Hack.exe Malware Analysis and Investigation Using Memory Forensics

Avie Triantoro[1], Nur Widiyasono [2], and Rohmat Gunawan [3]

[1,2,3]Informatics, Siliwangi University, Tasikmalaya, Indonesia
*avietriantoro@gmail.com

Abstract Currently, the development of malware is very fast. Malware is inevitably created or developed every day. In early 2020 there was a Hack.exe Malware attack which was a form of cybercrime. These crimes impact data that has been exploited for crimes at the next level. Expertise in the process of investigating malware analysis requires sufficient knowledge so that the results obtained in this study are malware architecture, the impact of attacks, the process of identifying the type of malware. Knowing the type of malware, a "countermeasure" can be done to protect devices infected with this type of malware. The method used for malware analysis is dynamic and memory forensics so that it can be seen that the malware process infects the system and then retrieves the victim's data, then the malware will make a connection or communication at the ip address 24.146.133.195. name ip address OOL-CPE-YNKRNY-24-146-128-0-20. The next process is the malware to shut down its system.

***Index Terms*— Malware Analysis, Dynamic, Hack, Memory Forensics.**

I. INTRODUCTION

Today, data is the most valuable asset. The techniques used to steal data vary widely. One of the ways is by using malware that is distributed by inserting it in an application or through certain files [1]. The survey institute stated that in the March 2019 edition there was 300,000 new malware created every day [2] .

Malware is created to damage or break into software and damage the operating system. The script that the attacker kept secret. The rapid development of malware requires users to be more strict and aware of the security of their data. Companies investing in the security of their data, but malware attacks continue to grow [3].

Malware is defined as any malware, malicious computer program, or malicious software, such as viruses (computers), trojans, spyware, and worms [4].Due to the increase in malware attacks, investigators are needed to carry out investigations. Performing a malware analysis requires special skills to detect and understand how the malware works. Malware is broadly divided into several categories, namely worms, viruses, Trojan horses, adware, and exploits. These types are the most frequently found bias, where each of these categories has different specifications [5]

Hack.exe is a family of zloaders, where since January 1, 2020, there have been many fraudulent emails feeds on various subjects, including prevention of COVID-19 fraud and the malware can steal user data and information [6]. Malware analysis using reverse engineering and memory forensic methods is one of the solutions that can be used today. Reverse engineering is used in the cyber world to find hidden information. Memory forensics is the analysis are used to track malware traces [7].

This research [4] performs analysis using dynamic methods and reverse engineering to be able to fully explain the characteristics of the Malware Flawed Ammyy RAT. The Flawed Ammyy malware has 12 functions, including malware that takes over the pointer function, compresses files, determines ANSI or OEM code functions, functions to select files that meet certain conditions, functions to handle predefined modules, determines whether files can be executed or no, can change the name of entries in the phonebook, compare a specific number of characters, can load a specific resource menu, and the function adjusts the buffer to the specified character.

This research [8] performed by reverse engineering technical analysis on biscuit malware to carry out the classification and identification of malware. The result of this research is that the classification process for malware identification can first be uploaded to the malware repository. The reverse engineering process can be carried out with standard procedures such as analyzing malware and analyzing the identity of malware.

II. LITERATURE REVIEW

A. *Malware*

Malware is malicious software that is deliberately programmed to damage a system or acquire computer data without the user knowing it. Viruses, Worms, Trojans, Key Loggers, Spyware, and Ransomware are examples of most malware us [9].

B. Dynamic Analysis

The analysis process is carried out by executing so that later it can monitor function calls, track information, perform function parameter analysis and trace instructions. Applications that feel suspect are usually run in a virtualized scope. An application behaves abnormally so the application can be categorized as a malicious application [10]

C. Memory Forensic

Memory Forensic is a way of analyzing sophisticated malware, root, and can detect cybercrime. Memory forensics is very useful in analyzing malware because it can be easily applied regardless of technology, system operations, software, and file systems [11]. The volatility tool allows identifying cyberattacks using malware or not [12].

III. METODOLOGY

This research has the following flow:

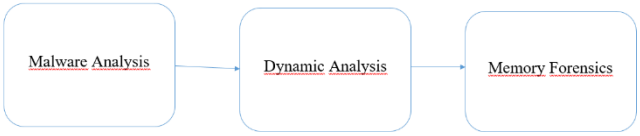

Fig 1. Research methodology flow

1. Malware Analysis

Malware analysis is carried out to get initial information about the malware that will be tested. This analysis will later find out where the sample was obtained, what is the MD5 value, what is the size of the malware hack file, and the type of malware hack file.

