MiNo: The Chrome Web Browser Add-on Application to Block the Hidden Cryptocurrency Mining Activities

Safa Aktepe
Department of Computer Science
Sam Houston State University
Huntsville, TX 77341, USA
sba007@shsu.edu

Cihan Varol
Department of Computer Science
Sam Houston State University
Huntsville, TX 77341, USA
cvarol@shsu.edu

Narasimha Shashidhar
Department of Computer Science
Sam Houston State University
Huntsville, TX, 77341, USA
nks001@shsu.edu

***Abstract*— Cryptocurrencies are the digital currencies designed to replace the regular cash money while taking place in our daily lives especially for the last couple of years. Mining cryptocurrencies are one of the popular ways to have them and make a profit due to unstable values in the market. This attracts attackers to utilize malware on internet users' computer resources, also known as cryptojacking, to mine cryptocurrencies. Cryptojacking started to be a major issue in the internet world. In this case, we developed MiNo, a web browser add-on application to detect these malicious mining activities running without the user's permission or knowledge. This add-on provides security and efficiency for the computer resources of the internet users. MiNo designed and developed with double-layer protection which makes it ahead of its competitors in the market.**

***Keywords* — Bitcoin, Coinhive, Coin Mining, Cryptocurrency Mining, Cryptojacking, Hidden Cryptocurrency Mining**

I. INTRODUCTION

Cryptocurrencies are the digital currencies designed to replace the traditional cash money we use. Cryptocurrencies are decentralized which means they are not controlled by a single government, nation, or any regulatory agency. [1] They are built through a complex peer-to-peer (P2P) network. Users act as nodes in very large networks in these systems.

The very first attempt to build a cryptocurrency goes back to the late 80s. Researchers wanted to develop a digital currency to provide truckers to buy fuel late night in the Netherlands so gas station employees will be safe from any robbery etc. [2]. Another attempt called DigiCash utilized a new type of encryption named blinding formula and it provided money to be transferred to or from an account without the common way from a bank or money-storage location. Even though the company purchased by Microsoft, DigiCash failed [3]. PayPal came in the 1990s which provided secure, encrypted money transfer service. It allowed users to send money directly [4]. These steps take us to today's cryptocurrencies.

By late 2008, the most popular cryptocurrency, Bitcoin founded by an individual called Satoshi Nakamoto. He developed a P2P electronic currency transfer software that allowed individuals to transfer currency to other individuals without a central corporation with the inspiration from the P2P file sharing networks from early the 2000s. He also developed digital cash in this system which is also the first successful form of cryptocurrency. [1] Bitcoin became the model for the thousands of other cryptocurrencies of today.

There are two ways to have cryptocurrencies for users. The first one is directly buying or trading in different global cryptocurrency stock markets such as Bittrex, Binance, Coinbase, etc. Second, and widely used is mining the cryptocurrency which is also the way of production.

Blockchain is the technology that supports almost every cryptocurrency in the market now. It is a public decentralized register of every transaction that has been carried out in that coin. These transactions are assembled into blocks that are verified to ensure they are legitimate by coin miners. It first checks for that coin has not been expended before the transaction cleared. Then, it checks for input and output expenses fit. Lastly, the next sequential transaction block is getting connected to it which is how cryptocurrencies are made [5].

Since there is not a central authority in the cryptocurrency system, there needs to be a way of gathering every transaction that occurred with a cryptocurrency in order to create a new block. Miners are the network nodes who are carrying out this task.

Creating the block is depending on a cryptographic hash with some certain requirements. The best way to arrive at a hash matching the correct criteria is basically calculating as much as possible and try to catch the matching hash. When the hash successfully matches, then a new block is formed and the user who found it is being awarded with the cryptocurrency [6]. It means that miners are competing to calculate more hashes than each other with the hope of finding the correct value before anyone else does. Besides the competition, the difficulty of the calculation of the hashes is getting harder after every new block. It used to be possible to mine cryptocurrencies with a regular computer when the system was new. However, this is not the case anymore. As the system expanded significantly with more and more people started mining, now this process requires more powerful hardware, such as strong processor, high-end GPU, or

978-1-7281-6939-2/20/$31.00 ©2020 IEEE

several connected GPUs, or special chips designed for mining activities.

