APP-13 · Mobile Threat Catalogue

Archived: 2026-04-29 07:08:17 UTC

Mobile Threat Catalogue

Sensitive Information Discovery via OS APIs

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-13

Threat Description: Apps may be granted permission, by the user or by default, access common data stores provided by the mobile OS. Common stores are contacts lists, call history, calendar, notes, or app clipboard. When apps used in differing personal and enterprise contexts have access to these stores, they may contain co-mingled personal and enterprise data. A malicious or invasive app granted access to these locations can collect any sensitive data stored there, likely with an intent to exfiltrate it to the attacker.

Threat Origin

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

Exploit Examples

An investigation of Chrysaor Malware on Android [2]

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 privacy-invasive behaviors by apps.

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

Use features such as Apple iOS Managed Apps, Android for Work, or Samsung KNOX Workspace that provide additional separation between personal apps and enterprise apps to mitigate the leakage of private information between work/personal contexts.

Mobile Device User

Use Android Verify Apps feature to identify apps that may violate privacy.

Mobile App Developer

Only request access to the minimal set of shared data stores (e.g., contacts, calendar), OS services (e.g. location services), and device sensors (e.g. camera, microphone) necessary for the app to provide functionality.

Only collect the minimal set of device or user data necessary for the app to provide functionality.

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. "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] ↩
