IBM Security
Thought Leadership White Paper

モバイルは泥棒達の新しい遊び場

モバイル・マルウェアからの保護方法

IBM

モバイルが広がると、脅威も広がる

はじめに

モビリティは、スマート・デバイスの継続的な増加、モバイル・アプリ開発の爆発的増加、作業ファイルへのアクセスの増加により、比類ない速さで企業を変革しています。企業は BYOD (個人所有機器の持ち込み可) ポリシーを採用し、仕事関連の活動で私用アプリの利用も許可することで、実質的にいつでもどこからでも仕事ができるように従業員に便宜を図っています。

ただし、企業は、機密情報の保護に必要なエンタープライズ級のセキュリティーを導入してこなかったので、このモビリティの爆発的成長に追いついていません。ハッカーと泥棒達はこの機会を利用して、ネットワークに侵入し、モバイル・エンドポイントから機密業務データを入手しています。IT とセキュリティーのリーダーがこれらのモバイルへの脅威を先見的に検出、分析、修復するには、最新の堅牢なセキュリティー・ソリューションが必要です。

推定 1600 万台のモバイル機器がいつの間にかマルウェアに感染しています。

企業におけるモバイルの爆発的増加

モビリティの成長に関わる数字は大きく膨れ上がっています。2014 年には、携帯電話数 (73 億台) は地球上の人口 (70 億人) を超えるだろうと予測されていました。[1]

Arxan Technologies によると、2014 年には、1,380 億のモバイル・アプリがダウンロードされており、2017 年には 2,680 億に倍増するだろうと見込まれています。[2]

消費者はスマート・デバイスとアプリを私用目的で取り入れて、このモバイルの動きを最初に促進しました。職場における BYOD の傾向は広がり続け、企業による人員全体の動員、購入費とサポート・コストの節約を助けています。実際、Gartner によると、2017 年には従業員の半数が BYOD を要求するでしょう。[3]

モバイル・アプリは新しい効率的なワークフローを従業員のために作り出しています。業務データ、電子メール、コンテンツへのシームレスなアクセスも増え続け、その結果、生産性が高まっています。企業は、各ビジネス・プロセスでモバイル・ファーストを取り入れて、社内のモビリティの成長をさらに広げることを検討し始めています。

モバイル・アプリが攻撃されたとき

ただし、ハッカーと泥棒達は、企業の変革で達成されるこれらの大きな進歩を台無しにしようとしています。モバイル機器への感染は急増し続け、2013 年には 20 パーセントだったのが、2014 年には 25 パーセントに増えています。推定 1,600 万台のモバイル機器がいつのまにかマルウェアに感染しています。[4]

モバイル・マルウェアは悪意のあるソフトウェアで、特にモバイル機器を攻撃するように設計されており、特定の OS の弱点に依存しています。

データ侵害の影響は非常に高くつくことがあり、会社のブランドへのダメージに加え、財務的なロスも生じる可能性があります。Ponemon Institute の見積もりによると、2014 年では 1 つのセキュリティー侵害で生じるコストは 350 万ドルでした。これは前年比 15 パーセントの増加です。[5]

図 1: ハッキングされた売り上げトップの Android と iOS のアプリ

悪意のあるモバイル・アプリから感染したデバイスは通常、実質的にすべての企業にとって最大のリスク源になります。Arxan Technologies によると、ユーザーが危険なネットワークに接続したり、リスクの高いアプリを信頼できないソースからインストールしたりすると、モバイル機器はマルウェアに対して無防備になります。売上トップの Android アプリと iOS アプリのそれぞれ 97 パーセントと 87 パーセントがハッキングされており、サードパーティ製アプリ・ストアで販売されています。[6]

Ponemon Institute の別の調査で判明した所見によると[7]、信頼できる企業のアプリや従来のアプリ・ストアで入手できるアプリでさえ、大きなリスクをはらんでいる可能性があります。回答者の 82 パーセントは、職場のモバイル・アプリによってセキュリティー・リスクが非常に大きく (50 パーセント) または大きく (32 パーセント) になったと言っています。ほとんどの従業員が「アプリのヘビー・ユーザー」(66 パーセント) であるにもかかわらず、半数以上 (55 パーセント) が、職場で許されるモバイル・アプリの使用方法を定義するポリシーが会社にはないと答えています。

