2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA)
Pimpri Chinchwad College of Engineering (PCCOE), Pune, India. Aug 26-27, 2022

Exploiting Honeypot for Cryptojacking: The other side of the story of honeypot deployment

Priyank Patel
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India
priyank.patel@somaiya.edu

Ashwini Dalvi
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India
ashwinidalvi@somaiya.edu

Irfan Sidddavatam
Department of Information Technology
K. J. Somaiya College of Engineering
Mumbai, India
irfansiddavatam@somaiya.edu

2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA) | 978-1-6654-8451-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCUBEA54992.2022.10010904

***Abstract*— Honeypots are a proactive mechanism to lure attackers into a pretentious setup. Until recently, honeypots have been applauded for discovering new attacks, attacker behavior patterns, and other findings related to the defensive mechanism. However, the presented work discussed how attackers could turn the honeypot mechanism into an offensive tool. The results are gathered from Cowrie – an open-source honeypot setup. The script is written to read commands executed by attackers from the Cowrie play log. In addition, the attack analysis documented attempts made by attackers to use honeypot resources for crypto mining.**

Along with exposing crypto-mining attempts made by attackers, the authors further analysed the log with custom written malware parser and IP address parser. The malware parser analysed details from all the files generated by the malware scanner. In addition, the IP parser did IP backtracing by analysing IPs in harmless, suspicious, and malicious categories.

Keywords—Honeypot, Cowrie, Crypto Mining, Malware Analysis, IP backtracing

I. INTRODUCTION

Nowadays, cyber security is an essential factor to look after for every organisation. The cybercriminals do not limit activities to craft attacks against targetted individuals or organisations but also attempt to exploit weak cyber infrastructure setup or information collected from social engineering. Cyber offence and defence evolved in accord with each other. In work [1], the authors offer a review of active and passive defence mechanisms in the cyber landscape. Authors mentioned deception technologies like Decoy, Honeypots, and Address Hoping under an active defence and commented that significant research in deception mechanisms is centred around Honeypots. Further, in work [2], the discussion is carried out on deception techniques with retrospective analysis and a futuristic perspective.

Cyber defence mechanism offers honeypot and honeynet setups to lure attackers. Honeypot is one of the defensive mechanisms opted by organisations to attract attackers to the exposed setup. Honeypot deployment is easy due to the advancement of visualisation technology. However, a honeypot is a vulnerable system and a deceiving mechanism that keeps track of malicious activities attackers attempt to inject into organisations' network environment and system. Three important key features of the honeypot discussed in [3] are sensibility, countermeasures, and stealth. The level of interaction in a honeypot is mainly classified as a low, medium or interactive honeypot, and each interaction aims to collect attacks and attacker's information. High-interaction honeypots (HIH) offer complete interaction between attackers and honeypot systems and is used for research purpose. HIH provides real operating systems and services with a probability of high risk. Low-interaction honeypots (LIH) offer little interaction between intruders and the honeypot system. It captures limited interaction information about the attacker. Therefore, LIH is less likely to be compromised and emulates the basic functions and some parts of OS (operating system) services.

Honeypot simulates the original machine, device, service or operating system (OS) based on the type of interaction level. This simulating property of the honeypot is setting up a trap for an attacker. For example, to prevent an attacker from attacking the SSH port, one would redirect its port number 22 to the honeypot system that simulates SSH services and then set up portrays SSH honeypot. One would assign the original SSH port as the port number, for example, 22222, to trick an attacker [4]. The use case of a honeypot is illustrated with The project honeypot statistics that identified spam servers, harvesters, bad web hosts and search engines active currently [5]. Researchers implement different use case driven honeypots. For example, in [6], a deep neural network based honeypot is implemented to mimic Modbus protocol-driven communication.

The research on honeypot is directed majorly in two ways. The first is the implementation of honeypots, and the second is data analysis for attack pattern inferences with other related metadata and visualisation of collected data.

Therefore, the present work offers novelty in documenting how the honeypot, which is still now depicted as a mechanism to collect attackers' data, is now abused by attackers—the presented work compiled attempts by attackers to use the honeypot hardware set up to mine cryptocurrencies. The following paper includes a related literature review, methodology, result and conclusion.

II. LITERATURE REVIEW

The literature survey is conducted with the objectives: Discussing work attempted with Cowrie Honeypot and Attempting Crypto mining at the end user resources.

