**Assessment 1: Review of Reverse Engineering Tools**CSI2107 Software Reverse Engineering   
 **Name: Marco Cavani   
Student ID: 105700227**

**Contents**

[The important of sandbox in malware analysis 3](#_Toc110727737)

[How sandbox works 3](#_Toc110727738)

[Sandbox unique functionalities 3](#_Toc110727739)

[Sandbox strengths and Weaknesses 3](#_Toc110727740)

[Sandboxes comparison 3](#_Toc110727741)

[**VirusTotal** 3](#_Toc110727742)

[**Hybrid Analysis** 3](#_Toc110727743)

[**Cuckoo Sandbox** 3](#_Toc110727744)

[Sandboxes analysis 4](#_Toc110727745)

[**VirusTotal** 4](#_Toc110727746)

[**Hybrid Analysis** 4](#_Toc110727747)

[**Cuckoo Sandbox** 4](#_Toc110727748)

[Sandbox Features 5](#_Toc110727749)

[Reference list 6](#_Toc110727750)

# 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 advantage of sandboxes relies on the fact that a malware can be tested in a secure environment however, the malware’s engineering evolving fast over the years, and there are reasons to consider that certain malware could potentially escape from such environment (Oliveria, 2022).

# Sandboxes comparison

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

**VirusTotal** has an intuitive user interface and allows malware analysis. similarly, to other sandboxes is possible to upload sample and checking for potential malicious URLs. The malware samples database allows to compare potential malicious component for a quick analysis. However, this tool provides a vast variety of antivirus and URL block listing services. The user can submit file or scan URLs directly from the web interface(VirusTotal, 2019)

**Hybrid Analysis** web page offers similar functionalities to VirusTotal such as the URL, the file upload method, and the functionality to search for binary code or hash string. However, there are some additional scanning methods like the integration with Yara, an open-source tool used to determinate whether or not a file or a URL is malicious by matching text or binary patterns with existing malware(www.hybrid-analysis.com, n.d.).

**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 make easy to analyse executable file, PowerPoint sheets, PDF documents, e-mail as well as webpages on virtual environments that runs supported operating systems(cuckoosandbox.org, n.d.).

# Sandboxes analysis

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, n.d.).

**VirusTotal** summary outlined those 60 antivirus vendors out of 70 marked the file as malicious. The detection section shows the vendors analysis, while more details about the nature of the file can be found under the detail section. the connection unit shown that no connection where detected. However, more data can be analysed from the behaviour section. Furthermore, it is possible to see comments or interact with the VirusTotat’s community through the community section(VirusTotal, 2019).

**Hybrid Analysis** overview shown the threat score, which was 100 out of 100 along with, the malware classification that labelled the malicious file as Trajan and the AV detection score which was the equivalent of 87 out of 100. The antiviruses measurements provided also where clear about the malicious nature of the executable file. Moreover, we can see that some file was scanned and labelled as trojan in the earlier in 2016. The MITRE ATTACK section shows the 14 focal malicious techniques detected.

**Cuckoo Sandbox** is by far the slowest one to come out with a report, however the result of the scanning is comprehensive and detailed. As it can be seen from the report this platform like the previous ones classified the file like very suspicious with a score of 10 out of 10. Cuckoo Sandboxes like the other platforms analysed in this document, provides the users with many useful information that can be used for malware analysis.

In my opinion all three tools are valid tools for testing and analysing malware as they are intuitive and secure. Moreover, they can provide with an array of different features for testing and analysing malware. For more clarification on different platform functionalities see the table below.

Table 1

|  |  |  |  |
| --- | --- | --- | --- |
| Sandbox Features |  |  | A picture containing text, clipart  Description automatically generated |
| Platform Support | SaaS | SaaS  Android | Windows  Mac  Linux  Android |
| Integration | * Browser Extension | * VirusTotal and OPSWAT Metadefender (online and on-site) * SIEM systems (e.g., HP ArcSight) * NSRL (Whitelist) * Thug honeyclient (e.g., URL exploit analysis) * Suricata (ETOpen/ETPro rules) * TOR (avoid e.g., external IP fingerprinting) * Phantom | * Browser Extension |
| 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 | **Hybrid Analysis**  Germany  www.hybrid-analysis.com | **VirusTotal**  United States  support.virustotal.com/hc/en-us/articles/115002126889-How-it-works | **Cuckoo**  Founded: 2014  cuckoosandbox.org |

# 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>.
* 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/uscert/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>.

‌