International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Browser Extension for Cryptojacking Malware Detection and Blocking

Shubham Patil[1], Sushant Shastri[2], Sriram Iyer[3], Prof. Vijay. N. Patil

[1,2,3]X76/15,Godrej station colony, Vikhroli(E), Mumbai-400079
BMC colony 1/10, Marve Road, Lower kharodi, Malad West, Mumbai-400095
[4]Information Technology Engineering, Bharati Vidyapeeth College of Engineering, Sector-7, C.B.D, Belpada, Navi-Mumbai-400614, India

---

Abstract - *Cryptojacking has been on the rise in the last few years and many people are not aware of this issue. Crptojacking is a type of attack where attacker utilizes the CPU power when all the systems visiting the site where the malware script is uploaded and uses their compute power to mine cryptocurrency for the attacker. This type of attack mostly goes unnoticed as many users are not aware of such a threat and if users aware of the problem they don't know the sites in which the malware is hosted. The website which hosts such malware doesn't ask the consent of the user and that makes such attack unethical. We propose on creating browser-based extension which will have the capability to detect such malware when user visits a certain webpage. Once the user opens a website it will check for the malicious JavaScript code in the contents of the HTML page. On detection it will generate a popup indicating the user that the site user is visiting contains cryptojacking script embedded in it. Now if the user wants to visit the website even after knowing this it will simply block the part of malicious script in the page the user is visiting and will allow the user to access the site without worrying about any of their compute power being used by the attacker to mine cryptocurrency for himself.*

Keywords: Cryptocurrency, Monero, Bitcoin, Cryptojacking, Extension, Cryptojacking Script, CPU power, GPU Power, Cryptojacking Websites.

1. INTRODUCTION

Cryptocurrency first came into existence in the year 2009 by pseudonymous developer Satoshi Nakamoto and the cryptocurrency he developed was called Bitcoin. Later many cryptocurrency came into the existence besides Bitcoin such as Monero, Litecoin, etc. The cryptocurrency market has undergone significant growth in 2017–2018. Due to this many people began investing in Cryptocurrency throughout the world. The concept of cryptojacking first came in to existence in the in late 2017 and start of 2018.Cryptojacking was a much easier way to use other people resources i.e CPU power for mining cryptocurrency for the attacker.

All of this is done by simply adding a javascript code to a webpage which attracts a lot of visitors. When user visits the website in which such javascript code is present it will utilize the entire CPU power of the user visiting that website for mining cryptocurrency like Monero for the attacker. Each visitor might only do a tiny bit of mining while they're there, but every user lending some hash power over time can generate real money. And users might not even notice what's happening. Now imagine if the website is being accessed by thousands or millions of users worldwide, all of those systems CPU power used by the attacker for his own gain without the user even realizing what is happening.

Nowadays almost about 80% of the world's population is connected to internet and Internet has become one of the most integral part of all of our lives. Cryptojacking is on the rise nowadays as many people don't even know what cryptojacking is and hence become easy prey for the attacker.

Thus with the browser-based extension we plan on making aware of all the users about cryptojacking and preventing unethical use of CPU power of the thousands of users without the consent of the user for attackers own gain.

2. LITERATURE REVIEW

Cryptojacking is the recent trends towards in browser mining of cryptocurrencies in particular the mining of monero through CoinImp and similar Websites.[1] When a user visits some particular websites it will may download some malware javascript code that executes at client-side of user's browser, which will lead to mining of a cryptocurrency typically without user's consent or knowledge and generates the revenue for the attacker who injects such code in the website. Such websites may prove to be as an alternative medium of generating the revenue, which offers premium content in exchange of mining, or may be unwittingly serving the code as a result of breach.[1]

Cryptojacking is unauthorized use of users compute power for mining cryptocurrency like Monero for himself.[2] This type of attack is unethical as the user is not even aware that his system is working as a miner for the attacker. Cryptojacking has been on the rise since late 2017 and is widely used in many websites as it enables the attacker to use the compute power of all the users visiting the website rather than buying a ASIC or

GPU and using his own system for mining cryptocurrency as the latter results in high electricity charges for the attacker.

