A Recapitalization on Crypto jacking and end to end Analysis of Ransomware Attacks

G. Prema Arokia Mary, N. Suganthi, M. S. Hema

Abstract - The recent trend of today's digital media is the usage of poisoned website to mine crypto currencies, these currencies are alternatives to traditional currencies which work based on decentralization, bit coin was the first currency to be establish in this way, crypto currencies are protected with block chain which can be simplified as growing chain. This block chain is managed by peer to peer network, based upon this blockchain network crypto jacking takes place, and hence cryptojacking is mining of one's digital currencies without their knowledge, hackers find cryptojacking more profitable because they are a lotcheaper and safe than compared to other digital thefts. Tracking and finding the cause of theft becomes very hard in this method because mining kits can be purchased at a very cheap cost. There are primarily two methods to be followed to get to the computer and to perform cryptojacking, one is to run a infected code on the host computer and the other is to make the user click the content with threat but widely both will be used for increased profit outcome. In this paper an overview of crypto currencies, method of decentralization, various mining techniques followed and different types of cybercrimes prevalent are discussed.

Keywords: Crypto jacking, Crypto currencies, Mining, Online scams.

I. INTRODUCTION

Currencies which are involved in digital transactions are called as crypto currencies .The recent trend of today's digital mediais the usage of poisoned website tomine crypto currencies , these currencies are alternativestotraditionalcurrencies whichworksonthebasisof decentralization[1]. Based upon the decentralization a new digital currency came into existence and it was termed as bit coin. After the invention of these currencies there are several other alternate coins created for the same purpose. Mining is considered to be the basic building blocks for these currencies. Bit Coin reachedahigh value of12,36,165 rupeespercoin in December2017[2]. Each and every crypto currencies are protected with block chain whichcanbesimplifiedasgrowing chain , This block chain is managed by peerto peer network , basedupon block chain crypto jackingtakes place .As mentioned earlier the first digital decentralized currency bit coin was found in the year 2009 and was secured by using SHA 256 but it was not successful .Later in October 2011, Lite coinwas released but it used script as its hash function instead of SHA-256 for security and was successful. Any crypto currency must meet these sixconditions according to Jan Lansky [5] Fig2.0 shows the rise of cryptojacking victims.

a) Ownership and overview of crypto currencies is maintained.

b) If new crypto currencies are created, then their circumstances are also defined.

c) Ownership of crypto currency units can be proved exclusively cryptographically.

d) Transactions are performed in which ownership of the cryptographic units is changed.

e) Only by proving current ownership of these units a transaction statement is issued.

f) Ifdifferent instructions for changing the ownership of the same cryptographic units are simultaneouslyentered , the system performs at most one of them.

Keeping in mind these six conditions thereareprimarilytwomethods tobefollowedtogettothecomputer, oneisto run a code onthehostcomputer and the other is to make the selected content with threat but widely both will beusedto increase the profitoutcome . In this paper a study ofcryptojacking site which generally abusesthe entire computingresourcesof itsusers tominefor crypto currencies[6] and a systematic3 phase analysis is used to identify mining scripts andalsoalarge-scale study is conducted on the prevalence ofcrypto jacking , wewillalsoexamineaboutthemotivationofcriminals thatperpetrate such attack and the key human factors and psychological aspects that help to make cyber criminal ssuccessful. Key areas assessed include social engineering(e.g., phishing, romance scams, cat fishing) ,online harassment (e.g., cyber-bullying ,trolling , revenge porn, hate crimes), identity-related crimes (e.g., identity theft,), hacking (e.g., malware, crypto jacking, account hacking) , anddenial-of-service , As a part of its contribution , the chapter introduces a summarytaxonomyof Cybercrimesagainstindividuals and a case for why they will continue to occur [8].

II. LITERATURE SURVEY

A basic conclusion can be drawn from various study of different crypto jacking methods followed and sites infected, and the following conclusion are interpreted

Manuscript published on 30 September 2019.

