Journal of Computer Engineering, Electronics and Information Technology (COELITE)

Journal homepage: https://ejournal.upi.edu/index.php/COELITE

Investigation of Cyber Malware Attacks On Server Networks Using SIEM Method Based On NIST 800-61

Ali Muhammad[1], Budi Jejen Zaenal Abidin[2], Yolanda Putri Yani[3], Nurul Widyastuti[4], Angge Firizkiansah[5], Miri Ardiansyah[6]*

[1,5]Departement of Informatics Engineering, Universitas Sains Indonesia, Bekasi, Indonesia
[2,3,6]Departement of Information Systems, Universitas Sains Indonesia, Bekasi, Indonesia
[4]Kementerian Agama, Indonesia
Correspondence E-mail: ali.muhammad@lecturer.sains.ac.id

ABSTRACT

The growth of cyber threats, especially malware attacks on servers, has increased significantly and is increasingly complex. These attacks can cause huge losses regarding data confidentiality, system integrity, and service availability. Slow and unstructured handling of security incidents can worsen the impact. This research aims to develop an efficient detection and response system to malware attacks, especially on servers that are the main targets of cyberattacks. This research uses a systematic and responsive approach using the NIST 800-61 Rev 2-based SIEM (Security Information and Event Management) framework in handling cyber incidents. The SIEM framework enables an investigation or digital forensics process that includes monitoring, correlating, and analyzing incidents. Meanwhile, NIST 800-61 Rev 2 aims to analyze the investigation process or digital forensics of cybercrime cases and generate digital evidence. The results of this study show that malware cyberattacks tend to be silent and do not show any anomalies on the server. Digital forensic evidence is presented to detect the veracity of a malware attack.

ARTICLE INFO

Article History:
Submitted/Received 02 Jul 2025
First Revised 11 Aug 2025
Accepted 29 Sep 2025
First Available online 01 Oct 2025
Publication Date 01 Oct 2025

Keyword:
Cyber Attack,
Malware,
Phishing,
SIEM NIST 800-61 Rev 2.

1. INTRODUCTION

In an increasingly advanced digital era, server networks are one of the main foundations in managing information and operating organizational systems, both in the government, education, health, and financial sectors. The development of this technology provides many conveniences, but it also opens a gap for cybersecurity threats, especially malware attacks. Malware is malicious software designed to damage, infiltrate, or steal data from computer systems and networks. It can take the form of viruses, trojans, worms, spyware, ransomware, and adware [1][2][3][4][5]. Malware cyberattacks have increased significantly every year, both in terms of number and complexity. In Indonesia, malware-based cyberattacks have targeted various sectors, including educational institutions, hospitals, and financial and service companies [4]. Many of these attacks are not detected early due to limitations in monitoring systems as well as a lack of awareness and preparedness from network managers. Therefore, early detection of malware is a crucial aspect of maintaining digital infrastructure security.

One of the evolving methods for dealing with cybersecurity incidents is the National Institute of Standards and Technology (NIST) approach that offers a systematic framework for responding to security incidents. SIEM (Security Information and Event Management) is a technology that supports incident detection and response in real time by combining log analysis, data correlation, and system monitoring [6][7][8][9]. Meanwhile, NIST Guide 800-61 Rev 2 provides a structural approach to handling incidents such as malware attacks, which includes four main stages: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity [4][10]. The application of the NIST 800-61 Rev 2 method integrated with the SIEM system is expected to detect and analyze malware attacks more effectively and efficiently. With SIEM technology, organizations can gain comprehensive visibility into network activity and proactively identify indications of attacks.

Much research has been conducted in the domain of digital forensics and network security, including malware investigations and system hacking. However, most of these studies have focused on the static analysis aspect and have not integrated the NIST incident response method thoroughly. For example, Kurniawan & Riadi examined Cerber ransomware analysis but only focused on network behavior without compiling a complete incident response flow [5]. Firmansyah's research presents forensic analysis on virtual routers using the NIST approach, but has not incorporated a SIEM-based approach to strengthen detection in real time [11][12][13]. Similarly, Ramadhan studied ARP poisoning attacks using the NFGP model, but focused on post-mortem analysis and Quality of Service measurement, rather than early detection [6][14][15][16].

Other research, such as by Azmi & Deris, uses the Deep Packet Inspection (DPI) approach to detect ransomware, but the approach is technical and has not been structured in a standard framework such as NIST. This shows that there is still a void in research that combines the NIST 800-61 Rev 2 framework with SIEM capabilities as an automated detection and response system to malware [1][16][17][18]. This research can be used as a foundation for building a malware detection and response system that is able to identify threats quickly and accurately with the support of standard frameworks and advanced technology. Given that modern malware is increasingly sophisticated in tricking traditional security systems, early detection and forensic analysis based on the NIST 800-61 Rev 2 framework is crucial. According to Amsor, digital forensics plays an important role in law enforcement in the digital

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

realm, but it will only be effective if the forensic system is able to identify and secure digital evidence from the beginning of an incident [19][20][21][22].

