



Cryptojacking



Cyber Security Project, IIIT Sri City

Group Members

Adwait Thattey - S20170010004

Kevin John - S20170010070

Nikhil Sampangi - S20170010136



Contents

1	<u>Scope</u>	3
2	<u>Objective</u>	3
3	<u>Justification of Title</u>	4
4	<u>Background</u>	5
5	<u>Literature Review</u>	6
	- <u>Study I</u>	6
	- <u>Study II</u>	11
6	<u>Our Analysis</u>	13
7	<u>Conclusion</u>	18
8	<u>Bibliography</u>	19

Scope

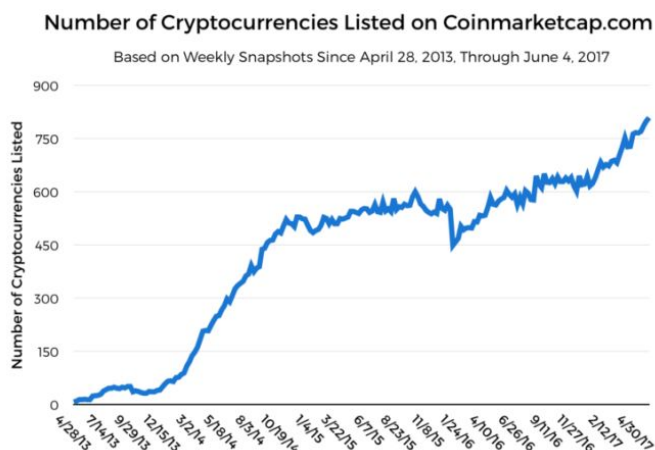
The scope of this project entails conducting an extensive research on the malicious practice known as cryptojacking by studying research papers, examining previous instances of this attack as case studies and reviewing articles, studies and other sources of information to formulate a comprehensive report on Cryptojacking.

Objective

This project aims to explore and cover the in depth analysis of Cryptojacking malware which includes understanding how it operates, why it is feasible, how it is deployed, and how to protect from it.

Justification of Title

Blockchain is one of the raging topics right now in computer science. A lot of research has gone into mechanisms of blockchains in the last decade. Blockchains have found new use cases in Healthcare, Banking, Transport sectors. However still, the most wide use of blockchains is crypto currencies.



Ever since the introduction of Bitcoin, the number of crypto-currencies in the market has steadily grown

Mining crypto currencies requires a large amount of computation power. In recent years, hackers have found ways to exploit individual machines to work towards mining the currency. This makes the problem very interesting from a cyber security perspective.

Also in the current covid crisis, the crypto currencies have seen a rally and investors move towards these digital alternatives. This will certainly lead to an increase in attacks in the near future and hackers try to exploit the situation maximum to their advantage.

Thus we found this topic exiting to research into and get in depth information on how these things work and how we can counter them in future

Background

Crypto-currency is a term used to denote digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit. Many cryptocurrencies are decentralized networks based on blockchain technology - which simply put is a ledger distributed in a decentralized fashion which stores the records of the provenance of a digital asset.

In a little under a decade, crypto-currency has developed from an esoteric experiment to one of the hottest topics in both the technology and finance fields. Since the emergence of Bitcoin as the first centralised crypto-currency in 2009, the industry has exploded and there are more than 1,500 different currencies now available.

Alongside all the investors and fortune hunters, crypto-currency has unsurprisingly become a major point of interest for cyber-criminals, and in many respects presents a perfect opportunity for criminal misuse. These cyber-crimes involving cryptocurrency can range from Ransomware

attacks which demand ransom in the form of bitcoin (or any other cryptocurrency) to running a script in someone else's device which in turn utilizes their computing power to mine crypto-currency. The former of the aforementioned examples is termed as Cryptojacking which constitutes the gist of this Research

Literature Review

We explored numerous articles and research papers for this project. Here we will summarize a few that we felt provided the good insight.