II. Background

Coinhive is the company created a script to let website owners can use to make money using website visitors' system resources to mine cryptocurrency called Monero. The goal of the system is to borrow a limited amount of the visitor's computer resources to mine cryptocurrency instead of bothering them with the ads. [7]. According to researchers from Trend Micro antivirus provider, attackers abused Google's Double Click ad platform to display malicious ad containing coin mining scripts to users from certain countries including Japan, France, Taiwan, Italy, and Spain [8]. These malicious ads were containing JavaScript which mines cryptocurrency known as Monero. 90% of the malicious ads displayed on YouTube were using the Coinhive's JavaScript which is publicly available. The remaining of the ads were using a similar script to avoid Coinhive's 30% cut from the earnings. These malicious scripts programmed to use 80% of the visitor's CPU. Even though officials announced that they removed all the malicious ads in less than two hours, professionals from Trend Micro proved that there were ads stayed longer than a week. Showtime is another video site targeted by the attackers by using mining scripts in ads. Independent security researcher Troy Mursch stated that attackers targeting video sites since users tend to spend more time on these sites and the more time user spent on the site means the more money attackers make [9].

AdGuard, a company specialized in blocking scripts from websites, released a report on October 2017. The report states that over 500 million computers affected by malicious cryptocurrency mining software all over the world. 220 of the top 100,000 websites had a mining script running on the background [10]. 220 may look like a small number however, this is only the number of websites with huge traffic. Also, hidden cryptocurrency mining trends were recently showed up at the time of this research which means this number possibly much bigger today.

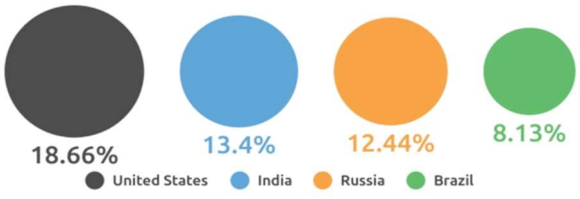

Fig. 1. Top 4 Countries of Websites using Mining Scripts [10]

Researchers discovered three different mining apps on these websites including LSEcoin, CryptoLoot, and MineMyTraffic [10]. Statistics show that more than 50% of the websites using the mining scripts from the four countries as the United States, India, Russia, and Brazil as shown in Figure 1. Another statistic from the research shows that the biggest part of the websites using mining scripts are websites offering free video downloads, torrent sites, and adult sites. Over 57% of the websites using mining scripts belong to four main categories which are TV/Video/Movies, File Sharing, Adult sites, and News/Media sites shown in Figure 2.

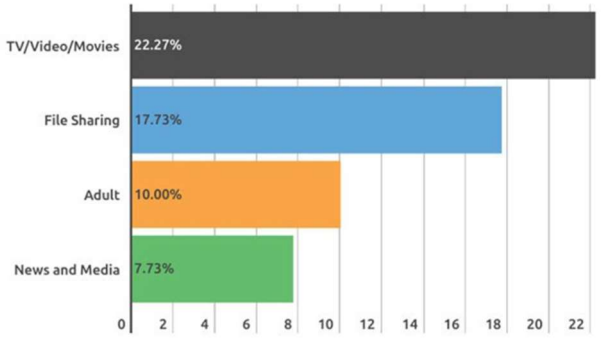

Fig. 2. Top Categories of Websites using Mining Scripts [10]

Since the popularity of web-based cryptocurrency mining is increased significantly, some of the antivirus programs started to add options to warn users for cryptocurrency-mining scripts hosted on websites and some of them giving users the option of blocking the activity. [9]

As shown in Figure 3, Google Chrome is the most widely used web browser in the world with a 59.9% share with the closest follower Safari with 15.7% [11]. Also, Chrome provides access to the task manager to manage the processes on the Developer Channel version which is one of the main functions we use. In this case, we decided to develop our add-on application on the Google Chrome web browser. Besides the high usage rate and functional benefits, a variety of the API libraries of the Google Chrome is providing access to many resources helping for efficiency.

