Coinhive's Monero Drive-by Crypto-jacking

Azizah Binti Abdul Aziz[1], Syahrulanuar Bin Ngah[2], Yau Ti Dun[3], Tan Fui Bee[4]

[1,2]Systems Network & Security (SYSnet), Faculty of Computing, Universiti Malaysia of Pahang, 26300, Gambang, Kuantan Pahang, Malaysia

[3,4]SyaArmy R&D Team, SysArmy Sdn Bhd, Wisma Zelan, No., 12,, 1, Jalan Tasik Permaisuri 2, Bandar Tun Razak, 56000 Kuala Lumpur, Malaysia

E-mail: azizah.official@gmail.com, syahrulanuar@ump.edu.my

Abstract. This paper provides study of behaviour on a drive-by crypto-jacking, specifically Coinhive's Monero. Crypto-jacking is a form of cyber threat where a host machine's processing power hijacked thru infected website to solve cryptographic puzzles as an unwitting participant. The sample study share host machine and network behaviours when host visited websites that have been embedded with Coinhive's Monero related script. These data collection of behaviour can be utilize to identify and detect Coinhive's Monero mining activities in networks.

Keywords: Coinhive's Monero, cryto-jacking, drive-by

1. Introduction

Cryptocurrency is digital currency that uses cryptography for security purpose, hence the term 'Crypto' in cryptocurrency. The first idea of cryptocurrency was circulated in the internet from a write up by Satoshi Nakamoto, an anonymous author of paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" that proposed a system for electronic transactions that would use individual host machine's resources to perform work that creates a "coin" and verifies the transfer of ownership of these virtual coins without being controlled by regulatory [1] One of common currency used are Monero (XMR) and Bitcoin (BTC).

Crypto mining in other hand refer to act of utilizing host machine's processing power to solve cryptographic puzzle, validate transactions and generate profit. As the value of cryptocurrency increases exponentially, the need of mining them also increases. Figure 1 shows the increases value and volume of cryptocurrency over the years [2]. Thus, cybercriminals resorted to illegal act of crypto-jacking to acquire more profit from crypto mining. Crypto-jacking is define as form of cyber threat where a host machine's processing power is hijacked to mine cryptocurrency as an unwitting participant [3].

These illegal activities may cause harm to organization's network as mining activities always resulted in workstation become slow or freeze that will hinder normal business activities, consuming power that will resulted in money loss and can also be used as "door" for something more malicious that may lead to data loss and cyber-attack. Online services have always been a target of internet attackers with new sophisticated tactics [4]

