Indicator Removal on Host: Disguise Root/Jailbreak Indicators, Sub-technique T1630.003 - Mobile

Archived: 2026-04-05 15:01:52 UTC

Other sub-techniques of Indicator Removal on Host (3)

ID	Name
T1630.001	Uninstall Malicious Application
T1630.002	File Deletion
T1630.003	Disguise Root/Jailbreak Indicators

An adversary could use knowledge of the techniques used by security software to evade detection.[1][2] For example, some mobile security products perform compromised device detection by searching for particular artifacts such as an installed "su" binary, but that check could be evaded by naming the binary something else. Similarly, polymorphic code techniques could be used to evade signature-based detection.[3]

Source: https://attack.mitre.org/techniques/T1630/003