficult to detect.

It is also worth answering the question contained in the title of the article. Cryptojacking can in a sense be seen and considered as a manifestation of the crisis behaviour of individual miners, which is particularly intensified during periods of the rise of speculative bubbles on the market of specific virtual currencies. This may be due to two economic reasons. Mining grown by individual miners is generally unprofitable, because their mining capacity as represented by their equipment is relatively small and in no way can compete with the so-called mines, which bring together large groups of users, creating gigantic computing power. In relation to the total computing power of typical mining farms, mining rigs of individual miners are only a part per thousand of their efficiency. Hence the resort of individual miners to not always legal attempts to make a profit, even at the expense of other Internet users. The second reason why an individual miner decides to use cryptojacking is that the variable costs of such an undertaking as cryptocurrency mining are very high and often prevent profitability. In addition, the complementary factor in cryptojacking are fixed costs – cybercriminal is not forced to buy their own equipment and operate it.

References

Behan, A. (2022). *Waluty wirtualne jako przedmiot przestępstwa*. Kraków: Krakowski Instytut Prawa Karnego Fundacja.

Browne, R. (2018). *Hackers Hijack Tesla's Cloud System to Mine Cryptocurrency*. Retrieved from https://www.cnbc.com/2018/02/21/hackers-hijack-teslas-cloud-system-to-mine-cryptocurrency-redlock.html

Co to jest phishing i jak się przed nim bronić? (2023). Retrieved from https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/

Cybersecurity and Infrastructure Security Agency [CISA]. (2021). *Defending Against Illicit Cryptocurrency Mining Activity*. Retrived from https://www.cisa.gov/news-events/news/defending-against-illicit-cryptocurrency-mining-activity

European Union Agency for Cybersecurity [ENISA]. (2020a). *Cryptojacking. Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa*. Retrieved from https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-cryptojacking-ebook-en-pl.pdf

European Union Agency for Cybersecurity [ENISA]. (2020b). *Threat Landscape 2020 – Cryptojacking*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cryptojacking/at_download/fullReport

Friedman & Nemecek, L.L.C. (2022). *What is Cryptojacking?* Retrieved from https://www.iannfriedman.com/blog/2022/may/what-is-cryptojacking-/

Gaździcki, M. (2021). *Co to jest cryptojacking i jak Intel oraz Microsoft chcą z nim walczyć*? Retrieved from https://geex.x-kom.pl/wiadomosci/co-to-jest-cryptojacking-i-jak-intel-oraz-microsoft-chca-z-nim-walczyc/

Gurwin, G. (2018). *Valve Bans Steam Game That Was Installing Cryptocurrency Mining Malware*. Retrieved from https://www.digitaltrends.com/gaming/steam-game-allegedly-mining-cryptocurrency/

Kovacs, E. (2021). *Iranians Charged for Cryptojacking after U.S. Firm Gets $760,000 Cloud Bill*. Retrieved from https://www.securityweek.com/iranians-charged-cryptojacking-after-us-firm-gets-760000-cloud-bill/

Largue, P. (2018). *European Water Utility Attacked by Cryptocurrency Mining Malware*. https://www.smart-energy.com/regional-news/europe-uk/cryptocurrency-malware-eu-utility/

Liberto, D. (2019). *Tesla's Cloud Was Hacked for Mining Cryptocurrency*. Retrieved from https://www.investopedia.com/news/teslas-cloud-was-hacked-mining-cryptocurrency/

Limited Liability Company. (n.d.). WIX Encyclopedia. Retrieved April 20, 2023 from https://www.wix.com/encyclopedia/definition/limited-liability-company-llc

Lueth, K. (2021). *State of the IoT 2020: 12 Billion IoT Connections, Surpassing Non-IoT for the First Time*. Retrieved from https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

McAfee. (2018). *McAfee Labs Threats Report June 2018*. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf

Meshkov, A. (2022). *Cryptojacking Surges in Popularity Growing by 31% over the Past Month*. Retrieved from https://adguard.com/en/blog/november_mining_stats.html

Mursch. T. (2019). *How to Find Cryptojacking Malware*. https://badpackets.net/how-to-find-cryptojacking-malware/

O'Donnell, L. (2018). *Cryptojacking Attack Found on Los Angeles Times Website*. Retrieved from https://threatpost.com/cryptojacking-attack-found-on-los-angeles-times-website/130041/

Peterson, B. (2017). *Zapomnij o kradzieży danych. Hakerzy włamali się do usług Amazona, by kopać bitcoiny*. Retrieved from https://businessinsider.com.pl/finanse/kryptowaluty/hakerzy-wlamali-sie-do-amazona-zeby-kopac-bitcoiny/7btxh3f

Pieleszek, M. (2019). *Bądź bezpieczny w cyfrowym świecie. Poradnik bezpieczeństwa IT dla każdego*. Gliwice: Helion, OnePress.

Radulovic, P. (2018). *Steam Game Pulled from Store after Allegations of Cryptocurrency Mining*. Retrieved from https://www.polygon.com/2018/7/30/17630664/steam-abstractism-cryptocurrency-mining

Symantec. (2019). *Internet Security Threat Report*. Volume 24, February 2019. Retrieved from https://docs.broadcom.com/doc/istr-24-2019-en

Tomczyk, J. (2018a). *Gra Abstractism kopała na Steamie w tle kryptowaluty*. Retrieved from https://www.chip.pl/2018/08/gra-abstractism-kopala-na-steamie-w-tle-kryptowaluty/

Tomczyk, J. (2018b). *Hakerzy wykorzystali nowe funkcje Excela do kopania kryptowalut*. Retrieved from https://www.chip.pl/2018/05/hakerzy-wykorzystali-nowe-funkcje-excela-do-kopania-kryptowalut/

Trend Micro. (2018). *Raport Trend Micro: Cyberprzestępcy odchodzą od spektakularnych ataków na rzecz kradzieży pieniędzy i zasobów obliczeniowych*. Retrieved from https://www.trendmicro.com/pl_pl/about/newsroom/press-releases/2018/20180830-cyberprzestepcy-odchodza-od-spektakularnych-atakow-na-rzecz-kradziezy-pieniedzy-i-zasobow-obliczeniowych.html

Trend Micro. (2019). *Trend Micro Security's 2019 Release Protects You Better Than Ever Against Ransomware, Coin-mining, Banking, and E-commerce Threats*. Retrieved from https://blog.trendmicro.com/trend-micro-securitys-2019-release-protects-you-better-than-ever-against-ransomware-coin-mining-banking-and-e-commerce-threats/

Two Iranian Nationals Indicted in Local Cryptojacking Case. (2021). Retrieved from https://www.justice.gov/usao-edmo/pr/two-iranian-nationals-indicted-local-cryptojacking-case

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553)

Vicente, M., Triunfante, J., & Gelera, B. (2019). *CVE–2019–2725 Exploited and Certificate Files Used for Obfuscation to Deliver Monero Miner*. Retrieved from https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-2725-exploited-and-certificate-files-used-for-obfuscation-to-deliver-monero-miner/

What Is Phishing? (2022). Retrieved from https://www.binance.vision/en/security/what-is-phishing