DOI:10.14421/ijid.2021.2423 IJID (International Journal on Informatics for Development), *e-ISSN: 2549-7448*
Vol. 10, No. 1, 2021, Pp. 53-61

Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method

Rusydi Umar[1], Imam Riadi[2], Ridho Surya Kusuma[3]
[1,3] Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: [1] rusydi@mti.uad.ac.id, [2] imam.riadi@is.uad.ac.id, [3] ridho2007048010@webmail.uad.ac.id

Article History
Received May 12th, 2021
Revised July 2nd, 2021
Accepted July 6th, 2021
Published August, 2021

***Abstract*—Ransomware viruses have become a dangerous threat increasing rapidly in recent years. One of the variants is Conti ransomware. Attacks become a severe threat and damage the system, namely by encrypting data on the victim's computer, spreading it to other computers on the same computer network, and demanding a ransom. The working principle of this Ransomware acts by utilizing Registry Query, which covers all forms of behavior in accessing, deleting, creating, manipulating data, and communicating with C2 (Command and Control) servers. This study analyzes the Conti virus attack through a network forensic process based on network behavior logs. The research process consists of three stages, the first stage is attack simulation, the second stage is network forensics by using live forensics methods, and the third stage is malware analysis by using statistical and dynamic analysis. The results of this study provide forensic data and virus behavior when running on ram and computer networks so that the data obtained makes it possible to identify ransomware traffic on the network and deal with zero-day, especially ransomware threats.**

***Keywords*—Conti Ransomware; live forensic; traffic network; hash signature; log**

1 INTRODUCTION

The advancement of the digital and information world makes data a valuable asset; data protection and security become necessary from various threats such as damage, natural disasters, and cybercrime. Cybercrime attacks have used ransomware viruses in recent years to make a profit. The attack triggers a security system mechanism to protect data access from intruders[1]. Virus Ransomware is the most challenging virus and frequently attack organizations in all industries and geographies[2]. These viruses are similar to other types of malware in various aspects, but some have different characteristics[3]. In May 2019, the city of Cartersville, Georgia, United States, was attacked by the Ryuk Ransomware virus caused by an employee accidentally clicking a link in a phishing email. The attack prevented access to 3 terabytes of the city's information, and it ended after the government paid a ransom of US$380,000 and a transaction fee of US$7,755.65.[4]. In 2020, the University of California, San Francisco paid $1.14 million in Bitcoin to restore access to encryption management software files[5],[6]. The perpetrator develops more sophisticated model attacks to avoid detection and gain many advantages[7],[8].

The followings are some previous studies, namely ransomware analysis through surface, runtime, and static code methods to identify detailed characteristics of Ransomware[9]; analysis of network activity and patterns against the WannaCry ransomware virus using dynamic methods[10]; ransomware analysis through traffic characteristics of android mobile networks to identify malicious activity[11]; analysis of RAT (Remote Access Trojan) malware using reverse engineering techniques[12]; detection and analysis of Cerber Ransomware based on network forensics behavior using the OSCAR (Obtain Information, Strategies, Collect Evidence, Analyze, Report) method[7]. Therefore, in this study, we offer an approach to analyze Conti Ransomware virus attacks based on behavior-based network forensics, static analysis, and dynamic analysis. This approach identifies abnormal traffic by Conti ransomware attacks on computer networks[13],[14].

This study uses a sample of the Conti Ransomware virus, a sophisticated 2021 model that can spread infection and encrypt data simultaneously. The characteristics of Conti are destructive by spreading through computer networks quickly after execution, targeting all encrypted data with the "TIYSV" extension, and enabling the encryption process without connecting to the C2 server[15]. Based on these characteristics, Conti attacks can spread on computer networks become a severe threat.

The research process consists of three stages: the first stage through simulating attacks on the host computer through a phishing website. The second stage is to carry out network forensic activities using live forensic methods to acquire virus files and discover network forensics behavior [16]. The third stage performs malware analysis activities using static analysis to identify signature files and dynamic analysis to determine the behavior of RAM [17] and computer networks based on logs. Logs play an essential role as a source of information that records all computer activities and can find out all the possibilities that can occur[18], especially during the process of analysis and network forensics [19].

Therefore, this study offers network forensics-based ransomware analysis and malware analysis as an initial step in generating virus signatures based on network indicators to enable the system to detect threats in computer networks and deal with zero-day attacks, especially the case of ransomware virus attacks, where the virus continues to grow.

2 METHOD

2.1 Network Forensics

Network forensics is part of digital forensics, which analyses network traffic to collect, use, identify, examine, link, and document digital evidence of digital artefacts. The obstacle that often occurs in the network forensic process is the collection and lack of evidence because network-based digital evidence is very volatile to change quickly[13]. Therefore, the network forensic process is carried out directly in collecting digital artefacts that can be used as forensic results and used in the behavior-based analysis in computer networks.

2.2 Methods

This study uses a live forensics method as a first step to identify the behavior of a virus that attacks one of the host computers in a computer network [20],[21]. The stages of the live forensic method in this study are as shown in Figure 1.

Figure 1. The live forensic method.

