Journal of Theoretical and Applied Information Technology
31st July 2015. Vol.77. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE RECOGNIZE OF MALWARE CHARACTERISTICS THROUGH STATIC AND DYNAMIC ANALYSIS APPROACH AS AN EFFORT TO PREVENT CYBERCRIME ACTIVITIES

[1]YUDI PRAYUDI, [2]SYARIF YUSIRWAN
[1,2] Department of Informatics, Universitas Islam Indonesia
Yogyakarta, Indonesia
E-mail: [1]prayudi@uii.ac.id, [2]5yarif.y.s@gmail.com

ABSTRACT

A lot of Malware used to carry and conceal the crime even included as a crime toolskit. This is forcing digital forensics investigators to perform malware forensics activities, namely to identify and analyze unknown malware before. Knowing the characteristics of malware will be one of the solutions from the prevention of cybercrime activity. One method that can be used is the combination of static and dynamic analysis to get a complete information about malware characteristics. In this study both the method used to analyze malware TT.exe, as well as handling solutions. The results obtained show that the use of both of these methods can provide a complete information about the characteristics of malware TT .exe. This research also has given a solution that can be done to prevent the spread of malware TT .exe

Keywords: *Malware Analysis, Static and Dynamic Analysis, Cybercrime*

1. INTRODUCTION

Malware is one of the most serious threats to system security [1]. Malware is a program installed on a system without the knowledge of the owner of the system. It is basically installed by the third party with the intention to steal some private data from the system or simply just to play pranks [2]. According to [3], malware has characteristics to avoid from forensics detection and forensics analysis. For that malware is often used as a means for the occurrence of a criminal activity.

PWC and RSA have made reports which are then cited by [4], shows that cybercrime is a serious threat, causing losses that could affect the national income of a country.

The growing issue of malware has been pushing The Science and Technology Committee to do some research about the interconnectedness of malware with cybercrime. The results show that there is a significant proportion of cyber-crime malware uses to perform some part of the crime [5]. Meanwhile, research from RSA [6] shows that the top cybercrime attack is generally done using malware. That is according to [1][7] malware is one of the most serious threats to system security and then categorize the malware as crime toolkits.

Studies conducted by Islam et al., (2009) in [1], mentioned that out of 450,000 files downloaded, approximately 18% contained malware programs. Furthermore, Panda Labs reported that the malware development has reached the highest number in the first quarter of 2014. PandaLabs detected 15 million new malware in the first three months, with an average increase of about 160,000 new types every day. Trojan remains as the most threatening malware; it amounts to 71.85% of the total malware ever created. In addition, the method of malware deployment is increasingly diverse and sophisticated, making it harder to be detected and analyzed [8].

In Indonesia, the ID-CERT (Indonesia Computer Emergency Response Team) has begun to collect data to report the spread of malware in the current situation [9]. In addition, some local vendors for antivirus have also carried out an analysis of malware deployment in Indonesia. In this regard, according to the data issued by Vaksin.com, Trojans becomes the most malware type in Indonesia with a total of 24.30%, followed by adware with 23.8% of all the total existing malware [10].

Malware can incorporate various techniques to not only avoid forensic detection, but can also avoid

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

forensic analysis [3]. The increasing number of malware that can be used to commit cybercrime activity has prompted law enforcement and digital investigators to explore the field of malware analysis. Malware analysis previously was undertaken by antivirus vendors and security researchers, but current malware analysis has also become part of digital forensics activity. It is later known as malware forensics, that is, forensics activities to identify and analyze unknown malware [11]. Furthermore, according to [12] digital forensics and malware analysis are two topics which both involve methods to find out as much as possible about something that happened, how and who was involved. The difference between digital forensics and malware analysis depends on what evidence you look for, which is in this case malware characteristics and patterns.

The goal of our research is to optimize the research paradigm for malware analysis using static and dynamic analysis and to improve the investigatory experience by employing an active approach to detecting malware activities. Malware analysis is an important part of understanding the objectives of the malware and how to defend against this threat [13]. The malware characteristics obtained from the analysis can serve as prevention of the spread of the malware itself and reduce the potential of cybercrime.

