Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 6, No. 2, May 2021, Pp. 133-140

Network forensics against ryuk ransomware using trigger, acquire, analysis, report, and action (TAARA) method

Rusydi Umar[1], Imam Riadi[2], Ridho Surya Kusuma[*3]
Departmend of Informatics[1,3]
Department of Information System[2]
Universitas Ahmad Dahlan, Indonesia[1,2,3]

Article Info
Keywords:
Ryuk Ransomware, TAARA, Log, Network Traffic, Hash Signature

Article history:
Received: March 02, 2021
Accepted: April 07, 2021
Published: May 31, 2021

Cite:
Surya Kusuma, R., Umar, R. ., & Riadi, I. . (2021). Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 6(2). https://doi.org/10.22219/kinetik.v6i2.1225

*Corresponding author.
Ridho Surya Kusuma
E-mail address:
Ridho2007048010@webmail.uad.ac.id

Abstract
This study aims to reconstruct an attack event and analyze the source of viral infection based on network traffic logs so that the information obtained can be used for a new reference in the security system. Recent attacks on computer network systems cannot be easily detected, as cybercrime has used a variant of the Ryuk Ransomware virus to penetrate security systems, encrypt drives, and computer network resources. This virus is very destructive and has an effective design with a file size of about 200,487 Bytes so it does not look suspicious. The research steps are done through Trigger, Acquire, Analysis, Report, and Action (TAARA). The forensic tools used to obtain log data are Wireshark, NetworkMiner, and TCPDUMP. Based on the results of forensic data obtained include a timestamp, source of the attack, IP address, MAC address, hash signature sha256, internet protocol, and the process of infection. Based on the data obtained in this study has been by the expected objectives.

1. Introduction

The rapidly accelerating era of information technology is making cybercrime also increasing. In2020, the Ryuk Ransomware virus became one of the major threats to nationalinfrastructure [1][2] and the widely used cybercrime was about 10.9% from 100%, resulting in considerable financial losses [3], at the end of October 2020 there was a 45% increase in cyber attacks on the health care sector globally, especially hospitals and health institutions [4]. Ryuk is highly destructive by penetrating security systems, mapping the scope of infection, encrypting data using the AES-256 cryptographic type and RSA public key (Rivest ShamirAdlemen) to encrypt AES (Advanced Encryption Standard) keys, and exploiting computer network resources. It has layered encryption and makes it stronger [5][6]. Encrypted data cannot be reopened until it pays a bitcoin ransom for its encryption unlockkey [7][8][9][10]. In previous studies on LockerGoga Ransomware through static and dynamic analysis to find encryption keys [11]. However, this approach is not a long-term solution and cannot track new variants that have been modified [12][13].

Other research through the detection of deep learning methods on neural networks when virus executable files are executed [14], using IRP (I/O Request Packet) logs [15], and detection of ransomware cerber against behavioral-based computer networks. This study approaches behavioral computer network analysis through network traffic logs because it can reconstruct the initial events of new infections with attacks of new techniques [16]. Based on that can answer the formulation of problems that can be described, namely: when the initial infection occurred, who was the victim of infection, where the location of the attack, why it can happen, what makes the infection occur, and how the infection occurred. The main step is to know the management characteristics and log records of computer network traffic [17]. Logs are resources that contain network activity thoroughly and describe each event that occurs [18][19]. Therefore, this research aims to conduct network forensics by reconstructing the Ryuk Ransomware attack, to determine the virus infection through suspected network traffic [18][20]. Ryuk's attack reconstruction in this study used network forensic methodology and TAARA. Based on log evidence, the results of this study include timestamp information, source of an attack, IP address, MAC address, signature, victim details, and know-how of the infection that occurred.

2. Research Methods

This research uses forensic computers that serve to collect, analyze, and obtain evidence on the metadata of entities or log activities that exploit computer networks [21][22]. The implementation of this forensic network is a form of an effort to find the signature of the ryuk attack, the signature that can be used to prevent attacks in the future.

2.1 Network Forensics

Network forensics is a branch of forensic digital science related to the analysis of traffic networks, finding all the possibilities that cause system violations, and live forensic investigation because the information is easily lost [23][24][25][26]. The technique applied to this case study is a honeypot, namely by trapping and monitoring network traffic using computers and forensic tools [27][28]. This study refers to several internet protocols that successfully capture log activity as early detection parameters of attacks such as TCP, HTTP (GET/POST), and DNS Traffic analysis [29][30].

2.2 TAARA Methodology

This research uses the TAARA methodology which is derived from of Threat Assessment & Remediation Analysis (TARA) methodology, this method has a more limited scope and needs, less time and resources to carry out threat assessment, while covering cyber threats, non-cyber, a chain of attack, and electronic warfare [31]. This method consists of five stages: Trigger, Acquire, Analyze, Report, and Action. Here is the process of working on problem-solving using taara methodology can be seen in Figure 1.

