COMPILER
Vol. 11, No. 2, November 2022, pp. 97~101
ISSN: 2252-2403 (Print), ISSN: 2549-2403 (Online)
Accredited Fourth Grade by Kemenristekdikti, Decree No:200/M/KPT/2020
DOI: 10.28989/compiler.v11i2.1369

Network Forensic of Cryptocurency Miners

Arief Ikhwan Wicaksono*, Rama Sahtyawan, Dedy Hariyadi
Department of Information Technologi, Jenderal Achmad Yani Yogyakarta University, Indonesia

Article Info

Article history:

Received November 3, 2022
Accepted December 31, 2022
Published December 31, 2022

Keywords:

Forensic
Cyber Security
Acquisition
Port Mirroring
Security Breach

ABSTRACT

As reported by BSSN in August 2022, Indonesia has traffic anomalies of 1.6 billion traffic, with 55.83% of anomaly findings containing malware, and the remaining 14.99% of information disclosure is another activity. Some of this data, when further analysed based on the type of attack, falls into the categories of breaches, successes, attempts, and failures. Investigate crimes related to the misuse of resources for illegal cryptocurrency mining activities. Therefore, this study should consider acquisitions from the network side as they apply to exist government agencies/institutions. This observation thereby provides information for later evidence, intruder detection, and prosecution of perpetrators who misuse resources for personal gain. As a result, the harvesting process can obtain valuable data from routers as a piece of digital evidence for investigating information about network attack activity and anomalies traffic.

Corresponding Author:

Arief Ikhwan Wicaksono
Department of Engineering and Information Technology,
Jenderal Achmad Yani Yogyakarta University,
West Ring Road, Yogyakarta
Email: ariefikhwanwicaksono@gmail.com

1. INTRODUCTION

Investigation of a study conducted by BSSN between January and August 2022 revealed 693,982,773 traffic anomalies or suspicious attempts to compromise Indonesian cybersecurity. Most of these are malware campaigns. Of all traffic anomalies, most of which were 55.83% malware attack activity, 14.99% information disclosure activity, and 10.45% Trojan horse activity. BSSN analyzed the types of attacks, traffic anomaly status was 61% compromised, 9% successful attacks, 27% attempted, and 3% failed. Based on data breach reports for the period January through October 11th, 2022, the Cyber Security Operations Office's Cyber Threat Intelligence (CTI) team consisted of 17 internal reports and 204 reports to Notified and created 221 data breach reports. The design of detecting cyber threats and attacks on the network is called intrusion detection system (IDS), IDS is typically implemented on the server side of the system. There are two detection models for this method: signature-based detection and anomaly-based detection [1]

Chief executives, chief privacy officers, and chief information officers should understand the three phases of a cybersecurity attack: before the attack, during the attack process, and after the attack is complete, according to an article written by American University researchers [2]. The goal of their Intrusion Detecting System (IDS) on network systems is early detection of cyberattacks before they are carried out. IDS is also very powerful in monitoring systems under attack. In this case, IDS is used in the second stage of the cyberattack. Much effort and research have been done to detect cyber-attacks that use computer and system networks. Previous research has used IDS to detect cyberattacks before and during security incidents [3]. One of the few anomalous activities on networks is attacks in the form of unauthorized access to resources that make users feel uncomfortable performing the activity. It is suspected due to crypto jacking activity. Crypto jacking is an attack on a network that takes advantage of all existing computer hardware and is carried out without the owner's permission. So, one of the losses that users have achieved is that their computer performance feels very heavy and annoying. One of the characteristics of computers infected with this attack is increased processor, memory, and graphics card performance. With port mirroring in Router OS, you can do live forensics by observing ports commonly used for Bitcoin mining activity. Ports used for mining activity typically run-on TCP ports 6641 and TCP 6642 [4], but it does not preclude the use of other protocols if any

mining activity is in progress. As such, it is hoped that this research will provide detailed detection and examination of which layers are being used during attacks based on live forensic techniques.

From previous research, IDS based on Router OS and Maltrail is still used as an effort to implement cyber security in the stage before and during cyber security incidents. This approach does not include mitigation steps as a follow-up effort after a cyber incident, namely using a digital forensics approach. The sub-field of digital forensics related to computer systems and networks is called network forensics, which performs analysis related to unusual events in the form of cyber-attacks on computer systems and networks for law enforcement or implemented regulations. Therefore, in this article, we propose an analytical process for detecting the activity of crypto mining, data should be collected on the router, and the digital evidence characteristics defined by live forensic methods.

