Indian Journal of Science and Technology, Vol 8(17), DOI: 10.17485/ijst/2015/v8i17/77209, August 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

New Malware Analysis Method on Digital Forensics

Sunghyuck Hong and Sungjin Lee*

Division of Information and Communication, Baekseok University, Korea;
sunghyuck.hong@gmail.com, lsj@bu.ac.kr

Abstract

Recently, Internet usage and development of web technique are getting increased rapidly. The number of Malware occurrence has rapidly increased and new or various types of Malware have been advanced and progressed, so it is time to require analysis for malicious codes in order to defense system. However, current defense mechanisms are always one step behind of Malware attacks and there is not much research on Malware analysis. The behavior of Malware is similar to common applications. It is difficult to detect Malware by its behavior. Malware's registry must be analyzed to detect. Therefore, we propose to a new approach for Malware analysis method based on registry analysis.

Keywords: Digital Forensics, Malware, Network Security, Registry Analysis

1. Introduction

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information or gain access to private computer systems. It can appear in the form of executable code, scripts, active content and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software. The term bad ware is sometimes used and applied to both true (malicious) Malware and unintentionally harmful software. Malware means executable code which was written for malicious purposes. Virus, worm and Trojan horse belonging to it and these are also called malicious codes. The computer malicious codes are evolving fast and performing malicious actions using various vulnerability over system[1].

Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Regin or it may be designed to cause harm, often as sabotage (e.g., Stuxnet) or to extort payment (Crypto Locker). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software[3] including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware and other malicious programs. It can take the form of executable code, scripts, active content and other software[4]. Malware is often disguised as, or embedded in, non-malicious files. As of 2011 the majority of active Malware threats were worms or Trojans rather than viruses[5]. In law, Malware is sometimes known as a computer contaminant, as in the legal codes of several U.S. states[6,7]. Spyware or other Malware is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics. An example of such software, which was described as illegitimate, is the Sony rootkit, a Trojan embedded into CDs sold by Sony, which silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying; it also reported on users' listening habits and unintentionally created vulnerabilities that were exploited by unrelated Malware[8]Software such as anti-virus, anti-Malware and firewalls are used to protect against activity identified as malicious and to recover from attacks[9].

This research paper is organized as follows. Section 2 provides related work. In Section 3, we proposed our new proposal for analysis Malware and Section 4 presents performance evaluation and discussion. Finally, conclusions are given in Section 5.

*Author for correspondence

2. Related Work

Recently, network security events are occurred very often. They created disasters all around the world such as internet fraud activities and data theft, etc. Malware was the key offender. Therefore, how to detect Malware is a very important issue for network security. Malware has the potential to harm the host, which designed to infiltrate or damage a computer system without the owner's informed consent (e.g., viruses, backdoors, spyware, Trojans and worms)[17]. There are many security incidents arisen by botnet, which has caused series dangers recently. Botnet is not a specific malware. However, a method, that possibly comprised of thousands or millions hosts controlled by hackers. In the past years, botnet-based attacks became popular and dangerous. In order to facilitate observation of botnets, many researchers have proposed separate detection schemes and detection mechanism for monitoring and defending against them.

Security expert Joe Stewart revealed that in late 2007, the operators of the botnet began to further decentralize their operations, in possible plans to sell portions of the botnet to other operators[18]. Some reports as of late 2007 indicated the botnet to be in decline, but many security experts reported that they expect the botnet to remain a major security risk online[19] and FBI considers that the botnet is a major risk to increase bank fraud, identity theft and other cybercrimes[18]. As a result, the further research on the advanced botnet designed by the attackers becomes important. It is necessary to conduct such research, so as to deal with the threat of botnet facing today. Otherwise, our Internet will frequently be attacked by the Nalware in the future. This paper developed a Malware behavioral analysis tool, Taiwan Malware Analysis Net, which can analysis the varietal Malware and output analysis report. The result scan support anti-virus to detect the known or unknown malware. There are many types of Malware. Table 1 shows all types of Malware[2-4,12-16].

3. Virtual Environment for Malware Analysis

VMware virtual computing environment was used for analysis Malware in order to prevent infection on a local PC because the PC has a need to analyze downloaded Malware on virtual computing environments in the same manner as the end user environment such as a CD-ROM or a USB device can also be directly connected to analysis.