2. PROBLEM OF MALWARE ANALYSIS

All the antivirus programs always update their capabilities to detect and prevent threats from to the existing malware, in fact, many new types of malware are found and nearly half of them are not detected by antivirus products. Even after three months, one of the three antivirus scanners fails to detect the sample of available malware [14]. According to Dambala, that cited by [15], it can take up to 6 months to make an anti-virus products recognize 100% of malware.

New types of malware are created with the ability to evade detection from antivirus. This is in line with research conducted by Palo Alto toward ± 26,000 malware samples obtained during three-month data retrieval in 1000 companies. He tested the samples using six best antivirus products. Surprisingly, it was found that 90% of malware samples were not able to be recognized by those antivirus products. New malware is designed with the ability to disguise themselves in the victim's computer or turn off the security system owned by the computer so that the malware can keep alive and continue spreading [16]. According to [1], sophisticated tools and methods, making malware activities more complicated for its detection.

Furthermore according to [17], one of the challenges in the malware analysis is malware often packaged with software that seems to provide legitimate functionality, with malicious behavior exposed only under certain "trigger conditions", e.g., when a command is received from a remote site controlled by an attacker. In addition [17] also mentioned that malware may incorporate with anti-analysis features so that malicious paths are avoided when executed within an analysis environment.

Among the many types of malware, one type that is undetectable is TT.exe malware. The malware was first reported and discussed in the site http://malwaretips.com on July 30, 2014. This malware is categorized as trojan/backdoor malware, and after being active, usually this type of malware installs itself into a computer and opens access for attackers/hackers [16]. This can be the first step of various acts of cybercrime, such as data destruction, theft of important information, or even other activities that cause material losses. When this research is conducted (January 2015), TT malware is still included in the category of malware that is unable to be detected by common antivirus software.

Therefore, we need another method to analyze the malware to get a complete information about the capability of such malware so that we can figure out how it works and the potential negative impacts it generates. According to [2], the use of static and dynamic analysis provides a number of advantages in terms of malware analysis, but the report does not explain how the implementation of that hybrid method usage for malware analysis.

In this research, static and dynamic analysis methods are combined in order to obtain a more in-depth information about TT. exe malware characteristics and the handling solutions. The hypotheses in this research are: malware analysis using the combined method of static analysis and dynamic analysis could gather information regarding the characteristics of malware and could provide a solution to deal with TT .exe malware infection.

3. CHARACTERISTIC OF MALWARE

Malware or malicious software is a program used to disrupt computer system, steal personal

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information, or gain access to one's computer system without permission. Malware can appear in various forms, such as codes, scripts, active contents, or software.

Alazab [7] has been doing research on how historical development as well as the characteristics of some malware. According to [7], demand in the underground market has become a trigger for the development of the malware.

According to [16][2], malware is usually described based on its form as follows:

a. Trojan/Backdoor is a malicious program that can install itself into the victim's computer to open the gate for hackers. Backdoor usually makes a hacker can connect into a victim's computer without permission and run certain commands on the computer.
b. A Botnet is malware that has the ability like backdoor, but when a computer is infected with a botnet, the computer will obey the orders as instructed by the server control.
c. Downloader is a program typically installed by hackers when they already have access to the victim's computer system. Malware belonging to downloader will download and install other malware onto the victim's system.
d. Information-stealing malware is malware that gathers information from a victim's computer and transmit the obtained data to a particular party. The examples of this type of malware are sniffers, password hash grabbers, and keyloggers.
e. A Rootkit is a program made to conceal the other malware so that it cannot be detected by antivirus.
f. Scareware is malware that aims to scare the victim with certain messages that require the victim to buy a particular program to eliminate the malware.
g. The Virus is a malicious program designed to destroy a computer system, such as by causing a breakdown in the operating system, excessive usage of memory in a computer, or performing data destruction.

According to [14], no computing platform or environment is immune to these threats, even the spectrum of malware that represent a real threat is expansive.

Furthermore, according to [18], malware cannot be detected by antivirus due to the following characteristics of malware:

- Analysis Avoidance: having special features to avoid an analysis in malware sandbox or any other security tools
- Persistence: having various ways of working that make the malware remain alive in the host for a long time.
- Hacking: having the ability to spread out through the network of infected computers and malware usually performs fingerprinting to the surrounding networks, as well as identifying vulnerable computers.

