IBM MaaS360 Mobile Threat Management

iOS および Android デバイスのモバイル・マルウェアを停止

主なメリット

- BYOD および企業所有デバイスの両方を安全にサポート
- ほぼリアルタイムで、モバイルの脅威を予防的に管理
- 企業および個人の情報の機密データ漏洩のリスクを低減
- 自動化されたアクションで、モバイルセキュリティのリスクを修復

モバイル・マルウェア – 次の大きなセキュリティの脅威

企業は、予測できないペースでモバイル化へ転換しています。個人所有デバイスの持ち込み (BYOD) のトレンドが、企業で広まっています。モバイル・アプリケーションは、従業員に対して新しく、効率的なワークフローを生み出します。仕事のデータ、電子メール、コンテンツへのシームレスなアクセスが並行して拡大し、こうしたトレンドから生産性が向上しています。

モバイルデバイスの人気や、企業の主力になっていくスピードの結果として、ハッカーや盗人がマルウェアによってモバイルデバイスを狙い、これが次の大きなセキュリティの脅威となっています。企業データは、特に不正なアプリケーションや悪意のある Web サイトに対して脆弱なのです。

- 2014 年、ダウンロードされたアプリケーションは 1,380 億。[1]
- モバイル・マルウェアが増大。常に、1,160 万台を超えるモバイルデバイスが悪意のあるコードに感染しています。[2]
- 最新の WireLurkerや Masque の攻撃は、iOS デバイスをターゲットにしています。[3,4]
- 会社のブランドへの損害が財政的な損失によって増大し、一度の違反のコストは 1,100 万ドルを超えると推定されています。[5]

IT およびセキュリティのリーダーは、モバイルマルウェアを予防的に検出、分析、修復できる最新かつ強固なセキュリティソリューションを必要としています。

企業のモバイル脅威を食い止める

IBM® MaaS360® Mobile Threat Management は、iOS および Android デバイスをマルウェアから保護できる、先進的なシステムです。企業のデータが損ねられる前に、リスクを検出し、脅威を管理できます。

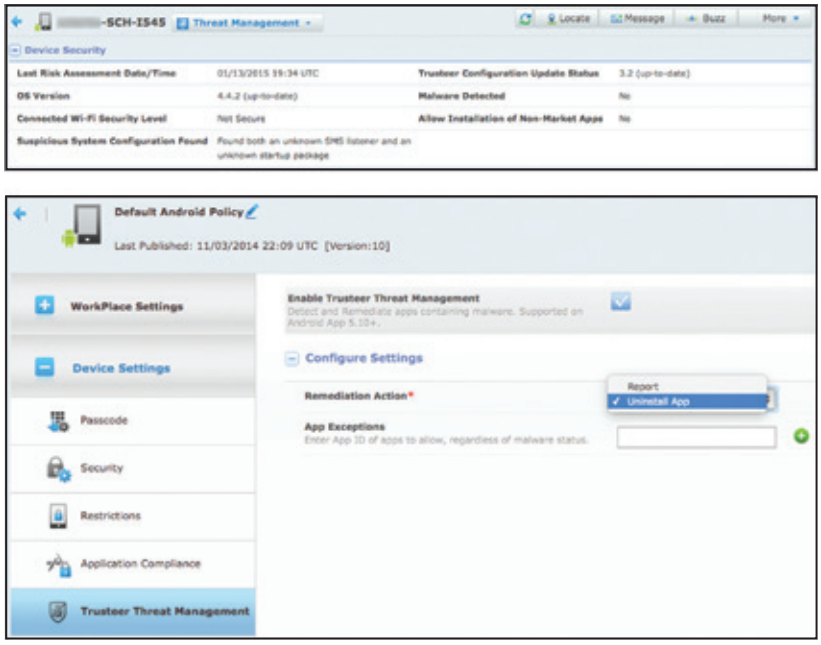

図 1:MaaS360 Mobile Threat Management での、保護されているデバイスやポリシーの設定に関するレポートデータの例

IBM Trusteer との統合で、®何億ものユーザーによって詐欺やデータ漏洩から組織を守るために活用されている、MaaS360 は、Enterprise Mobility Management (EMM) に新しいセキュリティのレイヤーを提供します。

