Lookout Phishing and Content Protection (PCP) の仕組み

モバイルにおけるフィッシングおよびコンテンツの脅威について

フィッシングは、攻撃者が組織のネットワークに対するアクセス権を得るための主要な手段となっています。エンドユーザーをだまして、悪意のある Web サイトやダウンロード サイトに誘導するリンクをクリックさせるのは比較的容易です。事実、Lookout が実施した独自調査のデータによると、最大 25% の従業員がフィッシング テスト中にだまされてクリックしました。攻撃者は、フィッシング攻撃の実行時に、電子メールが最もコストのかからない方法であることを見出しました。多くの組織はファイアウォール、ゲートウェイ、スパム フィルターなどによって実現する電子メール セキュリティ保護に既に投資を行っています。それらの保護は、デバイスが仕事用の電子メールを目的としてのみ使用されている場合にはモバイルにおけるフィッシング攻撃阻止に役立ちます。ただし、こうした保護は、従業員が会社と個人の両方の電子メールおよびアプリにすべて同じデバイスでアクセスできる場合にはあまり現実的ではなくなってきました。

モバイル端末におけるフィッシングは、独特でありながら、問題は複雑化しています。会社の電子メール以外の、以下のような新しいチャネルで攻撃を配信できるようになったためです。

個人メール – フィッシング メールが個人のメール アカウントに送信される可能性があります。その場合、多くの無料メール サービスに設けられている主要なセキュリティー保護をバイパスし、ユーザーをだましてリンクをクリックさせ、対象デバイス上のデータを侵害し、会社のデータにアクセスします。

SMS テキスト メッセージ – 無防備なユーザーに短縮リンクを含むテキストを送信します。このリンクは悪意のある Web サイトに誘導したり、悪意のあるアプリや監視ウェアのダウンロードを引き起こします。

悪意のある広告ネットワーク – URL 情報は、他のサービスとやり取りし、ユーザーにより良質なエクスペリエンスを提供するため、道筋を示したり、ショッピング サイトに接続したり、コンテキスト関連広告を表示したりするために、モバイル アプリに組み込まれています。ただし、アプリが悪意のある URL にアクセスするようプログラムされていると、マルウェアやスパイウェア用のプラグインのダウンロードが引き起こされることがあります。

メッセージング プラットフォーム – WhatsApp、Facebook Messenger、Instagram などを介してユーザーにスパイウェアをダウンロードするよう誘い込むメッセージを送信します。

企業にモバイル フィッシングに対する保護が必要な理由

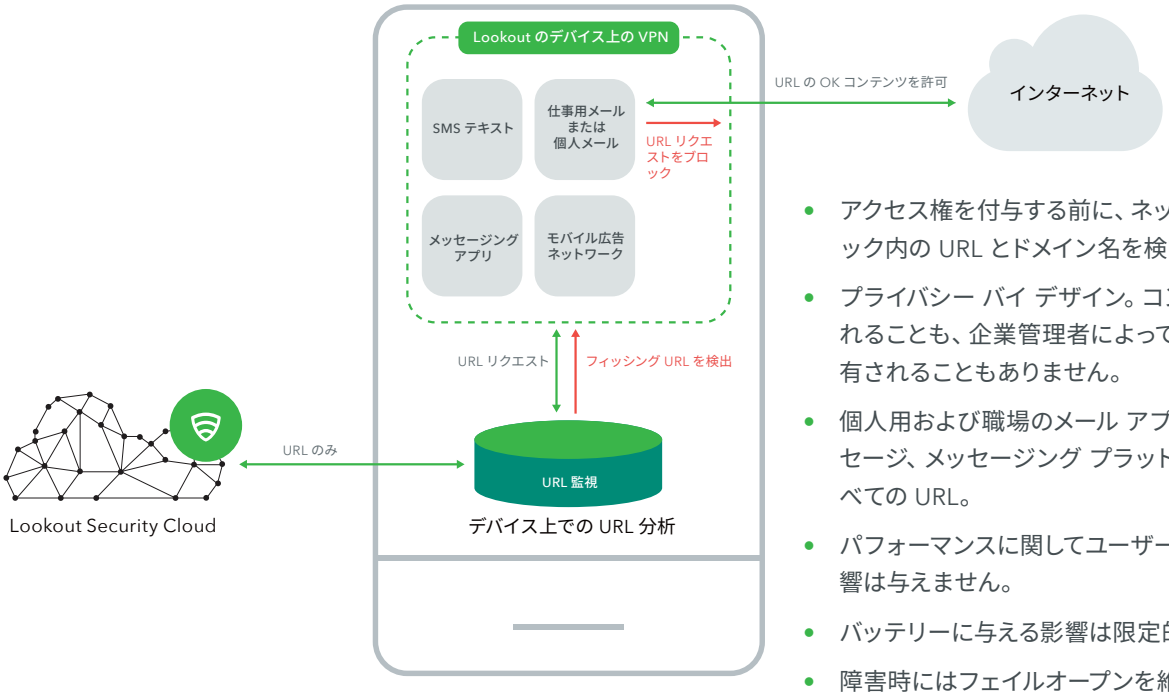
IDC によると、30% 以上の組織で、2018 年[1] に従業員がモバイル フィッシング攻撃の対象になったことが報告されています。実際、Lookout ユーザーの 56% が、使用しているモバイル デバイスでフィッシング URL を受信し、タップしてしまっています。このようなユーザーは、年間平均で 6 つのフィッシング URL をデバイスでタップしています。

