ZIMPERIUM®

Management is Not Security

モバイル脅威防御がサイバーセキュリティ戦略に不可欠な理由

数年前、会社の電子メールを個人デバイスから確認することは、雇用主からあまり好まれない可能性がありました。しかし、現在、企業組織において、個人用デバイスの使用が標準となってきています。2022年のZimperiumのGlobal Mobile Threat Reportによると、仕事で使用されている携帯電話の66%は従業員個人のものが使われています。

COVID-19のパンデミックに伴うリモートワークは、この変化の部分的な原因です。たとえば、従業員は、オフィスにいるだけでなく自宅で働く場合も、個人デバイスからOffice 365、G Suite、JIRA、Okta、Salesforceなどの生産性向上アプリケーションを使用しています。また、個人および企業所有のデバイスも、日常的に多要素認証(MFA)のために使用されており、企業データへの非モバイルアクセスも使用されています。

職場での個人用デバイスの使用により、従業員の生産性は向上します。しかし、それはまた、デバイスとデータ間の境界線が曖昧になり、サイバー犯罪者が企業情報を盗用する機会が増えることになります。その結果、犯罪者は戦術を進化させ、複数のチャネルを活用してフィッシング攻撃を実行しており、モバイルデバイスが新しいバックドアとなっています。

モバイルデバイスは、個人の身元に直接繋がっています。これらのデバイスは、従来のオフィス周辺外での作業データへのアクセスを得るために、個人の身元を確認するために使用されます。犯罪者による企業のデータへのアクセスがこれまで以上に増え、従来のエンドポイントよりもはるかに保護されていない、モバイルデバイスのユーザーがターゲットになります。モバイルデバイス管理(MDM)などの従来のセキュリティおよび管理は、高度な脅威を効果的に検出および解決するには不十分です。名前が示すように、MDMはデバイスを管理します。モバイル脅威防御(MTD)のようなより積極的なモバイルセキュリティツールは、犯罪者と従業員自身から企業を保護するために不可欠です。

