Viswanath Srinivasan Chirravuri

D.Eng. | DC7 | G34657239 | October 12th, 2024

CSCI 6015: Homework-7

Exploring Malware Analysis Techniques: Static vs. Dynamic Analysis and Analyzing Cuckoo Sandbox

Introduction to Malware Analysis

Malware analysis is a critical process used to examine malicious software (malware) to understand its functionality, origin, and potential impact. Organizations use malware analysis to develop countermeasures and detect vulnerabilities exploited by malicious actors. Two primary methods to explore malware include static analysis and dynamic analysis. Each method offers unique advantages and drawbacks, making them complementary in nature. In addition to manual analysis, automated tools like Cuckoo Sandbox are used to streamline the malware examination process, providing deeper insights into how malware operates within a controlled environment.

Static Analysis

Static analysis involves examining the malware's code without actually executing it. Analysts decompile or disassemble the malware to inspect its structure, strings, and binary data, looking for clues about its behavior.

Pros of Static Analysis:

1. Safer to perform: Since the malware is not executed, static analysis is relatively safe and can be conducted without the risk of triggering harmful actions on the system. This makes it ideal for analyzing highly destructive malware that could damage the environment if run.
2. Identifies code-level details: Static analysis allows analysts to examine the actual code, providing insights into how the malware is constructed, including the presence of any obfuscation techniques, encryption, or specific function calls.

Cons of Static Analysis:

1. Inability to detect runtime behavior: Static analysis cannot reveal what happens when the malware is executed, such as what system modifications are made or how it interacts with network components. It only shows the potential, not actual, behavior.
2. Time-consuming and requires expertise: Static analysis can be extremely time-consuming and requires significant expertise in reverse engineering to interpret complex or obfuscated code. Automated static analysis tools often miss hidden behaviors or heavily encrypted payloads.

Dynamic Analysis

Dynamic analysis, on the other hand, involves running the malware in a controlled, isolated environment (such as a virtual machine or sandbox) to observe its real-time behavior.

Pros of Dynamic Analysis:

1. Reveals runtime behavior: One of the biggest advantages of dynamic analysis is its ability to demonstrate what the malware does when executed. Analysts can observe the actual network communication, file modifications, registry changes, and more, providing a clearer picture of its intentions.
2. Easier to identify obfuscated code: Since dynamic analysis involves running the malware, it can bypass obfuscation or encryption techniques that might be hidden in static analysis. The malware reveals its true behavior during execution, which is valuable for understanding advanced threats.

Cons of Dynamic Analysis:

1. Risk of evasion: Some malware is designed to detect when it is being run in a virtual or sandbox environment and will not execute its malicious payload. This means dynamic analysis might not always provide a complete picture, as the malware may behave differently in a real-world setting.
2. Potential for system infection: Despite being conducted in a controlled environment, there is always a slight risk of malware escaping the sandbox or virtual machine and infecting the host system. Proper precautions must be taken to ensure complete isolation of the testing environment.

Cuckoo Sandbox as a Malware Analysis Tool

Cuckoo Sandbox is an open-source tool widely used for dynamic malware analysis. It allows analysts to safely run and monitor malware in an isolated environment. Cuckoo Sandbox provides comprehensive reports detailing what the malware does during execution, such as API calls, file system activity, and network connections.

Insights Gained from Cuckoo Sandbox:

1. Behavioral patterns: Cuckoo Sandbox provides detailed behavioral analysis of malware. It records all actions the malware takes while running, including file creation, deletion, and modification, changes to system settings, and communications with remote servers. This gives security analysts a clear understanding of the malware's operational intent.
2. Network activity: The tool can capture all network traffic generated by the malware, allowing analysts to track command-and-control (C2) servers or malicious domains the malware attempts to contact. This can aid in mapping the larger threat landscape and understanding how the malware propagates or exfiltrates data.
3. System impact: Cuckoo Sandbox offers insights into the malware's impact on the host system, including memory utilization, process creation, and registry alterations. This helps identify specific system vulnerabilities that the malware exploits.

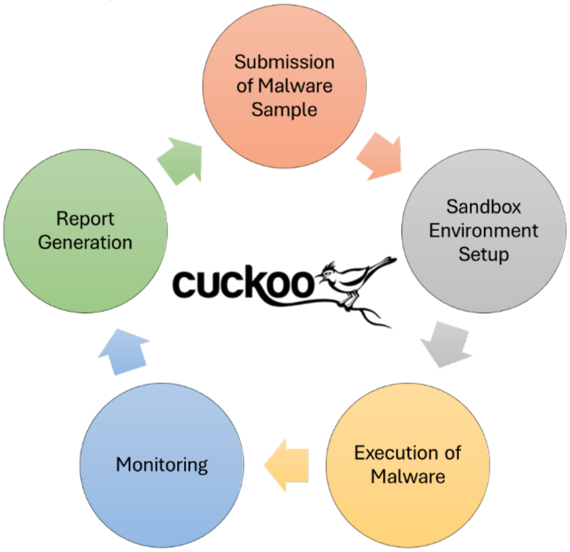

Figure 1.0 Cuckoo sandbox workflow for dynamic analysis

1. Submission of Malware Sample: The analyst submits the malware sample to the Cuckoo Sandbox.
2. Sandbox Environment Setup: Cuckoo Sandbox sets up a controlled virtual machine or isolated environment to run the malware.
3. Execution of Malware: The malware is executed within the isolated environment.
4. Monitoring: Cuckoo Sandbox monitors and logs the malware's behavior, including:
   a. API calls
   b. File system modifications

   c. Registry changes
   d. Network communications

5. Report Generation: A detailed report is generated, providing insights into the malware's actions during execution.

Conclusion

Both static and dynamic analysis have important roles in understanding malware, each with its own set of advantages and challenges. While static analysis excels in identifying underlying code structures, dynamic analysis provides real-time insights into how the malware behaves in execution. Tools like Cuckoo Sandbox significantly enhance dynamic analysis by providing an automated, safe environment to execute malware, generating comprehensive reports that help analysts develop mitigation strategies. Combining both static and dynamic approaches, along with tools like Cuckoo, provides the most complete picture of a malware's capabilities and intentions.

References

CrowdStrike. (n.d.). Malware analysis. Retrieved October 12, 2024, from https://www.crowdstrike.com/en-us/cybersecurity-101/malware/malware-analysis/

Varonis. (2023, August 22). Cuckoo sandbox: Analyzing malicious files. Retrieved October 12, 2024, from https://www.varonis.com/blog/cuckoo-sandbox

*** END OF DOCUMENT ***