Conventional malware detection systems often function only reactively. The addition of SIEM capabilities in incident management can help perform automated detection, log evidence collection, and in-depth data correlation [23][24][25][26]. As stated by Butarbutar, the implementation of the NIST framework has proven effective in structuring the stages of network forensics, but it needs to be optimized with a system capable of analyzing network traffic in real time [10][27]. In addition, Nofiyan's research shows that the use of NIST methods for phishing forensic analysis can help investigate attack patterns [7][28][29]. However, the approach is still manual and has not been integrated with SIEM technology. Use of SIEM This research is the main differentiating aspect that strengthens the urgency of the research, because in addition to adopting standard forensic methods, this research also addresses challenges in the effectiveness of actual malware detection.

Investigating malware cyberattacks is very important because malware is malicious software specifically designed to damage, infiltrate, or steal data and confidential information from computer systems and networks. This research aims not only to detect and analyze malware cyberattacks. But also to present forensic evidence that can be used as a reference for policy makers in securing confidential data and information, both from within computer systems and through networks.

2. METHODS

This research uses a systematic and responsive approach using the SIEM (Security Information and Event Management) framework based on NIST 800-61 Rev 2. The steps of this research are as follows, as shown in **Figure 1**:

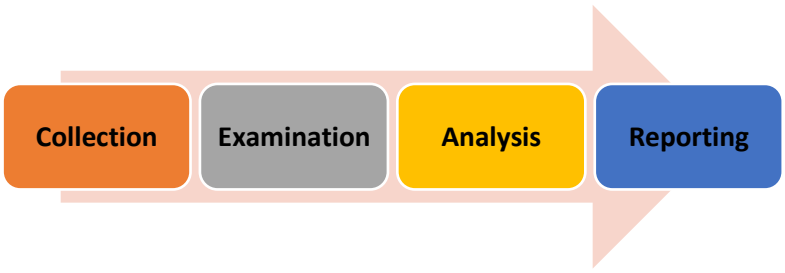

Figure 1. Research Stages Using the NIST Method

2.1. Data Collection

Collecting data on malware attacks is done by handling evidence and the digital evidence acquisition process. Evidence handling is the process of separating digital evidence on malware attacks from other attack evidence processes. In this process, malware attack data is labeled according to the standardization set in an organization/company. This labeling process is used to facilitate the forensic investigation stages that will be carried out. Next, the data will be moved to the storage location. This moving process is called the digital evidence acquisition process. The digital evidence acquisition process is carried out by moving log files or records of malware attack activity to a predetermined storage medium. The process of retrieving malware attack activity records can be done live forensically. Live forensic is a process of retrieving malware attack data that is carried out while all networks and systems are running, as shown in **Figure 2**.

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

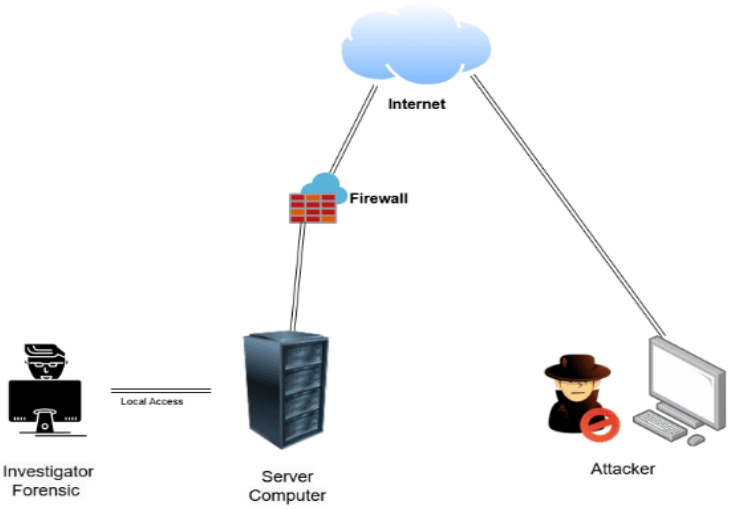

Figure 2. Network Investigation Acquisition Process

2.2. Examination

In the investigation process, forensic investigators examine log files or records of attack activity that are investigated as anomalies in malware attacks on a system or network. This investigation process can be done and identified early through the Wireshark application. In contrast to DoS (Denial of Service) attacks, which can be identified directly by the compaction of traffic or network traffic that is different from usual. Malware cyberattacks tend to be silent and require special expertise in the utilization of in-depth forensic tools.

2.3. Analysis

The analysis in this study uses SIEM or Security Information and Event Management based on NIST 800-61 Revision 2 from the National Institute of Standards and Technology. SIEM or Security Information and Event Management is a comprehensive approach to managing information security and identifying with a response to security threats. SIEM combines technology and identification processes in collecting resources, analyzing an activity log on a network, and reporting security data from various sources, including logs, network devices, software, and the use of applications or other software on both desktop, mobile, and virtual devices.

