APP-12 · Mobile Threat Catalogue

Archived: 2026-04-05 21:45:25 UTC

Mobile Threat Catalogue

Malicious Device Information Gathering

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-12

Threat Description: Persistent information that can be used to identify or characterize a specific mobile device in one or more contexts, such as IMEI, IMSI, MAC address, phone number, mobile OS, or installed apps, may be collected by a malicious or privacy-invasive app to facilitate future attacks. These values, particularly in combination, greatly increase potential for geo-physical or behavioral tracking, device fingerprinting, and impersonation attacks against the device or its user.

Threat Origin

The Google Android Security Team's Classifications for Potentially Harmful Applications [1]

Exploit Examples

Slembunk: An Evolving Android Trojan Family [2]

An investigation of Chrysaor Malware on Android [3]

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Deploy MAM or MDM solutions with policies that prohibit the sideloading 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.

Perform application vetting to identify inappropriate behaviors by apps including permission requests made by the apps

Use application threat intelligence data about potential data collection risks associated with apps installed on devices

Mobile Device User

Use Android Verify Apps feature to identify apps that may abuse permissions to perform data collection.

Consider the use of devices that support Android 11 or higher, in which applications have limited visibility of what other apps are on the device.

References

1. The Google Android Security Team's Classifications for Potentially Harmful Applications, Apr. 2016; https://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_PHA_classificati [accessed 8/25/2016] ↩

2. W. Zhou et al., "Slembunk: An Evolving Android Trojan Family Targeting Users of Worldwide Banking Apps", blog, 17 Dec. 2015; www.fireeye.com/blog/threat-research/2015/12/slembunk_an_evolvin.html [accessed 8/25/2016] ↩

3. "An investigation of Chrysaor Malware on Android", blog, 3 Apr. 2017; https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html [accessed 4/5/2017] ↩