This method consists of four stages: preservation, collection, examination, and analysis[22]. Here is a description of the flow of live forensic methods consisting of fourth stages, namely:

- Preservation is the stage of maintaining the integrity of the evidence found not to be lost or changed.
- The collection is gathering evidence related to crimes such as assault to assist the investigation process.
- The examination examines the evidence on digital artefacts to obtain evidence relating to a criminal act. The result of this stage can be vital information such as Ip Address, MAC Address, port, and virus file.
- The analysis analyses the examination process results to identify files used as evidence of assault cases on computer networks.

2.3 Malware Analysis

Malware analysis is a study to find out the behavior of malware, identify its characteristics, and function to build a

better defense to protect an organization's network. Here are some reasons for conducting malware analysis in this study:

- This analysis helps determine the type of malware that includes information theft, HTTP bots, spam bots, rootkits, keyloggers, RATs, Ransomware, and others[10].
- This analysis enables the identification of network indicators associated with malware so that they can be used to detect infections through network monitoring. For example, it finds that malware is contacting a specific domain or IP address during the analysis process. It can create signatures, monitor network traffic, and detect every host that contacts that domain or IP address.
- This analysis helps in determining the motive for the attack. For example, in the research finding that malware steals banking credentials or encrypts specific data, the purpose of the attack is to gain monetary gain.

The malware analysis process consists of three types: static analysis to identify viruses without running them to obtain signatures based on the identity of the virus file. The dynamic analysis identifies viruses by running them in a virtual environment to determine their behavior and characteristics. Code analysis identifies the program that is in the virus file to find out the working principle and function[10],[23]. Therefore, in this study, we use static and dynamic types of malware analysis.

2.4 Ransomware Analysis

Ransomware analysis is a research process to identify behavior, characteristics, resulting impact, and others. This analysis has the same three techniques as malware analysis, except that its use is more specific to Ransomware, namely surface, runtime, and code[9].

The purpose of this analysis is divided into two parts to determine the size of the damage. The first part is a binary analysis which includes its behavior when it infects the victim's computer and the second part is a behavioral analysis which includes the reaction of the virus to the computer network.

The process of initiating ransomware analysis in this research is through artefacts found in network forensics, virus file acquisition at the forensic stage, and performing ransomware analysis that focuses on behavior in computer networks.

2.5 Ransomware

Ransomware virus attacks generally consist of five stages, namely exploitation, delivery, backup spoliation, file encryption, and user notification in action to master data[24]. Here is a description of each stage of a ransomware attack, namely:

- Exploitation and infection are the first stages of infection, starting with a user accidentally running a file infected with malware. A general malware is inserted into the email or through a phishing website, thus paving the way for exploitation and inserting Ransomware.
- Delivery and execution are the stages of sending ransomware viruses into the system, and then the virus is executed[25].
- Backup spoilation is the stage of the virus immediately searching for and deleting backup files[26].
- File encryption is a virus stage encrypting all data and uniquely identifying each section[27],[28]. The encryption process takes several minutes to hours, depending on internet network latency.
- User notification and clean-up is the stage where the virus has finished the encryption process and gives an instructional message, and asks the victim for a ransom if they want to re-access the data.

2.6 Forensic Tools

The following are some of the forensic tools used in this study, as shown in Table 1.

Table 1 Tools Forensic

No.	Tools	Version	Function
1.	Wireshark	3.4.3	Capture Network
2.	Pestudio	9.09	Analysis Static
3.	Noriben	V1.8.4	Analysis Dynamic

Table 1 provides information on the tools used as data collectors in the ransomware analysis process, namely Wireshark for network analysis by capturing every data packet log and seeing what happens to network traffic[9]; Pestudio to identify specific files without having to run them obtained from data packet logs in computer networks. Noriben is a forensic software that works by recording memory logs to find out viruses' behavior, including access, delete, rename, create data or files[29].

2.7 Virtual Lab Design

This study uses a virtual environment to carry out attack scenarios, network forensics processes, and monitor networks against Ransomware[30]. The process of building a virtual environment using VirtualBox software allows virtualization of computers complete with operating systems and applications, along with the design of the virtual environment or what is known as a virtual lab, as shown in Figure 2.

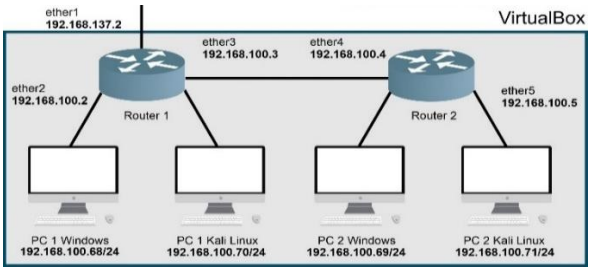


Figure 2. LAN network topology.

Figure 2 provides an overview of a complete virtual lab and computer network. The network topology implemented in the virtual lab is the Local Area Network (LAN) network topology.

The virtual lab consists of six devices: two routers with MikroTik OS, two computers with Windows 7 OS, and two computers with Kali Linux OS. Router1 acts as a central router that provides internet network access and is connected directly to the network driver on the central computer system, thus enabling router2 and client computers to connect.