NIST 800-61 Revision 2 is the best forensic investigation guide published by the National Institute of Standards and Technology to keep an organization or company able to effectively and efficiently maintain and handle data and information leaks. Data and information leaks can result in security incidents, either from malware attacks or other cyberattacks that disrupt the course of business processes in an organization or company, as shown in **Figure 3**.

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

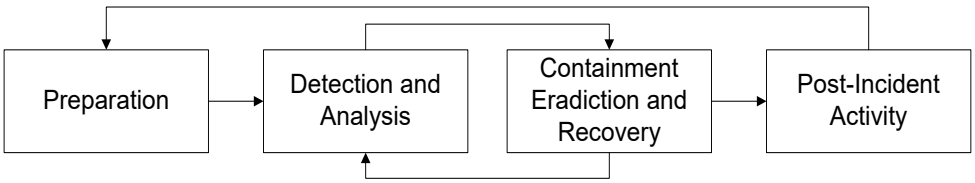

Figure 3. Stages of Network Forensic Analysis Using the SIEM Method Based on NIST 800-61 rev 2

The steps of the SIEM method based on NIST 800-61 Rev 2 are as follows:

1. Preparation

Preparation is an investigative process to identify the resources and personnel involved in responding to a data and information security incident, as well as the development of an incident response plan. The forensic investigator determines the incident response plan regarding the steps to deal with a malware attack.

2. Detection and Analysis

Detection and Analysis is a stage that involves detecting and collecting information about information security incidents that occur. Forensic investigators use a variety of forensic tools to detect malware attacks and analyze malware attacks.

3. Containment, Eradication, and Recovery

Containment, Eradication, and Recovery is the process of reacting to the detection and evaluation of malware/ransomware, which involves containment of the incident, eradication of the cause of the incident, which is malware, and recovery of information systems and data. This stage guides the forensic investigator in determining the appropriate mitigation in dealing with the attack. If at this stage no mitigation can be found, the process will return to the previous stage, namely the Detection and Analysis stage. Then continue to enter this stage again. The Detection and Analysis stage and the Containment, Eradication, and Recovery stage will continue to repeat until they find mitigation or anomalies that occur on the network.

4.Post-Incident Activity

Post-Incident Activity is the process of analyzing the incident response to identify any areas for improvement, as well as updating the incident response plan and training personnel. At this stage, the forensic investigator creates a report on the ransomware/malware attack and conducts an evaluation to safeguard the system and avoid another malware/ransomware attack.

2.4. Reporting

The reporting stage is the process of presenting the results of the analysis that has been carried out on malware cyberattack records. Findings and analysis related to evidence of malware cyberattack records in detail are attached to this reporting document.

3. RESULTS AND DISCUSSION

This research uses network investigation data released by malware traffic analysis with the code 2017-01-28. The identification results are:

3.1. Victim Computer Detection (Forensic Investigator)

The results of the identification of information on the victim's computer or the computer used by the forensic investigator are as follows described in **Table 1**:

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

Table 1. Victim Computer Description

Identification Name	***Computer on Log File***
IP Address	172.16.4.193
Host Name	Stewie_PC
MAC Address	5c:26:0a:02:a8:e4
Windows User Account Name	STEWIE-PC

3.2. Network Traffic Identification

The network evaluation results in the log file code 2017-01-28 do not show any anomalies or attacks that burden the network with the presence of large-scale data or information transmission. The results of the investigation of network traffic that looks normal can be seen in **Figure 4** below.

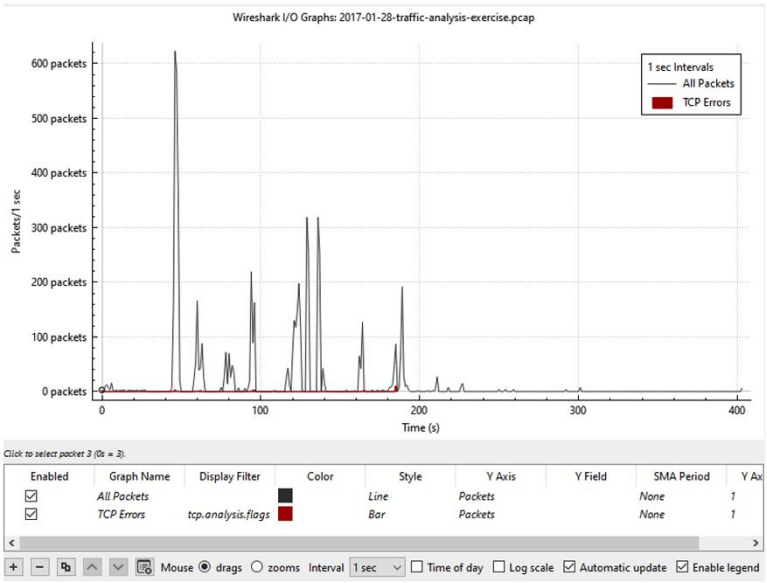

Figure 4. Network Traffic Investigation Results

3.3. Malware Identified in Wireshark Application

Malware detection can be done through the Wireshark application. Filter data using HTTP. request. Suspicious activity usually comes from domains with unusual endings, such as [dot] top. In **Figure 5**, it is explained that the anomalous data in the log file code 2017-01-28 can be p27dokhpz2n7nvgr.1jw2lx.top and several other files.

