Detection And Analysis Cerber Ransomeware Based on Network Forensics Behavior

By Imam Riadi

WORD COUNT 4726 TIME SUBMITTED 16-NOV-2018 08:02AM
PAPER ID 42008837

Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior

Ade Kurniawan[1] and Imam Riadi[2]
(Corresponding author: Ade Kurniawan)
Department of Informatics Engineering, Universal University[1]
Kompleks Maha Vihara Duta Maitreya, Sungai Panas, Batam 29456, Kepulauan Riau, Indonesia
(Email: ade.kurniawan@uvers.ac.id)
Department of Information System, Ahmad Dahlan University[2]
(Received Apr. 3, 2017; revised and accepted July 2, 2017)

Abstract

Kaspersky and other information security firms mentioned 2016 as the year of Ransomware. The impact of attacks has allowed financial damage on the business or individual. The FBI estimates that losses incurred in 2016 will top US$ 3 billion. Meanwhile, cyber criminals use malware: Trojans, Spyware, and Keyloggers, all of which require long tremendous effort to transfer benefits into their bank accounts; while Ransomware makes the process automatic and easy by using a business model of Ransomware as a Service (RaaS). Therefore, Ransomware are made more sophisticated and more effective as to avoid detection and analysis. In this paper, we present a new insight into detection by analyzing Cerber Ransomware using Network-Forensic-Behavioral-Based. This paper is aimed to reconstruct the attack of timestamp, to identify the infected host and malware, to compromise websites involved in the chain of infection, to find campaigns scripts, and to exploit kits and payload Ransomware.

Keywords: Cerber; Detection; Malware; Network Forensic; Ransomware

1 Introduction

A hospital in Los Angeles in 2016 occurred "network infiltration" by disabling the network and computers with Ransomware, cyber criminals demanded a ransom of $ 17,000 to restore the network and computer full of important and confidential information of patients [15]. Ransomware is a type of Malware that restrict access to information by encrypting files and folders with a key is impossible to resolve and the cybercriminal will ask a ransom to unlock access to files and folders [14, 15, 31].

Ransomware is becoming popular among cyber criminals to make money in an easy way [22]. Ransomware has an impact of damage and anxiety to the business characterized by an increased the number of attacks Ransomware statistical average 100-300 percent in 2016 [17, 25, 33] with the report number of incidents increased up to 4000 percent [16]. In 2016 and is estimated in 2017 there was three Ransomware is TeslaCrypt, Locky, and CERBER who rules the world of Ransomware [11, 25]. Now Malware authors create Ransomware more sophisticated, more effective, and using anti forensic to avoid detection and analysis of each commit crimes [3, 26, 32].

Ransomware detection method generally divided into three approaches; Static feature- based, host-based and behavior-based Network Behavior Analysis [8, 19, 27]. Static feature- based widely used by antivirus software and easily avoided by attackers, such as an attacker using packaging techniques or structural change their malware code [4]. Host-behavior-based methods or dynamic analysis where artifacts malware is executed in an environment VM (virtual machine) which also has limitations due to the current Malware can detect a VM environment or host computer [9, 29] and also less capable of detecting new malware samples, and tends to produce false warnings or generate misclassification [19].

Cerber ransomware can infect via several different methods with the impact more damaging and more expensive. General scheme of distribution, spread and infections of ransomware through Network-based such as downloading a file, e-mail phishing, drive-by download or compromised website and others [26, 31] and therefore in this paper, we offer an approach to the detection and analysis Cerber Ransomware with Network Forensics Based behavior Method of because this approach has the ability to identify abnormal traffic patterns during the operation of the network. [18, 30]

Use of the approaches Network Forensic Behavior Based could reconstruct the events of the beginning of a spread, starting with the first infection of CERBER Ransomware on the host computer named STIWIE PC, find the Trojan Godzilla, pseudoDarkleech script as the Campaign to redirect network traffic victim to the server

of exploit kit (EK) and a payload Ransomware used by cyber criminals.

This paper is structured as follows, in Section 2 we describe Ransomware, Cerber, and Network Forensics. In Section 3 we describe Methodology, the hardware, and software used to analyze Cerber Ransomware by using Network Forensics Behavior Based. In Section 4 which is the result of an analysis of the findings of this paper. Section 5 is part of the Conclusion and Future Work.