2.8 Ransomware Attack Scenarios

Scenarios are built as closely as possible to actual conditions to be a study case. The attack on this scenario uses a phishing website. Here is a look at the phishing website home page as in Figure 3.

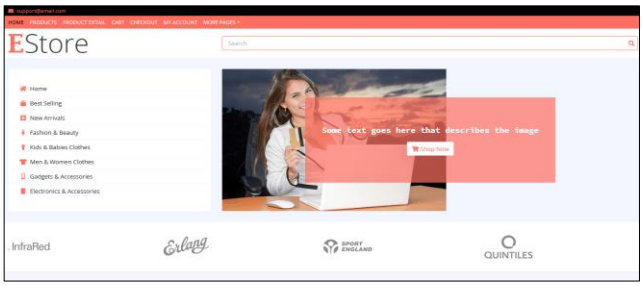


Figure 3. Phishing website.

Figure 3. shows the home page view of the website used for phishing ransomware attacks in this study. The attack scenario begins with the attackers gathering information related to sites frequented by a host computer. The second stage injects the exploit file into the phishing website. The third stage of the exploit dropped Ransomware on vulnerable systems so that users are affected to download and execute malicious files[31]

3 RESULT AND DISCUSSION

An incident report containing a summary of the Conti Ransomware virus attack on the host computer occurred on Sunday at 21:00 on April 14, 2021. Below are the stages and results of network forensics against ransomware attacks using the live forensic method. This study uses network forensics to reconstruct the infection that occurred and analyze the behavior of the virus based on network traffic logs. The following are the steps of network forensics and the results obtained based on the live forensic method.

3.1 Preservation

The first step is using the integrity of the preserved artefact as a source of information and obtaining digital evidence, namely, network traffic logs obtained from monitoring network traffic on forensic computers, as in Figure 4.

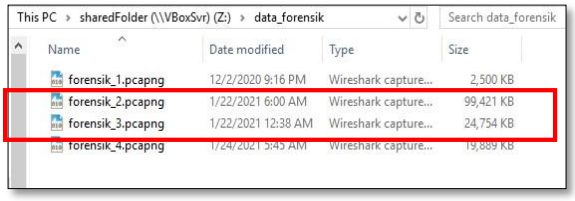


Figure 4. File storage

Figure 4 provides information that digital artefacts are available, i.e. several sets of network traffic log files. Two of four log set files have file sizes that exceed the standard in this study, with a log file storage size of 20 Kilobytes. The two files are 99,4 Kilobytes and 24,7 Kilobytes in size, so an investigation is needed to see what is happening.

3.2 Collection

The second step collects the data obtained from the ransomware attack, such as the ransom request proof in Figure 5.

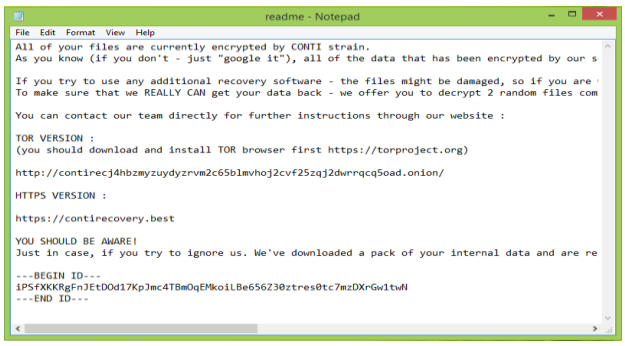
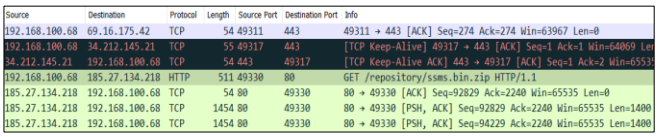


Figure 5. Message Ransomware

Figure 5. shows the ransom message that appears on the desktop screen of the host computer affected by a virus infection with IP Address 192168. 100. 68/24. The contents of the ransom message inform that Conti has encrypted the data on the host computer. The next step is to perform a log analysis of the network traffic log records, based on the

investigation obtained information that the user has downloaded specific suspicious files. The following captures the log file download process, as shown in Figure 6.



Source	Destination	Protocol	Length	Source Port	Destination Port	Info
192.168.100.68	69.16.175.42	TCP	54	49311	443	49311 → 443 [ACK] Seq=274 Ack=274 Win=63967 Len=0
192.168.100.68	34.212.145.21	TCP	55	49317	443	[TCP Keep-Alive] 49317 → 443 [ACK] Seq=1 Ack=1 Win=64069 Le
34.212.145.21	192.168.100.68	TCP	54	443	49317	[TCP Keep-Alive ACK] 443 → 49317 [ACK] Seq=1 Ack=2 Win=6553
192.168.100.68	185.27.134.218	HTTP	511	49330	80	GET /repository/ssms.bin.zip HTTP/1.1
185.27.134.218	192.168.100.68	TCP	54	80	49330	80 → 49330 [ACK] Seq=92829 Ack=2240 Win=65535 Len=0
185.27.134.218	192.168.100.68	TCP	1454	80	49330	80 → 49330 [PSH, ACK] Seq=92829 Ack=2240 Win=65535 Len=1400
185.27.134.218	192.168.100.68	TCP	1454	80	49330	80 → 49330 [PSH, ACK] Seq=94229 Ack=2240 Win=65535 Len=1400

Figure 6. Network traffic when downloading the payload

Figure 6 displays a network traffic log capture, the Traffic log in the image that shows a black indicator on the TCP internet protocol, which means it is poor TCP communication, while the green indicator means that communication is going well, then the log captures the host computer sending the request. Specific files on the HTTP protocol.