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

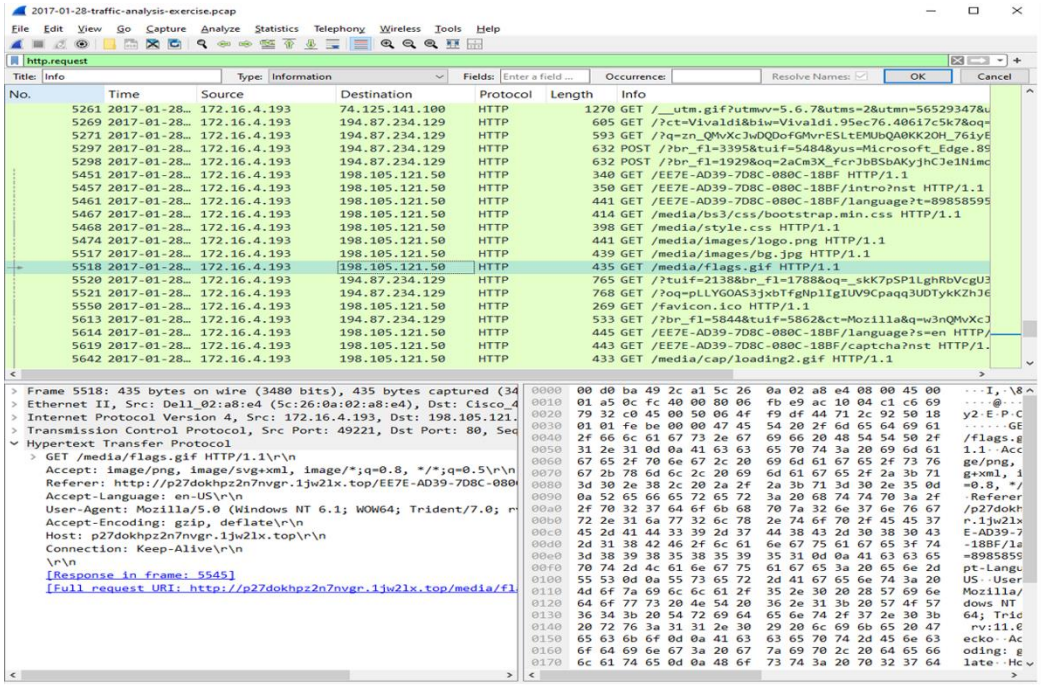

Figure 5. Anomaly Detection in Wireshark Application

3.4. Malware, Ransomware, and Trojans Identified on Any Run App

Checking using any run application obtained information that the log file code 2017-01- 28 contains the domain p27dokhpz2n7nvgr.-1jw2lx.top. This domain is a domain associated with Cerber malware, ransomware, and trojans as shown in **Figure 6**.

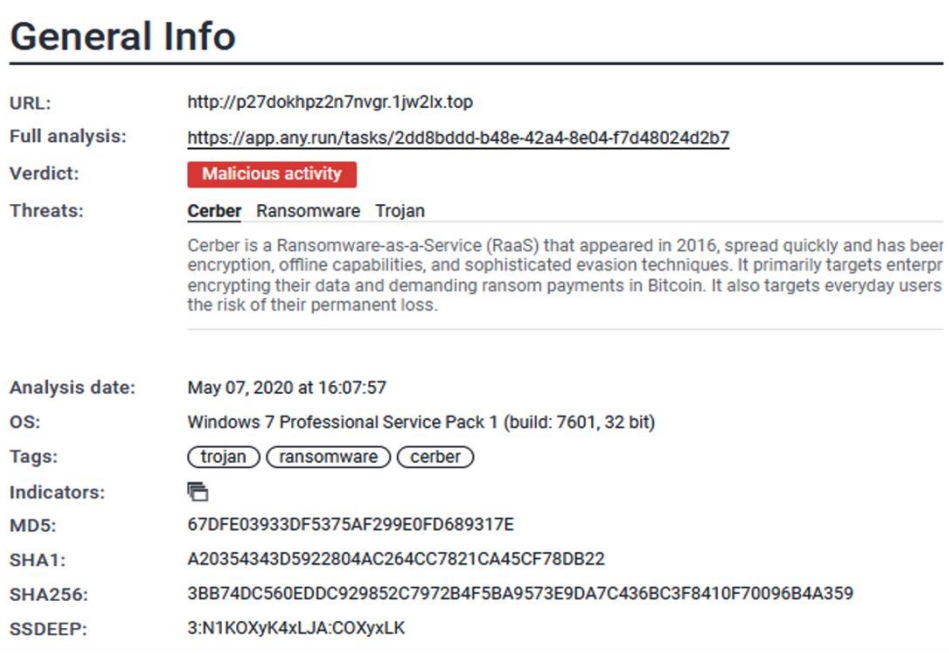

Figure 6. Any Run Application Testing Results

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

3.5. Ceber Ransomware Identified in Hybrid Analysis Application

Another test on the log file code 2017-01-28 was using the hybrid analysis application. The test results show that p27dokhpz2n7nvgr.-1jw2lx.top is a domain containing Cerber and ransomware with a threat score of 100/100 and AV Detection of 30%. However, BforeAI analysis shows that the domain is clean and 0% of malware. The results of the investigation and analysis with the hybrid analysis application can be seen in **Figure 7**.