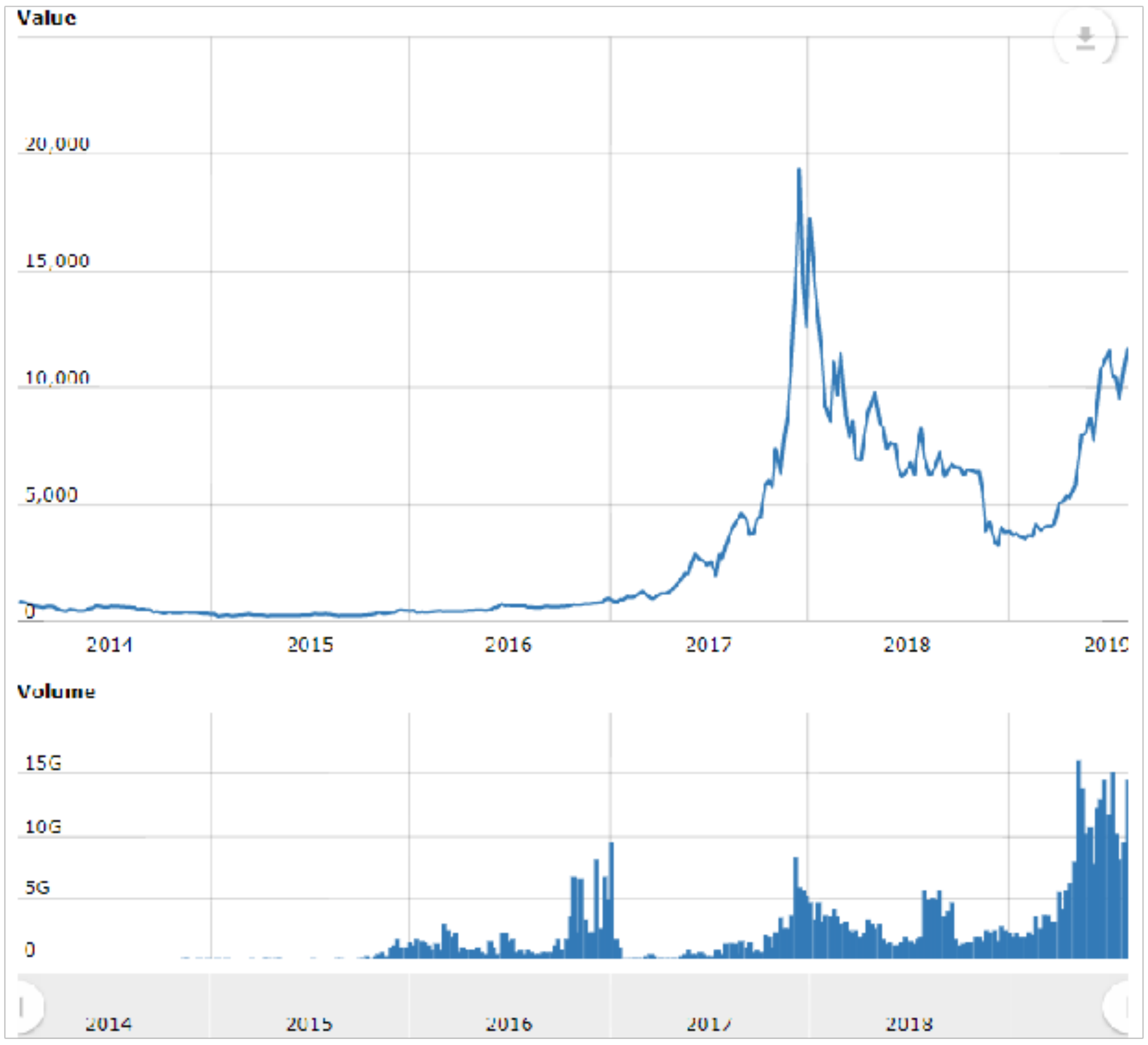

Figure 1. Crytocurrency value and volume over the years

2. Coinhive's Monero

Monero is one of the cryptocurrencies used worldwide besides Bitcoin. Due to its high level of privacy where its transactions are virtually untraceable by outsider, Monero have been one of choices for cybercriminal to do transaction.

One of the cryptocurrency mining services that mines for Monero is Coinhive. Coinhive provide its users with JavaScript that can be embedded in webs sites. The purposes of this JavaScript are to do mining by using websites' visitors' resources. This will eventually lock up visitors' browser and drains the device's battery.

Based on report produced by security firm, Malwarebytes [3], their telemetry identified usage of silent Coinhive JavaScript of 3M/day during the period of January 10 to February 6, 2018. Silent version of Coinhive refer to JavaScript version that enable script owner to utilise visitor host machine resources to do mining without their consent.

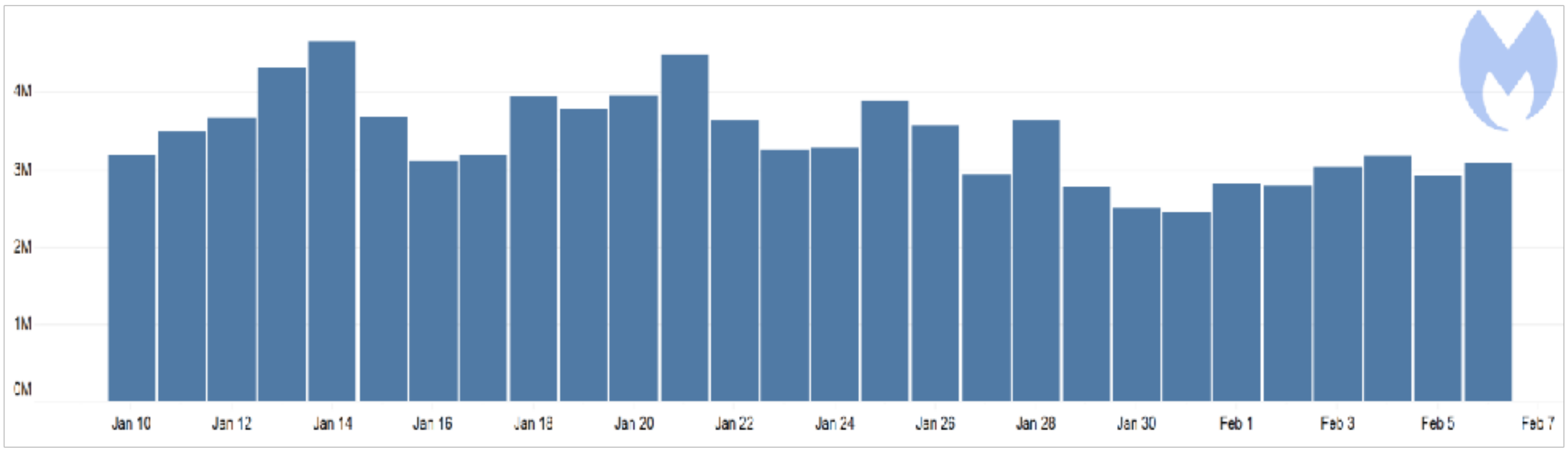

Figure 2. Usage statistics for the silent version of Coinhive

Researcher at Krebs On Security considered Coinhive as the top malicious threat to web users as they found nearly 32,000 websites running Coinhive's JavaScript miner code as for March 2018 [5].

3. Crypto-jacking thru drive-by compromise

'Drive-by compromise' refer to exploit technique to gain access of a system and its resources when user visited compromised websites while browsing. Cybercriminals embedded malicious code modules in websites and it will be deployed in user's browser when they visit the compromised website. This method often leaves no traces of malicious files (file-less), thus making it difficult to be detected by end point protection (EPP) such as antivirus [6]. This method often observed been leveraged by cybercriminals to launch crypto mining modules on users' machines to hijacked its resources. Figure 3 shows typical anatomy of drive-by compromise.