2 Basic Theory

2.1 Ransomware

Ransomware is a type of malware that restricts access to important information an individual or company with a way to encrypt files and will ask for a ransom payment in exchange for the decryption key to restoring encrypted files [7, 26]. The embryo of ransomware called PC Cyborg started in 1989 by Dr. Joseph Popp [20].

After infection, the PC Cyborg will hide all the file folders and encrypt files on the C: drive. A script message asked for a ransom of $ 189 directed to the PC Cyborg Corporation [26]. The first attack Ransomware uses public key cryptography to incorporate a combination of viruses and Trojan horses called cryptovirus and they called "cryptovirological attacks" [35]. The five phases of ransomware [26] shown in Figure 1:

Figure 1: Five phases of ransomware

The following explanation of the five-phase mentioned above:

Exploitation and infection: Ransomware file needs to be executed on a computer. The spreading process and infection are often carried out through phishing emails or exploit security holes in software applications, for example, Adobe Flash and Internet Explorer.

Delivery and execution: After Exploitation and infection processes, Ransomware executable will be sent back to the victim's system. After executing, the mechanism of this process can take several seconds, depending on network latency. Ransomware is most often executable network deployment through strong encrypted and placed in the folder % APPDATA% or% TEMP% in the user profile.

Back-up spoliation: shortly after Delivery and execution processes, Ransomware will search for a file and folder backup and delete all the files for avoiding the victim that will restore files and folders that have been encrypted. In a Windows system, vssadmin tool delete volume shadow copy of the system, such as cryptolocker Ransomware and Locky will run the command to remove all shadow copies of the system. File encryption; once the file, folder and shadow copy back-up were completely removed, the malware will perform the secure key exchange with the command and control (C2) server, build an encryption key that will only be used on the local system. Ransomware will identify uniquely to each local system to distinguish the strong encryption keys among them using the AES 256 algorithm the encryption process can take anywhere from several minutes to hours depending on network latency, number and size of documents and the number of connected devices.

User notification and clean-up: in this phase extortion requests and payment instructions are presented to the victim. Instructions extortion requests and saved to the hard drive, sometimes the instruction file in the same folder with the encrypted files as an example of CryptoWall version 3 with the file name HELP_DECRYPT.

2.2 Cerber Ransomware

Cerber is one kind of sophisticated malware, with a business model Ransomware as a Service. Emerging Cerber Ransomware about 4 March 2016 in Russia and the spread is usually through botnets, spam emails and drive-by downloads [28]. When it infected, the victim data files are encrypted using AES encryption algorithm and will be notified to the victim must pay a ransom of its ordinary in the form of digital currency such as Bitcoins to receive and access their files get back [5].

Cerber will identify each victim by country, by checking the IP Geolocation country of origin of the victim, if the computer of one of the following countries (Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine, Uzbekistan) will end itself and does not encrypt the computer [24].

After the executed, CERBER will install itself in the folder% AppData% {2ED2A2FE-872C-D4A0-17AC-B01404F1CBA}. Windows configures automatically boot into Safe Mode and the next reboot the network mode Cerber start automatically when the user logs into Windows, to run the screensaver when the system is idle for execute itself every minute and display false alert system until the computer is restarted [2]. To make sure the victim will be begging ransom, Cerber left three notes (# decrypt MY FILES # .html, # decrypt MY FILES

.txt, and # decrypt MY FILES # .vbs) in each folder that has been encrypted.

2.3 Network Forensic

Network Forensics is a branch of Digital Forensics that use proven scientific techniques to collect, to use, to identify, examine, linking, to analyze, and documenting digital evidence from several sources of digital evidence and electronic evidence [1, 21, 23]. Network Forensic very reliable to capture the network traffic to and from one or multiple hosts that can later be revealed channels, methods, and the spread of malicious code [12, 23].

Obstacles often faced by the Network of Forensic investigators are gathering evidence and acceptance are often vague, poorly understood, or lack of evidence. When performing network forensics, investigators often work with a live system (online) that cannot be taken offline. This may include routers, switches, servers and other types of network devices [30].

Forensic evidence gathering for network similar to the collection of digital forensic investigation [10] but digital evidence network-based often highly volatile and should be collected through active ways inherent of evidence gathering system [6, 30].

