International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 3 ǁ March 2023 ǁ PP. 478-484

Cryptojacking Detection With Process Analysis

Dr.Y.Venkataramana Reddy[1], S.Bhaskar[2], G.Vinila[3],B.Abhilash[4]
[1]*Associate Professor, Anurag University-Hyderabad*
[2][3][4]*UG Scholar, Anurag University-Hyderabad*
[1]*yvreddyit@cvsr.ac.in,* [2]*sombhaskarmudhiraj@gmail.com,* [3]*vinigudipati@gmail.com*
[4]*abhi.bollagani25@gmail.com*

Abstract— *Cryptojacking is a type of cyberattack that entails the unlawful mining of cryptocurrencies on another person's computer. It is a rising threat that has the potential to seriously harm the victim's machine. We provide a desktop-based cryptojacking detection programme to solve this problem, which identifies and reduces the danger by combining static and dynamic analysis methods. The programme is set up as a desktop programme that continuously scans the system's resources for any odd activities. Our programme is quite effective at identifying and thwarting cryptojacking assaults, according to the findings of our evaluation of its performance using a dataset of known cryptojacking malware variants and actual attacks.*

Keywords: *CPU monitoring, Cryptojacking, Crypto Mining, Mining pool, Crypto Currency.*

Date of Submission: 11-03-2023 Date of acceptance: 25-03-2023

I. INTRODUCTION

Malicious crypto mining, commonly referred to as cryptojacking, is a sort of cyberattack in which an attacker mines cryptocurrencies on the computer of a victim without that victim's knowledge. Typically, the attacker infects the victim's computer with malware to enable them to use the computing power for cryptocurrency mining. Attacks including cryptojacking can seriously harm the victim's computer, resulting in sluggish performance, overheating, and even hardware damage. Cryptojacking assaults are becoming more and more common, thus it is crucial to identify and mitigate them.

The concept and implementation of a desktop PC cryptojacking detection tool are presented in this research study. Our programme is made to keep an eye out for any strange patterns in the system's CPU and memory consumption that might point to a cryptojacking attempt. To find malicious processes connected to cryptojacking, the programme combines static and dynamic analysis methodologies. The risk of cryptocurrency jacking has increased with the growing use of cryptocurrencies. Crypto jacking is the term for the illicit mining of cryptocurrencies using a computer's resources without the user's knowledge or agreement. Poor system performance, hardware damage, and even data theft are all effects of crypto jacking. Users can defend their systems against this threat by using anti-virus software.

II. LITERATURE REVIEW

Cryptojacking is becoming more and more of a problem for both people and companies. Because of this, the creation of detection technologies meant to spot and stop such assaults has increased. This study of the literature intends to investigate current research on desktop cryptojacking detection systems that do not rely on machine learning.

In one study, Malini et al. (2020) suggested a method based on behavioural analysis for identifying cryptojacking attempts. In order to find irregularities that would point to a cryptojacking assault, the technique examined numerous system performance data, including CPU consumption, memory usage, and network traffic. With few false-positive rates, the authors found encouraging findings in detecting cryptojacking assaults.

A detection tool that combines static and dynamic analysis was suggested in a different study by Alshahrani et al. (2020) to help identify cryptojacking assaults. In the static analysis, known cryptojacking signatures were checked in the source code, and in the dynamic analysis, the system's behavior was watched for indications of cryptojacking activity. High detection rates and low false-positive rates were reported by the authors.

In a paper published in 2021, Li et al. suggested a detection tool that combined behavior-based and signature-based analysis into a hybrid approach. To detect cryptojacking activities, the tool examined system performance parameters like CPU and memory utilization as well as network traffic. High detection rates and low false-positive rates were reported by the authors.

Rakesh Kumar and colleagues' "Detection of Cryptojacking Malware Using CPU Usage Based Method" (2021) - In this research, a CPU utilization-based method for identifying cryptojacking malware is proposed. The method analyses CPU use trends and looks for anomalies that can point to the presence of malware that steals cryptographic keys.