Figure 1. Methodology TAARA

Here's a description of the TAARA methodology flow consisting of five main and interconnected sections:

Trigger: This is the incident that led to the investigation.
Acquire: this is a process that is carried out due to a response incident thus involving the activity, obtaining, and collecting information and evidence relating to the trigger.
Analysis: all evidence collected, correlated, and analyzed. The sequence of events is identified. Related questions such as whether the incident occurred; who is involved; the extent of the vulnerability; and so on were answered. Based on the information collected during this stage, it is necessary to collect additional data. The analysis then begins on newly obtained evidence.
Report: this is part of report generation based on the results of the previous analysis.
Action: this section generally contains actions implemented as recommended in the report.

2.3 Lab Environment

The lab development in this study used a combination of Virtualbox and GNS3 software as virtual network environment computers, as in Figure 2.

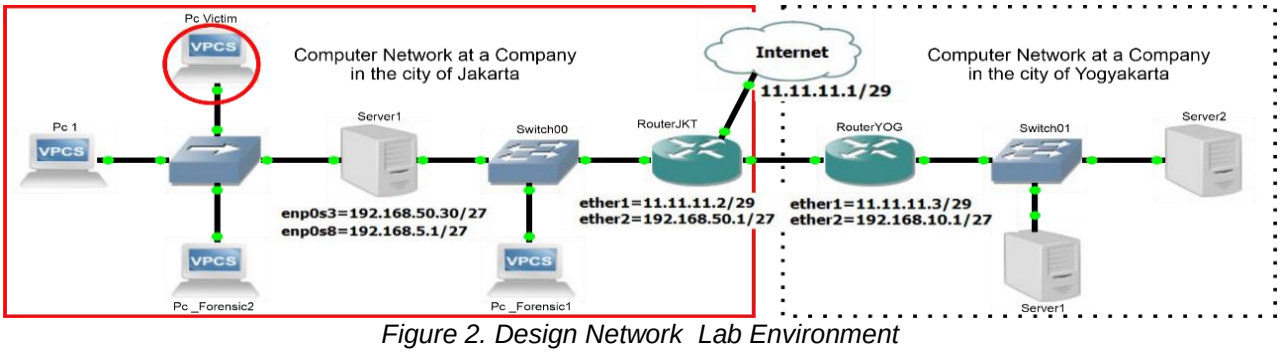

Figure 2. Design Network Lab Environment

The network design in the lab seems to include a MAN (Metropolitan Area Network) network consisting of two routers with positions in the cities of Jakarta and Yogyakarta. This research focuses on routerJKT paths that are self-directed from Pc_Forensic1, Server1, Pc_Forensic1, Pc1, and Pc Victim. Here is the network configuration in the lab so that it allows devices to connect [32], for details can be seen in Table 1.

Table 1. Configuration Network

Device	Port	IP Address	Netmask	Gateway	Os
RouterJKT	Ether 1	11.11.11.2	255.255.255.248	11.11.11.1	Mikrotik
	Ether 2	192.168.50.1	255.255.255.224	11.11.11.2	
RouterYOG	Ether 1	11.11.11.3	255.255.255.248	11.11.11.1	Mikrotik
	Ether 2	192.168.15.1	255.255.255.224	11.11.11.3	
Server1	Enp0s3	192.168.50.30	255.255.255.224	192.168.50.1	Ubuntu Server
	Enp0s3	192.168.5.1	255.255.255.224	192.168.50.30	
Client	Nic	192.168.5.2-30	255.255.255.224	192.168.5.1	Win7,8.1, Kali Linux

Based on Table 1, describes the network configuration consisting of Device, Port, IP Address, Netmask, Gateway, and Os in the lab environment. The study case in this study is a simulation of a ryuk ransomware virus attack with phishing website techniques on computer networks. This simulation aims to answer the problem formula [10]. then the attacker prepares a virus file (https://app.any.run/submissions) and uploads a fake website file http://www.skincareshop.42web.io, leading the victim to download it and execute it, the file exploits by dropping the virus into the system, then the attacker actor waits for the right time to start his evil activity [33]. Viruses map networks, understand the scope of infections, and system vulnerabilities to avoid both network and anti-virus security detection.

3. Results and Discussion

The network forensic process is carried out by simulating a targeted attack on one of the computers on the LAN (Local Area Network) network. Based on that investigation and analysis are done through a forensic network [27]. Some forensic tools in this study are presented in Table 2.

