Customizing Cuckoo Sandbox for Malware with Tricky Execution Conditions

Yu-Seong Kim, Sang-Hoon Choi, Ki-Woong Park
System Security Lab.Daejeon University, System Security Lab. Kongju National University
Dept. Computer and Information Security Sejong University
kys10044@gmail.com, csh0052@gmail.com, woongbak@sejong.ac.kr

Abstract— As the number of malware has been increased, much time and manpower are required for analysis. Automating malware analysis is critical for organizations that process large numbers of malicious programs. Such automation allows analysts to focus on the tasks that require human insights. However, automating malware analysis has been considered as a challenging issues. As malware tends to introduce technological innovations, malware is executed only when every execution condition are satisfied. For example, a malware has an execution condition that the malware can be executed only when a specific file is located on a different path or, the actual attack occurs only after multiple malwares are executed in a step-by-step manner, or the registry file must be imported before the malware is executed. In these cases, most of the automated malware analysis system cannot complete the analysis process. In this paper, we present our effort to customize Cuckoo Sandbox for enabling analysis of malware with tricky execution conditions. Our customizations for Cuckoo Sandbox include the analysis request module, and the analysis module of Cuckoo sandbox. This allows Cuckoo Sandbox to analyze malwares with various execution conditions efficiently.

Keywords: Malware Analysis, Tricky Execution Condition, Sandbox

Ⅰ. Introduction

According to the overall malware statistics report by Kaspersky, in 2015, a total of 1,966,324 malware infections were detected [1]. This shows about 5,387 malware infections per day. Recent hacking incidents that threaten national security gives caution that it can make our society a big mess, and the scale of the damage caused by cyber-attacks exceeds the magnitude of the damage caused by natural disasters there [2]. Analyzing these malwares requires much time and manpower. Therefore, automating malware analysis is critical for organizations that process large numbers of malicious programs. Such automation allows analysts to focus on the tasks that require human insights. However, automating malware analysis has been considered as a challenging issues. As malware tends to introduce technological innovations, malware is executed only when every execution condition are satisfied [3, 4]. For example, a malware has an execution condition that the malware can be executed only when a specific file is located on a different path or, the actual attack occurs only after multiple malwares are executed in a step-by-step manner, or the registry file must be imported before the malware is executed. In these cases, most of the automated malware analysis systems cannot complete the analysis process. In this paper, we present our effort to customize Cuckoo Sandbox [5] for enabling analysis of malware with tricky execution conditions. Our customizations for Cuckoo Sandbox include the analysis request module, and the analysis module of Cuckoo sandbox. This allows Cuckoo Sandbox to analyze malwares with various execution conditions efficiently.

The organization of this paper is as follows. Section 2 describes related issues about two types of failure to analyze malware by automated malware analysis tools, Section 3 presents a customizing Cuckoo Sandbox for malware with tricky execution conditions. Section 4 describes our conclusion of this paper.

Ⅱ. RELATED ISSUE

In this section, we present two types of failure to analyze malware using automated malware analysis tools [6].

The first type of failure is due to an interactive malware that waits for specific user interaction to perform malicious behavior. For example, there has been a PDF file that does not trigger any malicious behavior until a user scrolls down to a specific page. In another case, malware in an already infected PC was executed only when there was a specific change in the input device such as by clicking or moving the mouse in a specific direction; a popup window warning was then displayed indicating that the PC was infected. Only when the user clicked the ‘OK’ button of the popup window, the malicious behavior of the malware is performed. Since these types of malware do not activate or display any suspicious or malicious behavior until there is a specific

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2016R1A4A1011761) and by the Ministry of Education (2015H1C1A1035859).

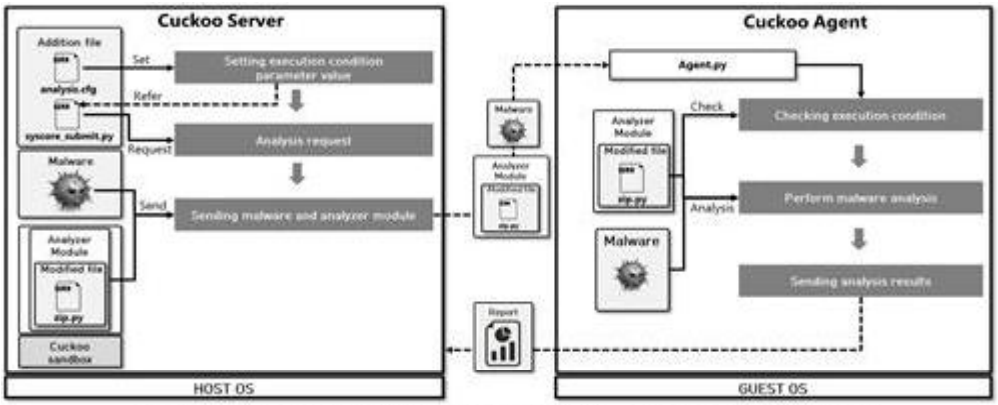

Fig. 1. ARCHITECTURE OF MODIFIED CUCKOO SANDBOX

user interaction, it is difficult to detect them using APT defense solutions with sandbox-based behavior analysis.