2. Dynamic Analysis

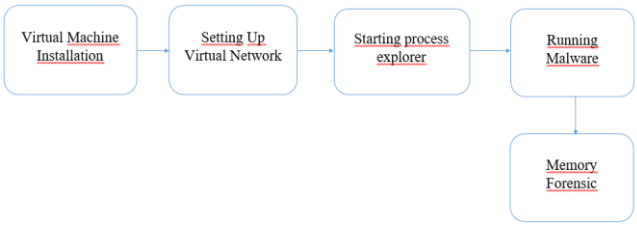

Fig 2. Dynamic analysis method flow

Virtual Machine Installation

The safe scope of research in malware analysis testing is within the virtual scope for performing malware sample testing. The scope of virtual machines is known as virtual machines. Testing is done in a virtual form intended to keep physical computers safe against the effects of the malware being examined. The virtual machine specifications used are as follows in Table I.

TABLE I

SPECIFICATION VIRTUAL MACHINE

Operating system	Windows 7
Memory	3040MB
Number of Processors	1
Storage	32GB
Network	NAT

Setting Up Virtual Network

setting up Virtual Network to perform network manipulation to fake a DNS response at the specified ip address on the local machine. Tools used to manipulate this network using ApateDNS.

Starting process explorer

Starting process explorer using the tools process monitor version 3.53, where these tools are used to see all processes that are running.

Running Malware

Running Malwaredone to see the behavior of malware when run. Testing is carried out in a virtual scope so that physical computers are safe from being affected by malware behavior

Memory Forensic

memory forensics volatility tools, to identify processes running in memory. Volatility can display all processes running on the computer and can also see the connections made by malware.

IV. RESULT AND DISCUSSION

1. Malware Analysis

Malware can be found on the website https://any.run/ as in Fig 3.

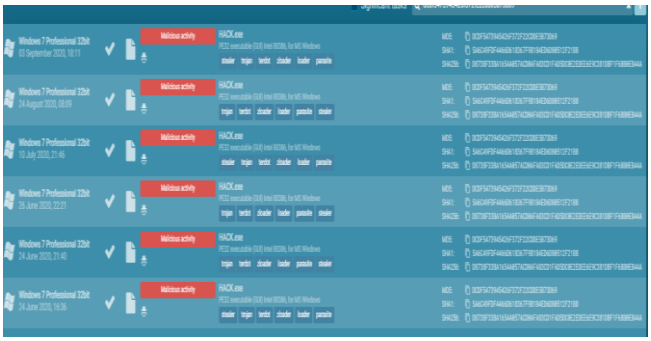

Fig 3. Website any.run

Malware object is taken from the website https://any.run/. This website provides a lot of malware that we can get. The hack.exe malware is then identified early using the fiscal tool as shown in Fig 4.

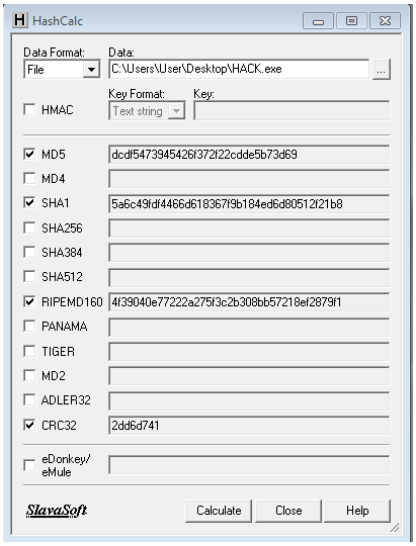

Fig 4. MD5 Malware hack.exe

Referring to Figure 4, it can be seen that the malware has a value of MD5 (Message-Digest algorithm 5) dcdf5473945426f372f22cdde5b73d69. The MD5 value is to ensure that the file is the same file and there are no changes in the contents of the file.

TABLE II

HACK.EXE MALWARE INFORMATION

Malware Name	HACK.exe
MD5	DCDF5473945426F372F22CDDE5B73D69
File Size	2,018 KB
File Type	Executable

2. Dynamic Analysis

A. Virtual Machines

The operating system the virtual box using windows 7, then for memory that is used 3040 MB and uses 1 processor with 32 GB of storage. Settings on the network use NAT because the network will make it safe when researching because it will not be sent directly to a physical computer but must go through a firewall first.