4. MALWARE ANALYSIS

One of the earliest research on malware was conducted by Dennis Distler in 2007 about the introduction of malware analysis by using code (static) analysis and behavioral (dynamic) analysis method. Nevertheless, on such research, malware analysis method used was still simple and was not as precise and complex as malware analysis today [19]. A similar study was conducted by [20] through malware analysis on biscuit apt1 using reverse engineering technique.

The same research was also carried out by Flores toward malwarewin32. kryptic by using static analysis method [21]. In this research, Flores used static analysis method to observe malwarewin32.kryptic by hashing on the malware and then continued with accessing the information and detecting a connection that had been made by the malware. The Static method applied on such research was not able to give a complete information about malware activity.

Meanwhile, according to [13] malware analysis is done in three separate phases; surface, dynamic and static analysis. Surface analysis consists of recognizing or discovering a malware signature. The dynamic analysis concerns with the execution of the software to be able to study its behaviour. Static analysis may be necessary in order to realize a complete understanding of the sample, or in certain cases necessary to be able to run the software in a controlled environment. His research used ircbot.exe and unknown.exe as the sample to be analyzed. His research demonstrated that the two malware samples, have different objectives and varying functionality.

Research on the techniques used by malware also has been done by [22]. In the study, they examined the techniques used by malware that made malware undetected by antivirus. In this case, according to [2], a combination of several methods and techniques for malware analysis can be applied to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

gather more in-depth information of malware activity. Static analysis, dynamic analysis, and hybrid analysis can be applied for the sake of malware analysis.

Meanwhile, according to [23], there are several techniques that can be used to perform malware analysis, such as:

- Static Analysis, malware analysis that is done without running a malware object being analyzed. It is the procedure of analyzing software without executing it [2]. This technique is much more secure than applying the dynamic analysis method [16]. While according to [3] static analysis focused on information gathering, dissasambly, symbol table regenaration, decompilation technique and methodology for determining the order of decompiling subroutines.
- Dynamic Analysis, malware analysis by way of running the malware. Malware as the object of analysis is run in a virtual machine or Sandbox so that the malware will not damage the actual computer system [16]. Dynamic analysis can be done through monitoring function calls, tracking the information flow, analyzing function parameters and tracing the instructions [2].
- Automated Malware Analysis, malware analysis method that is carried out automatically in the malware sandbox [24].
- Volatile Memory Analysis, malware analysis method has done by analyzing a memory dump or images of computer memory that has been infected with malware.

According to [14], malware analysis is becoming an important field of specialization for forensic analysts. The challenge is, mostly malware author, they have a very good understanding of digital forensic methods and endeavor to make a forensic analysis as difficult as possible. Furthermore, [14] stating that, the authors of malware are becoming increasingly profit-driven and are incorporating techniques to make their code as stealt and undetectable as possible.

5. METHODOLOGY

To do the analysis of TT.exe malware, the steps is given as follows:

- Preparing samples of malware. Samples of malware used were taken from malwaretips.com. The type of TT.exe malware was first reported on July 30, 2014.
- Creating virtual machines using Virtualbox application as a place to perform dynamic analysis of malware
- Performing malware analysis using static analysis and dynamic analysis of TT.exe malware to identify the characteristics of malware as well as knowing the impact of damage or data theft done by malware TT.exe
- Making a general report regarding the characteristics of TT .exe malware
- Providing recommendations for treatment and prevention as a solution to address the spread of TT .exe malware infection.

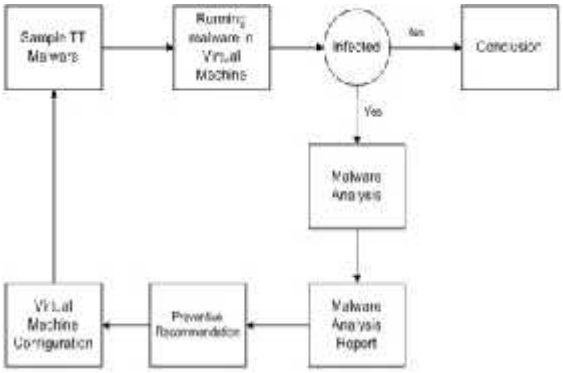

Figure 1 The Main Steps in Malware Analysis

Figure 1 shows the illustration of research step that has been conducted.