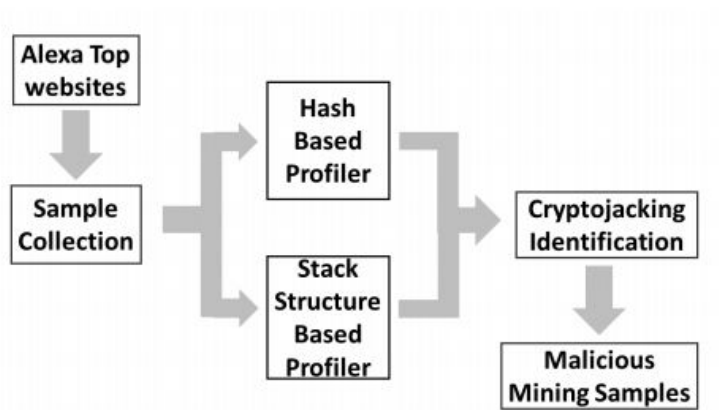
Paper I

Geng Hong & Zhemin Yang (2018). A Systematical Study about Cryptojacking in the Real World. (Fudan University)

Goal: This paper presents a new behavior-based crypto-mining detector for tracking browser based crypto-mining called CMTracker. It leverages a set of inherent characteristics of cryptojacking scripts for automatically tracking Cryptocurrency Mining scripts in websites.

Using CMtracker, it provides findings and statistics on how much browser-based crypto-mining is prevalent.

Working:



CMTracker applies mainly 2 methods for tracking crypto minings

Hash based profiler:

It tracks a set of fixed signatures from 9 commonly used hashing libraries (like "cryptonight_hash", "sha256", "crypto" etc.). Then it calculates the cumulative time of the websites they spent on hashing. Normal websites take upto 0.5% of time for hashing. Since mining requires a lot of hashing, this number can go up to 20% on websites that are mining

currencies. All the websites that use more than 10% of the time in hashing are directly classified as mining and rest are further analyzed.

Stack Structure Based Profiler:

Has function analysis is straightforward but can be easily evaded with code obfuscation techniques. The idea is that cryptocurrency miners run heavy workloads with repeated behavioral patterns revealed by their execution stack, which can be utilized as an important tip for identifying the existence of cryptocurrency mining. A normal webpage rarely repeats the same calling stack for more than 5.60%. Thus, if a dedicated thread repeats its call chain periodically (in a fixed time interval), and the call chain occupies more than 30% of the whole execution time in this thread, it is reported as a cryptocurrency miner.

Findings:

After scanning 853,936 popular web pages CMTracker found 2,770 cryptojacking samples, which included 868 among Alexa top 100K. It is estimated that at the time of this research, nearly 10 Million users were affected each month. Further analysis showed that these cost around 278K kWh extra energy consumption per day and the attackers were able to earn over 59K US dollars a day.

They found the following distribution of target areas among the positive websites

Websites Category	# Websites with Scripts	Percentage (%)
Art and Entertainment	752	27.1
Adult	360	13.0
Internet and Telecom	323	11.7
Business	182	6.6
Game	180	6.5
Others	973	35.1
Total	2,770	100

Blacklisting: AT the time of this research, the 2 most popular blacklisters [NoCoin](#) and [MinerBlock](#) were able to detect less than 51% of total websites flagged by CMtracker rendering them not as effective.

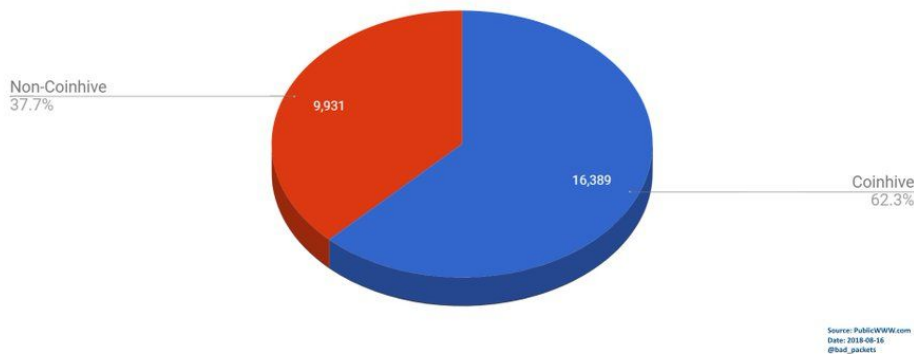
Evasion Techniques used by mining scripts:

- Limiting CPU usage: Most of the scripts do not use more than 70% of the available CPU so that the users do not experience much lag and they are not easily detected.
- Code Obfuscation for Mining Scripts: About 20% of the scripts flagged by CMTracker were using techniques that made it very hard to detect by automatic trackers.
- Payload Hiding: Instead of injecting malicious payload directly to the cryptojacking webpages, many attacks chose to hide their malicious code in 3rd party libraries.

