Detecting Malware and Sandbox Evasion Techniques

By Created by:Dilshan Keragala

Archived: 2026-04-05 19:19:59 UTC

System integrity is a cardinal component of information security. It ensures that information systems operate within some desirable limits. Internet security threats such as malware and highly malicious programs are on the rise, resulting in the necessity for extensive research efforts to develop mechanisms that can counter various threats. Malware Sandbox analysis is an effective mechanism having received propositions as a potential solution. When using Malware Sandbox analysis, samples of malware are executed to determine their behaviors. The results of this action are then recorded for subsequent study. This paper first will explain the nature of malware, then discuss the available methods to detect and control various malware activities. Finally, it will examine the general Sandbox structure, with a major focus on a novel behavior based malware detection method leveraging Sandbox-evasion behaviors as an avenue to detecting, mitigating or totally evading the malware.
