# Video Capture, Technique T1512 - Mobile

Archived: 2026-04-02 10:36:59 UTC

An adversary can leverage a device's cameras to gather information by capturing video recordings. Images may also be captured, potentially in specified intervals, in lieu of video files.

Malware or scripts may interact with the device cameras through an available API provided by the operating system. Video or image files may be written to disk and exfiltrated later. This technique differs from Screen Capture due to use of the device's cameras for video recording rather than capturing the victim's screen.

In Android, an application must hold the `android.permission.CAMERA` permission to access the cameras. In iOS, applications must include the `NSCameraUsageDescription` key in the `Info.plist` file. In both cases, the user must grant permission to the requesting application to use the camera. If the device has been rooted or jailbroken, an adversary may be able to access the camera without knowledge of the user.

---

Source: https://attack.mitre.org/techniques/T1512