Giacomo Marciani and colleagues' "CPU-Based Detection of Bitcoin Mining Malware" (2021) - This study suggests a method for spotting cryptocurrency mining malware by keeping an eye on CPU use. The technology analyses CPU utilization patterns and looks for irregularities that can point to the presence of mining malware using machine learning algorithms.

By Ali Al-Waely et al., "Detecting Cryptojacking Attempts on Internet of Things Devices Using CPU Performance" (2021) - This study suggests a technique for monitoring CPU performance to identify cryptojacking attacks on Internet of Things (IoT) devices. In order to assess CPU performance trends and find anomalies that can point to the presence of cryptojacking malware, the approach employs machine learning methods.

Nishanth Kumar and colleagues' "A Study on Cryptojacking Detection Methods" (2021) - This study offers a thorough analysis of the methods currently used to identify cryptojacking malware. The survey uses CPU performance and utilization methodologies in addition to other methods like network traffic monitoring and behavioral analysis.

Haein Park and colleagues' "Cryptojacking Detection in Large-Scale Networks Using CPU Usage" (2020) - This study suggests a technique for monitoring CPU consumption to identify cryptojacking malware in massive networks. The technique analyses CPU consumption trends and looks for anomalies that can point to cryptojacking malware using machine learning methods.

Last but not least, Chen et alstudy .'s from 2021 included a detection tool that employed a heuristic method to spot cryptojacking behavior. To find unusual activity, the tool examined a number of system performance characteristics, such as CPU and memory consumption. With few false-positive rates, the authors observed encouraging findings in identifying cryptojacking attacks.

Overall, the research indicates that desktop cryptojacking detection systems can be created successfully without the use of machine learning. To detect cryptojacking activities, these technologies often include behavioral analysis, static and dynamic analysis, and heuristic algorithms. The findings of these studies are encouraging and lay the groundwork for future research in this field, but more study is required to assess the efficiency of these tools in real-world circumstances.

III. METHODOLOGY

The purpose of our detection programme is to keep an eye out for any odd CPU or memory consumption patterns that could be a hint of a crypto jacking attempt.

We create a desktop programme that users can install to use the detecting tool. The utility periodically checks the system for unusual activity while running in the background. When cryptocurrency mining malware is found, the programme alerts the user and requests that they take the necessary steps.

Design

Our cryptojacking detection programme is made to keep an eye out for any strange patterns in a computer's CPU and memory utilization that can point to a cryptojacking attempt. To find malicious processes, the tool combines static and dynamic analysis methods. The tool analyses the file's attributes and metadata, including its size, creation date, and digital signature, during the static analysis stage to assess whether it is harmful. The programme watches the system's process tree during the dynamic analysis stage to look for any processes connected to cryptojacking.

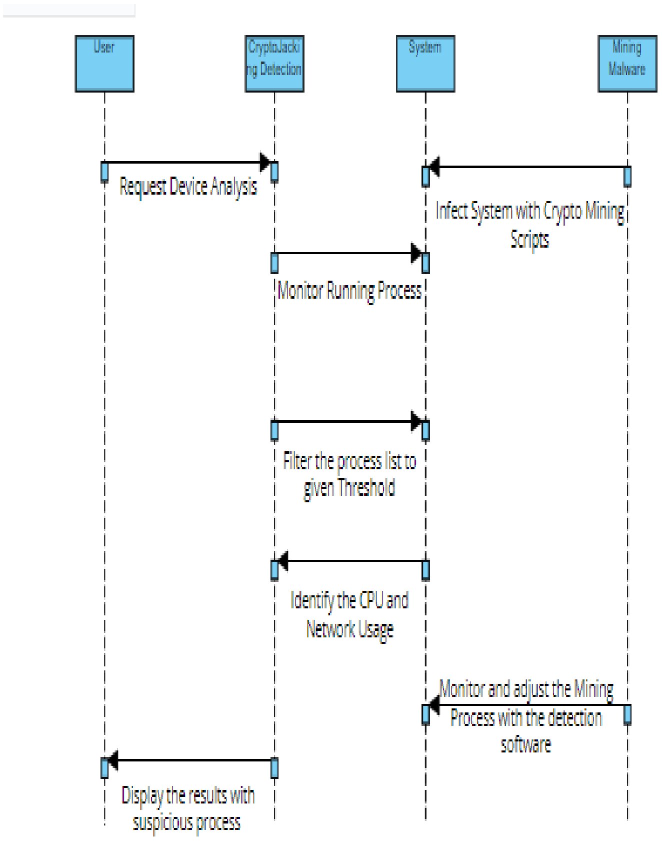
Static Analysis:

The tool analyses the file's attributes and metadata, including its size, creation date, and digital signature, during the static analysis stage to assess whether it is harmful. The utility also conducts a hash comparison to find any known harmful files and tries to see if the file is included in any databases of known malware.

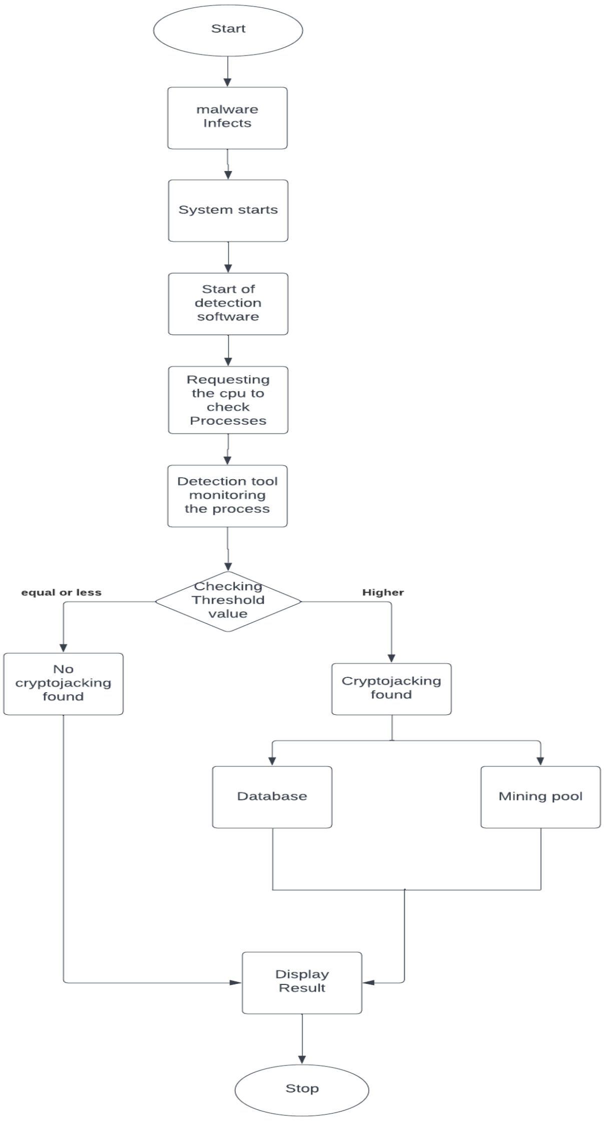
Dynamic Analysis:

The programme watches the system's process tree during the dynamic analysis stage to look for any processes connected to cryptojacking. The programme detects processes that consume a lot of CPU and memory, and it continuously checks the system for any modifications to the patterns of resource usage. The utility also checks to see whether the suspicious process creates any odd network connections.

Working process


User
CryptoJacki ng Detection
System
Mining Malware
Request Device Analysis
Infect System with Crypto Mining Scripts
Monitor Running Process
Filter the process list to given Threshold
Identify the CPU and Network Usage
Monitor and adjust the Mining Process with the detection software
Display the results with suspicious process

When the cryptojacking detection application is running, the CPU will examine all open programs and their consumption of memory and processor. When the application's value threshold exceeds the specified normal value, cryptojacking is considered to have occurred. So, we can identify desktop cryptojacking by using the CPU and threshold value.