2. RESEARCH METHOD

The standard used for digital forensics worldwide is ISO/IEC 27037: 2012 and ISO/IEC 27042:2015. The process of conducting digital forensics according to ISO/IEC 27037: 2012 consists of four phases: identification, collection, capture, and storage [5]. Otherwise, ISO/IEC 27042:2015 analytic and interpretation focus can be seen in figure 1 [6]. This article will focus on the acquisition phase. The phase of copying digital evidence from electronic evidence by incorporating technical documents and activities that occurred during a cybersecurity incident. Capture techniques in digital forensics generally fall into three categories [7]:

1. Manual capture. It is a technique performed by digital evidence first responders and an electronic evidence capture technology by directly reading and searching digital evidence based on electronic evidence under limited time constraints. The integrity level of digital evidence is very weak, so this technique is given a low priority.
2. Physical Capture. A technique used by digital evidence first responders to obtain digital evidence by making an identical copy of the electronic evidence. This technique is also known as the cloning technique.
3. Logical Acquisition is a technique performed by digital evidence first responders by copying digital evidence of objects or files proven to be related to a crime. This procedure depends on a variety of conditions, such as high-capacity systems, systems connected to other systems that cannot be powered off, and the size of the system being captured. Sometimes called capture.

Figure 1. Process Workflow as Digital Forensic Process ISO / IEC 27037: 2012 and ISO / IEC 27042:2015

Based on these two standards, the acquisition process on network devices is allowed to be carried out live. This is influenced by using devices that cannot be turned off, therefore the process of acquiring digital evidence in the form of network traffic can be done directly. The process of acquiring digital evidence in the form of network traffic uses the SPAN method on Cisco devices or Port Mirroring on Miktorik. This method is also applied to the network interface intercept process. Even though the machine used to acquire is not functioning, it will not affect the quality of the network.

Increasingly complex computer systems and networks require integrated monitoring capabilities. This is an attempt to improve the quality and security and maintain the user's comfort when using the services of computer systems and networks. A network forensic approach can be used to investigate and analyze cyber-attacks against computer systems and networks to generate anomalous activity and malicious traffic [3]. Switch using a forensic network approach the procedure for obtaining digital evidence on network devices such as can be completed using port mirroring techniques. Another term for port mirroring is SPAN (Switch Port Analyzer). This is a technique of copying traffic from the port through which the main traffic passes to other media [8]. Completing the traffic copy using the port mirroring technique is done by exporting the traffic as digital evidence into a pcap formatted file [9][10].

This article performs a live capture process using the port mirroring technique on Router OS. The function as a medium or additional electronic evidence for storing a copy of network traffic from port mirroring technology. This allows files stored on disk memory cards to be classified as digital evidence, like memory cards in smartphones [11] . Based on the two standards adopted in this paper in the form of an intercept process as shown in figure 2. The access source (ingress) will be acquired by the intercept method

recorded by DEFR. All network traffic received by the client (egress) is the same as that received by DEFR.

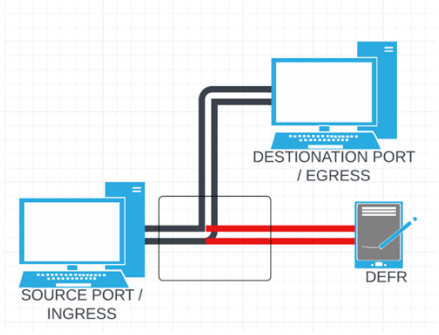

Figure 2. Port Mirroring on Network Topology by Digital Evidence First Responder (DEFR)

3.1. Minning Simulation Test

During the simulation phase, we mine through the network. The purpose of this mining is to leave anomalies in the router. Port mirroring allows loggers to copy data packets sent by a host through a switch and forward a copy of the data to a network log file. You can combine the benefits of port mirroring with sniffers to capture mirrored data from specific ports. Packet analysis applications can be used to manipulate mirrored packet data. In this case, mining activity on address 192.168.10.1 via port 6641 TCP. The result that hosts is mining without being seen as burdening access traffic on the network

3.2. Live Forensic Acquissition and Analysis

A challenge for router forensics is volatile data stored in memory that is discarded after a router reboot or shutdown. This situation is why live forensic techniques must be employed in this process. Acquisition should be performed as soon as possible after the incident [7]. Acquisition is initiated on a computer connected to the network as a client. The analytical process must be able to link information from different variables, such as supplementing information with other information, to explain events and attack activity. The stages of the analysis data field shown in Figure 3.