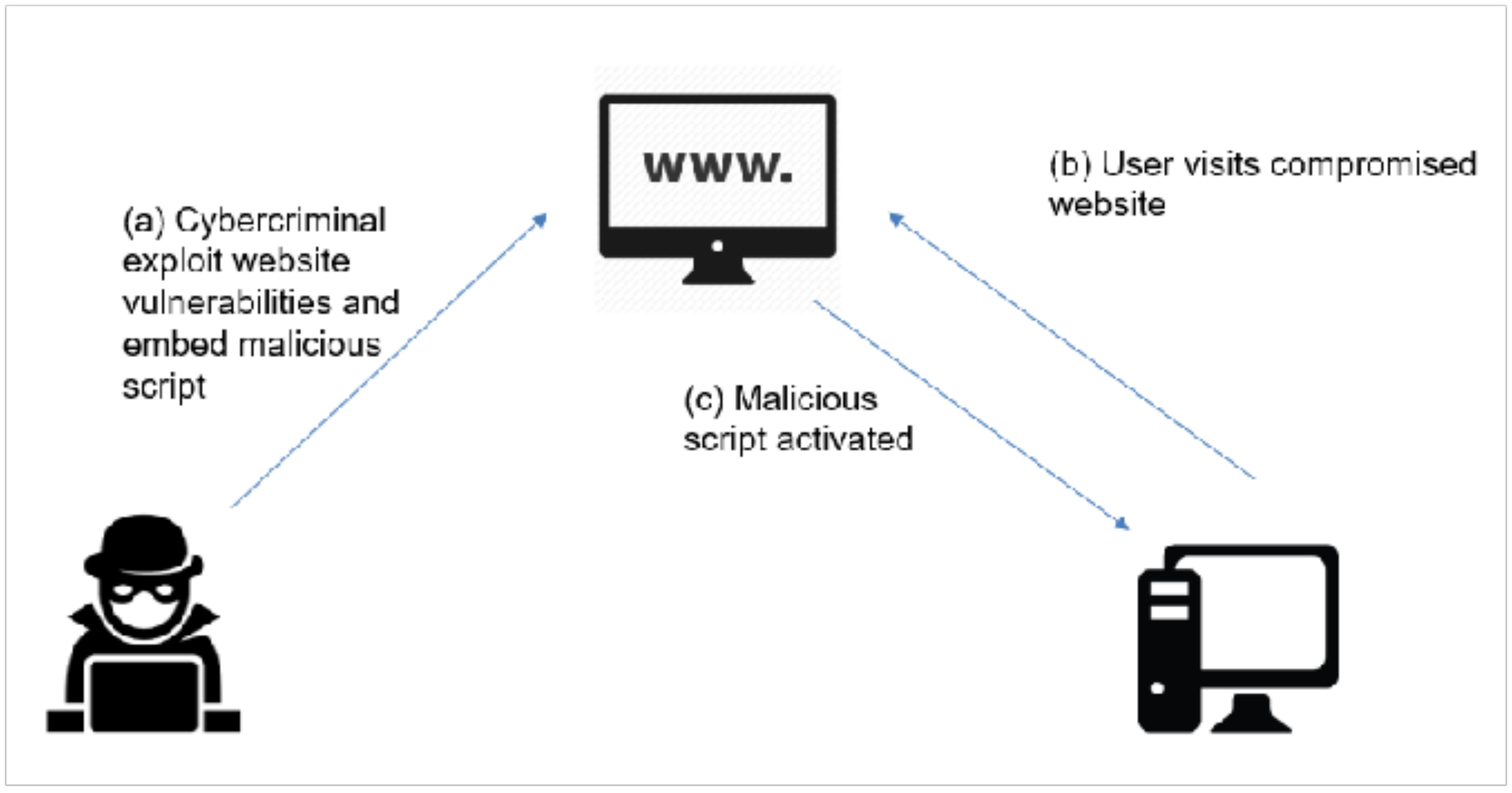
www.
(a) Cybercriminal exploit website vulnerabilities and embed malicious script
(b) User visits compromised website
(c) Malicious script activated

Figure 3. Typical anatomy of drive-by compromise

Even though file-based detection is near impossible for drive-by crypto-jacking, there are alternative detection method that are more feasible to identify and detect drive-by crypto-jacking which is behavior-based detection.

4. Research Methodology

Detecting mining activities similar to this is becoming a challenging task due to increasing connectivity of systems that gives greater access to the internet and makes it easier for cyber criminals to do illegal activity that gives benefit to them.

Thus, to overcome this problem, analysing mining behaviour will help to established the pattern of behaviour where it then can be utilized to detect mining activities in a network.

In this study, several work stages have been identified for the methodology for the research. Initially, an investigation on the cryptomining activities and how it contributes to cyber risk are done.

a) Stage 1: Preliminary study. This initial study will start by reviewing on how Coinhive's Monero works and collecting sample of infected website.
b) Stage 2: Design controlled environment. In this stage, designs of controlled environment architecture and applications are done that are appropriate for mining behaviour analysis environment.
c) Stage 3: Testing the samples. This stage involves with visiting the suspected websites and collects relevant data.
d) Stage 4: Analysing data collected. At this stage, all data collected is analysed and grouped into appropriate group based on the findings.

5. Sample case Coinhive's Monero mining behaviour

In order to identify behavior pattern of crypto-jacking via Coinhive, we leverage 53 public websites that have been reported as source of Coinhive' Monero distribution for our sample case. These websites all have "coinhive" string in their source page. Traffic and host machine behavior are observed starting from the before, during and after user visited the website.