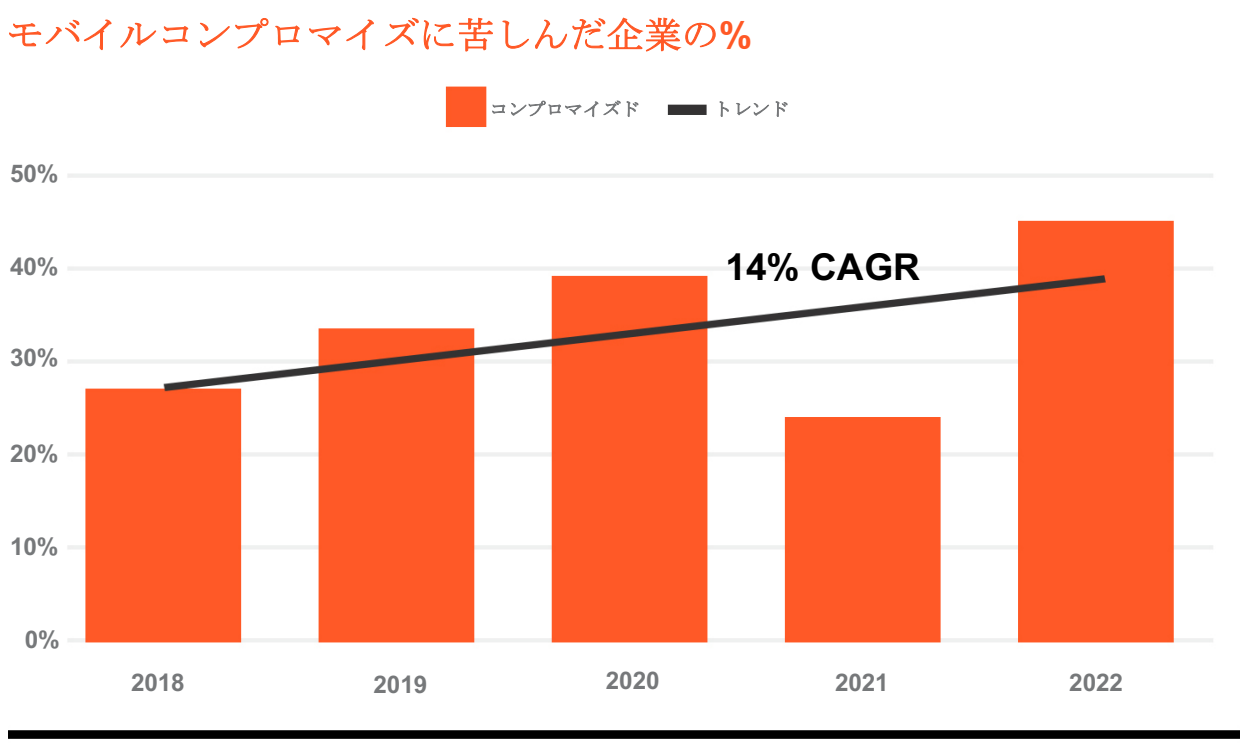


図1. モバイルデバイスを使用することで、データの損失やダウンタイムにつながるコンプロマイズに苦しんでいることを認めた回答者の割合。
[n=601, 671, 876, 856, 632]

（出典：Verizon Mobile Security Index 2022）

BYODの影響

BYODは、過去数年だけで劇的に変化しました。COVID-19のパンデミック以前、企業の60%が、BYOD政策が整備されていないと報告しました。環境が大きく変化している一方で、かなりの数の組織にBYOD政策がありません。2022年グローバルモバイル脅威レポートによると、約30%の組織にBYOD政策がありません。

企業環境でのモバイルデバイスの導入状況を検討する際、電子メール、アプリ、またはその他の通信チャネルで企業情報にアクセスするこれらのデバイスの多くが、包括的なモバイルセキュリティソリューションによって保護されていないことは驚くべきことです。MDMによって管理されるデバイスには、モバイルデバイスを制御するエージェントがあり、コンプライアンスがない場合、管理デバイスポリシーの遵守が不十分な従業員が多くいるため、モバイルデバイスを消去する機能が備わっています。Zimperiumは、企業に接続されているスマートフォンの平均66%が管理されておらず、回答者の5%はデバイスがまったく管理されているかどうかわからないということを明らかにしています。

平均的な電話ではかなりのスペースが仕事に使用されています：モバイルデバイスにインストールされているアプリケーションの10%は仕事に関連しています。一般的に100から120のアプリがインストールされていることを考えると、従業員の携帯電話には10から12の仕事に関連するアプリケーションが存在していることになります。

これらのデバイスが、いかなる方法においても監視されず保護されていないとします。この場合、機密性の高い企業データや資格情報は、モバイル版トロイの木馬や、中間者攻撃(MiTM)、ランサムウェア、フィッシング詐欺、悪質なアプリなどによって傍受される可能性があります。実際、ほとんどのユーザーは、手遅れになるまで、モバイルデバイスにこれらの脅威があることをおそらく知りません。被害金額は高額です：2021年のデータ侵害の平均コストは424万ドルでした。リモートワークにより生じた不正は、約107万ドル分さらに高額になっています。