Table 1. Types of Malware

Types	Specification
Virus	A computer virus is a Malware program that, when executed, replicates by inserting copies of itself into other computer programs, data files or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be infected. Viruses often perform some type of harmful activity on infected computers, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts or logging their keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves-the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.
Worm	Network worm is usually a standalone program which runs without any user intervention. It spreads itself to other computers in the same LAN which has vulnerabilities. While the virus is a program or programming code that can graft its copy onto another program including the operating system. The virus cannot run automatically, it needs to be activated by the host program. Both the computer worm and virus can replicate and spread themselves, which makes it difficult to distinguish them. Especially, in recent years, more and more virus comes to use worms' technology. Meanwhile, worm adopts the virus technology too.
Trojan Horse	Trojan horses are computer programs that presented as useful or harmless in order to induce the user to install and run them, but also have some hidden malicious goal, such as enabling remote access and control with the aim of gaining full or partial access to the infected system. On the one hand, since polymorphism of Trojan horses, it is hard for the signature-based technology, which is the mainly used method in current anti-virus program, detecting them; On the other hand, Trojan horses have very little immediate impact on the normal operation of a system and they may go under detected for a significant period of time, allowing the attacker a large window of opportunity.
Bot	The detection of bots, Malware instances that run autonomously on a compromised host, has been a challenging problem since the bots,

	played a key role in launching all Internet threats such as DDoS, spam, information extortion, click fraud, etc. Signature-based malware detection has been the major defense against any malware including bots.
Backdoor	Security threats are coming from various sources, like natural factors or users do not have authorization to access to the network and using the software. These threats are result to the lack of authentication, authorization and auditing control, cipher algorithms weaknesses, weak keys, the risk partnership, untrustworthy data center and disaster recovering failure. According to the last Microsoft's Security Intelligence Report, in over the last decade, the spread of Malware became the crime story online. Nowadays estimates of the number of well-known threats, such including viruses, worms, Trojans, backdoors, exploits, password stealers and spyware in the millions and a backdoor has a high rate of intrusions that happens to global networks in the world. In summary, Backdoor is a hidden communication channel.
Key-logger	Key-logger is transmitted to the malicious code that an attacker to monitor and record the input from the keyboard. A key-logger is a type of surveillance software that has the capability to record every keystroke you make to a log file, usually encrypted. A key-logger recorder can record instant messages, e-mail and any information you type at any time using your keyboard. The log file created by the key-logger can then be sent to a specified receiver. Some key-logger programs will also record any e-mail addresses you use and Web site URLsyou visit. Key-loggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, key-loggers can also be embedded in spyware allowing your information to be transmitted to an unknown third party
Spyware	Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. However, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
Adware	Adware is the common name used to describe software that is given to the user with advertisements embedded in the application. Adware is considered a legitimate alternative offered to consumers who do not wish to pay for software. There are many ad-supported programs, games or utilities that are distributed as adware. Today we have a growing number of software developers who offer their goods as "sponsored" freeware (adware) until you pay to register. If you're using legitimate adware, when you stop running the software, the ads should disappear and you always have the option of disabling the ads by purchasing a registration key.

3.1 Analysis Tools

For step-by-step analysis of the infection, we used various analytical tools depending on each situation. Table 2 shows our analysis tools.

File analysis toolsare shown in Table 3 which can analysis Malware on Windows file format. Network analysis tools are shown in Table 4.

4. Experimental Results

A method of analyzing the malicious code can be classified in two ways: larger static analysis (Static Analysis) analysis and dynamic (Dynamic Analysis). In addition, the target to obtain information or to attack the infection by analyzing the malicious code, the operating

Table 2. System Analysis Tools

Types	Specification
Filemon	Malware is open to the external file, create and remove such as for modulating the behavior can be analyzed in real time.
Regmon	Malicious codes can be analyzed in real time using the register that the value of the system.
Winalysis	Previously stored information such as the file system or registry key, such as processes, allow the execution of malicious code and then you can see the changes.
procexp	List the running processes in a tree format.