In this sample case, for host machine, Windows 10 with Chrome Ver. 68.0.3440 are used as browser to surf the websites and Intel ® Core ™ i7-5500u CPU, 2.40GHz is used as CPU. Different browser application and CPU may have different result. Whereas, Juniper Firewall SRX and Cisco ASA firewall are used to monitor the traffics.

5.1. Host level

Immediately when host visit the infected websites, we observed sudden increment of CPU and memory usage for browser application. With average increment of CPU up to 99.4% and memory utilization of 532.7 MB. Figure 4 shows differences of CPU utilization before and during host visited websites with Coinhive's Monero, whereas Figure 5 shows differences of memory before and during host visited the websites.

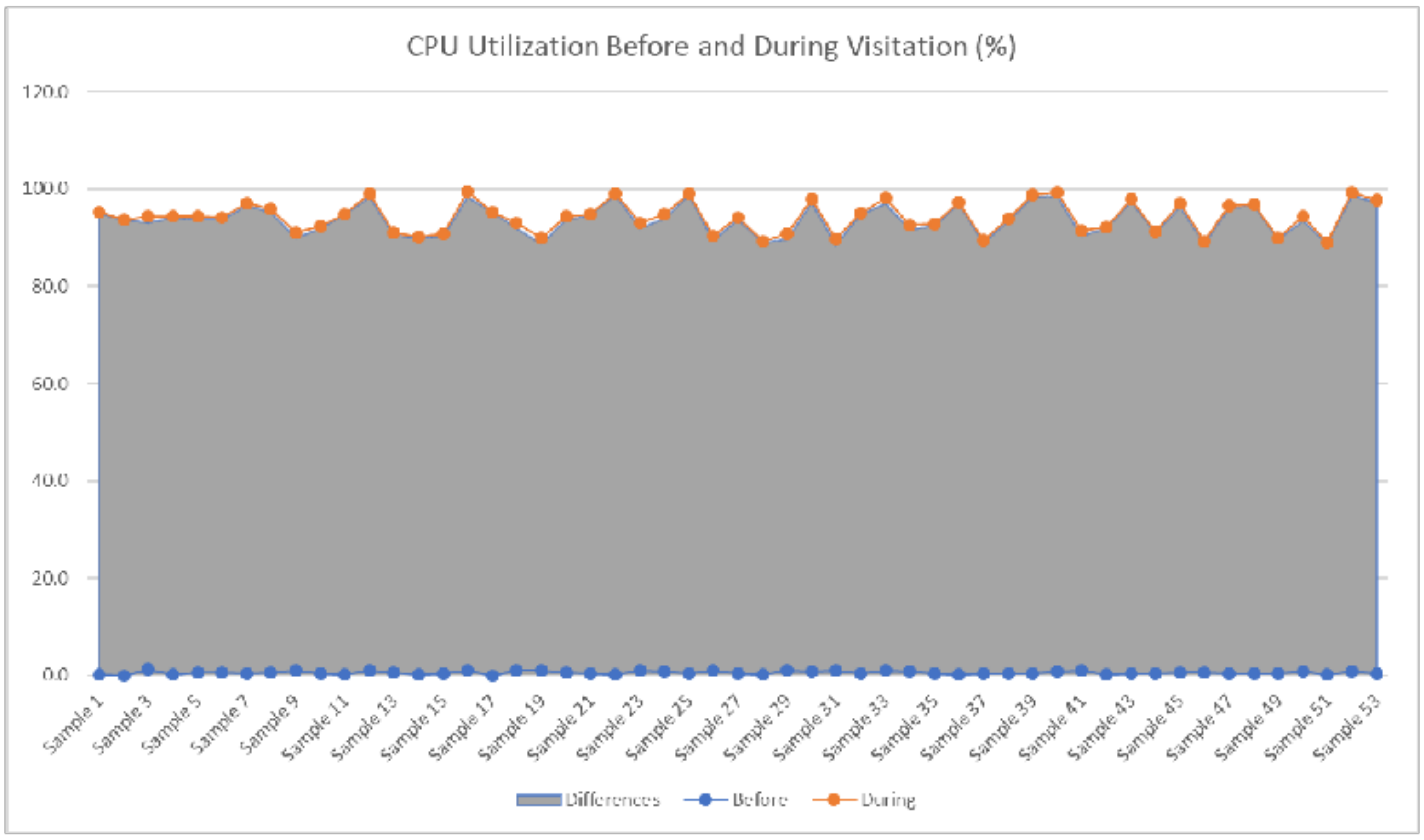

Figure 4. CPU utilization before and during host visiting the websites.