Table2. Forensic Tools

No.	Tools	Version
1.	Wireshark	3.4.3
2.	NetworkMiner	2.6
3.	TCPDUMP	4.99.0

Table 2, describing the forensic tools used to capture logs, Wireshark has the advantage of reading the content of each data traffic packet, NetworkMiner has the advantage of reading host-based data logs, and TCPDUMP is usually used for network troubleshooting [34]. These tools are used to obtain traffic network activity as awhole [35].

3.1 Trigger

An incident report containing a summary of the Ryuk Ransomware virus attack on a host computer that occurred on Thursday at 10:26 a.m. on February 18, 2021. The following ransom message can be seen in Figure 3.

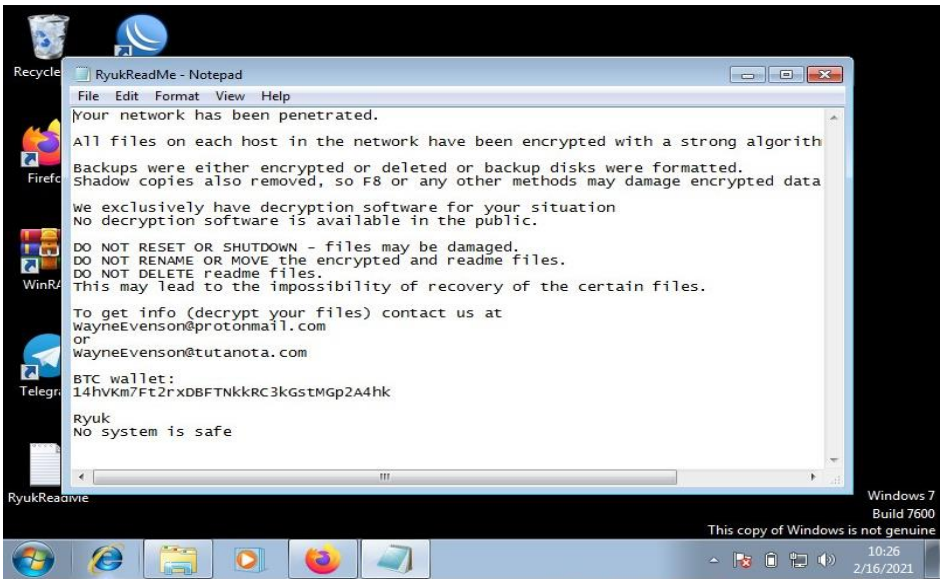

Figure 3. Ryuk Ransomware Attack

The details of the victim's computer are as follows: OS used is PC3, windows 7 64Bit, hostname: roby-pc, user account name: roby, IP Address: 192.168.5.15, and MAC Address 08:00:27:CD:6C:FF (PcsCompu_CD:6C:FF). Based on the ransom demand message known type of ransomware is Ryuk, the attacker's email is WyneEvenson@tutanota.com, and the bitcoin link 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk.

3.2 Acquire

Based on the incident report that occurred, the steps taken in this study collected traffic network activity log data that includes the LAN sector of the host computer, server, or router to obtain information and evidence related to the events in the report. Suspected host computer infection originated from users who neglected phishing links by accessing the website http://www.skincareshop.42web.io, following the appearance of the suspected website in Figure 4.

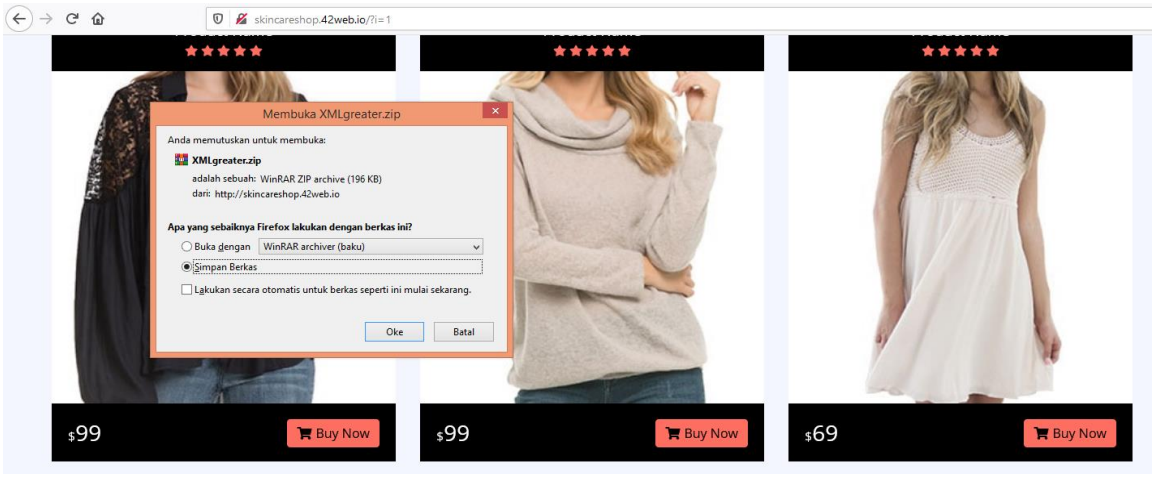

Figure 4. Phishing Website

In Figure 4, displays the sending of payload files through downloads performed by users. Proses file download is generally recorded data on the activity log. Based on this, the search and investigation of incident reports are based on logs that record file download activity on router traffic as shown in Figure 5. Namely capture logs using Wireshark tool.