脅威アクターが拡大された攻撃面を悪用する方法

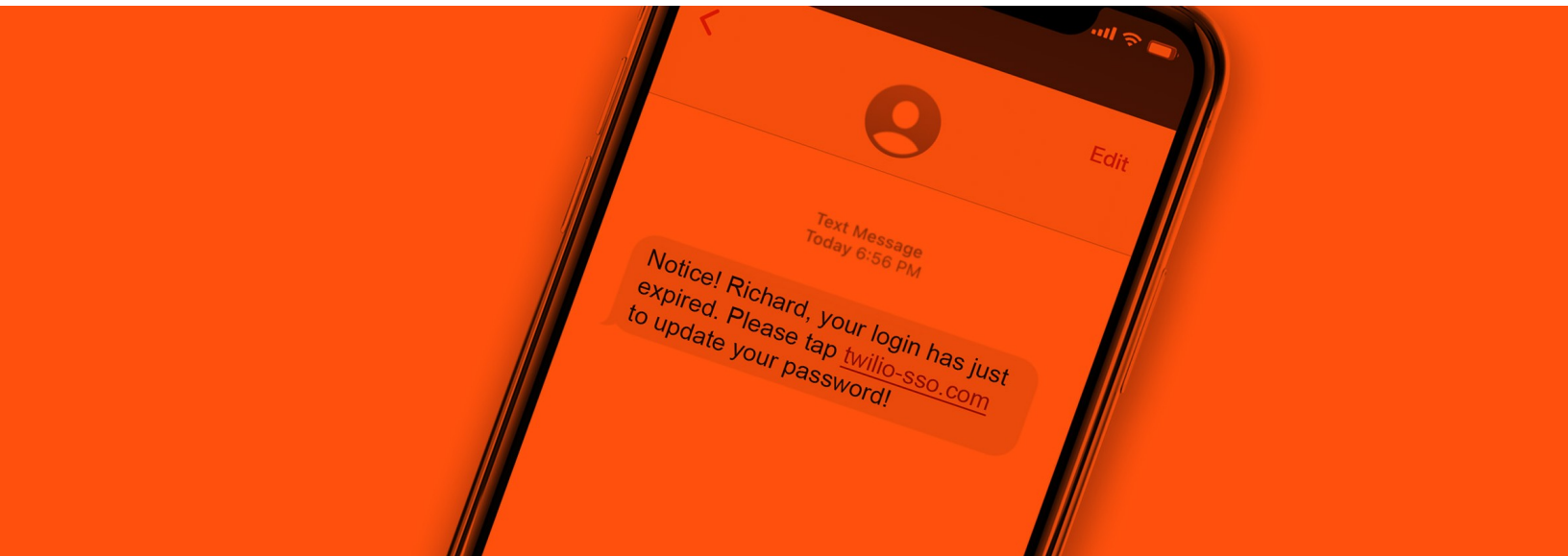
10年前は、IT部門は組織を攻撃から保護する際に、ここまでの心配は不要でした。セキュリティは、「周囲を保護する」よりも進化しています。デスクトップなどの従来のエンドポイントは、オンサイトに存在せず、会社が所有しています。過去には、これらのアセットは、セキュリティの層によってオンプレミスで保護されていました。

スマートフォンやタブレットは、家族、友人、同僚と繋がる方法を変革したモバイルデバイスです。しかし、従業員は電子メール、SMS、アプリ、連絡手段アプリなどのコミュニケーションチャネルにアクセスするため、新しいリスクが仕事の場面で生じています。

従業員が所有するデバイスは、企業管理下に登録されている場合でも、管理が課題です。また、高度な脅威をブロックするのに必要な可視性が欠けています。デバイス所有者に付与されたレベルの制御と権限が欠けているため、ITチームが脅威を修正したり、リスクのあるデバイスを特定したりすることは困難です。しかし、企業所有のデバイスも同じ課題に直面しています。実際、企業組織の42%が、モバイルデバイスやWebアプリケーションが2020年にセキュリティインシデントにつながったと報告しています。職場の不正なアプリが企業データにアクセスできる割合と同じであることが示されています。また、暗号化や認証が欠けているため、ITおよびセキュリティリーダーの10%が保護されていないアプリがあることを報告しています。

企業が懸念するべきリスクは、モバイルの脅威だけではありません。厳格に保護されると思われるアプリにおいても、さまざまな種類のマルウェアの標的となっています。公式アプリストアから入手するアプリは通常安全ですが、検査を通ったものでもマルウェアが含まれているものもあります。Zimperiumの調査によると、1つの例として、モバイルウォレットや銀行アプリを含む米国内の121件の金融アプリが、トロイの木馬によって攻撃されています。これらのアプリによって、機密データにアクセスしたり、資格情報を盗んだり、盗まれた情報を共有が発生しています。このマルウェアは、通常のアプリに偽装されて隠されており、大部分は、主要なアプリストアからデバイスにダウンロードされます。

脅威アクターは、多くのアプリのセキュリティが強化されていないという事実と、ユーザーがデバイスの脆弱性に影響する権限と設定にほとんど注意を払っていないことにつけ込んでいます。その結果、モバイルデバイスは企業データへの新しく簡単なアクセス方法であると考えられています。悪質なアプリケーションや、不正なネットワーク、またはデバイス自体の侵害は、犯罪者が企業資産へアクセスしようとする方法の一つにすぎません。たとえば、クラウド通信会社Twilioは、従業員がSMSのスピアフィッシング攻撃を受けた結果発生したデータ侵害について最近公表しました。「SMSフィッシングメッセージは、Twilioの従業員にパスワードが期限切れになったか、変更される予定であることを警告するメッセージによってリンクをクリックさせるものでした。」