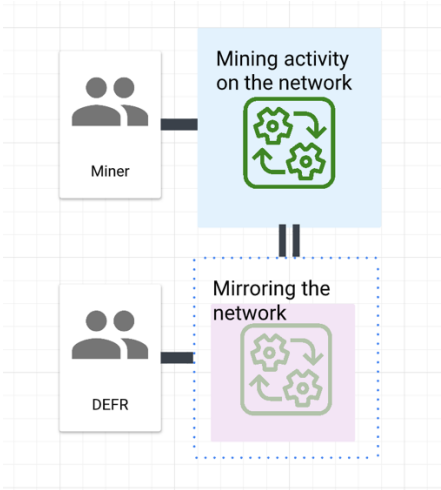

Figure 3. Live Acquisition Analysis

Observational data begins with the observation of log activity in Figure 4, which shows anomalous activity. In this case it is impossible for human behavior over port 6641 that he makes many requests per second. To ensure that other connections support mining activity, DEFR forces all connections leading to target IPs to be captured live and on a regular basis to obtain strong corroborating evidence. As the result of analysis, it reports that the mining activity is using another common port (TCP 6641 and TCP 6642) from miner.

3.2. Log Test

In order to understand the characteristic of digital evidence on Router OS, we perform lost, volatile, exist, and non-volatile test from log files. Understanding log files aims to determine the character of digital evidence taken from routers, log file testing is needed to measure how much log capacity can be accommodated, mirroring duration, log resistance to filtering the latest activity, and the ability of log data to be forensic. Log data plays an important role in the success of reading data if the observation has taken place. The weakness of

direct acquisition indeed lies in the loss of log files in the event of an electrical disturbance which eventually causes DEFR to lose the observation sequence, but log file robustness testing must still be carried out to comply with ISO/IEC 27037:2012 and ISO/IEC 27042:2015 work standards.

4. RESULTS AND ANALYSIS

When investigating cyberattacks against a complex ecosystem of computer systems and networks, it is necessary to record and monitor network traffic on routers. Network traffic recording and monitoring results can be saved to media for later analysis. This phase is part of the Identification, Collection, Acquisition, and Preservation under SNI ISO/IEC 27037: 2014. The router identified in this article is a Mikrotik RB1100HX2 that supports a switched port analyzer for logging and monitoring network traffic. The Switched Port Analyzer feature of the Mikrotik RB1100HX2 router is implemented in the Port Mirroring feature. Port mirroring technology is used as a live capture in computer systems and networks when recording network traffic [12]. The Mikrotik RB1100HX2 router has a chipset that supports switching. The chipset used by the RB1100HX2 is the Atheros 8327. Two Atheros 8327 chipsets are installed on ports Ethernet 1 – Ethernet 5 (Switch 1) and Ethernet 6 – Ethernet 10 (Switch 2).

The stages of port mirroring in Mikrotik are: interface ethernet switch -target=ether2 0 use the command to enter the switch menu. Router OS is used to handle network traffic data for port mirroring. The Raspberry Pi previously had a system application installed that used Maltrail to detect malicious traffic. Maltrail logs all network traffic at Layer 3. This is classified as unusual activity on the network. Anomalous network activity recorded and processed by Maltrail comes from multiple public providers of cybersecurity intelligence, including Kurhaus, alien vault, ransomwaretrackerurl, malc0de, ransomwaretrackerdns, and cobalt strike RouterOS's Port Mirroring and Maltrail-based Maltrail-based Malicious Traffic Detection System, the evidence obtained is a Wireshark-like .pcap not based on file format digital evidence. However, electronic devices for recording and monitoring network traffic can also be used as electronic evidence. For this study, the electronic evidence that can be collected according to the SNI ISO/IEC 27037: 2014 standard is routers and memory cards. Since routers are in a critical ecosystem, they cannot be physically secured.