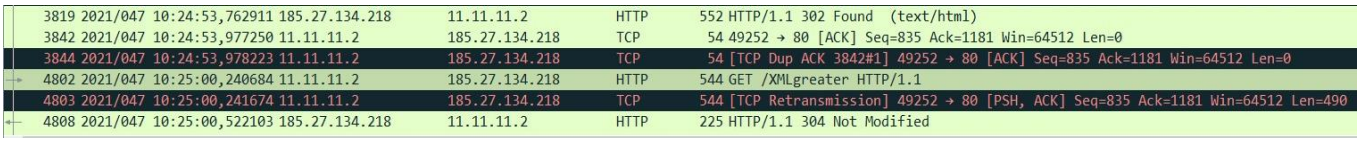

Figure 5. Capture log on Jakarta Router Sector

Network traffic log collection starts from aLAN, server, or router. In Figure 5, indicates the retrieval of network traffic log data where communication between the router and the server website occurs. A log that displays a black indicator on the TCP internet protocol, means that the communication failed or is known as bad TCP and the green log indicates the communication was successful so that a payload transfer occurred using the HTTP protocol. On bad TCP log analysis does not close the possibility as one way to avoid detection of security systems. The next process retrieves log data on the 1st forensic computer that reviews server traffic. In monitoring network sector server traffic logs using the host-based NetworkMinner tool. The NetworkMinner tool displays communication sessions between infected hosts and specific websites over TCP internet protocol, HTTP, and access on port 80. The tool has a log files feature that can be used to monitor specific sending and receiving of files and features DNS logs to strengthen analysis and additional information. DNS traffic logs can display various required information such as client, client port, server port, DNS Query, DNS Answer, and others. The process of acquisition of log data on the 2nd forensic computer of the LAN sector using TCPDUMP and Wireshark tools.

3.3 Analysis

Based on the log data that has been collected, proses log analysis begins by connecting the results of log data on the server and LAN sectors to reconstruct the occurrence of infection events. LAN sector log data is required to view the process data of the downloaded file that was successfully logged in without being detected, following the CAPTURE logs of TCPDUMP obtained as shown in Figure 6.

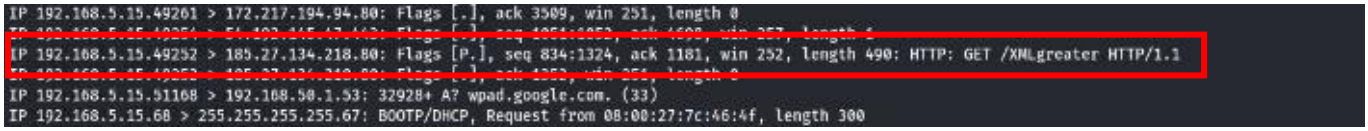

Figure 6. TCPDUMP Logs

The TCPDUMP logline displays suspicious activity. The log describes a file request with a packet length of 490 from IP address 192.168.5.15 port 49252 to IP address 185.27.134.218 port 80 via HTTP protocol. The information in the log identifies that the host computer accessed the server's website through the GET request service to download the XMLgreater file. based on the log lines in the red box, the XMLgreater file does not have a specific extension so it looks suspicious, further tracing by processing the logs using the Wireshark tool seen in Figure 7.

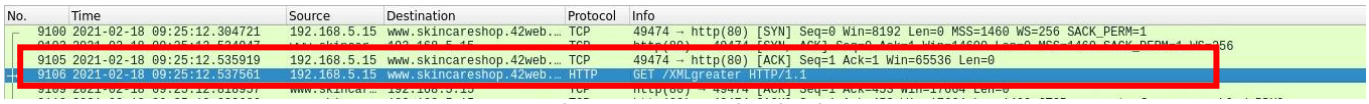

Figure 7. Log Wireshark

Wireshark's traffic log results show the process of sending a specific file to the host computer over the TCP protocol with the destination port 80. Also, Log Wireshark displays DNS destination information intended by the host computer that is skincareshop.42web.io or IP Address 185.27.134.218. Based on the logline in the red box allows tracing by retrieving files sent as investigations and digital evidence. The next process is the analysis log on the sector server to obtain additional information in the reconstruction of infection events as seen in the DNS logs in Figure 8.