Our analysis of this paper:

This paper was published in early 2018. At that time a major percentage of browser based crypto-mining operations were powered by Coinhive.

Number of websites found with a JavaScript cryptocurrency miner



Stats from Aug 2018

Thus this paper reflects the same. Majority of the websites flagged by CMTracker make use of CoinHive.

After CoinHive closed operations in late 2018, browser based crypto-mining fell drastically and hasn't fully recovered. However there are other alternatives available today, even though they are not as easy to use. This is bound to reflect back on the statistics. So it is likely that the top 100k alexa websites will contain a less percentage of positive websites today.

Paper II

Marius Musch & Christian Wressnegger. Web-based Cryptojacking in the Wild
(Technische Universität Braunschweig Institute for Application Security, Germany)

This report provides analysis on Web-based Cryptojacking has become profitable in recent years and what are the technological advancements that make it efficient to deploy browser based crypto mining.

Why web based crypto mining has become profitable:

Traditionally, digital currencies like BitCoin used proof of work functions that required a lot of computation power to mine which could be provided by high power GPUs setup on mining rigs. Mining on normal CPUs was not feasible.

As a remedy, alternative cryptocurrencies were developed in the community that make use of memory-bound functions for constructing computational puzzles. Examples are CryptNote and CryptoNight that form the basis for alternative cryptocurrencies that can be efficiently mined on regular desktop systems providing the foundation for web based crypto mining. CryptoNight determines the hash value for an input object by extensively reading and writing elements from a 2 Megabyte memory region that makes it ideal for CPU use as memory access are faster in CPUs.

Major crypto currencies that work on this foundation and principles are Monero and Electroneum. Most web based mining libraries/ snippets mine these or similar currencies. Profitable mining on desktop systems and the availability of different currencies following the same cryptographic protocol render these currencies an ideal target for web-based mining.

How most web based crypto mining is deployed:

Low level programming languages are essential for efficient mining. JavaScript and ActionScript in itself, do not provide efficient primitives for low-level programming. However recent additions to standards have introduced technologies that make it possible and easier to mine on websites. Some of these are:

WebSockets: These allow fast and efficient communication between server and the client which are essential for mining

WebWorkers: Even though async programming is present in Javascript, Webworkers increase the threading capacity ten folds. This allows the code to scale with growing CPU cores, which makes it more efficient to deploy mining scripts

WebAssembly: This is the most recent addition, which increases the capacities of browsers a lot. It allows compilation of high level code from Rust/C++ into low level Wasm code that can be executed on stack based virtual machines. It makes it much easier to write mining scripts as it enables compiling cryptographic primitives, such as specific hash functions, from a high-level programming language to low-level code for a browser which is much more efficient.

Our Analysis

Overview

Cryptojacking is a rising online danger that disguises itself as a normal program on a PC or cell phone and uses the machine's assets to mine many different online digital money known as Cryptocurrency. It's a hazard that can take over browsers, also also a wide range of gadgets, from computer and PCs, to mobile phones and even system servers as well as microcontrollers. Like other attacks the intention is monetary benefit, yet unlike other threats, it's intended to remain hidden the victim.

What are Crypto-currencies

Cryptographic forms of money are types of digital cash that exist just in the online world, with no genuine physical structure. They were made as an option in contrast to conventional money, and picked up prominence for their forward-looking plan, development potential, and annonymity. One of the earliest, most successful forms of cryptocurrency, Bitcoin, came out in 2009. By December 2017, the value of a single bitcoin had reached an all-time high of nearly \$20,000 USD. All digital forms of money exist as encrypted decentralized monetary units, openly transferable between internet users.

What is cryptojacking?

Cryptojacking is a method to use people's gadgets (phones, PC, tablets), without their consent or knowledge, to secretly mine crypto coins on the individual's PC. Rather than building a dedicated cryptomining PC,crackers/hackers use cryptojacking to take processing assets from their victims' machines.

Most cryptojacking malware is made to stay invisible from the user, however that doesn't mean it's not incurring significant damage. Cryptomining softwares slows down other processes, increases your power bills, and deteriorates the lifespan of your machine. If your machine becomes slow or fan speeds is higher while not running taxing tasks, a cryptojacking malware may have been installed on your device.

Why cryptojacking is popular?

The straightforward motivation behind why cryptojacking is gaining popularity with crackers/hackers is more money for less risk. With ransomware, a hacker might get three individuals to pay for every 100 PCs infected. With cryptojacking, every one of the 100 of those infected machines work for the cracker/hacker to mine digital currency. Over and above till discovered the infected machine keeps mining Cryptocurrencies.