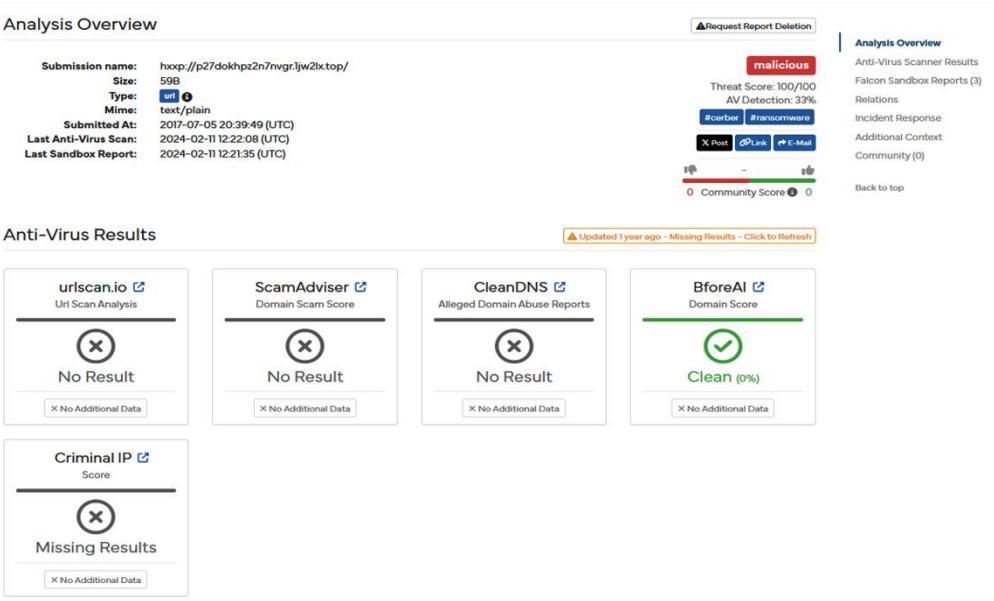

Figure 7. Results of Investigation and Analysis of Hybrid Analysis Application

But Falcon Sandbox has another report. Falcon Sandbox reports that the domain p27dokhpz2n7nvgr.-1jw2lx.top is malicious. Repot's Falcon Sandbox analysis can be seen in **Figure 8** below.

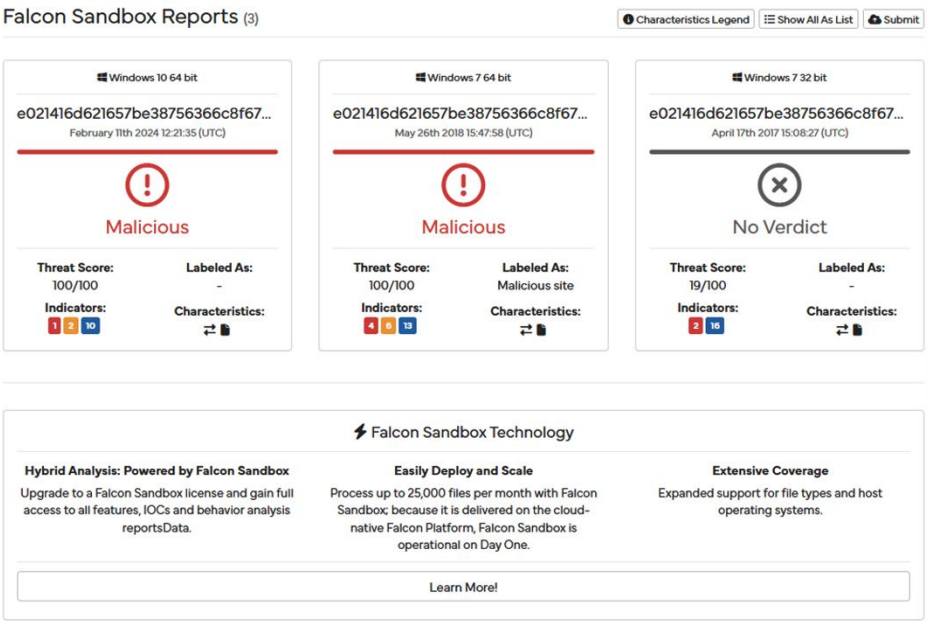

Figure 8. Falcon Sandbox Analysis Results on Hybrid Analysis Application

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

3.6. Cerber Ransomware Identified in Total Virus App

The log file code 2017-01-28 was then tested using virus total. The test results show that the log file contains a ransomware-type network trojan named cerber. The results of the total virus application analysis can be seen in **Figure 9.**

