IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.2, Jan 2019 E-ISSN: 2347-2693

Impact of Crypto-Mining Malware on System Resource Utilization

K.Berlin[1*], S.S. Dhenakaran[2]

[1]Ph.D Research Scholar, Department of Computer Science, Alagappa University, Karaikui, India
[2]Department of Computer Science, Alagappa University, Karaikui, India

[*]*Corresponding Author: berlinjenson@gmail.com*

Available online at: www.ijcseonline.org

***Abstract*—** Nowadays, the whole world works in modern technology. Peoples are paying more attention to complete the process in a sophisticated way without putting the much human effort. End-user thinks that only poor knowledge about application usage leads to data security issues. But application providing companies camouflage the truth behind the name of the user sophistication. Even a small piece of a script code can make the huge data security issues. That type of problems is called cryptocurrency malware. Cryptomining malware is nothing but software code and designed to take system resources without the knowledge of authorized end users. The role of cryptomining is stealing computer's resources with the help of auto inject of malware code in a crook way while making online communications on websites. A website owner uses these malware codes to take visitor's system utilization to gain more earning. Cryptomining malware easily injects electronic devices like computers, smart phones to increase earnings from cryptocurrency mining.

***Keywords*—**Component, Formatting, Style, Styling, Insert (key words)

I. INTRODUCTION

The count of cyber criminals increased more day by day due to the lack of security while making online transactions. In the present scenario trendy hacking method is crypto-currency mining. Crypto currency malware is also known as crypto mining malware or crypto jacking. Crypto currency malware is a simple software code bound with websites when the users have click on the website it automatically injects with their systems and takes the CPU power and system resources etc. Kaspersky cyber security lab report said cyber criminals earn $ 30,000 of every month using crypto mining malware. To collect the crypto-currency crypto miming malware takes the victim's system power secretly.

The small piece of malicious crypto mining code can run on the visitor's devices. Recently some crypto mining malware plays a very big role in very popular. In browser based crypto mining malicious code directly injected on the browser without any installation. Dubbed loapi is one of the powerful crypto mining malware and is designed to target the processor of smart phone devices and damage physical parts also. This crypto mining code has reduced the activity of the victim's processor and causes the physical damage on battery. Finally, it may destroy the devices. Top most wanted malware are: coinhive, rigek, cryptoloot, roughted, fireball, globeimposter, ramnit, virut, conficker, rocks etc. In second section these malware categories has explained in detail.

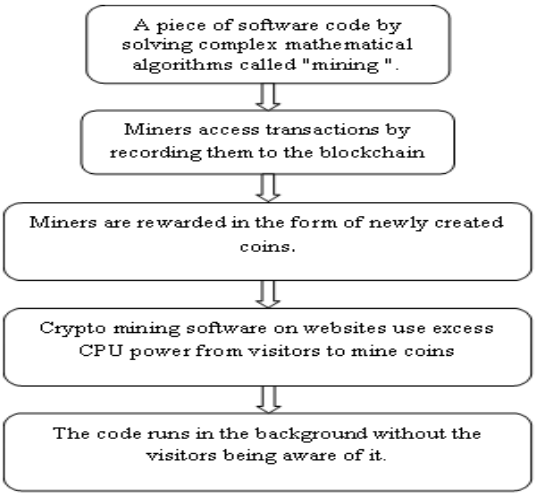

Figure 1. The process of Crypto Mining Malware

II. MALICIOUS CRYPTO MINING MALWARE

Activities and causes of crypto mining malware have explained in above section. The detailed explanation of each malware is defined here.

A. Coinhive

Coinhive malware is the alternate way of gaining revenue from webmasters for crypto currency mining. It is the most popular malware of online hacking today. Coinhive malware

inject java script mining code on the user visiting website to steal the device's CPU utilization. After infected of coinhive malware the general symptoms increase the graphics card usage and CPU utilization, 50 percent of the CPU power accessed by the web browser, slowly minimize and maximization of windows, program runs in slowly, system slowness when using web browser[1]. Globally 23 percent of organizations are affected by coinhive crypto mining malware.

Preventing from coinhive crypto mining malware need to follow the below process which are monitoring file integrity regularly, access online file from trusted sources only, creation of security policy[2], update system regularly, install updated security antivirus.

Table 1. Analysis of Coinhive malware

Name of the malware	Company of hacked websites	Embedded via	Affected countries
Coinhive	The Los Angeles Times, Blackberry, Politifact, Showtime, UK, US, Canadian government websites.	WiFi Hotspot, YouTube advertisements.	Japan, France, Taiwan, Italy, Spain.

B. RIG EK

Rig ek is the most powerfull exploit kit is used to install Trojans and ransomware. After 2017 rig ek has been changed its process into crypto mining to gain profit of crypto miners. From the recent news, RIG EK was observed in a Trojan called Grobios. Rig EK used in Ramnit, it collects important credentials from the visitor's systems. Rig EK used domain shadow often it avoids the detection. Rig EK supports the following malware are, locky ransomware, CrutoMix, Ramnit banking Trojan, CryptoShield,Cerber, Spora, Remcos, Bunitu Trojan, WannaCry, CryptWall, CTB-Locker, PayCrypt, VirLock. The research record of Trustwave SpiderLabs said that, the infection rate of per day is 27,000 machines and totally observed 1.3 million infections around the world wide[3]. Users should follow three things to protect systems from Rig EK which are, patch management, train to users to observe infected websites, add extra layer to the antivirus to increase the endpoint security.