Figure 8. NetworkMinner DNS Logs

DNS traffic logs obtained from the NetworkMinner tool describe server information1 with IP address: 192.168.50.30; port: 53; DNS server: 8.8.8.8; forward the request of the host computer with the os windows port: 55436; to communicate with DNS Query www.skincareshop.42web.io, the server forwards the query through the router so that the host computer and the website server are successfully connected. The website receives a request from the host computer and sends the file, the file submission process is successfully captured with log files that provide DNS communication request information between the host and the URL seen in Figure 9.

Figure 9. NetworkMinner Log Files

Traffic log files provide some information about the file that passes through the server sector namely type, size, protocol, port, delivery time, and destination. Based on the logline in the red box provides information that a file with the name XMLgreater has an extension type .zip, 200.487 Bytes, the process of sending using TCP internet protocol from IP address 185.27.134.218 port 80 to IP Address server 192.168.50.30 port 49448, and the file sent on February 18, 2021. Log files provide the information needed in the investigation process and the right choice to identify any files that come out or go in on network traffic. Further investigation on the host-based logs can be seen in Figure 10.

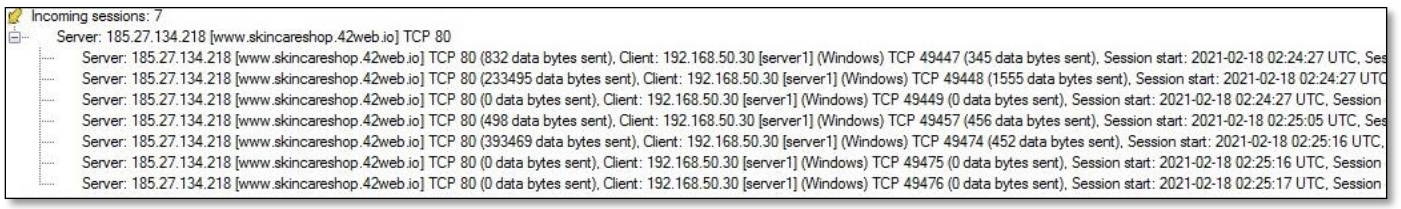

Figure 10. Log Host Network Minner

The results of the investigation log hosted on NetworkMinner provide information on the number of sessions on the process of sending files that pass through the server that is seven sessions needed in a single file submission. The information consists of per-session time, server IP address, URL, server port, and client port used, the session data can be used as additional data to identify which host with IP address performs file access and requests on a particular website. The process of tracing the source of the file by identifying the location of the IP Address URL using the website geolocation so that it can track the origin of the IP address of the website server as in Figure 11.

Figure 11. The IP address of the Website Server

The results of the identification process using a geolocation website showed the website servers were from the city of Lincoln, the English territory, the United Kingdom of Great Britain, and Northern Ireland. Based on these findings, it can be assumed that the C2 server (command and control) comes from the same IP address of 185.27.134.218. the next investigation process by conducting an examination analysis of the downloaded files. Analysis of files is done using the Wireshark tool because this tool allows obtaining in-depth information regarding data packet transmission by utilizing the following TCP stream feature as can be seen in Figure 12.

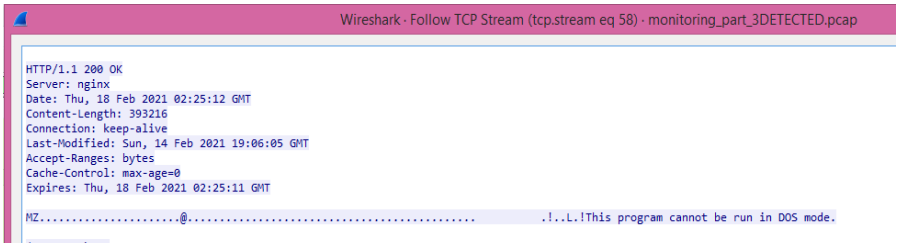

Figure 12. Packet Analysis

The results of the data packet analysis in Figure 12 with XMLgreater file format provide information on the type of server used is nginx and the file has a first-header"MZ" followed by the message "This program cannot be run in DOS mode". The first header identifies the existence of executable functions commonly used by malware. Based on that every file that contains the header should be alerted. The next process is static analysis by extracting, identifying, and testing whether the file is a virus, the "XMLgreater file" command indicates the output file identity has a PE32 executable function for MS Windows and a "shasum -a 256 XMLgreater" command indicating the identity of the file with the sha256 hash code as follows:23f8aa94ffb3c08a62735fe7f ee5799880a8f322ce1d55ec49a13a3f85312db2. The hash code is then tested by searching for similarity of file identity in search engines as shown in Figure 13.