Figure 9. PCAP File Analysis With Virus Total Application

3.7. Phishing Domains Identified in Kaspersky

Malware identification was also performed using the Kaspersky application. The results of the identification and detection of the log file code 2017-01-28 were declared clean by karspersky. The results of the investigation and analysis can be seen in **Figure 10** below:

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

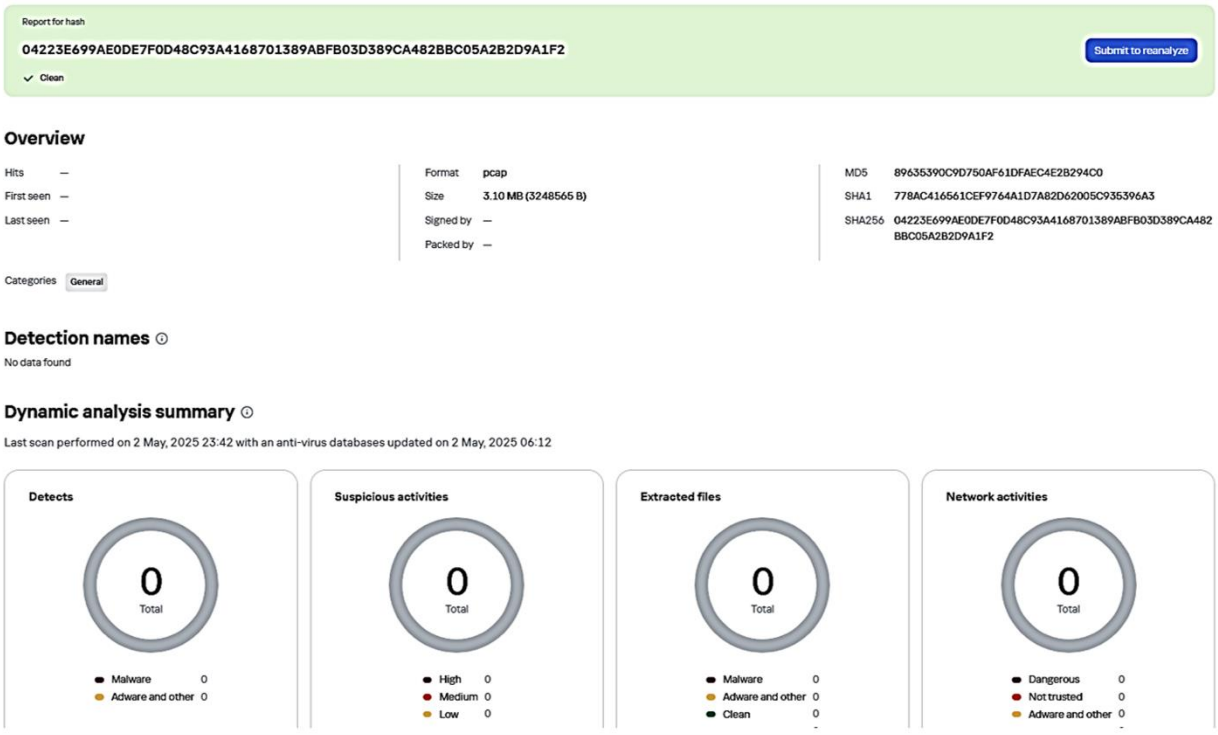

Figure 10. Results of Investigation and Detection of Malware in log files by Karspersky

However, Kaspersky warned of a web phishing attempt on the domain p27dokhpz-2n7nvgr.1jw2lx.top. The results of the analysis and investigation can be seen in **Figure 11**.