IV. Background

There are many methods that browser-based attacks, malicious software downloads, and phishing scams can infect a computer with cryptojacking malware. Once the victim's computer has been infected, the virus can operate in the background and use system resources for cryptocurrency mining without the user's knowledge. Finding and preventing cryptojacking attacks has become crucial due to their increasing frequency..

A.Cryptocurrencies

When cryptocurrencies first emerged, they were designed to do away with the necessity for third-party organizations in online money transfers and payments. The methods now in use do not work well for the online environment of today, as explained by Nakamoto. While Nakamoto's Bitcoin provided a solution, it also paved the stage for the emergence of numerous other ideas. As a result, hundreds of marginally distinct new cryptocurrencies have started to emerge, each focusing on a particular issue, such as speedier transactions, improved anonymity, or reliability. This thriving ecosystem has also stimulated a great deal of study into other cryptocurrency-related areas, including various networks, assaults, consensus methods, and many others.

B.CPU Monitoring

CPU surveillance is nothing new. The operating system, the hardware firmware, or specially created APIs can all offer the user a variety of CPU metrics. More sensors beyond those in the CPU may occasionally be provided by the motherboard itself. These sensors give the user access to additional information and, in certain cases, more accurate readings than those provided by the CPU. The ideal situation would be to have metrics available by default on the majority of operating systems or hardware, along with having them give comprehensive coverage. Taking this into account would ensure that the final solutions, which would be based on the specified measurements, would function flawlessly across the widest range of platforms. The increased CPU consumption by the browser process is one of the most obvious changes on a system when it starts using these mining techniques based on the browser. Malicious JavaScript will be loaded to the client if it happens via a website; otherwise, if the user is not already infected via their browser, it will be a separate process, and the malicious code will be in a foreign language.

C.Cyptocurrency mining

Mining is the process of drawing, obtaining, or obtaining something useful from a pile. Since the discovery of the valuable metals in the earth's core, we have a solid understanding of the mining concept. The most valuable materials we can mine include gold, silver, copper, salt, iron, oil, and many others. There has never been a method for mining. To extract something of immense value from a mass of useless items calls for a constant, exhausting effort. Mining is the name for this laborious activity. If we wish to find gold or any other precious metal, we may need to delve far below the surface of the earth. The result can be successful or unsuccessful at times.

If the conclusion is unsuccessful, we must dig again and go through the same process until we locate the mine containing the valuable metal and extract it from it. Cryptocurrency. Cryptocurrency refers to the brand-new kind of money protected by encryption. The recent tendency has leaned heavily towards cryptocurrencies, and this era has seen many of them. One of the most widely used cryptocurrencies nowadays is bitcoin.

Ether, Litecoin, and many more are among the additional currencies. Mining of cryptocurrencies What is mining a cryptocurrency? What distinguishes mining for cryptocurrencies from mining for conventional commodities? Is mining for cryptocurrencies the same as conventional mining? What distinguishes mining for cryptocurrencies from mining for regular currencies? The broad definition of cryptocurrency mining is the extraction of cryptocurrency. Traditional mining and cryptocurrency mining are not the same thing. By resolving challenging mathematical equations and problems, bitcoin mining is done to obtain cryptocurrency units.

There is no central controlling body for the cryptocurrency. As a result, there are only so many units of the coin. Each unit has a unique digital data and key that can only be discovered by doing an enormous number of calculations. It must be accompanied by a cryptographic hash that satisfies specific criteria in order to correctly produce a block. Just calculate as many as you can and wait until you receive a hash that matches the required requirements is the only practical approach. A new block is created when the correct hash is discovered, and the miner who discovered it is rewarded with bitcoin units.