B. Setting Up Virtual Network

ApateDNS which has been installed on virtual then click the start server button as in Fig 5 the current localhost ip address becomes 127.0.0.1.

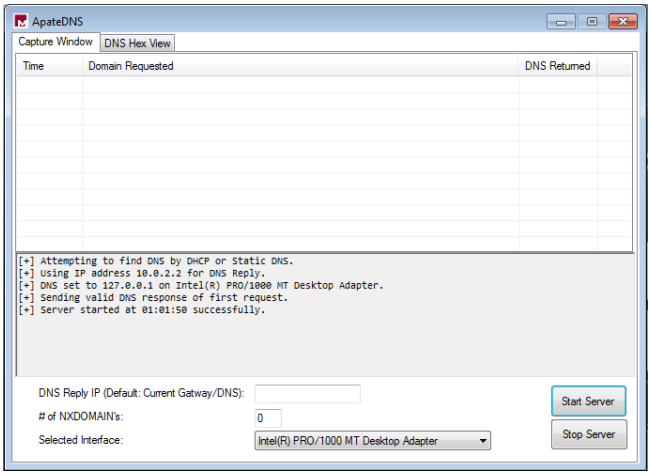

Fig 5. ApateDNS

Referring to Figure 5, the process of running an application that will always reply using ip 10.0.2.2 which causes the computer to appear as if it is connected to the internet.

C. Starting process explorer

This stage uses version 3.53 of the process monitor tools. This application has a feature to view all activities running on the computer. Referring to Fig 6, the process monitor tool can filter all processes running on the computer.

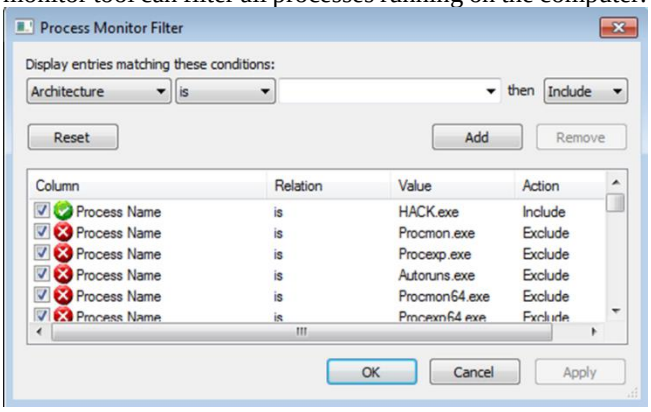

Fig 6. Filter Process Monitoring

Process filter on Fig 6 displayed only hack.exe malware to make it easier to perform analysis. Perform filter by looking at the process name of all malware activities so that we can see it as in Fig 7.

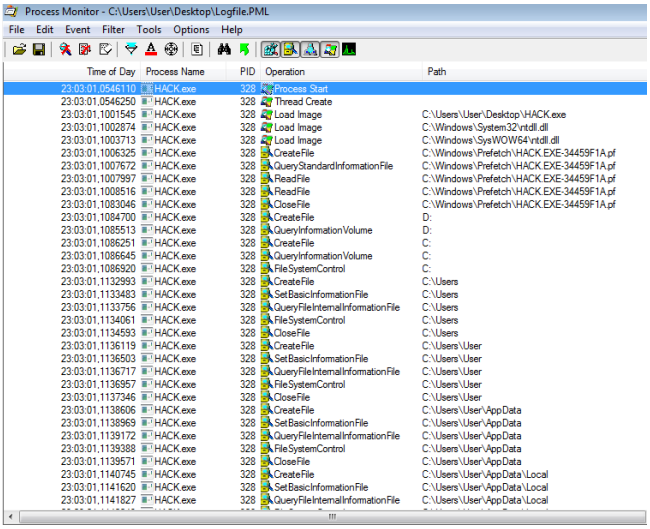

Fig 7. Process monitor hack.exe malware

Referring to Fig 7, hack.exe malware is all activities performed by malware. The malware performs many activities such as reading files, creating files, connecting, closing files, and so on. We can pay attention to the activities carried out by each step that is carried out by the malware. In Fig 7 we can see that the malware creates files, sets basic information files, controls file systems, and closes files in each file directory.

