ソリューション概要

共謀するモバイル アプリを阻止する

モバイルアプリは便利な通信手段となっています。しかし、この通信チャネルを悪用した狡猾な攻撃が発生しています。個別に分析したときには不審な動作もなく、無害に見えるアプリでも、同じ端末にインストールされた他のアプリと連携し、情報を交換したり、不正な行為を実行する場合があります。

共謀するモバイル アプリについては、『McAfee Labs 脅威レポート: 2016年6月』で詳しく分析していますが、この手法は検出を困難にする新しい手段として不正なアプリで使用されています。セキュリティ上の理由から、モバイル オペレーティング システムはアプリをサンドボックスに隔離して機能を制限し、アプリに付与する権限を厳格に制御しています。しかし、モバイル オペレーティング システムには、サンドボックスの境界を越えてアプリ間で通信を行い、情報を交換する手段が用意されています。

検出を回避するため、攻撃者は機能と権限の異なる複数のアプリを利用し、目的を達成しようとしています。たとえば、アプリAには重要な情報に対するアクセスが許可され、アプリBにはインターネット接続が許可されているとします。それぞれのアプリが別々にインストールされている場合、アプリAはデバイスの情報を外部に送信できず、アプリBは重要な情報にアクセスできません。しかし、同じ端末にインストールされると、アプリAからアプリBに重要な情報が送信され、この情報がアプリB経由で外部に流出する可能性があります。

モバイル アプリの共謀で検出が回避されると、次のような不正行為が実行される可能性があります。

- **情報の窃盗**: 意図的かどうかに関わらず、重要な情報や機密情報にアクセスできるアプリが他のアプリと連携し、情報を端末の外部に送信する可能性があります。
- **金銭的な詐欺行為**: 金融取引を行うアプリやAPIに別のアプリが情報を送信する可能性があります。
- **サービスの誤使用**: アプリがシステム サービスを制御し、別のアプリから情報やコマンドを受信する可能性があります。
- **特権の昇格**: アプリが別のアプリに上位の特権を付与し、重要なデータを収集したり、有害な行為を行う可能性があります。

intel Security

共謀するモバイルアプリを阻止する

共謀するモバイル アプリの攻撃を阻止するため、次のような対策を実施しましょう。

- **信頼できるアプリストアまたはパブリッシャーからアプリを入手する。**承認された提供元は、公開しているアプリを定期的にスキャンし、マルウェアの有無を検査しています。
- **「提供元不明」のアプリをインストールできないようにする。**承認されていないアプリのインストールを防ぎましょう。
- **広告が埋め込まれたソフトウェアを使用しない。**広告が過度に表示される場合、複数の広告ライブラリが存在する可能性があります。この場合、アプリが共謀するリスクが高まります。
- **インストールの前にアプリの評価とレビューを確認する。**他のユーザーがセキュリティ問題を報告していないかどうか確認しましょう。
- **端末のジェイルブレイクやルート化を行わない。**アプリがシステム レベルのアクセス権を取得し、不正なソフトウェアがインストールされる可能性があります。
- **モバイル管理ソリューションを配備する。**ユーザーにインストールを許可するアプリを管理しましょう。

共謀するモバイル アプリを阻止するIntel Securityのソリューション

McAfee® Mobile Security for Android

新しいアプリのダウンロード、インターネットの閲覧、オンライン バンキングを行うときに、McAfee Mobile Security for Androidがモバイル端末を保護します。McAfee Mobile Security for Androidは、McAfee Labsの脅威研究者が提供する情報により、共謀するモバイル アプリを含む不正なアプリを特定し、モバイル端末での実行を阻止します。McAfee Mobile Security for Androidを使用すると、モバイル端末を保護し、単独または複数のアプリを安全に利用できます。

McAfee Mobile Security for Androidは次の機能を提供します。

- リアルタイム スキャンにより、メール、SMS、添付ファイル、ファイルを自動的にスキャンし、不正なコンテンツの存在を検査します。
- Smart Schedulerでスケジュールを設定し、フルスキャンを実行できます。
- 自動更新により、脅威研究者が提供する最新の情報を取得し、共謀するモバイル アプリを含む様々な脅威から保護します。
- アプリがプライバシーに違反すると自動的に報告・警告を行い、安全でないアプリを削除できるようにします。
- 脅威が存在する可能性のある危険なサイトをブロックします。

詳細情報

Towards Automated Android App Collusion Detection（共謀するAndroidアプリの自動検出）、McAfee Labsと英国の複数の大学が共同で実施した調査の報告書

Colluding Apps: Tomorrow's Mobile Malware Threat（共謀するアプリ: 新しいモバイル マルウェアの脅威）、『IEEE Security & Privacy』に掲載された記事

Analysis of the Communication Between Colluding Applications on Modern Smartphones（共謀するアプリがスマートフォン上で行う通信方法の分析）、第28回ACSAC（Annual Computer Security Applications Conference）の論文集

A Survey on Application Collusion Attacks on Android Permission-Mechanism（アプリの共謀によるAndroid権限に対する攻撃の調査）、International Journal for Scientific Research & Development

Towards a Systematic Study of the Covert Channel Attacks in Smartphones（スマートフォンの通信チャネルに対する攻撃の体系的な研究）、SecureComm（ネットワーク セキュリティに関する年次国際会議）

Automatic Detection of Inter-Application Permission Leaks in Android Applications（Androidアプリ間での権限リークの自動検出）、IBM Journal of Research and Development

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒150-0043 東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店　〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810-0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com