Table 3. File Analysis Tools

Types	Specification
Strings	It can analyse internal strings in file with combination of specific option.
dumpbin	The Microsoft COFF Binary File Dumper (DUMPBIN.EXE) displays information about Common Object File Format (COFF) binary files. You can use DUMPBIN to examine COFF object files, standard libraries of COFF objects, executable files and dynamic-link libraries (DLLs).
Ollydbg	OllyDbg is a 32-bit assembler level analysing debugger for Microsoft Windows. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable.
IDA Pro	IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger that offers so many features it is hard to describe them all.

Table 4. Network Analysis Tool

Types	Specification
TCPView	TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint.
TDIMon	TDIMon monitors system and identifies problems caused by bad network settings. It also lets you analyze the system usage.
Fopen, openports	Fopen can write out running process port list.
Wireshark	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.
Paros	A Java based HTTP/HTTPS proxy for assessing web application vulnerability. It supports editing/viewing HTTP messages on-the-fly. Other features include spiders, client certificate, proxy-chaining, intelligent scanning for XSS and SQL injections etc.

system in the process, object of the malicious code, it is possible to determine information such as propagation path, can correspond to the malicious code and further spread to be variants there. In this study, we introduce an analysis method for malicious code analysis tools. Table 5 shows a sample Malware.

Table 5 shows that we have tested for analysis registry. After installing Malware, we checked out registry changes. Figure 1 shows that new registry list after installing Malware.

4.1 Sample Malware Analysis

We have checked out for actual Malware how to implement on PC. Winalysis v3.0 in Figure 1 is a snap shot tool for comparing before and after Malware running on PC, so it can be checked out which files are generated, modified,deleted with a time interval. Figure 1 shows Winalysis which has a snapshot icon on the menu to capture before and after changed files. Filters button in Figure 2 set and changes on Files, Groups, Registry and Services. Configure Event Filters' default setting is C:₩WINDOWS₩SYSTEM32. However, it can be clicked on Include button and add user definition directory in Figure 2. Test button in Figure 2 can be found differences after running Malware.

Table 5. **Sample Malwares**

Manufactures	Name of Malware
AhnLab-V3	- Win-Trojan/Scar.2971136
Avast	- Win32:Malware-gen
Kaspersky	- Trojan.Win32.Scar.dsjn
McAfee	- Artemis!EC71A93DFCD4
nProtect	- Backdoor/W32.Agent.2971136
ViRobot	- Trojan.Win32.Scar.2971136

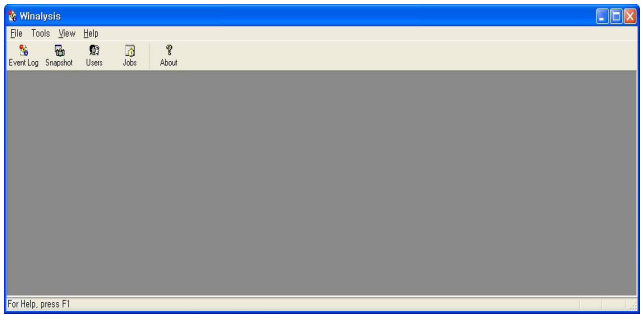

Figure 1. Winalysis screen.

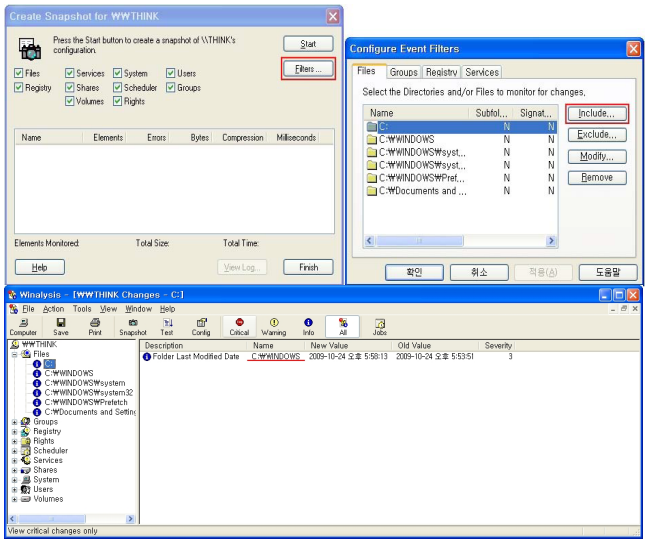

Figure 2. Filters on Winalysis.