Recently, a method of detecting and interrupting unauthorized, browser based crypto mining is proposed, based on semantic signature-matching. The approach addresses a new wave of crypto jacking attacks, including XSS-assisted, web gadget-exploiting counterfeit mining. Evaluation shows that the approach is more robust than current static code analysis defences, which are susceptible to code obfuscation attacks. An implementation based on in-lined reference monitoring offers a browser-agnostic deployment strategy that is applicable to average end-user systems without specialized hardware or operating systems.[5]

In a recent paper it shows the demonstration of how crypto jacking occurs by giving an overview of CPU or memory consumption of our computer. It also gave an outlook on Crypto Jacker Software. It is a software that combine CoinImp, Authedmine and Crypto-loot and incorporate these into a word press plugin with added search engine optimization (SEO) functionality. It focusses that how software works as in that software the users can load meta data from destination url, making it feature highly in search engine rankings. Moreover, it also does social cloaking a kind of phishing technique. It also suggested how you can protect yourself from crypto mining by using the techniques such as ad-blocker etc.[6]

3. ACTUAL IMPACT ON USER SYSTEM THROUGH CRYPTOJACKING ATTACK

In this paper it tries to demonstrate how cryptojacking attack actually affects the user's system computing power with the help of two ways. For this, two scenarios have been considered. First, scenario we consider the user system before executing the cryptojacking malware script. Second, scenario we consider the user system after executing the cryptojacking malware script which is injected in particular website and is running at background of user's system. This attack we prove with the help of first, checking the cpu performance of the user's system through inspecting the taskmanager of the system.

The second way this paper tries to prove the attack is through running the simple java code in the system that prints the number from 1 to 1000000 and display its execution time in millliseconds. This experiment is shown in the paper to demonstrate how cryptojacking malware script also affects the performance of other task executing simultaneously in the system.

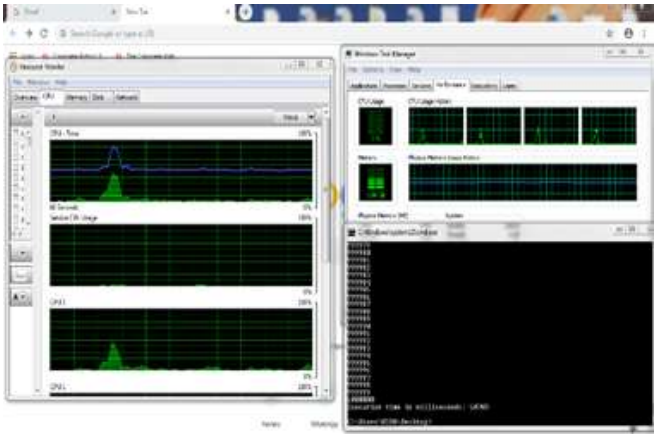

Fig1. Scenario of user system before executing cryptojacking malware script.

From the above figure it is shown that **before** visiting any website in the browser that contains cryptojacking script the cpu performance of the system is recorded as approximately 9% of the system. Also the java code of printing 1 to 1000000 numbers took the execution time of approximately 68556 milliseconds which is nearly about 69 seconds.

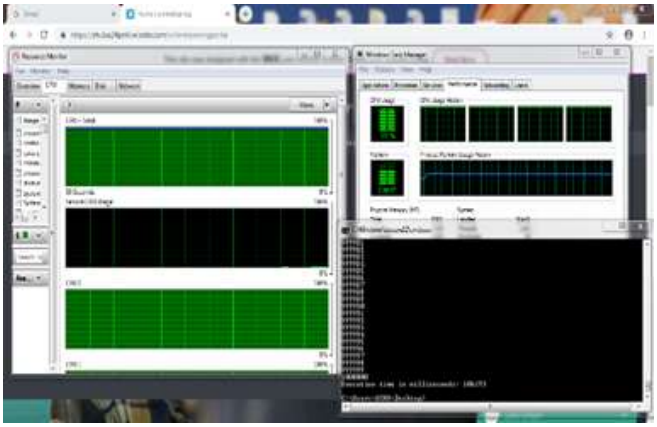

Fig 2. Scenario of user system after executing cryptojacking malware script running at the background of the system when the user visits the website having such script injected in it.

From the above figure it is shown that **after** visiting any website in the browser that contains cryptojacking script the cpu performance of the system jumps to full 100% thereby utilising the whole cpu consumption of the system. Also the java code of printing 1 to 1000000 numbers took the execution time of approximately 89242 milliseconds which is nearly about 83 seconds. Thus, it concludes that when the user visits such websites having such cryptojacking script injected in it, such script continuous to run at the background of the system thereby affecting the execution time of the other tasks running simultaneously in the system.

