ActiveSyncに頼ったデバイスを攻撃するモバイルマルウェア

モバイルプラットフォームは、長年、PCセキュリティをすり抜けてきましたが、世界中でモバイルデバイスが普及するにつれ、モバイルプラットフォームに対するセキュリティ脅威は増大する一方です。モバイルデバイスはPCより安全と言っても、ハッカーはモバイルOSを悪用し、価値あるデータにアクセスする新しい方法を執拗に模索しています。現在、4つの大きな脅威が、非常に巧妙な方法でiOSとAndroidデバイスを狙っています。ユーザーは、データが盗まれるまで、自分のデバイスが攻撃を受けていることに気づかないかもしれません。

MobileIron

MKT-9585 V1.2

ActiveSyncだけでメールを使用する企業は、特にこれらの脅威に脆弱です。ActiveSyncのMDM機能が限られているためです。ActiveSyncのMDM機能の多くは古いWindows OSにのみ対応し、iOSやAndroidではまったく動作しないものもあります。[1] Stagefright、Keyraider、XcodeGhost、YiSpecterなどのモバイルマルウェアの脅威に対抗できるのは、MobileIronのようなエンタープライズモビリティ管理（EMM）プロバイダーだけです。

Stagefright、Keyraider、XcodeGhost、YiSpecterなどのモバイルマルウェアから企業のアプリとデータを保護できるのは、MobileIronのようなEMMプロバイダーだけです。

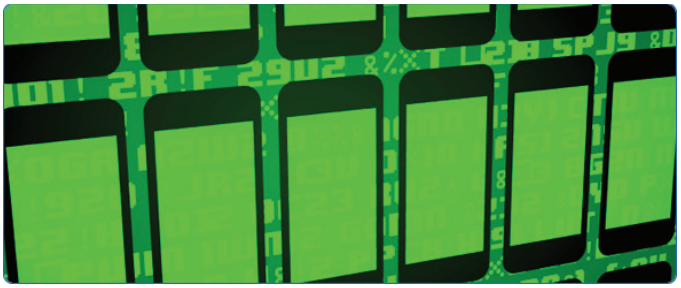
Stagefrightの攻撃対象はAndroidデバイスの99%

- **仕組み：**Stagefrightは、Androidメディアライブラリの脆弱性を悪用します。攻撃者はまず、悪意のあるマルチメディアメッセージをMMSで送信します。脆弱性のあるAndroidデバイスがメッセージを受信すると、マルチメディアプレビュー機能を通じて自動的にマルウェアがダウンロードされ、感染します。注意すべきは、リンクのクリックやアプリのダウンロードなど、ユーザーが何もしなくても、悪意のあるコードが電話に入り込むことです。MMSを受信するとすぐに感染します。
- **企業に与える影響：**Stagefrightは、データの窃盗、マイクの乗っ取り、カメラの使用などを通じて、感染デバイス上でスパイウェアと同様に作用するため、企業は十分に警戒する必要があります。

XcodeGhostが何千もの感染アプリでiOSデバイスを攻撃

- **仕組み：**XcodeGhostは、Apple App Storeに侵入した感染アプリを通じて、ジェイルブレイクしたデバイスもジェイルブレイクしていないデバイスも攻撃します。アプリは、iOS（およびOS X）開発者が、Appleの公式ダウンロードサイト以外の悪意あるサイトからAppleのXcode SDKをダウンロードすることによって、意図せずにXcodeGhostに感染します。開発者は、このようにセキュリティの低下したXcodeを使用してアプリを開発することで、知らないうちにアプリにマルウェアを隠しています。これまでに4,000以上のXcodeGhostアプリがMobileIronのパートナーであるFireEyeによって特定され、AppleによってApp Storeから削除されました。
- **企業に与える影響：**従業員がXcodeGhostに感染したアプリを個人所有または会社所有のモバイルデバイスにダウンロードすると、ビジネスデータが深刻なリスクにさらされます。マルウェアがリモートコマンド＆コントロール（CnC）を通じて、デバイス上でのWebページ表示、偽のパスワードプロンプト表示、認証情報の窃盗を可能にします。

[1] *Beehler, Eric。"Using Microsoft Exchange ActiveSync for MDM: What you can and can't do.（MDMにMicrosoft Exchange ActiveSyncを利用する：できることとできないこと）" http://searchmobilecomputing.techtarget.com/tip/Using-Microsoft-Exchange-ActiveSync-for-MDM-What-you-can-and-cant-do*



Keyraiderが225,000以上のAppleアカウントからデータを窃盗

- **仕組み：**KeyRaiderは、ジェイルブレイクによってオペレーティングシステムの内蔵セキュリティ機能の多くが失われたデバイスをターゲットとします。そしてユーザー名、パスワード、証明書、プライベートキーなどを盗み取ります。
- **企業に与える影響：**企業は、ジェイルブレイクしたモバイルデバイスから会社情報へのアクセスを特に念を入れてブロックする必要があります。Keyraiderのようなマルウェアは、iPhoneやiPadを制御し、会社のメール、文書、その他のデータにすぐにアクセスします。

