Assessment 1: Review of Reverse Engineering Tools   
   
CSI2107 Software Reverse Engineering   
   
   
   
   
   
   
   
Name   
Student ID

Table of Contents   
Introduction ........................................................................................................... 2   
The functionality of sandboxes and their unique features ..................................... 2   
Sandbox strengths and weaknesses ...................................................................... 2   
Strengths ............................................................................................................ 2   
Weaknesses ........................................................................................................ 2   
Evaluation of sandboxes - Cuckoo, Any.run and VirusTotal ................................... 3   
References ............................................................................................................. 5

Importance of Sandboxes for Malware Analysis   
   
Malware analysts rely on sophisticated tools to detect, examine, and share   
information about new malware variants. One such noteworthy tool is the   
utilisation of a sandbox. A sandbox is a virtual environment employed to observe   
and control malicious applications in a safe ecosystem. The malware is then   
allowed to play out its malicious behaviours to its fullest potential while the   
sandbox entraps it in this virtual framework. This, therefore, protects the host   
system, and the malware sample can be studied and documented without any   
threat to other endpoint systems (Khalimov et al., 2019).   
   
How Sandbox Works   
   
A sandbox works by separating the actual bare metal machine from a VM   
(Virtualised Machine). It further creates a separate or predominantly isolated   
network structure in contrast to the native network and processing environment.   
It does this for a variety of reasons, including first analysing the malware to   
protect the hosting system from the adverse effects of the malware. Secondly, it   
makes it easier to study and examine the running process of the malicious   
activities by letting malware run unimpeded in the fake environment (Jamalpur,   
Navya, Raja, Tagore, & Rao, 2018).   
   
Sandbox unique functionalities, strengths, and weaknesses   
   
Sandboxes have unique features that set them apart from other malware tools and   
make them highly desirable for analysts. Because malware runs entirely in a   
sandbox, its malicious characteristics can easily be identified by monitoring clever   
obfuscation tactics, network connection requests to IP’s or domains, file   
downloads or uploads, any restricted user information requests, and other   
behaviour deemed hostile to the operating system (Liu & Wang, 2019). Sandboxes   
can further be optimised by custom modules such as, e.g., the implementation of   
Yara rules which can scan the malware for trigger code snippets.   
   
Strengths   
- Sandboxes can be run in VMs or containerised environments and quickly   
spun up, restored, or destroy.   
Weaknesses

- Sandboxes do not consistently deliver the necessary covert characteristics   
resembling a bare-metal machine, therefore failing to deceive the malware.   
Evaluation of sandboxes - Cuckoo, Any.run and VirusTotal   
   
For consistency, all three sandboxes have been tested with a sample (CISA, 2021).   
Further comparisons are listed in Table 1.   
   
Cuckoo is an advanced, extremely modular, and 100% open-source malware   
analysis system. It flagged the hash as very suspicious, with a score of 10 out of   
10 using only static analysis. Assumptions may be made that the malware   
recognised the sandbox environment and terminated any dynamic analysis.   
Cuckoo lists sections .data and .ndata with high entropy, close to 8, indicating   
obfuscation utilising compression or encryption, and identified   
DisableThreadLibraryCalls as the main ingress library (Morgenstern, 2016).   
Additionally, it lists the MISP (Malware Information Sharing Platform) level as one,   
with a description related to the Colonial Pipeline attack. Conclusively, it also   
groups 55 antivirus applications with positive signatures for this hash (Sethi,   
Chaudhary, Tripathy, & Bera, 2018).   
   
Any.run conversely, produced a highly detailed static and dynamic analysis up to   
and including a screenshot of the ransomware note. Similar to Cuckoo, it identified   
file type as PE32. The behaviour activities are divided into Malicious, Suspicious   
and Info, and lists all .exe files, their PID codes, processes, and registry changes.   
A unique feature of Any.run is the Mitre ATT&CK mapping, which gives a detailed   
and categorised breakdown of adversaries' active defence techniques (Any.run,   
2021).   
   
VirusTotal had 58 out of their 69 security vendors flagged this hash as malicious.   
Noteworthy findings compared to other sandboxes include Network   
Communication info such as Crowdsourced IDS Rules listings and Dataset Actions.   
The latter identified system property lookups related to Windows ShadowCopy   
functionality. The unique features of VirusTotal include browser plugins available   
for most browsers and the highest utilisation, 71, of other antivirus vendors   
(VirusTotal, 2021).

Table 1. – Sandbox comparison

References   
   
Alvarez, V. M. (2021). YARA in a nutshell. Retrieved from   
https://virustotal.github.io/yara/   
   
Anlyz. (2021). Malware Sandboxing 101: The Ultimate Guide. Retrieved from   
https://anlyz.co/blog/malware-sandboxing-101-ultimate-guide/   
   
Any.run. (2021). Any.run Interactive Malware Analysis. Retrieved from   
https://app.any.run/   
   
CISA. (2021). Malware Analysis Report (AR21-189A). Retrieved from https://us-  
cert.cisa.gov/ncas/analysis-reports/ar21-189a   
   
Feng, P., Sun, J., Liu, S., & Sun, K. (2020). UBER: Combating Sandbox Evasion via   
User Behavior Emulators, Cham.   
   
Greamo, C., & Ghosh, A. (2011). Sandboxing and virtualisation: Modern tools for   
combating malware. IEEE Security & Privacy, 9(2), 79-82.   
   
Jamalpur, S., Navya, Y. S., Raja, P., Tagore, G., & Rao, G. R. K. (2018, 20-21 April   
2018). Dynamic Malware Analysis Using Cuckoo Sandbox. Paper presented   
at the 2018 Second International Conference on Inventive Communication   
and Computational Technologies (ICICCT).   
   
Khalimov, A., Benahmed, S., Hussain, R., Kazmi, S. M. A., Oracevic, A., Hussain, F.,   
. . . Kerrache, C. A. (2019). Container-based Sandboxes for Malware   
Analysis: A Compromise Worth Considering. Paper presented at the   
Proceedings of the 12th IEEE/ACM International Conference on Utility and   
Cloud Computing, Auckland, New Zealand. https://doi-  
org.ezproxy.ecu.edu.au/10.1145/3344341.3368810   
   
Liu, Y., & Wang, Y. (2019, 15-17 March 2019). A Robust Malware Detection System   
Using Deep Learning on API Calls. Paper presented at the 2019 IEEE 3rd   
Information Technology, Networking, Electronic and Automation Control   
Conference (ITNEC).   
   
Morgenstern, T. (2016). Malware Terms for Non-Techies – Code Entropy. Retrieved   
from https://www.cyberbit.com/blog/endpoint-security/malware-terms-  
code-entropy/   
   
Sethi, K., Chaudhary, S. K., Tripathy, B. K., & Bera, P. (2018). A Novel Malware   
Analysis Framework for Malware Detection and Classification using Machine   
Learning Approach. Paper presented at the Proceedings of the 19th   
International Conference on Distributed Computing and Networking,   
Varanasi, India. https://doi-  
org.ezproxy.ecu.edu.au/10.1145/3154273.3154326   
   
VirusTotal. (2021). VirusTotal - How it works. Retrieved from   
https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-