マルウェアに、あなたの組織のモバイル移行を邪魔させないでください。企業の生産性のイニシアティブと、MaaS360 が提供するセキュリティでバランスをとってください。

モバイルマルウェアの検出と修復

- iOS および Android のアプリケーションを、継続的に更新されるデータベースから得られるマルウェアの署名や悪意のある挙動によって検出、分析します。
- アプリケーションの例外を追加して、許容されるアプリケーションの利用をカスタマイズ
- きめ細かいポリシーコントロールを設定して、適切なアクションを行う
- ほぼリアルタイムのコンプライアンス・ルール・エンジンを活用して、修復を自動化
- マルウェアが検出された場合は、ユーザーや責任者へ警報
- 感染したデバイスを My Alert Center で、検出したイベントを My Activity Feed ダッシュボードで表示
- マルウェアに感染したアプリケーションを自動的にアンインストール (Samsung SAFE などの Android デバイスを選択™)
- アクセスをブロック、選択的または全面的にデバイスをワイプ
- MaaS360 コンテナ・ソリューションの使用を制限
- 以下を含む、デバイスの脅威属性を収集、表示:
  - 検出したマルウェア
  - 不明な SMS リスナーやスタートアップパッケージなどの不審なシステム設定を発見
  - セキュアでない Wi-Fi ホットスポットへの接続
  - 市販されていないアプリケーションのインストールの許可
  - オペレーティングシステムのバージョン
- マルウェア検出イベントの監査履歴のレビュー

補足的なジェイルブレイクおよびルート検出

- 感染した、あるいは脆弱なモバイルデバイスの検出
- 攻撃者にオペレーティングシステムでの塚権限を与える可能性がある、ジェイルブレイク iOS やルート Android デバイスに対して保護
- ジェイルブレイクやルートデバイスの検出をマスクしようとする隠匿者やアクティブな隠匿テクニックを発見
- アプリケーションの更新なしでも、無線通信を経由して更新される検出ロジックの更新で、高速で移動するハッカーにも機敏に対応
- セキュリティポリシーやコンプライアンスルールの設定で、修復を自動化
- アクセスをブロック、選択的または全面的にデバイスをワイプ

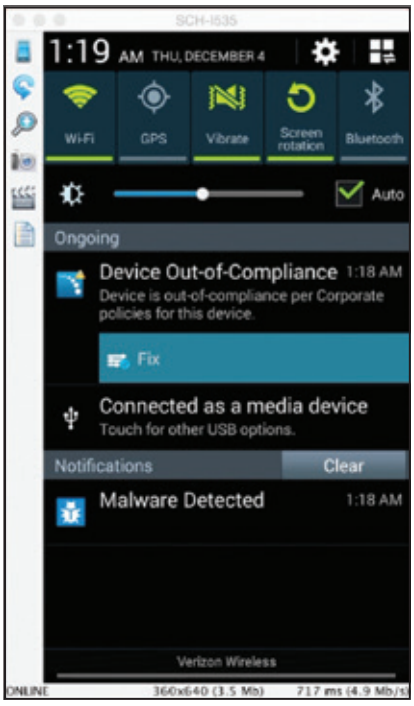

*図 2:*デバイスでのマルウェア通知の例

IBM Security Trusteer Mobile Risk Engine

- 適応性の高いマルウェア防止のために、保護とサイバー犯罪インテリジェンスのレイヤーを提供
- 最新の攻撃パターンを迅速に検出し、適応できるので、マルウェアが詐欺を犯せる機会は実質的にゼロです
- デバイスやアプリケーションのリスク要因に基づいて、ほぼリアルタイムでモバイルリスクの評価を実行
- 継続的な更新で、最新のマルウェア、ジェイルブレイク、ルートをチェック

IBM Security 詐欺防止ソリューションの詳細については、日本IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。
ibm.com/security.