***** Correspondence Author (s)

G.PremaArokia Mary, Department of Information Technology, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India. (Email: premaarokiamary.g.it@kct.ac.in)

N.Suganthi, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India.(Email: suganthi.n.it@kct.ac.in)

M.S.Hema, Department of Computer Science and Engineering Aurora's Scientific Technological and Research Academy, Hyderabad, Telangana, India. (Email: ghema_shri@yahoo.co.in)

Retrieval Number: F12910986S319/2019©BEIESP
DOI:10.35940/ijeat.F1291.0986S319
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

- 2outof each 1000websiteshasaweb-basedminerthat is triggered and started at the fraction of second the website is visited, the targeted crypto currencies are byte coin, Monera and many other of similar kinds, but a common web assembly code are used in many website scenarios by the miners that include a coin hive . Fig 1.0 shows the rise of Monera in one year. This clearly states that Web-based crypto jacking is common in this digital world.
- Usually attackers target may be across various websites, but the attacker might use only one kind of API key across many designated websites because of this reason a code may run in parallel website in mining currencies but an average estimate to an attacker is defined to be 23,835.70 rupees per day thereby Mining profits are usually average.
- In popular mining sites like coin hive and crypto loot, the underlying static detection patterns are inefficient against customized, variants of the mining code and hence better web-based mining techniques is required which is clear that Defenses in today's market are in sufficient. This might lead to more effective technologies to rise.

Now we proceed to see about the various methods in which cryptojacking on website is carried out.

2.1. Crypto jacking in Websites based on Online Mining

Digital Currencies, in specific cryptocurrencies uses block chain to provide decentralized control, while the other currencies involves solving puzzles in order to validate transactions, but in case of crypto currencies a specific hardware is used so that it is profitable and in addition to this, memory bound currencies have also enhanced the effectiveness of mining .blockchain is where the records keep growing in size and each block is secured with a cryptographic hash function.[4]

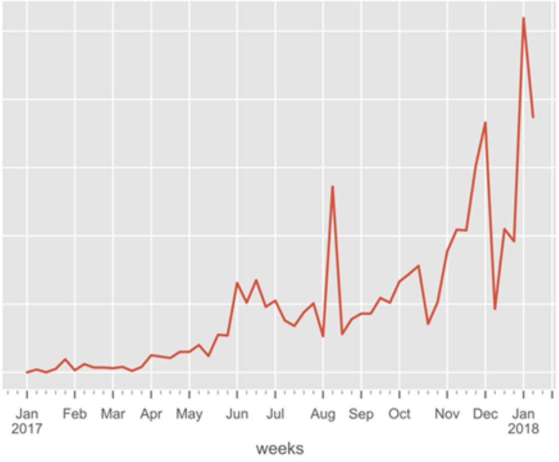


Fig 1.0 Rise of Monera in a period of one year

Traditional crypto currency has always used CPU's computing power for creating various puzzles to be formed, hence the effectiveness of the mining totally depends on how effective the CPU memory is, but this tends to be a great draw back because if the creation of puzzles totally depends on the CPU power then a drastic power degradation is noted. Basic Crypto currencylike bit coin used this method. But instead of this alternative bit coins have been formed where the memory bound function is used to create puzzles and this tends to be comparatively faster because of the usage of multi-level caching to overcome this problem an Alternate to traditional CPU usage memorybound methods where introduced, More than the concept of bit coins, privacy has increased here due to the concept of anonymous transactions. This keeps the sender and receiver hidden in the network, the profitability as well as availability has increased due to this method. Added to this the transactions provides a basis for conducting crypto jacking across manipulated website. [12]

2.2. General working of miners in the website.

The general working of web miners is associated with some key terms which are briefed below

2.2.1.Web sockets

Web sockets are used in many scenarios which includes chat, multiplayer games but in data mining they are helpful in communicate on between miners through a web server and considered to be a weak indicator of web mining.