A. Discussing work attempted with Cowrie Honeypot

Cowrie honeypot captures Username and Password combinations i.e. authentication attempts (tried, failed attempts and successful attempts), Source IP address, Source and Destination port, timestamp, SSH version, session id, eventid, sensor and message, along with Commands (in tty

folder) and downloaded files. Cowrie Honeypot has even log and play log.

The attributes of the event log are researched in literature to draw inferences from a collected log. For example, in work [7], the Cowrie honeypot was used for logging attack trials on open SSH port banking applications. The login attempts were analysed using the overall log detail in the form of graphs and visualisations with additional programs. The most frequent login attempts were observed using the Splunk enterprise dashboard. In work [8], Cowrie honeypot log attributes were monitored over months to analyse the attack and network traffic patterns. Also, log analysis based on geographical zone was included in the study. The Cowrie log analysis is not only studied to comprehend attack patterns but also to realise the attacker's behaviour [9].

The Cowrie setup could mimic Linux-based systems. The Cowrie honeypot is deployed in various environments. The authors [10] deployed three publicly available IoT Botnets, namely, Mirai, Bashlite, and Lightaidra, with Cowrie to detect unusual patterns in the log with the help of process mining. The work [11] analysed the data collected from Cowrie honeypot in an IoT environment with supervised learning models. The algorithms employed for attack classifications were SVM, Random Forest, J48 decision tree, and Naive Bayes. The attacks were classified as SSH attacks, implantation of malicious payload, spying, XOR distributed denial of service, etc. The authors discussed honeypot forensics by facilitating machine learning models to classify attacks. In work [12], the authors implemented machine learning-based classifiers to distinguish benign and malicious SSH-enabled remote call sessions. In work [13], researchers investigate attack vectors similar to Mirai Botnet by analysing Telnet port on Cowrie honeypot.

The research attempts are made to predict the attack patterns like in [14] authors visualise Cowrie logs with ELK stack to predict directory traverser pattern of the attacker. Another such attempt is presented by authors [15], where Q learning-based reinforcement learning is employed to make Cowrie honeypot adaptive to hide it from attackers. In work [16], the authors mentioned that attackers could detect the deceptiveness of the Cowrie honeypot with automated tools. Thus it is required to comprehend the Cowrie honeypot implementation artefacts better to offer deception which attackers could not detect. In an extension of the mentioned study, authors [17] also present how improvised configuration would offer better deception over the default configuration of Cowrie honeypot.

Along with work to improve the performance of Cowrie honeypot, work is presented on how to read Cowrie logs in runtime [18]. The authors used GPT-2 (Generative Pre-trained Transformer -2) model trained with Cowrie honeypot log data to transform data into question and answer problems. Customised parser of GPT-2 enabled dynamic log reporting with Cowrie setup.

The work facilitated with Cowrie honeypot focused on using Cowrie event logs with different objectives, but the limited or rather not much attempt documented on working with the play log of Cowrie honeypot. Therefore, in the present work, the authors worked with the play log of Cowrie Honeypot.

B. Attempting Crypto mining at end user resources

The following review documented research discussing crypto mining attempts at end user expenses. The origin of the discussion of crypto mining at the user's end began when Javascript-enabled API facilitated running mining script in browser setup.

The researchers are investigating the attackers' attempts to mine the cryptocurrencies at the expense of the victim's resources. The work [19] presented a taxonomy of crypto-related attacks. Crypto mining malware that is executed in browser and memory and cryptoviral attacks were discussed to confirm traces of digital forensics evidence left after the attacks.

The attack known as a Drive-by attack or web-based crypto jacking is a typical attempt to mine cryptocurrencies without the user's consent. In [20], the authors investigated what qualifies for cryptojacking because of the possibility that website owners might willingly share a resource for crypto mining as an alternate form of advertisement revenue.

In work [21], the authors presented the study on attacks executed via a web browser. The executable binary was installed in the victim's machine via malicious javascript. The work further discussed mechanisms to detect and protect from such attacks. The defence against crypto jacking is proposed in literature like [22], where researchers attempt a novel approach, 'Mine Sweeper', to detect crypto jacking attacks.

The crypto mining attempts are researched with web-based crypto-jacking, but certain studies like [23] discussed static and dynamic crypto mining malware analysis. Further, work [24] proposed a network metadata-based approach to detect illicit mining attempts. Also, work [25] offered a discussion on the need to detect and prevent crypto jacking in an environment of internet-connected devices.

Along with variants of cryptojacking, cryptojacking is also examined in different infrastructure setups such as the Cloud environment. For example, in [26], the authors discussed 11 possible practical scenarios for cryptojacking in Cloud infrastructure. In addition, the authors outlined different attack vectors along with related tools and techniques for execution.