The second type of failure is due to a time-consuming malware that are difficult to control in an automated analysis system. Most APT defense solutions use controlled environments such as a virtual machine or sandbox to analyze behavior automatically. Due to the limitations of hardware resources in analysis systems, it is difficult to keep the virtual machine or sandbox in operation until the behavior of malware has fully taken place. Taking advantage of this limitation, attackers create malware with 'scheduling' techniques to execute behaviors at a specific time. This is called a 'time-bomb' or 'Trojan nap'. This time-bomb method requires some specific APIs such as a sleep API, and there are some APT defense solutions that classify a program as malware if it uses one of those specific APIs. However, this can cause false positives since the corresponding APIs are also used in normal programs.

Ⅲ. Customizing Cuckoo Sandbox

In this section, we present a customized Cuckoo Sandbox for enabling analysis of malware with tricky execution conditions. As shown in Fig. 2, our customizations for Cuckoo Sandbox include the analysis request module, and the analysis module of Cuckoo Sandbox. The analysis request module has the following two files. The *analysis.cfg* file in Custom Cuckoo Server, set the parameter value of the tricky execution condition for malware analysis with tricky execution condition. And the *syscore_submit.py* in Custom Cuckoo Server, instead of using the *submit.py* of the Cuckoo Sandbox for a common malware analysis request, it requests malware analysis with tricky execution condition by referring to *analysis.cfg* and *zip.py* file in the analysis module of Cuckoo sandbox. It has built-in functions for malware analysis with tricky execution conditions.

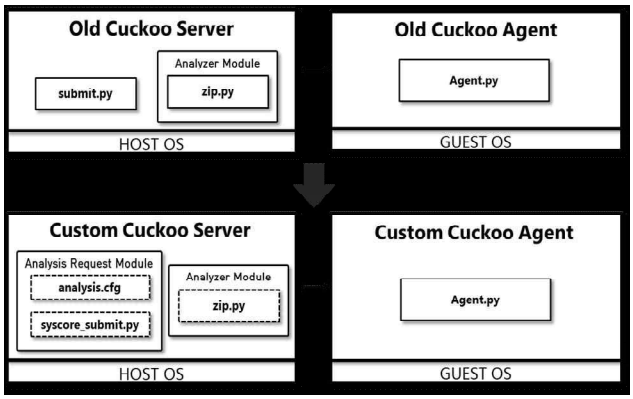

Fig. 2. CUSTOMIZED OF CUCKOO SANDBOX

As shown in Fig. 1, the Cuckoo Sandbox has a Cuckoo Server on the HOST OS for setting and requesting a dynamic malware analysis and Cuckoo Agent on the GUEST OS for a dynamic analysis upon the request. Through the *analysis.cfg* file on Cuckoo Server, Cuckoo Agent sets the parameters related on execution conditions of malware to be analyzed. The parameters include following configuration options: settings malware file naming, setting the password for compressed files, routing multiple malware, and setting step-by-step execution order for multiple files. After that, the file *syscore_submit.py* parses the *analysis.cfg* configuration value and requests analysis for the malware with the tricky execution condition. At the same time as requesting the analysis, the malware execution parameter, the malware to be analyzed, and the analyzer module are transmitted to Cuckoo Agent. Cuckoo Agent then receives malware execution parameter, malware with tricky execution condition, and the analyzer module in *Agent.py* file from the Cuckoo Server. Then, malware analysis with set execution conditions is performed by checking the execution condition parameter value in the analyzer module's *zip.py* file. Finally, the Cuckoo Agent sends the analysis results to Cuckoo Server.

Ⅳ. CONCLUSION

Automating malware analysis is critical for

organizations that process large numbers of malicious programs. Such automation allows analysts to focus on the tasks that require human insights. However, automating malware analysis has been considered as a challenging issues. In this paper, we present our effort to customize Cuckoo Sandbox for enabling analysis of malware with tricky execution conditions. As a result, this allows analysis of malware with various execution conditions, allowing analysts to efficiently analyze and respond. Further work will perform a various experiments and profiling for advanced malware dynamic analysis engines. Through this, we will do additional research for hacker identification by extracting feature information of fundamental malware as well as limited common behavior analysis.

References

[1] Shcherbakova, NDDG Maria Vergelis Tatyana. "Kaspersky security bulletin. spam and phishing in 2015." (2016).

[2] KISA Press, “Security Development Strategy”, KISA, 2015

[3] Hopkins, Etc "Exploit Kits: The production line of the Cybercrime economy?." 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). IEEE, 2015.

[4] The Ultimate Guide to Angler Exploit Kit for Non-Technical People, Heimdal Security, May. 18, 2016

[5] C Guarnieri, M Schloesser, J Bremer, A Tanasi, “Cuckoo sandbox-open source automated malware analysis,”, Black Hat USA, 2013

[6] AhnLab. Press, “Invasion of Malware Evading the Behavior-based Analysis”, AhnLab, Feb. 21, 2014