Lookout®

ホワイトペーパー

モバイル フィッシング: 現代の企業が直面する現実と誤った通念

モバイル端末は、フィッシング攻撃を仕掛ける犯罪者たちが利益を得るための新たなターゲットになっています。攻撃者は、既存のフィッシング対策をうまくすり抜けて、モバイル端末を攻撃しています。こうした攻撃により、セキュリティの欠点が浮き彫りになり、機密データや個人情報が憂慮すべきペースで漏洩しています。

大半の企業は、従来型のファイアウォール、メール ゲートウェイ、エンドポイントセキュリティによって、メール ベースのフィッシング攻撃から守られています。加えて、近年のユーザーは、フィッシング攻撃を見破るのがうまくなっています。しかしモバイルにおいては、ユーザーにとっても既存のセキュリティ テクノロジーにとっても、フィッシング攻撃を特定し阻止することはますます難しくなっています。

モバイル端末におけるフィッシングは、独特でかつ問題をより複雑化しています。

モバイル端末は、従来型のファイアウォールの外部に接続され、通常はエンドポイントのセキュリティ ソリューションを持たず、デスクトップでは使われなかった多くの新たなメッセージ プラットフォームにアクセスします。さらに、モバイル ユーザー インターフェースには、ハイパーリンク上にマウスを置いて宛先を表示するなど、フィッシング攻撃を特定するために必要な詳細な情報機能が不足しています。その結果、IBM によるとモバイルユーザーがフィッシング詐欺に遭う確率は、 3 倍も高くなっています。

結局のところ、モバイル端末に大量の個人データと企業データが収められていることが、フィッシング攻撃の格好の標的となる理由です。

実際、従来型のフィッシング保護と教育を受けていたにもかかわらず、2011 年から 2016 年の間にモバイル端末でフィッシング URL を受信し、クリックした Lookout ユーザーは全体の 56% にも上ります。これらの攻撃は Lookout に阻止されていますが、 Lookout ユーザーがモバイル端末でフィッシング URL を受信し、クリックする割合は、2011 年以降前年比で平均 85% も上昇しています。

モバイル上のフィッシングの問題は、企業が認識しているよりもはるかに巧妙かつ深刻です。企業でフィッシング攻撃に対する保護を、モバイル端末を含む全方面で実現するには、まず、現代のフィッシングにまつわる誤った通念を打破して、セキュリティと IT の専門家が現実を把握する必要があります。そして、情報に基づいて企業のデータを守る方針を決断するために、事実を手に入れる必要があります。

