Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Investigation of Malware Redline Stealer using Static and Dynamic Analysis Method Forensic

Nur Widiyasono[1], Siti Rahayu Selamat[2,*], Angga Sinjaya[1], Rianto[1], Randi Rizal[1,2], Mugi Praseptiawan[2,3]

[1] Department of Informatics, Faculty of Engineering, Siliwangi University, Tasikmalaya, 46115 Indonesia
[2] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka 76100, Malaysia
[3] Department of Informatics, Institute of Technology Sumatera, ITERA, 35365 Indonesia

ARTICLE INFO

Article history:
Received 22 November 2023
Received in revised form 4 March 2024
Accepted 15 June 2024
Available online 15 July 2024

Keywords:
Malware Investigation; Redline Stealer; obfuscation; static and dynamic analysis; forensic

ABSTRACT

Redline Stealer is a malware variant discovered in early March 2020 by proof point analyst. Redline is famous for its ability to bypass the antivirus scan. Redline Stealer was created by hacker with the purpose to steal victim's information such as login data, password and credit card information from the browser application that used in infected computer. This research uses static and dynamic methods to analyze redline stealers. The process of static analysis is carried out by observing the malware's sample file, while dynamic analysis is carried out by monitoring malware's activity when the malware is running on the system. This research show that Redline Stealer uses the obfuscation feature based on .net, which can run only when there is an internet connection, stealing sensitive information, especially in a browser application. The conclusion of this research is Redline Stealer can be classified as a stealer malware that can steal important data on the infected system. The result of the analysis using the strings extract and decompile did not find any information because this malware uses the obfuscation feature, so the static analysis did find fewer information than the dynamic method.

1. Introduction

Technological developments and advances not only have a positive impact on society [1,2], but technological developments and advances also have negative impacts [3,4], one of which is the emergence of various types of cybercrimes, such as the spread of malware [5,6]. Malware is a program that is used for cybercrime crimes [7] with various purposes including seeking pleasure and seeking profit such as wiretapping and theft of personal information [8]. Malware can contain malicious code such as Viruses, Worms, Trojan Horses, can also create BackDoors that can steal personal information or take control of someone's computer system [9-11].

Malware is generally made to damage or break into a software or operating system [12,13] through a script that is kept secret or in another sense is hidden by the creator of the malware [5].

* *Corresponding author.*
E-mail address: sitirahayu@utem.edu.my

https://doi.org/10.37934/araset.48.2.4962

Malware is currently growing rapidly [14], thus requiring computer users to be more vigilant in protecting important information or files on the computer so that they are not taken and misused by unauthorized people [15,16]. Proofpoint analysts discovered a new malware variant called Redline Stealer in early March 2020 [17]. This malware has gained notoriety for its ability to evade detection and steal sensitive information from infected devices. Redline stealer malware steals login data and credit card information from browser applications.

Redline Stealer malware is malware that threatens data privacy security in the digital era; this is quite worrying, so more research is needed in the field of malware, especially on Redline Stealer. Malware analysis can generally be done with two methods, namely Dynamic Analysis and Static Analysis [18]. Static analysis is done by directly observing the malware source code without running the malware, while dynamic analysis is done by observing how the malware works when it is run on a system. The analytical methods used in this study are static and dynamic methods. Malware analysts mostly use a combination of these methods because of the wide scope and the number of tools available to produce a detailed and thorough analysis. The static and dynamic analysis method has also been used in several previous studies, including those carried out by [5,19,20] in identifying diverse malware.

This research uses the Redline Stealer malware as an object of forensic investigation. The methodology used in this paper is static analysis and dynamic analysis. Malware analysis in this research was carried out in an isolated virtual lab to avoid spreading malware on computers.

2. Methodology

In this section, the methodology of research in the investigation of malware Redline stealer is shown in Figure 1.

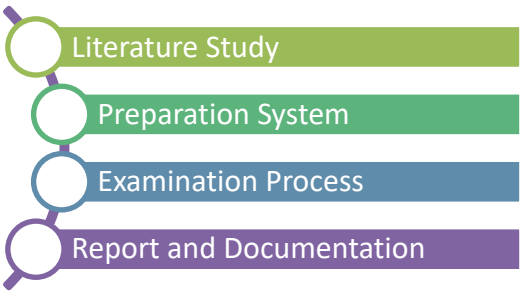

Fig. 1. Methodology

2.1 Literature Study

A literature study is carried out by collecting data and information from books, media, journals, experts, or the results of other people's research, which aims to develop the theoretical basis used in conducting research. Reference books and journals can contain brief descriptions or comprehensive explanations of malware analysis.

2.2 Preparation System

Preparation System is the process of preparing all the requirements needed to carry out malware analysis. Preparations include installing the operating system on a virtual machine, installing tools, and downloading malware samples.

2.3 Examination Process

The static analysis process uses several techniques to obtain information on the redline stealer malware as follows: Malware Fingerprint, File Type Identification, Strings Extract, Decompile, and Obfuscation Detect. Dynamic analysis is done by running and monitoring Redline Stealer malware samples. This monitoring process is carried out using two techniques, namely Process Monitoring and Network Monitoring.

2.4 Report and Documentation

The last stage is documentation to store the results of the data obtained from the malware analysis process using static analysis and dynamic analysis methods. The documentation is in the form of data output from videos, images, or the results of output data and information from analysis tools, which are then set forth in the research report.