モバイル脅威防御の紹介

新しいビジネス上の課題とニーズに対処するために、テクノロジーは進化してきました。近代的なモバイル時代は、現在の脅威に対処するのに役立つ新しいカテゴリのセキュリティを必要としました。モバイル脅威防御(MTD)は、デバイスや、ネットワーク、アプリケーション全体のモバイル脅威を防止し、検出する包括的なモバイルセキュリティソリューションです。MTDは、機械学習(ML)や行動分析などのさまざまな技術を活用して、脅威、アプリの検出、デバイスの脆弱性管理を検出します。

MTDとMDMは、モバイルの脅威からビジネスを保護する広範な目標を共有しています。MTDはモバイルセキュリティテクノロジースタックに高度な機能が追加されています。MTDツールは過去10年間に市場に登場しましたが、それらのほとんどは、デバイス上の包括的な保護を提供せず、更新またはアクティブなネットワークに接続する必要があります。

Gartnerの2014年の企業モバイルセキュリティのハイプサイクルで発表された、Mobile Advanced Threat Defense (MATD)は、ソリューションカテゴリとして最初のものです。当時、MATDはAdvanced Threat Defense (ATD)市場のサブセットとして考えられていました。しかし、MTDはすぐに独自のソリューション市場となり、同年のGartner EMEA IT インフラストラクチャおよびオペレーション管理サミットでMTDとして登場しました。

モバイル脅威防御は、モバイルエンドポイントを攻撃や脅威から保護する積極的な方法です。MTDは、包括的な警告システムとして機能し、デバイスを継続的にスキャンして脅威から保護します。デバイスが安全でない場合—パッチが作成されていないソフトウェアなどの攻撃や脆弱性がある場合—ユーザーと企業の両方に通知されます。

モバイルデバイスの保護をしていますか、またはそれらを管理していますか？

MDMは、その名前が示すように、管理ツールです。MDMはデバイス自体を制御するため、組織がアプリを安全に配布し、オペレーティングシステム(OS)要件を最小限に設定し、アプリをブロックすることができます。

MDMは、デバイスが破られようとする場合に、セキュリティチームに通知して基本的な脅威保護を提供します。ただし、MDMだけを使用して、MITRE ATT&CKフレームワークでカバーされている脅威の多くから組織をできる限り保護したい場合は、デバイスの使用がほぼ不可能なほどの制限をかける必要があります。さらに、御社のユーザーは、個人デバイスや、アプリ、データのプライバシーに関する制御に懸念を持っています。さらに、御社にはネットワーク、フィッシング、アプリからの脅威を検出または解決する機能がありません。

MTDは、SSLストリッピング、中間者攻撃(MiTM)、フィッシング、不正なネットワーク、マルウェア、その他の攻撃など、いくつかの種類の攻撃をスキャンします。デバイスや、ネットワーク、フィッシング、悪質なアプリの攻撃を介したモバイル脅威を検出および防止するために、デバイス上および機械学習に包括的なソリューションが導入されます。MTDソリューションを使用すると、セキュリティチームが厳格なセキュリティとコンプライアンス義務を満たすために必要とするセキュリティポリシーにより、より多くの制御が行われます。さらに、MTDプロバイダーは、プライバシーポリシーを含めることで、デバイスが保護されている間、従業員がプライバシーを損なうことなくデータを取り扱う方法を理解しやすくする必要があります。

MTDとMDMツールを組み合わせて活用することで、いくつかの利点があります。たとえば、MDMがモバイルデバイスに登録され、ポリシーを適用し、企業リソースへのアクセスが許可されると、従業員にとって日々の生産性を妨げる制限は限定的です。セキュリティチームは、デバイスをリアルタイムで監視し、インストールはほぼ不要で、MTDアプリをデバイスに導入することができます。これにより、従業員のプライバシーを守りながら組織での採用率が大幅に向上します。

