

# Assessment 1: Review of Reverse Engineering Tools

CSI2107 Software Reverse Engineering

**Name: Marco Cavani**

**Student ID: 10570027**

## Contents

The important of sandbox in malware analysis .....	3
How sandbox works .....	3
Sandbox unique functionalities .....	3
Sandbox strengths and Weaknesses.....	3
Sandboxes comparison .....	3
<b>VirusTotal</b> .....	3
<b>Hybrid Analysis</b> .....	3
<b>Cuckoo Sandbox</b> .....	4
Sandboxes Review .....	4
<b>VirusTotal</b> .....	4
<b>Hybrid Analysis</b> .....	4
<b>Cuckoo Sandbox</b> .....	4
Sandbox Features.....	5
Reference list .....	6

## **The important of sandbox in malware analysis**

Sandboxes are important tools in the dynamic malware analysis field; they are used to detect and analyse malware without compromising the end-point system. In fact, a sandbox provides a secure virtual environment that prevents malware infecting actual operating systems while testing for malicious activities. Sandboxes can be used as an additional layer of the end-user machine to isolate potential malicious executable files from the actual operating systems. It can be used to test suspicious software or analyse malware. This tool works well in malware analysis as it can provide a better understanding of malware behaviour (Maass et al., 2016).

## **How sandbox works**

Sandboxes are designed to protect computer systems by providing a separated network environment where is safe to detect, test and evaluate potential treats represented by malicious code or software. Sandboxes help malware analysts to understand the nature of infections by allowing malware to spread its payload without compromising the actual system(Cirelly, 2022).

## **Sandbox unique functionalities**

Sandboxes have unique functionalities that can be used for isolating malware or testing new software for potential bugs. In many cases sandboxes have advanced features that allow analysts to monitor for suspicious behaviours related to potentially malicious components. Suspicious malware's behaviour could include downloading additional files or sending suspicious server requests. Sandboxes also prevent unauthorised access to the main host during testing(Maass et al., 2016).

## **Sandbox strengths and Weaknesses**

The advantages of sandboxes rely on the fact that a malware can be tested in a secure environment. however, duo to the malware's engineering fast evolution over the years, certain malware could potentially escape from such environment (Oliveria, 2022).

## **Sandboxes comparison**

The following section compares three different sandboxes: Cuckoo Sandbox, VirusTotal and Hybrid Analysis.

### **VirusTotal**

Virus total provides a vast variety of antivirus and URL block listing services. The platform has an intuitive user interface that allows malware analysis. The user can upload sample or check for malicious files directly from the browser. Additionally, The VirusTotal malware samples database allows to compare potential malicious component with pre-existing malware. (VirusTotal, 2019)

### **Hybrid Analysis**

Hybrid Analysis is a free malware analysis tool that can be used for both dynamic and static analysis. The web page offers similar functionalities to VirusTotal such as the URL and the file upload method along with the opportunity to search using binary code or hash strings. ([www.hybrid-analysis.com](http://www.hybrid-analysis.com), n.d.).

### Cuckoo Sandbox

Cuckoo Sandbox is an open-source automated analysis software capable of targeting any malicious file within various operating system such as Windows, Linux, MacOS and Android. The functionalities provided by Cuckoo Sandbox facilitate the analysis of executable file, PowerPoint sheets, PDF documents, e-mail as well as webpages on a virtual environment ([cuckoosandbox.org](http://cuckoosandbox.org), n.d.).

## Sandboxes Review

The following tools have been used to test a malware sample for malware analysis purpose. The suspicious file: *yitaly.exe* is a malware sample downloaded from the internet. The test will be conducted from Kali Linux VM using VirusTotal, Hybrid Analysis and Cuckoo sandbox on the Firefox browser([www.cisa.gov](http://www.cisa.gov), n.d.).




**VirusTotal** results shown 60 antivirus vendors out of 70 marked the executable file as malicious. Also, it provides information about the nature of the malware, the vendor analysis, the malware behaviour, the suspicious connections made by the executable file and many other useful information about the malware. (VirusTotal, 2019).

**Hybrid Analysis** overview shown the threat score, which was 100 out of 100 along with, the malware classification, the AV detection score, the antiviruses measurements, and The MITRE ATTACK section which outlined 14 malicious behaviours.