One of the common tools for cryptojacking is XMRig miner. XMRig software injects malicious code into existing system vulnerabilities without modifying the source code. XMRig miner is used as a reference malware signature to detect cryptojacking attacks with a work novel solution titled 'TrustSign' [27]. The work [28] demonstrated web-based threats to cloud infrastructure by documenting instances of XMRig miner setup run on cloud environments by attackers. As mentioned in [29], one cryptojacking malware is JenkinsMiner which uses XMRig miner to facilitate cryptojacking.

The literature review confirms that independent studies examine Cowrie honeypot artefacts to detect new attack vectors and inspect cryptojacking attempts. But there is no mention of work discussing the exploitation of honeypot for crypto mining. Thus dissecting the attacker's command with Cowrie play log and presenting results on the attempt of crypto mining at the expense of honeypot resources make the proposed work novel in its contribution.

III. METHODOLOGY

The honeypot solution implemented and studied on AWS is Cowrie (SSH honeypot). Figure 1 depicts the architecture of honeypot deployment.

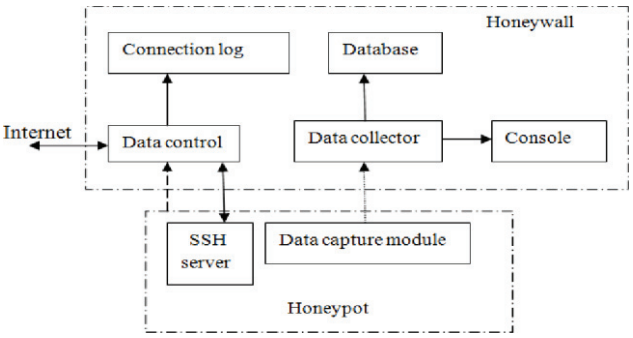

Fig. 1 Architecture of honeypot deployment

As shown in figure 1, the implemented setup of the Cowrie honeypot is comprised of Honeywell. Additionally, data handling is managed and run through Honeywell.

The present work is carried out with both event and play logs. The event log collected the IP addresses. The collected IP addresses are analysed to investigate whether the IP address is active or inactive, related malware signatures, and classification of IPs as benign or malicious.

The data collected contains all the interactions related to the attacker's session with the Honeypot machine. Further, all the data associated with the malware is analysed to identify the malware signature.

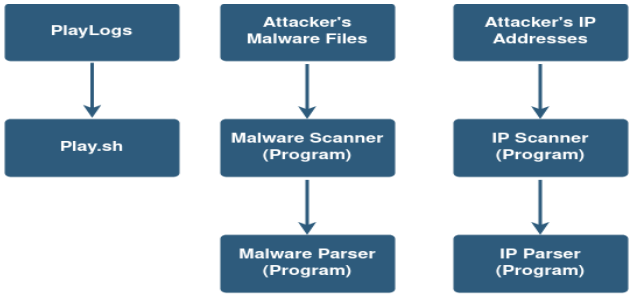

Fig. 2 Log investigation with the proposed approach

Figure 2 shows an improvised Cowrie log investigation approach.

In the present work, the authors worked with a play log of Cowrie Honeypot. The play log of Cowrie is screencasting in UML file format. Though instance-wise, play log is accessible, neither extraction of command nor query search is possible with play log. Thus authors exerted an improvised approach to work with Cowrie play log.

A customised script is written to extract commands from the play log. The concatenation of play logs is attained to have a complete play log of a particular Honeypot instance. Further, play logs are converted into text format for processing. Finally, regex operations are applied to extract the command. Upon extracting the command from the play log, it is found that attackers are attempting to use Honeypot resources for bitcoin mining.

PlayLogs module will extract input commands from Play Logs. Malware Scanner will scan all the input files for malware. Further, Malware Parser will extract the malware analysis details from all the files generated by the malware scanner. The data attributes of the file generated by the malware scanner comprised id, type, confirmed-timeout, timeout, harmless, suspicious, undetected, malicious, type-unsupported, failure, results, and date. Figure 3 depicts malware signature labelled as undetected and malicious on a sample of collected honeypot log.