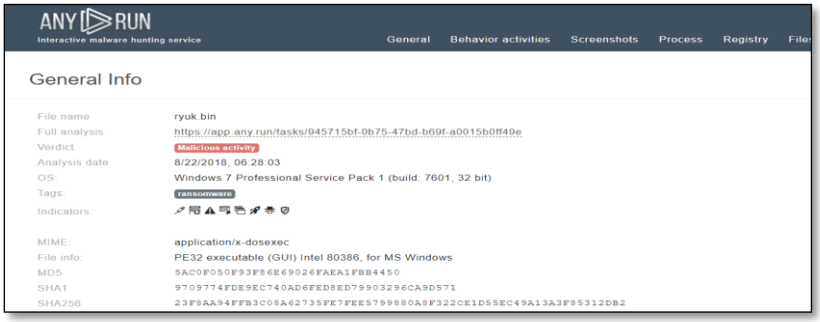

Figure 13. File Type Search

The result of searching the file type in the browser found that the obtained hash code is similar. The hash code and the pe32 file function executable ransomware virus is located in one of the online sandbox ANY RUN. Based on this, a conclusion can be drawn: The file type downloaded from the website www.skincareshop.42web.io with the IP address of 185.27.134.218 is ryuk ransomware.

This log analysis shows that Ryuk's attack took advantage of network segmentation, users are less aware of phishing attacks, select an item, download, and execute a file. Therefore, open remote access to avoid being suspected, which looks like a legal process, thereby disabling network security and anti-virus systems. Ryuk's attack feature is a. RYK encrypted with AES key.

3.4 Report

Here is a summary of the overall investigative information that has been found in the trigger, acquire, and analysis sections. This summary serves to answer the problem formulation and make improvements to the security system. Incident Report i.e. Ransom message appears with encrypted file occurred at 10:26 WIB, On Thursday, 18-02-2021, an infection occurred on a host computer with hostname: roby-pc; IP address: 192.168.5.15; MAC address: 08:00:27:CD:6C:FF; OS windows 7 64Bit; and ryuk ransomware virus type. Here are the results of the analysis static signature to make an indicator of the compromise virus file as in Table 3.

Table 3. Indicators of Compromise (IOCs)

File	Result
Sha256	23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2
Size	200,487 Bytes
Type	PE32 executable (GUI) Intel 80386 for MS Windows
Location Drop	C:\Users\roby-pc\AppData\Roaming\XMLgreater.zip
Source	http://www.skincareshop.42web.io/XMLgreater
Description	EXE file for Ryuk Ransomware

In Table 3, showing the specifications of virus files successfully obtained from network traffic log searches, here are the suspicious traffic found, which can be seen in Table 4.

Table 4. Suspicious HTTP Traffic

№.	Source	S. Port	Destination	D. Port	Info
1.	192.168.5.15	49474	www.skincareshop.42web.io	80	Access
2.	185.27.134.218	80	192.168.5.15	4974	Connected
3.	192.168.5.15	4974	185.27.134.218	80	Request
4.	185.27.134.218	80	172.128.194.94	-	Serif. Digital
5.	172.128.194.94	80	192.168.5.15	4974	Send and downloaded

Table 3 shows how infection incidents occur through the download of ransomware files on phishing websites www.skincareshop.42web.io and these reconstructions are obtained based on evidence of network traffic logs. Based on the data obtained by this study managed to find digital evidence related to how the initial infection occurred, this study can be used as a first step for further research, especially in the scope of reverse engineering.

3.5 Action

Here is an effort made to avoid attacks, so that this incident does not happen again in the future and become a reference for the improvement of network security systems. The use of anti-ransomware, namely the function of backup or data recovery so that in the event of a system attack can be restored immediately [36]. Socialization to employees about fake emails and websites serves to train and remind employees of the dangers of phishing and social engineering attacks, and updates on intrusion prevention systems (IPS).

4. Conclusion

The results of this study showed that the ryuk ransomware virus infection process is not easily detected by security systems on computer networks because the executable function of this virus is encrypted and the file size is in kiloByte size. Analysis of traffic log activity on the network provides information on the characteristics of Ryuk infection does not spread to other client computers, the way the infection works is that when the virus has been successfully embedded or dropped into a system, the virus does not immediately perform an attack but the virus will sleep while the actor (attacker) monitors the vulnerability of the system so that potential victims do not feel there is a threat, this virus will act to encrypt files after getting orders from actors. The use of TAARA method can be used to provide vulnerability gap information, accelerate IT parties in addressing attacks in a structured and systematic way on computer networks. further research can strengthen malware intrusion detection systems and identify signatures obtained from the ocsp protocol.