モバイルでフィッシング攻撃に遭う確率の上昇

2011 年以降の毎年

モバイル上でフィッシング URL を受信し、クリックした Lookout ユーザー

目次

モバイル上のフィッシングに関する誤った通念 その 1

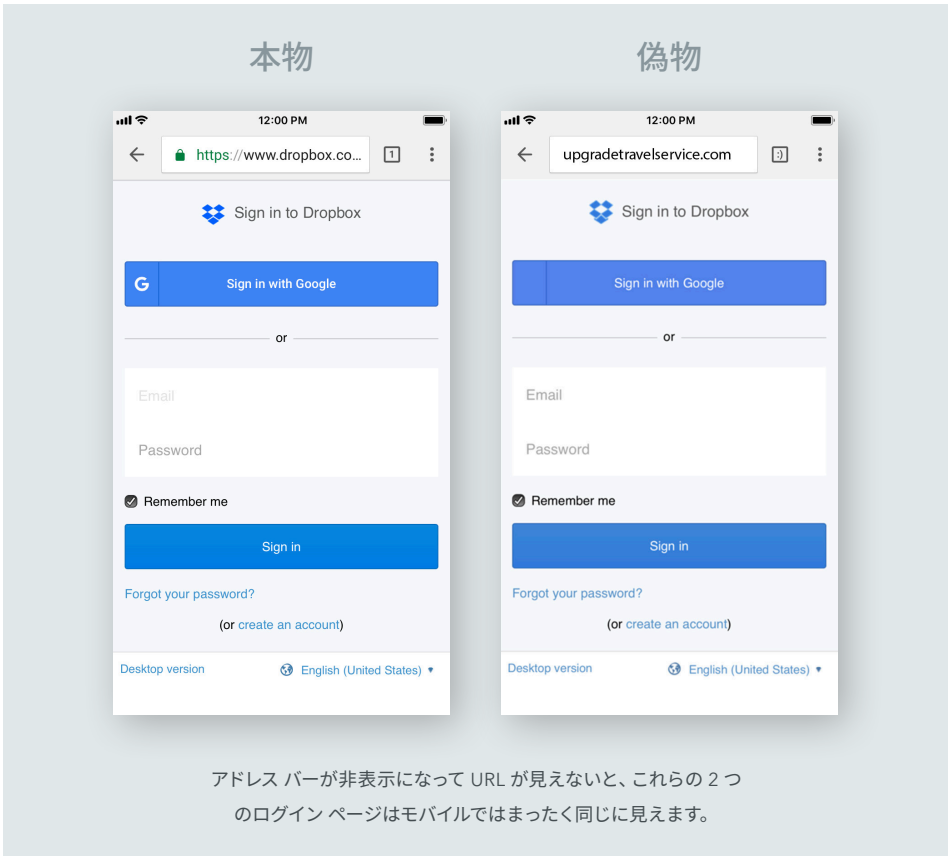
モバイル端末の保護は既存のフィッシング保護だけで十分である。

従来、企業はファイアウォール、メール ゲートウェイ、エンドポイント用アンチウイルス、さらにはユーザーへの教育によって、従業員がフィッシング メッセージを受信したり、だまされたりしないよう保護してきました。これは、完全に企業が所有し、管理するPCなどの固定デバイスでは有効なアプローチです。しかし、ほとんどの最高情報セキュリティ責任者 (CISO) が身にしみて知っているように、モバイル端末はこれには当てはまりません。

今日のモバイル端末は、企業が保有する端末でさえも、私用にも使われています。従業員は、仕事で使うスマートフォンでランチの支払をし、個人メールを送信し、家族の写真を撮り、ソーシャルメディアをチェックし、顧客の記録を確認し、訪問先への道順を調べ、財務報告にも目を通しています。ゲーム アプリ、デート アプリ、メッセージ アプリは、会社の最も重要なデータを含むドキュメントリーダー、社内メール、ファイル共有アプリ、その他のアプリのすぐ隣にあります。

例えば、メールは間違いなくフィッシング攻撃者にとって最初の攻撃ポイントで、MovableInk の U.S. Consumer Device Preference Report によれば、現在メールの 66% 以上がまずモバイル端末で開封されます。企業が企業メールの保護に力を入れる一方、モバイル上の個人メールは攻撃者に新たな侵入口を開いています。

ほとんどの信頼性の高い個人向けメール プロバイダは、標準レベルのフィッシング保護を備えていますが、攻撃者はこうした技術を回避する方法を発見し、従業員をだまして機密情報を渡したり、悪意あるアプリをダウンロードしたりするように仕向けます。それが、企業データに通じる道を開くことになります。抜け目のない攻撃者は、個人メール アカウントを標的にして企業フィッシング攻撃を実行しています。企業メールで利用されるレベルの厳重な保護は、個人メールには適用できないことを知っているからです。さらに、個人メール用と、企業メール用のアカウントが、いずれも同じモバイル端末に置かれていることも把握しています。



アドレス バーが非表示になって URL が見えないと、これらの 2 つのログイン ページはモバイルではまったく同じに見えます。

フィッシング サイト (個人をだまして情報を提供させるように細工されたウェブページ) の巧妙さを目にすれば、こうしたサイトがなぜ攻撃者にとって効果的な手段なのか容易に理解できるでしょう。要点を示した次のログイン ページをご覧ください。特にモバイル端末の比較的小さな画面上では、専門家であっても偽物と本物を見分けるのは困難です。

しかし、メールはフィッシングが影響を与える分野の1つに過ぎません。一方、モバイル端末は、攻撃対象になるアクセス ポイントとして新たなジャンルを開きました。

モバイル フィッシングのキルチェーン

モバイル端末には、1 回誤ってタップするだけで侵入されてしまいます。ブラウザ ウィンドウ上の悪意ある URL をタップしてしまう場合もあれば、知らないうちにアプリがバックエンドで接続する悪意ある広告ネットワークの URL や、ユーザーをだまして企業のアクセス認証情報を提供させる個人メール内のリンクかもしれません。その 1 回のタップによって、攻撃者はユーザーのインフラに侵入し、貴重なデータに到達することができます。

