Differences between Free Open Source and Commercial Sandboxes

G.KALE[1] , E.BOSTANCI[2] and F.V.ÇELEBİ[3]

[1] Kilis 7 Aralik University, Kilis/Turkey, gkale@kilis.edu.tr
[2]Ankara University, Ankara/Turkey, ebostanci@ankara.edu.tr
[3]Ankara Yildirim Beyazit University, Ankara/Turkey, fvcelebi@ybu.edu.tr

***Abstract* – Nowadays, rightly so, the concept of cyber security is very important. The most effective weapon in this area is undoubtedly malicious software. Therefore, it is more important to analyze malware effectively and to prevent possible harms. One of the techniques to analyze the malware is sandboxing. There are too many sandbox options in the wild that can be preferred depending on situations and the service provided. In this paper, the differences between free open source and commercial sandboxes have been discussed. There have been several advantages and disadvantages between them that is mentioned in the result.**

***Keywords* – Malware, malware analysis, free open source sandbox, commercial sandbox.**

I. INTRODUCTION

MALWARE is a malicious software that is installed on victim machines or systems without owner consent and performs malicious actions such as stealing secret information and allowing remote code execution, and it can cause denial of service. Recently, the number, complexity and the severity of these malicious types of software have been increasing and presenting huge information security challenges to computer systems. To understand the malicious activity of the malware, it is needed to be analyzed [1].

Malware analysis is a critical process of identifying malware behavior and their main goals. It is important to know what the malware are doing and what they want in real. So, it is more understandable of how a malware works. But malware analysis involves a complex process in its activity like forensics, reverse engineering, disassembly, debugging and so on. These activities take a lot of time in the progress [2]. As the result of analysis; a lot of useful information like IPs of Command and Control (C&C) servers, indicators of compromise, file access, whether the malware was packed or not, if it has obfuscated code or not, whether it spreads on the network or not [3]. If these are considered, malware analysis is an important task that is still improving by the researchers to take more accurate and detailed results.

Malicious code analysis aims to achieve a deeper understanding of a malware functioning. As shown in the figure 1; malware analysis methods are divided into two groups as static (code) and dynamic(behavioral). The dynamic malware analysis is divided again into two groups as manual and automatic [4].

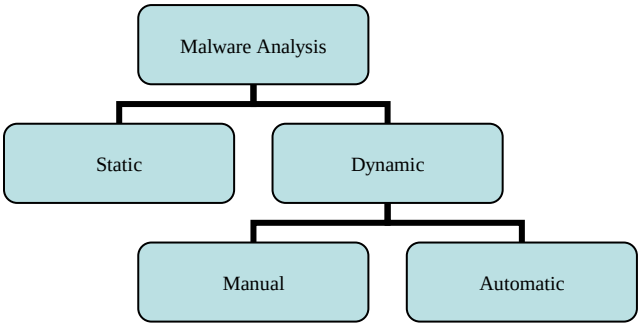

Figure 1: Malicious Code Analysis

The main idea of static analysis is analyzing the malware without executing it. It means that, the instructions and codes are interpreted to know what the malware does and what its real aim is. Although static analysis has the benefit of enabling the detailed clarification of every one of the sample's functions, it is extremely costly because it requires someone with a deep understanding of programs, operating systems, hardware, and other mechanisms to decipher each individual line of code. Sometimes the source code isn't available to observe, and it is impossible to analyze the malware if it is obfuscated or packed. So, third party software, reverse engineering and other techniques is needed and employed to analyze the malicious code [5].

Dynamic analysis, on the other hand, can be used to analyzed samples that employ obfuscation (code encryption, etc.), packing and observes the malware activity without the need to work directly on the samples, and so analysis can be performed relatively quickly in comparison with static analysis. The malware is executed in a safe and controlled environment. Otherwise, the malware can affect and disease the systems where the malware is executed and diffused over network [5]. Malware infection on your system can cause damage to your system such as file deletion, change in registry, file modification, stealing confidential data/information, and so on. With dynamic analysis, you can monitor the changes made to the file system, registry, processes, and its network communication.

Due to limitations of static analysis, researchers and

students focus on dynamic malware analysis. Generally, a virtual machine or sandbox is used for dynamic malware analysis. As malware became more sophisticated, the sandboxing is used to analyzed malware easily, safely and securely without compromising our system. Due to the complexity and the proliferation of the malware around the internet, it is also very difficult and time consuming to manually inspect the malware [6]. Traditional security solutions like firewall, intrusion detection systems, intrusion prevention systems, web gateways and anti-virus software are defenseless and powerless towards zero-day malware exploits thus nullifying the efforts and infrastructure deployed by organizations and security agencies. Therefore, security professionals are also deploying sandboxing techniques to detect the dynamic and polymorphic nature of malware [7].