3.3 *Examination*

In this third step, perform a search on the captured logs to obtain information on suspicious network traffic logs and test the files accessed by the host computer.

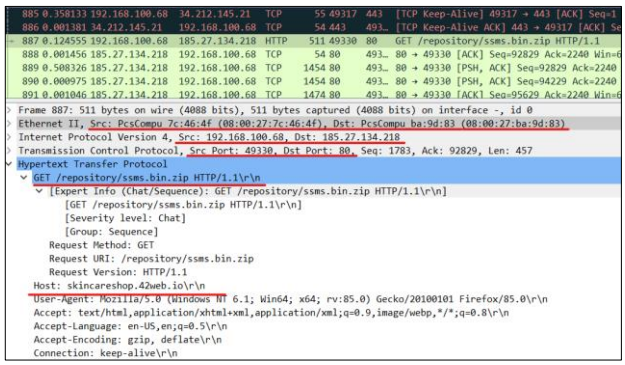


Figure 7. Network traffic log tracking

Figure 7 provides tracing information against the network traffic log on the HTTP protocol that accesses a particular file. Search results include IP address, Mac address, port, file name, websites visited by the host computer, and possible file acquisition. The following is the file testing process through the virustotal.com website, as shown in Figure 8.

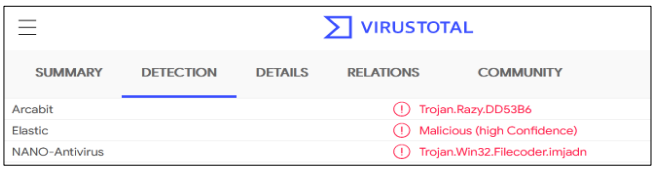
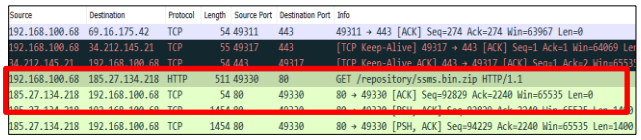


Figure 8. File test result

Figure 8 provides information on the test file results, which shows that the file contains a trojan virus. Based on that, the following process performs an analysis of the attacks that occurred.

3.4 *Forensic Analysis*

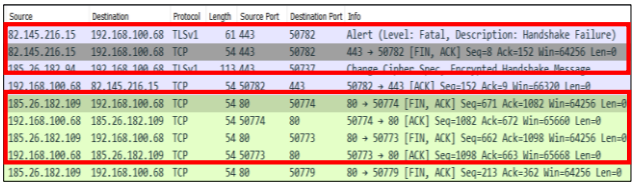
The fourth stage performs forensic analysis based on log data and files containing viruses. The analysis process connects logs to how infections and viruses run on computer networks. The following is a log analysis of the virus file download process, as shown in Figure 9.



Source	Destination	Protocol	Length	Source Port	Destination Port	Info
192.168.100.68	69.16.175.42	TCP	54	49311	443	49311 → 443 [ACK] Seq=274 Ack=274 Win=63967 Len=0
192.168.100.68	34.212.145.21	TCP	55	49317	443	[TCP Keep-Alive] 49317 → 443 [ACK] Seq=1 Ack=1 Win=64069 Le
34.212.145.21	192.168.100.68	TCP	54	443	49317	[TCP Keep-Alive ACK] 443 → 49317 [ACK] Seq=1 Ack=2 Win=6553
192.168.100.68	185.27.134.218	HTTP	511	49330	80	GET /repository/ssms.bin.zip HTTP/1.1
185.27.134.218	192.168.100.68	TCP	54	80	49330	80 → 49330 [ACK] Seq=92829 Ack=2240 Win=65535 Len=0
185.27.134.218	192.168.100.68	TCP	1454	80	49330	80 → 49330 [PSH, ACK] Seq=94229 Ack=2240 Win=65535 Len=1400

Figure 9. Network traffic logs

Figure 9 displays network traffic log information when there is communication between IP Address 192.168.100.68 to a website with IP Address 185.27.134218 via port 80, HTTP protocol, and info from packets is to get service requests to download suspicious SMS files. bin.zip. Below is the suspicious advanced network traffic log saw in Figure 10.