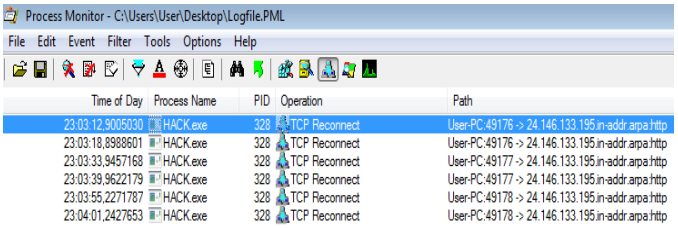

Fig 8. Process monitor network malware hack.exe

Referring to Fig 8, where it can be seen that the malware is always synchronizing to the ip address 24.146.133.195. Any information that has been obtained, the malware synchronizes on the ip, and for deeper information on the ip address 24.146.133.195 using the Whois Ip Look Tool.

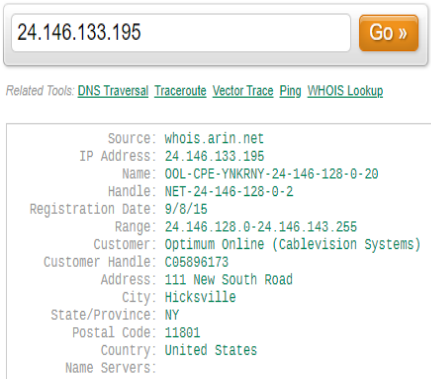

Fig 9. Whois Ip Look Tool ip address 24.146.133.195

Fig 9 can display information ip address 24.146.133.195 has the name OOL-CPE-YNKRNY-24-146-128-0-20, country United States, and city ip address 24.146.133.195 Hicksville.

3. Memory Forensic

Forensic memory analysis using volatility tools. This analysis process will display the processes running on the memory and the connections used.

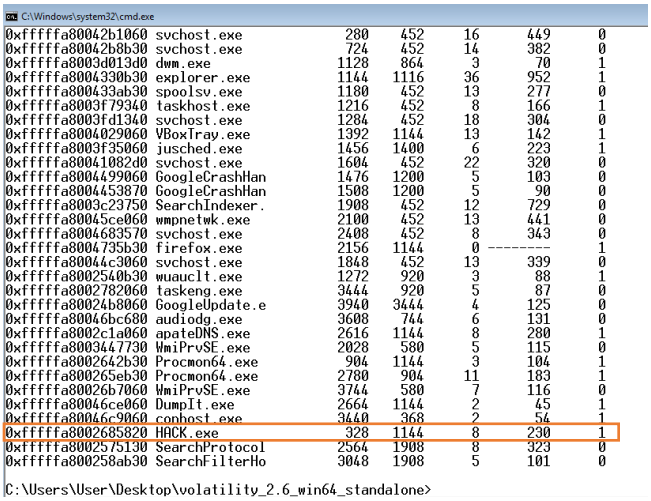

Fig 10 Volatility pslist process

Fig 10is a command to display all processes running on the computer using the command volatility_2.6_win64_standalone.exe pslist –f USER-PC-20201001-060252.raw –profile = Win7SP1x64. Volatility executes the command and displays all processes traveling on the computer. Hack.exe malware appears to be running in the process and running on PID 328.

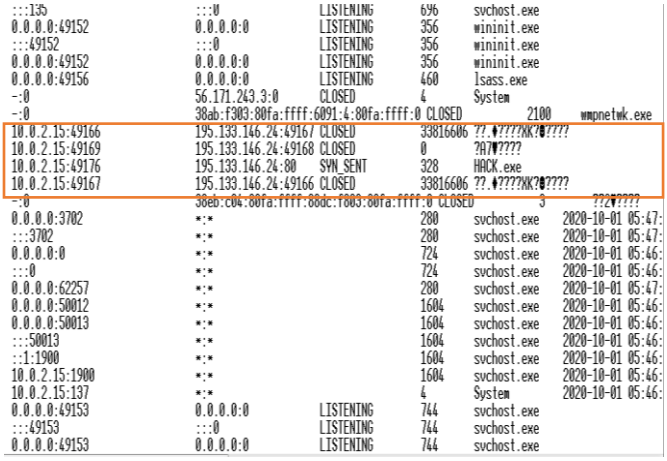

Fig 11 Netscan volatility process

Referring to Fig 11 by using the command volatility_2.6_win64_standalone.exe netscan –f USER-PC-20201001-060252.raw –profile = Win7SP1x64, all the connections that interact with the computer are displayed. Hack.exe malware is seen interacting with the ip address 195.133.146.42 and trying to synchronize the intended ip. It can be seen that there is a difference in Figure 11 and Figure 8, where the ip recorded on the inverted ip volatility is not like in Fig 8, the ip recorded is 24,146,133,195.

```
C:\Users\User\Desktop\volatility_2.6_win64_standalone>volatility_2.6_win64_standal
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa8002685820 0x0000000001360000 HACK.exe             OK: executable.328.exe

C:\Users\User\Desktop\volatility_2.6_win64_standalone>
```