Cite: Surya Kusuma, R., Umar, R. ., & Riadi, I. . (2021). Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 6(2). https://doi.org/10.22219/kinetik.v6i2.1225

References

[1] N. Naik, P. Jenkins, N. Savage, and L. Yang, "Cyberthreat Hunting - Part 1: Triaging Ransomware using Fuzzy Hashing, Import Hashing, and YARA Rules," *IEEE Int. Conf. Fuzzy Syst.* , vol. 2019-June, pp. 1–6, 2019. https://doi.org/10.1109/FUZZ-IEEE.2019.8858803

[2] S. Il Bae, G. Bin Lee, and E. G. Im, "Ransomware detection using machine learning algorithms," *Concurr. Comput.* , no. December 2018, pp. 1–11, 2019. https://doi.org/10.1002/cpe.5422

[3] C. Coveware, "Key Trends 75% of all attack Ransomware 80% of attack exfiltrate data Ransomware Exfiltration Average Size of Organization Ransomware Exfiltration Techniques," no. December 2020, pp. 2020–2021, 2021.

[4] "Cyberaanvallen gericht op zorgorganisaties zijn sinds november 2020 met 45% gestegen / Cybercrime | Cybercrimeinfo.nl | De bibliotheek voor de bestrijding van digitale criminaliteit."

[5] CISA, "Ransomware Activity Targeting the Healthcare and Public Health Sector Alert (AA20-302A)," *Cisa*, pp. 13, 2020.

[6] E. Berrueta, D. Morato, E. Magana, and M. Izal, "A Survey on Detection Techniques for Cryptographic Ransomware," *IEEE Access*, vol. 7, pp. 144925–144944, 2019. https://doi.org/10.1109/ACCESS.2019.2945839

[7] I. Kara and M. Aydos, "Static and Dynamic Analysis of Third Generation Cerber Ransomware," *Int. Congr. Big Data, Deep Learn. Fight. Cyber Terror. IBIGDELFT 2018 - Proc.*, pp. 12–17, 2019. https://doi.org/10.1109/IBIGDELFT.2018.8625353

[8] T. Xia, Y. Sun, S. Zhu, Z. Rasheed, and K. Hassan-Shafique, "A network-assisted approach for ransomware detection," *arXiv*,2020.

[9] T.M. Liu, D. Y. Kao, and Y. Y. Chen, "Loocipher ransomware detection using lightweight packet characteristics," *Procedia Comput. Sci.* , vol. 176, pp. 1677–1683, 2020. https://doi.org/10.1016/j.procs.2020.09.192

[10] I. Riadi, S. Sunardi, and M. E. Rauli, "Identification of WhatsApp Digital Evidence on Proprietary Operating Systems Using Live Forensics," *J. Tech. Electro*, vol. 10, no. 1, pp. 18–22, 2018. https://doi.org/10.15294/jte.v10i1.14070

[11] A. Adamov, A. Carlsson, and T. Surmacz, "An analysis of lockergoga ransomware," *2019 IEEE East-West Dec. Test Symp. EWDTS 2019*, pp. 1–5, 2019. https://doi.org/10.1109/EWDTS.2019.8884472

[12] S. Saxena and H. K. Soni, "Strategies for ransomware removal and prevention," *Proc. 4th IEEE Int. Conf. Adv. Electr. Electron. Information, Commun. Bio-Informatics, AEEICB 2018*, pp. 2018–2021, 2018. https://doi.org/10.1109/AEEICB.2018.8480941

[13] S. Sheen and A. Yadav, "Ransomware detection by mining API call usage," *2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 983–987, 2018. https://doi.org/10.1109/ICACCI.2018.8554938

[14] R. Agrawal, J. W. Stokes, K. Selvaraj, and M. Marinescu, "University of California, Santa Cruz, Santa Cruz, CA 95064 USA Microsoft Corp., One Microsoft Way, Redmond, WA 98052 USA," pp. 3222–3226, 2019.

[15] M. A. Ayub, A. Continella, and A. Siraj, "An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network," *Proc. - 2020 IEEE 21st Int. Conf. Inf. Reuse Integr. Data Sci. IRI 2020*, pp. 319–324, 2020. https://doi.org/10.1109/IRI49571.2020.00053

[16] A. Kurniawan and I. Riadi, "Detection and Analysis of Cerber Ransomware Using Network Forensics Behavior-Based," *Int. J. Netw. Secur.* , vol. 20, no. 5, pp. 1–8, 2018. https://doi.org/10.6633/IJNS.201809_20(5).04

[17] M. Zulfadhilah, I. Riadi, and Y. Prayudi, "Log Classification using K-Means Clustering for Identify Internet User Behaviors," *Int. A. Comput. Appl.*, vol. 154, no. 3, pp. 34–39, 2016. https://doi.org/10.5120/ijca2016912076

[18] S. Datt, *Learning Network Forensics,* vol. 1, no. 1. Birmingham - Mumbai, 2016.

