Implementation of Malware Analysis using Static and Dynamic Analysis Method

By Imam Riadi

International Journal of Computer Applications (0975 – 8887)
Volume 117 – No. 6, May 2015

Implementation of Malware Analysis using Static and Dynamic Analysis Method

Syarif Yusirwan S
Universitas Islam Indonesia
Jln. Kaliurang km.14.5,
Yogyakarta

Yudi Prayudi
Universitas Islam Indonesia
Jln. Kaliurang km.14.5,
Yogyakarta

Imam Riadi
Ahmad Dahlan University
Jln. Prof.Dr.Soepomo,
Janturan, Yogyakarta

ABSTRACT
Malware analysis is a process to perform analysis of malware and how to study the components and behavior of malware. On this paper it will use two methods of malware analysis, static analysis and dynamic analysis. Static analysis is a method of malware analysis which done without running the malware. While dynamic analysis is a method of malware analysis which the malware is running in a secure system [7]. Malware analysis is important, since many malware at this day which is not detectable by antivirus. Now viruses are made with special ability to avoid detection from antivirus [9]. On this research we will focus on implementation of malware analysis using static analysis and dynamic analysis method.

General Terms
Computer Security

Keywords
Malware Analysis, Malware Analysis with Static and Dynamic Analysis, Malware Analysis with Static Analysis, Malware Analysis with Dynamic Analysis.

1. INTRODUCTION
Currently, the number of programs created for the purpose of crime and illegal grow quickly. Many of these programs are malware that is created to support the growth of the organization, computer crime. Of course, criminals take advantage of the malware to take over computers and steal personal data, confidential or otherwise use such information for profit. The addition of the number of malware for doing crime forced more digital forensic investigator for malware analysis and use tools that previously were part of the antivirus vendors and security researches. Today, malware forensics has become part of computer forensics [12]. The goal of malware forensics is to identify and analysis unknown malware. Many of the new malware created with the ability to evade detection from antivirus. Therefore, it is necessary to get the malware analysis a complete information regarding the ability of malware so they can be aware of impact damage or theft of data that can be performed by malware [9].This research will be used malware TT.exe as a malware sample. Malware TT.exe is a malware that recently discovered by researchers and has been share on malware research community [15]. The advantages of this malware are its ability to avoid detection from antivirus. Antivirus usually only able to detect new malware when their get updates on its database. Based on that ability malware TT.exe will be used as sample and become object of malware analysis using static analysis and dynamic analysis method with the aim to give an explanation on the process of malware.

2. RELATED WORK
Previously, Distler [1] has used static and dynamic analysis for malware analysis.Meanwhile, Ari [16] also been doing malware analysis with reverse engineering techniques using biscuit apt1 as a malware sample. Another malware analysis research also doing by Flores [3] with win32.Kryptic. In the mean time, Daoud [12] has research regarding technique used by malware to avoid detection from antivirus. Research conducted by Uppal [8] more focus on technique and tools used in malware analysis.

Most of the literature we came across during our research was either focused on static analysis method or technique used for analysis malware without running the application directly. Whereas our work is combines two methods of malware analysis, static and dynamic analysis method to get more detail information for characteristics of malware.

3. MALWARE ANALYSIS METHOD
Malware analysis is a process to perform the analysis of malware and how to study the components and behavior of malware. For analysis malware, there are two main techniques for analysis malware that are the most commonly used method was static analysis and dynamic analysis. Static analysis is a method of analysis of malware that done without running the malware, so analysis using this method is much more secure than using the method of dynamic analysis. Malware analysis using the method of static analysis can be divided into two stages, namely basic static analysis and advanced static analysis. Whereas dynamic malware analysis is a method of analysis of malware by running the malware. To make it more secure, malware will run inside a virtual machine so the malware will not damage your computer system [1][3][5][7]. Malware analysis using the method of dynamic analysis can be divided into two stages, namely basic dynamic analysis and advanced dynamic analysis. Malware analysis method can be seen in Fig 1.