3 Methodology

Preparation stage starts with the setup of hardware and software that will be used in this study. Hardware used in this study is a Notebook Processor: Intel (R) Core (TM) i7-6500U CPU @ 2.30GHz, 8GB RAM, 250GB SSD, Intel 530 Graphics Card. Software used in this study is Wireshark Version 2.2.5 and dataset from `http://www.malware-traffic-analysis.net/`.

In general, there are three methods for detecting malware: static feature, host behavior, and network-based behavior [7, 30, 32]. Detection methods used in the study Cerber Ransomware is a network-based behavior. Network behavior is to identify traffic patterns that did not occur during normal operation of the network by checking Packet Inspection: checking header, protocol, viruses, spam. Signature Detection: It monitors the content of packets in the network and comparing the pattern of attacks before configuration [23].

Inside the Network Forensics Investigation research, we use OSCAR Methodology (Obtain Information, Strategies, Collect Evidence, Analyze and Report) [30]. Illustration of the Methodology is shown in Figure 2.

Figure 2: OSCAR methodology

3.1 Obtain Information

Two important things that need to be done network forensic Investigator at the beginning of the investigation: to obtain information about the incident itself and get information about the environment. Important points to note regarding the incident is a description of what happened, the timestamp (date, time, and method of the invention of the incident), people involved, systems and data involved, the manager Incident and processes, legal issues, time for investigation/recovery/resolution and Goals.

Social and political dynamics could change during the incident, investigators need to spend some time understand and respond to specific events. The following things about the environment: Business models, Legal issues, network topology, network available sources of evidence, Organizational structure, Incident Response Management Process, Resources available (staff, equipment, funding, and time).

3.2 Strategies

Network Forensics Investigator must work efficiently [18], because of network forensics keeps potential sources of very important evidence, some of which are also very volatile. Strategies points to consider in network forensic is Understanding the purpose the period of the investigation, a list of resources (personnel, time, and equipment), identify possible sources of evidence, to estimate the value and the cost of obtaining the evidence, list prioritizes the acquisition and plans initial acquisition/analysis.

3.3 Collect Evidence

Three essential components that must be done each time the Network Forensic Investigator to obtain evidence: Document, Capture and Store/Transport. Make sure the document keeps a log of all the systems accessible and all actions taken during the collection of evidence, as well as noting the date, time, sources of, methods of acquisition, and the name of the investigator and the chain of custody [23, 30].

3.4 Analysis

The important elements to consider in the Analyze phase is:

- Correlation: The advantages of network forensics involves multiple sources of evidence such as time stamp and other sources of evidence that can be correlated that would become sources of new evidence.
- Timeline: Once a data source is some evidence has been collected and correlated, we are building a timeline of activities, recount comprehension who is doing what, when, and how the basis of the case.
- Events of Interest: Certain events will stand out, potentially more relevant than another event. Network

forensics investigator must isolate events of interest and search for to understand how it happened.

- Interpretation: The necessary expertise to identified potential sources of additional evidence and build a theory of possible events. It is most important that you separate your interpretation of the evidence of the fact. Your interpretation of evidence always hypotheses, which can be proved or disproved.

3.5 Report

Reporting the most important aspect of the investigation, any Network Forensic report must be attention to the following points:

- Conceived by non-technical layman: Legal Team, Manager, Human Resources Personnel;
- Delivered detailed and structured;
- Factual.

In short, should be able to explain the results of an investigation is unreasonable to non-technical people, while retaining scientific principles.

4 Result

In our research focus is on the side of the detection and analyze. Obtain Information from this study suspected of infection and spread of Ransomware in a corporate environment via a Network. Phase Strategies the company before infected with malware is to installing packet capture tools to capture every traffic if an illegal act when there is either an attack from the inside or from the outside that later can become digital evidence to support the forensic measures if there is a violation of the law. The dataset for research using sample data from `http://malware-traffic-analysis.net/index.html`, file format packet capture (PCAP) with a filename 2017-01-28 traffic-analysis.pcap file size 3,173 KB.