モバイル上のフィッシングに関する誤った通念 その 2
攻撃はメールだけで行われる。

これまでの通念に反し、フィッシング攻撃はメールだけの問題ではありません。モバイル端末は、悪意ある攻撃者にまったく新しい攻撃の道筋を開きます。攻撃者は、SMS や MMS、さらに多くの人に使用されている WhatsApp、Facebook、インスタグラムのような個人用ソーシャル メディア アプリやメッセージ プラットフォームを、フィッシングの手段として活用するようになりました。

従業員は、実際に SMS フィッシング攻撃の被害に遭っています。 Lookout の調査によれば、従業員の 25% 以上が自分の地域の番号に偽装された電話番号からの SMS メッセージにあるリンクをクリックしたことがあります。

こうした新たな攻撃経路がセキュリティの専門家たちによって見過ごされてしまうと、企業は危険にさらされます。最近のメール以外で発生したフィッシングの事例を一見すると、その理由が分かります。

ViperRAT

ViperRAT は、高度な形態の 監視ウェア です。ViperRAT の背後にいる脅威の攻撃者は、ソーシャル メディア プラットフォーム上で女性になりすまして被害者を引き付け、悪意あるアプリをダウンロードさせます。攻撃者は関係を築いてから、被害者にソーシャル メディア プラットフォーム上で「もっと簡単にコミュニケーションを取る」ためアプリをダウンロードするように求めるメッセージを送信します。

ViperRAT が盗んだ情報があれば、攻撃者は、被害者がどこにいるか、誰とつながっているか (連絡先のプロフィール写真を含む) を把握できます。さらに、被害者が送信したメッセージ、閲覧履歴、端末上の他のアプリからのデータをキャプチャするスクリーンショット、端末で話された音声や再生された音楽、それに無数の画像 (端末のカメラが向けられたあらゆる対象を含む) を見ることができます。

ViperRAT についての詳細

Facebook フィッシング キャンペーン

F-Secure の研究者は、iOS と Android ユーザーを標的にしたフィッシング キャンペーンを特定しました。攻撃者は被害者に、彼らが YouTube の動画に登場していることをほのめかすメッセージを Facebook Messenger 経由で送信します。被害者が iOS または Android 端末でリンクをクリックすると、端末の種類を検知して、被害者の認証情報を読み取るように設計された Facebook のログインページに似せたページを特定的に送ります。PC ユーザーを対象にする場合とは違います。この種の攻撃は、被害者をソーシャル エンジニアリングして、企業が使用する認証情報など、サービスの認証情報を渡すように仕向けます。

Facebook フィッシング キャンペーンについての詳細

こうしたフィッシング攻撃は今日存在する多くの攻撃のほんの数例に過ぎませんが、攻撃者がメールを超えて、モバイル端末を標的にしていることを物語っています。モバイル端末があっという間にそうした攻撃の主要ベクトルになった理由も浮き彫りにしています。

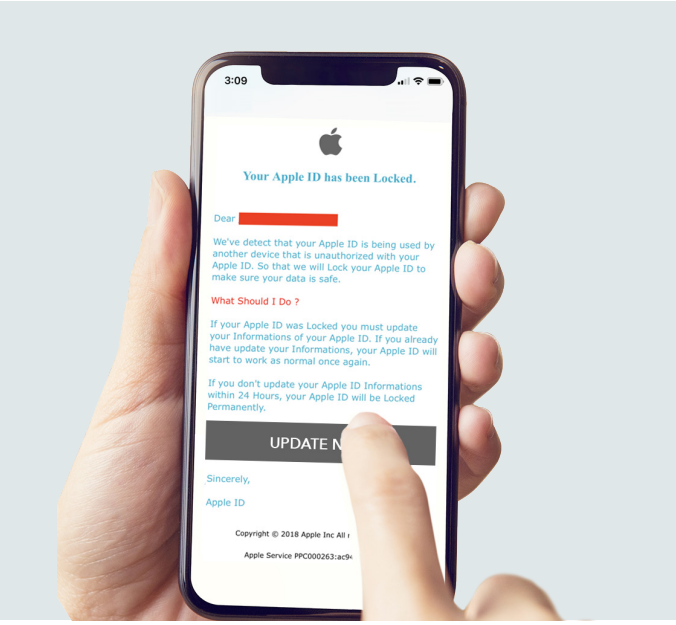
- モバイル端末は、前述のような新たなメッセージ プラットフォームを提供しています。
- 端末は多くの場合は管理されておらず、エンドポイント セキュリティを備えていないため、攻撃からの保護が比較的手薄になっています。
- モバイル端末に備わった機能 (例えば、位置情報、前面／背面カメラ、マイク、音声通話、テキスト メッセージ、メール、アプリなど) と、人々がいつでも電話を持ち歩いているという事実から、多くの場合モバイルでの監視がより効果的です。

