Behavioral Analysis of Malware Using Dynamic Sandboxing

**Abstract**

This project investigates behavioral analysis of malware using three different dynamic sandboxing environments. These three environments are Any.Run, Hybrid Analysis, and VirusTotal. By automation, feature extraction, and data parsing, we aim to streamline workflow for detection of behaviors. These will include API calls, registry edits, and network behavior. Our results and findings show the effectiveness that automation has in detecting malware behavior as well as show the advantages of a multi-tool approach for behavior analysis.

**Introduction and Motivation**

Malware analysis is important when it comes to understanding threats and developing effective detection. Traditional malware analysis can be very time consuming and daunting. Real-time detection needs automation to help keep up with the threats that are constantly evolving. In this project, we will be using cloud-based sandbox environments to look at and analyze malware behavior. The automation we use is meant to streamline detection of potential malicious behavior and improve the extraction of important behaviors related to those malwares.

**Related Work/Background**

Sandboxing and dynamic malware analysis are effective ways to look at the behaviors of malware. Sandboxing environments allow us to observe behavior in isolation. Any.Run gives us an interactive and real-time monitoring capability. Hybrid Analysis shows detailed static and dynamic analysis. VirusTotal offers limited behavioral analysis using an extensive threat intelligence database. Automation allows us to significantly reduce the time spent on manual analysis which improves the overall efficiency of the analysis.

**Proposed Method/Framework**

* **Sandboxes**
  + **Any.Run:** Any.Run is configured for interactive and real-time monitoring of malware behavior within a secure Windows environment
  + **Hybrid Analysis:** Hybrid Analysis is a cloud-based sandbox environment with both static and dynamic analysis statistics. This is particularly useful for API calls and network behavior
  + **VirusTotal:** VirusTotal is primarily for multi-engine scanning and limited behavior data.
* **Automation**
  + **File Submission Automation:** Pythons scripts automate submission of malware samples to Any.Run, Hybrid Analysis, and VirusTotal.
  + **Feature Extraction and Parsing:** Scripts get and parse JSON reports from the platforms. They extract API calls, file modifications, and network activity.
  + **Behavioral Indicators:** Key indicators are selected for analysis. These will include API call frequency, registry edits, and network behavior
* **Programming Tools**
  + **Python:** Python is used for scripting
  + **JSON:** JSON is used for report parsing.

**Experimental Results / Analysis**

We were able to use three different malware samples of three different types of malwares. These different types were ransomware, trojans, and standard viruses.

* **Sample Results**
  + **Ransomware:**
    - Significant file system changes
    - Encryption library API calls
    - External network requests
  + **Trojans:**
    - Affected registry settings
    - Affected network connections
    - Indicating communication with command-and-control servers
  + **Virus:**
    - Replication activity by infecting other executable files
    - Altered system files or introduced malicious code
    - Modifications to registry keys for persistence and autorun

**Automation Results**

* + Automation reduced the time needed for the things that would be repetitive and more time-consuming. Those things would include manual submissions and data parsing. We identified key indicators for the malware which included IPA call spikes and suspicious IP addresses. This allowed for quick recognition of potentially harmful and malicious behavior throughout the samples.

**Conclusion**

This project shows the effectiveness of automation and dynamic sandboxing. The sandboxes were able to allow us to see key behaviors of the malware and automation was able to help us improve the overall efficiency of our analysis. Any.Run, Hybrid Analysis, and VirusTotal provided use with key features that allowed us to go deeper into observing and analyzing malware behavior.

**References**

* ANY.RUN. (n.d.). *Interactive online malware sandbox*. Retrieved from <https://any.run>
* Hybrid Analysis. (n.d.). *Free automated malware analysis service*. Retrieved from <https://www.hybrid-analysis.com>
* Wikipedia contributors. (n.d.). *VirusTotal*. In Wikipedia. Retrieved from <https://en.wikipedia.org/wiki/VirusTotal>
* Zeltser, L. (n.d.). *Free automated malware analysis sandboxes and services*. Retrieved from <https://zeltser.com/automated-malware-analysis/>
* Comparitech. (2024). *10 best malware analysis tools – Updated 2024!* Retrieved from <https://www.comparitech.com/net-admin/best-malware-analysis-tools/>
* Bitdefender. (n.d.). *The differences between static and dynamic malware analysis*. Retrieved from <https://www.bitdefender.com/en-us/blog/businessinsights/the-differences-between-static-malware-analysis-and-dynamic-malware-analysis>
* Singh, R., & Leong, K. (2020). AI-assisted malware analysis: A course for next generation cybersecurity workforce. *arXiv*. Retrieved from <https://arxiv.org/abs/2009.11101>
* Dutta, P., & Basak, S. (2019). Agent-based vs agent-less sandbox for dynamic behavioral analysis. *arXiv*. Retrieved from <https://arxiv.org/abs/1904.02100>