V. CONCLUSION

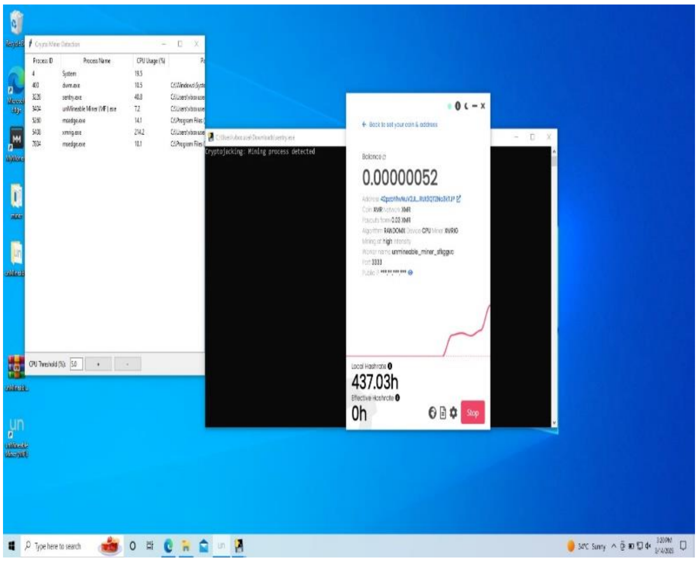
Cryptojacking is a developing cybersecurity risk that might result in serious monetary losses, harm to an organization's reputation, and legal and regulatory repercussions. It is a kind of attack where cybercriminals use a company's processing power without that company's knowledge or agreement to mine cryptocurrency. System sluggishness, higher electricity costs, and serious reputational harm can all result from this kind of attack.

To shield companies from this expanding threat, cryptojacking assaults must be detected. A cryptojacking detection system can offer real-time monitoring of system operations and network traffic to find any suspect cryptojacking activity. The system must be built to recognize and blacklist suspicious IP addresses linked to cryptojacking activity, recognize and identify crypto mining scripts running on the system or network, detect and identify crypto mining scripts, analyze system resource usage to spot any unusual patterns that might indicate cryptojacking activity, and produce alerts and reports to inform administrators when cryptojacking activity is discovered.

To offer a complete defense against cyber threats, the system should be created to connect with current security systems. The risk of cryptojacking assaults, which can result in major monetary losses, reputational harm, and legal and regulatory repercussions, can be greatly reduced by a reliable cryptojacking detection system. Organizations can safeguard their networks, systems, and data against this expanding threat and guarantee business continuity by putting in place a thorough cryptojacking detection system.

As a result, businesses need to emphasis cryptojacking detection in their cybersecurity plan. A thorough cryptojacking detection system may greatly lower the likelihood of assaults and safeguard networks, systems, and data from this rising danger. Organizations may maintain company continuity and safeguard themselves from financial losses, reputational damage, and legal and regulatory repercussions by putting in place a reliable cryptojacking detection system.

VI. Expected output

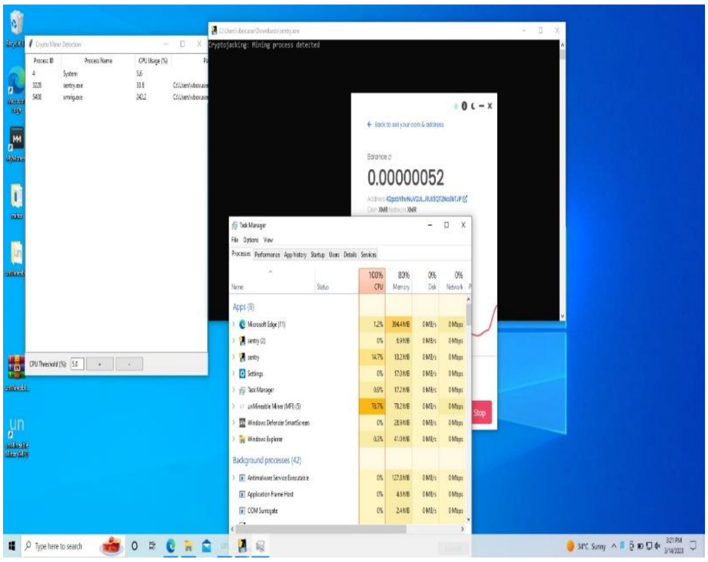


Crypto Miner Detection

Process ID	Process Name	CPU Usage (%)	Pa
4	System	19.5	
400	dwm.exe	10.5	C:\Windows\Syste
3226	sentry.exe	40.8	C:\Users\vboxuse
3404	unMineable Miner (MF).exe	7.2	C:\Users\vboxuse
5280	msedge.exe	14.1	C:\Program Files (
5408	xmrig.exe	214.2	C:\Users\vboxuse
7604	msedge.exe	10.1	C:\Program Files (