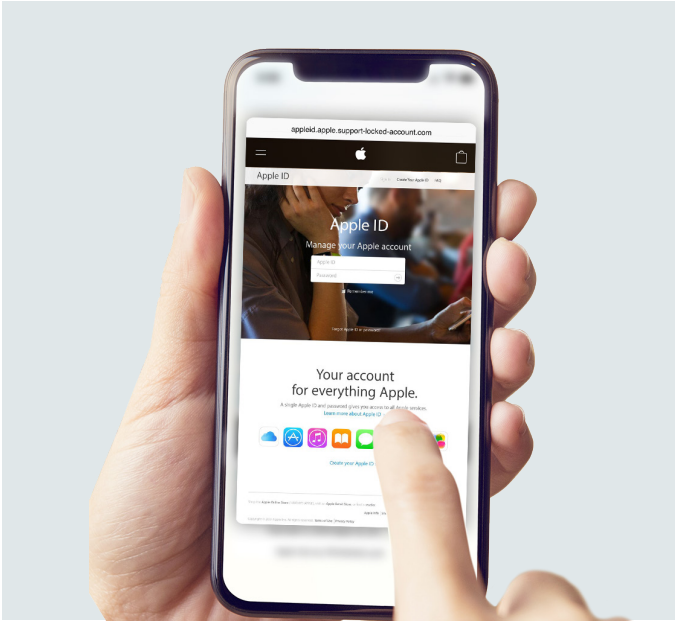
モバイル フィッシングに関する事実 その 1
PC よりもモバイルで人をだましてフィッシング攻撃に誘う方が簡単です。

現在のモバイル端末の特性、機能、さらには画面サイズまでもが、フィッシングで攻撃者にとって都合の良い要素になっています。モバイル端末は、本物と偽物のサイトを見極めることをより困難にし、かつ従来型の企業セキュリティペリメーターの外で利用されております。

例 1

研究によると、携帯電話で疑わしいリンクをクリックする確率は、PC に比べると 3 倍になることが示されています。ユーザーがハイパーリンク上にマウスを置いてリンク全体を確認できる PC に比べて、モバイルではクリックする前にリンクを確認することがはるかに難しいのです。それに加えて、モバイル アプリ (Facebook など) 内のウェブ閲覧でも、ユーザーが訪問している URL を知ることはほぼ不可能であり、その点からも、攻撃者がモバイルを標的として好む理由が明らかです。



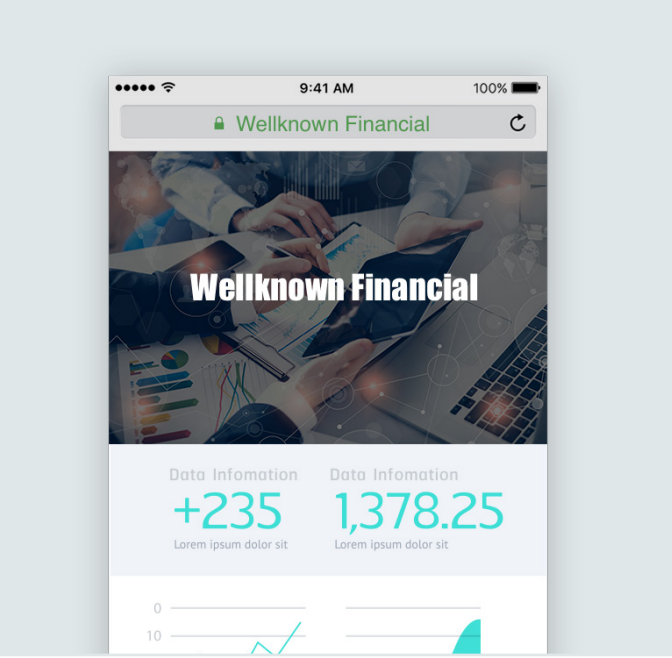


状況の説明: モバイルでリンクがどこにつながっているのかを確認するのは極めて困難です。例えば、iOS 上のリンクをタップせずに押す (3D Touch) と、リンクされたページが読み込まれます。攻撃者が、本物らしく設計されたフィッシング ページを使用している場合、ユーザーは偽装ウェブサイトを本物のウェブサイトと区別するのに苦労します。

