APP-30 · Mobile Threat Catalogue

Archived: 2026-04-06 01:19:43 UTC

Mobile Threat Catalogue

Exfiltration Evades Analysis

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-30

Threat Description: Malicious apps that collect and exfiltrate sensitive data have multiple communication channels available. In addition to using encryption, steganography, or other obfuscation techniques over an inspected Wi-Fi connection, apps may exfiltrate data over a cellular connection, which cannot be directly analyzed using an enterprise network security mechanism. While requiring a receiver with proximity to the device, apps can also potentially exfiltrate data over Bluetooth or NFC connections. Common use of these channels are interfaces to device peripherals or short-range data transfers, making these channels less likely to be monitored by enterprise security mechanisms.

Threat Origin

Dissecting Android Malware: Characterization and Evolution [1]

Exploit Examples

Not Applicable

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 application threat intelligence data about potential data exfiltration risks associated with apps installed on COPE or BYOD devices

Use app-vetting tools or services to identify apps that appear to exfiltrate data.

Mobile Device User

Use Android Verify Apps feature to identify apps that may abuse communication channels to exfiltrate data.

References

1. Y. Zhou and X. Jiang, “Dissecting Android Malware: Characterization and Evolution”, in Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012, pp 95-109; http://ieeexplore.ieee.org/document/6234407/?arnumber=6234407 [accessed 8/25/2016] ↩