© Copyright IBM Corporation 2016

IBM Systems and Technology Group
Route 100
Somers, NY 10589

Produced in Japan
January 2016

IBM、IBM ロゴ、ibm.com、および X-Force は、世界の多くの国で登録された International Business Machines Corporation の商標です。BYOD360™、Cloud Extender™、Control360®, E360®、Fiberlink®、MaaS360®、MaaS360® およびデバイス、MaaS360 PRO™、MCM360™、MDM360™、MI360®、Mobile Context Management™、Mobile NAC®、Mobile360®、Secure Productivity Suite™、Simple. Secure. Mobility.®、Trusted Workplace™、Visibility360®、および We do IT in the Cloud.™ およびデバイスは、IBM 社の一員である Fiberlink Communications Corporation の商標または登録商標です。他の製品名およびサービス名等は、それぞれ IBM または他社の商標である場合があります。現時点での IBM の商標リストについては、次の Web サイトをご覧ください。(**ibm.com**/legal/copytrade.shtml)でご覧いただけます。

Apple、iPhone、iPad、iPod touch、および iOS は、米国、その他の国における Apple Inc. の登録商標または商標です。

本書の情報は最初の発行日の時点で得られるものであり、IBM によって予告なしに変更される場合があります。掲載されている製品・サービスは IBM がビジネスを行っているすべての国・地域でご提供可能なわけではありません。

性能データとお客様の事例は、説明目的のみのために提示しています。実際の性能結果は、特定の設定や運用条件によって異なる場合があります。他社の製品またはプログラムと IBM の製品またはプログラムを併用した場合の操作の評価および検証は、お客様の責任で行ってください。

本資料の情報は「現状のまま」提供され、商品性、特定目的への適合性に対する保証、および非侵害の保証または条件を含め、いかなる明示的または黙示的な保証も行いません。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

適用されるすべての法令と規則の順守は、お客様の責任範囲とします。日本 IBM は、法律上の助言を提供することはいたしません。また 日本 IBM のサービスまたは製品が、お客様においていかなる法を順守していることの裏付けとなることを表明し、保証するものでもありません。

IBM の将来の方向性および指針に関する記述は、予告なく変更または撤回する場合があります。

確実なセキュリティー体制への取り組みについて:IT システムのセキュリティーでは、社内外の不適切なアクセスの防止策、検出、対応に取り組むことで、システムと情報を保護しています。不適切なアクセスにより、情報が改ざん、破壊、または不正流用される可能性があり、システムへのダメージや他者への攻撃といったシステムの悪用が生じることがあります。IT システムまたは製品によってセキュリティー対策が万全になると考えることは危険であり、1 つの製品またはセキュリティー対策で不正アクセスを完全に有効に防ぐことはできません。IBM のシステムと製品は、包括的なセキュリティー・アプローチの一部として設計されています。そのため、運用手順を追加することがどうしても必要となり、効果を最大限に高めるには、他のシステム、製品、サービスが必要になることがあります。IBM は、システムと製品が他者による悪意のある行為または不正行為から免れることを保証するものではありません。

Please Recycle

1 Arxan の年次報告書: "*State of Mobile App Security Reveals an Increase in App Hacks for Top 100 Mobile Apps*"、2014年11月、Arxan Technologies, Inc., https://www.arxan.com/2014/11/17/arxans-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/

2 Kindsight Security Labs マルウェア・レポート – Q4 2013, Alcatel-Lucent, http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf

3 Xiao, Claud, WireLurker:「A New Era in OS X and iOS Malware, Blog post on Palo Alto Networks」、2014年11月5日、http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

4 Zue, Hui, Wei, Tao and Zhang, Yulong「Masque Attack:All Your iOS Apps Belong to Us」、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

5 2013 サイバー犯罪コスト調査:United States, Sponsored by HP Enterprise Security, Ponemon Institute, 2014年10月, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

WGD03057-JPJA-01