Kurzvorstellung

Absicherung gegen konspirative Mobilgeräte-Apps

Mobilgeräte-Apps benötigen heutzutage eine bequeme Möglichkeit, um untereinander kommunizieren zu können. Leider können diese nützlichen Kommunikationskanäle aber auch dazu genutzt werden, heimtückisches Verhalten zu verbergen. Wenn zwei oder mehr Apps voneinander getrennt analysiert werden, scheinen die einzelnen Apps vielleicht vollkommen harmlos zu sein. Doch wenn konspirative Mobilgeräte-Apps auf demselben Gerät installiert werden, können sie Informationen austauschen und böswillige Aktivitäten durchführen.

Im *McAfee Labs Threat-Report vom Juni 2016* werfen wir einen genauen Blick auf konspirative Mobilgeräte-Apps, die einen neuen Ansatz verwenden, um der Erkennung zu entgehen. Aus Sicherheitsgründen isolieren Mobilgeräte-Betriebssysteme ihre Apps in Sandboxes und kontrollieren strikt die Fähigkeiten sowie die zulässigen Berechtigungen. In den Mobilgeräte-Betriebssystemen ist jedoch auch dokumentiert, wie Apps über Sandbox-Grenzen hinweg miteinander kommunizieren und Informationen austauschen können.

Beim Versuch, der Erkennung zu entgehen, können Angreifer mehrere Apps mit unterschiedlichen Funktionen und Berechtigungen nutzen, um dennoch ihre Ziele zu erreichen. Beispiel: App A kann sensible Informationen abrufen und App B auf das Internet zugreifen. Wenn die Apps einzeln installiert werden, kann App A keine Daten aus dem Gerät herausleiten und App B hat keinen Zugriff auf sensible Informationen. Doch wenn beide Apps auf demselben Gerät installiert sind, kann App A sensible Informationen an App B senden, die diese Informationen an ein externes Ziel weiterleitet.

Konspirative Mobilgeräte-Apps verbergen zum Beispiel folgendes böswilliges Verhalten:

- **Informationsdiebstahl:** Eine App mit Zugriff auf sensible oder vertrauliche Informationen arbeitet (absichtlich oder unabsichtlich) mit einer oder mehreren anderen Apps zusammen, die diese Informationen über die Grenzen des Geräts hinaus sendet.
- **Finanzdiebstahl:** Eine App sendet Informationen an eine andere App, die Finanztransaktionen oder kostenpflichtige API-Aufrufe durchführen kann.
- **Dienstmissbrauch:** Eine App kann einen Systemdienst kontrollieren und erhält Informationen oder Befehle von einer oder mehreren anderen Apps.
- **Erhöhung von Berechtigungen:** Eine App mit höheren Berechtigungen kann anderen Apps die gleichen Berechtigungen verleihen und damit Zugriff auf sensible Daten oder schädliche Aktionen ermöglichen.

intel Security

Absicherung gegen konspirative Mobilgeräte-Apps

Intel® Security empfiehlt verschiedene Vorgehensweisen zum Schutz vor konspirativen Mobilgeräte-Apps:

- **Verwenden Sie nur Apps von vertrauenswürdigen App-Stores und Anbietern**, da autorisierte Quellen die gelisteten Apps routinemäßig auf Malware prüfen.
- **Legen Sie fest, dass keine Apps aus „unbekannten Quellen" installiert werden dürfen**, um die Installation nicht-autorisierter Apps zu verhindern.
- **Vermeiden Sie Software mit eingebetteter Werbung**, da eine hohe Anzahl an Werbeeinblendungen auf das Vorhandensein mehrerer Werbebibliotheken hinweist und damit die Möglichkeit konspirativer Funktionen steigt.
- **Lesen Sie die Bewertungen einer App vor der Installation**, um zu erfahren, ob andere Benutzer dieser App bereits Sicherheitsprobleme hatten.
- **Verzichten Sie darauf, das Gerät einem Jailbreak zu unterziehen oder zu rooten**, da Apps dadurch Zugriff auf Systemebene erhalten und böswillige Software installieren können.
- **Verwenden Sie eine Mobilgeräte-Verwaltungslösung**, um zu kontrollieren, welche Apps von Benutzern installiert werden können.

So kann Intel Security vor konspirativen Mobilgeräte-Apps schützen

McAfee® Mobile Security for Android

Wenn Sie neue Apps herunterladen, im Internet surfen oder Online-Bankgeschäfte erledigen, schützt McAfee Mobile Security for Android Ihr Mobilgerät vor Bedrohungen. McAfee Mobile Security for Android verwendet die von den McAfee Labs-Bedrohungsforschern bereitgestellten Daten, um böswillige Apps (einschließlich konspirative Mobilgeräte-Apps) zu erkennen und deren Ausführung auf Ihrem Mobilgerät zu blockieren. Mit McAfee Mobile Security for Android ist Ihr Mobilgerät geschützt, sodass Sie gefahrlos alle Apps oder App-Kombinationen verwenden können.

McAfee Mobile Security for Android bietet folgende Funktionen:

- Nutzt Echtzeit-Scans zur automatischen Prüfung von E-Mails, Textnachrichten, Anhängen und Dateien auf böswillige Inhalte.
- Führt mit Smart Scheduler geplante sowie vollständige Scans durch.
- Aktiviert automatische Aktualisierungen, um zu gewährleisten, dass die aktuellsten Daten von Bedrohungsforschern verwendet werden und Sie so vor allen Bedrohungen (einschließlich konspirativen Mobilgeräte-Apps) geschützt sind.
- Meldet und warnt Sie, wenn eine App die Privatsphäre verletzt, und gibt Ihnen die Möglichkeit, unsichere Apps zu deinstallieren.
- Blockiert riskante Webseiten, die Bedrohungen enthalten können.

Weitere Informationen

Towards Automated Android App Collusion Detection (Automatische Erkennung konspirativer Android-Apps), ein gemeinsamer Forschungsbericht von McAfee Labs und Forschern mehrerer britischer Universitäten.

Colluding Apps: Tomorrow's Mobile Malware Threat (Konspirative Apps: Die Mobilgeräte-Malware-Bedrohungen von morgen), ein Artikel der Zeitschrift IEEE Security & Privacy.

Analysis of the Communication Between Colluding Applications on Modern Smartphones (Analyse der Kommunikation zwischen konspirativen Apps auf modernen Smartphones), Berichte zur 28. Jahreskonferenz zu Computersicherheitsanwendungen.

A Survey on Application Collusion Attacks on Android Permission-Mechanism (Umfrage zu Angriffen mit konspirativen Apps und dem Android-Berechtigungsmechanismus), International Journal for Scientific Research & Development.

Towards a Systematic Study of the Covert Channel Attacks in Smartphones (Systematische Untersuchung heimlicher Channel-Angriffe auf Smartphones), International Conference on Security and Privacy in Communication Networks.

Automatic Detection of Inter-Application Permission Leaks in Android Applications (Automatische Erkennung von Inter-App-Berechtigungslecks in Android-Apps), IBM Journal of Research and Development.

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com