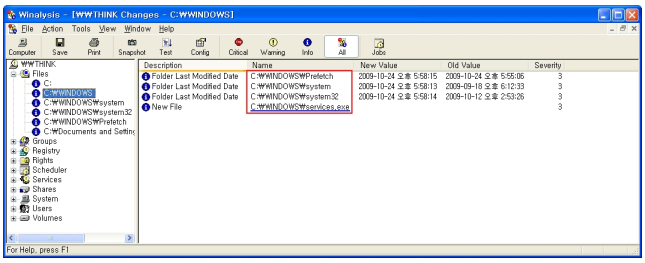

Figure 3. Showing changes after running Malware.

Table 6. Modified or Generated File Information

Directory name	Generated files
WINDOWS	services.exe
WINDOWS₩Prefetch₩	CONIME.EXE-13EEEA1A.pf CMD.EXE-087B4001.pf FSERVICE.EXE-2E4F6E14.pf NET.EXE-01A53C2F.pf NET1.EXE-029B9DB4.pf RUNDLL32.EXE-2313F110.pf SERVICES.EXE-14D2412D.pf SERVICES.EXE-2B0DDD57.pf
WINDOWS₩system₩	sservice.exe
WINDOWS₩system32₩	fservice.exe reginv.dll winkey.dll

Figure 3 shows us what changed after running Malware. As you can see, C:\Windows fold has been changed. Prefetch, system, system32 folders have been changed and services.exe file is generated in Windows folder. Therefore, Malware may generate some files in

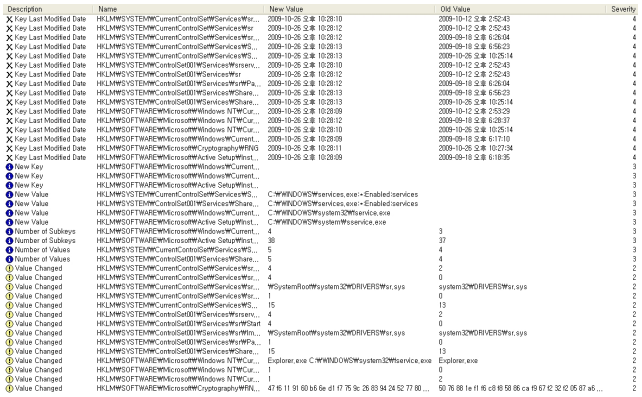

Figure 4. Modified or generated files.

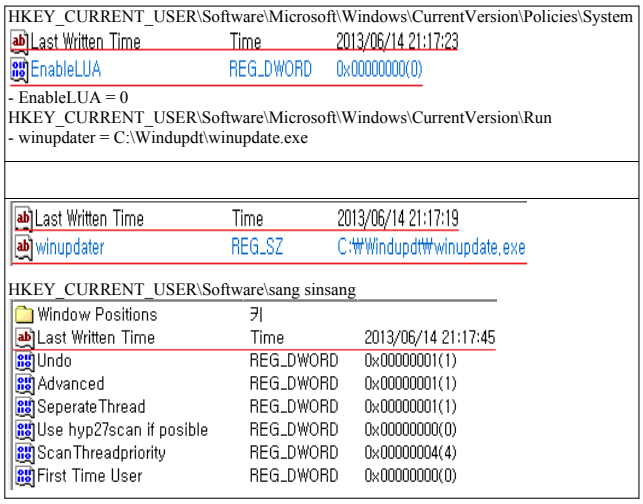

Figure 5. Added new registry.

Prefetch, system, system32 folders. Table 6 shows modified or generated files after running Malware. These files in Table 6 are generated after installing sample Malware, so if you find these files on your PC, Malware must be installed.

