Impair Defenses: Device Lockout, Sub-technique T1629.002 - Mobile

Archived: 2026-04-05 16:27:32 UTC

An adversary may seek to inhibit user interaction by locking the legitimate user out of the device. This is typically accomplished by requesting device administrator permissions and then locking the screen using `DevicePolicyManager.lockNow()`. Other novel techniques for locking the user out of the device have been observed, such as showing a persistent overlay, using carefully crafted "call" notification screens, and locking HTML pages in the foreground. These techniques can be very difficult to get around, and typically require booting the device into safe mode to uninstall the malware.[1][2][3]

Prior to Android 7, device administrators were able to reset the device lock passcode to prevent the user from unlocking the device. The release of Android 7 introduced updates that only allow device or profile owners (e.g. MDMs) to reset the device’s passcode.[4]

Source: https://attack.mitre.org/techniques/T1629/002