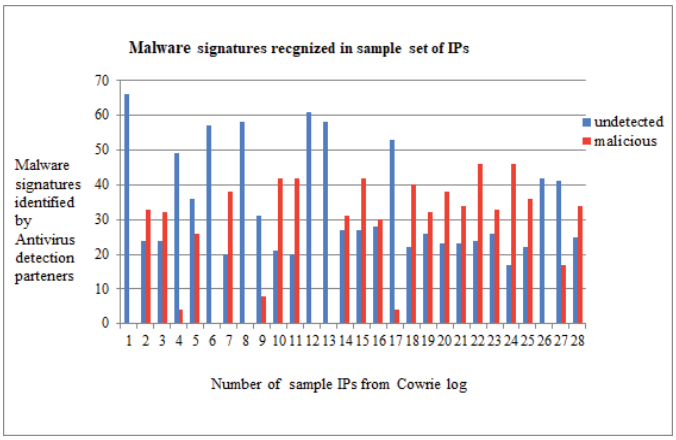

Fig. 3 Malware analysis of sample honeypot log

IP Scanner extracts all the IP addresses from the Cowrie logs and scans all the collected IP addresses for malicious activities. IP Parser collects all the data related to malicious IP addresses and parses the details to BackTrace.csv. Figure 4 shows one of the data attributes of BackTrace.csv consists of the IP owner's country.

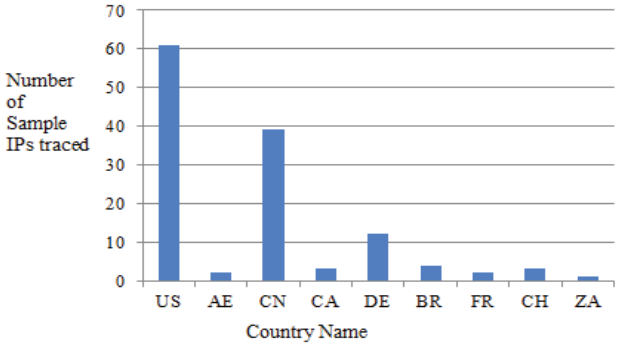

Fig. 4 Country analysis of IPs of sample honeypot log

With the proposed setup, Cowrie logs are collected and analysed for IP address information and identify traces of malware signatures. But the main focus of the proposed work is to document the attempt made by the attacker to use honeypot resources to mine cryptocurrencies.

Figure 5 depicts the attacker's attempt to learn the CPU architecture of the honeypot setup. Again, one can see that attacker executed the commands and tried to get the CPU architecture and model information.

Figure 6 and figure 7 show after obtaining the details, attackers downloaded the miner script from their custom hosted server and executed it using shell scripting.

