APP-29 · Mobile Threat Catalogue

Archived: 2026-04-05 21:30:04 UTC

Mobile Threat Catalogue

Command-and-control Traffic Evades Analysis

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-29

Threat Description: Mobile OS offer built-in and encrypted communication channels that may appear to be normal traffic or occur out-of-band (over a cellular connection), thereby evading detection by Wi-Fi-based enterprise traffic analysis tools. Google offers Google Cloud Messaging (GCM) and newly, Firebase Cloud Messaging (FCM), which provides two-way communication. Apple offers the Apple Push Notification Service (APNS), which offers one-way communication from server-to-device. Both services are commonly used within mobile apps, which makes detecting abuse of these services difficult.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

Mobile Malware Evolution: 2013 [1]

DroydSeuss: A Mobile Banking Trojan Tracker [2]

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Deploy MAM or MDM solutions with policies that prohibit the side-loading of apps, which may bypass security checks on the app.

Deploy MAM or MDM solutions with policies that prohibit the installation of apps from 3rd party (unofficial) app stores.

Use app-vetting tools or services to identify remote access control apps that receive commands over notification or messaging serices or other communication channels.

Mobile Device User

Disable access to notification or messaing services to apps for which such functions are not actually used.

Use Verify Apps feature to identify potentially harmful apps.

References

1. V. Chebyshev and R. Unuchek, “Mobile Malware Evolution: 2013”, blog, 24 Feb. 2014; https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/ [accessed 8/25/2016] ↩

2. A. Coletta et al., “DroydSeuss: A Mobile Banking Trojan Tracker - A Short Paper”, in Proceedings of Financial Cryptography and Data Security 2016, 2016; http://fc16.ifca.ai/preproceedings/14_Coletta.pdf [accessed 8/25/2016] ↩