3. Results

3.1 Preparation System

The preparation system used in this research is to prepare a virtual machine that will be used as a malware analysis lab and to prepare a research object, namely the redline stealer malware sample. The virtual machine used is VirtualBox version 6.1.40 r154048. The first preparation system to do is to install the operating system on the virtual machine. The operating system used in this study is Windows 10. System specifications used as an analysis lab are shown in Table 1 and Table 2.

Table 1
Specification of personal computer

Item	Value
OS Name	Windows 11 pro
Language	English (United States)
Username	MEMNON
Time Zone	(UTC-+07:00) Bangkok, Hanoi, Jakarta
Memory	16 GB RAM
Storage	1500 GB

Table 2
Specification of virtual machine

Item	Value
VM Application	Virtual Box
OS Name	Microsoft Windows 10 Enterprise LTSC
Language	English (United States)
Username	MUMKAR
Time Zone	(UTC-+08:00) Pacific Time (US & Canada)
Memory	4 GB RAM
Storage	60 GB

Table 1 shows the specifications of the computers used during the malware analysis process; Table 2 shows the specifications of the virtual systems that have been installed on the virtual box, and the allocation of physical hardware used for virtual machines. The tools used for each analysis technique carried out in this study can be seen in Table 3.

Table 3
List of tools used

Analysis Technique	Tools Used
Fingerprint Malware	Hashmyfile
File Type Identification	CFF Explorer
String Extract	Shell Extensions
Decompile	DnSpy
Obfuscation Detect	De4dot
Process Monitoring	Process Monitor
Network Monitoring	Wireshark

The redline stealer malware sample used as the object of this study was downloaded from the bazaar.abuse.ch website. The website provides many live malware samples that can be downloaded for free. The sample malware is downloaded from the website in ZIP form with the password "infected" (Figure 2).

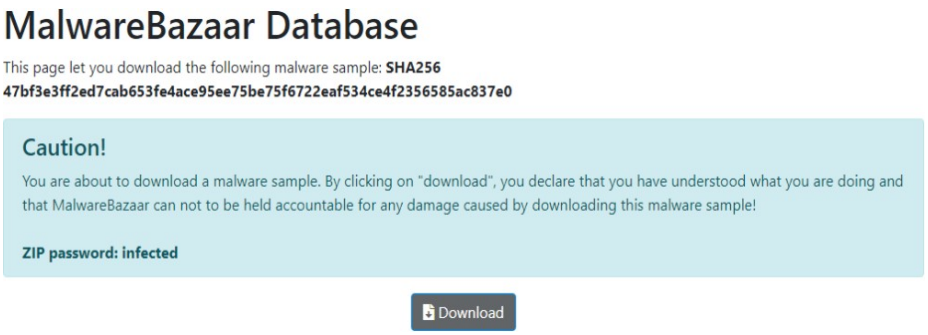

Fig. 2. Malware baazar

The sample malware is then extracted and named "samplemalware.exe" as shown in Figure 3.

Fig. 3. Sample malware

3.2 Examination Process

The Examination Process is carried out on a virtual machine that has been prepared in the preparation system process. The examination process consists of static analysis and dynamic analysis. Static analysis can contain important information that is useful for the dynamic analysis process. Therefore, the examination process in this study is carried out in the order of static analysis first and then dynamic analysis.

3.2.1 Static analysis

Static analysis is a method of analyzing malware without running the malware. Static analysis consists of several stages, as shown in Figure 4.

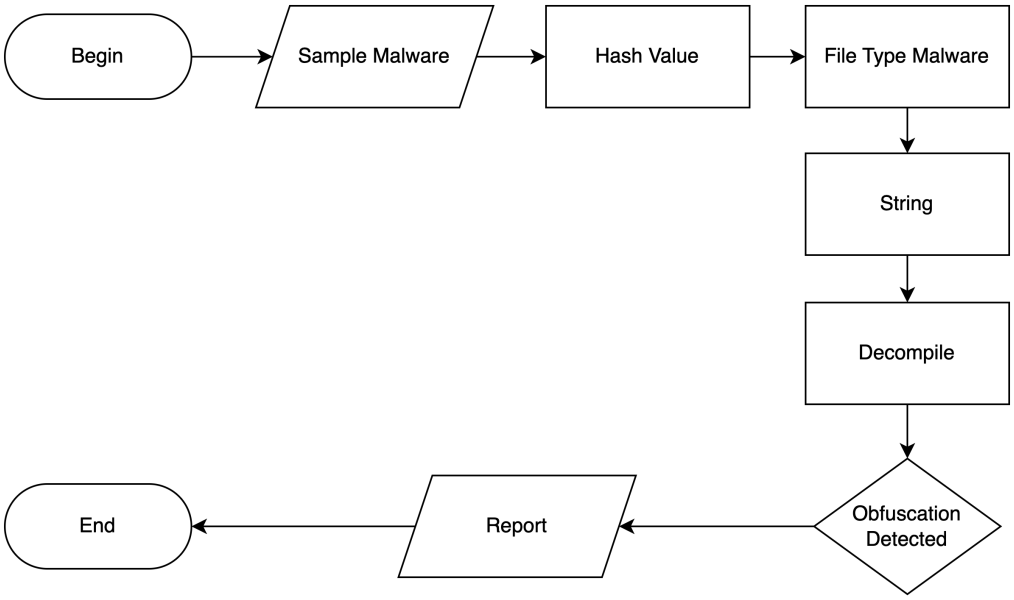

Fig. 4. Flowchart static analysis

A. Fingerprint Malware

The tool used at this stage is Hashmyfile, this stage aims to see the hash value of the malware sample file. The hash value of the malware sample file is used to check the authenticity of the malware sample file by comparing the hash value obtained from Hashmyfile and the hash value obtained from bazaar.abuse.ch. The results of examining the hash value using the Hashmyfile tool can be seen in Figure 5.