4.1 Analysis

Timestamp in the digital forensic very important role because it contains information related to the show in a condition when or time [1]. Detection and forensic analysis using Wireshark Network with filter HTTP.request first thing to do is to determine when the first time the host computer is infected, show in Figure 3 shows the first time an infected computer is on time 2017-01-27 22:53:54 UTC or January 28, 2017 05:53:54 SE Asia Standard Time.

After knowing the date and time of the infection the next phase is to detect and analyze the IP and the hostname of the computer has been infected. IP detection, MAC Address Hostname and NetBIOS analysis performed by using filter NBNS. NetBIOS is an application which allows a computer to communicate with computers

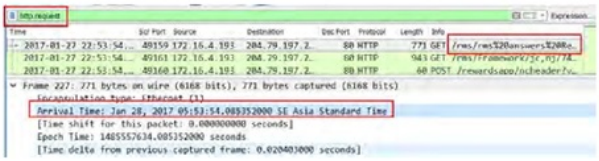

Figure 3: Date and time of the infection

on the Local Area Network (LAN). Analysis of IP and MAC address of who the victims were first the infected show in Figure 4, IP Host Computers infected victims is 172.16.4.193 with MAC Address 5c: 26: OA: 02: a8: e4 the network card from hardware vendors Dell and with Host Stewie name PC.

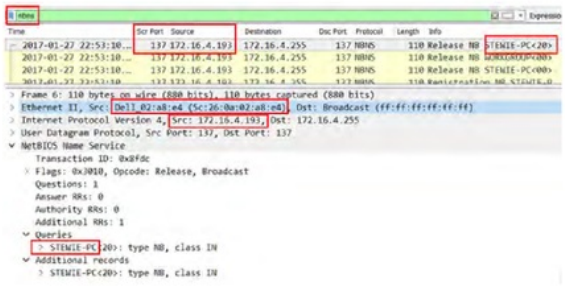

Figure 4: NBNS traffic analysis in wireshark

IP, MAC Address and hostname we already know, the next phase determine malware which infects the host name of the Stewie PC. After deep analysis of several packet shown in Figure 5 traffic to the domain.top, usually malware author used domain.top in conducting criminal activities. List Domain [13] which is generally used is Domains lclebb6kvohlkcml.onion [.] link lclebb6kvohlkcml.onion [.] nu bmacyzmea723xyaz.onion [.] link bmacyzmea723xyaz.onion [.] nu nejdtkok7oz5kjoc.onion [.] link nejdtkok7oz5kjoc.onion [.] nu.

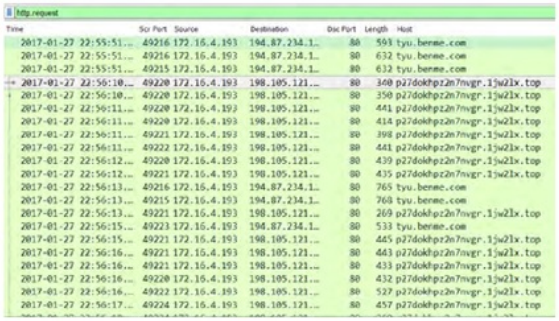

Figure 5: Information gathering

From result analyze was we found that the domain

used by cyber criminals, with the aid the Google search engine with the keywords p27dokhpz2n7nvgr.1jw2lx.top. Google.com search results show in Figure 6 describes found malware which infects PCs Stewie is CERBER Ransomware.

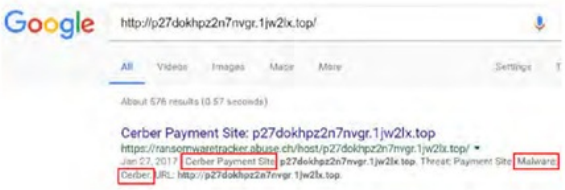

Figure 6: Result p27dokhpz2n7nvgr.1jw2lx.top

In Figure 7, we show the result of PCAP that has been uploaded to https://www.virustotal.com alert shows the results of Suricata that display found an actor/cybercriminal Cerber used RIG EK (Exploit Kit).

