jamf

セキュリティ360：

最新トレンドレポート

2024

要約

Jamfが毎年リリースするセキュリティレポートは、顧客データ、最新の脅威に関するリサーチ、注目すべき業界イベントを基に、サイバー脅威がどのように進化しているかについて徹底的に調査。デバイスを侵害し、ユーザを騙し、組織に侵入し、最終的に重要な企業秘密や個人情報を盗むために活発に利用されている多種多様な攻撃ベクトルについて、思慮深い評価を提供します。本稿の最後には、業界のベストプラクティスと、規模の大小を問わず組織がセキュリティポスチャ全体を改善するために講じることのできるアクションを新鮮な視点でまとめています。

はじめに

Security 360レポートは、進化する脅威に幅広い視点からアプローチし、実際のデータを基にその年、最も影響を与えた攻撃ベクトルを分析するとともに、セキュリティベストプラクティスに対する組織の取り組みを評価。さらに生産性を高め、従業員をこれまでにない大胆な方法でつなぐアプリケーションについて調査します。

レポートでは、世界中の組織が効果的な管理に取り組むリスクを4つのカテゴリーに分けて分析します：

I. デバイスリスク

II. アプリケーションリスク

III. マルウェアリスクと攻撃の進化

IV. Webベースリスク

これらの脅威トレンドに加えて、業界のベストプラクティスをデバイス、アプリケーション、インフラストラクチャ管理プロセスに組み込むことを推奨する専門家の"基本回帰"的なアドバイスについても取り上げます。

以下にそれらベストプラクティスの例を幾つか紹介します：

- 管理とセキュリティが一体化した製品を使用し、保守管理しなければならないエージェントの数を最小限に抑えつつ、利用可能なポリシーコントロールを最大化する。
- 業界または地域のベストプラクティスに従ってエンドポイントを強化する。
- オペレーティングシステム（OS）とアプリケーションのリリースおよびパッチを最新の状態に維持することで脅威への露出を抑える。
- 多層防御を実装する。

このレポートを通じて、組織が既知の脅威に対する防御を強化しながら、同時に新たな攻撃への露出を減らすためのアドバイス、さらに進化を続けるソーシャルエンジニアリングに着目し、ますます巧妙化する攻撃からユーザを守るためのヒントを提供します。

最後に、Jamfのリサーチおよびアドバイスは、Apple、Microsoft、AndroidなどOSの種類、また会社所有のデバイスかBYO（Bring Your Own）デバイスかに関係なく、ビジネスデータを扱うすべてのデバイスに適応します。

360レポートについて

私たちは、現代のワークプレイスに影響を及ぼす最重要セキュリティトレンドについてもっとよく理解したいと考えています。

これには複数の生産性パズルのピース、つまりデバイス、ユーザ、アプリケーションが関係しており、それらを全て結びつけて総合的に理解する必要があります。キートレンドに関する情報、本稿で使用する統計データ、そしてそれらの組み合わせ方は、弊社の顧客ベースにおけるセキュリティトレンドの分析に加え、Jamf Threat Labsチームが独自に実施したOSやアプリケーションの脆弱性に関する調査から導き出したものであり、4つそれぞれのセクションで悪意のある攻撃やPoC（Proof of Concept）攻撃について掘り下げます。

調査方法

今年のレポートで明らかになったセキュリティトレンドが実際に与える影響を理解し、定量化するために、Jamfが保護する1500万台のデスクトップコンピュータ、タブレット、スマートフォンデバイスのサンプルを調査。

分析は2023年第4四半期、直前の12ヶ月間を対象に、90の国と複数のプラットフォーム（macOS、iOS/iPad、Android、Windows）にわたって実施されました。

データを収集し取り扱う際のプライバシー保護と高いセキュリティ基準を維持するため、調査で分析されたメタデータは個人情報や組織を特定する情報を含まない集約されたログから得られたものを使用しています。

重要な理由

この分析の意図は恐怖心を煽ることではなく、進化するサイバーセキュリティトレンドや、デバイスや組織のセキュリティポスチャにさらなる影響を与える可能性を持つトレンドについて、企業やユーザの皆様と情報を共有することです。さらにデバイス、ユーザ、組織データのあらゆる側面を保護する、エンドポイントセキュリティのベストオプションやセーフガードの大規模な活用法についても解説します。

セクション 1: デバイスリスク

ワークコンピューティングが最新化されるのにつれて、従業員が日々使用するデバイスは著しく複雑化し、コンテキスト情報を検出する内蔵センサー、重いコンピューティングサイクルをオフロードしてより高いパフォーマンスを達成するコプロセッサ、さらにBluetooth、NFC、WiFi、セルラーなど接続の増加がこの複雑性を高める原因となっています。これらの追加は、概して、すべて善意に基づいて行われており、ともすれば見過ごされがちですが、それぞれの要素はアタックサーフェスを広げるという副作用を伴います。

現代のデバイスにはさまざまなリスクが存在します。しかし幸いなことに、大半の組織はこうしたリスクを適切なツールとプロセスによって効果的に管理することができます。

各デバイスで最新のオペレーティングシステムを維持することは、おそらく組織が実施できる最もインパクトのある、そして唯一の方法ですが、誰もがイノベーションのスピードについていけるわけではありません。

コンフリクトの恐れや、アップデートのたびに互換性をテストしなければならない過剰な数のエージェントなど、ソフトウェアアップデートの適用を遅らせる理由は数多くあります。しかし、OSのアップデートを行わなければ、既知の脆弱性を放置した、悪用されても仕方のない状態でデバイスが稼働している可能性が高いことを意味します。

これらの脆弱性は、デスクトップやノートパソコン以外にも影響を及ぼします。Jamfの調査では**モバイルユーザの40%が既知の脆弱性を持つデバイスを使用**していました。より重要なビジネスアプリケーションがモバイルデバイスで実行されるようになる中で、これら機密データ保管庫はますます標的にされていますが、より良いプラクティスによって効果的に攻撃を撃退できる可能性があります。

2023年の調査結果

"8%の企業でモバイルデバイスが外部のアプリストアにアクセスしていた"

"モバイルユーザの40%が既知の脆弱性を持つデバイスを使用している"

2023年の調査では"8%の企業でモバイルデバイスが外部のアプリストアにアクセス"していました。アクセスする意図に悪意がなくとも、外部のアプリストアは、巧妙な表現でユーザーをミスリードし、内部セキュリティを崩壊させる不審なアプリをダウンロード、実行させようとするアプリケーションで溢れています:

デバイス上で悪意のあるコードを実行
GatekeeperやエンタープライズセキュリティAPIなどの機能が悪意のあるコードの実行を阻止する

内部のセキュリティ保護をバイパス
セキュリティ審査なくデバイス上で実行されるアプリケーションを制限したい理由

権限のないビジネスデータにアクセス
機密情報は依然脅威アクターが狙う主要なターゲットのひとつ

許可なくプライバシーデータを取得
AppleのTTC（Transparency, Consent and Controls）がインストールされた不正なコードによって回避されたことが明らかとなり、プライバシープ保護はエンドポイントセキュリティにとって極めて重要であり