例 2

大型モニターの画面を見ると、URL は「wellknownfinancial.com」ではなく「wellknownfinancial.com----------fakesite.xyz」であることに気付くかもしれません。しかし、モバイル ブラウザはアドレス バーの URL を短縮するので、いずれの場合も「wellknownfinancial.com---」しか表示されません。右の例にあるように、ブラウザが、URL を実際にアクセスしているウェブサイトを持つ会社の名前と置き換える場合もあります。この場合、URL が本物であるかどうかを判断するのはさらに難しくなります。

モバイル ブラウザは、ユーザーがスクロールしている間アドレス バーを隠し、画面の幅のためアドレス バーに表示される文字数を制限することで、ウェブサイトの URL を見えにくくすることもしばしばあります。この場合、こうした考え抜かれたデザインの最適化が、公然とフィッシング攻撃を仕掛ける攻撃者の能力を高めることにつながります。



状況の説明: アドレス バーは、実際の URL ではなく会社名だけを表示しています。

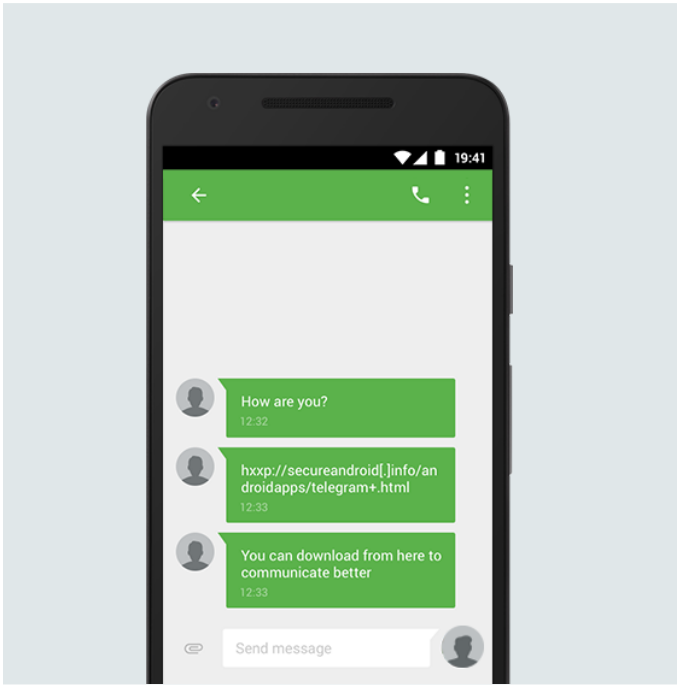
例 3

モバイル端末がファイアウォールの背後にあれば、従業員がフィッシング リンクをクリックしても、ファイアウォールが機能して接続が阻止されます。しかし、モバイル端末はそもそも「モバイルである (持ち運べる)」ことが売りなので、一般に従業員はファイアウォールの外側で過ごす時間の方が多くなります。モバイル端末は、ほとんど常に従来のペリメター セキュリティの外部にあるため、従業員が (例えば、会社からの帰宅中に) 悪意ある URL に遭遇した場合、そこにはもはや従業員を守るファイアウォールは存在しません。企業が従来のペリメター セキュリティのみを採用している場合、攻撃者は不正アクセスを行いやすくなります。