CPU Threshold (%): 5.0

```
Cryptojacking: Mining process detected
```



Crypto Miner Detection

Process ID	Process Name	CPU Usage (%)	Pa
4	System	5.6	
3226	sentry.exe	33.6	C:\Users\vboxuse
5408	xmrig.exe	242.2	C:\Users\vboxuse

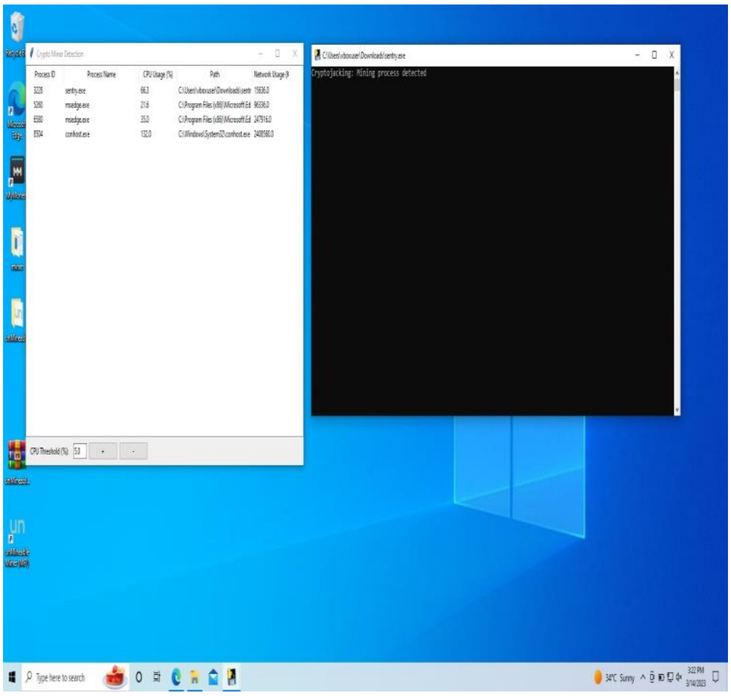
CPU Threshold (%): 5.0

```
Cryptojacking: Mining process detected
```

Task Manager

Name	Status	100% CPU	80% Memory	0% Disk	0% Network
Apps (8)					
Microsoft Edge (11)		1.2%	394.4 MB	0 MB/s	0 Mbps
sentry (2)		0%	6.9 MB	0 MB/s	0 Mbps
sentry		14.7%	13.2 MB	0 MB/s	0 Mbps
Settings		0%	17.0 MB	0 MB/s	0 Mbps
Task Manager		0.9%	17.2 MB	0 MB/s	0 Mbps
unMineable Miner (MFI) (5)		78.7%	79.2 MB	0 MB/s	0 Mbps
Windows Defender SmartScreen		0%	28.9 MB	0 MB/s	0 Mbps
Windows Explorer		0.3%	41.0 MB	0 MB/s	0 Mbps
Background processes (42)					
Antimalware Service Executable		0%	127.8 MB	0 MB/s	0 Mbps
Application Frame Host		0%	4.6 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.4 MB	0 MB/s	0 Mbps

File Options View
Processes Performance App history Startup Users Details Services
← Back to set your coin & address
Balance
0.00000052
Address 42pzbYfwNuV2JL...RU13QT2No3KTJP
Coin XMR Network XMR
Stop
Type here to search
34°C Sunny