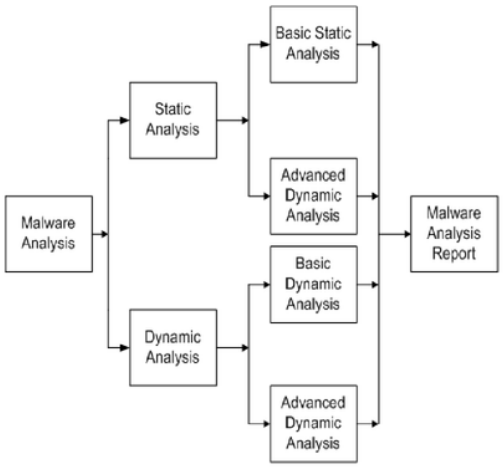

Fig 1: Malware analysis method

3.1 Basic Static Analysis
The basic method in static analysis, carried out testing against a program which is alleged as malware with doing the scanning using antivirus, moreover also doing hashing, and detection of packed or obfuscated at the program. As well as conducting an analysis of the structure of portable executable which is owned by the program.

3.2 Advanced Static Analysis
In the advanced method of static analysis, further analysis will be undertaken of the method of static analysis with analysis against the strings, linked libraries and function as well as using IDA disassembler.

3.3 Basic Dynamic Analysis
The basic method in dynamic analysis, will be build a virtual machine that will be used as a place to do a malware analysis. In addition, malware will be analysis using malware sandbox and monitoring process of malware and analysis packets data made by malware.

3.4 Advanced Dynamic Analysis
In the advanced method of dynamic analysis, further analysis will be undertaken of dynamic analysis methods with debugging on malware, analysis the registry and do an analysis on a windows system.

3.5 Malware Analysis Report
From the results of malware analysis using static analysis and dynamic analysis method, we will obtain a report of information on the characteristics of malware.

4. MALWARE ANALYSIS TECHNIQUE
In this section, we will explain some of the technique which will be used in this research for malware analysis.

4.1 Detecting Packed/Obfuscated
Packed or repacked malware is malware that has been modified using a runtime compression so that the malware will become more difficult to be recognized by antivirus and make it more difficult for malware researchers doing malware analysis [13]. While the obfuscated was a method to make the source code or machine language of a program becomes more elusive. Obfuscated normally used by programmers at their program in order to make harder to be hijacked, but malware makers also use these techniques to create his malware becomes more difficult to be detected and analyzed by malware researchers [7].

4.2 Deobfuscated
Deobfuscated is a method to restore or clean the program that previously have been protected by obfuscated. By doing deobfuscated, the language machine or assembly language of a program that had previously been scrambled, can be restored as before, so it will make more easy for researchers to conduct analysis of malware [2].

4.3 Disassembler
Disassembler is a computer program that converts machine language into a language that is easier to understand by humans. By doing a disassembler, researchers will be able to perform malware analysis and try to understand malware with analyze the assembly language and collecting information from malware program which can be used to identify the characteristics of malware [2].

4.4 Reverse Engineering
Reverse engineering is a process of taking parts of software or hardware, analyzing the function and the information obtained and then translate that process into a language that is more easily understood by humans. The purpose of reverse engineering is usually to duplicate or improve the functionality of the original product. Whereas, on malware analysis purpose of doing reverse engineering is to understand the workings of a malware [2].

4.5 Debugging
Debugging is a method to find the process and instructions of assembly/machine language that is obtained when running a program or piece of hardware. Debugging on a malware made to get information about the workings of malware by looking at the instructions made by the malware [14].

5. MALWARE ANALYSIS TOOLS
On this research will used several program to help analysis of malware using static analysis and dynamic analysis [2][3][5][7][8][10][16]. For malware analysis with basic method of static analysis can be performed with tools such as can be seen in table 1.

Table 1. Brief overview of basic static tools

Basic static analysis tools	Description
Virustotal.com	Virustotal is a website that provides a malware check against program.
Md5deep	md5deep is a set of programs to compute MD5, SHA-1, SHA-256 on an arbitrary number of files.
PEiD	Tools for detecting packed/obfuscated techniques.
Exeinfo PE	Tools for detecting packed/obfuscated techniques.
RDG Packer	Tools for detecting packed/obfuscated techniques.
D4dot	Tools to remove obfuscated .Net Reactor technique.
PEview	PEview is tools to display the structure and content of the Protable Executable.

For malware analysis with basic method of dynamic analysis can be performed with tools such as can be seen in table 2.

Table 2. Brief overview of basic dynamic tools

Basic dynamic analysis tools	Description
Virtualbox	VirtualBox virtual machine that is used as a place to run the malware.
Anubis	Anubis is a malware sandbox created specifically for automatic malware analysis.
Comodo Instant Malware Analysis	Comodo Instant Malware Analysis is a malware sandbox created specifically for automatic malware analysis.