回答者の大半 (67 パーセント) が、アプリ・ストアを設けていても、従業員は他のソースの未検証のモバイル・アプリを使うことができると認めていますが、回答者の 30 パーセントだけが、エンタープライズ・アプリ・ストアを導入していると答えています。さらに、企業の 55 パーセントが、エンタープライズ・アプリ・ストアから業務アプリを個人用デバイスにダウンロードして使うことを従業員に許可していると答えています。

モバイル・マルウェアの現状

モバイル・マルウェアとは

モバイル・マルウェアは悪意のあるソフトウェアで、特にモバイル機器を攻撃するように設計されており、特定の OS の弱点に依存しています。悪意のあるプログラムの 共通のタイプ 3 つを以下に紹介します。

- スパイウェア – ある種のデータを取得して、利益のためにハッカーに提供するデバイス・データ泥棒
- トロイの木馬 – ユーザーの知らぬ間にデバイスやアプリの機能に影響し、自動トランザクションを実行し、通信を開始するマルウェア
- 脱獄またはルート化マルウェア – 特定のデバイスの管理権限とファイルアクセス権をハッカーに提供

脅威について知り、モバイル・エンドポイントに集中している理由を理解するため、サイバー犯罪者の思考プロセスを見てみましょう。モバイル機器は、機密データに至る最も簡単な道の 1 つです。企業のバックエンド・システムがファイアウォール、侵入防止システム、アンチウイルス・ゲートウェイによって十分保護されている一方で、会社所有デバイスまたは個人所有デバイスのいずれも同じレベルの保護を採用していないことがほとんどです。個人所有デバイス (BYOD) は境界の外側にあり、通常、企業の管理外になっているため、特に無防備です。

ハッカーがエンドポイントを攻撃する場合、マルウェアを使ってユーザーになりすまし、個人を特定できる情報 (PII) と認証情報を取得します。次に、ユーザーのアカウントを乗っ取って、認証されたセッションを使ってプライベート・データを収集し、不正取引を行います。

不安だらけの Android

Android は 81.2 パーセントのシェアで市場を席巻し、IDC によると、2014 年に出荷されたデバイスは 10 億台以上です。[8] 現在、コンシューマー市場を支配していますが、企業での採用はよくいっても低調でした。

Android が今日のモバイル業界でマルウェアの感染に対して最も無防備なモバイルの 1 つである理由は、プラットフォームとアプリ・エコシステムの基本設計とオープン性にあります。