Table 2. Analysis of Rig EK

Rig EK supported Malware	Impact of Malware	Types of Attack
Cerber	Loss of Information	Ransomware
Spora		
CryptoMix	Loss of CPU Resources	Open Proxy
CryptoShield		
Remcos	Possible legal issues	Remote Access Control
Bunitu Trojan		
Locky Ransomware	Data Loss	Crypto-currency mining
Ramnit Banking Trojan		

C. CryptoLoot

Cryptoloot malware is a small piece of java script software code to mine for crypto currency. The main goal of this malware is processing for crypto currency with the use of CPU and GPU power. Once the infected website has opened automatically the malware scripts run and executing in the background process. For the longer period of time malware remains on your computer it may cause or fire the entire system. The infection of crypto loot may come from the following executable files which are patches, license activators for software, game cracks. A crypto criminal infects the victim's system through .zip and .rar files. They fool users as the name of trusted documents like, invoice of products, banking statements, purchase receipts etc. such a way crypto loot malware abuse 100 percent of system resources without the user's knowledge.

Table 3. Analysis of CryptoLoot malware

Malware name	Inject via	Symptoms	Obtained digital currency
CryptoLoot	Spam E-mails, Executable Files	Crashes, Excessive CPU Consumption, unresponsiveness .	Monero

D. Fireball

Fireball malware has designed to hack browsers and target to change search engines. The exact work of fireball is run any code on victim's systems remotely. Fireball can steal secret credentials and hack social communications via dropping of other malware. Fireball drops botnet and ransomware malware on the endpoints and takes down the web servers. It infected 250 million computers over the worldwide. Fireball is also called as browser hijacker, mostly it spread through bundling. The infected countries are Brazil, India, Mexico, Indonesia, and United states. Twenty percent of corporate networks are affected from United states, China, India, Indonesia, Brazil.

Table 4. Analysis of Fireball Malware

Name of Malware	Infected countries	Percentage of Infected systems [4]	Percentage of affected corporate networks
Fireball	India	10.1	43
	United States	2.2	10.7
	Brazil	9.6	38
	Indonesia	5.2	60

E. Loapi Malware

Loapi is one of the android crypto mining malware designed to take over the computing power of the infected device to mine Monero. Loapi is not present on the Play store and there is no evidence of its presence anymore. Loapi malware

once installed, it gets full access of device administrator. Loapi once enters into the devices does two important things that are hides the app shortcut and shows it as a trusted application. If loapi gets the access of administrator it connects with multiple servers and download malicious modules and execute it. This malicious files have shown like .so and .dll extensions. The main functionality of the Loapi malware is self preservation, which means preserve itself when users try to uninstall it.

Loapi android malware can inject into mobiles through the following links like opening URL, creating shortcuts on the device, displaying video advertisements, downloading and installing applications.

Table 5. Analysis of Loapi Malware

Name of Malware	Inject via	Impact of malware	Obtained Currency
Loapi	Advertisements, SMS, Opening pages of social networks includes Facebook, Instagram, VK	Demanding admin with endless pop ups, contiously perform malicious activities untail device fails, device battery gets hign internal heat, gets device break down, lock the screen and close the device manager.	Monero

III. STATISTICAL ANALYSIS

A. *Coinhive versus CryptoLoot*

Both coinhive and cryptoLoot are web based malware and kind of cryptojacking to mine cryptocurrency to the website owners in the form Monero digital currency. In the sense of browser cryptomining is entirely based on the vsitor's system resources. Attackers uses piece of java script code and inject into website without knowing of end users. the table clearly shown the comparative analysis of both Coinhive and CryptoLoot.

Table 6. Comparative analysis of Coinhive and cryptoLoot

Comparative Parameters	Coinhive	CryptoLoot
Infected websites	6,303	225
Revenue of attackers	30 %	12 %
Revenue of website owners	70 %	88 %
Category Position	#1	#11
Market Share	49.08 %	1.75 %