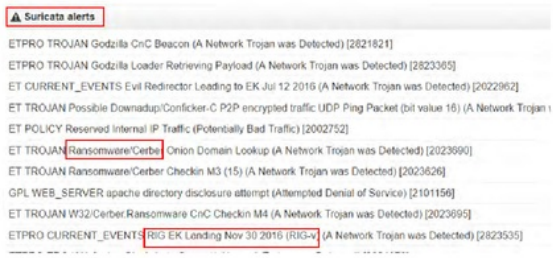

Figure 7: RIG exploit kit landing

Another scenario when the pcap file is ran on Snort as shown in Figure 8 RIG exploit kit landing page has detected. Exploit Kit (EK) is a server-based framework, exploitation by taking advantage of vulnerabilities in a software application that usually associated web browser and infects the victim without realizing have been infected. RIG EK is a gateway delivery and distribution of malware that functions direct the victim to execute a malware payload.

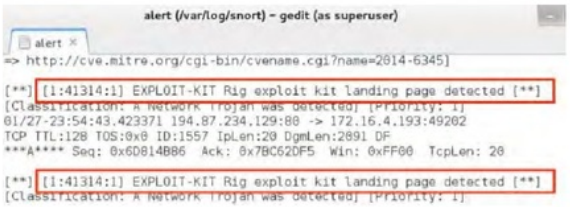

Figure 8: Snort result

In Figure 9 shows the result of the filtering http.request and ip.addr eq 194.87.234.129 that shows the IP address associated with Rig EK. In general, the spread of Ransomware using two methods: first through malicious spam (mail spam) and Exploit Kit. Malicious spam (mail spam) is a way of spreading and distribution directly to a ransomware victims to enter the link that has been infected with malware and takes an active part on the victim to click a link or attachment files that have been injected malware. The second method is to use exploits Kit. Exploits Kit (EK) is designed to work behind the scenes, which is used by cyber criminals to automate the exploitation of security holes in the victim's machine when it is active browsing [34]. EK does not require such active actions of the victim clicks on a link or attachment.

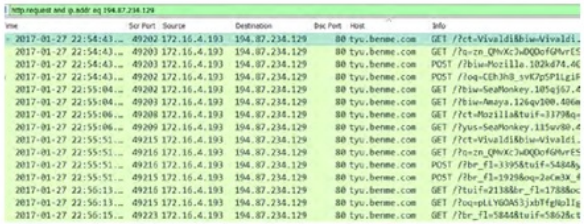

Figure 9: HTTP requests to the rig exploit kit internet protocol address

Filtering of HTTP requests on all IP addresses EK Rig in Wireshark, phase detects and analyze RIG EK and the website domain that mediates the spread of and infection of the host computer by way of the Following TCP Stream the packet as shown in figure 10. Following the results of the TCP stream shows the result found host computer is a www.homeimprovement.com address. From analysis of known victims access to bing.com is doing a search with keywords "remodeling your kitchen cabinets" in the address Referrer: `http://www.bing.com/search?q=home+improvement+remodeling+your+kitchen\&qs=n\&sp=-1\&PQ=homeimprovement+++yourremodeling`

Figure 10: Follow HTTP stream to find referrer

From result analyze www.homeimprovement.com been compromised website in spreading RIG EK. RIG EK is a sophisticated delivery method, the system for distributing malware via EK involves many other components in the chain of events malware infection. Basically, RIG EK with various tricks to direct traffic to the server EK users before sending malware. Actors used campaigns to guide