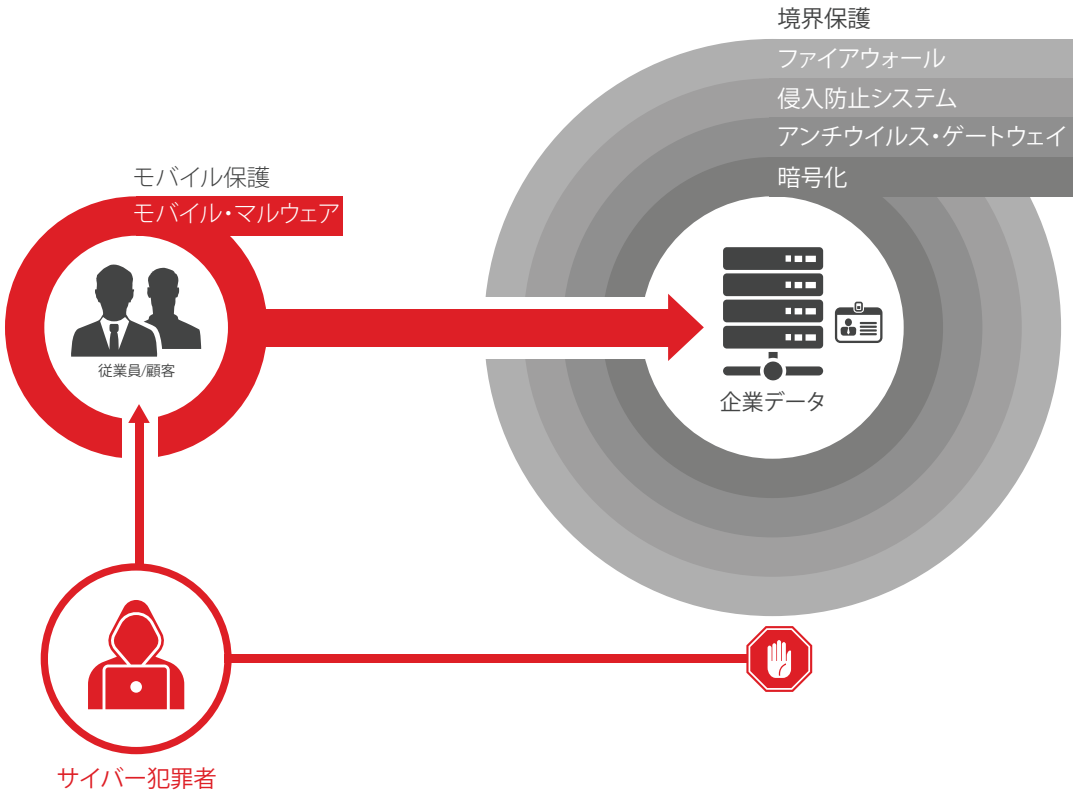

*図 2:*犯罪者は最も弱いリンクを攻撃して、機密データにアクセスする

Android が今日のモバイル業界でマルウェアの感染に対して最も無防備なモバイルの 1 つである理由は、プラットフォームとアプリ・エコシステムの基本設計とオープン性にあります。Android がハッカーと泥棒にとって最も簡単なターゲットの 1 つになっているのは、次の特性が原因です。

- Android アプリはサードパーティ・アプリ・ストアや Web サイトからダウンロード、インストールできる。
- Apple は各 iOSアプリを厳しくチェックし、承認してから iTunes に公開しているが、Google Play Store ではそのような体制をとっていない。
- Android アプリに署名するデジタル証明書が管理されていない。これらのアプリは通常、自己署名されており、アプリ開発者をたどることができない。そのため、Android アプリをハッキングして、マルウェアを注入し、署名を書きかえることが簡単にできる。

サイバー犯罪者は、PC の OS プラットフォームとは異なるモバイル OS プラットフォーム上の脆弱性を攻撃するための、創造性に満ちた新しい方法を常に研究しています。

Google は Google Play Store から悪意のあるアプリを駆逐するために、セキュリティー・プラクティスを実装しました。ストアにアプリがアップロードされるとスキャンを実行し、マルウェア、スパイウェア、トロイの木馬を検出して削除しています。新しいマルウェアを見つけた場合は、Google Play Store のすべてを過去にさかのぼって検証し、怪しいファイルをストアから削除することができます。また、Google の利用規約とコンテンツ・ポリシーに違反した開発者のアプリとアカウントは無効化されます。

ただし、前述したように、売上トップの Android アプリの 97 パーセントがハッキングされており、サードパーティ・アプリ・ストアや Web サイトで見つけることができます。したがって、従業員 (またはその子供) が非公式ソースの 1 つから最新の無料プレミアム・ゲーム・アプリを会社所有または個人所有の Android デバイスにダウンロードしてインストールした場合、そのデバイスはマルウェアに感染したと見なしていいでしょう。会社は、ポリシーとユーザー研修を制定して、このような習慣を防止することはできますが、Android デバイスは自動保護レイヤーがないと無防備になることがあります。

Android マルウェアの例には、SVPENG という銀行系トロイの木馬がありますが、ロシアと欧州の金融機関をターゲットにしているのが発見されました。SVPENG は、モバイル・マルウェアが大きく進化した代表例です。この攻撃では、銀行アプリ・ユーザーを直接ターゲットにします。オーバーレイ攻撃という一般的な PC マルウェア手法を使い、被害者をだまして認証情報を提供させます。

この攻撃の場合、感染デバイスのマルウェアはユーザーが銀行のモバイル・アプリを開くのを待ちます。モバイル銀行アプリ・セッションが開始したことを特定すると、アプリの上に銀行のアプリの外観を真似た画面を表示します (「オーバーレイ」という語はここからつきました)。しかし、このページは実際には偽装ページです。ユーザーはそれが本当の銀行のページだと思って、何も疑わずにマルウェア生成ページで操作を実行し、銀行の認証情報を入力します。

オーバーレイ攻撃は同様に、企業の機密データにも脅威をもたらすことがあります。従業員が何も知らずに業務用の認証情報を入力すれば、泥棒はその情報を入手して、企業システムに入り、データに大損害を与えることができます。

