Technical Brief

Sideloading from Unofficial App Stores: Despite the Risks, Why Do We Do it?

Introduction

For most smartphone and tablet users, installing an app is a simple and safe process that involves purchasing or downloading a file from the Apple App Store or Google Play Store. However, there is an alternative. 'Sideloading' is the process of downloading and installing apps onto a mobile device from a source that is not an official consumer or enterprise app store. With considerable benefits for the user, this method is continuously growing in popularity. However, it has also proven to present considerable risks which many users remain unaware of.

In their 2018 Year in Review, Google reported that Android devices that install apps from sources other than Google Play were 8 times more likely to have a Potentially Harmful App (PHA). As well as this, there have been numerous reports of sideloaded apps compromised with hidden Trojans, spyware, click fraud and phishing code, that if installed on a mobile device, could pose a serious danger to the security of the device and the data it holds.

Let's have a closer look at sideloading; how it works, the potential risks, and why it is that even when warned of the risks, so many people continue to download their apps from unofficial app stores?

What is sideloading?

The process of sideloading involves manually downloading and installing an app onto a device directly from an installer file outside of an official app store. There are two distinct ways that this is done on Android and iOS devices.

Android

For Android, sideloading used to require the user to simply tick a box in their device settings that would enable the download of an app .apk file from an 'unknown source', i.e. any source that is not the Google Play Store and therefore not monitored and vetted by its security feature, Google Play Protect. Following the release of Android 8 Oreo however, this process has changed significantly. Now the user is presented with a warning dialog box and must grant permission to

install every time they wish to sideload an app from an unofficial source. This has the positive effect of preventing apps from installing other apps without the user's permission, unless they specifically enable the ability in the device settings. However, even with these settings enabled, users can download from third party app stores such as 'Getjar', 'Mobogenie', 'SlideME' and 'Appbrain' or they can simply search for android .apk files and choose from the legion of available offerings online.

iOS

For iOS, there have also been considerable changes to the way in which unofficial apps are made available in recent years. Previously it was thought that only jail-broken iPhones or iPads could be used to download from unofficial sources. However, it was recently discovered that several rogue marketplaces, dubbed 'DarkSideLoaders', have made it possible to download millions of apps for non-jailbroken iOS devices. App developers have discovered a way to use Apple's Enterprise Developer program to distribute apps outside of the app store. The process involves posing as a legitimate business to obtain an Apple Enterprise App certificate, normally issued to enterprises that want to create their own internal apps for employees, and then simply asking the user to trust this publisher when installing the app. Earlier this year TechCrunch uncovered more than a dozen hardcore pornography and real-money gambling apps as well as modified versions of popular iOS apps such as Spotify, Angry Birds and Minecraft developed under this program and available for download independently of the App Store.

The Risks

Although not all third party app stores may pose a risk to device and data safety, it cannot be denied that without regulations or checks sideloading has its risks. In recent years there have been innumerable reports of unofficial apps found downloaded with hidden threats. These threats, mainly consisting of malware such as Trojans and spyware, are usually designed to inhibit the use of mobile devices and to collect sensitive information.

Both the App Store and Google Play Store pride themselves in their ability to vet and monitor all apps before and after they are made available for download to their customers. Google's Play Protect security feature describes itself as "the most widely deployed mobile threat protection service in the world", scanning over 50 billion apps across 2 billion devices every day and vetting more than 500k apps per day. In 2018, Google found that 0.68% of devices that installed apps from outside the Google Play Store were affected by one or more PHAs, while the PHA install rate for apps inside the official store was only 0.04%.

Similarly, since the release of the App Store in 2008, Apple have sought to differentiate the iPhone as an impenetrable, safe device that is available only to apps that have been vigorously reviewed and approved in accordance with their strict policies and standards. Therefore, by distributing via unofficial third party marketplaces, apps can access operating functions that would normally not be permitted by apps vetted by the App Store and Google Play Store.

Circumventing their strict rules and policies means that potentially, unofficial apps could be

used to install malware or phishing software onto a device, to exploit known or zero-day vulnerabilities to take over a device, or to access private operating system API's to steal data. On Android, there have been numerous reports of sideloaded apps attempting to root devices, install apps without user permission, and communicate to known malicious sites online. On iOS, unofficial apps have been used as Remote Access Trojans, allowing attackers to gain access to mobile devices of employees while active on internal corporate networks, putting both personal and corporate sensitive data at risk.

Why do people use unofficial app stores?

If they lack the protection and security guarantees of apps from official stores, why is it that so many users continue to use unofficial app stores? We have found that there are three main reasons.

Avoiding content fees

The biggest reason seems to be a simple one: users want to download content without paying for it. Many third party marketplaces offer games and wallpapers, content especially attractive to children, for free to entice unsuspecting users to download. When it was discovered in 2015, the unofficial marketplace vShare offered all of the top ten paid apps on the App Store for free, including well-known titles such as Grand Theft Auto and Clash of Clans. Alternative versions of popular apps such as Spotify and Pokemon Go, offering the same services without the regular ads or fees, were also discovered on the platform earlier this year. Unofficial apps can also give users access to streamed content such as movies, TV shows and music, as well as downloadable pirated content and torrent files, all free of charge.

Geographical restrictions

Users may also turn to unofficial app stores to get around geographical restrictions of content. Apps and other media are often only initially released to select regions, meaning people living in other locations may be forced to wait months or even years to access the content themselves. For example when events like Game of Thrones' final season or the release of Marvel's Avengers: Endgame earlier this year made it extremely important for people to access content as it was released to avoid spoilers and stay up-to-date with the latest cultural phenomena.

No other option

The third reason why device users may use third party sources to download apps is simply because it is the only way the content is made available. In 2018, Fortnite, the hugely popular online video game announced that it would be made available for download to Android devices but with a catch. Instead of downloading via the Google Play Store, users would need to sideload the game's .apk file from developer Epic Games' website before then installing the app. In situations like this, users who wish to access the game are left with little choice but to sideload the app and therefore potentially leave themselves vulnerable to compromise.

Key Takeaways

As enterprise mobility increases and over 80% of worker tasks are expected to take place on mobile by 2020, it is crucial that every employee device and the data it accesses is secured. But with the increased use of sideloading and so many of us using our mobile devices for personal as well as professional business, it is easy to see how a seemingly simple act like downloading a free version of a game or streaming the latest episode of our favorite TV show could have serious consequences for the safety of our personal as well as corporate data.

As evidence has shown, circumventing the preventative measures set out by Google and Apple is not difficult and many users are still able to access third party app stores. Without the safeguards and restrictions supplied by the official app stores, users cannot guarantee that sideloaded apps will be safe and legitimate. In order to ensure the safety of our apps, access to unofficial app stores must be avoided or in some cases blocked completely.

Want to find out more about sideloading, unofficial apps stores, and ensuring your mobile device is protected from malware?
Contact Corrata today