Router devices are known for their port mirroring technology specifications and capabilities. In the case of the Raspberry Pi, the collection or seizure of electronic equipment as electronic evidence follows procedures such as recording specifications, storage in special containers for evidence, labeling, and recording chain of custody. On the other hand, for electronic evidence in the form of memory cards, duplication or imaging of digital evidence takes place in the form of information from malicious traffic detection systems. After cloning or imaging, the memory card is treated as electronic evidence. This storage device also requires additional hash information from the memory card as a form of storage phase. At the final stage, all evidence in the form of log files, memory cards, and clone/imaging results was brought into the lab for proper analysis for further electronic and/or digital evidence processing.

5. CONCLUSION

Cybercrime incidents against computer systems and networks of institutions with complex networks must be handled carefully with evidence to avoid impacting the institution's business processes. According to SNI ISO/IEC 27037: 2014, partial or logical investigations of complex computer systems and networks are permitted because the running system must not be stopped. The article concludes that network traffic capture can be done using port mirroring or SPAN technique. Additionally, network traffic information is stored using a Router OS.

REFERENCES

[1] A. Iswardani and I. Riadi, "DENIAL OF SERVICE LOG ANALYSIS USING DENSITY K-MEANS METHOD," *J. Theor. Appl. Inf. Technol.*, vol. 20, no. 2, 2016, Accessed: Nov. 03, 2022. [Online]. Available: www.jatit.org.

[2] I. Riadi, J. E. Istiyanto, and A. Ashari, "Internet Forensics Framework Based-on Clustering," *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 12, 2013, Accessed: Nov. 03, 2022. [Online]. Available: www.ijacsa.thesai.org.

[3] I. Riadi, J. E. Istiyanto, A. Ashari, and Subanar, "Log Analysis Techniques using Clustering in Network Forensics," *undefined*, vol. 10, no. 7, 2013, Accessed: Nov. 03, 2022. [Online]. Available: http://www.arin.net/registration/agreements.

[4] G. Gomes, L. Dias, and M. Correia, "CryingJackpot: Network Flows and Performance Counters against Cryptojacking," *2020 IEEE 19th Int. Symp. Netw. Comput. Appl. NCA 2020*, Nov. 2020, doi: 10.1109/NCA51143.2020.9306698.

[5] U. Duta Bangsa Surakarta, F. Teknik dan Teknologi, U. Jenderal Achmad Yani Yogyakarta, F. Ely Nastiti, and F. Sain dan Teknologi Universitas Respati Yogyakarta, "Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO/IEC Faulinda Nastiti Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO/IEC 27037:2014 Dedy Hariyadi Farida Nur Aini," 2703, Accessed: Nov. 03, 2022. [Online]. Available: https://www.researchgate.net/publication/328848272.

[6] D. Hariyadi *et al.*, *Buku panduan forensik digital*, 1st ed. Yogyakarta: CV Baskara Media, 2022.

[7] S. Raghavan, "Digital forensic research: current state of the art," *CSI Trans. ICT*, vol. 1, no. 1, pp. 91–114, Mar. 2013, doi: 10.1007/S40012-012-0008-7.

[8] M. Kassim, … M. R.-2022 I. 12th, and undefined 2022, "Network Analysis of Students' Online Activities via Port mirroring Switch Port Analyzer," *ieeexplore.ieee.org*, Accessed: Nov. 03, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9794504/.

[9] P. Eden *et al.*, "Forensic readiness for SCADA/ICS incident response," *scienceopen.com*, 2016, doi: 10.14236/ewic/ICS2016.16.

[10] M. Yang, Y. Wang, H. D.-2014 F. International, and undefined 2014, "Design of Win Pcap Based ARP Spoofing Defense System," *ieeexplore.ieee.org*, Accessed: Nov. 03, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6995023/.

[11] M. Mazdadi, I. Riadi, A. L.-I. J. of Computer, and undefined 2017, "Live forensics on routeros using api services to investigate network attacks," *academia.edu*, Accessed: Nov. 03, 2022. [Online]. Available: https://www.academia.edu/download/55897709/Journal_of_Computer_Science_IJCSIS_February_2017_Part_II.pdf#page=171.

[12] G. Stoitsov, V. R.-T. Journal, and undefined 2014, "One implementation of API interface for RouterOS," *temjournal.com*, vol. 3, no. 2, 2014, Accessed: Nov. 03, 2022. [Online]. Available: https://www.temjournal.com/documents/vol3no2/8/One implementation of API interface for RouterOS.pdf.