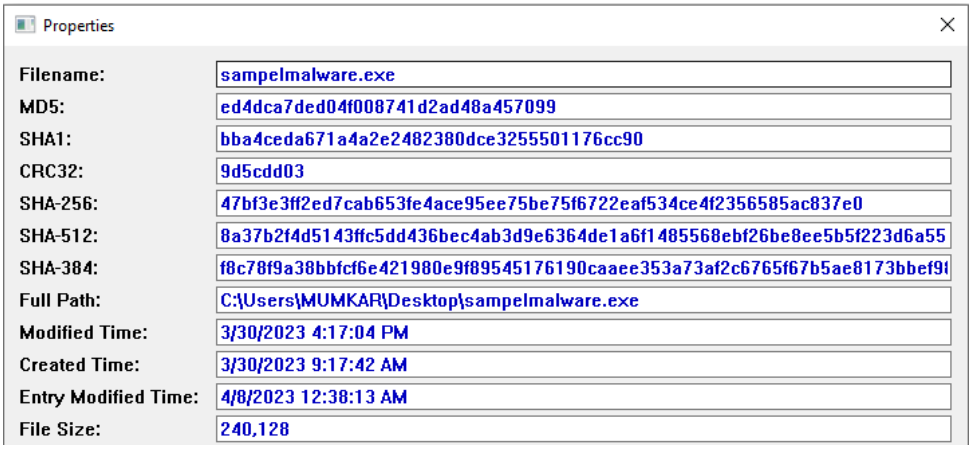

Fig. 5. Hash value of malware sample

The results of examining the hash value using Hashmyfile show that the value generated by Hashmyfile is the same as the information obtained from the website bazaar.abuse.ch, meaning that

the file is original or identical and has not been modified. A comparison of hash values can be seen in Table 4.

Table 4
Comparison of hash value file malware

Hash	Source	Hash Value	Information
MD5	Hashmyfile	ed4dca7ded04f008741d2ad48a4 57099	Identical
	Malware Bazaar	ed4dca7ded04f008741d2ad48a4 57099	
SHA-1	Hashmyfile	bba4ceda671a4a2e2482380dce3 255501176cc90	Identical
	Malware Bazaar	bba4ceda671a4a2e2482380dce3 255501176cc90	
SHA-256	Hashmyfile	47bf3e3ff2ed7cab653fe4ace95ee75be75f6722eaf 534ce4f2356585 ac837e0	Identical
	Malware Bazaar	47bf3e3ff2ed7cab653fe4ace95ee75be75f6722eaf 534ce4f2356585 ac837e0	

B. File Type Identification

The malware samples were processed using the CFF Explorer tool. The information generated from this process is that the sample malware is a 32-bit Portable Executable (PE) file compiled using .NET (Figure 6), which shows that the file is a type of file that can be run on the Windows operating system.

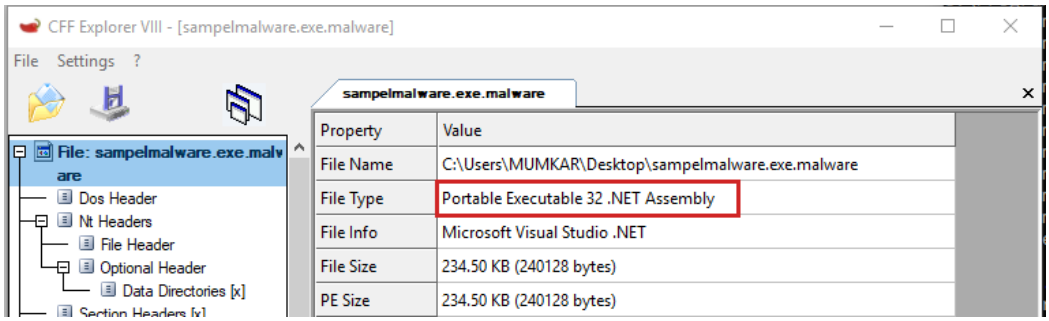

Fig. 6. Detection of malware sample file types

C. String Extract

The analysis carried out at this stage is to take strings from the redline stealer malware samples to get strings. The application used is Shell Extensions. The results of the string extraction performed on the Redline Stealer malware sample file are shown in Figure 7.