Source	Destination	Protocol	Length	Source Port	Destination Port	Info
82.145.216.15	192.168.100.68	TLSv1	61	443	50782	Alert (Level: Fatal, Description: Handshake Failure)
82.145.216.15	192.168.100.68	TCP	54	443	50782	443 → 50782 [FIN, ACK] Seq=8 Ack=152 Win=64256 Len=0
185.26.182.94	192.168.100.68	TLSv1	113	443	50737	Change Cipher Spec, Encrypted Handshake Message
192.168.100.68	82.145.216.15	TCP	54	50782	443	50782 → 443 [ACK] Seq=152 Ack=9 Win=66320 Len=0
185.26.182.109	192.168.100.68	TCP	54	80	50774	80 → 50774 [FIN, ACK] Seq=671 Ack=1082 Win=64256 Len=0
192.168.100.68	185.26.182.109	TCP	54	50774	80	50774 → 80 [ACK] Seq=1082 Ack=672 Win=65660 Len=0
185.26.182.109	192.168.100.68	TCP	54	80	50773	80 → 50773 [FIN, ACK] Seq=662 Ack=1098 Win=64256 Len=0
192.168.100.68	185.26.182.109	TCP	54	50773	80	50773 → 80 [ACK] Seq=1098 Ack=663 Win=65668 Len=0
185.26.182.109	192.168.100.68	TCP	54	80	50779	80 → 50779 [FIN, ACK] Seq=213 Ack=362 Win=64256 Len=0

Figure 10. Network traffic logs

Figure 10 provides information on suspicious network traffic logs in the log with the TLSv1 port 443 protocol. The packet info column in the log contains a warning message and a description of Handshake Failure. Furthermore, the network log shows suspicious data transfer activity on the intense TCP protocol between the host computer with IP Address 192.168.100.68 and IP Address 185.26.182.109, which always refers to port 80. Based on this information, the LAN network has been disrupted and infected. Therefore, further analysis by tracing the IP address 185.26.182.109 using the robtex.com website.

The search results for IP Address 185.26.182.94 originating from Amsterdam, North-Holland, NL therefore, the IP address is the address of the C2 server located in the Netherlands. Based on this log and search data, the communication that occurs is malware communication to the C2 server with IP Address 185.26.182.109. The following is an infection process reconstruction data based on network logs that describe the behavior of viruses in computer networks, as shown in Table 2.

Table 2 Virus infection network traffic

IP Src.	Prot.	IP Dest.	Info
185.27.134.218	HTTP	192.168.100.68	Downloading Virus
192.168.100.68	TLSv1	185.26.182.109	Virus to C2 server
192.168.100.68	TLSv1	185.26.182.94	Connected C2 server
185.26.182.94	TCP	192.168.100.68	Sending Data
82.145.216.15	TLSv1	192.168.100.68	Handshake
192.168.100.68	SMB2	192.168.100.69	Spreading Virus

Table 2 provides information about the reconstruction of infection attack incidents due to users who accidentally downloaded a malicious file and executed it immediately after the virus tried to contact the C2 server. The table above shows that the virus managed to contact the C2 server using the TLSv1 protocol and connected to the server's IP address, namely 185.26.182.94, then the virus carried out its malicious activities.

The following process in this research is to do malware analysis. This study implements static and dynamic analysis of virus files that have been acquired in the previous network forensics process to enrich knowledge about the behavior of the Conti ransomware virus on computer networks, making it possible to find out the signature of the virus[32].

3.5 Static Analysis

The static analysis stage tests the ssms.bin.zip file obtained from the forensic process to find the virus signature without running it. The following are the results of the file review using Pestudio tools, as shown in Figure 11.

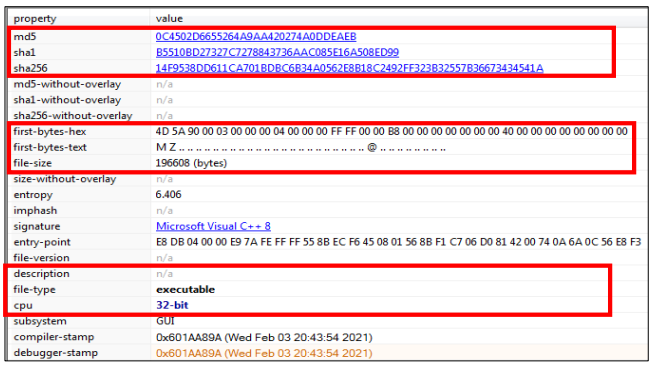


Figure 11. Testing on files

The test results provide signature information on files that include the values md5, sha1, and sha256. The file indicated malware marked with first-bytes-hex "4D 5A", first-bytes-text "M Z", and targeted attacks on Windows OS with file-type executables and has a size of 196.6 Bytes. The attacker targets computers with 32-bit operating systems and has a GUI subsystem; in addition, a signature is obtained from the file indicating that the file uses software Microsoft Visual C++. Further testing on virustotal.com is in Figure 12.