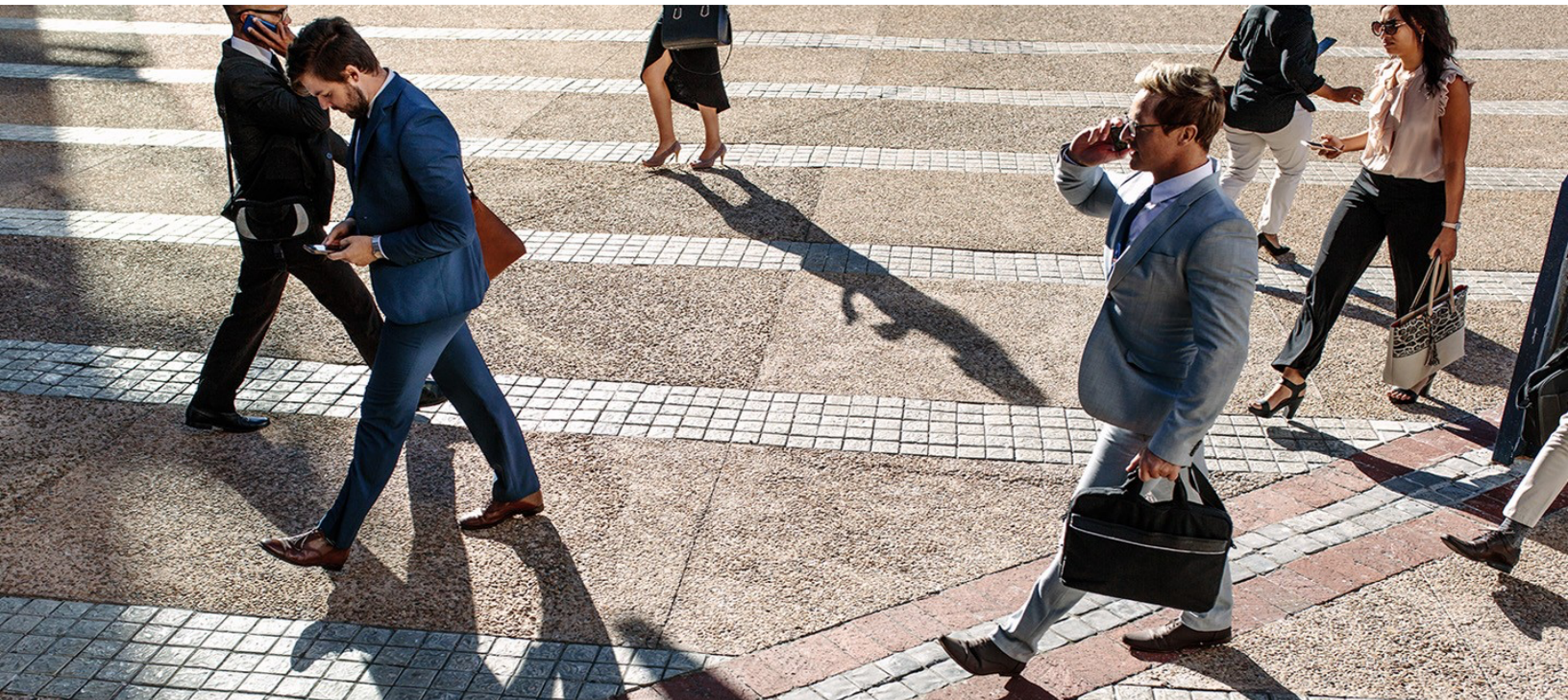
モバイルデータセキュリティとプライバシーの懸念

企業の半数以上(60%)が、モバイルデバイスで従業員が電子メールを確認することを許可しており、さらに31%の企業が検討しています。BYODの保護は、いくつかの理由で企業所有デバイスを保護するよりも難しい場合があります。第一に、従業員が所有するデバイスは、従業員のものです。従業員として、何ができるか、雇用主によってダウンロードできないことは何なのかを指示される必要ないと感じています。

従業員の財産にモバイルエコシステムをスキャンするオンデバイスエージェントをインストールすることは、特にプライバシーに監視て侵入的と見なされる可能性があります。セキュリティ要件に応じて、MDMを使用している企業は、電子メールアカウントを設定し、アプリストアからアプリをダウンロードして制限し、従業員のデバイスがコンプライアンスであることを確実にするために個人データと支払い情報を機密に収集することができます。当然、データと場所がセキュリティチームによって処理される方法について従業員は懸念を抱きます。

これらの理由により、BYODの保護に関しては、セキュリティチームは低い採用率にとどまっています。従業員は、プライバシーは尊重すべきであり、適切な量と品質の情報が、セキュリティ上の理由からデバイスから収集されているだけであることを知っておきたいと考えています。

従業員のプライバシーを守るためには、ユーザーの個人データの機密性を保護することが重要です。適用されるデータプライバシー法や規制を遵守することは、データがコンプライアンス基準を満たしていることを確実にする上で最重要です。モバイルセキュリティを導入するセキュリティチームは、場所や業界に応じて、どのデータプライバシー法と規制を遵守すべきかを判断するために、社内顧問に相談する必要があります。これらの要件を、従業員のデバイス上のプライバシーポリシーや、プライバシー推奨、著名なプライバシー通知があるモバイルセキュリティアーキテクチャに組み込みます。また、デバイスを保護することが個人データを保護するために重要である理由について理解することをサポートします。