6. RESULT AND ANALYSIS

In addition to what is presented in this paper, the results of the research can also be seen on [25]. To analyze the malware with the basic static analysis method, several programs have been used that can help the process of malware analysis. In Table 1, it is seen the programs and the results obtained from the basic static analysis of malware.

After performing basic static analysis, then the next step is to do a basic dynamic analysis. To analyze the malware with the basic dynamic analysis method, a number of programs have been run to help the analysis process.

Table 1 Malware Analysis - Basic Static Analysis

Journal of Theoretical and Applied Information Technology
31st July 2015. Vol.77. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Basic Static Analysis Method	Tools	Results
1	Sending malware samples to Virustotal.com	Virustotal.com	44 of 55 antivirus engines detected that this malware belongs to Trojan type.
2	Hashing on the malware	Md5deep	md5 value: [illegible]
		PEiD v0.92	Microsoft Visual C# / Basic .NET
3	Detecting packed or obfuscated malware	Exeinfo PE	[illegible] / Not Reverse
		RDG Packer Detector v0.7.4	No Packer v4.x
4	[illegible]	[illegible]	Malware which was decompressed [illegible]
5	Portable Executable (PE) Analysis	PEView	Time creation of program: Date : Wednesday, 30 July 2014 Time : [illegible] UTC Section : Section / Virtual Size / Size of Raw Data .text / [illegible] / [illegible] .rsrc / 00001528 / [illegible] .reloc / 0000000C / 00000200

Table 2 shows the programs, and the results obtained from the basic dynamic analysis of malware. For malware analysis with advanced static analysis method, some programs were run to assist the process of malware analysis. Table 3 gives the program, and the results obtained from the advanced static analysis of malware.

Table 2 Malware Analysis - Basic Dynamic Analysis

No	Basic Dynamic Analysis Method	Tools	Results
1	Creating Virtual Lab	Virtualbox	Virtual lab used additional applications such as: 1. Windows 7 OS 2. Google Chrome 3. Mozilla Firefox 4. Flash Player 5. Java 6. Shadow Defender
2	Malware Sandbox for Malware Analysis	Anubis	1. When the malware was executed, the malware would import some DLL, such as [illegible], kernel32, advapi32, [illegible], and [illegible]. 2. Malware also added some keys in the registry
		Anubis	From the result of malware analysis using Anubis, it was not obtained any information that can help the malware analysis.
3	Sandbox Malware for Malware Analysis	Comodo	From the result of an analysis of Sandbox Comodo Malware, only a little information was successfully gathered from the malware, that is, the malware infected [illegible]
		Monitor Process	1. once the [illegible] malware was run, the malware performed some other processes, namely [illegible], [illegible] and [illegible] 2. The malware would also run the [illegible] process
4	Monitoring malware activities	Explorer Process	1. When executed, the malware would start a new process with the randomly created name. 2. Once finished running the process, the malware would remove itself from the monitoring process so it would not be visible.
5	Detecting DNS activities	ApateDNS	Malware tried to connect to [illegible] but the server had been disabled
6	Network package analysis	Wireshark	When the malware was active, the malware would receive the encrypted data of [illegible] from the [illegible] address. The malware also attempted to contact the address of [illegible]

For performing malware analysis with advanced dynamic analysis method, several programs were chosen to help the process. Table 4 displays the programs, and the results obtained from the advanced dynamic analysis of malware.

The analysis has been carried out in this research are the analysis of functional and relational analysis. According to [1] functional analysis is analysis to understand how a particular piece of malware behaves on a compromised system, while relational analysis is an analysis of how components of malware interact, and how various systems involved in a malware incident relate to each other.