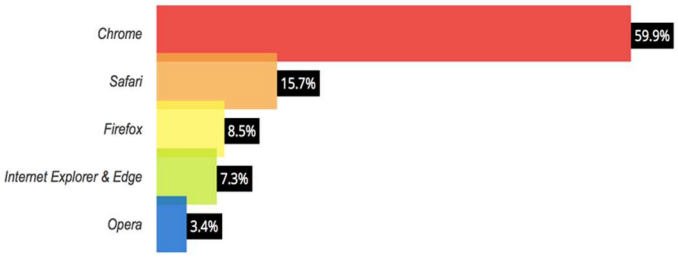

Fig. 3. Global Web Browser Market Share [11]

III. MiNo

To the best of our knowledge, there are only a few miner blocking applications available in the literature, such as NoMiner, AntiMiner, etc. They are all using a single layer protection mechanism and designed to only control some specific scripts. Single-layer protection mainly based on searching specific cryptocurrency miner scripts on the websites. It is obvious that it's not sufficient for catching all the malicious processes working on the browser since there will be new scripts and new techniques every day and it will be hard to follow up and update the list. Therefore, MiNo has a double layer protection mechanism which provides better protection with more control for the user.

MiNo consists of two main protection mechanisms to detect the cryptocurrency miners and protect system resources from being used without the user's consent. The first mechanism is the detection of the malicious cryptocurrency miner scripts and malicious URLs and the second one is the detection of high CPU usage of the processes running on the background. Both mechanisms can be active at the same time and the user can have double-layer protection. However, the user can disable the program or any of the protection mechanism anytime. We will review these functions of the MiNo below with details.

A. Script and URL Detection

The first control is based on the detection of the cryptocurrency scripts and malicious URLs. MiNo collects the malicious cryptominer scripts and URLs from an external file calls filters.txt inside the assets folder when it is installed into the Chrome browser. These filters in the file have been acquired from various resources including previous works and online resources. Once the MiNo has collected the filters, it can access the resources and requests of the web page with the functions provided by the Chrome API. In this case, MiNo has enough time to check the content before a web request is made by Chrome. Thereupon, MiNo scans the resources of the web page to check if there is any malicious script or URL. Currently, there is not an automatic update mechanism for the txt file where scripts and URLs stored. Content will be updated manually with newer versions. However, a mechanism to update the blacklist automatically from various resources can be considered as a future work of MiNo.

There are three possible results at this point. If there is no malicious script or URL found, then the web page will be loaded regularly without any change or block by MiNo. If MiNo detects only malicious script or scripts in the content, it would continue to serve the web page to the user however, it will prevent the malicious script from being included in the web request. Since the script is not included in the web request, it cannot run on the background. In this case, MiNo will only block the malicious content and let the user access the web page without any threat to computer resources. On the other hand, if MiNo detects any malicious URL, it will block the whole web page and will not let the user access to the web page in order to protect the system resources.

B. High CPU Usage Detection

The second mechanism is based on controlling the CPU usage rate of the processes running on the Chrome web browser. MiNo controls the CPU usage of the processes and blocks the malicious processes using a higher CPU rate than the set value. Hence, this is the biggest and most important difference of MiNo from its competitors.

There is a separate process created in the background for each content working on Chrome such as web pages and add-on applications and various information including name, CPU usage, network usage, etc. of these processes can be accessed by task manager and Chrome API. We first designed MiNo to determine the number of the cores of CPU through the Chrome API and use the variable limit of the CPU usage rate accordingly. However, after our detailed tests in both "known malicious websites" and "known clean websites" this method did not work as efficiently as planned. There were many false-positive results appeared during the tests. At this point, we redesigned the CPU usage control function with a single set value regardless of the number of CPU cores. After a careful review of the experiment and test results, we determined the optimum value for the limit is 80%. However, users can still adjust the default value of the limit of high CPU usage from the settings page.

All processes that are actively running in Chrome are listened on the background and the CPU usage is controlled every time the resource usage of the processes is updated. If any process momentarily exceeds the limit of high CPU usage, MiNo marks this process as suspicious and starts to watch it for 10 seconds. MiNo calculates the average CPU usage rate of these 10 second period and if this average value is over 80% then this process is marked as harmful and blocked. Users will be notified with either badge over the icon and/or popup notification per user preferences. MiNo also keeps records of the blocked processes in the history page with details.