Process ID	Process Name	CPU Usage (%)	Path	Network Usage (B
3228	sentry.exe	66.3	C:\Users\vboxuser\Downloads\sentr	15636.0
5260	msedge.exe	21.6	C:\Program Files (x86)\Microsoft\Ed	96336.0
6580	msedge.exe	35.0	C:\Program Files (x86)\Microsoft\Ed	247916.0
8504	conhost.exe	132.0	C:\Windows\System32\conhost.exe	2408560.0

CPU Threshold (%): 5.0

```
Cryptojacking: Mining process detected
```

References

[1]. Larson, Selena (2018-02-22). "Cryptojackers are hacking websites to mine cryptocurrencies". CNNMoney. Retrieved 2021-04-17.

[2]. "Cryptojacking malware was secretly mining Monero on many government and university websites". TechCrunch. Retrieved 2021-04-17.

[3]. Lachtar, Nada; Elkhail, Abdulrahman Abu; Bacha, Anys; Malik, Hafiz (2020-07-01). "A Cross-Stack Approach Towards Defending Against Cryptojacking". IEEE Computer Architecture Letters. 19 (2): 126–129. doi:10.1109/LCA.2020.3017457. ISSN 1556-6056. S2CID 222070383.

[4]. Caprolu, Maurantonio; Raponi, Simone; Oligeri, Gabriele; Di Pietro, Roberto (2021-04-01). "Cryptomining makes noise: Detecting cryptojacking via Machine Learning". Computer Communications. 171: 126–139. doi:10.1016/j.comcom.2021.02.016. S2CID 233402711.

[5]. "Coinhive domain repurposed to warn visitors of hacked sites, routers". BleepingComputer. Retrieved 2021-04-17.

[6]. Hwang, Inyoung. "What is cryptojacking? How to detect mining malware - MediaFeed". mediafeed.org. Retrieved 2021-05-11.

[7]. "Brutal cryptocurrency mining malware crashes your PC when discovered | ZDNet". ZDNet.

[8]. Peter Coogan (17 June 2011). "Bitcoin Botnet Mining". Symantec.com. Retrieved 24 January 2012.

[9]. Goodin, Dan (16 August 2011). "Malware mints virtual currency using victim's GPU". The Register. Retrieved 31 October 2014

[10]. Ryder, Greg (9 June 2013). "All About Bitcoin Mining: Road To Riches Or Fool's Gold?". Tom's hardware. Retrieved 18 September 2015.

[11]. "Infosecurity - Researcher discovers distributed bitcoin cracking trojan malware". Infosecurity-magazine.com. 19 August 2011. Retrieved 24 January 2012.

[12]. Lucian Constantin (1 November 2011). "Mac OS X Trojan steals processing power to produce Bitcoins: Security researchers warn that DevilRobber malware could slow down infected Mac computers". TechWorld. IDG communications. Retrieved 24 January 2012.

[13]. "E-Sports Entertainment settles Bitcoin botnet allegations". BBC News. 20 November 2013. Retrieved 24 November 2013.

[14]. Mohit Kumar (9 December 2013). "The Hacker News The Hacker News +1,440,833 ThAlleged Skynet Botnet creator arrested in Germany". Retrieved 8 January 2015.

[15]. McGlaun, Shane (9 January 2014). "Yahoo malware turned Euro PCs into bitcoin miners". SlashGear. Retrieved 8 January 2015.

[16]. Liat Clark (20 January 2014). "Microsoft stopped Tor running automatically on botnet-infected systems". Retrieved 8 January 2015.

[17]. Hornyack, Tim (6 June 2014). "US researcher banned for mining Bitcoin using university supercomputers". PC world.com. IDG Consumer & SMB. Retrieved 13 June 2014.

[18]. "Harvard Research Computing Resources Misused for 'Dogecoin' Mining Operation | News | The Harvard Crimson".

[19]. "Now even YouTube serves ads with CPU-draining cryptocurrency miners". ArsTechnica. January 26, 2018.

[20]. Palmer, Danny. "Cyber criminals are installing cryptojacking malware on unpatched Microsoft Exchange servers"