SOLUTION BRIEF

Safeguarding Against Colluding Mobile Apps

Mobile apps today must have a convenient way to talk to each other. Unfortunately, these useful communication channels can also hide insidious behavior. When two or more apps are analyzed independently, the behavior of a single app can seem completely harmless. But when colluding mobile apps are installed on the same device, they can exchange information and perform malicious acts.

In the *McAfee Labs Threats Report: June 2016,* we take an in-depth look at colluding mobile apps, which are a new method that malicious apps use to make detection difficult. For security, mobile operating systems isolate their apps in sandboxes, restrict their capabilities, and clearly control which permissions they have. However, mobile operating systems also include many ways for these apps to communicate and exchange information with each other across sandbox boundaries.

Looking to evade detection, attackers may try to leverage multiple apps with different capabilities and permissions to achieve their goals. For example, App A has permission to sensitive information while App B has access to the internet. When each app is installed individually, App A can't send that information off the device while App B can't access the sensitive information. Only when installed on the same device can App A send the sensitive information to App B, which sends the information to an external destination.

Colluding mobile apps allow the apps to avoid detection as they perform malicious behaviors such as:

- **Information theft:** When an app with access to sensitive or confidential information collaborates (willingly or unwillingly) with one or more other apps to send information outside the boundaries of the device.
- **Financial theft:** When an app sends information to another app that is capable of financial transactions or financial API calls.
- **Service misuse:** When one app can control a system service and receive information or commands from one or more other apps.
- **Elevation of privilege:** When one app provides its higher privileges to other apps to collect sensitive data or perform harmful actions.

Safeguarding Against Colluding Mobile Apps

McAfee recommends several good practices to protect against colluding mobile apps:

- **Use apps from trusted app stores and publishers** because authorized sources routinely perform malware scans on their listed apps.
- **Disable the ability to install apps from "unknown sources"** to prevent installation of apps that have not been authorized.
- **Avoid using software with embedded advertising** because excessive ads may indicate the presence of multiple ad libraries, which increase the possibility of collusion.
- **Research the ratings and reviews of an app before installing it** to see if other users have had security issues with the app.
- **Don't "jailbreak" or "root" the device** as that allows for apps to gain system-level access and possibly install malicious software.
- **Deploy a mobile management solution** as a mechanism to control the apps that users can install.

How McAfee Can Help Protect Against Colluding Mobile Apps

McAfee® Mobile Security for Android

When you download new apps, browse the internet, or even bank online, McAfee Mobile Security for Android protects your mobile device from threats. McAfee Mobile Security for Android uses intelligence provided by McAfee Labs threat researchers to identify malicious apps, including colluding mobile apps, and stops them from running on your mobile device. With McAfee Mobile Security for Android, your mobile device is protected and can use any app or combination of apps with confidence.

McAfee Mobile Security for Android provides the following features:

- Uses Real-time Scan to automatically scan emails, text messages, attachments, and files for malicious content.
- Performs scheduled full scans using the Smart Scheduler.
- Enables automatic updates to ensure that the latest intelligence from threat researchers is protecting you from all types of threats, including colluding mobile apps.
- Automatically reports and alerts if an app performs a privacy violation, and allows you to uninstall unsafe apps.
- Blocks risky websites that may contain malicious threats.

Further Reading

Towards Automated Android App Collusion Detection, a research report developed jointly between McAfee Labs and researchers from several UK universities.

Colluding Apps: Tomorrow's Mobile Malware Threat, an article from IEEE Security & Privacy magazine.

Analysis of the Communication Between Colluding Applications on Modern Smartphones, Proceedings of the 28th Annual Computer Security Applications Conference.

A Survey on Application Collusion Attacks on Android Permission-Mechanism, International Journal for Scientific Research & Development.

Towards a Systematic Study of the Covert Channel Attacks in Smartphones, International Conference on Security and Privacy in Communication Networks.

Automatic Detection of Inter-Application Permission Leaks in Android Applications, IBM Journal of Research and Development.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com