Help Net SecurityJanuary 10, 2018

Apps most frequently blacklisted by enterprise security teams

Appthority released its Enterprise Mobile Security Pulse Report for Q4 2017, which details the apps most frequently blacklisted by enterprise mobility and security teams.

TOP 10 BLACKLISTED ANDROID APPS

Application Name	Version	Category	Risk Score	Score Driver
Facebook	91.0.0.17.68	Social	6	Accesses Address Book/Camera/ Calendar/Microphone/SMS Archive, Tracks Location
Messenger [Facebook]	98.0.0.18.71	Communication	7	Sends Address Book/SMS Messages
Instagram	10.5.1	Social	5	HTTPS Exceptions
Frozen Frenzy Valentine Hearts	1.5.1	Game_Puzzle	5	HTTPS Exceptions
Bakery Story: Cats Cafe	1.5.5.9.3	Casual	6	Sends IMEI, Sends Data Unencrypted
Candy Blast Mania	1.6.2.3g	Arcade	5	HTTPS Exceptions
Dragon Story: Sun and Moon	2.4.0.1s54g	Game_Casual	5	HTTPS Exceptions
Dot Eater	1.3.4	Casual	6	Sends Data Unencrypted
Flick Shoot (Soccer Football)	3.4.5	Sports	6	Sends Data Unencrypted
Black Luxury Theme for Huawei	1.1.11	Personalization	6	Sends IMEI, Sends Data Unencrypted

Most blacklisted apps

For iOS devices, popular dating app Tinder made the list of most blacklisted apps, joining WhatsApp Messenger and Pokémon GO, which topped the list for the second consecutive quarter. For Android, the top blacklisted apps were WhatsApp Messenger, Facebook Messenger and Instagram, all new to the list from the previous quarter.

Enterprises blacklist apps for a range of security concerns, including security policy compliance and concerns about data handling. Most of the Android and iOS apps that were blacklisted in Q4 scored in the data leakage range. For Android, this was primarily due to sending data unencrypted. For iOS, this was for accessing the address book, camera and microphone, as well as tracking location and sending sensitive data unencrypted.

Riskiest Android and iOS apps

Research shows that many popular apps present in enterprise environments have mobile threat risk scores indicative of data leakage and vulnerabilities.

The riskiest Android apps in enterprise environments include: Deutsche Telekom Online Manager, NFL Mobile, OMD Mobile, Uber and WhatsApp Messenger. The riskiest iOS apps found in enterprises included Dropbox, Facebook Messenger, Instagram, Pandora, Spotify and WhatsApp Messenger.

TOP 10 BLACKLISTED IOS APPS

Application Name	Version	Category	Risk Score	Score Driver
WhatsApp Messenger	2.17.71	Social Networking	7	Sends Address Book
Pokémon GO	1.37.1	Games	6	Accesses Address Book/Camera, Tracks Location
Tinder	8.2.0	Lifestyle	7	Sends SMS Messages
百度贴吧-上贴吧，找组织 (Baidu Tieba)	7.9.0	Social Networking	6	Accesses Camera/Microphone, Tracks Location, Sends Data Unencrypted
QQ	6.5.6	Social Networking	6	Accesses Address Book/Camera/ Calendar/Microphone, Tracks Location, Sends Data Unencrypted
QQ同步助手-一键备份联系人的换机神器 (QQ International)	6.8.7	Utilities	6	Accesses Address Book/Camera, Tracks Location, Sends Data Unencrypted
WeChat	6.5.21	Social Networking	7	Sends Address Book/Sensitive Data Unencrypted
Battery Doctor - Master of Battery Maintenance	7.4.8	Utilities	7	Sends SMS Messages/Sensitive Data Unencrypted
PDF Reader	5.1	Utilities	7	Sends SMS Messages
手机百度 - 世界很复杂，百度更懂你 (Mobile Baidu)	9.3.6	Utilities	6	Accesses Address Book/Camera/ Microphone, Tracks Location, Reads Clipboard, Sends Location/Device Name/ Data Unencrypted

Leading destination countries for the top Android and iOS apps are the United States, Ireland and Germany. The United States, with over 85% of mobile app connections, saw the percent of trustworthy connections decline from 32% to 30.4% for Android connections and from 15% to 14.2% for iOS connections.