Process Monitor	Process Monitor is a program that monitors and displays all activities within the system in real-time.
Process Explorer	Process Explorer is a program that monitors the processes that are currently in the system path of the computer.
ApateDNS	ApateDNS is a tool that is able to find out the IP address which is contacted by the malware.
Wireshark	Wireshark is a program that can take the data contained in the packet network for analysis malware.

For malware analysis with advanced method of static analysis can be performed with tools such as can be seen in table 3.

Table 3. Brief overview of advanced static tools

Advanced static analysis tools	Description
BinText	BinText is a program which is capable of searching and display character strings from a binary file.
Dependency Walker	Dependency Walker is a program that performs the scanning modules on 32 bit or 64 bit programs.
IDA	The Interactive Disassembler (IDA) is a disassembler program.

For malware analysis with advanced method of dynamic analysis can be performed with tools such as can be seen in table 4.

Table 4. Brief overview of Advanced dynamic tools

Advanced dynamic analysis tools	Description
OllyDbg	OlldyDbg are the tools used to perform debugging/reverse engineering to malware.
Regshot	Regshot is tools that are used to help analyze the registry.

On this research will be used malware TT.exe as a sample malware, and the test will be performed using the malware analysis static and dynamic analysis method. Details of the process malware analysis method can be seen in Fig 2.

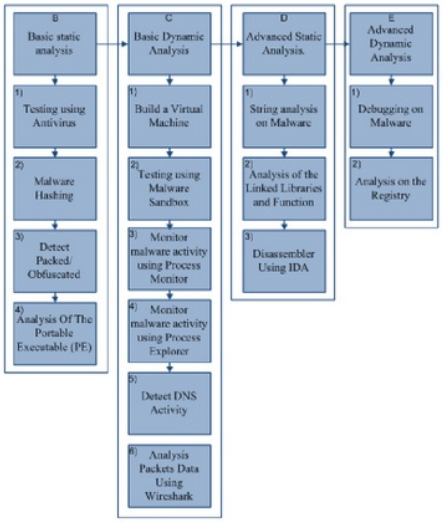

Fig 2: Detail procedure of malware analysis

6. RESULT

To demonstrate the effectiveness of the static and dynamic analysis method we have performed certain experiments by executing the malware sample and observing the response of the system.

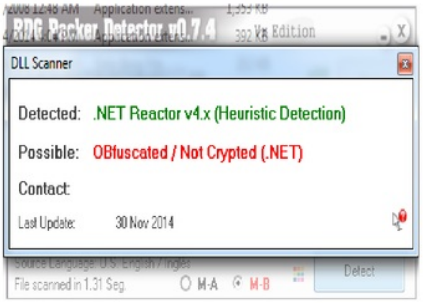

Fig 3: RDG Packer Detector to identify malware packer

In figure 3 we can seen the program which be used for identified packed/obfuscated technique owned by a malware program. The result from detection of malware TT.exe known as obfuscated technique with .Net Reactor v4.x as a possible packer.

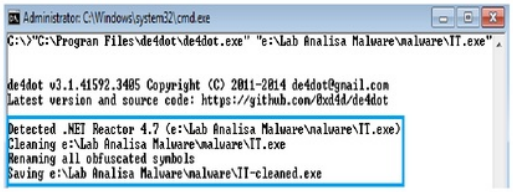

Fig 4: Clean obfuscated technique with d4dot

Once the type of packed/obfuscated is already known, the next step is finding way how to deobfuscated protection of malware. On this experiment can be used d4dot program to clean up the malware obfuscate.

Fig 5: New clean malware TT.exe generate by d4dot

On figure 5 shows the results obtained clean malware using the extraction of malware TT.exe using d4dot. At this point, clean malware TT.exe will be used for further analysis.

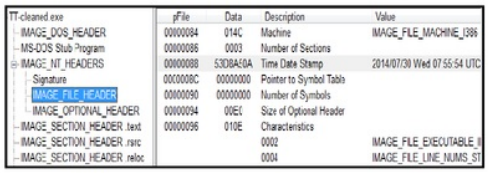

Fig 6: Analyzing PE with program PEview

On figure 6 shows the experiment using program PEview for doing analysis on portable executable own by a malware. From this experiment will be obtained the time of malware create.

