APP-31 · Mobile Threat Catalogue

Archived: 2026-04-06 01:15:51 UTC

Mobile Threat Catalogue

Masquerading as a Legitimate Application

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-31

Threat Description: 3rd party apps may duplicate the appearance and interface of a legitimate app, such as a banking app, to trick the user into supplying authentication credentials or other sensitive information intended for the app being spoofed. This threat was facilitated on Android devices before 5.0, as a malicious app could determine if a target app was running in the foreground, then initiate an activity to gain focus and intercept credential entry by the user.

Threat Origin

Phishing on Mobile Devices [1]

Exploiting Androids for Fun and Profit [2]

The Latest Android Overlay Malware Spreading via SMS Phishing in Europe [3]

Password-Stealing Instagram App [4]

Hackers Sneak Malware Into Apple App Store ‘To Steal iCloud Passwords’ [5]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Consider the use of devices that support Android 5.0 and later, in which ActivityManager.getRunningTasks() has been modified to stop leaking information about the current foreground activity, increasing the difficulty of

malicious apps being able to perform a user interface spoofing attack

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 app-vetting tools or services to identify apps that attempt to spoof the interface to other apps or common web sites, such as banking sites.

Mobile Device User

Consider the use of devices that support Android 5.0 and later, in which ActivityManager.getRunningTasks() has been modified to stop leaking information about the current foreground activity, increasing the difficulty of malicious apps being able to perform a user interface spoofing attack

Use Android Verify Apps feature to identify potentially harmful apps.

References

1. A.P. Felt and D. Wagner, Phishing on Mobile Devices, presented at Web 2.0 Security & Privacy 2011, 26 May 2011; https://people.eecs.berkeley.edu/~daw/papers/mobphish-w2sp11.pdf [accessed 7/27/2022] ↩
2. R. Hassell, Exploiting Androids for Fun and Profit, presented at Hack In The Box Security Conference 2011, 12-13 Oct. 2011; http://conference.hitb.org/hitbsecconf2011kul/materials/D1T1 - Riley Hassell - Exploiting Androids for Fun and Profit.pdf [accessed 8/25/2016] ↩
3. W. Zhou et al., “The Latest Android Overlay Malware Spreading via SMS Phishing in Europe”, blog, 28 June 2016; www.fireeye.com/blog/threat-research/2016/06/latest-android-overlay-malware-spreading-in-europe.html [accessed 8/25/2016] ↩
4. J. Clover, “Password-Stealing Instagram App ‘InstaAgent’ Reappears in App Store Under New Name”, MacRumors, 22 Mar. 2016; www.macrumors.com/2016/03/22/password-stealing-instaagent-app-reappears/ [accessed 8/25/2016] ↩
5. T. Fox-Brewster, “Hackers Sneak Malware Into Apple App Store ‘To Steal iCloud Passwords’”, Forbes, 18 Sept. 2015; www.forbes.com/sites/thomasbrewster/2015/09/18/xcodeghost-malware-wants-your-icloud/ [accessed 8/25/2016] ↩