IBM X-Force® Application Security Research Team は最近、Dropbox SDK for Android の脆弱性を発見しました。被害者が知らないうちに、または被害者が認証しなくても、攻撃者はこの脆弱性を使って、攻撃者がコントロールしている Dropbox アカウントにモバイル機器のアプリを接続することができます。[9] この脆弱性は DroppedIn と呼ばれ、ユーザーのデバイスにインストールされた悪意のあるアプリを使う方法、または Web サイトからドライブバイ手法をリモートで使う方法の二通りやり方で突破することができます。

これは、Dropbox SDK バージョン 1.5.4 ～ 1.6.1 を使った、Android アプリ内の認証メカニズムの重大な不具合です。ただし、IBM Security Team が Dropbox の問題を公表してからわずか 4 日以内に、Dropbox SDK for Android v1.6.2 の不具合は解決されました。DroppedIn の脆弱性の概要は、SecurityIntelligence.com のブログ投稿 (脚注 9 を参照) にあります。

ハッカーが DroppedIn の脆弱性を利用できたのは、悪意のあるアプリを Android デバイスに簡単にインストールできたからです。サイバー犯罪者は、PC の OS プラットフォームとは異なるモバイル OS プラットフォーム上の脆弱性を攻撃するための、創造性に満ちた新しい方法を常に研究しています。

Android が企業で採用可能になるまでには、これからも数々の課題に直面するかもしれませんが、Google と機器メーカーによる最新のセキュリティー機能の進展、先進的な Enterprise Mobility Management (EMM) ソリューション・プロバイダーのサポートによって、企業と政府機関での採用が後押しされています。コンシューマー (従って、従業員) が Android デバイスを使用することを選択した場合、会社はモバイル・マルウェアの防止に必要なセキュリティーと保護を実現する必要があります。

iOS は脆弱ではない

iOS デバイスは複数の主な理由により、エンタープライズ市場を席巻してきました。iPhone が 2007 年に初登場すると、プロフェッショナルたちは会社提供の古いスマートフォンの代わりに、個人の iPhones を仕事に使い始めました。iOS アプリのサンドボックス化したアーキテクチャーと動作のおかげで、プラットフォームには設計時からセキュリティーが組み込まれるため、ユーザーが意図的にセキュリティー・システムをバイパスしない限り、ハッカーがデバイス全体、複数のアプリに感染させることは困難です。

最初コンシューマー市場だけに目を向けていた Apple は、エンタープライズ市場の可能性にすぐに気付きました。Mobile Device Management (MDM) ソリューション・プロバイダーの助けを借りて、IT リーダーがデバイス、アプリ、データをより確実に保護、管理できるコントロールを組み込み始めたのです。

Android のオープン・アプリ・アーキテクチャーとは違って、Apple のデバイス/アプリ環境ははるかに閉ざされた傾向にあります。iOS デバイスが脱獄されていない限り、パブリック iOS アプリは、iTunes App Store からしかダウンロードしてインストールすることはできません。iTunes にアップロードされたアプリは、厳しい検証プロセスを経てから Apple によって正式に公開されます。さらに、iOS アプリの署名にはデジタル証明書が必要なため、アプリ開発者をたどることができます。

これらの理由のため、iPhones と iPad は企業、政府機関、教育機関の間で長年にわたって人気があり、受け入れられてきました。ただし、これほど豊富なセキュリティー対策が講じられていても、iOS デバイスをハッキングしようとする試みはストップしていません。事実、WireLurker や Masque Attack という新しいマルウェアを含め、iPhones と iPad を独創的な方法で感染させたインシデントがあります。

WireLurker はMac OS デバイスとiOS デバイスの両方を狙う新しいクラスのマルウェアです。[10] WireLurker がユニークなのは、脱獄されていない iOS デバイスでも、感染した Mac OS デバイスに USB ケーブルで接続すると、感染できることです。

