STA-6 · Mobile Threat Catalogue

Archived: 2026-04-06 00:16:44 UTC

Mobile Threat Catalogue

Malicious Apps Installed via USB

Contribute

Threat Category: Mobile Operating System

ID: STA-6

Threat Description: When connected through USB, potentially malicious applications can be installed on the mobile device, sometimes without the user's knowledge. These applications can be installed intentionally by the user, or by an infected computer or charging station.

Threat Origin

Mobile Iron Q4 Mobile Security and Risk Review [1]

Government Mobile and Wireless Security Baseline [2]

Exploit Examples

Injecting Malware into iOS Devices via Malicious Chargers [3]

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

To reduce the probability of this attack, follow general best practices for securing systems to which a trusted mobile device may synchronize or access debugging functionality. For example, ensure the OS and applications maintain current security updates, endpoint protection software is installed, and systems are monitored for anomalous behavior.

Consider use of Android 4.2.2 or later devices. In Android 4.2.2, connections to ADB are authenticated with an RSA keypair. This prevents unauthorized use of ADB where the attacker has physical access to a device. [4]

Consider the use of Android 6.0 or later, in which users must confirm to allow USB access to files, storage, or other functionality on the phone. The default behavior permits charging only. [5]

Consider the use of iOS 7.x or later, in which synchronization with a computer over USB that requires the device be unlocked and the user confirm an explicit trust request. Failure to establish trust permits charging only.

Provide extra device chargers to users that plug directly into an electrical socket and encourage users to use them instead of plugging into potentially malicious USB charging stations or USB ports on potentially infected computers.

Mobile Device User

To prevent some varities of this attack, ensure ADB debugging is disabled.

To reduce the probability of this attack, do not accept prompts to trust untrusted systems.

Consider use of Android 4.2.2 or later devices. In Android 4.2.2, connections to ADB are authenticated with an RSA keypair. This prevents unauthorized use of ADB where the attacker has physical access to a device. [4]

Consider the use of Android 6.0 or later, in which users must confirm to allow USB access to files, storage, or other functionality on the phone. The default behavior permits charging only. [5]

Consider the use of iOS 7.x or later, in which synchronization with a computer over USB that requires the device be unlocked and the user confirm an explicit trust request. Failure to establish trust permits charging only.

Provide extra device chargers to users that plug directly into an electrical socket and encourage users to use them instead of plugging into potentially malicious USB charging stations or USB ports on potentially infected computers.

References

1. Q4 Mobile Security and Risk Review, white paper, MobileIron; https://www.mobileiron.com/sites/default/files/qsreports/files/security-report-Q415-v1.2-EN.pdf [accessed 8/25/2016] ↩
2. Government Mobile and Wireless Security Baseline, CIO Council, 23 May 2013; https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf [accessed 8/1/2022] ↩
3. B. Lau et. al. , Injecting Malware into iOS Devices via Maliscious Chargers, presented at BlackHat, 2013. https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf [accessed 8/23/16] ↩
4. “Security Enhancements in Android 4.3”; https://source.android.com/security/enhancements/enhancements43.html [accessed 8/29/2016] ↩ ↩2
5. “Security Enhancements in Android 6.0”; https://source.android.com/security/enhancements/enhancements60.html [accessed 8/29/2016] ↩ ↩2