Lookout ユーザーがモバイル デバイスで悪意のある URL をタップ受信した割合は、2011 年以降前年比で平均 85% も上昇しています。

[1]ソース:IDC 2018 U.S. Enterprise Mobility Decision Maker Software Survey

保護の仕組み

Lookout の人工知能エンジンは、ゼロデイや既知のサイバーセキュリティーの脅威から企業を保護し、フィッシング攻撃をリアルタイムで検出できます。Lookout Phishing AI は、新しいフィッシング サイトが作成されていないかインターネットをクロールして検出します。Lookout では、常時稼働のこの検索方法によって、ユーザーが標的になり、攻撃が開始される前の構築段階で、悪意のある Web サイトを検出します。



- アクセス権を付与する前に、ネットワーク トラフィック内の URL とドメイン名を検証します。
- プライバシー バイ デザイン。コンテンツが検証されることも、企業管理者によって特定の URL が共有されることもありません。
- 個人用および職場のメール アプリ、テキスト メッセージ、メッセージング プラットフォームからのすべての URL。
- パフォーマンスに関してユーザーが認識できる影響は与えません。
- バッテリーに与える影響は限定的です。
- 障害時にはフェイルオープンを維持します。

デバイス上で Lookout Phishing and Content Protection によって、電子メール (企業または個人)、SMS テキスト、メッセージング アプリ、埋め込み型のアプリ ブラウザーからのあらゆる URL リクエストが検査され、Lookout によって悪意があると識別された Web サイトのリクエストが動的にブロックされます。

Lookout Phishing and Content Protection ではローカルにホストされている VPN を使用して、トラフィックを分析し、デバイス上のブラウザーまたはアプリが疑わしい URL にアクセスしようとするとそのことを検出します。ユーザー プライバシーを確保するため、MES コンソールに報告されるのは問題の有無と検出数のみです。管理者がこの機能を使用してデバイスの閲覧履歴やトラフィックを表示することはできません。Lookout for Work アプリでは、この機能は「セーフ ブラウジング」と呼ばれます。

プライバシーとデータ収集

Lookout は製品開発においてプライバシー バイ デザイン[2] アプローチを採用しています。Lookout は、当社のセキュリティー価値を実現するために必要なデータのみを収集します。送信中および保存中のデータが確実に保護される状態を確保します。また、当社が収集し、管理者に表示する個人データを詳細に制限する堅固なプライバシー制御も行っています。

Lookout は、エンドユーザーの信頼を勝ち得て、規制に対するコンプライアンス状態を維持するため、最高レベルの認定と承認を獲得することに努めています。Lookout のコンプライアンス戦略は次のとおりです。

- EU-U.S. Privacy Shield – 2016 年 10 月に達成
- FedRAMP In Process – 2017 年 3 月に達成
- ISO 27001 – 2017 年 6 月に達成
- ISO 27018 – 2017 年 12 月に達成
- GDPR – GDPR 規制 (EU) 2016/679 適合

[2] https://en.wikipedia.org/wiki/Privacy_by_design

URL 分析に対する重点的な取り組み

Lookout Phishing and Content Protection ではデバイスとクラウド ベースの AI ドリブンの、電子メール、SMS メッセージ、ネットワーク、メッセージング プラットフォームからリクエストされる URL 分析を組み合わせて活用します。こうしたアプリのコンテンツが収集、格納、または企業管理者と共有されることはありません。トラフィックまたはコンテンツがデバイスからリダイレクトされたり、任意の Web ゲートウェイを通過したりすることはありません。

Lookout の GDPR に対するコミットメント

一般データ保護規則 (GDPR) によって、EU 在住者のプライバシー保護に対する新しい規則が課されています。Lookout は、GDPR (規則 (EU) 2016/679) を遵守するための推奨される技術的および組織的対策を含め、商業的に合理的なあらゆる努力を払っています。

GDPR には、組織が個人情報を収集、格納、使用、保護する方法に関する要件が含まれています。Lookout は、GDPR コンプライアンス状態を維持するための高度な要件に準拠することを重視しています。

Lookout が選ばれる理由

個人の電子メール、テキスト、メッセージング プラットフォームやアプリに対するフィッシング攻撃に対して強力な防衛線を張り、フィッシングに対する防御をモバイルまで拡大します。

モバイル デバイスの安全な業務への利用を促進し、保護されている企業ネットワークの内外どちらにいても、悪意あるコンテンツから従業員を守ることにより、デジタル変革を推進します。

Web やコンテンツといった、データの窃取を狙う攻撃者から最も標的とされやすいモバイル上の攻撃ベクトルを含め、あらゆるモバイル リスクから幅広く包括的に保護します。

Lookout の特徴

- Lookout では、グローバルな規模、およびモバイルにフォーカスした世界最大級のモバイル セキュリティ データセットを蓄積しています。Lookout は世界各国の 1 億 7 千万以上の端末と 7 千万以上のアプリからセキュリティ データを収集しており、1 日あたり 9 万のアプリが新たに追加されています。
- このグローバル センサー ネットワークでは、リスクを示す複雑なパターンをマシン インテリジェンスで検知することによって、人による分析のみでは見落とされがちなプラットフォームでの予測を可能にしています。人による分析のみでは見落とされがちなプラットフォームでの予測を可能にしています。
- モバイルはコンピューティングの新しい時代を象徴するものであり、このプラットフォーム専用のセキュリティ ソリューションも刷新することが求められています。Lookout は 2007 年からモバイルに特化したセキュリティ ソリューションを提供しており、この分野の専門技術を備えています。

Lookout を利用すれば、IT を可視化し、セキュリティ チームのニーズを満たしながら、生産性を低下させることなくモバイルのセキュリティ対策をすることが可能になります。現代のモバイル機器を安全に保つ方法について詳しくは、lookout.com/jp までお問い合わせください。