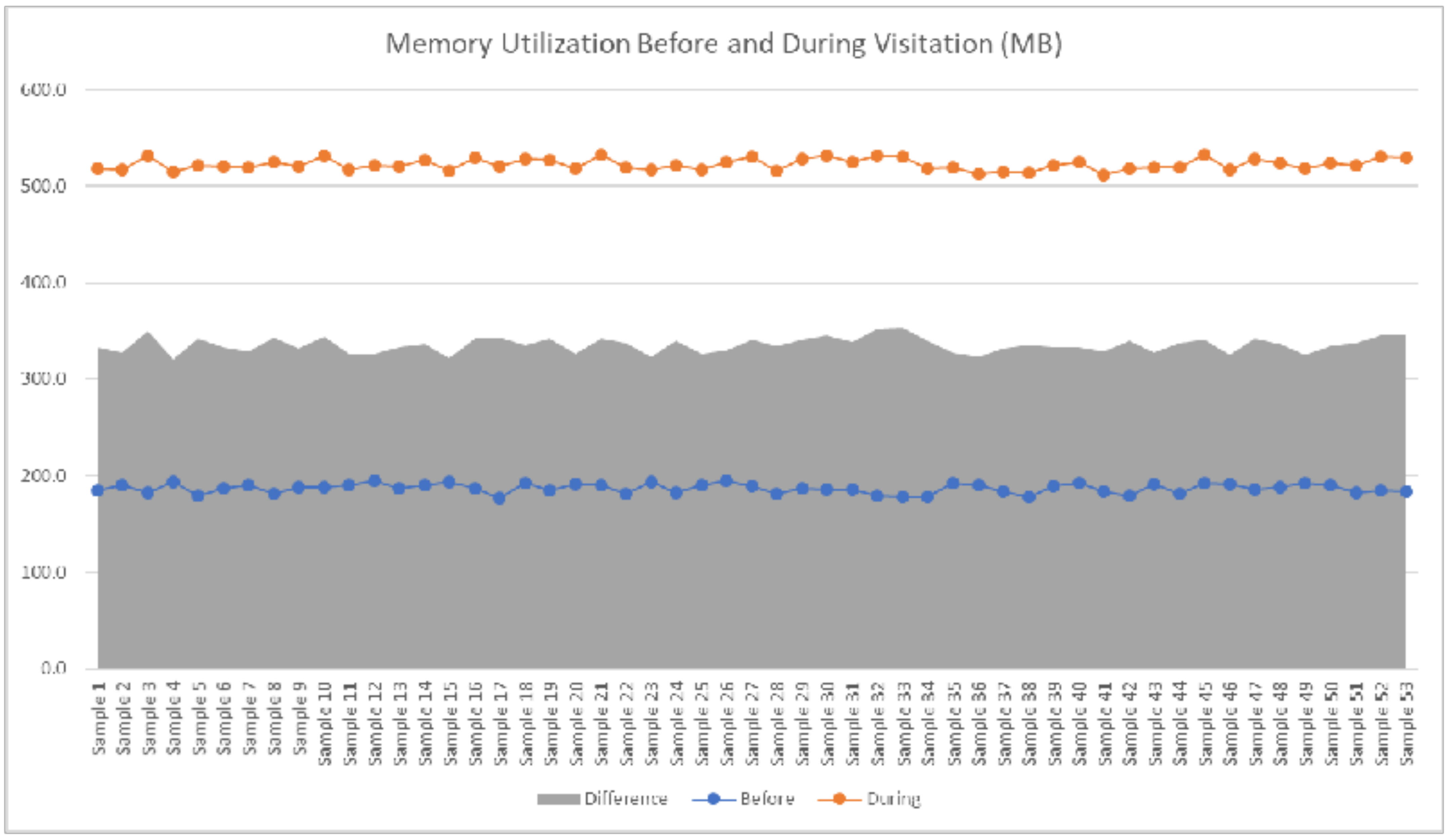

Figure 5. Memory utilization before and during host visiting the websites

75.47% of the sample case shows high utilization of CPU and memory continues even after the browser windows that used to visit the websites closed. We found that this is due to hidden browser windows that have been initiated during the infection phase under the taskbar. The hidden window's coordinates vary based on each user's screen resolution. Figure 6 shows sample of hidden browser as observed.

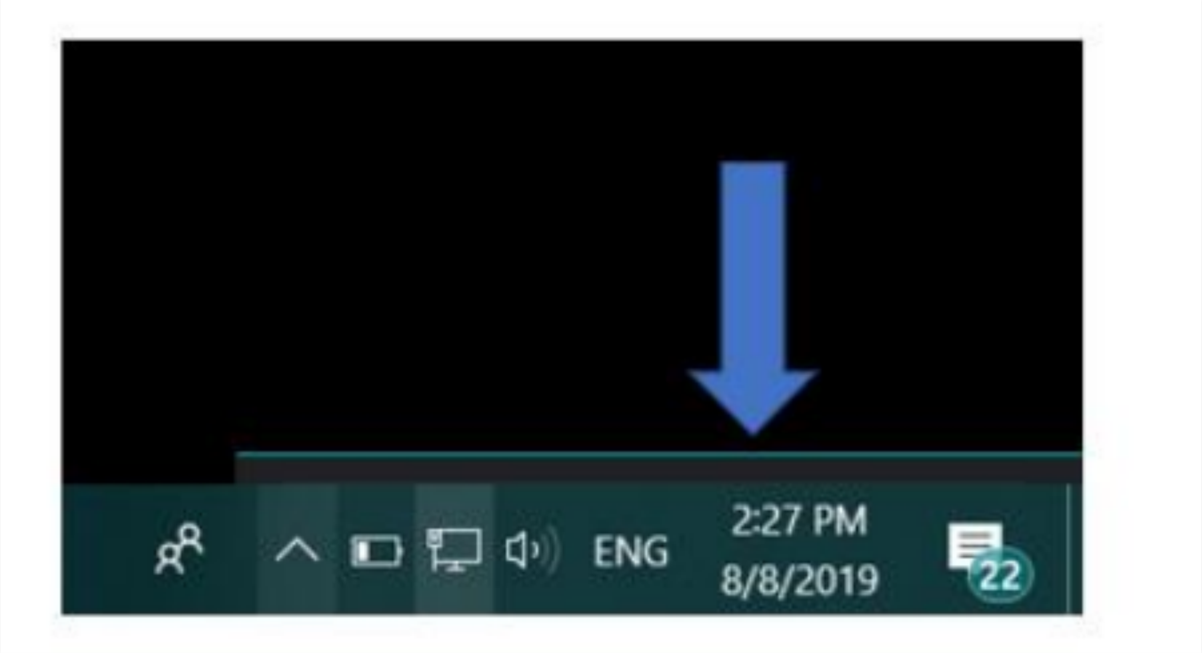

Figure 6. Hidden browser as launched during mining activities.