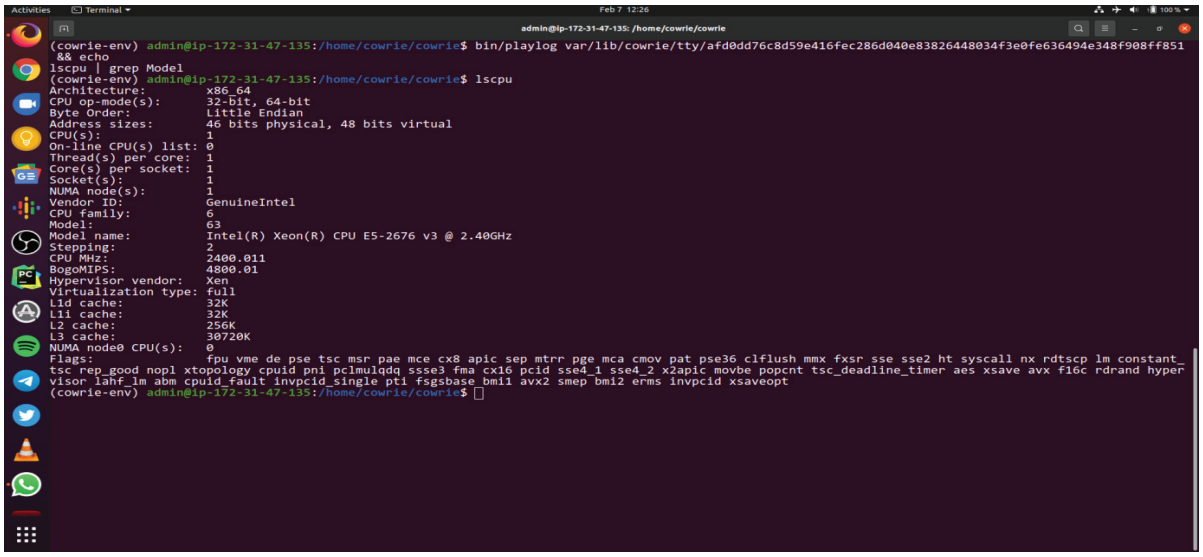

Fig 5. Attacker's attempt to read CPU architecture of Honeypot setup

Fig 6. Attacker's attempt to download mining script

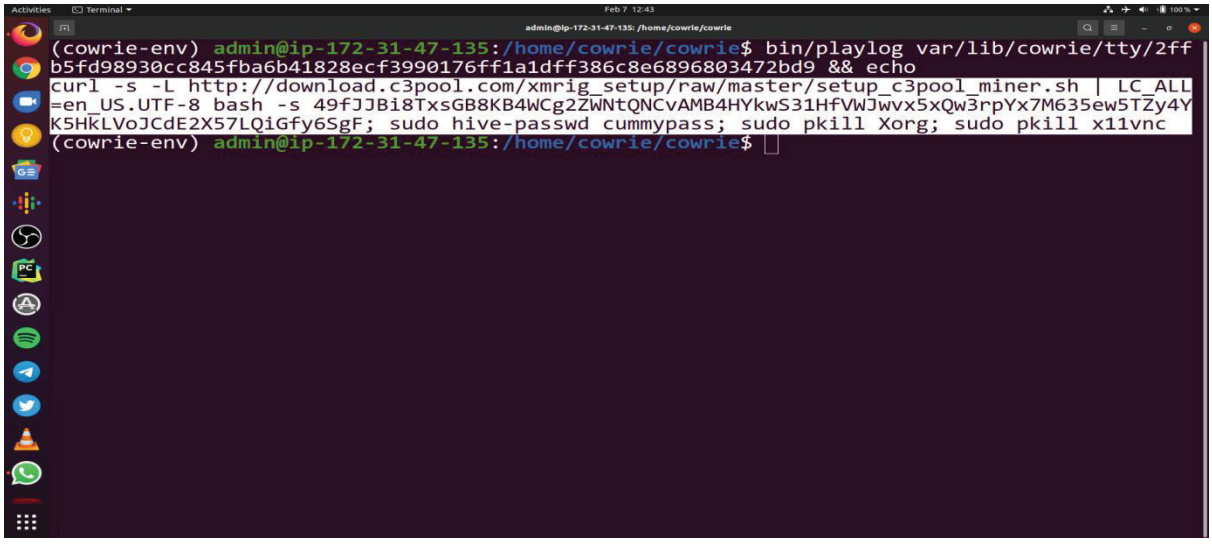

Fig 7. Attacker's attempt to run mining script with shell scripting

IV. CONCLUSION

The proposed work documented a cryptojacking attack on the honeypot. In addition, the proposed work elaborates on how honeypot resources are exploited for crypto mining.

The logs collected by Cowrie Honeypot are analysed for IP backtracking and Malware signature analysis. The presented work documented attempts of an attacker to run an XMRig mining setup on a honeypot. After conducting a literature survey, the authors concluded that the work discussed in this paper is the first of its kind to report crypojacking attempts on the honeypot. The future scope of work includes offering breadcrumbs to attackers on a honeypot setup to attempt cryptojacking. Furthermore, by collecting such honeypot data, one can learn and decipher current attack trends or methodologies used by attackers from the respective IP address and particular country or region.

REFERENCES

[1] Goethals, P. L., & Hunt, M. E. (2019). A review of scientific research in defensive cyberspace operation tools and technologies. Journal of Cyber Security Technology, 3(1), 1-46.

[2] Zhang, L., & Thing, V. L. (2021). Three decades of deception techniques in active cyber defense-retrospect and outlook. Computers & Security, 106, 102288.

[3] Fan, Wenjun, Zhihui Du, Max Smith-Creasey, and David Fernandez. "Honeydoc: An efficient honeypot architecture enabling all-round design." IEEE Journal on Selected Areas in Communications 37, no. 3 (2019): 683-697.

[4] Zuzčák, M., & Bujok, P. (2019). Causal analysis of attacks against honeypots based on properties of countries. IET Information Security, 13(5), 435-447.

[5] Project Statistics | Project Honey Pot [Online] Available: https://www.projecthoneypot.org/statistics.php [Accessed: April 2022].

[6] Siniosoglou, I., Efstathopoulos, G., Pliatsios, D., Moscholios, I. D., Sarigiannidis, A., Sakellari, G., ... & Sarigiannidis, P. (2020, July). NeuralPot: An industrial honeypot implementation based on deep neural networks. In 2020 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-7). IEEE.