Fig 12. Dump file process

Referring to Fig 12 is the dump file process using the volatility_2.6_win64_standalone.exe command procdump –p 328 –D dumpfile –f USER-PC-20201001-060252.raw –profile = Win7SP1x64 after running the data is dumped so that it becomes an executable file which later The file can be uploaded to virustotal.com as shown in Fig13.

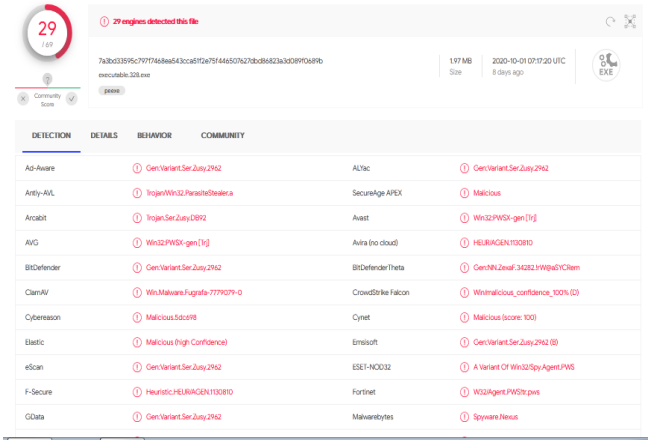

Fig 13. Virustotal analysis

Refer to Fig 13 after being analyzed by virustotal.com, it turns out that the malware is a trojan and can be detected by 29 anti-viruses. Halis virustotal.com analyzes that files entered on the website are a variant of malware.

Malware workflow

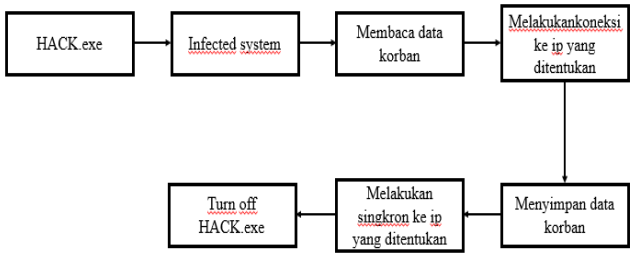

Fig 14. Hack.exe malware workflow

Referring to Fig 14 shows how the hack.exe malware works on the system. Malware that has been run is infected with the system. The malware then reads the necessary data, such as the system used by the computer, personal data on the victim's computer, and the hardware used by the victim, which will be stored by the malware. After the data is stored then synchronizes on the ip 24.146.133.195. Malware will continue to run the process shown in Figure 14 even though the victim's computer has no connection.

Prevention

malware in particular Hack.exe malware can be prevented by the following things:

1. Be on the lookout for all email submissions from unknown sources
2. Files files from unknown sources not to download or run
3. Install and activate the antivirus which can detect hack.exe malware

Recovery of systems infected with hack.exe malware

victims who have been infected by hack.exe can do the following things:

1. Install an antivirus that can detect hack.exe malware as shown in Figure 13
2. Performs a scan on the computer using an antivirus
3. Users must change their user name and password for social media or anything

V. CONCLUSION

This study, entitled "Hack.Exe Malware Analysis with Reverse Engineering and Memory Forensic Methods" is based on the research that has been done, it can be concluded as follows:

1. The malware analysis process is carried out using dynamic methods, riverse engineering, and memory forensics. The malware analysis process begins with the installation of a virtual machine, virtual network settings, process monitor filters, diassemblers, and memory forensics.

2. The way the hack.exe malware works is to infect the system, read data and store the data needed. Synchronize with the ip address 24.146.133.195.

Thank-you note

The author is grateful to Allah SWT, with his grace and grace this research can be completed. The author would like to thank the supervisors who always guided patiently in carrying out this writing and research, to parents with all their support and to related parties who have helped the author in completing this research.

ACKNOWLEDGEMENT

The author is grateful to Allah SWT, with his grace and grace this research can be completed. The author would like to thank the supervisors who always guided patiently in carrying out this writing and research, to parents with all their support and to related parties who have helped the author in completing this research.