Figure 7 shows percentage breakdown where mining activities continues even after the main browser closed.

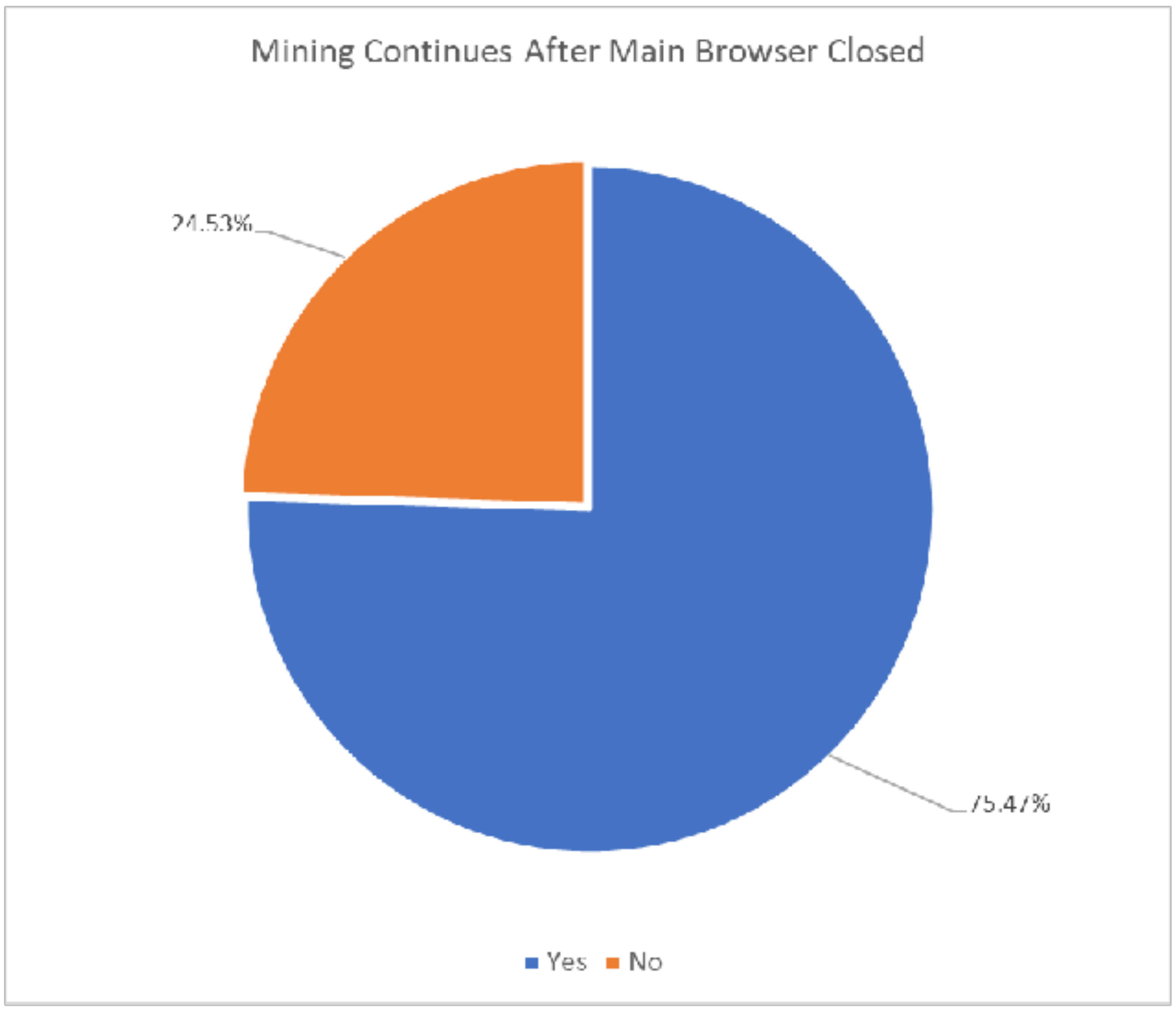

Figure 7. Percentage breakdown for host that continue mining activities even after the main browser have been closed.

5.2. Network level
In controlled environment, as host visited the infected websites, we are able to observe two (2) group of behaviour, where we labelled as Group A and Group B. For Group A, we observe multiple persistent outbound traffic toward the infected websites. This match with typical cryptocurrency mining activities. Host visited the websites, JavaScript on the websites triggered and mining started. Refer Figure 8.

