APP-16 · Mobile Threat Catalogue

Archived: 2026-04-05 22:46:02 UTC

Mobile Threat Catalogue

Premium SMS Fraud

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-16

Threat Description: SMS messages were initially charged to a cellular subscriber's account on a per-message basis. However, some services use SMS messaging as a subscription or one-time payment method. The charge associated with the SMS message is placed on the cellular subscriber's account and collected along with standard cellular service fees. This model enables malicious app developers to potentially collude with premium SMS service providers to commit fraud against users. The subscriber is held responsible for the fraudulent charges by the cellular carrier. Early forms of this attack exploited the weak OS permission models that allowed apps to send premium SMS messages without user interaction, which prompted improvement by affected OS developers. Contemporary variants must instead exploit vulnerabilities in the mobile OS to send messages without user knowledge and consent.

Threat Origin

Dissecting Android Malware: Characterization and Evolution [1]

Exploit Examples

zSone, RogueSPPush, GGTracker malware described in Dissecting Android Malware: Characterization and Evolution [1]

Mkero: Android malware secretly subscribes victims to premium SMS services [2]

Chinese Android botnet 'netting millions' [3]

Android Security 2015 Year In Review [4]

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Ensure Android devices are running a recent version of Android, as starting in Android 4.2, user confirmation is needed before apps can send premium SMSs (source: https://source.android.com/security/enhancements/enhancements42.html).

Perform application vetting to identify SMS fraud by apps including permission requests made by the apps.

Use application threat intelligence data about potential SMS fraud risks associated with apps installed on devices.

Mobile Device User

Ensure Android devices are running a recent version of Android, as starting in Android 4.2, user confirmation is needed before apps can send premium SMSs (source: https://source.android.com/security/enhancements/enhancements42.html).

Use Android Verify Apps feature to apps that attempt to abuse SMS functionality.

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] ↩ ↩2

2. C. Page, “MKero: Android malware secretly subscribes victims to premium SMS services”, The Inquirer, 9 Sept. 2015; www.theinquirer.net/inquirer/news/2425201/mkero-android-malware-secretly-subscribes-victims-to-premium-sms-services [accessed 8/25/2016] ↩

3. T. Espiner, “Chinese Android botnet ‘netting millions’, says Symantec”, ZDNet, 10 Feb. 2012; www.zdnet.com/article/chinese-android-botnet-netting-millions-says-symantec/ [accessed 8/25/2016] ↩

4. Android Security 2015 Year In Review, Google, 2016; https://source.android.com/security/reports/Google_Android_Security_2015_Report_Final.pdf [accessed 8/25/2016] ↩
