Corrata
IMMUNE SYSTEM FOR MOBILE

Technical Brief

Why Google and Apple's Malware Protection Might Not Be Good Enough

Introduction

Mobile malware can take many different forms. Spyware, adware, ransomware, and Trojans are commonly hidden in seemingly innocent apps and communications designed to fool users to take over, damage, and steal information from mobile devices. And with 42 million mobile malware attacks occurring every year, the problem only seems to be getting worse. So what are two of the biggest mobile operating system developers, Apple and Google, doing in response to this growing problem and is this enough?

Google and Apple's security features

Google Play Protect

Google Play Protect (GPP) is Google's built-in security feature for Android devices. Describing itself as "the most widely deployed mobile threat protection in the world", GPP combines new and existing security technology to scan over 50 billion apps across 2 billion devices every day ensuring that the official Google Play Store is free from any malicious software or "Potentially Harmful Apps" (PHAs). According to Google, all apps are rigorously analysed by security systems and Android experts before publishing to the Play Store, while all devices are regularly scanned to ensure that apps behave as they should. Any apps found to be exhibiting signs of malicious or improper behavior are promptly flagged to the user or removed from the device. In their 2018 Year in Review, Google reported an overall reduction of 15% in Android PHAs following the release of GPP, with the number of PHAs installed from inside the Google Play Store decreased to only 0.04%.

Apple

Meanwhile, since the release of the App Store in 2008, Apple have sought to differentiate the iPhone as an impenetrable, safe device available only to content that has been approved in accordance with the company's strict policies and standards. Apple state that they "review all apps and app updates submitted to the App Store in an effort to determine whether they are reliable, perform as expected, and are free of offensive material". Apps are examined under strict technical, content, and design criteria including performance, functionality, permissions

required, description accuracy, and user interface to determine whether apps are legitimate and safe for iOS users.

Google's Protection not what it seems

Despite Google's positive findings in their 2018 Year in Review, we continue to see reports of fraudulent or malicious apps discovered on the Google Play Store. In July of this year alone, 205 harmful apps with over 32 million installs were hosted on the official Play Store. In March 2019, a Motherboard investigation found more than 20 Android apps advertised as offering promotions from cell phone providers but instead installing malware to steal data and leave devices vulnerable to additional hacking. Similarly, Trend Micro recently discovered several supposed 'beauty camera' apps redirecting users to pornographic content and phishing websites while also collecting private data from the device. One of the most high profile of these discoveries occurred in 2018 when 12 apps on the Google Play Store designed to look like race-car driving games were discovered being used to install malware with full access to device network traffic. The apps had been downloaded by more than half a million Android users, with two even Trending on the Play Store, before the discovery was made further highlighting the limits of Google's security capabilities from Google Play Protect.

iOS apps misbehaving

Despite its image as a secure and trustworthy source for apps and content, the Apple App Store has also fallen victim to potentially malicious apps evading its vetting standards. In January 2019, researchers discovered more than a dozen iPhone apps covertly communicating with the same command and control server previously used by known Android malware. 'Goldluck' was a strand of mobile malware previously known to infect classic and retro games on the Google Play Store and affecting over 10 million Android users. By embedding backdoor code into the device, Goldluck allowed hackers to access high-level device privileges and run malicious commands like sending premium SMS messages without the victim's knowledge. Last year researchers were surprised to discover 14 iOS 'retro game' apps (that made it through Apple's strict vetting process) communicating with the same server used by the Goldluck malware, a historically Android-focused threat. Although found to be mainly benign, the communications did present some evidence of sending IP address information and user location data back to the server. While the apps themselves were not technically compromised and did not contain any malicious code, the link to this server presented a serious risk for data exposure and highlighted the potential for hackers to gain access to iOS devices via seemingly innocent apps from the App Store.

Circumventing the official app stores altogether

Malware is not just restricted to official app store downloads however. Given that the Google Play and App Store have these security features and content restrictions in place (that, despite their flaws, do present significant obstacles for app developers), a technique to completely circumvent the official stores has been developed. '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.

For Android apps, this is a relatively simple process, done by enabling the download of an app .apk file from an 'unknown source'. Hundreds of unofficial Android apps are readily available for download using this method both online and via third-party marketplaces such as Getjar, Mobogenie and Appbrain.

For iOS the process is a little more complicated but possible nonetheless. Just this year it was discovered that malicious app developers could pose as legitimate businesses to obtain Apple Enterprise App certificates, allowing them to validate and distribute apps independently of the official App Store. Pornography, gambling and fake versions of gaming apps developed under this program have all been discovered available for download to iOS devices and simply require users to 'trust' the app's publisher before installing.

Although not used exclusively by fraudulent apps, many hackers and malicious app developers have used the process of 'sideloading' in order to avoid security checks and regulations. By taking advantage of users' attempts to avoid paying for content or to overcome geographical release restrictions, sideloading provides malicious developers with the perfect vehicle to spread Trojans, spyware, adware, and click fraud malware

Not all malware delivered via apps

Despite all of Google and Apple's best efforts to monitor the content and validity of all their apps, the reality remains that apps are not the only platforms used by malicious actors to deliver malware to mobile devices. Given the amount we now use our mobile devices for communication, it has become increasingly common for channels such as email, SMS, social media sites, and messaging services like WhatsApp to be used to distribute these threats. More and more attackers are preying on the trust we so often put in these services and using them to send links to malicious websites or downloads in the hope that someone will unwittingly click. One of the most high profile instances of malware distribution in recent years was Trident/Pegasus, a targeted spyware attack sent via SMS that exploited three zero-day vulnerabilities causing catastrophic data loss on iOS devices. The attacks allowed hackers to jailbreak devices and gain access to messages, calls, emails, and end-to-end encrypted apps to collect information including passwords and contact lists.

While just two weeks ago it was discovered that a vulnerability in the audio call feature of the hugely popular messaging app WhatsApp could be used to inject Pegasus spyware into a device, regardless of whether the user answered the call or not. Described as "the most sophisticated"

attack ever seen on an endpoint, the discovery of Trident/Pegasus has served as a major wake up call and reminder that any and all platforms have vulnerabilities and that blind trust in companies like Google and Apple may not be enough to protect from them.

Ensuring devices are protected

If we cannot rely on Apple and Google's security features, what can we do to protect ourselves from the threat of mobile malware? Firstly, education and exercising vigilance is key. Mobile device users need to be aware of the potential dangers involved in processes like sideloading, while caution should always be taken when clicking on links or downloads in messages online. Even when we trust the source, we need to be aware of suspicious behavior or any offers that may seem too good to be true.

As humans however, it is inevitable that we may be fooled by cyber threats via seemingly innocent apps or other communications. To ensure protection from all forms of mobile malware, including ransomware, spyware, and Trojans, external security is essential. Dedicated mobile security products, such as Corrata Security and Control, that block access to suspicious sources such as unofficial app stores or malicious sites, and constantly monitor devices for evidence of malware infection are becoming more and more necessary to prevent malware infection and protect our sensitive data. So if your organization is concerned about the security of your data, now is the time to consider upgrading your defenses against mobile malware as well as the other threats we face in a mobile-first world.

Want to find out more about how you can ensure the safety of your mobile devices?
Contact Corrata today