Another great feature of MiNo with this mechanism is that it will control not only the web pages but also the add-on applications. Whenever an extension is installed and run on Chrome by the user, there will be a process created for this extension. Since MiNo controls all the running processes regardless of the type, in case if there is any malicious software exist in the extension it will be blocked by MiNo due to high CPU usage.

IV. Experiment

Our experiment for the MiNo based on various website visits with controlling both scripts and URLs and high CPU usage detection mechanisms together and separately. We classified websites as "Known Malicious Websites" which is the group of websites known by containing cryptocurrency miners and "Known Clean Websites" which is the group of websites known as clean from any cryptocurrency miners.

A. Known Malicious Websites

We used various internet resources to find websites contain cryptocurrency miners to use in our tests for MiNo. We visited 200 of these websites and a Chrome extension known as having a cryptocurrency miner for test purposes while testing both detection mechanisms together and separately. The results of the test are reflected in Figure 4.

MiNo detected cryptocurrency miners in 148 of the 201 websites (~74%) when both detection mechanisms were active. 7 of the 201 websites (~3%) have been detected by only the CPU usage control mechanism. Even though there is no cryptocurrency miner detected by the script/URL control mechanism, MiNo detected and blocked these malicious processes from the high CPU usage. These results show the importance of double-layer protection and the biggest advantage of MiNo against its competitors with having the CPU usage control mechanism.

46 of the total 201 websites (~23%) have only been detected by the script/URL detection mechanism. These websites either use a malicious script that is not active anymore and it doesn't perform any mining activities or it is still active but use a very limited rate of CPU power. Even though the scripts are old and not actively running, the threat is not clear completely since these scripts can still be used to mine cryptocurrency anytime. Hence, we kept them on our blacklist. An important point to mention at this point is MiNo only blocks the malicious script when it is detected and the user can still use the website regularly. Overall MiNo detected and blocked the scripts or websites 100% in the tests on known websites with cryptocurrency miners.

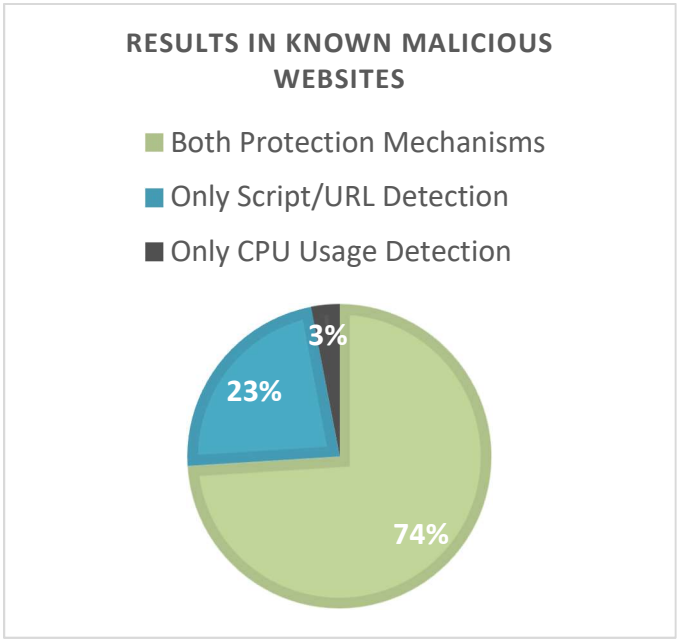

Fig. 4. MiNo test results in known malicious websites

B. *Known Clean Websites*

The second part of the tests has been done on known clean websites. MiNo has not detected anything and take no action on 97% of the websites. However, 5 of the 151 websites, 3%, are using higher CPU than MiNo's set limit of 80 as shown in Figure 5. In this case, MiNo blocked these websites. Even though we consider these results as false-positives, it can also be considered as a protection of the system resources with or without cryptocurrency miners.

V. Conclusion

Cryptocurrencies took their places in our daily lives and we are facing more and more incidents of misusing cryptocurrency mining every day. With the increasing popularity of the blockchain system which is also known as the technology of the Bitcoin and other alternate coins such as Ethereum, Litecoin, Ripple, and thousands of other coins, attackers finding different ways to take advantage of these areas. Hidden cryptocurrency mining in internet user's browsers without permission or knowledge of the user is one of the most popular trends especially recently [12]. According to recent research done by the IT Security company Quick Heal Technologies over three million cryptojacking hits detected between January-May 2018 [13]. Also, it is expected these numbers and cryptojacking attacks to grow in the near future since cryptocurrencies still attract cybercriminals due to market values.