There are two types of sandboxes which is free open source and commercial. The differences between them is searched only in this paper. In literature review, mostly some kind of sandboxes are used in relevant searches to take the results from malware analysis, rarely some of them have compared each other and explained how to improve the sandbox techniques. For example; in paper [8], the comparison has been made between two most commonly used malware behavior analysis sandboxes which are Anubis and Cuckoo. In paper [6], it has been mentioned briefly to some sandbox products like Anubis, Norman Sandbox Analyzer Pro, Joe Sandbox Document Analyzer and Cuckoo Sandbox as malware analysis tools. In paper [7], the effectiveness of sandboxing and evasion techniques has been evaluated.

II. SANDBOX

As defined by Wikipedia, "In computer security, a sandbox is a security mechanism for separating running programmes. It is often used to execute untested code, or untrusted programmes from unverified third-parties, suppliers, untrusted users and untrusted websites [9].

Typically, sandbox technologies use VM environments like VMware, Xen, Parallels/Odin and VDI (Virtual Desktop Infrastructure), which allow a user or an administrator to run one or more "guest" operating systems on top of another "host" operating system. Each guest operating system executes within an emulated environment and allows managed access to both virtual and actual hardware. In theory, the environment provided by the VM is self-contained, isolated, and indistinguishable from a "real" machine. VM technology has long been considered an effective approach for analyzing malware because it provides an isolated environment or sandbox where the malware can be triggered and monitored [10].

Sandboxes provide a virtual environment for the execution of programs and restrict their full access to the host machine. They work in a virtual environment imitating like a full a physical machine with dedicated hardware and system resources assigned to it. It resembles a live system without any access to the outer world. Suspicious files are made to execute on this safe environment to analyze the malware behavior. Sandboxing has been widely adopted in various applications and software for providing security and protection from malicious content [7].

However, advanced malware can discover a VM environment and tailor its actions to avoid detection. Conventional sandbox analysis works by inserting artifacts into the guest operating system, which allow advanced malware to determine if a system is running in a virtual environment or sandbox. These artifacts include additional operating system files and processes, supplementary CPU features, and other components necessary for the virtualization to work. The malware then employs several evasion techniques that are completely invisible to the sandbox, allowing it to penetrate a file or network without detection by even the most sophisticated cyber threat protection systems [lastline].

Main methodologies to analyze malware for observing functional characteristics in a controlled environment like sandbox is based on:

a) comparison of the operating system status before and immediately after the malware execution, and
b) runtime actions monitoring

Sandbox features include monitoring of:

- created or modified files;
- access or system registry key modifications;
- dynamic loaded libraries;
- virtual memory accessed areas;
- created process;
- instanced network connections; and
- data transmitted over the network [4].

There are too many sandbox products in the wild. It can differ from each other to their deterministic properties. These are:

- Supported file types that will be analyzed
- Supported platforms that the analysis run on
- Information from the file, applications and URL's that is taken from the result of analysis
- Techniques that is used to avoid detection by malware
- Whether the emulation or visualization is used or not
- The accuracy of analysis
- Indicator of Compromise (information extracted from analysis)
- Supported import and export file formats
- Reports from analysis and the formats of reports
- Number of malware samples to be analyzed (Scalability)
- Size of the malware samples to be analyzed
- The performance of the sandbox
- Zero-day detection capability
- Good building sandbox
- Whether it is under active development or not

There are too many sandboxes that can be free and commercial. Also, some of them are not under service. Table 1

shows the sandboxes below.

Table 1: Free and Commercial Sandboxes

Sandbox Name	Free	Commercial
GFISandbox	-	x
Norman Sandbox	-	x
Cuckoo Sandbox	x	x
Virustotal	x	x
Malwr	x	-
ThreatAnalyzer	-	x
Wildfire	-	x
Forti Sandbox	-	x
FireEye	-	x
Lastline	-	x
Valkryie	-	x
VmRay	-	x
Joe Sandbox	-	x
Any.Run	-	x
VxStream Sandbox	x	x
Detux Sandbox	x	-
Noriben	x	-
Procdot	x	-
Firejail	x	-

A. Advantages of Free Open Source Sandbox

Researchers mostly prefer free open source sandboxes in their researches. There area some advantages for using free open source sandboxes that are listed below:

1) Analyze many different malicious files as well as malicious web sites in different environments [11].
2) Dump and analyze network traffic even when encrypted.
3) Optional plugins can be used.
4) Build them according to your target.
5) It is costless.