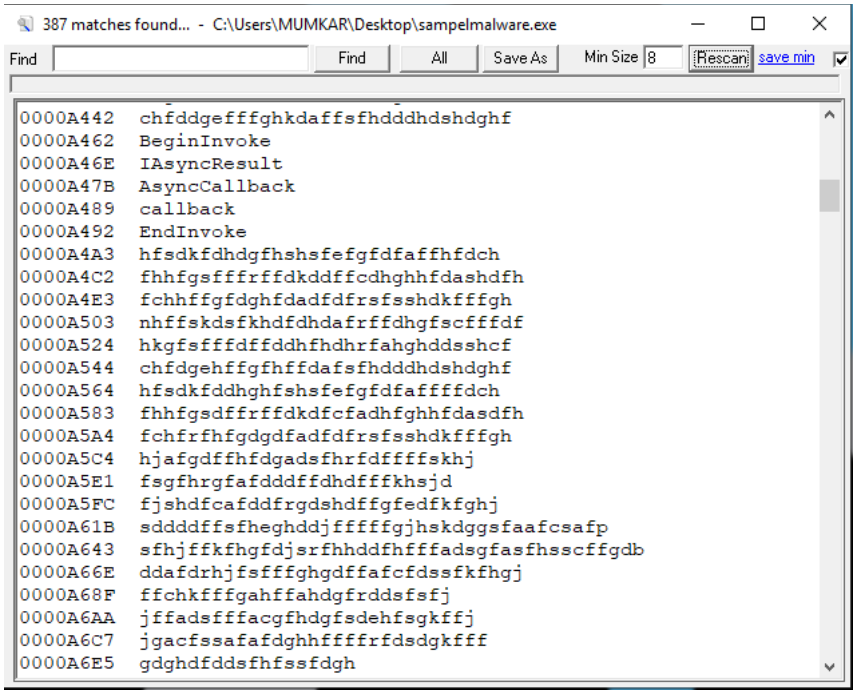

Fig. 7. Strings extract

The results of the string extraction that has been carried out only get random data, as shown in Figure 7; in other words, it does not produce any findings regarding the malware. The reason for not finding any information from this malware sample is because there is an obfuscation in the malware.

D. Decompile

The decompile process in this study uses the dnSpy tool. The decompilation process aims to convert machine language into high-level language so that it can be understood easily. The results of the decompile process are shown in Figure 8.

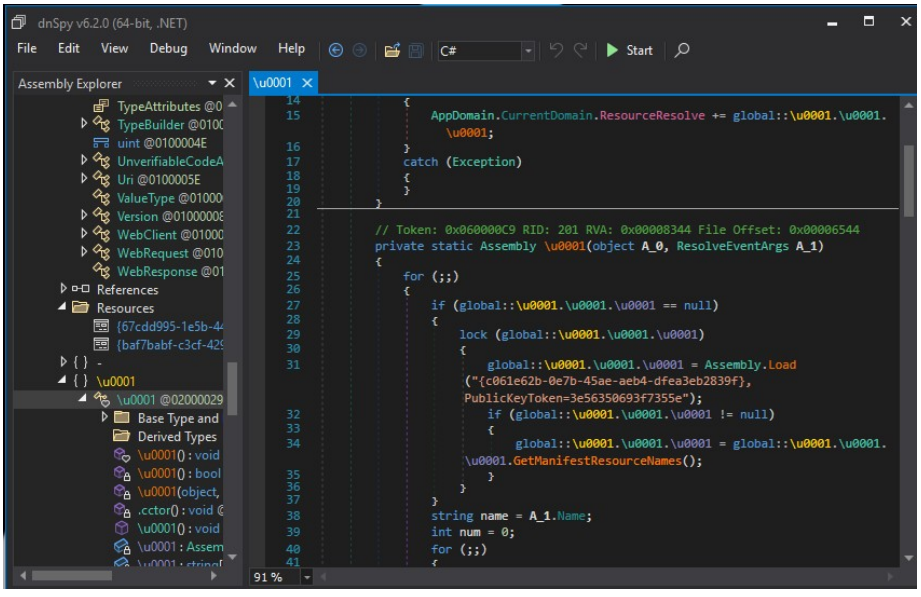

Fig. 8. Result decompile

E. Obfuscation Detect

The process of Obfuscation detection is to detect obfuscation on malware samples. This process aims to detect obfuscation used by malware authors. The tool used to detect obfuscation in this study is de4dot, as shown in Figure 9.

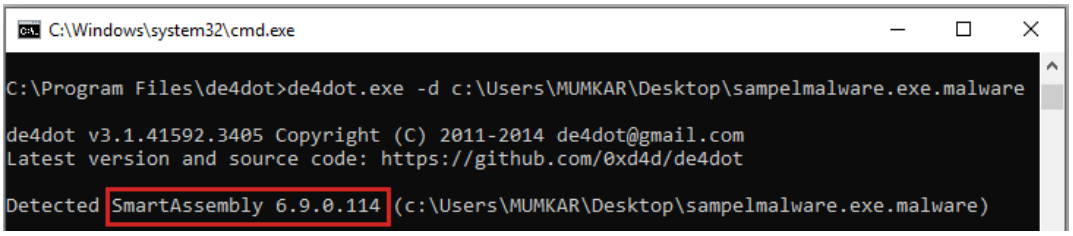

Fig. 9. Obfuscation detect

Information obtained from the Obfuscation Detect process on the redline stealer malware sample file using de4dot is that the malware sample file was detected using SmartAssembly 6.9.0.114, so it is necessary to DE obfuscate the malware sample. The DE obfuscate process is carried out using the de4dot tool shown in Figure 10.