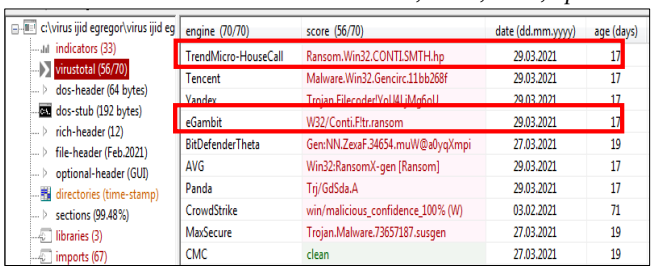


Figure 12. Testing files on virustotal.com

Figure 12 displays information on the results of virus file testing using the Pestudio tool. The tool is connected to the www.virustotal.com website and tests files with 70 antivirus engines with a scanning process. Scan results showed that 56 out of 70 machines indicated that the file was ransomware-type malware, one of the machines determined that the Ransomware was Conti type. Below are the results of an advanced static analysis of the Conti ransomware virus file, as shown in Figure 13.

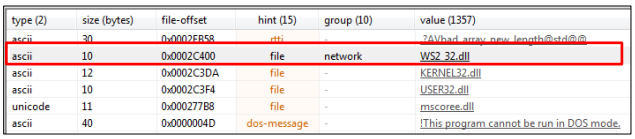


Figure 13. Static analysis results

Figure 13 provides information about the capabilities of the virus that allows extending the infection to other computers by accessing the computer network through the WS2_32.dll library, increasing the escalation using the user32.dll library and the KERNEL32.dll library to access data. The following analysis aims to verify the behavior of the Conti ransomware virus that can spread on computer networks.

3.6 Dynamic Analysis

The subsequent analysis is to perform dynamic analysis by running the type of Conti virus in a virtual environment to identify the behavior of the virus attack on the host computer and obtain a Conti Ransomware analysis with the Network Forensics-Based Behavioral. The following results from a dynamic analysis that captures log files and records virus activity on the host computer, as shown in Figure 14.

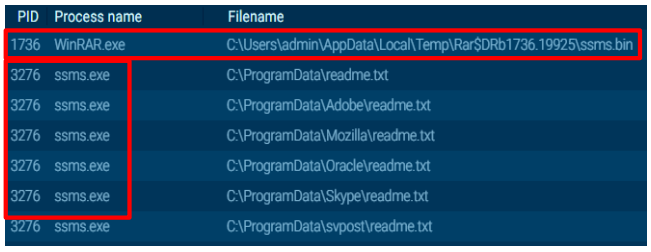


Figure 14. Log virus activity files

The log files in Figure 14. provide information about virus files dropped on the directory address "C:\User\admin\App Data\Local\Temp\Rar$DRb1736.19925\ssms.bin with PID 1736. The virus runs on RAM with PID 3276, and the Process name is ssms.exe, then the virus starts accessing, manipulating, encrypting data, and other malicious actions as in Figure 15.

PID	Process name	Filename
3276	ssms.exe	C:\Users\admin\Desktop\hotelphentermine.rtf.TIYSV
3276	ssms.exe	C:\Users\admin\Desktop\legalplaces.jpg
3276	ssms.exe	C:\Users\admin\Desktop\legalplaces.jpg.TIYSV
3276	ssms.exe	C:\Users\admin\Desktop\plusreceive.png

Figure 15. Log files data encryption

Figure 15 indicates the encryption process performed by the virus against the data with the addition of the extension suffix "TIYSV" in the directory "C:\"; at the same time, this virus immediately performs a deployment to increase the scope of encryption on other computers. Here are the results from dynamic analysis by monitoring and capturing network traffic logs while the virus is running, as shown in Figure 16.

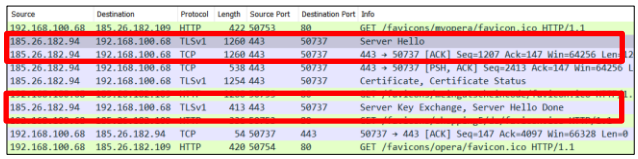


Figure 16. Log malicious connect to C2 server

The log capture in Figure 16 provides information on the occurrence of communication between IP Address 192.168.100.68 on the host computer and IP Address 185.26.182.94, followed by the description "Server Hello", "Server Key Exchange, Server Hello Done", and the header length is 1260 Bytes. The Conti Ransomware virus carried out the communication to contact the C2 server based on the log information. Next is a graph that depicts the behavior of viruses in accessing network protocols, as shown in Figure 17.

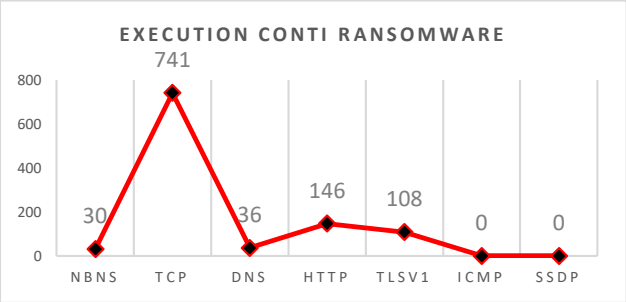


Figure 17. Log network execution Conti Ransomware

Figure 17 shows the behavior of the virus in accessing a computer network to communicate with the C2 server and carry out its malicious actions through the TCP protocol. Viruses use the NBNS protocol to spread infections or find security holes on other computers.

The following is a capture of network traffic logs when the virus spreads infection and encrypts data on other computers on the computer network, as shown in Figure 18.