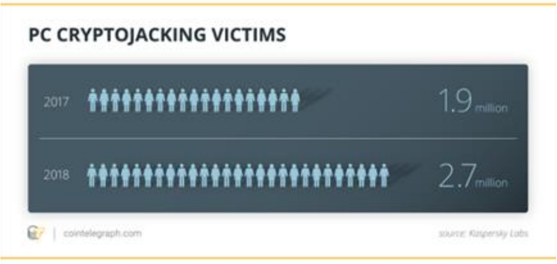


Fig2.0 Statistics of cryptojacking victims

2.2.2.Web workers

Web workers are found in the year 2015 and are found that it is supported by most of the browsers, the support concurrent computations in the background and enables java script to perform multi thread computations. Event driven concurrency, managing the available resources are the other functionalities of the traditional model even though web workers are not necessary to perform web mining, they provide us with better utilization of available resources in the implementations [9]. And thereby we consider that web workers are a productive tool to identify the efficient mining activity.

2.2.3Web assembly

Even though there are communications between the web miners it remains inefficient for realizing its usage, the underlying java codes are complicated as well as expensive for interpretation. Web assembly solves this problem, by executing was code in stack based virtual machine in the browser, and thereby improving the loading time and execution time. Web assembler is supported by common browsers including chrome, safari, Firefox. [14].it holds perfect for performing mining because it allows compiling of cryptographic primitives which includes hash functions from high level to low level programming language.

The basic implemented mining software is coin hive after which several variants similar to coin hive was implemented by using crypto note protocol including JSE coin and Crypto loot. The basic underlying structure of these mining software includes how they share the working of web sockets, web miners and web assembly for effective mining.

Retrieval Number: F12910986S319/2019©BEIESP
DOI:10.35940/ijeat.F1291.0986S319
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The corrupted code is distributed to various website owners and this file is included with a small snippet with further configuration and customization [19]. In some cases, additional indirection is not possible to link miners, on start up the miners instantiates the desired number of web workers and web sockets connecting to the mining pool to create the hash function, in such cases the probability of finding a

miner becomes less but the miner receives a job represented by a blob and a target. The blob is similar to crypto note block and contains the current header. The hash of Merkle tree root allows crypto jacking to securely link the mined block to previous chain. [6]. On seeing the general working of the structure it's important to know about how to identify these miners.

III. METHODOLOGIES USED BY WEB MINERS& RESULTS

3.1.General Approach:

The identification process consist of three different phases which includes

a) Imprecise initial analysis to create a pool of candidates similar to each other or detection of candidate sites

b) Validation of mining scripts ,Arun-time analysis to isolate the real miners within the candidates , and

c) Generalization of miner characteristics , extraction of static indicators, that allow the identification of non-active mining scripts

Phase 1: Under this first phase we will consider different websites to create a mining pool, with host mining scripts .in order to do so compilation of set of hints from potential sites are rendered along with the run time. The various hints are extracted from manual analysis of verified mining scripts. Apart from this suspicious site are marked which uses miner typical web technologies which are not present in general web namely web assembly of web workers[16]. On occurrences of these indicators in site, the sites are marked as potential mining candidates, thus at the end of this process the potential mining websites are marked or identified.

Phase 2: There cannot be a convincing result in the identification of mining scripts and hence validation of mining scripts has to be done. and this is because of multitude of reasons to use web workers, web assembly. However, the constant and potentially unlimited usage of CPU, caused by a single function within parallelized scripts is a unique phenomenon of crypto jacking [3]. Thus, to trace out this pattern we conduct a prolonged run time analysis to crack the pattern of crypto jacking. These sites have some unique characters which include no interaction from other external devices, remains idle after initial rendering. Once the page is loaded all the java scripts are initialized, the CPU usage remains on high level and thereby we conclude that the site host has an active crypto jacking java script.