The danger of getting caught is likewise considerably less than with ransomware. The cryptomining code runs clandestinely and can go undetected for quite a while.. When found, it's extremely difficult to trace back to the source, and the victims have no incentive to do so as nothing was stolen or encrypted.

How cryptojacking works?

There are numerous ways your PC can get infected with cryptojackers. Classic techniques like phishing, malicious links in emails, popup downloads etc will download and install crypto-mining programs into your PC. Once your computer is infected it runs constantly in the background allowing the hacker to control how much of the PC's processing power should be

used. The software may also traverse horizontally through a person's network and infect other PCs in the network.

An alternative cryptojacking technique is called drive-by cryptomining. Just like malicious ad exploits, the method involves embedding a block of JavaScript code into a website. After that, it mines crypto coins on your PC that visit the website. Drive-by Cryptomining affects mobile devices as well.

Why is Cryptojacking harmful?

Compared to the damage that a serious ransomware infection or Advanced Persistent Threat can inflict, a crypto-jacking attack seems like a fairly minor risk. While enterprises should indeed prioritize these more obviously dangerous threats, mining does create several problems that should not be ignored.

From a user point of view, Cryptojacking malware can completely bring your PC to a halt by overloading your CPU and GPU to mine crypto-currencies. In some cases, crypto-jacking has even been reported to cause physical damage to its targets. The average laptop or desktop machine is resilient enough to sustain mining software with no ill effect other than slightly overheating, but many mobile devices are not able to weather the strain. This is especially a problem with web based cryptomining. Most websites can be opened using a mobile as well as a desktop. But mobile devices can not cope up with the load of mining and often slow down the devices causing immense frustration in the users.

From an enterprise point of view If an enterprise is being targeted with a watering hole attack that is designed to hit as many employees as possible, the combined toll of the processing power

being stolen by the mining software can considerably slow the network. A particularly bad case with a script that uses a lot of CPUs could lead to a DDoS-type situation that disables the network and causes major issues for the organisation. This can also use up a significant amount of computation power, which is a problem for small companies and open source communities that rely on small, limited (often borrowed or donated) computing capacity. Even a mild incident can be a very disruptive to key operations, as well as causing a great deal of irritation among staff

Real-world cryptojacking examples

Cryptojacking has been implemented in many different schemes to mine crypto currency. Most delivery methods have been derived from regular malware distribution. To name a few large scale attacks.

Spear-fishing PowerGhost -

It is a stealthy malware that can avoid detection in a number of ways. It first uses spear phishing to gain a foothold on a system, and it then steals Windows credentials and leverages Windows Management Instrumentation and the EternalBlue exploit to spread. It then tries to disable antivirus software and competing cryptominers.

Graboid -

Graboid is the first known cryptomining worm. It spreads by finding Docker Engine deployments that are exposed to the internet without authentication. Palo Alto Networks estimated that Graboid had infected more than 2,000 Docker deployments.

BadShell

Badshell used PowerShell to execute commands. a PowerShell script injects the malware code into an existing running process. It also used Task Scheduler to ensure persistence and the Registry to hold the malware's binary code.

How can I protect myself from cryptojacking?

Regardless of whether you have been cryptojacked locally on your framework, or through the program, it tends to be hard to physically identify the intrusion afterward. Similarly, finding the root of the high CPU use can be troublesome. Procedures may be concealing themselves or veiling as something genuine so as to impede you from stopping the abuse. As a bonus to the cryptojackers, when your PC is running at most extreme limit, it will run very slow, and in this way be more hard to investigate. As with all other malware precautions, it's much better to install security before you become a victim.

One clear alternative is to block JavaScript in the program that you use to surf the web. In spite of the fact that that interferes with the drive-by cryptojacking, this could in like manner prevent you from utilizing capacities that you like and need. There are also specialized programs, such as “No Coin” and “MinerBlock,” which block mining scripts in well known browsers. Both have extensions for Chrome, Firefox, and Opera.