ユーザに無断で、あるいは同意なしに監視
先述した通り、モバイルデバイスは常に私たちの手元にあるため、脅威アクターはますますモバイルデバイスを標的とするようになっており、モバイルの常にコネクトされている特性を利用して会話を盗聴、SMSを傍受、GPSで物理的な動きを追跡する

感染デバイスからネットワークに不正侵入
悪意のあるコードがインストールされた次への段階として起こる

コンプライアンスの設定

コンプライアンスとは一般的に、CISベンチマークやNIST規格のような、データのプロセス、使用、保管に関するガイドラインに整合させることですが、組織には独自のニーズやアプローチがあります。よってここでは、デバイス設定、データセキュリティ、ユーザワークフローを脅威アクターから守るため、実装しているシステムに整合するようそれらを標準化させること全般をコンプライアンスと呼びます。

Apple独自のセキュリティ機能のコンプライアンストレンドに関するキーポイント：

FileVault：ストレージ内のデータを暗号化することでユーザデータを保護するこの基本機能は、MDMソリューションにより導入、設定、暗号化キーの管理が容易にできるにもかかわらず、調査対象**"デバイスの36%で無効化"**されていた。

Gatekeeper："App Storeおよび認定デベロッパのアクティベーション率90%"を誇るGatekeeperは、悪意のあるソフトウェアのインストールを防ぐ重要なセキュリティレイヤー。**Appleはデベロッパが収集を公表しているデータのみを収集しているか各アプリを検証しており、Gatekeeperはこのユーザープライバシー保護の基礎となるセキュリティ機能である。**

ファイアウォール：多くのモバイルデバイスがWebベースの脅威によってハッカーの標的にされている**ことを考慮すると、"Macの55%でファイアウォール機能が無効化されていた"のは憂慮すべき事実。**MDMソリューションにより簡単に導入できるファイアウォールを有効にすることは業界のベストプラクティスであり、デバイスが許可されていないアプリケーションやサービスから接続されるのを防ぐ。

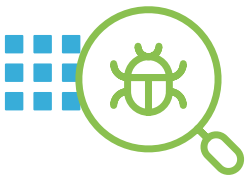
画面ロック： データに対する許可されていないアクセスを防ぐとともに、ローカルに保存されている全データの暗号を解くキーとしても機能するモバイルデバイスの基本機能。**2023年は"デバイスの3%でロック画面が無効化されており、ロック画面を無効化したユーザが1人でも存在した組織の割合は25%にのぼった "。**

セクション II：アプリケーションの利用とリスクの拡大

アプリケーションの脆弱性管理

最新のハードウェアで最新のOSを実行する真新しいデバイスであっても、そのデバイスで実行されるアプリケーションが古く、攻撃者に度々悪用されているバグが含まれていれば、攻撃に脆弱な可能性があります。ハードウェアとOS、そしてデバイス上で実行されるアプリケーションの全てで脆弱性を管理することが不可欠です。

Jamfの調査では"2023年、デバイスの2.5%に脆弱なアプリケーションがインストール"されていました。割合としては少ないですが、**2023年末時点の世界のモバイルデバイス推定台数168億台**にこの数値を当てはめると、世界全体で約4億2000万台の脆弱なデバイスが存在することになります。



2.5%の
デバイスに脆弱性のあるアプリケーションがインストールされていた。

2種類のアプリケーション

脅威に関する調査を通じて、組織では根本的に異なる2つのタイプのアプリケーションが使われていることが明らかになりました。ネイティブ（オンデバイス）アプリケーションはデバイスリソースを利用してコードを実行し、エンドユーザに機能を提供するのに対し、Webアプリケーションはインターネット上（通常はSaaS環境やプライベートクラウド上）にホストされ、処理やデータストレージはデータセンターやリモートサーバで行います。

Jamfの調査は、どちらのアプリケーションタイプであってもリスクは不可避であることを示しています：

- 脆弱性はアプリケーションソフトウェア内で管理される必要があります。クラウドでホストされるアプリケーションはネットワークに接続されているというその特性から、デバイス上にあるアプリケーションよりも遠隔から改ざんされるリスクが高まります。
- デバイスとリモートアプリケーションの間には複数のネットワークが存在しています。よって、クラウドホスティングアプリケーションのリスク管理において最も重要なのは**転送中のデータ保護**です。
- **保存データの保護は**、どちらのアプリケーションタイプにおいても重要です。クラウドホストティングアプリケーションは一般的にデータセンター境界で保護されますが、最近のアプリケーションはオープンソースソフトウェア、共通基盤、共有のコンピューティングリソースで構築されるケースが増えています。

組織が管理するデバイスについては、常時モニタリングすることでこれらのエンドポイントについて洞察を得ることができますが、個人所有のスマートフォンのような管理されていないデバイスについてはどうでしょうか？確かに違いはありますが、管理デバイスと非管理デバイスの両方に当てはまることもあります。例えば：

- どちらにも脆弱性がある。
- どちらもセンシティブデータを保管する。
- すべてを管理する必要がある。
- アプリケーションとビジネスデータを許可されたユーザのみに制限する理想的なセキュリティを実現するには、リアルタイムのリスクベースのアクセスポリシーが不可欠。

つまり、インフラを包括的に保護するための選択肢はただひとつ：それはそれぞれのアプリケーションタイプを理解し、Webベースとオンデバイスアプリのリスクに対処するレイヤードセキュリティ保護を実装することです。

デバイスおよびアプリケーションの管理機能にセキュリティツールの能力と洞察を融合した、より統合的なITプログラムを導入することで、組織はよりレジリエントな職場を実現できます。そのカギとなるのが、深層防御型のセキュリティ戦略であり、デバイスのリスクポスチャの変化に対応する補完的制御を組み込むことで、インフラ全体を網羅するホリスティックな保護を提供。同時にビジネスデータは、Webベースアプリの各リクエストに固有のセキュアなトンネルを介してルーティングされます。

加えて、さらにもう一層のセキュリティコントロールで上記を管理と結びつけ、より堅牢な構成プロファイル、管理されたアプリ実行、自動化された脆弱性修正ワークフローによってコンプライアンスを強化。デバイスの種類、所有形態、ネットワーク接続に関係なく、ベースラインを提供、および基本レベルのデバイスセキュリティを実装し、生産性を維持します。

最も利用されているクラウドホスティングビジネスアプリ

Microsoft　Google　Dropbox

Adobe　Box　Slack　Okta

Atlassian　Salesforce　Zoom

脆弱性およびリスクの管理

サードパーティのアプリストアからアプリケーションを入手する際、無料ダウンロードは確かに魅力的ですが、ユーザが求めている以外のものが付いてくることが少なくありません。Jamfが実施したプラットフォーム別の調査では、サードパーティアプリのダウンロード数はAndroidがiOSよりも2倍多く、

またAppleはハードウェアとソフトウェアラインの両面からセキュリティおよびプライバシー保護の強化を続けていますが、今回の調査結果は、増加する標的型の脅威はAppleにとっても無関係ではないことを示唆しています。

"Androidのサードパーティアプリダウンロード数はiOSの2倍"