B. Disadvantages of Free Open Source Sandbox

Although some free open source sandbox is under active deployment, they have some disadvantages as well.

1) It can be detected by sophisticated malwares and malwares can hide their malicious activity.
2) If the malware sample is shared with online free solutions and detected by them, you are basically informing the attacker that the malware has been detected.
3) Some malwares are written to execute on the specific execution of some event like pressing of specific keys or typing of some string on keyboard or scrolling of mouse [7].
4) Deploying a sandbox is a very delicate process with many steps and pitfalls [12].
5) It can not give a detailed result for your target.

C. Advantages of Commercial Sandbox

Some commercial malware sandboxes offer on-site alternatives to cloud solutions or a combination of on-site installation with private cloud support.

1) It gives you a complete view of every aspect and element of a threat, from infection vector to payload execution.
2) Some of them are not use or require emulation or virtualization.
3) It logs and analyzes all the resulting activity without any manual intervention.
4) It can also monitor the behaviors between system calls or API functions, not only the calls itself.
5) Some of them are invisible to malware.
6) It has more user-friendly interface.
7) A professional service supports.
8) It has more extra plugin support.

D. Disadvantages of Commercial Sandbox

Some commercial sandboxes are paid does not mean that they haven't any disadvantages.

1) The challenge is not to build a sandbox, but rather to build a good one.
2) The implementation of a commercially supported sandbox comes with a hefty price tag and often an annual support contract in the six or seven figure range [12].
3) Some of them can be detected by advanced and sophisticated malwares.
4) Some of them can not detect the zero-day or unknown malwares.

III. CONCLUSION

In conclusion, free open source and commercial sandboxes can be used for malware analysis systems and researches. Both have advantages and disadvantages. Some researchers and students prefer free open source sandboxes that is still under active deployment. Because it is free in price and open source and you can customize the sandbox settings according to your target. The countermeasures must be taken by you in free open sources sandbox. So, it is more difficult to build. But for accurate results in malware analysis without detecting from advanced and sophisticated malwares, with a good service support, it is better to use the commercial ones within the possibilities. In future works, good designed and effective sandboxes can be improved as well.

REFERENCES

[1] Ö. Aslan, R. Samet, "*Investigation of Possibilities to Detect Malware Using Existing Tools*" *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications*, pp. 1277–1284, Oct 30-No 03 2017.

[2] D. Oktavianto, I. Muhardianto, Cuckoo Malware Analysis.Packt Publisihing, 2013.

[3] M. Vasilescu, L. Gheorghe and N. Tapus, "Practical Malware analysis based on Sandboxing," *2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference*, 11-13 September 2014.

[4] C. A. Andrade, C. G. Mello and J. C. Duarte, "Malware automatic Analysis," 2013 BRICS Congress on Computational Intelligence & 11th Brazilian Congress on computational Intelligence, Ipojuca, pp. 681-686, September 2013.

[5] H. Nakakoji, T. Kito, T. Shigemoto, N. Hayashi and S. Yamashita, "Automatic Malware Analysis Technology to Defend against Evolving Targeted Attacks," Hitachi Review, vol. 63, pp. 80–86, 2014.
[6] N. Kaur, A.K. Bindal, "A Complete Dynamic Malware Analysis" International Journal of Computer Applications, vol. 135, pp. 20–25, February 2016.
[7] M. Mehra, D. Pandey, "Event Triggered Malware: A New Challenge to Sandboxing" *IEEE INDICON 2015*, pp. 1–6, December 2015.
[8] J. T. Juwono, C. Lim and A. Erwin, "A Comparative Study of Behavior Analysis Sandboxes in Malware Detection," International conference on New Media (CONMEDIA), 2015.
[9] https://en.wikipedia.org/wiki/Sandbox_(computer_security)
[10] https://go.lastline.com/rs/373-AVL-445/images/Lastline_Advanced_Malware_%20Detection_WP.pdf
[11] S. R. Ayala, "An Automated Behavior-Based Malware Analysis Method Based on Free Open Source Software" Universitat Oberta de Catalunya, *January 2017*.
[12] J. Ortiz, "Deployment of a Flexible Malware Sandbox Environment Using Open Source Software" 2015 The SANS Institute, July 2015.