一般的なモバイル脅威

犯罪者は、お金があるところを常に狙っています。昔は、彼らは馬車や銀行を襲っていました。今では、企業のデータは金銭的価値があり、職場で個人的なモバイルデバイスを使用している労働者がますます増えている中で、犯罪者はこれらのモバイルエンドポイントを標的としています。私たちのチームが実際に確認した最も一般的なモバイル脅威の一部を以下に示しています。

フィッシング

フィッシングは、サイバー犯罪者が効果的であると判断しており、今でも存在しているサイバー脅威です。ユーザーがフィッシング詐欺を見つけ、回避するように訓練されているという事実にもかかわらず、Zimperiumの研究で、2021年にはモバイルユーザーの10人に1人が悪意のあるリンクをクリックしたことがわかりました。実際、攻撃の90%はフィッシング攻撃から始まります。ユーザーは自分の携帯電話で仕事の電子メールを確認する可能性が高いことが原因です。

マルウェア

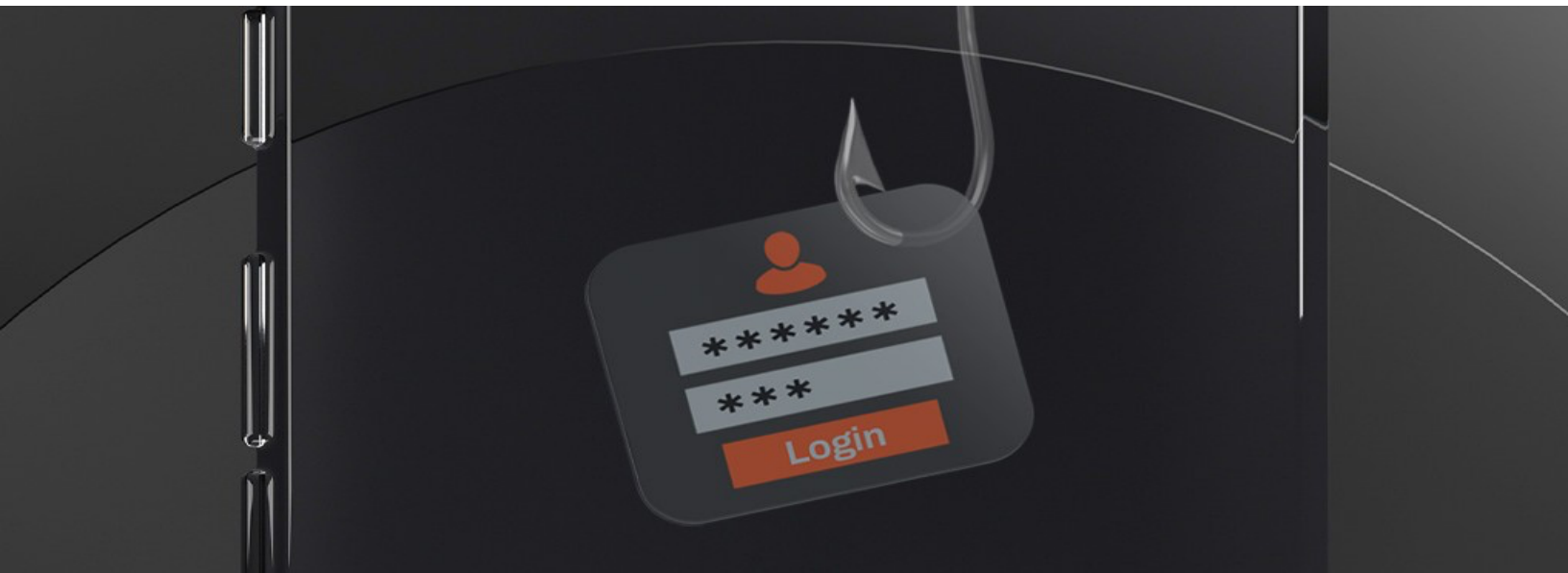
マルウェアは、モバイルデバイスに深刻な影響を与える一般的な脅威です。モバイルエンドポイントの４件中の1件が2021年にマルウェアに感染しています。最近のITとセキュリティリーダーに関する調査によると、52%の組織がウイルスやランサムウェアなどのマルウェア攻撃を経験しています。トロイの木馬は、ユーザーが意識せずダウンロードしたモバイルアプリ中にあったモバイルマルウェアの一例です。

