

Virtualization/Sandbox Evasion, Technique T1633 - Mobile

Archived: 2026-04-05 17:08:40 UTC

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors after checking 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's behavior to disengage from the victim or conceal the core functions of the payload. They may also search for VME artifacts before dropping further payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](#) during automated discovery to shape follow-on behaviors.

Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](#) such as checking for system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment.

Source: <https://attack.mitre.org/techniques/T1633>