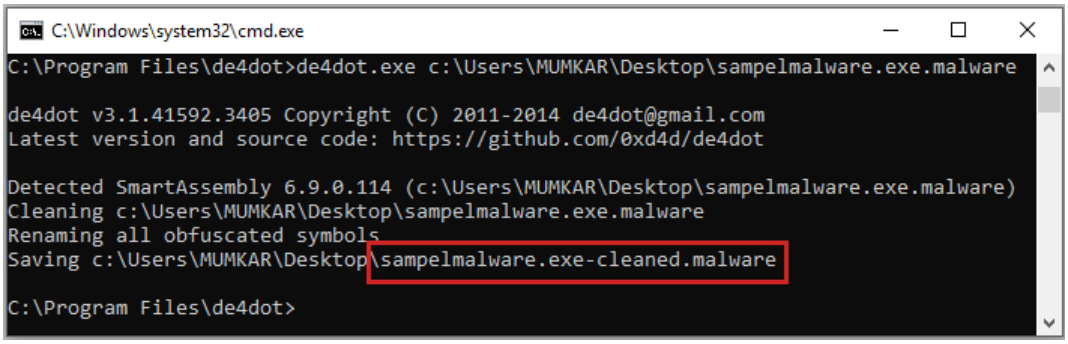

Fig. 10. DE obfuscate using de4dot

The result of the DE obfuscate process is a file that has gone through the DE obfuscate process with the file name "samplemalware.exe-cleaned.malware". The malware sample files that have gone through the DE obfuscate process are only used for the string extraction process, while for the dynamic analysis process, the malware samples used are the original ones. Some information changes regarding the original malware samples and malware samples that have gone through the DE obfuscate process are shown in Table 5.

Table 5
List of tools used

Condition	Original Files	After DE-obfuscate Process
File Name	samplemalware.exe.malware	samplemalware.exe- cleaned.malware
SHA-256	47bf3e3ff2ed7cab653fe4ace9 5ee75be75f6722eaf534ce4f2 356585ac837e0	9b7d632262e3c794fba25bb818a fe3bdbd73c9edec179fef7bba9bd 4a8c1b621
File Size	234.50 KB (240128 bytes)	229.50 KB (235008 bytes)

Malware sample files that have been DE obfuscated will be obfuscated again to ensure the obfuscation of the malware samples has been successfully removed.

The result of the second obfuscation detection process on the malware sample (Figure 11) is that the malware sample is still detected by an obfuscation with an unknown obfuscator. The DE obfuscate process on the malware sample cannot be carried out because the malware sample uses an unknown obfuscator.

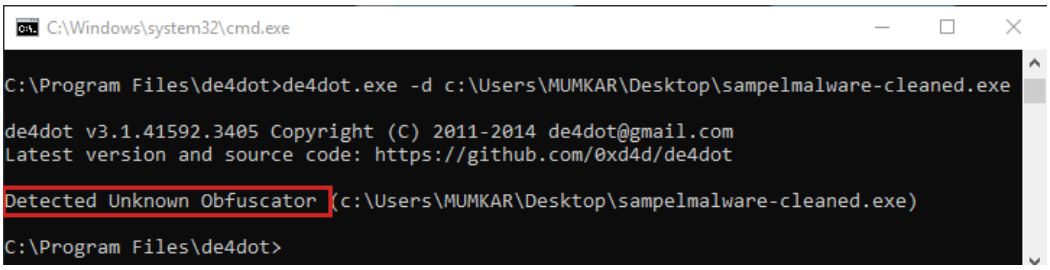

Fig. 11. Obfuscation detect 2

3.2.2 Dynamic analysis

The dynamic analysis process is carried out by monitoring activities, interactions, and effects on the system caused by malware when it is run. The steps taken in the dynamic analysis process are shown in Figure 12.

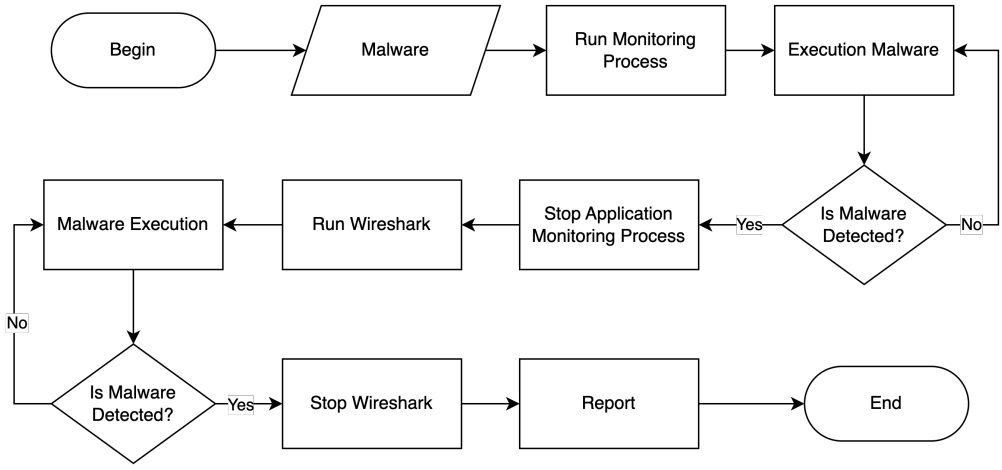

Fig. 12. Flowchart dynamic analysis

A. Process Monitoring

The tool used to carry out process monitoring in this study is the Process Monitor tool. The first step in the Process Monitoring stage is to run the Process Monitor application, which will be used to monitor what activities are being carried out by the redline stealer malware samples that will be executed. The Process Monitor application is run first before the malware sample is run; after the Process Monitor application is run, the redline stealer malware sample is run, and it is seen what processes are made by the malware.

Figure 13 shows the sample malware.exe that was successfully run and made several processes that were carried out on the Vbc.exe file. Process tree analysis related to samplemalware.exe gets information that vbc.exe is a child of the samplemalware.exe process, as shown in Figure 14.