ゼロクリック攻撃

ゼロクリック攻撃は、悪意のあるリンクをクリックするなど、ユーザー側の動作を必要としない攻撃です。ゼロクリック攻撃では、攻撃者は、事前に未知の脆弱性を悪用して、デバイスに独自のエントリポイントを作成することができます。モバイルデバイスでのゼロデイ脆弱性の悪用が増加しています。2021年には、このような攻撃はAndroidデバイスとiOSデバイスの両方で466%増加しました。

不正なWi-Fiネットワーク

モバイルデバイスは、携帯電話サービスが脆弱な場合に任意のWi-Fiネットワークに接続すると、簡単に犯罪者のターゲットとなります。Wi-Fiネットワークは、脅威アクターによって実際に簡単に悪用されています。不正なWi-Fiネットワークは、犯罪者がデバイスを侵害する強力な方法の一つです。犯罪者は、コーヒーショップゲストなどの一般名を持つ偽のWi-Fiネットワークを使用し、騙して信用を得ます。しかし、この不正なネットワークは、アクティビティを追跡したり、情報を盗んだり、マルウェアを起動したりするためのゲートウェイとして機能します。



モバイル固有のセキュリティ考慮事項

モバイルセキュリティには、従来のサイバーセキュリティとは異なる対策が必要であることを理解することが重要です。モバイルデバイスの技術は、従来のエンドポイントとは異なる機能を有しています。そのため、セキュリティ考慮事項が従来とは異なります。以下に、より一般的に引用されているモバイル固有の考慮事項の2つを紹介します：

デバイス状態

デバイスの状態とは、ソフトウェアがデバイスに自由にフラッシュできるかどうか、検証が強制実行されているかどうかの指標です。Androidには、2つの状態があります：ロックとロック解除。一方、iOSデバイスはロックされることになっていますが、ユーザーのルートアクセスを与え、Appleによる制限を迂回するためにジェイルブレイクすることがあります。

ロックされていないAndroidには、セキュリティリスクがあります。Androidがロック解除されている場合、デバイスの物理的な制御を取得する脅威アクターは、デバイスを再起動し、そのデータにアクセスし、それらを維持する意図されたセキュリティ対策をバイパスします。同様に、ジェイルブレイクされたiPhoneは、マルウェアやその他の脅威により影響を受けやすくなります。

脆弱なアプリケーション

モバイルアプリケーションは、私たちのモバイルデバイス上のエンターテインメントの源です。銀行アプリを使うことで財務に関して職場での生産性を維持できます。今日では、120件のアプリがスマートフォンに保存されています。しかし、アプリの脆弱性は、考えられているよりも一般的です。モバイルアプリ開発者のコードは、従業員と顧客データを公開し、プライバシーとセキュリティを危険にさらしています。モバイルアプリは、犯罪者にダウンロードしてリバースエンジニアリングしたり、一般的なブランドを模倣するために再構築したりできます。これには、あらゆるパスワードとSMSメッセージを犯罪者に渡すデバイス上の機密な権限を有効にする意図があります。

脅威検出における機械学習の役割

MTDの積極的なアプローチは、機械学習（ML）によって可能になりました。MLモデルは、アルゴリズムを使用する人工知能の一種であり、情報を収集するにつれてさらに正確な予測を行います。

機械学習モデルは、トレーニングとチューニングによって作成されます。アルゴリズムは、一連のトレーニングデータにさらされています。トレーニングデータは、データセット（脅威データなど）で何を探すべきかというモデルを進化させます。初期トレーニングが行われたら、モデルは、正しい推定が行われるかどうかを確認する前に未知のデータにさらされます。データサイエンティストは、モデルを調整し、それをさらに多くのデータに公開し、学ぶことをサポートします。

脅威検出では、これがどのように見えますか？MLモデルは、攻撃を検出するためにさまざまな方法を使用しています。たとえば、classifierを使用して、リンクがフィッシング詐欺の一部であるか、アプリが実際にはマルウェアである可能性かを判断できます。

