Hooking, Technique T1617 - Mobile

Archived: 2026-04-05 18:20:12 UTC

Adversaries may utilize hooking to hide the presence of artifacts associated with their behaviors to evade detection. Hooking can be used to modify return values or data structures of system APIs and function calls. This process typically involves using 3rd party root frameworks, such as Xposed or Magisk, with either a system exploit or pre-existing root access. By including custom modules for root frameworks, adversaries can hook system APIs and alter the return value and/or system data structures to alter functionality/visibility of various aspects of the system.

Source: https://attack.mitre.org/techniques/T1617