YiSpecterが密かにデバイス上のユーザーデータを取得

- **仕組み：**YiSpecterは、非公開またはApple iOS APIでサポートされていないプライベートAPIを使用し、ジェイルブレイクしたデバイスにもジェイルブレイクしていないデバイスにも感染します。これらのAPIを使用するアプリは通常、Appleのアプリ検査プロセスでブロックされますが、YiSpecterは他にも3つの経路で広がります。すなわち、ISP、ペアリング中にデバイスに感染するWindows上のワーム、そしてオフラインのアプリインストールです。
- **企業に与える影響：**YiSpecterは、iOSデバイスに感染すると、ユーザーの許可なくiOSアプリを変更、インストール、起動できます。また、ダウンロードしたアプリで既存アプリを上書きする、ユーザーが通常のアプリを起動しようとするとフルスクリーン広告を表示する、Safariのデフォルト検索エンジンを変更する、Webページをブックマークして開く、デバイス情報をCnCサーバーにアップロードするなども可能です。このマルウェアは、削除しても自動的に再出現します。[2]

[2] *Xiao, Claud。“YiSpecter: First iOS Malware that Attacks Non-jailbroken Devices by Abusing Private APIs.（YiSpecter：プライベートAPIの悪用によってジェイルブレイクしていないデバイスを攻撃する初のiOSマルウェア）” 2015年10月4日。http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/*

MobileIronでモバイルデバイスをマルウェアから保護

ActiveSyncは、モバイルデバイスで簡単にメールを利用できる便利な機能ですが、iOSとAndroidに対するモバイルマルウェア攻撃に企業をさらすことになります。MobileIronは、すべてのマネージドデバイスをこのような脅威から守るセキュリティを提供します。

モバイルアイアンが脅威を検出/緩和

MobileIronは、まずデバイスのポスチャー、すなわちセキュリティ状態を判断することにより、このような脅威の多くを排除します。ポスチャーチェックでは、デバイスがジェイルブレイクされていないこと、デバイスとユーザーの両方がネットワークへのアクセスを許可されていること、デバイスが承認されたアプリとOSバージョンを使用していることを確認します。セキュリティポスチャーの条件を満たしているデバイスのみが、そのデバイスで、またはネットワークを通じて会社の情報にアクセスできます。

デバイス上にマルウェアを検出すると、MobileIronは自動的にコンプライアンスアクションを実行し、デバイスの検疫、社内データの削除、そのデバイスから社内データへのアクセス防止を実行します。

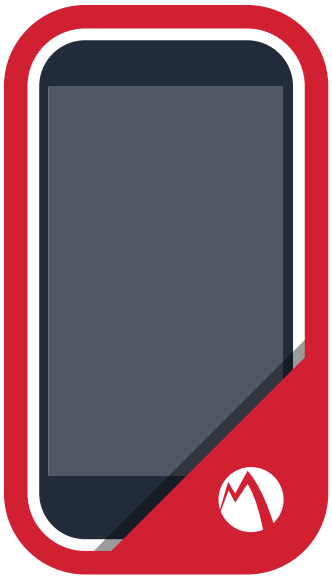
MobileIronでセキュリティを確保：

- OSバージョンの識別
- ジェイルブレイク/ルート検出
- アプリバージョンの検出
- 非マネージドアプリによるアクセスをブロック
- 条件付きデバイスアクセス（ネットワークアクセスをブロック）
- コンプライアンスアクション/デバイス検疫
- ビジネスアプリ/データのセレクティブワイプ
- 脅威通知の検出とアラート

モバイルデバイスのセキュリティを今すぐ改善する2つの方法

個人所有または会社所有を問わず、従業員が使用するすべてのデバイスのセキュリティをActiveSyncだけでなくMobileIronでも確保します。

ActiveSyncトラフィックがMobileIron Sentryを通じてのみ流れるよう構成し、セキュアでない、または感染したデバイスが社内データにアクセスするのを防ぎます。



モバイルの脅威：	MobileIronによる脅威の緩和：
Stagefright： 感染したMMSダウンロードを通じてAndroidデバイスをターゲットとします。	専用に暗号化したAndroidコンテナで会社のメール、アプリ、データのセキュリティを確保します。
Keyraider： ジェイルブレイクしたデバイスから機密データを盗みます。	会社からジェイルブレイクしたデバイスへのアクセスを検出し、拒否します。
YiSpecter： ユーザーの許可なくiOSアプリを変更、インストール、起動できます。	バージョン8.4より前のiOSを実行するデバイスを特定し、検疫します。

MobileIronとエコシステムパートナー：

XcodeGhost： 感染したApp Storeアプリを通じてiOSデバイスをターゲットとします。	FireEyeやLookoutなどのエコシステムパートナーと協力して感染したアプリを特定し、それを実行するデバイスを検疫します。

このような脅威の詳細とMobileIronが御社のモバイルデバイスに提供するセキュリティと保護については、MobileIron（globalsales@mobileiron.com）までお問い合わせください。

MobileIron