Table 3 Advanced Static Analysis

No	Advanced Static Analysis Method	Tools	Results
1	String Analysis on Malware	BinText	1. Malware was able to manipulate other programs. 2. The malware was able to record keyboard and [illegible] activities and function like Keylogger. 3. The malware could shut down the victim's computer when needed. 4. The malware is a client-server based program.
2	Analysis of Linked Libraries and Function	Dependency Walker	1. The malware was able to create new processes, files, and [illegible]. 2. The malware ran CMD and performed a specific command. 3. The malware gathered information about the victim's computer. 4. The malware was able to manipulate another process. 5. The malware was able to add/remove/change data in the registry. 6. Malware made its body active at the time Windows was turned on. 7. The Malware was capable of downloading data through the internet.
3	Disassembling Analysis	IDA	1. The malware was able to be a keylogger that can read activities carried out by the user. 2. The malware could infect other programs. 3. The malware could shut down the process from the other program. 4. The malware would create another program after being run.

Table 4 Advanced Dynamic Analysis

No	Advanced Dynamic Analysis Method	Tools	Results
1	Debugging Analysis	OllyDbg	1. When the malware was run, the malware would start a new process. 2. The malware gathered information about the victim's computer. 3. The malware also made a new file in the victim's computer. 4. The malware also created a new process and inserted itself into the "startup" process. 5. In addition, the malware was also able to infect other programs. 6. The malware also infected the Remote Desktop. 7. The malware would remove itself after the process has finished.
2	Making an analysis on the registry	Regshot	1. The malware removed program schedule in the Task Scheduler. 2. The malware turned off the security system against firewall, antivirus and anti-spyware. 3. The malware activated Tracing in Windows 7 so that the programs that were run would be infected by the malware. 4. The malware turned off automatic updates on Windows 7. 5. Malware activated [illegible] to send information to the victim's server. 6. Malware turned off protection system of Windows Defender. 7. Malware could activate itself when Windows was first turned on and malware could also clone itself to the new address.
3	Doing an analysis on Port Windows 7	Netstat	Malware opened TCP Port [illegible] as an entry way for hackers.

Journal of Theoretical and Applied Information Technology
31st July 2015. Vol.77. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From the results of malware analysis with static and dynamic method above, and based on the information presented in [25], then the characteristics of TT.exe malware are as follows:

- TT.exe malware is a type of trojan created on Wednesday, July 30 2014, whose target activity is in Windows 7 and Windows 8.
- When TT.exe malware is active, the malware will run some processes such as copying itself to %AppData\ Roaming% address. Besides, the malware also gives some registry commands that enable TT.exe malware to run when the computer system is turned on. When TT.exe malware already infects the victim's computer, the malware will utilize most of the computer memory to run the program, as well as infecting other programs found in the computer. TT.exe malware will also turn off most of the Windows security system, such as Windows Defender, Firewall, System Restore, as well as contacting server malware that is in the address of alhanexchange.com. TT.exe malware also opens the way for hackers to penetrate the computer system by opening port 313436. The flow of TT.exe malware infection can be seen in Figure 2.

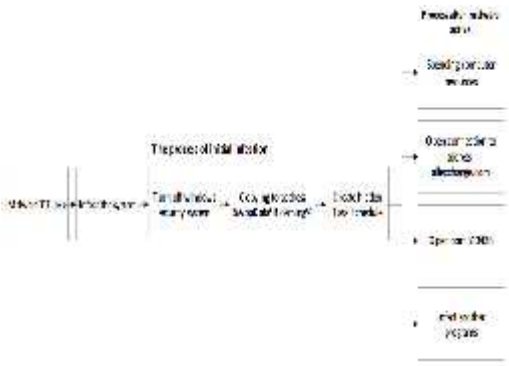

Figure 2 The Characteristics of TT.exe Malware Source Picture From [25]

- TT.exe malware is getting into a computer system through emails, spam/ pirated freeware that has not been able to be detected by the antivirus.
- TT.exe malware infects the computer system and turns off the Windows security system, including firewall, antivirus, Windows Defender, and System Restore.
- TT.exe malware will copy itself to the AppData\Roaming address and can run itself automatically when Windows starts to run.
- Computer system infected by TT.exe malware has certain characteristics, that is, high intensity of CPU computer usage and difficulty in running a computer program.

From the results of malware analysis, it is identified that TT.exe malware clones itself to the addresses below:

- C:\User\ < user name > \AppData\ Roaming \ <random>.
- C:\User\ < user name > \AppData\ Roaming <random> \ <random> \. exe.