[7] Lakh, Y., & Shymkiv, R. (2019, October). Using Honeypot Programs for Providing Defense of Banking Network Infrastructure. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 527-532). IEEE.

[8] Thom, J., Shah, Y., & Sengupta, S. (2021, January). Correlation of cyber threat intelligence data across global honeypots. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0766-0772). IEEE.

[9] Sadique, F., & Sengupta, S. (2021, June). Analysis of attacker behavior in compromised hosts during command and control. In ICC 2021-IEEE International Conference on Communications (pp. 1-7). IEEE.

[10] Coltellese, S., Maria Maggi, F., Marrella, A., Massarelli, L., & Querzoni, L. (2019, October). Triage of iot attacks through process mining. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" (pp. 326-344). Springer, Cham.

[11] Shrivastava, R. K., Bashir, B., & Hota, C. (2019, January). Attack detection and forensics using honeypot in IoT environment. In International Conference on Distributed Computing and Internet Technology (pp. 402-409). Springer, Cham.

[12] Dumont, P., Meier, R., Gugelmann, D., & Lenders, V. (2019, May). Detection of malicious remote shell sessions. In 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-20). IEEE.

[13] Bontchev, V., & Yosifova, V. (2019). Analysis of the global attack landscape using data from a telnet honeypot. Information & Security: An International Journal, 43, 264-282.

[14] Mehta, S., Pawade, D., Nayyar, Y., Siddavatam, I., Tiwart, A., & Dalvi, A. (2021, September). Cowrie Honeypot Data Analysis and Predicting the Directory Traverser Pattern during the Attack. In 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-4). IEEE.

[15] Suratkar, S., Shah, K., Sood, A., Loya, A., Bisure, D., Patil, U., & Kazi, F. (2021). An adaptive honeypot using q-learning with severity analyser. Journal of Ambient Intelligence and Humanized Computing, 1-12.

[16] Cabral, W., Valli, C., Sikos, L., & Wakeling, S. (2019, December). Review and analysis of cowrie artefacts and their potential to be used deceptively. In 2019 International Conference on computational science and computational intelligence (CSCI) (pp. 166-171). IEEE.

[17] Cabral, W. Z., Valli, C., Sikos, L. F., & Wakeling, S. G. (2021, June). Advanced cowrie configuration to increase honeypot deceptiveness. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 317-331). Springer, Cham.

[18] Setianto, F., Tsani, E., Sadiq, F., Domalis, G., Tsakalidis, D., & Kostakos, P. (2021, November). GPT-2C: a parser for honeypot logs using large pre-trained language models. In Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (pp. 649-653).

[19] Zimba, A., Wang, Z., Chen, H., & Mulenga, M. (2019). Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks. KSII Transactions on Internet and Information Systems (TIIS), 13(6), 3258-3279.

[20] Eskandari, S., Leoutsarakos, A., Mursch, T., & Clark, J. (2018, April). A first look at browser-based cryptojacking. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 58-66). IEEE.

[21] Zimba, A., Wang, Z., Mulenga, M., & Odongo, N. H. (2020). Crypto mining attacks in information systems: An emerging threat to cyber security. Journal of Computer Information Systems, 60(4), 297-308.

[22] Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., & Vigna, G. (2018, October). Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1714-1730).

[23] Pastrana, S., & Suarez-Tangil, G. (2019, October). A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth. In *Proceedings of the Internet Measurement Conference* (pp. 73-86).

[24] Russo, M., Šrndić, N., & Laskov, P. (2021). Detection of illicit cryptomining using network metadata. *EURASIP Journal on Information Security*, *2021*(1), 1-20.

[25] Swedan, A., Khuffash, A. N., Othman, O., & Awad, A. (2018, June). Detection and prevention of malicious cryptocurrency mining on internet-connected devices. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (pp. 1-10).

[26] Jayasinghe, K., & Poravi, G. (2020, January). A survey of attack instances of cryptojacking targeting cloud infrastructure. In *Proceedings of the 2020 2nd Asia pacific information technology conference* (pp. 100-107).

[27] Nahmias, D., Cohen, A., Nissim, N., & Elovici, Y. (2019, July). Trustsign: trusted malware signature generation in private clouds using deep feature transfer learning. In *2019 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE.

[28] Swimmer, M., Yarochkin, F., Costoya, J., & Reyes, R. (2020). Untangling the Web of Cloud Security Threats.

[29] Tziakouris, G. (2018). Cryptocurrencies—a forensic challenge or opportunity for law enforcement? an interpol perspective. *IEEE Security & Privacy*, *16*(4), 92-94.