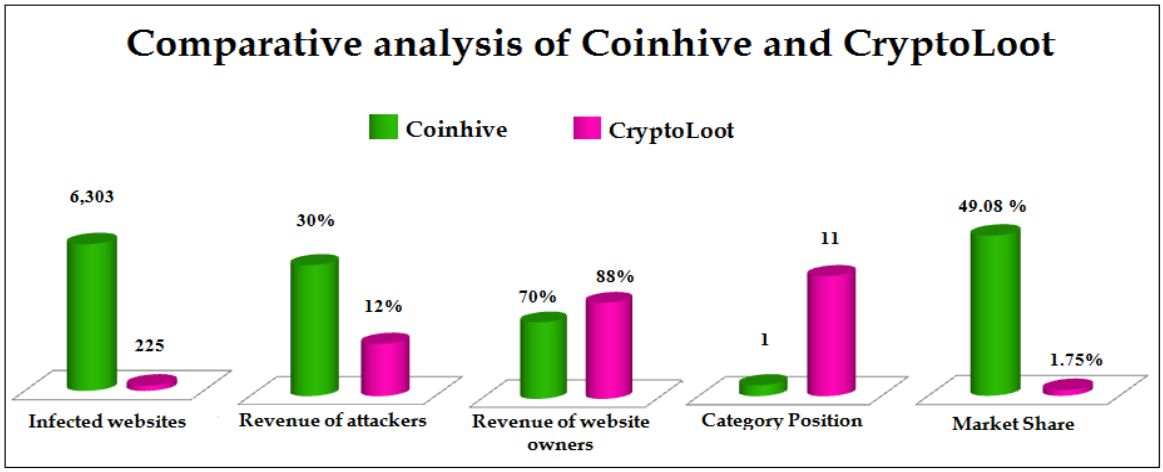

Figure 2. Comparative analysis of Coinhive and cryptoLoot

B. *Compare of Coinhive with other malware*

The recent news of Troy Mursch[5] from bad packets report said nearly 50,000 websites are infected by the crypto currency mining malware. 4,200 websites are affected by coinhive malware, some of them are listed here. Cuny.edu from New York city University, uscourts.gov from court information portal, lu.se from Lund University, slc.co.uk from UK's students loan company[6] ect. Infected websites by various crypto mining malware is shown below as a graphical representation.

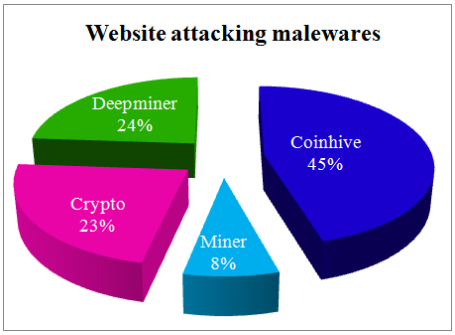

Figure 3. Coinhive compared with other malware in the sense of infected websites.

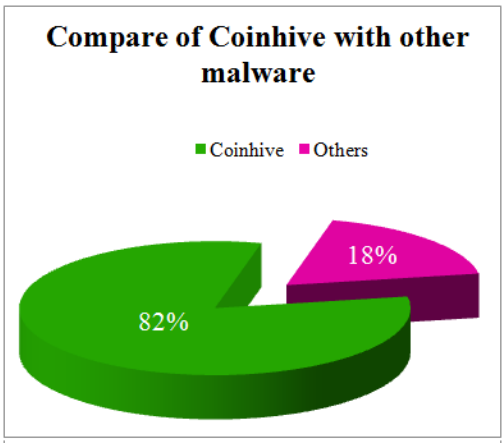

Figure 4.Compare of Coinhive with other malware

IV. CONCLUSION

Nowadays our living sense entirely based on the digital world, for every moves/transactions people are wants to be live with internet and system requirements. When they are working with internet it's not safe as 100 percent. This paper fully concentrates on the crypto currency mining or crypto mining malware spread out of internet. Globally it is a very big business for every website owners with the help of crypto mining attackers. Once malware has installed, it fries the whole system. So people should aware of crypto mining malware while accessing the internet. Careless in behavior and lack of system knowledge is the only reason for system infections. Mostly malware installation has done through the fake e-mails and SMS. So before click on e-mail attachments think out of whether the source came from a trusted one or not. Because browser or websites not having the capability of malware detection. Through this paper, we recommend that users should uninstall the unknown applications regularly and download needed applications from trusted sources.

REFERENCES

[1] https://malwaretips.com/blogs/remove-coinhive-miner-virus
[2] https://www.getastra.com/blog/911/remove-crypto-mining-malware-cms-wordpress-magento-drupal/
[3] https://www.cyber.nj.gov/threat-profiles/exploit-kit-variants/rig
[4] https://en.wikipedia.org/wiki/Fireball_(software)
[5] https://ethereumworldnews.com/researcher-finds-nearly-50000-websites-running-cryptocurrency-mining-malware
[6] https://www.theregister.co.uk/2018/02/11/browsealoud_compromised_coinhive

Authors Profile

K. Berlin, received her M.Phil degree in Alagappa University, Tamil Nadu. Now she is pursuing her Ph.D (Computer Science) research in the same university. The field of her research is data security in cryptography. Four Research papers are published in Journals and Conferences.

S.S.Dhenakaran, a faculty member is working in the Department of Computer Science, Alagappa University, Tamil Nadu, India. He has acquired a doctoral degree in Computer Science and Engineering during 2008. Completed post graduation in mathematics during 1984, PG degree in computing during 2003. To his credit, he has more than 95 articles in international journal and conference. His field of research is Data Security using Cryptography. His familiar research fields are Optimization Techniques, Algorithms and Data mining.