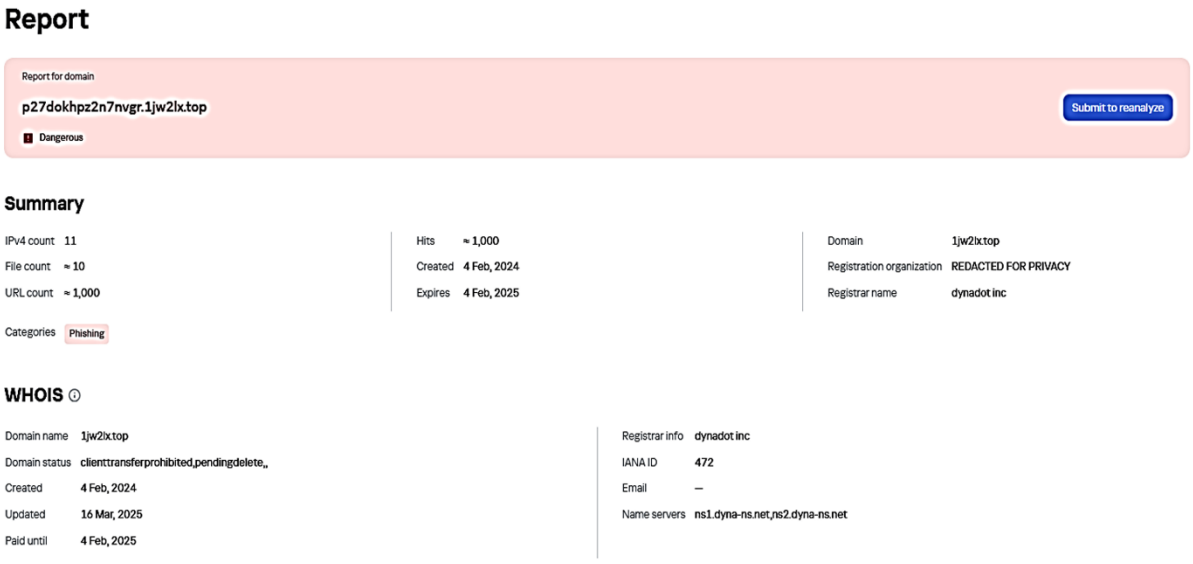

Figure 11. Investigation and Detection Results of p27dokhpz2n7nvgr.1jw2lx.top by Karspersky

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

3.8. Potential and Threat of Cerber/Cerberus Malware Operation

Analysis of the mitre attack application showed that cerber/cerberus has been used in private operations for two years. This malware is a banking trojan whose use can be rented on forums and black markets. Some of the actions that can be performed by this cerber or cerberus trojan are as follows:

1. Cerberus communicates with the C2 server using HTTP.
2. Cerberus can update the malicious payload module on command.
3. Cerberus hid its icon from the app vault after its first launch.
4. Cerberus disabled Google Play Protect to prevent its future discovery and removal.
5. Cerberus can remove itself from the device on command.
6. Cerberus can record keystrokes.
7. Cerberus can generate fake notifications and launch overlay attacks against attacker-defined applications.
8. Cerberus can inject inputs to grant itself additional permissions without user interaction and to prevent app deletion.
9. Cerberus can collect the location of the device.
10. Cerberus pretends to be the Adobe Flash Player installer.
11. Cerberus communicates with C2 using HTTP requests over port 8888.
12. Cerberus uses string blurring techniques and standardized payloads.
13. Cerberus can obtain the device's contact list.
14. Cerberus can collect messages, information, or data from a device.
15. Cerberus can send messages, information, or data from the device.
16. Cerberus can obtain a list of installed applications.
17. Cerberus can collect device information, such as default apps and device locale.
18. Cerberus avoids analysis by only activating the malware after recording a certain number of steps from the accelerometer.

4. CONCLUSION

The conclusion of the research investigating malware cyberattacks on server networks using the SIEM method based on NIST 800-61 Rev 2 is as follows:

1) Malware attacks tend to be invisible in network traffic, but malware can transfer data from the target computer to the attacker's computer.
2) Some forensic investigation applications may not be able to identify malware in attack logs or log files. However, the foresight and experience of the investigator are the key milestones in conducting a malware investigation.
3) In reporting evidence data in the form of attack records or log files, evidence of analysis and detection of malware attacks can be attached.
4) Cerberus malware cyberattacks pose a more dangerous threat than Denial of Service (DOS) attacks because cerberus malware attacks are capable of stealing confidential information and data.

5. ACKNOWLEDGMENT

This study was funded by the UIN Sunan Gunung Djati Bandung. The research resources and facilities provided by the computer science department were instrumental in this study.

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

6. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

7. REFERENCES

[1] A. S. D. Azmi dan S. T. S. Deris, "Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang," Indonesian Journal of Multidisciplinary on Social and Technology, vol. 1, no. 2, pp. 176–183, 2023.

[2] A. Nofiyan, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)," Jurnal Sarana Teknik Informatika, vol. 8, no. 2, pp. 11–23, 2020.

[3] B. A. H. Pratama, "Analisis dan Investigasi Forensik Aplikasi Instagram dan Threads Dalam Mendapatkan Bukti Digital Menggunakan Metode Nist 800-86," Kohesi: Jurnal Multidisiplin Saintek, vol. 5, no. 3, pp. 1–18, 2024.

[4] J. A. Lestari dan G. Taufik, "Penerapan NIST 800-61 REV 2 Untuk Analisa Ransomware Attack Pada," Jurnal Infortech, vol. 6, no. 1, 2024.

[5] A. Kurniawan dan I. Riadi, "Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior," International Journal of Network Security, vol. 20, pp. 836–843, Sep. 2018, doi: 10.6633/IJNS.201809.

[6] R. A. Ramadhan, A. T. Tira, dan M. R. Fadhilah, "Forensik Jaringan: Analisis Serangan Client dan Pengukuran Quality of Service oleh ARP Poisoning menggunakan Network Forensic Generic Process (NFGP) Model Network Forensic: Analysis of Client Attack and Quality of Service Measurement by Arp Poisoning," SISTEMASI: Jurnal Sistem Informasi, vol. 13, no. 2, pp. 713–727, 2024.