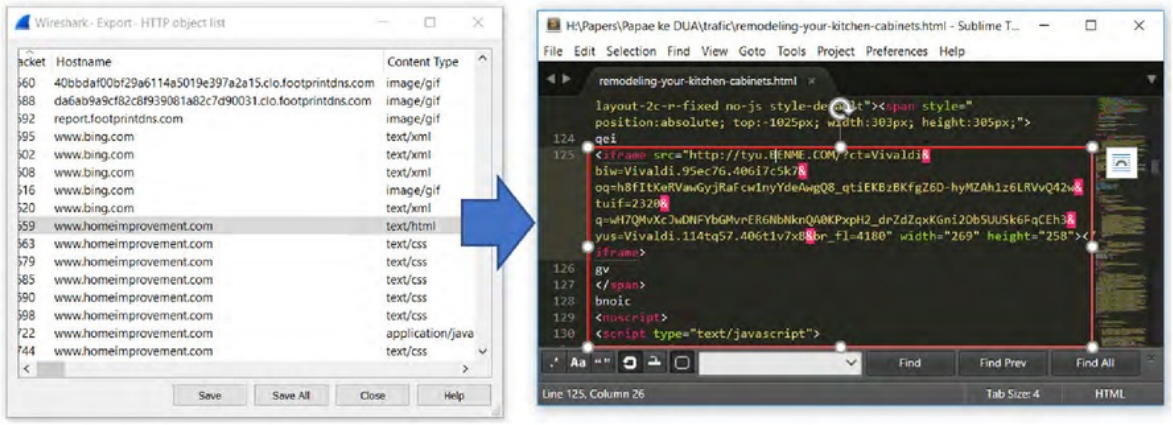

Figure 11: Export object list and pseudoDarkleech script

traffic to the victim server EK. Actors and campaigns two different terms, an actor may use one or several campaigns to distribute malware. One actor may have used the same campaigns to distribute various types of malware. The next stage was to determine the campaign's script used to deliver Cerber is a way to export object in the packet capture as shown in Figure 11.

PseudoDarkleech is a commonly used campaigns Cerber author, function to redirect traffic from the victim to Exploit Kit server with a stealth mode. The pseudoDarkleech script has the task of injecting web pages and a web server through on the root level.

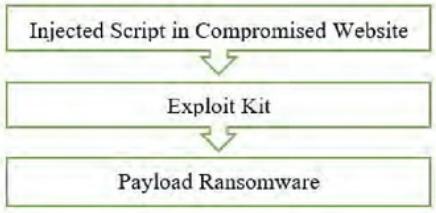

Figure 12: Chain of events pseudoDarkleech campaign

Explanation chain of events is as follows pseudoDarkleech campaign shown in Figure 12:

1) The first victim visits a website (compromised website) that have been compromised or malicious scripts injected and malicious script from compromised websites to make an HTTP request on Exploit Kit Landing Page.

2) Landing page EK finding and determine whether the computer has vulnerability are usually browser-based applications and Adobe flash player and furthermore sending EK Exploit to take advantage of the vulnerable application.

3) If the exploit is successful, EK sending payload Ransomware and carry out activities to access and encryption of files and folders unnoticed, the victim completely have been infected by the payload Ransomware.

5 Conlusion and Future Work

The use of Network Forensic Behavior Based successfully detect and analyze Cerber Ransomware as through the reconstruction Cerber Ransomware chain of events as shown in Figure 13.

Figure 13: Chains of event

Started from the host computer named STIWIE PC, the victim then performs a search on a search engine bing.com for the referral advice from search engine bing.com STIWIE visits www.homeimprovement.com PC. Website analysis shows the results found have been injected by cyber criminals/actors of making the site into a Compromised Websites for the Campaign. The analysis phase detected Campaign successfully used pseudoDarkleec script to redirect a victim to the server by using RIG Exploit Kit EK to download a malware payload that named CERBER Ransomware for future work required Network Forensic deep on the side of compromised websites and Exploits Kit server. Exploit Kit is currently in delivery has encrypted binary code that has made it harder to be detected and analyzed.

Furthermore, the suggestion to users to stay updated browser application and patch vulnerability because the weakest point in the security chain is the human being, the solution is to strengthen the end point in a human side to build "Human Firewall".

References

[1] K. de, R. Imam, and L. Ahmad, "Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (owasp) framework," *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 6, pp. 1363–1371, 2017.

[2] A. Alexander and C. Anders, "The state of ransomware, trends and mitigation techniques," in *IEEE East-West Design*, 2017.

[3] A. A. Ali and Z. N. A. Kamarul, "Attack intention recognition: A review," *International Journal of Network Security*, vol. 19, no. 2, pp. 244–250, 2017.

[4] L. Andy, C. Armour, and B. pearce. Jack, "Ransomware becomes the most prevalent form of malware and hits an ever-wider range of victims," *Network Security*, vol. 2017, no. 2, pp. 1–2, 2017.

[5] P. Athina and K. Vasilios, "Differential malware forensics," *Digital Investigation*, vol. 10, no. 4, pp. 311–322, 2013.

[6] I. Baca, J. Cosic, Z. Cosic, "Forensic analysis of social networks (case study)," in *Proceedings of 33rd International Conference on Information Technology Interfaces*, pp. 219–223, 2013.