Phase 3: By using the runtime measurements of the first two phases we will be able to find out the active users with active mining scripts, but by this process we will miss out the inactive members during the test these sites could be inactive due to various reasons which includes, delay in execution of mining scripts and waiting for external events like initial interaction with the web page [10]. To create a solution to this problem we extract java script code from the validating mining sites that is responsible for starting and conducting the mining operation along with parsed web assembly functions, sort them and then use the hash of the third code.as a result we obtain generalized fingerprints and identify the common mining scripts even in inactive state from the following we can identify the total number of sites with web based miners[2].Most of us are unaware of the different internet scams that are prevalent in this modern world each has its own method of implementation and impact on individual.

3.2. Types of cyber crimes

There are different types of Cybercrime or computer related crimes that an individual has to be aware of, while using the online transactions. The damages caused by these crimes can affect different an individual in many different ways directly or indirectly. Sometimes these crimes may also happen across different nations and this is hence called as cyberwarfare where the computers of different nations are participated, it is more like a battlefield with modern communications and technologies [7].

- These crimes can happen having the computer as the target.
- In some cases, Crimes can take place with itself performing the attacks.
- In other cases, it turns out to be a threat against a specific gender, especially female and hurting them emotionally and mentally.
- Sometimes the nation itself is the target for the attackers or it might be even a group of individuals

3.2.1.Internet fraud

In most of the cases under this constrains the victim is made to unwillingly give money on the favor of the terrorists, usually they pretend to be in some NGO or pretend to use the money for a absolute social cause like helping orphan children, or helping people who are diseased. Apart from this there are several other scams which are included under this they are online gift card scams where the attackers run a brute force application in the retailer's computers to make sure the numbers of gift cards that are not been used yet, and these cards are being misused by these attackers [11]. Further the most interesting part in these types of scams is that there are automotive fraudsalso prevailing, in these scams a fake account is created where there is false information of sales of car or any automobile vehicle which catches the eyes of interested clients, then a demand of advance is claimed as the client is interested money is rendered into the attacker's hands [20]. Internet tickets are also a trending online fraud where false tickets are sold online for a particular concert and the customers are being cheated, in 2008 Olympics such a fraud has been done where false tickets are sold from a genuine website leading to huge capital loss.Scams also involve typical financial gain as the prime motive. Once the criminals purchased pop-up browser advertisements which appeared on victims computer screens and locked their browsers [18].

Reports indicate that over 40,000 people across the globe were victimized and defrauded out of more than$25 million USD [18]. They were using tactics to deceive individuals, many of whom were elderly and potentially more vulnerable.

3.2.2. Drug Trafficking

This has become the most common in today's internet world, this kind of cybercrime is where the illegal drugs are being transacted in dark web using an open source software named tor or invisible internet project. Both are anonyms network where the transactions are hidden.in 2011 a online official dark web marker names SILK WORM was released where illegal purchase of drugs where monitored. Tons of drugs were also seized from various middle east countries and its statistics are denoted in fig 3.0 for further references [15].

