proofpoint™

Why App Stores Cannot Protect Enterprises from Malware and Dangerous Apps

Proofpoint Mobile Defense Team, December 2015

By restricting app distribution to curated app stores, mobile devices are not subjected to the 60 million new malware samples per year that are spammed out through billions of email attachments and malicious URLs that infect PC computers.

However, attackers have adapted to the mobile environment, just as they have adapted to every security defense we have erected in the past two decades.

Enterprises cannot rely on trusting consumer-oriented app stores that do one-time vetting to protect them from attackers. Here are 18 examples of how app stores fail to protect enterprises from malware and dangerous apps, and cannot provide compliance or privacy protection.

1. There are no privacy or security certification standards for publishing apps, either for consumers or enterprises. App stores do not give any indication, certification or warranty of security or compliance.

2. App stores publish millions of consumer apps that are developed by people all around the world, and these apps usually mine and sell user data to make money. These apps may not be appropriate for enterprise or government users, particularly executives or IT personnel with access to critical data or systems. App stores do not make that information available to enterprises or consumers.

3. App stores have a very narrow definition of malware. For example, Google says that malware is app that tries to break the operating system. Apps that root Android devices are not malware if they tell you that this is what they will do.

4. App stores do not enforce apps to have privacy policies, nor are they reviewed. If consumers use apps that do not have privacy policies, that is their choice. This is rarely acceptable in enterprises or government agencies. About half of apps have no privacy policy, meaning that any data they gather is not protected, and many app developers publish fake links to other company privacy policies.

5. App stores vet an app once, when it is submitted. However, malicious app communications can often only be detected months after apps are published. Two recent examples are XcodeGhost and iBackdoor malware for iPhone and iPad that infected thousands of apps available on the App Store in the US and other countries for months, before it was detected. Millions of devices downloaded these apps and are still infected.

6. App stores do not have the real-time global threat data that is needed to continually re-test apps to detect malicious communications or newly identified attacks.

7. Apps stores do not verify that apps use encrypted communications, and do not monitor the data that apps communicate. App stores also do not track which countries and to whom apps send data. Without this information, consumers and enterprises cannot make informed decisions about compliance, security or privacy.

8. App Stores don’t enable enterprises or consumers to validate actual app behavior. App stores do not discern between an app that reads one address book entry to show you a phone number from another app that reads your entire personal and corporate address book and sends it to a malicious server. It may be OK for a consumer to have an app that sends their calendar and address book to a server in China that has no privacy policy and no legal standing in the USA. Such an app is not appropriate for the CEO or sales executive of a public company.

9. App stores do not spend hours, days or weeks to validate the security of an app. While it can take up to 2 weeks for app stores to get around to validating a new app in their queue, they only spend between 1 minute and 11 minutes to verify an app and approve it, once it enters the actual validation process.
10. When app stores remove published apps that are later detected as infected, malicious or dangerous, many users are not notified. These “zombie apps” can pose risks for months or years.
11. App stores do not effectively test the behaviors of apps that use obfuscation tools to defeat code analysis, requiring extensive user simulation for testing.
12. App stores cannot detect malicious behavior that is only triggered after an app is approved and published to the app store.
13. App stores cannot check for company-specific attacks, such as “sleeper cell” apps that do not trigger malicious behavior until a command & control server detects that they are being run from inside a targeted company’s network.
14. Scanning an app when it is submitted to an app store cannot detect zero-day attacks. There are between 30-70 new mobile OS security vulnerabilities discovered each month (hundreds per year). Most are discovered by security researchers and not the OS developers. As mobile OSes add more functionality, there is more scope for vulnerabilities.
15. App stores do not correlate publisher reputation information between Android and iOS and vice versa. Thus an untrusted publisher of apps on one platform can start to publish similar apps on the other without the benefit of a history of prior malicious or dangerous detections.
16. App store vetting does nothing to detect side-loaded apps on Android or enterprise-signed apps on iOS such as YiSpecter and WireLurker, which can be targeted to enterprise users by spear-phishing.
17. There are many legitimate third party Android app stores including Amazon, Samsung and Sony that have varying levels of vetting and controls.
18. App stores do not check if apps copy and steal usernames and passwords from online sites such as Linkedin, Google, Facebook, SalesForce and DropBox. By improperly logging into these sites, hundreds of apps are storing and forwarding authentication credentials to their own servers.

about proofpoint
Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint’s expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

proofpoint™
892 Ross Drive
Sunnyvale, CA 94089
1.408.517.4710
www.proofpoint.com