Virtualization/Sandbox Evasion: User Activity Based Checks, Sub-technique T1497.002 - Enterprise

Archived: 2026-04-05 16:38:33 UTC

Adversaries may employ various user activity checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors.[1]

Adversaries may search for user activity on the host based on variables such as the speed/frequency of mouse movements and clicks [2] , browser history, cache, bookmarks, or number of files in common directories such as home or the desktop. Other methods may rely on specific user interaction with the system before the malicious code is activated, such as waiting for a document to close before activating a macro [3] or waiting for a user to double click on an embedded image to activate.[4]

Source: https://attack.mitre.org/techniques/T1497/002