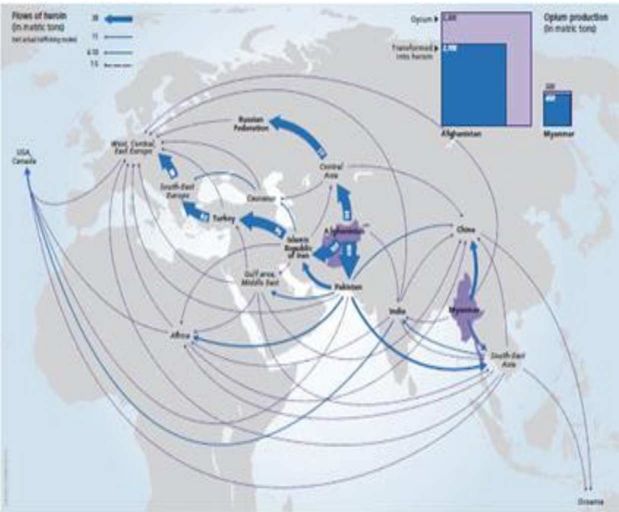


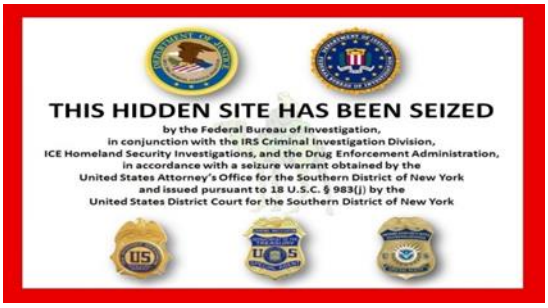
Fig 3.0 spread of drugs in silk worm website

the web page silk worm was officially shutdown by law enforcement fig 4.0 but it was again launched as silk worm 3 reloaded. Fig 4.0 shows the official notice of the shutdown of the websites.

3.2.3. Child abuse

Child abuse otherwise called as cyber molestation or child abuse is the other most important cybercrime prevailing in today's media, here the children are subjected to various threats physically and mentally it includes child prostitution and child pornography ,further children are agitated towards sex through child grooming where emotional attachment towards the children are gained by the attackers. These attacks can be possible through internet or cellphones. This can be further extended as cyber bullying where the children are subjected to bullying which develop a negative feeling within themselves which leads to suicidal thoughts [12].

Various laws are being implemented to prevent these types of crimes and bullying, it is been noted that these groomers who try to gain access to the children physically are not from outside but from their own family or friends.



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Fig 4.0 A notice issued by the government officials for website being seized

3.2.4. Crimes using computer against individuals

The target of the attacker might be against a particular individual specifically this might include the mental damage which is caused to the individual for which legal actions cannot be filed against, the individual may get emotionally devastated in such cases [13]. The major advantage in these scams are that they do not require any specific technical expertise. This type of scams may include a variety of techniques which includes phishing, identity theft, hacking, ransomware, malware attacks, online frauds, identity threats. Each one is entirely different from one another but their motive remains the same throughout.fig5.0 shows the different types of crimes [14]. These crimes where prevalent before the existence of computers but now the attackers are more equipped with modern technologies.

3.2.5.Crimes against a group

This is where the entire group is subjected to attacks. They require high computer skills to manage

the entire scam these include different types of scams such as denial of service, computer viruses, malwares which are incorporated in the targeted computers to gain particular access or financial gains.

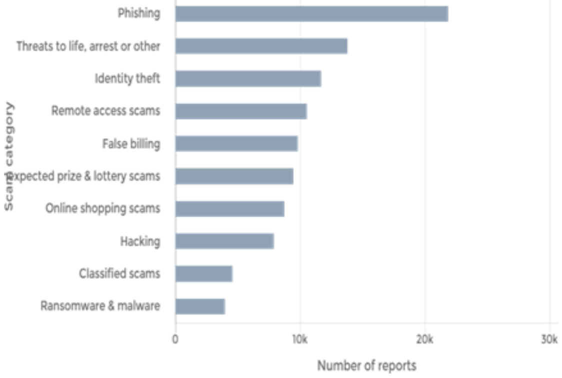


Fig. 5.0 Statistics of various types of cybercrimes.

3.2.6. SQL injections

Codes are injected into the entry field, this code is generally infected and it exploits vulnerability of the application software, it can gain access of the data and spoof identity temper with existing data. It was found in 1998 and it leads to unauthorized viewing of user's data. Tables and documents, in order to reduce this type of attack input validation is mandatory along with installation of updated firewall [13].

3.2.7 Domain hi-jacking

This includes hacking of the domain name itself without the permission of its original registered owner. Usually such domain names are used for illegal access or used in dark web which leads to financial loss for the actual domain holder. Enabling two factor authentications can be considered to reduce its prevalence but only to a certain extent. Records show us that this scam where dominant during the speculation of online asserts [17].

