Environment Awareness Final Paper.pdf

Archived: 2026-04-05 20:43:40 UTC

Sida 3 av 17

Introduction

A Sandbox is an isolated and instrumented detonation environment where malware can be deployed and observed without causing any harm to the actual system. This type of system is used for dynamic malware analysis and behavior-based detection. In order for Sandboxes to work, it is necessary that the executed file exhibits malicious behavior, otherwise it will be classified as benign.

Following this requirement, the main objective of cyber actors and their Sandbox evasion techniques is to hide the actual behavior of the file and therefore avoid being labeled as a potentially malicious threat.

This investigation will cover the group of techniques used by malware to detect if it is being executed in a controlled environment, such as a system with the presence of Sandbox technology, or a system with the presence of forensic analysts and tools. As a result, any malicious program that implements this kind of maneuvers will be aware of these environments and change their behavior to avoid detection or attempt to exit to avoid further analysis.

The most common responses to these types of detections are:

● The program ends abruptly when it detects that it is being detonated.

However, this option is not recommended since it is likely to raise suspicion.

● The program ends abruptly and shows an error message related to a missing module or a corrupted executable file in order to avoid suspicion.

● The program performs only benign operations in order to be classified as a non-malicious file.

In the next section, each of the categories, and their respective sub-techniques, which are part of the Environment Awareness will be deepened and explained to mark a clear understanding of how cyber actors carry out the detection of the controlled environments.

Source: https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc/edit