To stop the spread of TT .exe malware infection, the malware must be blockaded through "Local Security Policies" as depicted in Figure 3. The configuration command of "Local Security Policies" that is used can be seen in Figure 4.

Malware prevention techniques as presented in Figure 4, has been run in a closed system. The analysis was done by comparing the infection process of malware TT. exe on the computer systems before and after the configuration is done. From these tests, it is known that after a configuration, the malware was not successfully activated by itself, this can be seen from its normal indication of CPU that runs on a computer system.

Figure 3 Local Security Policies Configuration

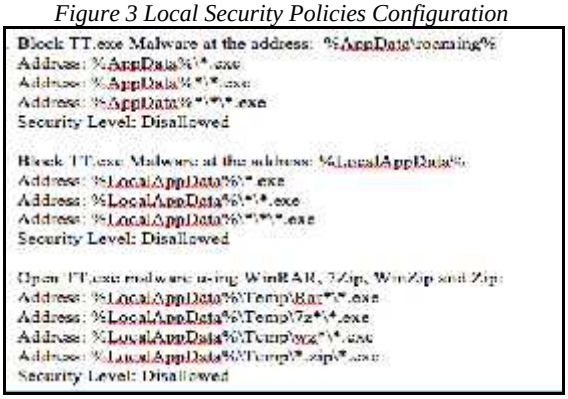

Figure 4 Security Configuration Command

In the experiments that have been conducted, applying preventive recommendations by running

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the patch as in Figure 4 was able to stop and disconnect the malware will infect the computer system.

The combination of static and dynamic analysis of malware requires quite a long time in the process. Dynamic analysis can easily detect the unknown malware by simply analyzing the behavior of the application, but the disadvantage of this analysis takes time as the executing time of the application, so in some cases, it is not fast neither safe [2].

According to [14], static analysis is very time consuming and easily hindered by anti-forensics in the form of code obfuscation, packers and protectors which are increasingly being used by malware authors. Valli [14] also mentioned that dynamic analysis, in contrast, does run the code and the analyst observes its behavior and interaction with the host and network via mechanisms such as registry, file and network monitoring tools. This technique is much easier to conduct than static analysis but is also easily eclipsed by the presence of malicious software that can detect the use of creating emulation resource in the environment such as VMware.

The success of doing an analysis of the characteristics of malware will provide knowledge to the digital investigator to handle the possibility of cybercrime activities that can be performed by the malware. One of them is to recognize the digital artefacts that can be created by the malware as well as prevention can be done so that the malware cannot walk properly.

Recognizing the characteristics of malware is a part of an effort to establish the patterns of malware. In this case, a combination of static and dynamic analysis is one of the stages of establishing a collection of knowledge that will facilitate the recognizing of a malware. According to [1], there is a three phase process for analysis malware: acquisition, detection and analysis as well as the development of the database. Thus what was done in this research to identify the characteristics of malware TT. exe can proceed with the recognizing of other types of malware that is not yet detected by anti-virus. The goal eventually is a comprehensive database that will facilitate the digital investigator to conduct the investigation process against cybercrime activities that are run by using the help of malware.

Although the characteristics of malware is likely to be increasing in sophistication and profitability, but a combination of techniques malware analysis through static and dynamic analysis that has been done can be used as a standard to recognize its a malware.

7. CONCLUSION

From the research on TT.exe malware using static analysis and dynamic analysis method, it can be inferred that:

- Basic static analysis method can be performed to make a preliminary identification of the malware, detect packed/obfuscated malware protection, as well as finding creation time of the malware. Meanwhile, malware analysis with advanced static analysis method is capable of providing more complete information about malware characteristics, such as the malware command to infect other programs, modify the registry and malware, and create new files and folders.
- Basic dynamic analysis method can identify DLL run by malware, the process done by malware in the system, as well as the connection between malware and the malware server. Meanwhile, malware analysis with advanced dynamic analysis method can provide information that has not been previously known with other methods, that is, the malware can off Windows security systems, such as firewalls, antivirus, and system restore.
- Based on the research conducted, the merging of two methods of malware analysis, namely static and dynamic analysis, can provide a complete picture of the characteristics of TT.exe malware. In addition, from the results above, a configuration can be made for preventing TT .exe malware infection.