最も直接的な脅威検出を得るためには、機械学習はクラウドではなく、デバイス自体にデプロイされ、デバイスがネットワークに接続されていない場合でも保護されることを確認する必要があります。侵入は、ミリ秒単位の一瞬で発生する可能性があります。機械学習アルゴリズムは、ローカルである事が必要です。これにより、できる限り速く稼働し、軟弱なWi-Fiやモバイルサービスによる被害に対応できます。

MTDを実装するためのトップ推奨事項

組織には、MTDソリューションの実装に関して選択肢があります。MTDは、独自で起動したり、他の統合エンドポイント管理(UEM)ソリューションまたはMDMと一緒に使用したりすることができます。

MDMソリューションと使用すると、MTDは、デバイスを管理する代わりに、実際のデバイスをモバイル脅威から保護するモバイルエンドポイントセキュリティ戦略の一部として機能します。**MDMの管理ポリシーは、MTDアプリのダウンロードを促し、MTD検出の有効化など、自動化を可能にし、管理者がMTDソリューションからの検出とポリシーに基づいて条件付きアクセスとセキュリティポリシーを自動化することを容易にします。**

たとえば、ユーザーが不正なWi-Fiネットワーク上にいる場合、MTDは、ユーザーと企業に脅威に対する警告を出します。また、ユーザーが安全なネットワーク上になるまでビジネスクリティカルなアプリへのアクセスをシャットダウンするために、MDMと連動して動作します。

MTDが管理されていないデバイスで独自に使用されている場合、MTDソリューションは、機械学習を使用してモバイルデバイス上の多くの攻撃を特定し、防止します。また、デバイス自体を積極的にスキャンして有害な行動、マルウェア、またはその他の脅威を検出することができます。MTDは、ユーザーに通知しますが、統合されたUEMソリューションの助けを借りずにアクセスをロックするなど、独自で行うことができるのは制御された修正に限られています。

両方のケースでは、脅威はローカルで処理されます。しかし、MTDは企業に報告することも、セキュリティチームが発生したすべての脅威を理解することもできます。ユーザーの受ける障害を大幅に減らすために、MDMでMTDソリューションを補完することを推奨します。両方を配置することで、ユーザープライバシーを保護し、重要なビジネスデータを保護することができます。

結論/推奨

Verizonによると、モバイルデバイスが組織の円滑な実行にどれほど重要であるかを尋ねられたとき、回答者の91%が7点以上、78%が8点以上と回答（合計10点として）しました。2022年モバイルセキュリティインデックスは、組織がどのように機能するかについて、「モバイルデバイスは重要である」と宣言しました。

モバイルセキュリティのコンテキストでは、ブロックと対策をすることとは、モバイルデバイスに対する脅威を見つけて修正することについて積極的に取り組んでいることを意味します。侵入の通知を待ってからでは、すでに遅すぎる状態です。脅威の存在をできるだけ早く見抜くことが重要です。

企業がモバイルリスクを積極的に対処するために、どのようなステップを取ることができますか？

1. モバイルリスクを分析：組織の特定のセキュリティニーズに基づいてリスクを評価し、優先順位を付けます。たとえば、デバイスの盗難は、リスクがどれほど大きいですか？デバイスとのマルウェアやユーザーの個人的な行動についてはどうですか？リスクレジスタを作成することにより、組織に対するリスクを迅速に特定することができます。

2. ゼロトラストを適用：無条件に信頼せず、検証します。今ではアプリケーションがクラウドにあり、モバイルデバイスは職場でますます重要になっています。ゼロトラストは、あらゆるセキュリティ戦略にとって重要です。データとネットワークが安全であることを確認するために、最低限の特権の原則を適用します。

3. MTDへの投資：MTDは、従業員のユーザーエクスペリエンスを損なうことなく、発生した際に、組織がリスクに対処することができます。Gartnerによると、MTDは、企業がより良く、賢く、高速なアクセス決定をするのをサポートするために「ゼロトラストアクセスを提供し、アプリケーション全体でシングルサインオン-を連携させ、テレメトリを生成し続ける手段として自立する」ことができます。

ZimperiumのMTDソリューションが、進化する脅威の状況から組織を積極的に保護するのに役立つ方法に関する詳細については、いつでもお問い合わせください。

推奨書籍

2022グローバルモバイル脅威レポート
モバイルバンキング詐欺：世界経済の脅威ゼロトラスト環境でBYODを実装する方法Verizonの2022年MSIモバイルセキュリティインデックス

ZIMPERIUM

詳細については、こちらをご確認ください：
zimperium.com
お問い合わせ先：844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244