WireLurker がデバイスを攻撃する一般的な仕組みはこうです。

- ユーザーが Mac OS デバイス上で、マルウェアに感染した OS X アプリを、おそらく非公式なサードパーティ・アプリ・ストアからダウンロードしてインストールします。
- ユーザーが、感染したアプリを実行し、ルート権限をアプリに許可します。それには、Mac OS デバイスの管理者パスワードが必要です。
- マルウェアに感染した OS X アプリを実行すると、アプリは複数の iOS アプリをダウンロードし、コンピューターを信頼する iOS デバイスが USB ケーブル経由で接続するのを待ちます。
- 感染した Mac OS デバイスを信頼する iOS デバイスが接続されると、マルウェア・アプリは悪意のある iOS アプリを iPhone または iPad にロードします。
- iOS アプリ自体は企業の署名が入ったアプリです。つまり、サイバー犯罪者が別の企業のアカウントに侵入したか、Apple に自分たちの iOS アプリを承認させたわけです。これらのアプリには、プロビジョニング・プロファイルもあるため、iOS デバイスに信頼されます。

何も知らないユーザーが、悪意のある iOS アプリを脱獄されていない iOS デバイスにアップロードすると、これらのアプリは情報を盗み、攻撃者のサーバーと定期的に通信することができます。

おそらく、WireLurker よりもさらにたちが悪いのは、最近発見された Masque Attack というマルウェアで、[11] これもやはり、脱獄されていない iOS デバイスを感染させることができますが、感染した Mac OS デバイスに接続する必要がありません。この攻撃の場合、エンタープライズ/アドホック・プロビジョニングでインストールされた iOS アプリと iTunes App Store の認可アプリの両方が同じバンドル ID を使用していれば、前者が後者にとってかわることができます。

Masque Attack がユーザーの本当のアプリに置き換わって情報を盗む経緯はこうです。

- ユーザーがどこかの Web サイトのリンクをクリックすると、企業の証明書で署名され、「New Angry Bird」といったようなラベルが付いていることのある悪意のあるアプリがダウンロードされ、インストールされます。
- 悪意のあるアプリは、銀行アプリやメール・アプリなど、同じバンドル ID を持つ正式なアプリに置き換わります。
- 攻撃者は元のアプリのログイン・インターフェースを偽装して、ユーザーの認証情報を盗みます。
- また、ローカル・データ・キャッシュを使って、メール・アプリの最近の電子メールなど、元のアプリの機能もエミュレートできます。

サイバー犯罪者がログイン認証情報とローカルでキャッシュされたデータを入手すると、ユーザーの機密データと財務情報が攻撃やデータ損失に対して無防備になります。

マルウェアからの保護機能は、エンタープライズ・モビリティ管理を満たす

IBM® MaaS360® Mobile Threat Management

IBM は IBM Security Trusteer ® との統合により、新しいセキュリティー・レイヤーを EMM にもたらして、モバイル・マルウェアや感染したデバイス (脱獄またはルート化されたスマートフォンやタブレット) からデータを守ります。

この独自の統合とシナジーは、企業/個人情報を犯罪目的のために入手しようと企んでいるハッカーと泥棒に対し、強力な防御を作り出します。

データベースを継続的に更新することで、マルウェアの署名の付いたiOSアプリとAndroidアプリを検出、分析します。

Trusteerは、不正やデータ侵害から企業を守るために非常に数多くのユーザーが利用しており、リスク認識とセキュリティー・インテリジェンスをMaaS360に提供します。

モバイル・マルウェアの検出と修復:

- データベースを継続的に更新することで、マルウェアの署名の付いたiOSアプリとAndroidアプリを検出、分析
- アプリの例外を追加することで、許容できるアプリの使用方法をカスタマイズ
- きめ細かいポリシー・コントロールを設定して、適切な対策を実行
- ほぼリアルタイムのコンプライアンス・ルール・エンジンを使って、修正を自動化
- マルウェアが検出されると、ユーザーと関係者にアラート通知
- My Alert Centerで感染デバイスを表示し、My Activity Feedダッシュボードで検出イベントを表示
- マルウェアの付いたアプリを自動的にアンインストール (Samsung SAFEなど一部のAndroidデバイス)
- アクセスをブロックし、デバイスの一部またはすべてをワイプ
- 次のようなデバイスの脅威属性を収集および表示:
  - 検出されたマルウェア
  - 不明なSMSリスナーやスタートアップ・パッケージなど、検出された疑わしいシステム構成
  - 危険なWi-Fiホットスポットへの接続
  - 市販されていないアプリのインストールを拒否
  - OSバージョン
- マルウェア検出イベントの監査履歴を検証