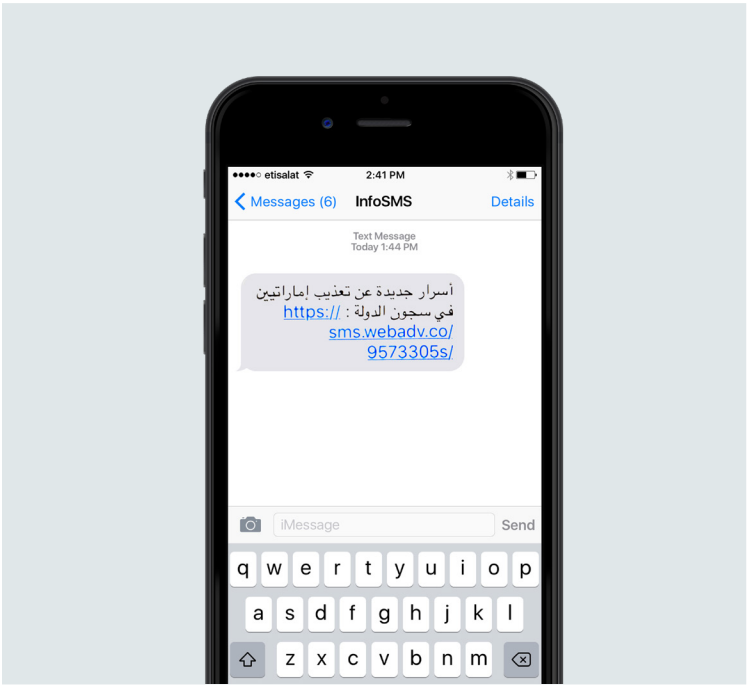
モバイル フィッシングに関する事実 その 2

モバイル マルウェアの製作者は、世間に出回るフィッシング技法、特に mAPT アクターを大いに活用しています。

モバイル フィッシングは、これまで以上に洗練された大規模攻撃の矛先になっています。最もアクティブなのが、モバイル向け持続的標的型脅威 (Mobile Advanced Persistent Threat； mAPT) 由来の攻撃です。「持続的標的型脅威 (Advanced Persistent Threat)」という用語は、一般的には、他の国家や大企業、事業、もしくは個人を持続的かつ効果的に標的とし、金銭的な利益や諜報活動を目的として情報を盗み出す能力を持つ特定のグループ (通常は国家) を言い表すための用語です。mAPT は、モバイルを標的として、この攻撃を行います。ここ最近のいくつかの事例を紹介します。



Dark Caracal SMS メッセージ



Citizen Lab がキャッチした Pegasus フィッシング SMS メッセージ。

- **Dark Caracal**
  Dark Caracal は、WhatsApp や Facebook 経由のフィッシング メッセージを使って、被害者が悪意あるリンクをクリックし、Android マルウェアをダウンロードするように誘い込みます。Pallas と呼ばれる Android マルウェアは、被害者の端末を監視して、大量のデータを収集します。

  Dark Caracal は、政府、軍隊、公益施設、金融機関、製造業、防衛関連企業などを標的にします。盗み取られるデータの種類は、ドキュメント、通話履歴、音声録音、セキュア メッセージング クライアントのコンテンツ、連絡先情報、テキスト メッセージ、写真、アカウント データなど、広範に及びます。

- **Pegasus**
  Pegasus 監視ウェア は、その重大度から世界中の注目を集めました。Pegasus を配信するオペレーターは、被害者に SMS でフィッシング メッセージを送りつけました。被害者がクリックすると、一連のサイレント イベントが起動し、Lookout がこれまでに確認した中で最も巧妙な iOS 端末のセキュリティ侵害攻撃が実施されました。同様に、Pegasus は一度端末に入り込むと、端末上のすべての活動を監視し、大量の機密データを収集しました。

mAPT 攻撃の精巧さは従来にないレベルであるため、周知することが重要です。

モバイル フィッシングに関する事実 その 3

人による操作だけではなく、アプリによって、無自覚に悪意ある URL にアクセスし、無防備なモバイル ユーザーにその URL が送りつけられることがあります。企業は、そのようなアプリについても警戒する必要があります。

URL を使用したりアクセス (クリック) したりするのは、エンド ユーザーだけではありません。アプリは、コードベースにある URL を使って、リアルタイムで情報を通信し、プルダウンします。この機能は、攻撃者が個人をフィッシングするのに使えます。これにより、悪意のある URL にアクセスする「良性アプリ」という、企業の心配の種となる新たな攻撃対象領域が形成されました。

例えば、アプリはしばしば広告を使って収益を上げています。そのために、アプリのコードには、広告配信 SDK が組み込まれています。これらの SDK は、エンドユーザーに広告を表示するため、見えないところで URL に接続します。良性アプリが攻撃者の実行する広告配信 SDK を使用する場合の手口は、SDK を使って悪意のある URL にアクセスすることで、エンドユーザーをだまして機密データを提供させることを意図した広告を表示させます。