ビジネスデータセキュリティと最新デバイス

ワークライフバランスと、リモートワーク／ハイブリッドワークを可能にするモバイル技術によりデータセキュリティは新たな局面を迎えており、メリットとデメリットは表裏一体となっています。例えば、在宅医療を行う医療従事者が使用するデバイスの場合、デバイスに保存された患者の記録、つまり保護医療情報（PHI）は、米国のHIPAA法によって保護されています。モバイルデバイスは外出の際、非常に便利ですが、一方で攻撃者はデバイス内に保存されているデータに加えて、デバイス自体も比較的容易に盗むことが可能です。簡単に言えば、ユーザが持ち運びやすいデバイスであればあるほど権限のない者が盗みやすくなるということです。

より手軽＝より大きなリスク

今日のデバイスは、必ずしも会社所有や会社支給のデバイスである必要はありません。利用可能なデバイス台数、ソフトウェアのライセンシングコスト、従業員選択プログラム、使いやすさなど、さまざまな要因から、業務で使用されるデバイスは個人所有のものと会社支給のデバイス&アプリが混在している場合が多く、最新のITおよびセキュリティ標準を採用し、組織の要件を満たした認可デバイスを使用する、許可されたユーザのみがセンシティブリソースやアプリケーションにアクセスできるようにすることが不可欠となります。

このためビジネスデータセキュリティに影響を与える最も重要なトレンドのひとつは、以下の2つに関するリスクです：

- BYOD（私物端末の業務利用）モデル
- シャドーIT

どちらも全てのデバイスタイプ、およびプラットフォームに懸念をもたらします。ユーザごとに使用するデバイスやプラットフォームは多様ですが、いずれにおいても可能な限り高い生産性を確保できるようにする必要があります。ユーザに力を与えることは、生産性を向上させる上で必須です。しかし、この統一性の欠如はさまざまなソフトウェアツールやサービス（そのすべてがさまざまなリスク要因を持つ）の混在を招き、データセキュリティが究極の代償を払うことになります。例えば、Google Chrome、Microsoft Edge、Mozilla FirefoxのようなWebブラウザは、ユーザが調べ物をしたり仕事をしたりするためのWebサイトをレンダリングするという重要な機能を毎日、毎分担っています。しかし、複数のアプリに各アプリの異なるバージョン、さらに各バージョンに関連するCVE（共通脆弱性識別子）を掛け合わせると、組織のリソースにアクセスするために使用されるデバイスフリート全体に存在する脆弱性の数は計り知れない数に増え、結果として、ビジネスデータは仕事や学校で使用される無数のデバイスで処理されています。

シャドーITは、アプリのサイドローディングなどユーザーがセキュリティ保護を回避してしまう恐れ、あるいはユーザーが（完全に審査されていない、または安全性が担保されていないバージョンのアプリを使用するリスクからビジネスデータでの利用が認められていない場合でも）自分の好きなクラウドベースアプリに依存ししまう恐れがあり、長い間悩みの種でした。Jamfの調査によると、仕事用デバイスにインストールされたサイドローディングアプリで最も多かったのはOnionとTorでした。どのアプリを自前のデバイスにダウンロードし、使用するかユーザー自身が決定権を持つ個人所有のデバイスでは、ソーシャルメディアプラットフォームにリンクされたメッセンジャーアプリが脆弱なアプリのトップ20にランクインしました。昨今、偽の求人情報を通じて、**脅威アクターがソーシャルメディアで被害者をエクスプロイトする**ケースが増えていることがその背景にあります。このような偽プロファイルは、DMでターゲットに直接接触し、暗号通貨投資に関する詐欺をおこなったり、もっともらしいデマを流したりしています。

シャドーITのモニタリングは、企業デバイスに関するコンプライアンス管理のひとつです。個人デバイスにおいては、デバイスが適切に構成され、業務に使用できる状態になっているだけでなく、ビジネスアプリと個人アプリのデータの流れを管理するポリシーなど、各種ポリシーが組織の基準に従って管理されていることを確認する必要があります。

ここでのキーポイントとは、ITチームとセキュリティチームは、ビジネスリソースを保護し、許可されたユーザのみにアクセスを制限することが仕事ですが、業務用と個人所有、さまざまなデバイスが混在していることはセキュリティに影響を与える変数であるということです。より大きなリスクをもたらすのは、企業がオープンアクセスを許可し、どこからでもアクセスできるようにしたアプリケーションです。この場合、ユーザの生産性を阻害しないように、企業は会社支給のデバイスでなくてもアクセスできるようにしています。さらに事態を泥沼化させているのは、ただ自分が楽をしたいがために、一部の従業員がポリシーを守っていないことです。例えば、業務データが保管されているクラウド上の場所を制限したいので、業務ネットワークが特定のサービス（例：クラウドストレージA）へのアクセスをブロックしているにもかかわらず、従業員が個人デバイスを使って機密ドキュメントを別のサービス（例：クラウドストレージB）に置いた場合、その従業員はポリシーに違反し、データを危険にさらしたことになります。

このような理由から、ユーザ認証、デバイスアセスメント、セキュアな接続を連携させるポリシーを導入することがベストプラクティスとなります。デバイスの種類、物理的な場所、オーナーシップモデル、OSプラットフォーム、ネットワーク接続に関係なく、各レベルでデバイス、ユーザ、データのセキュリティと管理を行う、深層防御戦略で保護を重ねることにより、管理、アイデンティティ、セキュリティのギャップを埋めることが必要です。

セクションIII：マルウェア解析と攻撃の進化

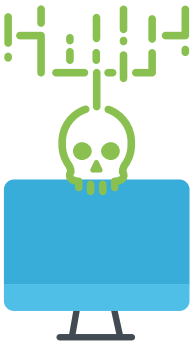
このセクションでは、2023年、組織に最大の脅威を与えたマルウェアの種類と、その頻度について詳説し、プラットフォームに影響を与える攻撃の継続的な進化と、悪質な行為者がどのようにOSレベルのツールの脆弱性を狙い、ユーザに誤ったセキュリティ意識を抱かせているかについて取り上げます（詳しくはこのセクションの後半で解説）。

macOSの脅威

ユーザーはオンラインで直面するリスクを見逃しているかもしれませんが、組織はビジネスアプリケーションの利用が増えたことで、ユーザがこれまで以上に標的にされやすくなっていることを理解しています。

ご存じですか？

"Macユーザの57%が「マルウェアはmacOSには存在しない」という主張に賛成、あるいはある程度同意しています。**The Hacker Newsが報じた調査結果**では、2023年"Macユーザの3人に1人が自分のデータはサイバー犯罪者にとって興味がないと考えている"ことが明らかとなりました。



21

Mac上で特定された 新たなマルウェアファミリ

Macはウイルスに感染しないという神話が根強い一方で、Jamf Threat LabsはmacOS上で約300のマルウェアファミリを追跡。実際、2023年には21の新しいマルウェアファミリがMacに出現しました。