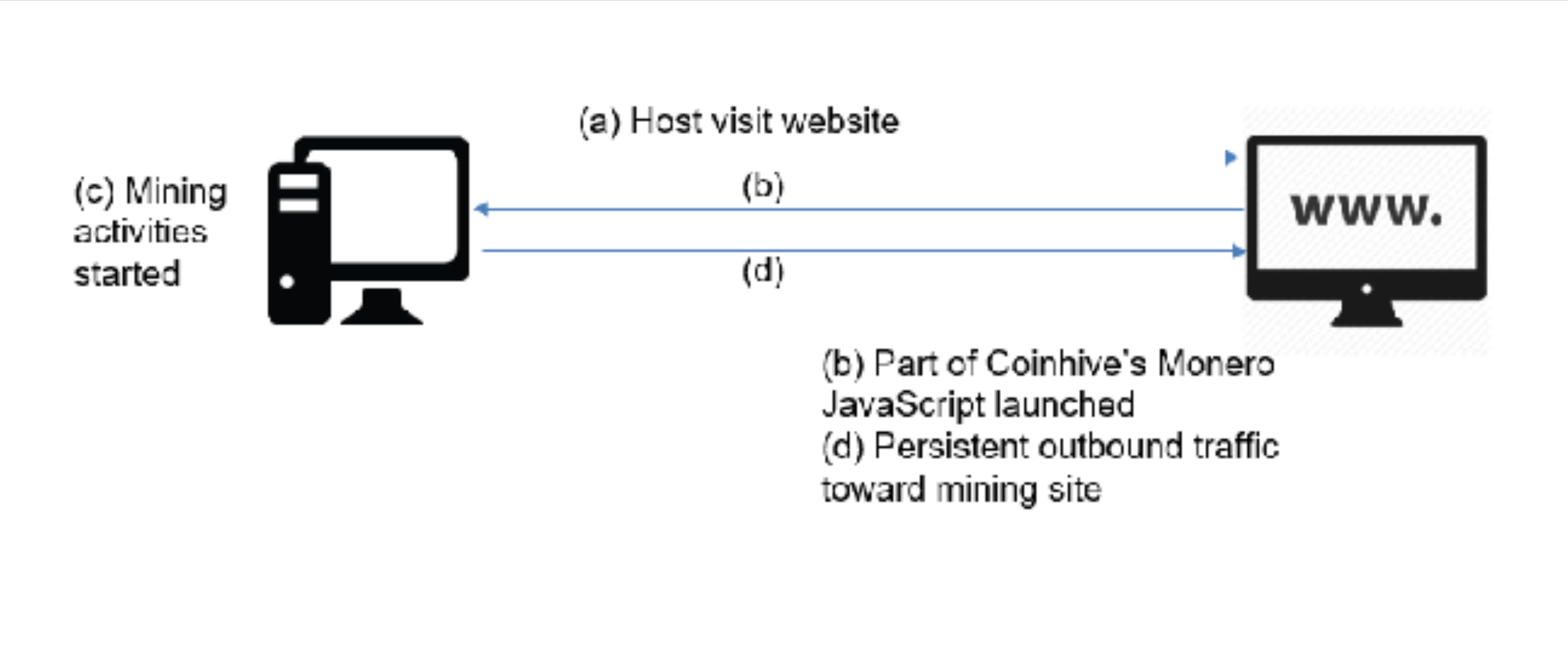
(a) Host visit website
(c) Mining activities started
(b)
(d)
www.
(b) Part of Coinhive's Monero JavaScript launched
(d) Persistent outbound traffic toward mining site

Figure 8. Anatomy of Group A Coinhive's Monero mining behaviour

Whereas for Group 2, instead of persistent outbound traffic to the visited website, we observe outbound traffic from host toward advertisement sites via content delivery network (CDN). Host visited websites, JavaScript triggered and redirect host to another sites. These redirected sites hosted another JavaScript that started the mining. Process from direction to host started mining create another hidden browser. At the time of research, we observed multiple persistent outbound traffic toward CDN, where host as hosts were mining at the mining sites. Refer Figure 9 for the anatomy