このような脅威は、「見えない」機能を活用しますが、効果の高いフィッシング攻撃が、必ずしも隠されているわけではありません。

Lookout によるフィッシング問題の解決方法

Lookout Mobile Endpoint Security の機能の 1 つである Lookout Phishing & Content Protection は、モバイル ファーストの世界でフィッシング攻撃から企業を保護することを目的にしています。

Lookout Phishing & Content Protection

検知 –メール (企業メールまたは個人メール)、SMS、チャット アプリ、ソーシャル メディアなどを含む、モバイル端末上のソースからのフィッシング攻撃を検知し、さらに、フィッシング攻撃からの保護に関するポリシーを定めます。

保護 – 認証情報のフィッシングなど、悪意ある動作の実行を試みる可能性がある、リスクの高いウェブサイトにホストされている既知の悪意のある URL へのモバイル端末の接続をブロックします。

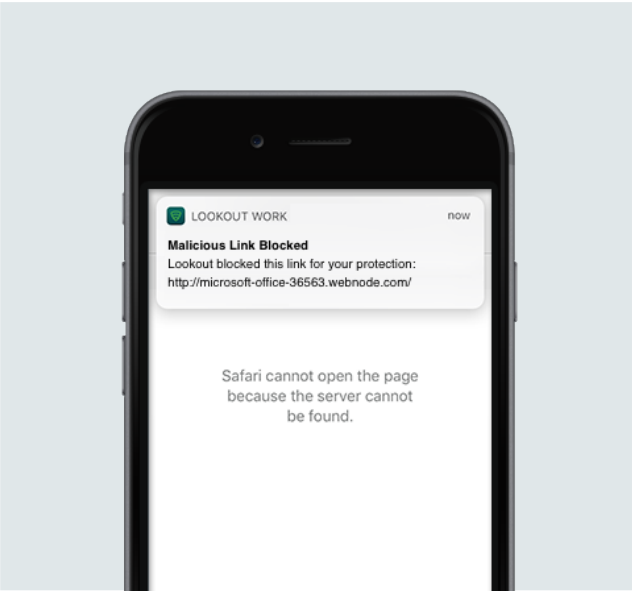
- 悪意のある URL には、広告詐欺、ボットネット、コマンド／コントロール センター、マルウェアへの感染およびマルウェアへのリンク、マルウェア コールホーム、マルウェア分散ポイント、フィッシング／詐欺、スパム URL、既知の脆弱性を持つ悪意のあるアプリまたはウェブサイトなどのリスクの高いコンテンツ、およびスパイウェアなどが含まれます。

解決 – 実際に URL にアクセスする際に、エンドユーザーに警告します。
このリアルタイム アラートにより、フィッシング サイトや悪意あるサイトのリスクにさらされることを防ぎます。

分析 – フィッシング リンクや悪意あるリンクをクリックするユーザーの頻度と重大性を可視化するとともに、端末が Phishing & Content Protection を有効化したかどうかを追跡します。この機能を有効化していない端末は、コンプライアンスに準拠していないとしてマークされ、大手 EMM ベンダーとの統合によって通常の企業の解決策を取ることができるようにします。

保護の仕組み

Lookout Phishing & Content Protection は、端末または従業員が悪意ある URL やフィッシング URL への接続を試みると、ネットワーク レベルで悪意ある接続の試みをブロックします。このアプローチの重要かつ独特な点は、メッセージの内容を調べることに依存していないことです。SMS、WhatsApp、Facebook Messenger、個人メールなど、モバイル端末上で使用されるソーシャル プラットフォームやメッセージ プラットフォームの多くは、機密性が高く、ユーザーにとってプライベートなものです。Lookout Phishing and Content Protection は、個人または端末が接続を試みるときに、URL のみを調べることによって、ユーザーのプライバシーを守ります。そうした URL をネットワーク レベルで調べることで、Lookout はユーザーがメール、テキスト メッセージ、ソーシャル ネットワーク、またはその他のアプリから、悪意ある URL やフィッシング URL につながるのを防ぎます。