IV. CONCLUSION

The prevalence of technology is a greatest asset to this generation, but it also leads us to various troubles. The impact these scams which are prevalent has on an individual are short term and, in some cases, they tend to be long term. The damage caused to the individual can be physical in some case while the others are emotional and mental too. In order to use the internet safe to its fullest potential it's important that we are aware of the various frauds that are prevalent in the society and various means for an individual to overcome the same.

REFERENCES

1. https://www.sec.cs.tu-bs.de/pubs/2018-cryptojacking.pdf
2. https://www.researchgate.net/publication/323654794_A_First_Look_at_Browser-Based_Cryptojacking.
3. https://www.researchgate.net/publication/328762019_Cybercrime_and_You_How_Criminals_Attack_and_the_Human_Factors_That_They_Seek_to_Exploit
4. Lansky, Jan "Possible State Approaches to Crypto currencies". Journal of Systems Integration. 9/1: 19-31. doi:10.20470/jsi.v9i1.335.
5. CoinMarketCap. CoinMarketCap - Market Capitalization of Crypto currencies. Website https://coinmarketcap.com/currencies/, May 2018.
6. N. van Saberhagen. Cryptonote v2.0. Technical report, CryptoNote, Oct. 2013
7. Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. Available from: https://www.researchgate.net/publication/328762019_Cybercrime_and_You_How_Criminals_Attack_and_the_Human_Factors_That_They_Seek_to_Exploit [accessed Dec 16 2018].
8. Whitty, M.T., Buchanan, T., "The online dating romance scam: The psychological impact on victims both financial and non-financial. Criminology & Criminal Justice ",16(2), 176-194 (2016)
9. Shachaf, P., Hara, N.: "Beyond vandalism: Wikipedia trolls" Journal of Information Science 36(3),357-370 (2010)
10. Button, M., Nicholls, C.M., Kerr, J., Owen, R., "Online frauds:" Learning from victims why they fallfor these scams", Australian & New Zealand journal of criminology 47(3), 391-408 (2014)
11. Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. Available from: https://www.researchgate.net/publication/328762019_Cybercrime_and_You_How_Criminals_Attack_and_the_Human_Factors_That_They_Seek_to_Exploit [accessed Dec 16 2018].
12. The Mirror: Sextortion scam: What to do if you get the latest phishing spam demanding bitcoin. http://www.mirror.co.uk /news/uk-news/revenge-porn-ruined-life-woman-4113969 (2014)
13. Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. Available from: https://www.researchgate.net/publication/328762019_Cybercrime_and_You_How_Criminals_Attack_and_the_Human_Factors_That_They_Seek_to_Exploit [accessed Dec 16 2018].
14. Slonje, R., Smith, P.K.: "Cyberbullying: Another main type of bullying", Scandinavian journal of psychology 49(2), 147-154 (2008)
15. Forbes:Thetopcybersecurityrisksinasia-pacificin2017. https://www.forbes.com/sites/riskmap/2017/01/11/the-top-cyber-security-risks-in-asia-pacific-in-2017/ (2017
16. Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. Available from: https://www.researchgate.net/publication/328762019_Cybercrime_and_You_How_Criminals_Attack_and_the_Human_Factors_That_They_Seek_to_Exploit [accessed Dec 16 2018].
17. BBC News: Identity fraud reached record levels in 2016. http://www.bbc.co.uk/news/uk-39268542
18. BBCNews:Webhost123-regdeletessitesinclean-uperror.http://www.bbc.co.uk/news/technology-36072240 (2016)
19. McDevitt, J., Levin, J., Bennett, S.: "Hate crime offenders: An expanded typology",Journal of SocialIssues 58(2), 303-317 (2002)
20. Mehrnezhad, M., Toreini, E., Shahandashti, S.F., Hao, F.: "Stealing pins via mobile sensors: actualrisk versus user perception". International Journal of Information Security 17(3), 291-313 (2017.