In addition, new registry has been generated under HKEY_CURRENT_USER\Software. These registry keys can prove that Malware has been deployed

5. Conclusion

Independent of the above tools used and the operating system under examination, there is a need for a preservation methodology to ensure that available volatile data is captured in as consistent and repeatable manner as possible. For forensics purposed, it is also necessary to maintain detailed documentation of the steps taken on

the live system and the integrity of the acquired data. The methodology in this research provides a robust foundation for the forensics preservation of volatile data on a live Windows system. This methodology is not intended as a checklist and may need to be altered for certain situation. However, it increases that chances that much of the relevant volatile data on the system will be obtained. Furthermore, this methodology and the supporting documentation will strengthen volatile data asa source of evidence, enabling an objective observe to evaluate the reliability and accuracy of the preservations process and acquired data.

According to the experimental results, Malware remains marks on registry. Therefore, registry analysis is an important tool to detect Malware and the best way to prevent Malware is monitoring registry changes at all the time. We used Winalysis for finding modified, generated or deleted files after running Malware. To detect Malware and prevent from Malware, Malware must be analyzed from the bottom of system level such as kernel or file system.

6. Acknowledgment

This research is supported by 2015 Baekseok University Research fund.

7. References

1. Skoudis E, Zeltser L. Malware: Fighting malicious code. 2004. Available from: http://books.google.com
2. Akira M, Toshimi S, Tomonori I, Tadashi I. Detecting unknown computer viruses - A new approach. Journal of the National Institute of Information and Communications Technology. 2005; 52(1/2):75–88.
3. Schneter B. Attack trees: modeling security threats. Dr Dobb's Journal.1999; 24(12):12–19.
4. Wu NQ, Qian Y, Chen G. A novel approach to Trojan Horse detection by process tracing. Proceedings of the IEEE International Conference on Networking, sensing and control (ICNSC'06); 2006. p. 721–6.
5. Geer D. Behavior-based network security goes main stream. Computer. 2006; 39(3):14–7.
6. Willems C, Holz T, Freiling R. Toward automated dynamic malware analysis using CWSandbox. IEEE Security and Privacy. 2007; 5(2): 32–9.
7. Li Z-Y, Tao R, Cai Z-H, Zhang H. A web page malicious code detect approach based on script execution. Fifth International Conference on Natural Computation (ICNC'09); 2009. 6:308–12.
8. Nachenberg C. Computer virus-antivirus coevolution. Comunications of the ACM. 1997; 40(1):46–51.
9. Skrzewski M. Flow based algorithm for malware traffic detection. Computer Networks in Communications in Computer and Information Science. Springer Berlin Heidelberg; 2011. p. 271–80
10. Ahmed I, Lhee KS. Classification of packet contents for malware detection. Journal in Computer Virology; 2011. p. 279–95.
11. Kwon J, Lee H. BinGraph: Discovering mutant malware using hierarchical semantic signatures. 7th International Conference on Malicious and Unwanted Software (MALWARE); 2012.p. 104–11.
12. Shoch J, Hupp J. The worm programs—early experience with a distributed computation. Communications of the ACM. 1982; 25(3):172–80.
13. Liu YF, Zhang LW, Liang J, Qu S, Ni ZQ. Detecting Trojan horses based on system behavior using machine learning method. International Conference on Machine Learning and Cybernetics (ICMLC). 2010; 2:855–60.
14. Xiaojun T, Zhangquan Z, Huimin S, Zhu W. The analysis of worm non-linear propagation model and the design of worm distributed detection technology. 9th International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES); 2010. p. 219–23.
15. Park Y, Zhang Q, Reeves D, Mulukutla V. AntiBot: Clustering common semantic patterns for Bot detection. Computer Software and Applications Conference (COMPSAC); 2010. p. 262–72.
16. Alminshid K, Omar MN. Detecting backdoor using stepping stone detection approach. Second International Conference onInformatics and Applications (ICIA); 2013. p. 23–5.
17. Huang H-D, Lee C-S, Hagras H, Kao H-Y. IEEE International Conference on Systems, Man and Cybernetics (SMC); 2012. p. 2821–6.
18. Tsai Y-L, Yeh L-Y, Lee B-Y, Chang J-G. IEEE 18th International Conference on Parallel and distributed systems (ICPADS); 2012. p. 724–5.
19. Huang HD, Lee CS, Wang MH, Kao HY. IEEE International Conference on Systems, Man and Cybernetics (SMC); 2013. p. 4652–7.