以下は、2023年に調査およびカウントされたマルウェアの内訳です：

マルウェアカテゴリ	全Macマルウェアに占める割合(%)
アドウェア	36.77
PUA	35.24
トロイの木馬	17.96
エクスプロイト	4.40
ランサムウェア	2.00
ダウンローダー	0.92
ハックツール	0.67
コインマイナー	0.64
証明書付きマルウェア	0.64
ドロッパー	0.56
インフォスティーラー	0.25
スパイウェア	0.23
マルウェア	0.20
キーロガー	0.04
ネットワーク	0.026
ウイルス	0.01
ローグウェア	0.01
ハイパーリンク	0.01

カテゴリはMacマルウェア全体に占める割合が高いものから低いものへと順番に並んでいます。ここからは、今回発見されたマルウェアに関して興味深いデータをいくつか紹介します。まずはPUA（望ましくない可能性のあるアプリケーション）です。このカテゴリーはアプリケーションがユーザーによって意図的にインストールされたものであるがそれ以外の点では無害である可能性、または検出を隠すためインストール中、意図的にユーザーから隠されたものである可能性があり、定量化が難しく、このような不確定要素があるため、ユーザはMac内で発生する意図しないアクションに警戒し続ける必要があります。

過去1年間にわたり、非常に多くのトロイの木馬ファミリが検出されました。この結果は、このタイプの悪意のあるコードのパッケージングと実行が非常に多様化していることを表し、マルウェア作成者の多さも裏付けています。**17%と"トロイの木馬"**は、macOSマルウェアコミュニティの中で人気が高まっている重要なリスクです。「悪者はシステムに何を挿入しているのか？」「なぜこのような戦術を使うのか？」考えてみましょう。結局のところ、トロイの木馬とは、内部に悪いものを隠したソフトウェアと定義されます。つまり必要なのは、脆弱性の管理だけでなく：

- 正規ソースからのアプリケーション取得
- （AppleのApp Storeなど信頼できるサードパーティ、または組織独自のセキュリティチームを通じた）審査プロセスの適用
- 最新のセキュリティソフトウェアの実行

Atomic Stealer

Telegramで宣伝されたAtomic Stealerは、攻撃者用のWebインターフェースを備えたMaaS（Malware-as-a-Service）です。情報窃取に特化し、アカウントパスワード、ブラウザデータ、セッションクッキー、暗号通貨ウォレットなど、さまざまな機密データを流出させることができます。特にAtomicはAppleScriptのダイアログ機能を悪用し、ユーザを騙して認証情報を提供させます。ユーザのパスワードが入力されると、macOSキーチェーンからさらに追加の機密データを盗み出します。このマルウェアはTor Browser、Photoshop CC、Notion、Microsoft Officeなどの正規アプリケーションを装って配布され、Google Adsのマルバタイジングを通して配信されていることも確認されています。

KandyKorn

このマルウェアは、朝鮮民主主義人民共和国の脅威アクターがブロックチェーンエンジニアを標的とした、より大規模で洗練された攻撃の一部として発見されました。攻撃者はDiscord上の偽のボットを介して多段階的なマルウェア攻撃を展開。最初の侵害では、さまざまな悪意のあるPythonスクリプトが関与し、追加のマルウェアコンポーネントをダウンロード。続いてPythonスクリプトはマルウェアの次の段階へのドロッパーとして機能し、C2サーバへの接続を確立。その後、反射型のバイナリ読み込みなど永続化や防御回避テクニックを採用した追加段階のマルウェアが使用され、最終的にはKandyKornマルウェアがメモリ内で実行されました。

JokerSpy

BlueNoroff APTグループによるものとされるJokerSpyは、日本の暗号通貨取引所を標的としていたところを最初に発見されました。このマルウェアは、侵害されたシステムにスパイウェアを送り込むために様々なバックドアを使用し、偵察のためにオープンソースのツールを使用します。Pythonスクリプトのバックドアによりダイナミックなコンフィギュレータの読み込みやコマンドの実行ができるようになり、悪意のある多様なアクションを可能にします。システム権限の評価に加え、JokerSpyはAppleのTCC（Transparency, Consent and Control）設定を悪用することが知られています。また、レッドチーム演習でよく使用されるオープンソースのmacOS向けポストエクスプロイト偵察ツールセットであるSwiftBeltを実行する可能性もあります。

Lockbit

Apple製品を標的とした主要なランサムウェアグループの最初の事例であり、VXUndergroundがマイルストーンとして評するLockBitは、Linux版のApple移植版が2022年前半に登場しました。初期のサンプルではアドホック署名が表示され、実行時に無効な署名ポップアップがトリガーされました。最新の情報では、LockBitはまだデータを流出させず、依然開発が活発に進んでいる考えられており、機能性が追加される可能性があります。実行に成功すると、このランサムウェアはオープンソースのライブラリを使用してファイルを暗号化し、ファイルシステムに身代金のメモを残します。

NokNok

NokNokは、イランの脅威アクターによるAPTマルウェアチェーンであり、被害者システムでの偵察とバックドア設置を目的として設計されています。攻撃者は、Royal United Services Institute (RUSI)になりすました標的型フィッシングメールを使用し、被害者にRUSIの名を冠した悪意のあるVPNアプリケーションをダウンロードするよう誘導します。インストールされると、NokNokはbashスクリプトを活用してバックドアを設置。サーバコマンドを受信し、自己終了または追加モジュールの実行を行います。これらのモジュールは、実行中のプロセス、システム情報、インストールされているアプリケーションのデータを収集し、パーシステンスを確保することもできます。確実なデータ伝送のために、NokNokは独自の暗号化を採用。さらにBase64のエンコーディングとセグメンテーションによって難読化されています。

iWebUpdate

iWebUpdateは、リモートサーバから任意のペイロードを取得、実行するように設計された継続的なダウンローダーです。iwebupdate.plistという名前のユーザ起動エージェントを通してパーシステンスを維持。起動すると、system_profilerなどのコマンドを実行して偵察。またOSのバージョン情報を収集し、コマンドやコントロールサーバーに送ります。ペイロードは/tmp/iwup.tmpの一時ファイルにダウンロードされ、解凍され、その後実行されます。このマルウェアは1時間ごとにサーバをチェックし、タスクを追加 します。

ObjCShellz

ObjCShellzは、BlueNoroff/Lazarus APTグループによるObjective-Cバックドアで、攻撃者は侵害されたシステムにシェルコマンドを発行することができます。コマンド&コントロールサーバとの接続を確立すると、シェルコマンドの実行が許可され、その結果が攻撃者にリレーバックされます。このマルウェアは、暗号通貨に特化した小規模な企業を標的とすることが多いBlueNoroffの活動、RustBucketキャンペーンの一部としてJamf Threat Labsによって初めて特定されました。

PureLand

PureLandは、合法なインディーズビデオゲーム "PureLand "の海賊版に埋め込まれた情報を盗むマルウェアです。このトロイの木馬化されたゲームは、メールで配布され、ユーザがプレイすると暗号通貨の生成を約束します。実は、PureLandはRealst Stealerと同時に発見されました。Realst Stealerは、非常によく似たソーシャルエンジニアリングの手口を用いるマルウェアですが、最終的なペイロードは異なります。