[7] I. Cabaj and W. Mazurczyk, "Using software-defined networking for ransomware mitigation: the case of cryptowall," *IEEE Network*, vol. 30, no. 6, pp. 14–20, 2016.

[8] K. Clemens, C. PaoloMilani, and K. C. and, "Effective and efficient malware detection at the end host clemens," in *Proceedings of the 18th Conference on USENIX Security Symposium*, pp. 70–82, 2011.

[9] P. Ebenezer and A. Aderemi, "Efficient feature selection technique for network intrusion detection system using discrete differential evolution and decision tree," *International Journal of Network Security*, vol. 19, no. 5, pp. 660–669, 2017.

[10] C. Eoghan, *Digital Evidence and Computer Crime*, Elsevier Academic Press, 2011.

[11] S. Gordon, "Malvertising hits dating websites," *Network Security*, vol. 2015, no. 9, p. 2, 2015.

[12] R. Imam, E. Jazi, A. Ahmad, and Subanar, "Log analysis techniques using clustering in network forensics," *International Journal of Computer Science and Information Security*, vol. 10, 2013.

[13] S. James, S. Drew, and S. Visiting, *Cerber & KeRanger: The Latest Examples of Weaponized Encryption*, Institute for Critical Infrastructure Technology, 2016.

[14] N. Khoa, T. Dat, M. Wanli, S. Dharmendra, "An approach to detect network attacks applied for network forensics," in *11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD'14)*, pp. 655–660, 2014.

[15] M. Labs, *Understanding Ransomware and Strategies to Defeat it*, Technical Report 1, Dec. 2016.

[16] M. Labs, *Mcafee Labs Threats Report*, Technical Report 1, Jan. 2017.

[17] MalwareBytes, *State of Malware Report*, Technical Report 1, Jan. 2017.

[18] M. H. Mate, S. R. Kapse, "Network forensic tool - concept and architecture," in *Fifth International Conference on Communication Systems and Network Technologies*, Apr. 2015.

[19] Z. Mohd, S. Shahrin, A. M. Faizal, S. S. Rahayu, and H. C. Yun, "A comparative study on feature selection method for n-gram mobile malware detection," *International Journal of Network Security*, vol. 19, pp. 1–7, 2017.

[20] Monika, Z. Pavol, and L. Dale, "Experimental analysis of ransomware on windows and android platforms: Evolution and characterization," *Procedia Computer Science*, vol. 94, pp. 465–472, 2016.

[21] B. Nadia, K. Mohamed, Z. Khaled, and B. Chafika, "Iwnetfaf: An integrated wireless network forensic analysis framework," in *Cybersecurity and Cyberforensics Conference (CCC'16)*, pp. 35–40, 2016.

[22] P. A. Networks, *Exploit Kit Getting in Any Means Neccasary*, Technical Report 2, June 2017.

[23] E. S. Pilli and R. C. Joshi, *Fundamentals of Network Forensics*, Springer, 2016.

[24] R. Pratyush and K. Prabhakar, "Network detection of ransomware delivered by exploit kit," *ARPN Journal of Engineering and Applied Sciences*, vol. 12, no. 12, pp. 3885–3889, 2017.

[25] A. Rab, A. Neville, A. Anand, *et al.*, *Ransomware and Businesses 2016*, Technical Report 1, July 2016.

[26] B. Ross, "Ransomware attacks: Detection, prevention and cure," *Network Security*, vol. 2016, no. 9, pp. 5–9, 2016.

[27] A. Saeed and S. Paul, "Optimised malware detection in digital forensics," *International Journal of Network Security*, vol. 6, no. 1, pp. 01–15, 2014.

[28] G. S. Sanjay and K. Kamalanathan, "Understanding and defending crypto-ransomware," *ARPN Journal of Engineering and Applied Sciences*, vol. 12, no. 12, pp. 3920–3925, 2017.

[29] D. Sanjeev, L. Yang, Z. Wei, and C. Mahintham, "Semantics-based online malware detection: Towards efficient real-time protection against malware," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, 2016.

[30] D. Sherri and H. Jonathan, *Network Forensics: Tracking Hackers Through Cyberspace*, Prentice Hall, 2012.