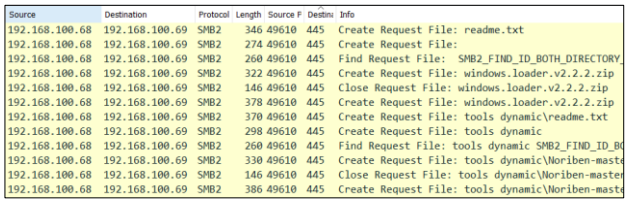


Figure 18. Log malicious attack another computer

Figure 18. shows the attack carried out by the virus via IP Address 192.168.100.68 accessing data on the client computer with IP Address 192.168.100.69 via the SMB2 protocol from port 49610 to port 445. The SMB2 protocol works for sharing and transferring files on the network computer; in this case, the log above shows an improper file transfer. The file transfer process often fails and forms a particular pattern with the message "Close Request", thus triggering suspicion of the process. Based on the network traffic log above, the spread of the virus to other computers uses several network protocols, as shown in the graph in Figure 19.

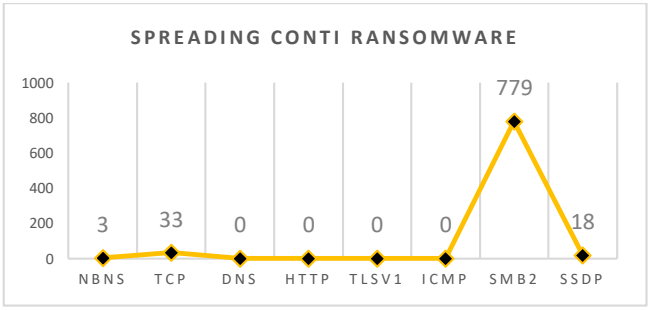


Figure 19. Log network execution Conti Ransomware

Figure 19 provides information on the behavior of the network log generated by the virus when it spreads to other computers on the same computer network by generating access logs on the SMB2 network protocol 779 times. Viruses use network protocols to access, manipulate, encrypt, transmit data and perform other malicious acts. Therefore, accessing the SMB2 protocol requires regular monitoring to minimize malware or ransomware virus attacks.

3.7 Report

This section provides an overall summary of information regarding the signature of a Conti ransomware attack on a computer network based on network forensic behavior and malware analysis. The following is the final result of the static

analysis that finds indicator compromise data (IOCs) as shown in Table 3.

Table 3 Data IOCs

File	Result
sha1	B5510BD27327C7278843736AAC085E16A508ED99
md5	0C4502D6655264A9AA42027A0DDEAEB
sha256	14F9538DD611CA701BDBC6B34A0562E8B18
Size	196.6 Bytess
Type	32-bit executable (GUI)
Drop	C:\User\admin\AppData\Local\Temp\Rar$DRb1736.19...
Source	185.27.134.218/repository/ssms.bin.zip
Signature	Microsoft Visual C++ 8
Library	ws2_32.dll, kernel32.dll, user32.dll
Dec.	Binary for Conti Ransomware

Table 3 shows that the capital for detecting detection and security systems against Conti ransomware virus attacks using IOCs data. The signature file uses IOCs data, namely the hash values of md5, sha1, and sha256. The results of forensic analysis and dynamic analysis in this study indicate that the behavioural signature of the virus attack based on the identification of malicious network traffic from the infected machine, as shown in Table 4.

Table 4 Conti ransomware network traffic

IP Src.	Prot.	IP Dest.	Info
185.27.134.218	HTTP	192.168.100.68	Downloading Virus
192.168.100.68	TLSv1	185.26.182.109	Virus to C2 server
192.168.100.68	TLSv1	104.109.85.142	Virus to C2 server
192.168.100.68	TLSv1	94.100.180.102	Virus to C2 server
192.168.100.68	TLSv1	185.26.182.114	Virus to C2 server
192.168.100.68	TLSv1	52.29.201.5	Virus to C2 server
192.168.100.68	TLSv1	185.26.182.94	Connected C2 server
185.26.182.94	TCP	192.168.100.68	Sending Data
82.145.216.15	TLSv1	192.168.100.68	Handshake Failure
185.26.182.93	TLSv1	192.168.100.68	Handshake
192.168.100.68	SMB2	192.168.100.69	Spreading Virus

Table 4 provides information about Conti ransomware virus infection attacks running on computer networks. The virus immediately contacted server C2 using six different server IP addresses and eventually connected to the IP address 185.26.182.94; this behavior can be used as a network signature for the Conti ransomware virus, as shown in Table 5.

Table 5 Network behavior signature

IP Src.	IP Dest.	Port
185.27.134.218	192.168.100.68	80
185.26.182.109	192.168.100.68	80
104.109.85.142	192.168.100.68	80
94.100.180.102	192.168.100.68	80
185.26.182.114	192.168.100.68	80
52.29.201.5	192.168.100.68	80
185.26.182.94	192.168.100.68	80

Table 5 makes data signatures of Conti ransomware virus network behavior based on forensic network log analysis and dynamic analysis. The detection system development process can then use the network behavior signature data.

