Bitdefender®

Mobile Operating System Wars – Android vs. iOS

Authors

Bogdan BOTEZATU – Senior E-Threat Analyst

Vlad BORDIANU – Malware Researcher, Clueful

Tiberiu AXINTE - Malware Researcher, Clueful

Table of Contents

When we introduced Clueful for Android, we thought mobile users should know what the applications on their devices were doing. One year and a couple hundred thousand analyzed applications later, Clueful intelligence has picked up an interesting trend: **applications are equally invasive and curious on iOS as on Android, even though one may argue that one of the operating systems is safer.**

For roughly a year, we have been collecting applications from the Play Store and iTunes to analyze both statically and dynamically. For the Android version of Clueful, we're aggregating 314,474 free applications, while the iOS version of Clueful holds references for 207,843 free apps. These applications are broken down into clues which give the user a transparent and comprehensive overview of what the application tries to access, what privileges it requires and how it is going to handle the data it has access to when sending it over the web.

A primer on application permissions

Before digging further, we need to mention that application permissions differ from one operating system to another. For instance, while Android permissions are declared at install and cannot be altered later, iOS permissions are granted at runtime, when device owners have to allow or deny access to various resources, such as current location. Regardless, both applications for Android and iOS can perform a range of interactions with the user's device, but also with third-party internet services.

Comparable clues

Our analysis focuses on the most intrusive behaviors that the application developer may have included in their software products. We have also taken into account behaviors that are very similar in both Android and iOS:

1. **Tracking location**

Location tracking is a major concern for both Android and iOS platforms. Its implementation and use are similar in both platforms and is often requested by advertisers via framework APIs to track users' habits. The Clueful test reveals that **45.41% of the iOS apps have location-tracking capabilities, even if they don't explicitly do that**, as opposed to **only 34.55% of the Android applications**.

Some Android applications that track location:

- Latest Nail Fashion Trends (v. 3.1) – com.nail.fashion.trends - with an estimated user base of between 100,000 and 500,000.

iOS applications that track location

- **PokerStars TV** (v. 2.2.2.0) - uses geolocation to track users' exact location
- **Cheezburger** (v. 1.2.2) - uses geolocation to track users' exact location

2. **Reading contact list**

While only 7.69% of Android applications could read the contact list, iOS applications are much snoopier – 18.92% of applications designed for iOS are technically able to looking into the contact list.

Android applications that read the contact list:

- **Longman Contemporary English** (v. 1.81) - com.flexidict.data.longmancontemporary, currently removed from the Play Store;
- **Cambridge American Idiom** (v. 1.81) - com.flexidict.data2.cambridgeamericanidioms – currently removed from the Play Store.

Some iOS applications that read the contact list:

- **OLJ (**v. 1.1) - reads contact names and contacts' email addresses and send them to a remote server.
- **3D Badminton II** (v. 2.026) - reads contacts' emails and sends them to a server in Hong Kong.

3. **Leaks your email address/ device ID**

Among the most interesting pieces of information for an advertising network are e-mail addresses and unique device IDs / IMEI. This data also may be shared with third parties to, for example, send consumers behaviorally targeted advertisements, according to a recent Federal Trade Commission report.

About 14.58% of the Android applications may leak your Device ID and 5.73% of the total number of apps may leak your e-mail. Following the security incidents in 2012, when the Blue Toad advertising agency leaked one million UDIDs, Apple decided to deprecate the UDID API.

Some Android applications that leak the e-mail address:

- Logo Quiz Car Choices (v. 1.8.2.9) – car.logo.quiz.game.free – between 100,000 and 500,000 installations

- Blowing sexy girl's skirt (v. 1.6.0) – yong.app.blowskirt – between 100,000 and 500,000 installations

Some Android applications that leak the device ID:

- **Football Games - Soccer Juggle** (v. 1.4.2) – com.madelephantstudios.BallTapp – between 100,000 and 500,000 installations

- **Logo Quiz NFL NHL MLB NBA MLS** (v. 1.0.2.8) – com.fesdra.logoquiz.ussport – between 100,000 and 500,000 installations

iOS applications that leak the device ID:

- **Ringtone Maker** (v. 1.7)- sends device id to "adfonic.net"
- **Paradise Island: Exotic** (v. 1.3.14) - sends device id to third-party websites (to "offer.17bullets.com", "islandexotic.17bullets.com", "ma.mkhoj.com", "1.trace.multiclick.ru", "a.jumptap.com", "soma.smaato.com")

4. Leaks your phone number

Phone numbers are the link between a user's physical identity and virtual persona. It allows an aggregating party to correlate information about the user's behavior in applications (what content they are interested in, what applications they have installed and so on, and possibly link this information to an existing person, represented by a name and surname. 8.82% of the applications analyzed by Clueful for Android might leak the device's phone number to third-party advertisers. Applications integrating the AirPush and (in some circumstances) LeadBolt frameworks allow the developer to collect, encrypt and send the device's phone number. In some countries, carriers block this behavior to safeguard the user's data.

Some Android applications that try to leak phone numbers:

- **Football Games - Soccer Juggle** (v. 1.4.2) – com.madelephantstudios.BallTapp – between 100,000 and 500,000 installations
- **Button Football (Soccer)** (v. 1.10.3) – com.sicecommentr.buttonfootball – between 1,000,000 and 5,000,000 installations

One major difference in Android is that it lets consumers choose where they install their applications from. Not only can users install applications from third-party markets, but they can also download APK files directly from the developer's website so they won't be able to enjoy the security mechanism implemented by Google in the Play Store (Google Bouncer). In the absence of supervision from Google, these applications could collect much more data than they actually need to function properly.

Grey-area behavior in applications

While accessing location services can be used legitimately by applications, sending location information over the web is not necessary for some apps and may pose risks for users in case of a data breach with the information harvesting company. This is a typical case of grey-area use, when something obviously unnecessary for the application's functionality gets retrieved just to complement the amount of user data aggregated already.

About 10% of the analyzed Android applications are may be doing this with or without the user's prior information, depending on the way the advertising SDK is configured and the way it is set up at the initial

boot. Others applications that send location information also leak the phone number and the user's e-mail address to ad vendors.

Malicious behavior by negligence in applications

While tracking location, reading contacts or interacting with social media sites can be part of functionality, significant threats come from improper implementations of technologies, such as protocols for sending data from the user's device to the cloud. For instance, leaking unencrypted device IDs or sending plain-text passwords during the authentication process is highly dangerous for a mobile device that is often connected to public, potentially monitored Wi-Fi access points.

Conclusions

An old proverb has it that if you're not paying for it, then you are the product being sold. The free application ecosystem is actually free for the user, but is heavily monetized by the developer. Succinctly put, the application becomes free only after the user has paid for it with his or her privacy. And the situation is even worse, as paying for an application neither stops the private information flow, nor brings back the information already stored on file. More than that, information collection takes place without the user even being aware of what they agree with during installation.

The ad-supported model has been around since the emergence of Internet and dramatically contributed to the expansion of the Web as we know it. Sources all over the world have signed up for advertising programs that pay for traffic and allow content to be distributed for free to the user.

But mobile adware is totally different: adware tightly integrates with the device – it does not run inside the browser, isolated from other applications. On mobiles, advertising frameworks can learn your communications habits, friends, friends' contacts, location and – more frequently – all of the above at the same time. This turns them into the modern equivalent of spyware built into the device you're using the most throughout the day.

Clueful's mission is to shed some light into the application ecosystem as well as to clearly pinpoint the privacy threats the user exposes to when installing something as simple as an application.