Detection of Compromise Client Software Binary, Detection Strategy DET0712

Archived: 2026-04-05 15:18:24 UTC

AN1838

Application vetting services could detect applications trying to modify files in protected parts of the operating system.
Verified Boot can detect unauthorized modifications to the system partition.[1] Android's SafetyNet API provides remote attestation capabilities, which could potentially be used to identify and respond to compromised devices. Samsung Knox provides a similar remote attestation capability on supported Samsung devices.

Log Sources

AN1839

Application vetting services could detect applications trying to modify files in protected parts of the operating system.
Verified Boot can detect unauthorized modifications to the system partition.[1] Android's SafetyNet API provides remote attestation capabilities, which could potentially be used to identify and respond to compromised devices. Samsung Knox provides a similar remote attestation capability on supported Samsung devices.

Log Sources
