APP-14 · Mobile Threat Catalogue

Archived: 2026-04-05 23:42:27 UTC

Mobile Threat Catalogue

Masquerade as Legitimate Application

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-14

Threat Description: Like well-behaved apps, a trojan app offers some functionality to the user, though a trojan also includes hidden functionality that is malicious or otherwise undesirable. One technique for deploying trojan functionality is to obtain the install packages for a legitimate app, decompile/disassemble it, introduce the trojan, and then generate a new install package. The app will appear to a user to be the legitimate app. Distribution of trojans is commonly achieved by submission to open 3rd party app stores or social engineering attacks claiming to offer users the app with incentives (lower cost, free, extras unlocked, etc.).

Threat Origin

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

Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices [2]

Dissecting Android Malware: Characterization and Evolution [3]

Exploit Examples

New Android Malware Family Evades Antivirus Detection by Using Popular Ad Libraries [4]

Slembunk: An Evolving Android Trojan Family Targeting Users of Worldwide Banking Apps [5]

Incident Response for Android and iOS [6]

Cloned banking app stealing usernames sneaks into Google Play [7]

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.

Use application threat intelligence data about potentially harmful apps installed on COPE or BYOD devices

Mobile Device User

Use Android Verify Apps feature to identify potentially harmful apps.

Mobile App Developer

To reduce the ease of an attacker to abuse existing app functionality, 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.

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. L. Neely, Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices, SANS Institute, 2016; www.sans.org/reading-room/whitepapers/analyst/mobile-threat-protection-holistic-approach-securing-mobile-data-devices-36715 [accessed 8/25/2016] ↩
3. 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] ↩
4. C. Zheng and Z. Xu, "New Android Malware Family Evades Antivirus Detection by Using Popular Ad Libraries", blog, 7 July 2015; http://researchcenter.paloaltonetworks.com/2015/07/new-android-malware-family-evades-antivirus-detection-by-using-popular-ad-libraries/ [accessed 8/25/2016] ↩
5. W. Zhou et al., "Slembunk: An Evolving Android Trojan Family Targeting Users of Worldwide Banking Apps", blog, 17 Dec. 2015; www.fireeye.com/blog/threat-research/2015/12/slembunk_an_evolvin.html [accessed 8/25/2016] ↩
6. Unauthorized App Discovered, in Incident Response for Android and iOS, www.nowsecure.com/resources/mobile-incident-response/en/case-studies/unauthorized-app-discovered.html [accessed 8/25/2016] ↩
7. M. Kelly, "Cloned banking app stealing usernames sneaks into Google Play", blog, 24 June 2014; https://blog.lookout.com/blog/2014/06/24/bankmirage/ [accessed 8/25/2016] ↩