Realst Stealer

Realst Stealerは、情報窃取に特化したRustベースのマルウェアで、主に侵害されたシステム上の暗号資産を狙います。このマルウェアはあまり知られていないビデオゲームに巧妙に埋め込まれていました。攻撃者はこれらのゲームへの特別先行アクセスを提供するとして個人に接触し、暗号を獲得するNFTベースのチャンスとして提示。ユーザがゲームを起動すると、Realst Stealerが起動し、システムを侵害し、暗号を盗むルーチンを開始します。

Rustbucket

RustBucketはリモートアクセスのトロイの木馬です。トロイの木馬は金銭的な利益よりもスパイ活動に重点を置いていることが多いですが、攻撃者のオブジェクトによっては重複するものもあります。一般的に、リモートシェル機能、キーロガー、情報窃取など、複数の異なる機能性を含んでいます。

APTグループBlueNoroff（有名なLazarus Groupの北朝鮮サブグループ）が使用するRustBucketは、複雑なソーシャルエンジニアリングキャンペーンによってユーザを狙う多段階的なマルウェアあり、最初のドロッパーはObjective-C、Swift、AppleScriptで書かれ、最終的なペイロードはRustで作られています。典型的なキャンペーンでは、マルウェアは良性のPDFリーダーを装います。ユーザは、この不正アプリケーションを使用して特定のPDFドキュメントを開くように誘導され、攻撃者のCommand and Controlサーバへのコールバックが開始されます。

WTFMiner

WTFMinerは、海賊版macOSアプリを通じて拡散する検出回避機能を持つクリプトジャッキングマルウェアです。その起源は、2019年以降、マイナーを複数の海賊版macOSアプリケーションにバンドルしたトレントアップローダーにさかのぼることができます。Jamfはコピーを入手することで、3世代にわたる段階的な開発を図式化。各バージョンで追加のステルス技術を採用していました。ダークWebルーティングを使用してステルス通信を行い、自身を正当なプロセスとして難読化し、アクティビティモニターが開かれるとシステムが終了。最新の亜種は、ディスクへの永続性の書き込みを回避し、ユーザがトロイの木馬化アプリを起動してマイニングを開始することに依存しています。

調査では、ランサムウェアが、そのファミリ数は最も少ないにもかかわらずこの分類に属するマルウェアが多数確認されたため、新種マルウェアリストのトップ5にランクインしました。昨年はTurtle RansomwareやLockbit for macOSなど、いくつかの新しいランサムウェアファミリが発見されましたが、Jamf Threat Labsによると"ランサムウェア"とラベル付けされたサンプルのほとんどは、もともと2020年に発見されたEvilQuestランサムウェアに引き続き属しています。

興味深いことに、多くの人は、EvilQuestのサンプルは主にサンドボックスのバグによって生成され、サンプルに微小な違いが生じ続けていると考えていますが、このランサムウェアは、2020年に発見されて以来、被害者に積極的に配信されていません。

実際に見つけたマルウェア

カスタマー環境において新たに確認されたマルウェアをより詳細に見ると、以下のマルウェアファミリがトップ10にランクインしています：

順位	ファミリ	総目撃件数に占める割合(%)	カテゴリ
1	genieo	13.63	アドウェア
2	imobie	12.25	PUA
3	generic	10.02	アドウェア
4	multiverze	6.84	アドウェア
5	tnt	6.19	PUA
6	ccleanmac	5.28	アドウェア
7	mackeeper	4.55	アドウェア
8	pirrit	4.45	アドウェア
9	macinformer	4.37	アドウェア
10	installcore	3.98	アドウェア

モバイルの脅威

Macはマルウェアと無縁であるという誤解がありますが、モバイル脅威、特にiOSなどプラットフォームにおける脅威は本物であり、単純な統計で定量化することは困難です。セキュリティ専門家は、これらの脅威がビジネスデータやユーザプライバシーに与える現実的な影響に直面しています。このセクションの後半では、2023年にセキュリティ研究者が発見した驚くべき事実を紹介すると共に、これらのモバイル脅威の詳細な性質について解説します。

注記: Jamfの調査結果に基づく、このセクションで用いられているパーセンテージは、特に本レポートの他のセクションと比較した場合、著しく低く見えるかもしれません。しかし"本を表紙で判断してはいけない"という慣用句はサイバーセキュリティにおいて特に重要です。なぜなら:

- 国連の推計によれば、**世界人口は2022年に80億人に到達**。
- 2023年現在、**世界のモバイルデバイスの総数は168億台と推定さ**れ、さらに 増加。
- **自宅でデスクトップまたはノートパソコンを使用する世界のユーザ** の割合は、前回2019年のレポート時と同じ47.1%で推移。
- **世界の1人当たりの平均デバイス所有台数**は3.6台。

人口、デバイスタイプ、1人当たりの平均デバイス台数の統計が、なぜ現代のモバイルセキュリティ脅威の影響を理解する上で重要なのでしょうか。Jamfの調査で示される数字には重要な意味があります。

> "2023年は、デバイスの**1%**、組織の**2%**がデバイスフリート内に潜在的に望ましくないアプリをインストールしていました。"

前述したように、1%は深刻な数値ではない、というよりも 気にするまでの数値でないように見えませんか?

しかし、それは間違っています。上記の統計に外挿することで、これらの割合が実際にはどれほど重要なものであるかを正確かつ現実的に把握することができます。

まず、現在世界中で使用されているモバイルデバイス台数から計算してみましょう。168億台の1%、すなわち1億6,800万台のモバイルデバイスにマルウェアがインストールされていることになります。では次に、世界人口80億人に目を向け、PCユーザ47.1%を除外して、モバイルユーザのみの数字に絞り込むと、37億6,800万人の潜在的モバイルデバイスユーザがいることになります。最後に、ここが少し厄介なのですが、絞り込んだユーザ数に、1ユーザあたりのモバイルデバイス平均所有台数3.6台を掛け合わせると、全世界で136億台になります。

さて、136億が168億より少ないことは、数学の達人でなくても一目瞭然ですが、ここからがややこしい部分です。世界平均とは、ひとつの世界的な指標を決定するために、各エリアを平均した数値です。しかし、ベースラインは地域によって異なり、中南米（3.1台）のように世界平均を下回る地域もあれば、西ヨーロッパ（9.4台）や北米（13.4台）のようにそれぞれ世界平均の3倍から4倍の地域もあります。地域差を調整するために数字を再計算すると、上記の地域別モバイルデバイス数は以下のようになります：

- ラテンアメリカ：11,680,800,000台
- 西ヨーロッパ：35,419,200,000台
- 北米：50,491,200,000台

ここからもうひといき！最後の計算です。ここで、モバイルデバイスのわずか1%がマルウェアに感染しているとするマルウェア感染率を、地域別に調整した値に外挿するとどうなるかを再考してみましょう：

- ラテンアメリカ：131,192,000台
- 西ヨーロッパ：397,808,000台
- 北米：567,088,000台

悪意のある攻撃者がデータ侵害を実行するには、どのデバイスでも（わずか1台でも侵害できれば）十分であることを忘れてはなりません。

攻撃の進化

2023年、Jamf Threat Labsチームは、iOS ベースのモバイルデバイスとそのユーザを標的とした複数の異なる複雑かつ強力なモバイル脅威を発見しました。