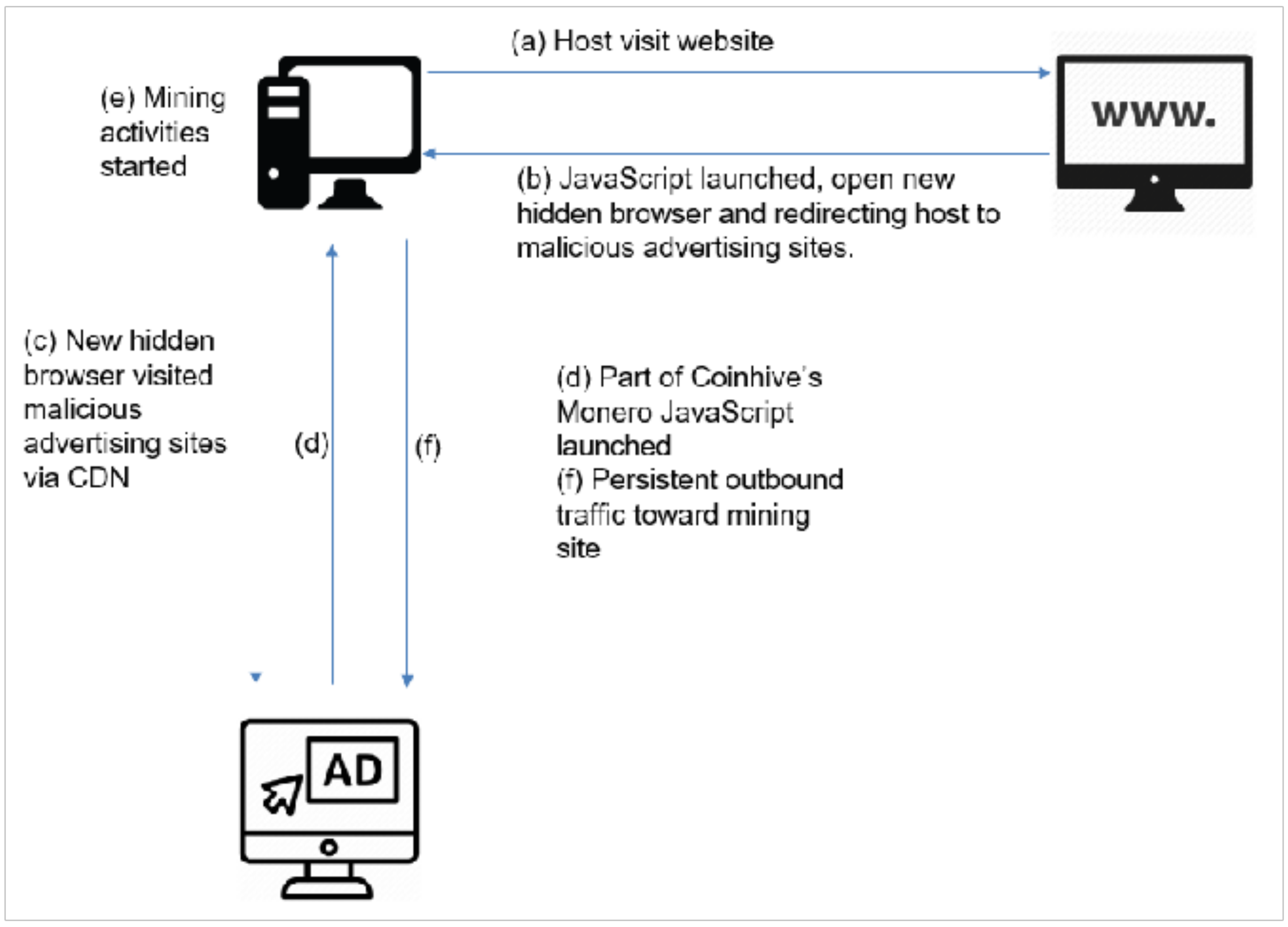
(a) Host visit website
(e) Mining activities started
WWW.
(b) JavaScript launched, open new hidden browser and redirecting host to malicious advertising sites.
(c) New hidden browser visited malicious advertising sites via CDN
(d)
(f)
(d) Part of Coinhive's Monero JavaScript launched
(f) Persistent outbound traffic toward mining site
AD

Figure 9. Anatomy of Coinhive Monero mining via advertistment sites

Table 1 shows summarize characteristic for group A and B

Table 1. Summarize characteristic for both group

Group A	Group B
• JavaScript that triggered mining resides on the visited websites • Persistent outbound traffic toward the infected websites from host machine.	• JavaScript that triggered mining does not resides on the visited websites • Persistent outbound traffic toward the redirected sites.

Based on the sample tested, instead of embedding JavaSript in the website like traditional drive-in exploit, cybercriminal leverage the technology of CDN and hosted the mining JavaScript in other sites, mainly advertisement sites for mining purposes. Hosts were redirected to these mining sites when visiting the infected websites. Thru this way, cybercriminal can maintain their infrastructure longer and able to infect large scale of host with minimum changes to crypto-jacking infrastructure.

6. Conclusion

Detecting mining activities is not just tedious but sometimes impossible and costly. Identifying these behaviors may assist to increase protection against organization. Based on the behavior identified, set of rules can be implement at network and host level to either preventing or detecting these activities.

Acknowledgments
The work is funded by Universiti Malaysia Pahang under Grant ID RDU1703294. The authors would like to thank all reviewers for their constructive comments, and Universiti Malaysia Pahang for the support.

References

[1] Berentsen, A. (2019). Aleksander Berentsen Recommends “Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto. 21st Century Economics, 7–8. doi:10.1007/978-3-030-17740-9_3

[2] Bitcoin price | index, chart and news | WorldCoinIndex. (2019). Retrieved from https://www.worldcoinindex.com/coin/bitcoin

[3] The state of malicious cryptomining. (2018, September 04). Retrieved from https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/

[4] Ahmed, A. A. (2015). Investigation Model For Ddos Attack Detection In Real-Time. International Journal of Computer Systems & Software Engineering, 1(1), 93–105. doi: 10.15282/ijsecs.1.2015.8.0008

[5] Krebs, B. (2018). Who and What Is CoinHive. Website https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive.

[6] Hong, G., Duan, H., Yang, Z., Yang, S., Zhang, L., Nan, Y., … Qian, Z. (2018). How You Get Shot in the Back. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS ’18. doi:10.1145/3243734.3243840

[7] Musale, M. (n.d.). Hunting For Metamorphic JavaScript Malware. doi:10.31979/etd.ky84-3b5q

[8] Cimpanu, C. (2018). Over 1.65 Million Computers Infected With Cryptocurrency Miners in 2017 So Far. Retrieved from https://www.bleepingcomputer.com/news/security/over-1-65-million-computers-infected-with-cryptocurrency-miners-in-2017-so-far/

[9] Eskandari, S., Leoutsarakos, A., Mursch, T., & Clark, J. (2018). A First Look at Browser-Based Cryptojacking. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). doi:10.1109/eurospw.2018.00014