[7] Nasirudin, Sunardi, dan I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," Jurnal Informatika Universitas Pamulang, vol. 5, no. 1, pp. 89–94, 2020.

[8] L. M. A. Arsada, "Penerapan Metode NIST untuk analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT)," Jurnal Ilmiah KOMPUTASI, vol. 20, no. 2, pp. 275–281, 2021.

[9] A. Yudhana, I. Riadi, dan R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," Jurnal Informatika: Jurnal pengembangan IT (JPIT), vol. 7, no. 1, p. 1, Jan. 2022.

[10] K. Butarbutar, "Forensic Network Analysis of Metarouter Using NIST SP800-86 Framework," Journal of SAKIRA (Secure And Knowledge-Intelligent Research in Cybersecurity And Multimedia), vol. 1, no. 2, pp. 39–50, 2023.

[11] Firmansyah, A. Fadlil, dan R. Umar, "Evaluasi Optimalisasi Alat Forensik Keamanan Jaringan pada Lalu Lintas," Edu Komputika Journal, vol. 10, no. 2, pp. 81–92, 2024.

[12] Firmansyah, A. Fadlil, dan R. Umar, "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST," JURNAL RESTI (Rekayasa Sistem Dan Teknologi Informasi), vol. 1, no. 10, pp. 91–98, 2021.

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

[13] Firmansyah, A. Fadlil, dan R. Umar, "Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien," Edu Komputika Journal, vol. 6, no. 2, pp. 54–59, 2019.

[14] D. S. I. Krisnadi, "Citra Forensik Dari Barang Bukti Elektronik Dengan Metode Physical Menggunakan Acquisition Tools Tableau Imager Dan Ftk Imager," Academia, 2020.

[15] K. D. O. Mahendra dan I. K. Ari Mogi, "Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases," JELIKU (Jurnal Elektronik Ilmu Komputer Udayana), vol. 9, no. 3, p. 381, 2021, doi: 10.24843/jlk.2021.v09.i03.p09.

[16] G. A. Marcoulides, "Discovering Knowledge in Data: an Introduction to Data Mining: Discovering Knowledge in Data: An Introduction to Data Mining," Journal of the American Statistical Association, vol. 100, no. 472, 2005, doi: 10.1198/jasa.2005.s61.

[17] M. A. Aziz, W. Y. Sulistyo, dan S. R. Astari, "Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO)," JURISTIK (Jurnal Riset Teknologi Informasi Dan Komputer), vol. 1, no. 01, pp. 8–15, 2021, doi: -10.53863/juristik.v1i01.341.

[18] M. A. D. Putra et al., "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86," Jurnal Sistem Informasi Galuh, vol. 2, no. 1, p. 10, Jan. 2024.

[19] F. A. Amsor dan M. Mulyana, "Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital," Journal Humaniora: Jurnal Hukum dan Ilmu Sosial, vol. 2, no. 1, p. 5, 2024.

[20] R. N. Dasmen, M. R. Pratama, H. Yasir, dan A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86," Jurnal Ilmiah Informatika, vol. 2, 2024.

[21] I. Riadi, A. Yudhana, dan M. A. Barra, "Copyright Forensik Mobile pada Layanan Media Sosial LinkedIn," JISKA (Jurnal Informatika Sunan Kalijaga), vol. 6, no. 1, pp. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.

[22] M. R. Setyawan, A. Yudhana, dan A. Fadlil, "Data Acquisition On Messenger Skype Using The National Institute Of Justice Method," Systemic: Information System and Informatics Journal, vol. 5, no. 2, pp. 13–18, 2020, doi: 10.29080/-systemic.v5i2.7.

[23] J. Han dan M. Kamber, Data Mining: Concepts and Techniques. Soft Computing, Second Edition, vol. 54, 2006, doi: 10.1007/978-3-642-19721-5.

[24] R. A. K. N. Bintang, R. Umar, dan A. Yudhana, "Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST," TECHNO, vol. 21, no. 2, p. 3, 2020.

[25] F. Ridho, A. Yudhana, dan I. Riadi, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," vol. 2, no. 1, pp. 111–116, 2016.

[26] S. Rachmie, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," JURNAL LITIGASI (e-Journal), vol. 21, p. 5, 2020.

[27] S. A. Sholikhatin, A. P. Kuncoro, A. L. Munawaroh, dan G. A. Setiawan, "Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security," Edu Komputika Journal, vol. 9, no. 1, 2023, doi: 10.15294/edukomputika. v9i1.57389.

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149

[28] S. Marcellino, H. B. Seta, dan W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute Of Justice (NIJ)," JURNAL INFORMATIK Edisi ke-19, no. 2, p. 2, 2023.

[29] I. Maulana dan A. Pujiyanta, "Analisis Forensik Aplikasi Penipuan Berbasis Android," JIKA (Jurnal of Informatics) Universitas Muhammadiyah Tangerang, vol. 8, no. 2, pp. 187–196, 2024.

DOI: https://doi.org/10.17509/coelite.v4i2.87286
p- ISSN 2829-4157 e- ISSN 2829-4149