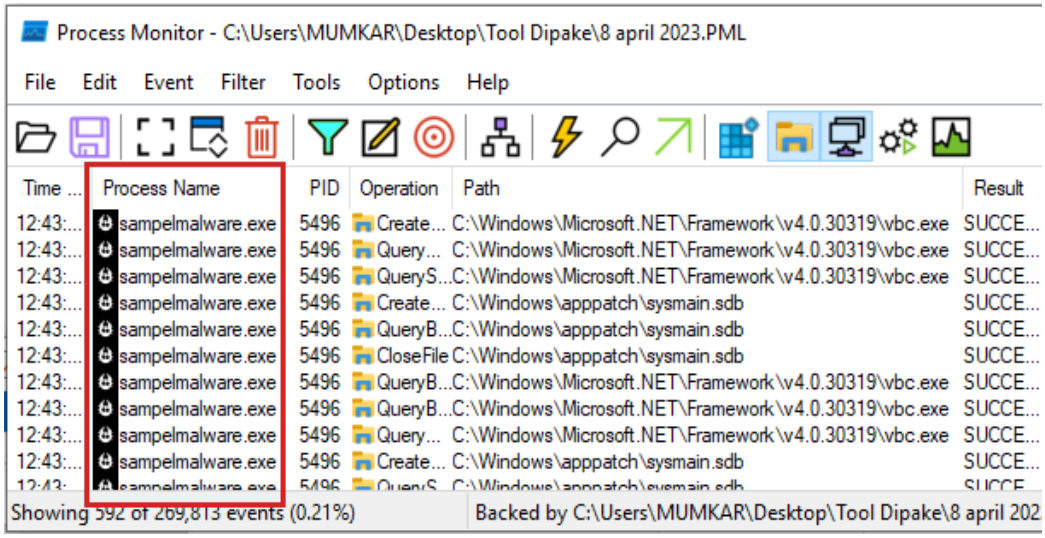

Fig. 13. Process monitoring after running malware

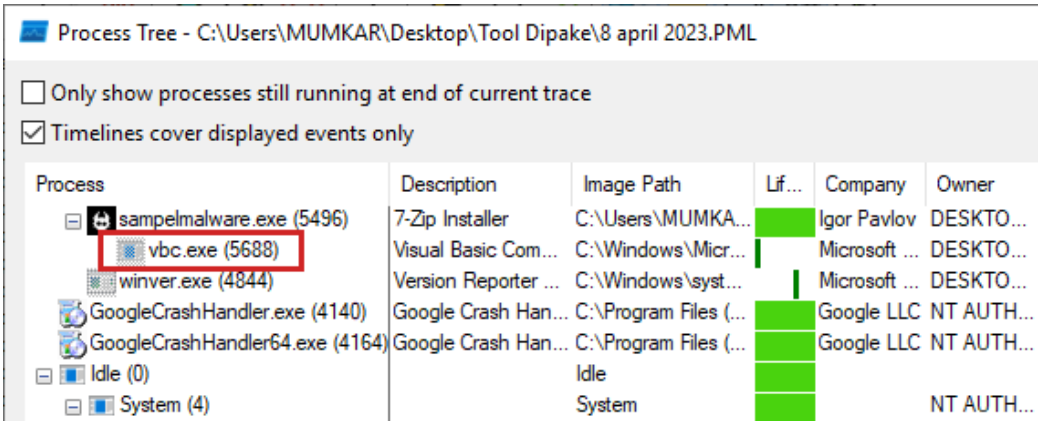

Fig. 14. vbc.exe child process tree

Figure 15 shows thatSamplemalware.exe runs another process, namely Vbc.exe, then Vbc.exe performs activities on the network as shown in Figure 15. It shows that Vbc.exe managed to communicate with the IP address 37.220.87.47.

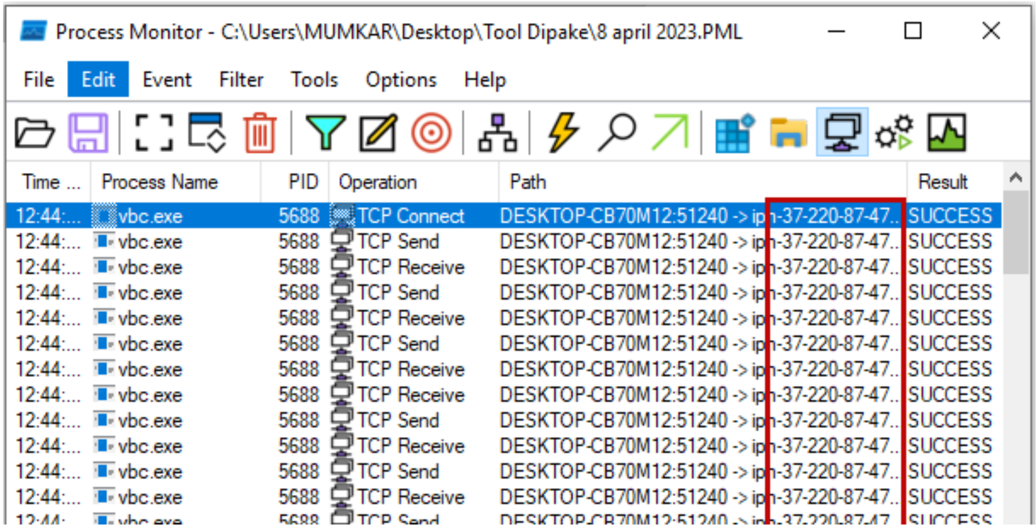

Fig. 15. *vbc.exe* doing activity network

B. *Network Monitoring*

The tool used to perform Network Monitoring in this study is Wireshark. The Wireshark application will be used to monitor network traffic on virtual systems. The next step is to run the redline stealer malware sample. The exchange of data sent by the malware was successfully monitored by the Wireshark tool; the Wireshark shows that there is an exchange of data for the IP address 37.220.67.47 (Figure 16).