**Cuckoo Sandbox** is by far the slowest one to come out with a report, however the result where modular and detailed. The file was declared suspicious. Like the previous ones, Cuckoo Sandboxes provides the users with many useful information that can be used for malware analysis ([cuckoosandbox.org](http://cuckoosandbox.org), n.d.).

In Conclusion, all three platform seem to be valid tools for testing and analysing malwares as they provide the user with much information. More detail about different platform functionalities can be seen from the table below.

Table 1

Sandbox Features			
Platform Support	SaaS	SaaS Android	Windows Mac Linux Android
Integration	<ul style="list-style-type: none"> <li>❖ Browser Extension</li> <li>❖ VirusTotal and OPSWAT Metadefender (online and on-site)</li> <li>❖ SIEM systems (e.g., HP ArcSight)</li> <li>❖ NSRL (Whitelist)</li> <li>❖ Thug honeyclient (e.g., URL exploit analysis)</li> <li>❖ Suricata (ETOpen/ETPro rules)</li> <li>❖ TOR (avoid e.g., external IP fingerprinting)</li> <li>❖ Phantom</li> </ul>	<ul style="list-style-type: none"> <li>❖ Browser Extension</li> <li>❖ API</li> <li>❖ Yara</li> </ul>	<ul style="list-style-type: none"> <li>❖ Browser Extension</li> <li>❖ API</li> </ul>
Max File Size	100MB	File up to 650 MB Email 350 MB	10 GB
API Support	✓	✓	✓
Browser Extension	✓	✓	✓
Dynamic Behavioural Analysis	✓	✓	✓
Static Analysis	✓	✓	✓
Training	Documentation/Community Support	Documentation/Community Support	Documentation/Community Support
Pricing	Free Version available.	Free Version available.	Free Version available
Support	Online Support	24/7 Support Online Support	Online Support
Company information	<b>Hybrid Analysis</b> Germany <a href="http://www.hybrid-analysis.com">www.hybrid-analysis.com</a>	<b>VirusTotal</b> United States <a href="http://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works">support.virustotal.com/hc/en-us/articles/115002126889-How-it-works</a>	<b>Cuckoo</b> Founded: 2014 <a href="http://cuckoosandbox.org">cuckoosandbox.org</a>

## Reference list

- Cirelly, J. (2022). *10 Best Malware Analysis Tools - Updated 2022! (Paid & Free)*. [online] Comparitech. Available at: <https://www.comparitech.com/net-admin/best-malware-analysis-tools/#:~:text=Cuckoo%20Sandbox%20is%20one%20of>.
- cuckoosandbox.org. (n.d.). *Cuckoo Sandbox - Automated Malware Analysis*. [online] Available at: <https://cuckoosandbox.org/>.
- Maass, M., Aldrich, J., Bauer, L. and Amizic, B. (2016). *A Theory and Tools for Applying Sandboxes Effectively*. [online] Available at: <https://www.cs.cmu.edu/~mmaass/pdfs/dissertation.pdf>.
- Oliveria, P. (2022). *Uncovering a macOS App Sandbox escape vulnerability: A deep dive into CVE-2022-26706*. [online] Microsoft Security Blog. Available at: <https://www.microsoft.com/security/blog/2022/07/13/uncovering-a-macos-app-sandbox-escape-vulnerability-a-deep-dive-into-cve-2022-26706/>.
- sourceforge.net. (n.d.). *Cuckoo Sandbox vs. Hybrid Analysis vs. VirusTotal Comparison*. [online] Available at: [https://sourceforge.net/software/compare/Cuckoo-Sandbox-vs-Hybrid-Analysis-vs-VirusTotal/#claim\\_hybrid-analysis.s](https://sourceforge.net/software/compare/Cuckoo-Sandbox-vs-Hybrid-Analysis-vs-VirusTotal/#claim_hybrid-analysis.s).
- VirusTotal (2019). *How it works*. [online] VirusTotal. Available at: <https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works>.
- www.cisa.gov. (n.d.). *MAR-10337802-1.v1: DarkSide Ransomware | CISA*. [online] Available at: <https://www.cisa.gov/uscrt/ncas/analysis-reports/ar21-189a>.
- www.hybrid-analysis.com. (n.d.). *Free Automated Malware Analysis Service - powered by Falcon Sandbox - Frequently Asked Questions*. [online] Available at: <https://www.hybrid-analysis.com/faq>.