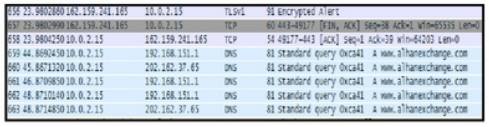

Fig 7: Analyzing malware network activity with wireshark

On figure 7 will be doing analysis with wireshark for detecting network activity performed by malware. At this experiment found malware TT.exe try to communicating with domain alhanexchange.com.

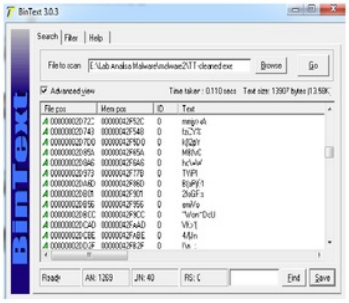

Fig 8: Analyzing string malware with Bintext

On figure 8 shows the program Bintext used to find strings from malware program which will make analysis of strings become more easily.

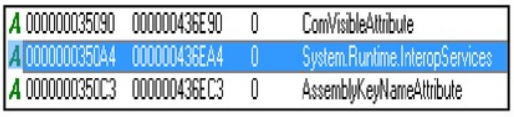

Fig 9: Example string from malware TT.exe

As an example can we seen in figure 9 which System.Runtime.InteropServices on malware strings can be interpreted as malware function who can intercepts keystroke at the keyboard or the mouse used by user.

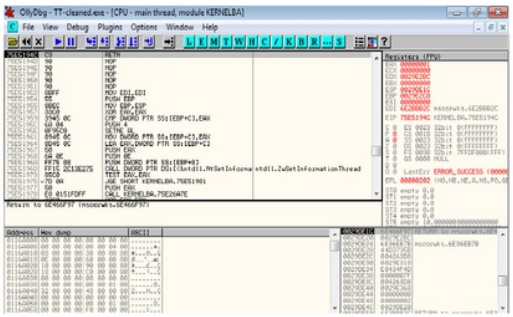

Fig 10: Debugging malware with Ollydbg

On figure 10, we can seen ollydbg which will be use for debugging on malware.

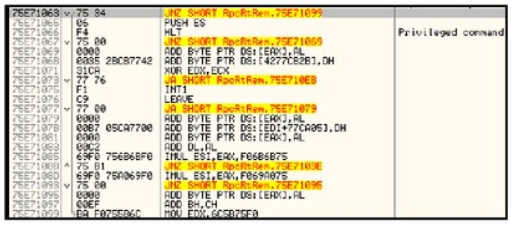

Fig 11: Example function of malware on Ollydbg

As an example can we seen in figure 11, malware TT.exe also infects RpcRtRem known as DLL needed by windows remote desktop.

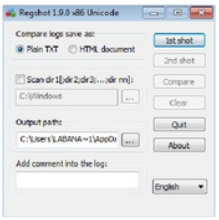

Fig 12: Analyzing registry with regshot

For figure 12 shows the Regshot is used to assist in the analysis of the registry. Regshot can help identify changes which create by malware on registry with compare state of registry before and after malware executed.

Fig 13: Analyzing registry with regshot

As an example on figure 13 we can seen malware create key on registry, which have function to run the malware everytime the operating system start.

Based on experiments done by researcher to malware TT.exe with method of static analysis and dynamic analysis, it was concluded from the analysis of malware as follows:

Malware TT.exe is a trojan type malware, created on wednesday july 30, 2014, targeting windows 7 and windows 8. In the beginning when malware TT.exe active, malware will run some process on the computer victim such as copy

itself to location %AppData\Roaming% and remove the original malware. Besides that, malware also create some registry which makes malware TT.exe run at the sartup. When malware TT.exe already infected the computer system, the malware will use a lot of computer memory to run the program as well as infect another programs which run in computer victim. Malware TT.exe also turning off most of the windows security system, such as windows defender, firewall, system restore, as well as contacting server malware in the address alhanexchange.com. Malware TT.exe also make a way for hacker to get access into computer system, by opening up port 313436. Process infection of malware TT.exe can be seen in Fig 14.

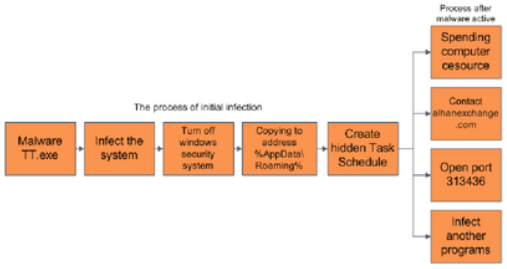

Fig 14: Process of malware TT.exe

7. CONCLUSION

In this paper, we focus on an implementation of malware analysis using static and dynamic analysis methods to provide guides and an overview about how to analyze a malware.