4. SYSTEM ARCHITECTURE

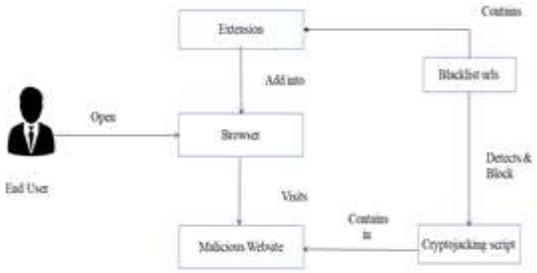

Fig3. Block Diagram

The front end system gives graphical interface in the form of a browser extension. When the user visit any website the system will check whether the particular website is using cryptojacking script for mining the cryptocurrency through user system. The system will match the url mentioned in the script with the list of urls stored in the database as the back-end of the system. If it matches, the extension will show some notification or pop-up message indicating that the particular website may have cryptojacking script embedded in it. Moreover, the extension will also provide the blocking functionality through which user can block the cryptojacking malware script running at the background thereby preventing the user's cpu power being stolen and without affecting the rest of the functionalities of website.

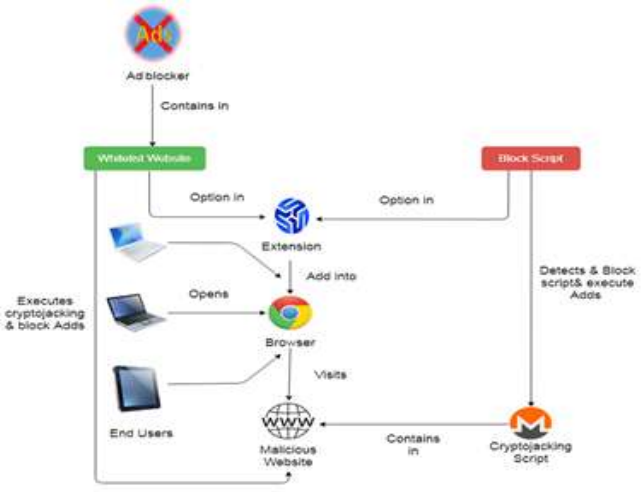

Fig.4 Architecture Diagram

5. PROPOSED SOLUTION

In this paper, it shows that the browser extension will help the users by alerting the user when such script is detected on the webpage the user is visiting. It will also enable the user to block only the malicious script in the webpage if user still wants to visit the website.

The system will detect all the websites that uses such cryptojacking script when the particular user visits that website. Moreover, for blocking the system will provide two options for user. First, option will contain whitelist option. This option is included because there are many users who irritate with the adds that displays on the website sometimes, the adds pop-pup in between thereby interrupting the execution time of user. So, when the user chose this option the website will continue to run the cryptojacking malware script but it will block all the adds contain in the website. The another option is blacklist option in which the system will completely block the malware script that contains in the website but the ads will continue to display it on website as there are people who are okay with the adds that displays on the website but can't compromise with the consumption of their system's computing power.

6. CONCLUSION

The Extension aims to prevent the users compute power from being stolen and utilized by attacker from mining cryptocurrency for himself. Attackers using user's CPU or GPU power for his gain without the consent of the user is unethical. Crypto jacking malware has the potential to slow the processes running on user's system without the user knowing what exactly is causing this change. The extension aims to block the script which causes this problem so that user can access the website without worrying of compute power being stolen from his system.

7. REFERENCE

1) A first look at browser based crypto jacking by Shayan Eskandari, Andreas Leoutsarakos, Troy Mursch, Jereny Clark Concordia University, Bad Packets Report.
2) Cryptojacking - Cryptomining in the browser by ENISA
3) Crypto jacking: How Hackers Are Mining Cryptocurrencies without your Knowledge by Sudhir Khatwani.
4) Digging into Browser-based Crypto Mining by Jan Ruth,Torsten Zimmermann,Konrad Wolsing, Oliver Hohfied chair of Communication and Distributed Systems RWTH Aachen University.
5) SEISMIC: Secure In-lined Script Monitors for Interrupting Cryptojacks :by Wenhao Wang, Benjamin Ferrell,Xiaonyang Xu,Kevin W.Hamlen and Shmang Hau from The University of Texas.
6) Cryptojacking : An Overview | Digital Shadows (https://www.digitalshadows.com/blog-and-research/)