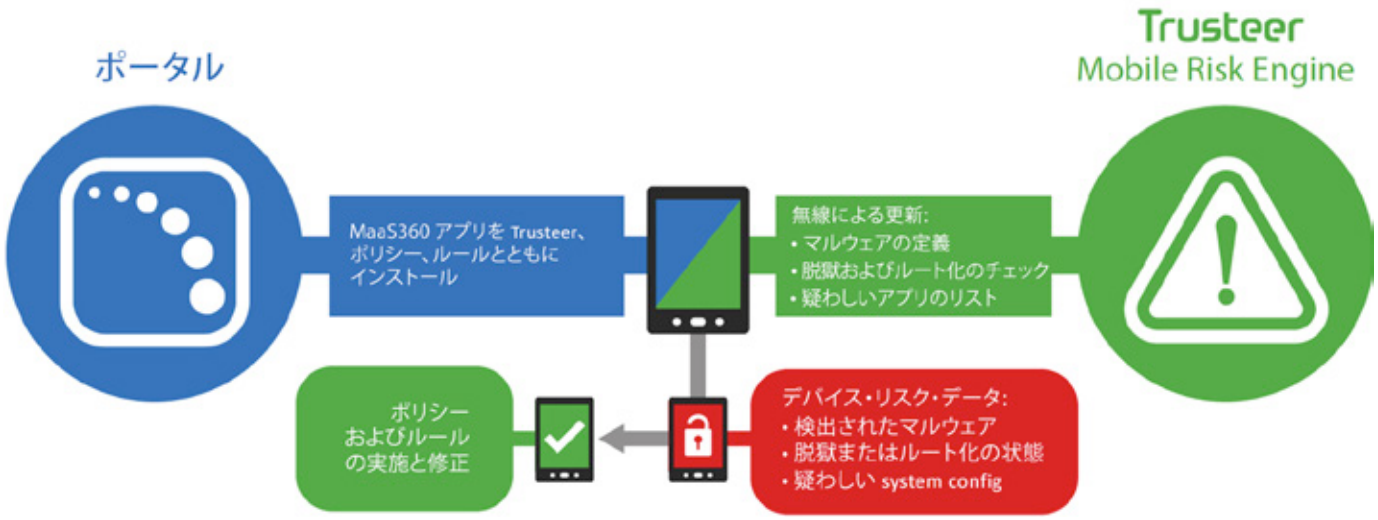

図3:MaaS360はTrusteerと連携して、モバイル・マルウェアと感染したデバイスを検出、分析、修正

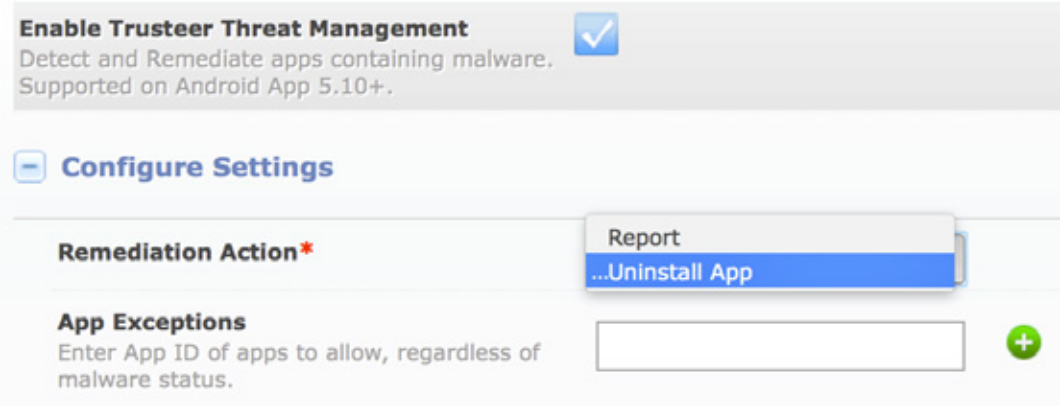

図 4:MaaS360 構成設定の一部

脱獄およびルート化のその他の検出:

- 感染または脆弱性のあるモバイル機器を検出
- 攻撃者にさらに多くの OS 権限を与えて、様々な攻撃ベクトルを可能にする、脱獄された iOS デバイスとルート化された Android デバイスから保護
- 脱獄されたデバイスとルート化されたデバイスの検出を逃れようとするハイダーや隠蔽手法を検出
- 動きの速いハッカーにより素早く対応するため、無線で更新された検出ロジックを適用。アプリの更新は一切不要
- セキュリティー・ポリシーとコンプライアンス・ルールの設定により、修復を自動化
- アクセスをブロック、デバイスの一部またはすべてをワイプ、またはデバイス・コントロールを削除

また、ユーザーのデバイスと情報をこのセキュリティー・レイヤー (コンシューマー向けにはまだ未対応) で保護することができます。

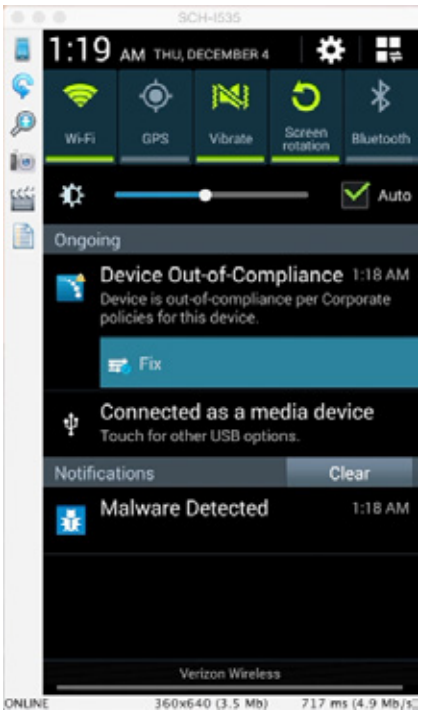

図 5:検出されたモバイル・マルウェアとコンプライアンスに違反したデバイスを示すスクリーンショット

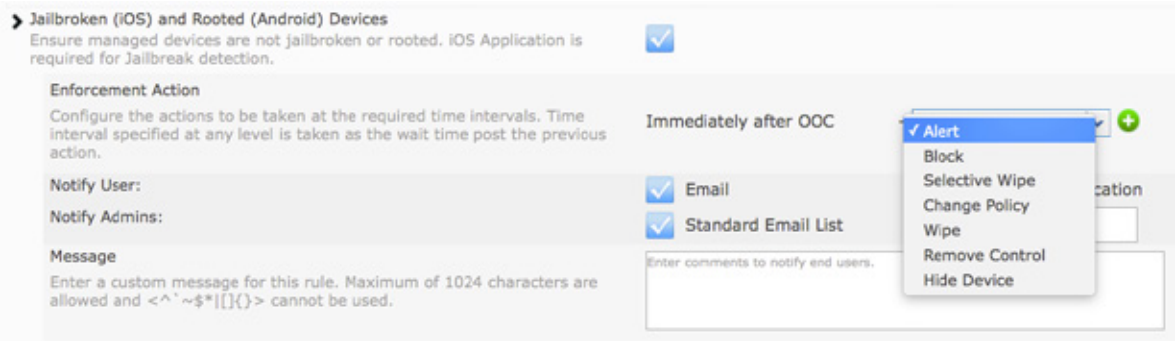

*図 6:*脱獄されたデバイスとルート化されたデバイスへのコンプライアンス実施アクションを構成する

Trusteer Mobile Risk Engine により、保護レイヤー、および適応型マルウェア防止を実現するサイバー犯罪インテリジェンスは、最新の攻撃動作をより迅速に検出して適応できるため、マルウェアが詐欺を働く機会は実質的にゼロになります。このエンジンは、最新のマルウェア、脱獄、ルートのチェック機能を実行するために、継続的に更新されており、デバイスとアプリの危険要因を基にほぼリアルタイムでモバイルのリスク評価を実行します。

主なメリット

MaaS360 Mobile Threat Management ソリューションのメリットは、企業のデバイスとデータをただ保護する以上のものがあります。ユーザーのデバイスと情報をこのセキュリティー・レイヤー (コンシューマー向けにはまだ未対応) で保護することができます。

ユーザを教育し、データを保護するために企業ができることはもっとあります。

BYOD と会社所有デバイスの両方を安全にサポート

雇用者が重宝する BYOD のメリットとして、個人データの保護を追加

ほぼリアルタイムでモバイルの脅威を先見的に管理

企業および個人情報の機密データ漏洩のリスクを軽減

企業、特に BYOD で Android をより広く採用できるように工夫

モバイルのセキュリティー・リスクが発生した場合は、自動的な措置を講じて修復

ユーザーの教育と保護

この MaaS360 Mobile Threat Management ソリューションのほか、企業がユーザーの教育とデータ保護のためにできることはもっとあります。