4 CONCLUSION

Based on the analysis of Conti ransomware attacks using live forensics and malware analysis methods, we have managed to get a picture of the network behavior signature in the research analysis of The Conti Ransomware attack on computer networks. This research shows that phishing websites can potentially attack computer networks caused by weak security segmentation and ignoring suspicious links. Detection systems using network forensic behavior in network traffic logs require high caution and take a long time. The advantage of using direct forensic methods is to obtain data for immediate analysis and apply malware analysis and enrich knowledge about the characteristics of malware attacks. Suggestions for further research are to build anticipation of Ransomware attacks through offline or online data backup systems and detection systems based on network traffic logs or specific internet protocols.

ACKNOWLEDGMENT

Thank to Universitas Ahmad Dahlan Yogyakarta for the support and facilitation of this research.

REFERENCES

[1] 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, DOI: 10.1109/ISI49825.2020.9280508.

[2] 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, DOI: 10.1109/access.2020.3023764.

[3] 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, DOI: 10.1002/cpe.5422.

[4] Filip Truta, "City of Cartersville Admits Paying Ryuk Ransomware Operators $380,000 - Security Boulevard," *www.securityboulevard.com*, 2020. https://securityboulevard.com/2020/03/city-of-cartersville-admits-paying-ryuk-ransomware-operators-380000/ (accessed January 20, 2021).

[5] Filip Truta, "University of California San Francisco Pays $1 Million to Ransomware Operators after June 1 Attack - Security Boulevard," *www.securityboulevard.com*, 2020. https://securityboulevard.com/2020/06/university-of-california-san-francisco-pays-1-million-to-ransomware-operators-after-june-1-attack/ (accessed January 20, 2021).

[6] 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, DOI: 10.1016/j.procs.2020.09.192.

[7] A. Kurniawan and I. Riadi, "Detection and Analysis Cerber Ransomware Using Network Forensics behaviour-based," *Int. J. Netw. Secur.*, vol. 20, no. 5, pp. 1–8, 2018, DOI: 10.6633/IJNS.201809_20(5).04.

[8] A. H. Mohammad, "Ransomware Evolution, Growth and Recommendation for Detection," *Mod. Appl. Sci.*, vol. 14, no. 3, p. 68, 2020, DOI: 10.5539/mas.v14n3p68.

[9] 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.

[10] Ferdiansyah, "Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware," *JUSIFO (Jurnal Sist. Informasi)*, vol. 2, no. 1, pp. 44–59, 2018, [Online]. Available:

http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf.

[11] C. Manzano, C. Meneses, and P. Leger, "An Empirical Comparison of Supervised Algorithms for Ransomware Identification on Network Traffic," *Proc. - Int. Conf. Chil. Comput. Sci. Soc. SCCC*, vol. 2020-Novem, 2020, DOI: 10.1109/SCCC51225.2020.9281283.

[12] T. P. Setia, A. P. Aldya, and N. Widiyasono, "Reverse Engineering untuk Analisis Malware Remote Access Trojan," *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 40, 2019, doi: 10.26418/jp.v5i1.28214.

[13] R. Umar, I. Riadi, and R. S. Kusuma, "Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TARA) Methods," pp. 197–204, 2021.

[14] A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, "Detecting ransomware using process behaviour analysis," *Procedia Comput. Sci.*, vol. 168, no. 2019, pp. 289–296, 2020, DOI: 10.1016/j.procs.2020.02.249.

[15] 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, DOI: 10.1109/ACCESS.2019.2945839.

[16] N. Hildayanti, "Forensics Analysis of Router On Computer Networks Using Live Forensics Method," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 1, pp. 74–81, 2019, DOI: 10.17781/p002559.

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

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

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

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

[21] A. Liu, H. Fu, Y. Hong, J. Liu, and Y. Li, "LiveForen: Ensuring Live Forensic Integrity in the Cloud," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 10, pp. 2749–2764, 2019, DOI: 10.1109/TIFS.2019.2898841.

[22] R. Umar, A. Yudhana, and M. Nur Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, p. 2951, 2018, DOI: 10.11591/ijece.v8i5.pp2951-2958.

[23] M. KA, *Learning Malware Analysis*. Birmingham - Mumbai: Packt Publishing Ltd., 2018.

[24] 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.

[25] 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, doi: 10.1109/ICACCI.2018.8554938.

[26] 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, DOI: 10.1109/tc.2020.3011214.

[27] M. Ahmed and H. Saeed, "Malware in Computer Systems : Problems and Solutions," vol. 9, no. 1, pp. 1–8, 2020, DOI: 10.14421/ijid.2020.09101.

[28] T. Xia, Y. Sun, S. Zhu, Z. Rasheed, and K. Shafique, "Toward A network-assisted Approach for Effective Ransomware Detection," *arXiv*, Aug. 2020, [Online]. Available: http://arxiv.org/abs/2008.12428.

[29] F. G. Hikmatyar, "for Handling Cybercrime Cases," vol. 7, no. 2, pp. 64–67, 2018.

[30] 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, DOI: 10.1109/ACCESS.2019.2907485.

[31] S. H. Kok, A. Abdullah, and N. Z. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2020, doi: 10.1016/j.jksuci.2020.06.012.

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