[31] E. Ti "Ransomware: Threat and response," *Network Security*, vol. 2016, no. 10, pp. 17–19, 2016.

[32] S. Toshiki, Y. Takeshi, A. Mitsuaki, C. Daiki, and Y. Takeshi, "Efficient dynamic malware analysis based on network behavior using deep learning," in *IEEE Global Communications Conference (GLOBECOM'16)*, pp. 1–7, 2016.

[33] M. I. Trend, *Trendlabs SM 2016 1H Security Roundup*, Technical Report 1, Jan. 2017.

[34] L. Yassine and S. E. Mamouna, "An approach to detect network attacks applied for network forensics," in *International Conference on Cyber Security And Protection Of Digital Services*, pp. 1–10, 2017.

[35] A. Young and M. Yung, "Cryptovirology: extortion-based security threats and countermeasures," in *IEEE Symposium on Security and Privacy*, vol. 5111, pp. 129–140, 1996.

Biography

Ade Kurniawan received his Masters degree in Digital Forensic in 2014 from Universitas Islam Indonesia. He is currently lcturer Department of Informatics Engineering of Universal University. His research interests include Computer, Network Security, and Digital Forensics.

Imam Riadi is an Associate Professor, Department of Information System, Ahmad Dahlan University. Received his PhD Degree in Faculty of Sciences from the Universitas Gadjah Mada. His research interest includes computer security, Network Forensic, and Data Minning.

Detection And Analysis Cerber Ransomeware Based on Network Forensics Behavior

ORIGINALITY REPORT

6%

SIMILARITY INDEX

PRIMARY SOURCES

1	Sajad Homayoun, Ali Dehghantanha, Marzieh Ahmadzadeh, Sattar Hashemi, Raouf Khayami. "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence", IEEE Transactions on Emerging Topics in Computing, 2017 Crossref	54 words — 1%
2	www.jatit.org Internet	48 words — 1%
3	researchcenter.paloaltonetworks.com Internet	43 words — 1%
4	David J. Marchette. "Computer Intrusion Detection and Network Monitoring", Springer Nature America, Inc, 2001 Crossref	22 words — < 1%
5	www.net-engineering.com Internet	21 words — < 1%
6	mdpi.com Internet	21 words — < 1%
7	Martin Husak, Jana Komarkova, Elias Bou-Harb, Pavel Celeda. "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security", IEEE Communications Surveys & Tutorials, 2018 Crossref	19 words — < 1%
8	Taniza Binti Tajuddin, Azizah Abd Manaf. "Forensic investigation	

	and analysis on digital evidence discovery through physical acquisition on smartphone", 2015 World Congress on Internet Security (WorldCIS), 2015 Crossref	18 words — < 1%
9	www.plati.com Internet	12 words — < 1%
10	ijcsit.com Internet	9 words — < 1%
11	Jana Uramova, Pavel Segec, Marek Moravcik, Jozef Papan, Tomas Mokos, Marek Brodec. "Packet capture infrastructure based on Moloch", 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2017 Crossref	9 words — < 1%
12	Adarsh S. V. Nair, Beegom A. S. Ajeena. "A Log Based Strategy for Fingerprinting and Forensic Investigation of Online Cyber Crimes", Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing - ICONIAAC '14, 2014 Crossref	9 words — < 1%
13	Toshiki Shibahara, Takeshi Yagi, Mitsuaki Akiyama, Daiki Chiba, Takeshi Yada. "Efficient Dynamic Malware Analysis Based on Network Behavior Using Deep Learning", 2016 IEEE Global Communications Conference (GLOBECOM), 2016 Crossref	8 words — < 1%
14	Alejandro Martin, Julio Hernandez-Castro, David Camacho. "An in-depth study of the Jisut family of Android ransomware", IEEE Access, 2018 Crossref	8 words — < 1%
15	Zhu, Shui Jin. "Drinking Water Quality Status and Contamination in Pakistan.(Report)", BioMed Research International Publications	7 words — < 1%
	"Computer and Network Security Essentials", Springer Nature,	

16 2018
Crossref

6 words — < 1%

EXCLUDE QUOTES OFF
EXCLUDE BIBLIOGRAPHY OFF
EXCLUDE MATCHES OFF