REFERENCES

[1] R. Adenansi and L. A. Novarina, "MALWARE DYNAMIC," *JOEICT (Jurnal of Education and Information Communication Technology) ,* pp. 37-43, 2017.

[2] Lintasarta, "http://blog.lintasarta.net/article/infografis-tips-mengamankan-bisnis-anda-dari-serangan-siber/," kamis april 2020. [Online]. Available: http://blog.lintasarta.net/.

[3] İ. Kara and M. Aydos, "Üçüncü Nesil Cerber Ransomware Zararlı Yazılımının Statik ve Dinamik Analizi Static and Dynamic Analysis of Third Generation Cerber Ransomware," *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism,* pp. 12-17, 2018.

[4] A. P. Aldya , N. Widiyasono and T. P. Setia , "Reverse Engineering untuk Analisis Malware Remote Access Trojan," *JEPIN (Jurnal Edukasi dan Penelitian Informatika),* pp. 40-45, 2019.

[5] A. H. Muhammad, B. Sugiantoro and A. Luthfi, "METODE KLASIFIKASI DAN ANALISIS KARAKTERISTIK MALWARE MENGGUNAKAN KONSEP ONTOLOGI," *TEKNOMATIKA,* pp. 16-28, 2017.

[6] D. Schwarz and M. Mesa, "https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns," rabu mei 2020. [Online]. Available: https://www.proofpoint.com/.

[7] P. B. Gadgil and S. Nagpure , "ANALYSIS OF ADVANCED VOLATILE THREATS USING MEMORY FORENSICS," *CONFERENCE ON TECHNOLOGIES FOR FUTURE CITIES (CTFC),* 2019.

[8] H. A. Nugroho and Y. Prayudi, "PENGGUNAAN TEKNIK REVERSE ENGINEERING PADA MALWARE ANALYSIS UNTUK IDENTIFIKASI SERANGAN MALWARE," *STMIK Dipanegara Makasar,* pp. 1-8, 2015.

[9] N. Zalavadiya and P. Sharma, "A Methodology of Malware Analysis, Tools and Technique for windows platform – RAT Analysis," *International Journal of Innovative Research in Computer and Communication Engineering* , pp. 5042-5054, 2017.

[10] D. Uppal, V. Mehra and V. Verma, "Basic survey on MalwareAnalysis,Tools and Techniques," *International Journal on Computational Sciences & Applications (IJCSA)* , pp. 103-112, 2014.

[11] C. Rathnayaka and A. Jamdagni, "An Efficient Approach for Advanced Malware Analysis using Memory Forensic Technique," *IEEE Trustcom/BigDataSE/ICESS,* pp. 1145-1150, 2017.

[12] F. Bahtiar, N. Widiyasono and A. P. Aldya, "Memory Volatile Forensik Untuk Deteksi Malware," *JuTISI,* pp. 242-253, 2018.

[13] R. Syaputra and S. , "Studi Literatur Analisis Malware Menggunakan Metode," *Jurnal Jaringan Komputer dan Keamanan,* pp. 14-24, 2020.

[14] D. R. Septani, N. Widiyasono and H. Mubarok , "Investigasi Serangan Malware Njrat Pada PC," *Jurnal Edukasi dan Penelitian Informatika (JEPIN,* pp. 123-128, 2016.

[15] B. Sarmun, "https://suaramerdekasolo.com/2019/08/30/waspadai-hese-ransomware/," Jumat Agustus 2019. [Online]. Available: https://suaramerdekasolo.com.

[16] S. Y. S , y. Prayudi and I. Riadi, "Implementation of Malware Analysis using Static and Dynamic Analysis Method," *International Journal of Computer Applications,* pp. 11-15, 2015.

[17] S. Megira, A. R. Pangesti and F. W. Wibowo, "Malware Analysis and Detection Using Reverse Engineering Technique," *IC-ELINVO* , p. 12, 2018.

[18] T. A. Cahyanto, V. Wahanggara and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware," *JUSTINDO, Jurnal Sistem & Teknologi Informasi Indonesia,* pp. 19-30, 2017.

[19] S. Almarri and D. P. Sant , "Optimised Malware Detection in Digital Forensics," *International Journal of Network Security & Its Applications (IJNSA),* pp. 1-15, 14.

[20] Microsoft, "Windows Dev Center," 2018. [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/ms684175(v=vs.85).aspx . [Accessed 2 Juli 2018].