モバイルデバイスはAppleプラットフォームのみで構成されているわけではありませんが、Jamfの調査は、脅威アクターがiOS/iPadOSプラットフォームを侵害するための斬新で検出が困難な攻撃の開発に向け、かなりの技術リソースを投入し、Appleエコシステムを標的とする傾向が強まっていることを繰り返し強調しています。

Apple は、セキュリティとプライバシーをデザイン哲学の重要な柱とすることで、この面での守りをリードしてきました。**消費者や企業データに対するモバイル脅威**についての同社調査によると、"データ漏洩の総数は2013年から2022年の間に3倍以上増加し、過去2年間だけで26億件の個人データが流出"しており、"2023年はさらに悪化する"と指摘しています。

ソーシャルエンジニアリングの進化

モバイル脅威は極めて現実的です。多くの新しいサードパーティアプリやサービスが年々一般化し、進化していますが、Jamf Threat Labsチームはこれを裏付ける、2023年新たに登場したiOSのセキュリティ脅威、ソーシャルエンジニアリング2.0を発見しました。

Pegasusの発見

Jamf Threat Labsは4月、Pegasusによって侵害された2台のデバイスに関する詳細な調査結果を公表しました。1台目は中東の人権活動家が所有していたiPhone 12 Max Proで、"複合的な侵害の指標とPegasusとの明確な関連性から分析の宝庫である"ことが判明。"ユニークな侵害の指標（IOC）とアクティブなスパイウェアキャンペーンの証拠 "が示されました。

さらにJamfは2台目となるデバイス、世界的な通信社に勤める欧州のジャーナリストのiPhone 6sのファイルシステムを解析する中で新たなIOCを発見。調査から脅威アクターは古いデバイスをターゲットにし続けていることが明らかになり、"組織のインフラの脆弱性を悪用し、あらゆる攻撃を仕掛けてくる"ためには手段を選ばないことを思い知らされました。

偽の機内モード

8月、Jamf Threat LabsはiOS 16でパーシステンスを実現するためのポストエクスプロイト技術を開発しました。UIを編集して適切な画面上のアイコンを表示すると同時に、すべてのアプリへのインターネット接続を切断することで、攻撃者はユーザを騙して機内モードが有効になっていると思わせ、実際には悪用されたiPhoneやジェイルブレイクされたiPhoneでデバイスへのネットワークアクセスを維持します。

機内モードは、旅行中のプライバシーと特定の規制へのコンプライアンスをさらに強化し、セキュリティとプライバシーを重視するユーザに安心感を提供します。しかし、この機能性を変更、インタラプトすることで、潜在的な脅威者は攻撃の連鎖に沿って移動しながら、影響を受けたiOSベースのデバイスへの不正アクセスを維持し、この攻撃の被害者は知らないうちに自分のデバイスが危険にさらされる可能性があります。

偽のロックダウンモード

12月、Jamf Threat Labは、ユーザの安全性、セキュリティ、プライバシーにとってより重大な結果をもたらす前述の概念実証に続く新たな技術の検証を行いました。Appleのロックダウンモードに注目した、この改ざん技術は、通常このサービスによって実装されるはずの機能性が一切実装されていない状況でありながら、ユーザーにはこのモードに関するすべての視覚的な合図を提供します。

デバイスに侵入した攻撃者は、悪意のあるコードを埋め込んで、ここで説明した攻撃を実行。ロックダウンモードを有効にすると、脆弱なデバイスの高リスクユーザは、ロックダウンモードの視覚的な合図を実装する攻撃者のコードを気づかずにトリガーしますが、デバイスの構成は何も変わらないのでエンドユーザにはiPhoneがある程度保護されているように見えます。しかし実際には保護されておらず、危険な状態にあり、脅威者が完全にアクセスできる状態になっています。

セクションIV：Webの脅威とオンラインのリスク

常にコネクトされた現代のデバイスの特性を活用し、ネットワーク経由でユーザやデバイスを攻撃したり、コマンド&コントロール信号を伝達したり、データを流出させたりする攻撃はWebベースの脅威に分類されます。この包括的な用語にはさまざまなタイプの脅威が含まれ、現代の脅威の中で最も大規模で巧妙で致命的で、さらに被害者には気の毒ですが最も成功を収めた攻撃でもあります。

Web脅威は、モバイルデバイスに対する攻撃チェーンの非常に重要かつ戦略的な部分であり、ユーザやデバイスは共に広くこの脅威にさらされます。アプリやOSのCVEエクスプロイトとは性質が異なるかもしれませんが、これは攻撃チェーンの重要な部分であり、強力な制御を実装すれば、組織はこれらをしっかりとコントロールすることができます。

Web脅威を他の脅威ベクトルの"代替"として扱うべきではありません。単なる輸送車と考えるべきです。Web攻撃は、攻撃を成功させるためにより伝統的な戦術と組み合わされることが多く、これらはすべて大きなパズルのピースであり、次のことが可能です：

1.脅威アクターに、最小限の労力で最大限の成功をもたらす。

2.最も厳格なセキュリティポリシーやコントロールをバイパスすることができる。

1番からフィッシングが最大の脅威であることは一目瞭然です。数百、数千のターゲットにSMSで悪意のあるリンクを送信するのにかかる時間はわずか数秒であり、一部のターゲットがクリックする可能性はキャンペーンを成功させるのに十分なほど高いといえます。

2番については、もしユーザが認証情報を渡し、個人を特定できる情報（PII）にアクセスしてしまえば、世界中のセキュリティ管理は全て無意味になります。システムまたはサービスを侵害するために必要なのは、ターゲットに認証情報を半ば説得力のある方法で提供するよう求めることだけです。

以下では、デバイスに影響を与える脅威の上位を特定するため、調査をさらに掘り下げます。

フィッシング

前述したように、フィッシングは最大の脅威であり、それは正当な理由があります。

まずは悪いニュースからお伝えしますが、フィッシング攻撃に引っかかったユーザは2022年から1%増加し、8%となりました。

これはつまり組織ではデータの保護とデータのセキュリティに重点を置いた教育が進んでいるように見える一方で、個人ユーザでは侵害が増加。攻撃者がソーシャルメディアなどの他の経路を通じてユーザを直接、より積極的にターゲットにしているという脅威の傾向と一致し、リモート／ハイブリッドワークで個人所有デバイスの業務使用を利用していると見て間違い無いでしょう。2023年、フィッシング攻撃の成功率は、モバイルデバイスの方がMacよりも50%高く、また、CISAが"全サイバー攻撃の90%以上がフィッシングから始まる"と指摘しているように、悪意ある攻撃者が個人データの侵害からビジネスデータへの侵害に軸足を移す足がかりとして、ユーザのプライマリデバイスを標的にするのは当然のことといえます。

"クリプトジャッキングはデバイスの1%、組織の9%"

サイバーセキュリティ業界が初めてクリプトジャッキングについて警告を受けたのは2011年。その後、2022年に最初の本格的な急増が報告され、インシデント数は1億4,000万件に到達。Statistaが指摘するように**世界全体で43%増加**しました。この急増に続いて、Sonic Wallの調べによると、**クリプトジャッキング攻撃の件数は2023年上半期だけで399%増の3億3,230万件に膨れ上がりました。**