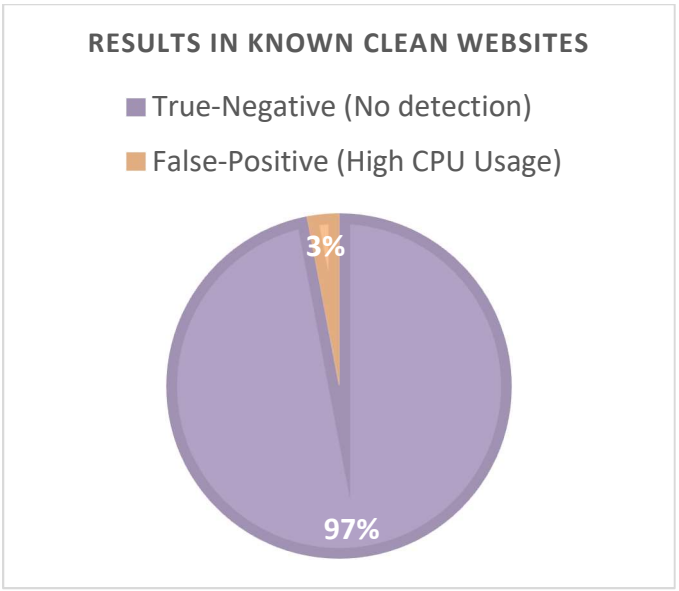

Fig. 5. MiNo test results in known clean websites

MiNo has been developed to prevent these cryptojacking attacks and protect users and their computer resources. It has two layers of protection mechanism which is not only the biggest difference from its competitors but also the source of its very high success rate of detecting and blocking malicious cryptocurrency scripts and websites.

There were two areas can be considered as future work for MiNo. One of them is adding a whitelist feature to create and improve a whitelist of trusted webpages which can be controlled by the user to prevent any possible false-positive results without disabling MiNo. The second one is using a longer control time for CPU usage detection function to prevent false-positives in clean websites due to instant high CPU usage. However, MiNo is still operating with a very high success rate with the current version. In this case, these can be considered as improvements to add on top of its current functionality.

References

[1] Biscontini, T. "Cryptocurrency" Salem Press Encyclopedia of Science. 2017.

[2] Griffith, Ken "A Quick History of Cryptocurrencies BBTC – Before Bitcoin" Bitcoin Magazine, April 16, 2014

[3] Pitta, Julie. "Requiem for a Bright Idea." Forbes. N.p., 1 Nov. 1999. Web. 5 May 2016.

[4] Grabianowski, Ed; Crawford, Stephanie. "How PayPal Works". How Stuff Works. 13 December 2005.

[5] "Blockchains & Distributed Ledger Technologies" BitcoinHub, January 19, 2018

[6] Shepherd, A. "What is Cryptocurrency Mining?" itpro.co.uk/ Mar. 13, 2018
[7] Pressman, A. "The Growing Threat of Cryptocurrency Mining Malware" Fortune.com. 1, Nov. 15, 2017
[8] Hruska, J. "YouTube's Covert Cryptocurrency-Mining Ads" *PC Magazine*. 14, Mar. 2018. ISSN: 23732830.
[9] Goodin, D. "Now even YouTube serves ads with CPU-draining Cryptocurrency Miners" Ars Technica, Jan. 1, 2018
[10] Meshkov, A. "Cryptocurrency Mining Affects Over 500 Million People. And They Have No Idea It Is Happening" Industry News, Cryptojacking, AdGuard Research Oct. 12, 2017.
[11] "Browser & Platform Market Share – February 2018" W3 Counter, Feb. 2, 2018
[12] Orcutt, M. "Hijacking Computers to Mine Cryptocurrency Is All the Rage" MIT Technology Review, Oct. 5, 2017
[13] Katkar, S. "Over 3 million cryptojacking incidents in 2018, more expected" Quick Heal, June 25, 2018