Although each malware has different characteristics, however the steps of analysis that has been done in this research can be applied for the purposes of analysis of other malware that hasn't been detected by anti-virus.

REFRENCES:

[1] S. Almarri and P. Sant, “Optimised Malware Detection in Digital Forensics,” *International Journal of Network Security and Its Applications*, vol. 6, no. 1, pp. 1–15, 2014.

[2] D. Uppal, V. Mehra, and V. Verma, “Basic survey on Malware Analysis , Tools and Techniques,” *International Journal of Computational Science and Applications*, vol. 4, no. 1, pp. 103–112, 2014.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] M. Brand, "Forensic Analysis Avoidance Techniques of Malware," in *Proceedings of 5th Australian Digital Forensics Conference*, 2007.

[4] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody," *International Journal of Computer Applications*, vol. 109, no. 9, pp. 30–36, 2014.

[5] The Science and Technology Committee, "House of Commons Science and Technology Committee Alcohol guidelines," London, UK, 2012.

[6] RSA, "THE CURRENT STATE OF CYBERCRIME 2014 An Inside Look at the Changing Threat Landscape," 2014.

[7] A. Alazab, J. Abawajy, M. Hobbs, R. Layton, and A. Khraisat, "Crime Toolkits: The Productisation of Cybercrime," in *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 1626–1632.

[8] Panda Labs, "Quarterly Report January-March 2014," 2014.

[9] ID-CERT, "Laporan Survey Malware Periode April-Mei 2014," Bandung, 2014.

[10] A. Tanujaya, "Kaleidoskop Sekuriti Indonesia 2014," 2014. [Online]. Available: http://www.vaksin.com/1214-kaleidoskop-sekuriti. [Accessed: 07-May-2015].

[11] W. Luo, N. Li, and Y. Tang, "Reverse Analysis of Malwares: A Case Study on QQ Passwords Collection," *Journal of Softwware*, vol. 5, no. 10, pp. 1706–1712, 2010.

[12] A. O. Flaglien, "Cross-Computer Malware Detection in Digital Forensics," Master Thesis, Gjovik University Collage, 2010.

[13] P. L. Wedum, "Malware Analysis ; A Systematics Appproach," Master Thesis, Norwegian University of Science and Technology, 2008.

[14] C. Valli and M. Brand, "The Malware Analysis Body of Knowledge (MABOK)," in *The 6th Australian Digital Forensics Conference*, 2008.

[15] M. Santillan, "70 % of Malware Infections Go Undetected by Antivirus Software , Study Says," *Tripwire*, pp. 1–6, 2015.

[16] M. Sikorski and A. Honig, *Practical Malware Analysis*. San Francisco, USA: No Starch Press, 2012.

[17] L. Cavallaro, P. Saxena, and R. Sekar, "On the limits of information flow techniques for malware analysis and containment," *Lecture Notes Computer Science. (including Subser. Lecturer Notes Artificial Intelligence. Lecturer Notes Bioinformatics)*, vol. 5137 LNCS, pp. 143–163, 2008.

[18] Palo Alto, "The Modern Malware Review," 2013.

[19] D. Distler, "Malware Analysis: An Introduction," 2007.

[20] H. A. Nugroho and Y. Prayudi, "Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan," in *KNSI*, Makasar Indonesia, 2014, pp. 27–28.

[21] R. Flores, "Malware Reverse Engineering Part 1," 2012.

[22] E. Al Daoud, I. Jebril, and B. Zaqaibeh, "Computer virus strategies and detection methods," *International Journal of Open Problems Computer and Mathematics*, vol. 1, no. 2, pp. 122–129, 2008.

[23] K. J. Zahn, "InfoSec Reading Room Case Study : 2012 DC3 Digital Forensic Challenge," 2013.

[24] Zeltser, Lenny, "Introduction to Malware Analysis", Presentation SANS Institute, pp. 1–36, 2009.

[25] S. Yusirwan, Y. Prayudi, and I. Riadi, "Implementation of Malware Analysis using Static and Dynamic Analysis Method," *Int. J. Comput. Appl.*, vol. 117, no. 6, pp. 11–15, 2015.