APP-21 · Mobile Threat Catalogue

Archived: 2026-04-05 17:20:45 UTC

Mobile Threat Catalogue

App Vetting Misses Malicious App

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-21

Threat Description: App vetting methods designed to detect malicious code are complicated by various code obfuscation techniques such as sandbox detection, encryption, and dead code (malicious functions unreachable by normal program execution). As a result, a malicious app subjected to app vetting may appear free of harmful code and safe to publish or distribute.

Threat Origin

Dissecting Android Malware: Characterization and Evolution [1]

Exploit Examples

CVE Examples

- CVE-2015-07555
- CVE-2016-5131

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.

Use app-vetting tools or services to identify untrusted apps that contain encrypted or obfuscated code.

Use application threat intelligence data about apps that contain encrypted or obfuscated code

Mobile Device User

Use Android Verify Apps feature to identify potentially harmful apps.

Mobile App Developer

To mitigate your app being detected as potentially malicious, do not arbitrarily encrypt or obfuscate code.

References