On the analysis of malware using basic method of static analysis, the first thing to do is doing identification at the program which is alleged malware or not, beside that on this method also detects packed/obfuscated technique used by malware, as well as finding malware creation time. Meanwhile, on the malware analysis with advanced static analysis methods capable of providing more complete information about characteristics of malware, such as the information of malware to infect another programs, as well as modifying the registry and create new files and folders.

Whereas on basic methods of malware dynamic analysis can discover DLL of malware, the process of malware inside the system, as well as the network connection performed by malware against the server. Meanwhile, malware analysis with the advanced dynamic analysis method can provide information not previously found by other methods, the malware is able to turn off windows security systems such as firewalls, antivirus and system restore.

Based on this research, the merging of the two methods of malware analysis that is static analysis and dynamic analysis is able to provide a more complete picture of the characteristics of malware TT.exe.

Further issues for malware analysis with static and dynamic analysis requires a long time in the process. On the future need to minimize the time for doing malware analysis but still obtain the detail result from the malware.

8. REFERENCES

[1] Distler, D. 2007. Malware Analysis: An Introduction. Jurnal of SANS Institute. December, 2007.

[2] Eilam, E. 2003. Reversing - Secrets of Reverse Engineering. Indianapolis: Wiley Publishing, Inc.

[3] Flores, R. 2012. Malware Reverse Engineering part1 of 2. Static analysis. Technical Report.

[4] Kaur, G., & Nagpal, B. 2012. Malware Analysis & its Application to Digital Forensic. International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 04 April 2012.

[5] Kendall, K., 2007. Practical malware analysis. Technical Report. Mandiant, Intelligent Information Security.

[6] Palo Alto Network. Analysis of New and Evasive Malware in Live Enterprise Networks. Technical Report. 1st Edition, March 2013.

[7] Sikorski, Michael, Honig, A. 2012. Practical Malware Analysis. San Francisco: William Pollock.

[8] Uppal, D., Mehra, V., & Verma, V. 2014. Basic survey on Malware Analysis, Tools and Techniques. International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

[9] Vigna, G. 2014. Antivirus Isn't Dead, It Just Can't Keep Up. Technical Report. Lastline Labs, May 2014.

[10] Zahn, K. J. 2013. Case Study: 2012 DC3 Digital Forensic Challenge Basic Malware Analysis Exercise. Journal of SANS Institute, August, 2013.

[11] Wenhua, Luo; Tang Yanjun, L. N. 2012. Reverse Analysis of Malwares: A Case Study on QQ Passwords Collection. Journal of Software, Vol. 7, No. 8, August 2012.

[12] Daoud, E. Al, Jebril, I. H., & Zaqaibeh, B. 2008. Computer Virus Strategies and Detection Methods. Int. J. Open Problems Compt. Math., Vol. 1, No. 2, September 2008.

[13] Arasu Bharati, S. R. 2014. Detection of Packed and Polymorphic Malware Using Malwise. International Journal of Advance Research in Computer Science and Management Studies. Vol. 2, Issue 1, January 2014.

[14] Almarri, S., & Sant, P. 2014. Optimised Malware Detection in Digital Forensics. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[15] Malwaretips.com. 2014.

[16] Ari N, H. 2014, Penerapan Analisa Malware Pada Biscuit apt1 Menggunakan Teknik Reverse Engineering. Journal of KNSI, February 2015.

Implementation of Malware Analysis using Static and Dynamic Analysis Method

ORIGINALITY REPORT

3%

SIMILARITY INDEX

PRIMARY SOURCES

1	Wu Liu. "Behavior-Based Malware Analysis and Detection", 2011 First International Workshop on Complexity and Data Mining, 09/2011 Crossref	71 words — 2%
2	puppylinux.org Internet	14 words — < 1%
3	www.comss.ru Internet	10 words — < 1%
4	Byung-Jin Lee, Won-Ho Jeong, Yong-Won Kim, Kyung-Seok Kim. "Error Reduction Approach for Performance Improvement in CSK Systems", International Journal of Computer and Communication Engineering, 2015 Crossref	8 words — < 1%

EXCLUDE QUOTES OFF

EXCLUDE MATCHES OFF

EXCLUDE BIBLIOGRAPHY OFF