[19] M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *Int. A. Comput. Appl.* , vol. 180, no. 35, pp. 23–30, 2018. https://doi.org/10.5120/ijca2018916879

[20] I. Riadi, R. Umar, and F. D. Aini, "Analysis of Anomaly Detection Traffic Comparison With Naive Bayes Method And Support Vector Machine (SVM)," *Ilk. J. Ilm.* , vol. 11, no. 1, pp. 17–24, 2019. https://doi.org/10.33096/ilkom.v11i1.361.17-24

[21] A. Kurniawan and Y. Prayudi, "Live Forensics Techniques On Zeus Malware Activities To Support Forensics Malware Investigation," *HADFEX (Hacking Digit. Forensics Expo.* , no. August 2015, pp. 1–5, 2014.

[22] G. O. Ganfure, C. F. Wu, Y. H. Chang, and W. K. Shih, "DeepGuard: Deep Generative User-behavior Analytics for Ransomware Detection," *Proc. - 2020 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2020*, 2020. https://doi.org/10.1109/ISI49825.2020.9280508

[23] D.C. Prakoso, I. Riadi, and Y. Prayudi, "Detection of Metasploit Attacks Using RAM Forensic on Proprietary Operating Systems," *Kinet. Technol game. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, pp. 155–160, 2020. https://doi.org/10.22219/kinetik.v5i2.1037

[24] R. Umar, A. Yudhana, and M. Nur Faiz, "Performance Analysis of Live Forensics Methods For Investigating Random Access Memory In Proprietary Systems," *Pros. Konf. Nas. 4th Asos. Progr. Postsarj. Teacher. Muhammadiyah High*, pp. 207–211, 2016.

[25] S. R. Davies, R. Macfarlane, and W. J. Buchanan, "Evaluation of live forensic techniques in ransomware attack mitigation," *Forensic Sci. Int. Digits. Investig.*, vol. 33, p. 300979, 2020. https://doi.org/10.1016/j.fsidi.2020.300979

[26] T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *Int. A. Comput. Appl.* , vol. 164, no. 8, pp. 31–37, 2017. https://doi.org/10.5120/ijca2017913717

[27] M. Hikmatyar, Y. Prayudi, and I. Riadi, "Network Forensics Framework Development using Interactive Planning Approach," *Int. A. Comput. Appl.*, vol. 161, no. 10, pp. 41–48, 2017. https://doi.org/10.5120/ijca2017913352

[28] S. Sibi Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi, and B. Raman, "Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks," *IEEE Access*, vol. 8, pp. 169944–169956, 2020. https://doi.org/10.1109/ACCESS.2020.3023764

[29] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane, "A Multi-Classifier Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware," *IEEE Access*, vol. 7, no. c, pp. 47053–47067, 2019. https://doi.org/10.1109/ACCESS.2019.2907485

[30] M. K.A., *Learning Malware Analysis*. Birmingham - Mumbai: Packt Publishing Ltd., 2018.

[31] J. Wynn *et al.*, "Threat Assessment & Remediation Analysis (TARA)," *MITRE Tech. Rep.*, no. October, pp. 60, 2011.

[32] Y.Purwanto and I. Riadi, "Implementation of Multimedia as a Learning Medium (Case Study: Subnetting Material On IPv4)," *JSTIE (Jurnal Sarj. Tech. Inform me.* , vol. 1, no. 1, pp. 201–208, 2013. http://dx.doi.org/10.12928/jstie.v1i1.2531

[33] P. Kim, *The Hacker Playbook 3*. United States: Secure Planet, 2018.

[34] L. Usman, Y. Prayudi, and I. Riadi, "Ransomware analysis based on the surface, runtime and static code method," *J. Theor. Appl. Inf. Technol.* , vol. 95, no. 11, pp. 2426–2433, 2017.

[35] M. S. Ahmad, I. Riadi, and Y. Prayudi, "Live Forensic Investigation From the User Side To Analyze Man in the Middle Attack Based Evil Twin Attack," *Ilk. J. Ilm.* , vol. 9, no. 1, pp. 1–8, 2017. https://doi.org/10.33096/ilkom.v9i1.103.1-8

[36] S. Baek, Y. Jung, A. Mohaisen, S. Lee, and D. Nyang, "SSD-assisted Ransomware Detection and Data Recovery Techniques," *IEEE Trans. Comput.* , vol. X, no. X, pp. 1–1, 2020. https://doi.org/10.1109/TC.2020.3011214