企業は以下のモバイル・セキュリティー活動を検討する必要があります。

- アプリケーションのセキュリティーについて従業員を教育する:サードパーティ製アプリケーションをダウンロードすることの危険性、デバイスのゆるい権限の許可が招く潜在的な危険について、従業員を教育します。
- BYOD デバイスを保護:エンタープライズ・モビリティ管理機能を適用することで、従業員が自分のデバイスを使えるようにしながら、企業のセキュリティーを維持します。
- 認可されたアプリ・ストアのみからダウンロードすることを従業員の許可する:Google Play、Apple App Store、会社のアプリ・ストア (提供されている場合) など、認可されたアプリケーション・ストアのみからアプリケーションをダウンロードすることを従業員に許可します。
- デバイスが感染した場合は、迅速に対処する:デバイスの感染が見つかったか、悪意のあるアプリが見つかった場合は、自動的に措置を講じる自動ポリシーをスマートフォンとタブレットに設定します。このアプローチにより、企業のデータを保護しながら問題を修復します。

MaaS360 を選ぶ理由

MaaS360 では、先進的なマルウェア保護機能、および業界最先端のエンタープライズ・モビリティ管理とセキュリティを統合しています。セットアップと操作を素早く簡単にでき、企業と個人双方のモバイル機器の機密データを保護できます。

IBM MaaS360 について

IBM MaaS360 は、業務のあり方に合わせて生産性とデータ保護を実現するエンタープライズ・モビリティ管理プラットフォームです。モバイル・イニシアチブの基盤として多数の組織から信頼されています。MaaS360 は包括的な管理機能を提供し、ユーザー、デバイス、アプリ、コンテンツへのセキュリティーを強力に制御することで、どのようなモバイル導入もサポートします。IBM MaaS360 の詳細と 30 日間の無料トライアルのご利用については、次の Web サイトをご覧ください。www.ibm.com/maas360

IBM Security について

IBM のセキュリティー・プラットフォームはセキュリティー・インテリジェンスを提供して、組織が人々、データ、アプリケーション、インフラストラクチャーを包括的に保護できるように支援します。IBM は、ID およびアクセス管理、セキュリティー情報およびイベントの管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、次世代侵入保護などのためのソリューションを提供しています。IBM は、世界で最も幅広くセキュリティー研究開発を行い、セキュリティーを提供している組織の一つです。詳細は、以下をご覧ください。
www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in Japan
March 2016

リサイクルにご協力ください

WGW03150-JPJA-01

1 「World to have more cell phone accounts than people by 2014」2013 年 1 月 2013 International Telecommunications Union、http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

2 「State of Mobile App Security」2014 年 11 月 2014、Arxan Technologies、https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

3 「Bring Your Own Device: The Facts and the Future」2013 年 5 月 2013、Gartner、http://www.gartner.com/newsroom/id/2466615

4 「Motive Security Labs Malware Report」2014 年下半期 2014、Motive Security Labs、http://www.gartner.com/newsroom/id/2466615

5 「2014 Cost of Data Breach Study:Global Analysis」2014 年、Ponemon Institute、http://www-03.ibm.com/security/data-breach/

6 「State of Mobile App Security」2014 年 11 月、Arxan Technologies、https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

7 「The State of Mobile Application Insecurity」2015 年 2 月、Ponemon Institute、https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov33432&S_TACT=102PW2CW

8 「IDC Worldwide Quarterly Mobile Phone Tracker」2015 年 2 月、IDC、http://www.idc.com/getdoc.jsp?containerId=prUS25450615

9 「DroppedIn: Remotely Exploitable Vulnerability in the Dropbox SDK for Android」2015 年 3 月、IBM Security、http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.Vb-1_SisG8W

10 「Wirelurker: A new Era in OS X and iOS Malware; Blog」PaloAlto Networks、2014 年 11 月 5 日、http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

11 Xue H.、Wie T.、Yulong Z.、「Masque:All Your iOS Apps Belong to Us」Fire Eye、2014 年 11 月 10 日、https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html