Lookout Phishing & Content Protection のメリット

Lookout Mobile Endpoint Security は、常にお客様の会社全体のモバイル リスク領域を容易に可視化できるように機能し、そのリスクを大幅に低減するポリシーを適用し、既存のセキュリティ ソリューションやモバイル管理ソリューションに統合されます。Phishing & Content Protection 機能を利用すると、さらに多くのメリットがあります。機能は以下の通りです:

フィッシング攻撃や悪意あるウェブサイトに対する強力な防御ラインを追加し、モバイルに対するフィッシング対策をメール、ソーシャル プラットフォーム、およびメッセージング プラットフォームまで拡大します。

「モバイル リスク マトリックス (Lookoutまとめ)」に示される「ウェブおよびコンテンツ」の脅威ベクトルは、企業データを盗み出す攻撃者によって最もよく使われるモバイル ベクトルです。この脅威ベクトルに対し、総合的な保護を提供します。

従業員が保護された企業ネットワーク内にいるかどうかに関わらず、悪意あるコンテンツから保護することによって、企業は自信を持ってスマートフォンを業務で活用することができます。

強固なプライバシー管理とユーザーや端末に関連する PII の収集を制限する能力を含め、データの最小化と目的を伴ったデータ収集原則に従うことで、エンドユーザーのプライバシーを保ちます。

Phishing & Content Protection 機能を備えた Lookout Mobile Endpoint Security を装備することで、企業はリスクを緩和し、企業内で安全にモバイルを活用できるようにする実証済みの方法を得ることができます。

リアルな保護を提供

モバイルの活用は企業を変革しました。文字通り、仕事のやり方が変化しています。企業は従業員の生産性と柔軟性を奨励する一方で、機密データ、従業員と顧客の情報、重要なネットワーク インフラを安全に保つ方法を積極的に模索しています。

- Lookout Phishing & Content Protection は、管理者が日々直面する実際のニーズや現実的な問題に対処します。
- 管理者は、従業員にモバイル端末での自由なウェブ閲覧を許可したい一方で、悪意あるサイトへのアクセスをブロックしたいとも考えています。
- 管理者は、従業員がモバイル端末でさまざまなブラウザを使用することや、リスクの高いウェブサイトの警告を受けないことを心配しています。そのため、ユーザーが使用許可を受ける前に、モバイル上に確実に警告が表示されるようにしたいと考えます。
- セキュリティ部門は、すべてのエンドポイントを均一に保護して、モバイルのギャップを埋めることを期待しています。
- IT 部門は、モバイル端末を実質的にファイアウォールの背後に置かせて、トラフィックをバックホールすると、従業員にとっては使いにくさや生産性の低下という問題を引き起こします。一方、Lookout のソリューションでは、企業はデジタルトランスフォーメーションを十分に活用して、従業員が BYOD (職場に持ち込まれた個人の端末) であれ、COPE (企業がプライベートでの使用を許可した端末) であれ、モバイル端末で安全に作業する方法を提供できます。

Lookout Mobile Endpoint Security は、モバイル化が企業にもたらす真のセキュリティ上の問題から保護するために開発されました。IT やセキュリティの専門家は、この最新機能を使って、モバイル上でのフィッシングが引き起こす問題に対応できます。

次のステップに進む:Lookout がどのようにサポートできるかを見る

悪意ある攻撃者は、巧妙な形態のフィッシングを利用して、閉ざされた企業の扉に侵入しようとしています。

セキュリティや IT の専門家は、一般にフィッシング攻撃にまつわる危険を認識していますが、企業の大半は PC などの従来型のエンドポイントの保護を重視してきました。これでは不十分です。

モバイル端末におけるフィッシングは、従来のエンドポイントに比べると、独特でかつ問題も複雑化しています。モバイル端末を含め、あらゆるベクトルのフィッシング攻撃に対する総合的な保護を模索する企業は、現状の選択肢以外にも目を向ける必要があります。Lookout Mobile Endpoint Security は、必要とされるよりハイレベルの防御を提供します。

モバイル機器を安全に保つ方法の詳細については、lookout.com までご連絡ください。

*データについて:上記のデータは、2011 年から 2016 年の間に Lookout Personal が保護した 6 千 7 百万台のモバイル端末の分析に基づいています。すべてのデータは匿名であり、この分析を実施するために企業のデータ、ネットワーク、またはシステムにアクセスしたことはありません。