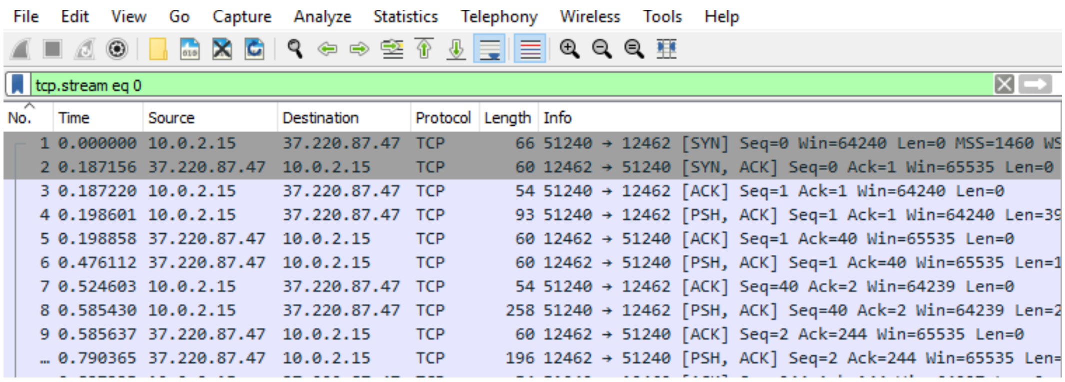

Fig. 16. *Malware* doing connection to 37.220.87.47

IP address 37.220.67.47 is the same IP address as the IP address connected to the system via Vbc.exe. The results of Network Monitoring using the Wireshark tool at the IP address 37.220.67.47 are shown in table 6. shows that the malware sends important information such as username, Windows version, time zone, files and applications running on the infected computer.

Table 6
Network Monitoring findings

Network Monitoring Results	Information
%USERPROFILE%	The malware server requests user profile data information infected system.
#.E.. OtherSideE%..MUMKARE..#Windows 10 Enterprise LTSC 2019 x64E'..English (United States)E)..	The malware sends information on the computer owner's name, Windows version and the language used to malware servers.
112.0.5615.49E%.5C:\Program Files\Google\Chrome\Application\chrome.exe.E9E...Internet ExplorerE..$11.00.17763.1 (WinBuild.160101.0800)E%./ C:\Program Files\Internet Explorer\iexplore.exe.....~?	Malware sends browser data installed on the infected computer.
"(.http://tempuri.org/Entity/Id8 softwaresV.	Malware sends data about the software installed on the infected computer.
&(UTC-08:00) Pacific Time (US & Canada)E.	The malware sends time zone information used by the infected computer.
.B?..b...i.E{E...available_packages.txtE...C: \Users\MUMKAR\Desktop\available_packages.txtE%.O.	The malware sends the information contained in the file available_packages. txt.
E...Users\MUMKAR\DesktopE'.....E{E...failed_packages.txtE..+C: \Users\MUMKAR\Desktop\failed_packages.txtE%.KGoogleChrome	The malware sends the information contained in the failed_packages.txt file.
.B....Id2.....(.http://tempuri.org/Entity/ Id9 processesV...s...a.V.D ....}@	Malware sends data containing processes running on the infected computer.

3.3 Report and Documentation

The findings with reporting on the testing and analysis conducted on the Redline Stealer malware can be seen in Table 7. shows that the analysis of the Redline Stealer malware using the static analysis and dynamic analysis methods yields different findings.

Table 7
Result findings on implementation and analysis

Result Findings	Static Analysis	Dynamic Analysis
Hash value	√	✗
Information on the type of malware sample file.	√	✗
Using the SmartAssembly 6.9.0.114 obfuscator.	√	✗
Run Vbc.exe.	✗	√
Malware server ip address 37.220.87.47.	✗	√
The malware server asks for a user profile.	✗	√
The malware sends username, windows version information and the language used.	✗	√
Malware sends installed browser information.	✗	√
The malware sends the timezone used.	✗	√
Malware sends files that are in the same folder as files malware.	✗	√
Malware sends data containing running processes.	✗	√

Figure 17 shows how the Redline Stealer malware works. The malware that has been executed creates a Vbc.exe process, and then Vbc.exe tries to connect the infected computer to the malware server with the IP address 37.220.67.47. Malware will only retrieve the data requested by the server and send the data to the server.

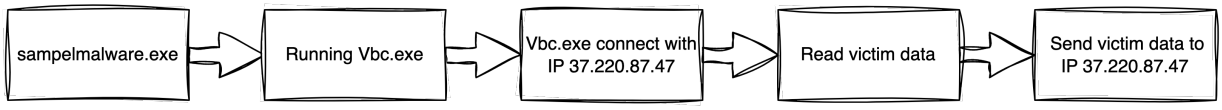

Fig. 17. Malware workflow

4. Conclusions

Based on the results of the research that has been done, it can be concluded that the analysis of the Redline Stealer malware using static analysis and dynamic analysis methods produces different findings. Static Analysis provides findings in the form of hash values, types of malware files, and obfuscators used in malware. Dynamic analysis produces findings in the form of how malware works, IP addresses, and steals important information from computers infected with the Redline Stealer malware. The strings extract and decompile technique on the Redline Stealer malware did not produce any findings. The Redline Stealer malware uses obfuscation, so the analysis process uses the static analysis method with the string extract and decompile technique, which does not provide any information about the malware.