クリプトジャッキングがいかに広く浸透しているかは、2023年前半、macOS向け商用ソフトウェアの海賊版コピーに埋め込まれた**クリプトジャッキングマルウェアをJamf Threat Labsチームが特定**したことからも十分分かるはずです。複数の調査結果が裏付けているように、クリプトジャッキングは、脅威アクターが、文字通りまた比喩的に、利用している危険なトレンドに君臨し続けています。単にリソースを盗むという段階をはるかに超え、犯罪行為が脅威アクターに大金を稼がせ、この脅威やその他のサイバー脅威を継続させる領域に突入しており、組織は今後真剣に取り組む必要があります。

悪意のあるネットワークトラフィック
悪意のあるネットワークトラフィックは、調査対象全体の"デバイスの11%"に大きな脅威を与えています。(マルウェアのインストールと混同しないよう注意。この脅威タイプについてはレポート後半を参照) 組織レベルで見ると、"組織の20%が悪意のあるネットワークトラフィックの影響を受けている"ことが判明しました。

悪意のあるネットワークトラフィックの例としては、以下のようなものがあります:

- マルウェアダウンロード
- コマンド&コントロール (C&C)
- データ流出
- 詐欺
- さらに細かく掘り下げていくと、"アンドロイドとiOSを搭載したモバイルデバイスがそれぞれ8%と6%を占めていました "。その他の注目すべき発見は以下の通り:
- **組織の2%がパスワード漏えい** (認証情報が同意なしにオンライン上にリリースされる) を経験している
- **危険なホットスポット (安全が確保されていない無線ネットワークで、無料で利用できる場合が多い) に接続しているユーザは全体の1%。**
- **約1%がMitM (Man-in-the-Middle) 攻撃** (脅威者が2つの被害者間で独立したコネクティビティを作り、データを収集するためにメッセージを中継し、多くの場合、メッセージを改ざんする) の影響を受けた。

これらのパーセンテージは、メディアに掲載されるような注目度の高い大きな数字ではありませんが、サンプルプールのデバイス数に照らし合わせると、この控えめなパーセンテージが実際の数字ではどの程度に相当するかがわかります。

- 30万台のデバイスでパスワード漏えいが発生
- 15万人のユーザが危険なホットスポットに接続
- 15万人弱がMitM攻撃の影響を受けた

これはつまり、下記の機会が最低でも15万回あるということを意味します:

- **脅威アクターによるデバイスの侵害**
  - ビジネスデータの取得
  - 他のエンドポイントへのピボット攻撃
  - ネットワークやサービスへの侵入
  - コンプライアンス違反が発覚したデバイス
  - 地方、州、連邦および/または地域の規制要件違反の発覚
  - インシデントに 派生する影響への法的責任
  - 民事および/または刑事責任
  - 企業の信頼失墜
  - パートナーシップの解除
  - ビジネス機会の喪失
  - 廃業・事業停止

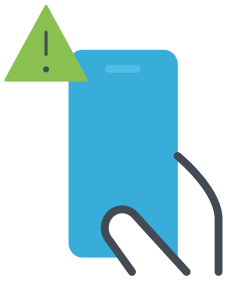
デバイスのコンプライアンス

ここまで3つの脅威トレンドについて解説してきました。調査結果はこれで全てではありませんがこのセクションでは一旦、脅威トレンドからデバイスのコンプライアンスを維持し、コンフィギュレータの脆弱性管理するための緩和戦略に焦点を移します。

本レポートでは、包括的な管理と深層防御のセキュリティ戦略を通じて全体的なコンプライアンスを達成し維持するためにIT チームとセキュリティチームが再び焦点を合わせるべき3つの分野をピックアップ。それぞれのエリアを深掘りし、調査結果に基づくデータ主導のガイダンスを提示します。

基本に立ち返る

最初のエリアは、他のセクションのツールや戦略を構築する基礎となる、デバイスコンプライアンスの中で最も重要な部分です。タイトルが示すように"基本に立ち返る"とは、エンドポイントプロテクションを保護する土台となることが何度も証明されている重要な機能性を強化してセキュリティ計画を推進することを意味します。



39%

の組織で既知の脆弱性を持つデバイスを1台以上保有していた。

パッチとセキュリティアップデート

Jamfの調査からなんと"組織の39%が既知の脆弱性を持つデバイスを1台以上保有している"ことが明らかになりました。セキュリティ専門家は、ゼロデイ脅威は特定が困難で、開発者がこの種の脅威を無効化するパッチをまだ作成していないため、脅威を緩和することがさらに難しいことを理解しています。しかし、ここでの問題は既知の脆弱性、あるいはパッチが利用可能な脆弱性に関するもの、つまり、ただ単にデバイスに脆弱性を修正するための重大なパッチやアップデートが適用されていないだけのことです。

上記の発見は、影響を受ける組織内のすべてのデバイスタイプに関連しますが、さらに厄介なのはモバイルデバイスであり、**"モバイルユーザの40%が既知の脆弱性を持つOSバージョンを使っている"**という問題です。つまり組織だけでなく、すべての利害関係者がデバイスのセキュリティに責任を負っているということなのです。さらに彼らは、新しくリリースされたOSアップデートやアプリケーションパッチを可能な限り迅速に適用するための反復ワークフローを通じて、フリート用のベースラインを微調整するという重要な役割も担っています。

デバイスのアップデートが遅れる主要な理由のひとつは、コンフリクトの恐れと、アップデートを必要とするエージェントが多すぎることです。

緊急セキュリティ対応（RSR）

MacとiOSベースのプラットフォームへの重要なセキュリティアップデートのインストールの遅れに対処するための協調的な取り組みとして、Appleは2023年前半に緊急セキュリティ対応（RSR）の配信を開始。RSRの導入により、対応デバイスへのダウンロードとインストールが自動化され、リスクを軽減するための重要なパッチの配信が効率化されました。Appleデバイスとユーザは、主要なソフトウェアアップデートとアップデートのギャップに注意することで、現存するエクスプロイトの侵入からより安全に保護されます。

macOSセキュリティコンプライアンスプロジェクト（mSCP）

mSCPとして知られるこのオープンソースプロジェクトは、Appleデバイスの管理とセキュリティ確保を担当するITチームやセキュリティチームが、コンプライアンス目標に沿ったセキュリティベンチマークを導入できるよう支援するものです。mSCPは、組織独自のコンプライアンスニーズに基づいて、デバイスのフリートへの導入された後に、コンプライアンスを実施するためのコンフィギュレーションペイロードと設定を生成するための論理的かつ体系的なアプローチを提供します。

セキュリティにおける管理の役割

管理とセキュリティは共生関係、すなわち相関概念にあります。エンドポイントセキュリティは、エンドポイントをアクティブに監視することで、デバイスを脅威から確実に保護しますが、管理なしでは、修復は手作業で時間のかかる作業となり、デバイスの数が増えれば増えるほど、またリモートであればあるほど、その難易度は飛躍的に高まります。逆に、管理ワークフローは、フリート内にどのような欠陥があるかを要約する最新のデバイステレメトリなしでは、デバイスのコンプライアンスを自動化することはできません。