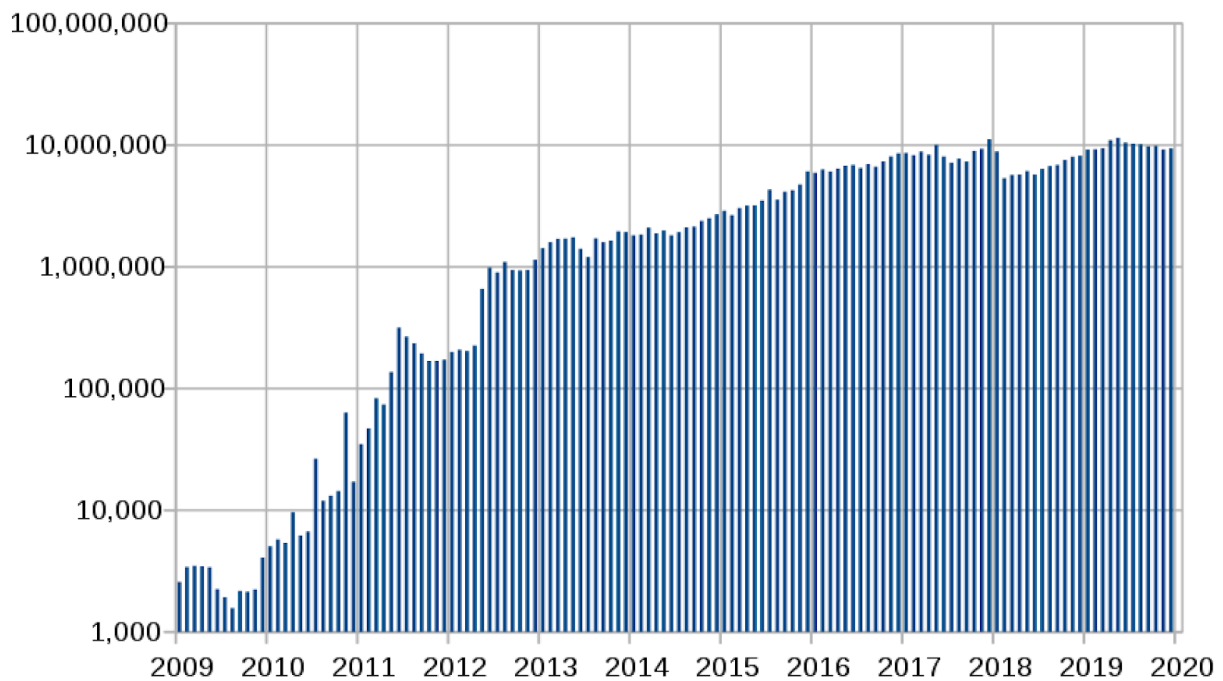
However the most useful option is to install a comprehensive cyber security Anti-virus / Anti-Malware software before you are infected. Most Anti-Virus software comes with a whole package of protection from multiple different attacks including cryptojackers They can detect signatures of Cryptojacking malware and stop it from running on the device before it even starts. At an enterprise level a company can conduct cyber security awareness workshops to keep employees upto date with such practices so they can be more aware and take necessary precaution while using their computers.

PTO->

Conclusion

It is without a doubt that cryptocurrencies will keep evolving more and more. In the future, many agencies and businesses will start using cryptocurrencies as means of payment. Even some of the government agencies are trying to adopt Blockchain Technology.

For Instance, take the case of the cryptocurrency BitCoin. Back in 2010 when nobody was aware what cryptocurrency was, the value of bitcoin was basically nothing but by December 2017 Bitcoin broke the trading charts by surging up to 20,000 dollars.



Number of bitcoin transactions per month src: Wikipedia

The owner of Snapchat, Jeremy Liew and Blockchain co-founder Peter Smith predicts that by 2030, this price will have reached \$500,000.

In Conclusion, Cryptocurrency brings with it a plethora of opportunities for the future, but along with these beneficial factors, it also brings the increase in Cyber attacks, malwares directed at Cryptocurrency. Cryptojacking has become a source of easy money for hackers. Protecting from cryptojacking is going to be especially important in the coming days of IOT future. As the number of connected devices in homes explode, so will the opportunities for hackers. There are already cases of hackers breaking into IOT devices like cameras and fridges in large amounts to mine crypto-currencies and these are certainly going to increase in the future.

Cryptojacking is often undermined by people and considered not as destructive as other malicious things like ransomwares and viruses. But this overlook has led to increased attacks in this area. Cryptojacking, just like other malware, prevents the devices from functioning normally, which might be performing some critical tasks. Thus this domain should be given equal attention as others.

In the coming future we will need investments and awareness programmes so to prevent and protect ourselves from Malwares such as Cryptojacking.