Acknowledgment

The authors wholeheartedly acknowledge the profound impact that the JKF research group at the Department of Informatics Siliwangi University and FTMK UTeM with the INSFORNET research group have had on this research. Their support, shared knowledge, and guidance have been pivotal, and the authors are deeply grateful for the privilege of working alongside such esteemed colleagues.

References

[1] Fransisca, Vika, and Widia Ningsih. "The Advancement of Technology and its Impact on Social Life in Indonesia." *Devotion Journal of Community Service* 4, no. 3 (2023): 860-864. ttps://doi.org/10.36418/devotion.v4i3.445

[2] Naikoo, Aasif Ali, Shashank Shekhar Thakur, Tariq Ahmad Guroo, and Aadil Altaf Lone. "Development of society under the modern technology-a review." *Scholedge International Journal of Business Policy & Governance* 5, no. 1 (2018): 1-8. https://doi.org/10.19085/journal.sijbpg050101

[3] Ryan, Ann M., and Eva Derous. "The unrealized potential of technology in selection assessment." *Revista de Psicología del Trabajo y de las Organizaciones* 35, no. 2 (2019): 85-92. doi: 10.5093/jwop2019a10. https://doi.org/10.5093/jwop2019a10

[4] Sjamsoeddin, Sjafrie. "Negative Impact of the Development of Science and Technology on the Aspects of National Defense and Security." *Journal of Survey in Fisheries Sciences* 10, no. 2S (2023): 1131-1142.

[5] Manoppo, Virgiawan Arshad, Arie SM Lumenta, and Stanley DS Karouw. "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi." *Jurnal Teknik Elektro dan Komputer* 9, no. 3 (2020): 181-188.

[6] Li, Yuchong, and Qinghui Liu. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments." *Energy Reports* 7 (2021): 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

[7] Perwej, Yusuf, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, and Anurag Kumar Jaiswal. "A systematic literature review on the cyber security." *International Journal of scientific research and management* 9, no. 12 (2021): 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

[8] Aslan, Ömer Aslan, and Refik Samet. "A comprehensive review on malware detection approaches." *IEEE access* 8 (2020): 6249-6271. https://doi.org/10.1109/ACCESS.2019.2963724

[9] Setia, Tesa Pajar, Nur Widiyasono, and Aldy Putra Aldya. "Analysis malware flawed ammyy RAT dengan metode reverse engineering." *Jurnal Informatika* 3, no. 03 (2018). https://doi.org/10.30591/jpit.v3i3.1019

[10] Waliulu, Raditya Faisal, and Teguh Hidayat Iskandar Alam. "Reverse Engineering Analysis Forensic Malware WEBC2-DIV." *Sinkron: jurnal dan penelitian teknik informatika* 3, no. 1 (2018): 113-119. https://doi.org/10.30865/komik.v2i1.902

[11] Thomas, Ciza. "Introductory chapter: Computer security threats." In *Computer security threats*. IntechOpen, 2020. https://doi.org/10.5772/intechopen.93041
[12] Brody, Richard G., Harold U. Chang, and Erich S. Schoenberg. "Malware at its worst: death and destruction." *International Journal of Accounting & Information Management* 26, no. 4 (2018): 527-540. https://doi.org/10.1108/IJAIM-04-2018-0046
[13] Saeed, Mariwan Ahmed Hama. "Malware in computer systems: Problems and solutions." *IJID (International Journal on Informatics for Development)* 9, no. 1 (2020): 1-8. https://doi.org/10.14421/ijid.2020.09101
[14] Sihwail, Rami, Khairuddin Omar, and KA Zainol Ariffin. "A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis." *Int. J. Adv. Sci. Eng. Inf. Technol* 8, no. 4-2 (2018): 1662-1671. https://doi.org/10.18517/ijaseit.8.4-2.6827
[15] Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." *Electronics* 12, no. 6 (2023): 1333. https://doi.org/10.3390/electronics12061333
[16] Humayun, Mamoona, N. Z. Jhanjhi, Ahmed Alsayat, and Vasaki Ponnusamy. "Internet of things and ransomware: Evolution, mitigation and prevention." *Egyptian Informatics Journal* 22, no. 1 (2021): 105-117. https://doi.org/10.1016/j.eij.2020.05.003
[17] Jeremy H and Axel F, "New Redline Password Stealer Malware," *Proofpoint*, Mar. 2020.
[18] Li, Ce, Zijun Cheng, He Zhu, Leiqi Wang, Qiujian Lv, Yan Wang, Ning Li, and Degang Sun. "DMalNet: Dynamic malware analysis based on API feature engineering and graph learning." *Computers & Security* 122 (2022): 102872. https://doi.org/10.1016/j.cose.2022.102872
[19] Riadi, Imam. "Implementation of malware analysis using static and dynamic analysis method." *International Journal of Computer Applications* 975 (2015): 8887.
[20] Gajrani, Jyoti, Vijay Laxmi, Meenakshi Tripathi, Manoj Singh Gaur, Akka Zemmari, Mohamed Mosbah, and Mauro Conti. "Effectiveness of state-of-the-art dynamic analysis techniques in identifying diverse Android malware and future enhancements." In *Advances in Computers*, vol. 119, pp. 73-120. Elsevier, 2020. https://doi.org/10.1016/bs.adcom.2020.03.002