前述のAppleのRSRは、管理の恩恵を受ける重要なパッチサービスの1つであり、デバイスがロックされているかログアウトしているかに関係なく、セキュリティ対応とシステムファイルが自動的にデバイスにインストールされるようにデバイスを構成する仕組みをITに提供します。

最後に、管理者の役割において重要な要素は、積極的なモニタリングがいかにコンプライアンスイニシアチブを支援するかという点です。前のセクションのネイティブアプリとクラウドベースのアプリの考察を参考にすると、モニタリングから得られる洞察は、エンドポイントの健全性のスキャンをIT/セキュリティに提供します。豊富なテレメトリデータで武装したこれらのチームは、アプリの安全性とデータセキュリティについてデータドリブンの決定を下すことができます。逆に言えばこのデータがなければ、例えばWebアプリにリモートアクセスしているエンドポイントのセキュリティ状況を、組織は知り得ることができないということです。

Jamf Compliance Editor（JCE）

Jamf Compliance Editorは、macOSセキュリティ・コンプライアンス・プロジェクト（mSCP）にもとづいて公開されたアプリケーションであり、コンプライアンスツールをJamfのMDMソリューションと組み合わせて、組織向けにカスタマイズされたコンプライアンスアセットを生成するだけでなく、JCEに組み込まれたインターフェースも統合するネイティブmacOSアプリを実現します。安全なAPIを介してJamf Proインスタンスを使用して新しく生成されたアセットをアップロードし、生成と展開の間のギャップをシームレスに橋渡しすることで、管理者がコンプライアンスをより迅速かつ効率的に適用できるようになり時間の節約をサポートします。

多層防御（Defense in depth）

どんな道具も完璧ではなく、すべての脅威を常に捕捉する銀の弾のようなソリューションは存在しません。どうにかして、どこかで、何かがうっかりすり抜けてしまいます。しかし、ITチームもセキュリティチームも、脅威が組織のリソースに影響を及ぼすリスクを最小限に抑えるための対策を講じないわけにはいきません。ある層がそれを捕らえられなかったとしても、他の層がそのリスクがはるかに悪いものになる前に捕らえる。それが多層防御です。

単に数多くのソリューションを寄せ集めるだけでなく、深層防御は、組織がセキュリティ計画を構築（またはアップグレード）する際に目指すべきセキュリティパラダイムであり、さまざまなソリューションをケーキのように何層にも統合します。各層はそれぞれ独自のセキュリティツールであると同時に、前の層のセーフティネットとしても機能し、万が一、脅威が次のレイヤーをすり抜けたとしても、それを軽減することができます。

Trusted Access

Jamf独自のセキュリティパラダイムは、Jamf Pro（管理）、Jamf Connect（アイデンティティ）、Jamf Protect（セキュリティ）ソリューションを組み合わせることで、管理者がインフラ全体にわたってフリート全体の管理を効果的に拡張し、同時にmacOS、iOS/iPadOS/tvOS、Android、Windowsを実行するMacやモバイルデバイスに包括的なセキュリティ保護を提供できる統合プラットフォームを形成できることを示す代表的な例です。

"2023年にジェイルブレイクまたはroot化されたデバイスを持っていた組織の割合＝1%未満"

この結果は仕事で使用するデバイスを不正改造/ルート化するユーザが減っている証拠であり、それは良いことです。しかし、モバイルデバイスの積極的な監視（セキュリティ）とゼロトラストネットワークアクセス（アイデンティティ）の動的なセキュリティポリシーの実施と自動化された修復（管理）を組み合わせることで、コンプライアンス違反のデバイスが組織のデータを危険にさらすことを防ぐ優れたワークフローが実現することを証明するものでもあります。

BYODやCOPE（Corporate Owned Personally Enabled）に依存した従業員選択プログラムは、ユーザの生産性向上には最適ですが、デバイスの管理不足や過剰なセキュリティは、データセキュリティやエンドユーザのプライバシーに影響を与える多くの問題を生み出す原因となります。管理とセキュリティの過不足に対するソリューションとしては、企業所有のデバイスと個人所有のデバイスの両方をサポートする階層化ワークフローを導入し、両方のタイプのデバイスが基本的なセキュリティポスチャを持つようにすることです。

例えば、会社支給のデバイスはゼロタッチ導入（管理）でMDMに自動登録され、個人支給のデバイスは認証情報（ID情報）でユーザ登録されるようにします。後者は前者と同じような構成ですが、ビジネスボリュームは、すべてのビジネスアプリとデータを、ユーザの個人アプリとデータを格納する個人ボリュームとは別の暗号化されたボリュームに格納します。さらに、ネットワーク上のプライバシーは、すべてのビジネストラフィックを暗号化されたマイクロトンネル（セキュリティ）を通してルーティングする一方で、個人的なネットワークトラフィックはインターネットに直接ルーティングすることで維持されています。最後に、エンドポイントセキュリティは、個人所有のデバイスと会社所有のデバイスの両方で同レベルの脅威検出と防御を行い、最新のデバイスヘルスデータに依存して、ビジネスリソースへのアクセス要求が行われるたびにエンドポイントの健康状態を判断します。ゼロトラストモデルに基づき、デバイスが検証された場合にのみアクセスが承認され、検証が失敗した場合は、デバイスを修復（管理）するための自動化ワークフローが導入され、リクエストは不承認のままとなり、その後、デバイス認証が再度試みられ、確認されれば、その時点で初めてリクエストが承認されます。

まとめ

- 企業所有および BYOD、すべてのデバイスで管理を確立する
- エンドポイントセキュリティ製品を使用してマルウェアを阻止し、テレメトリを収集することで、さらなる分析と脅威の発見を行う
- コンプライアンスを遵守する
- 企業 キャンパスネットワークを離れるデバイスを含めエッジ環境でのセキュリティを実装する
- 暗号化されたトンネルを使用して安全に接続し、データの傍受を回避する
- ゼロトラストプログラムを実装する
- エンドユーザのプライバシーを尊重する

この調査について

今日の職場では、仕事を遂行するためにデバイス、ユーザ、アプリケーションのすべてがコネクトされている必要があり、Jamfはそれらに影響を及ぼしている最大のセキュリティトレンドについて、より深く理解する必要があると考えました。この論文に記載されている情報や統計は、当社カスタマーベースにおけるセキュリティ動向の分析、OSやアプリケーションの脆弱性に関する独自調査、アンダーグラウンド調査の結果を基にしています。このようなセキュリティトレンドが現実に与える影響を理解するため、私たちはJamfが保護するiOS、macOS、iPadOS、Android、Windowsの各デバイス1,500万台のサンプルを、世界90カ国で12カ月にわたって調査。この分析は2023年第4四半期に実施されました。本調査において分析されたメタデータは、個人または組織を特定する情報を含まない集計ログから抽出されたものです。私たちがこの分析を行ったのは、脅威に対する不安を煽るためではなく、お客様自身、またお客様のユーザに与えられている選択肢を提示し、デバイス、ユーザ、そして組織のデータをあらゆる側面から確実に保護する方法をアドバイスするためです。セーフガードを守りセキュリティポスチャを拡張する方法に関する詳細については、当社にお問い合わせください。

出典：Jamf Threat Labs