スマートフォンはPCよりも安全？（前編）：

フィッシングのリスクはPCの3倍　ニュースに出ない、モバイルセキュリティの怖い話

https://www.itmedia.co.jp/enterprise/articles/1908/26/news094.html　[PDF出力]

「モバイル端末には、PCのようなセキュリティ機能がタダでついている」という認識をしている人はいないだろうか。確かにモバイル端末には、過去にPCが受けてきた攻撃を参考にしたセキュリティ対策がされている。しかし犯罪者は、そんなユーザーの油断を狙った攻撃を仕掛けてきている。

2019年08月28日 11時00分 更新

[柴佑佳，**ITmedia]**

新しくPCを購入するとき、われわれは当たり前のようにセキュリティソフトウェアを同時に購入し、インストールする。しかしスマートフォンやタブレットといった、モバイル端末の場合はどうだろうか。

モバイル端末のセキュリティ対策と聞いても、ピンと来ない方もいるだろう。少し詳しい人でも、「iOSなら安全でしょう？」程度の認識かもしれない。しかし、近年話題になる企業のセキュリティインシデントが、従業員のモバイル端末への攻撃を発端としたものであったら？

「モバイル端末はPCより安全」という認識は、ある面においては正しい。しかし、PCのセキュリティ対策と同じような認識でいると、深刻な被害の当事者となるリスクがある。モバイル端末と自社の機密情報を守るために企業はどうするべきか。モバイルセキュリティベンダーの考える「ゼロトラストモデル」の現状を追った。

モバイル端末はPCよりも安全なのか？

「『なぜモバイル端末は、PCよりもセキュリティインシデントの話を聞かないのか？』と、よく質問されます」と、モバイルセキュリティベンダーLookoutのCSO（最高戦略責任者）を務めるアーロン・カックリル氏は語る。

Lookout CSO アーロン・カックリル氏

「私のような古い人間は特に、PCとインターネットが世の中に広がっていった時代に、さまざまな事件が発生したのを覚えています。一方で、モバイル端末に関して、同様の報道を見る機会はあまりありません」（同氏）。

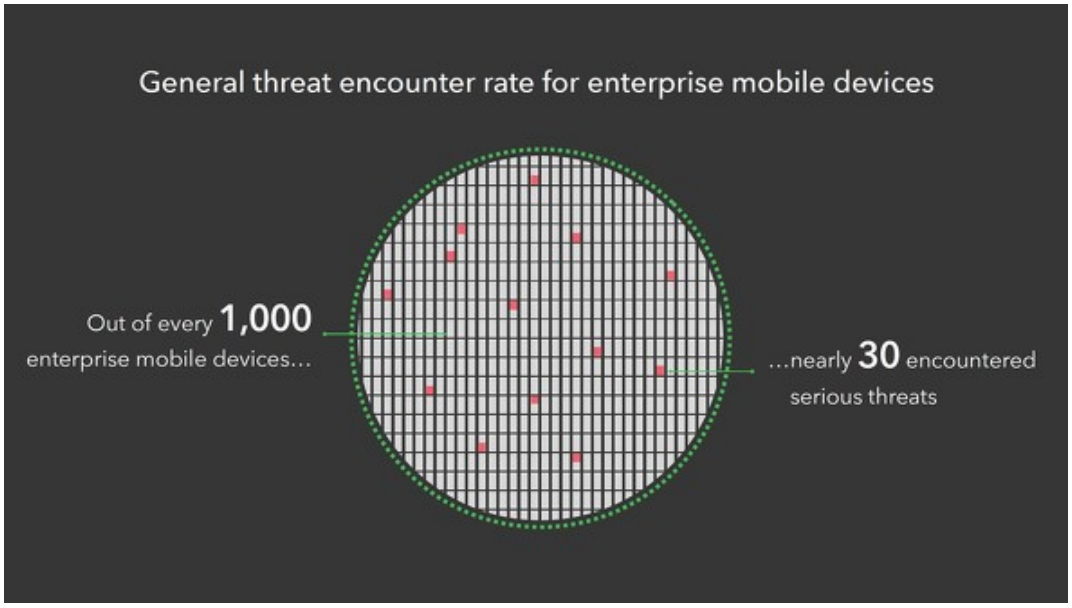
モバイル端末はそもそも、過去にPCが受けてきた攻撃や被害の経験に基づいて作られている。そのため、PCと同じような攻撃には概ね対策が施されているという。PCが受けてきたような被害の報道を見ないため、「モバイル端末はPCよりも安全」という認識になっているユーザーは少なからずいるだろう。

しかし、カックリル氏によれば、「モバイル端末はスパイにとって、夢のようなデバイス」なのだという。

今、攻撃者が狙っているのは「モバイル端末」

現在、多くのビジネスパーソンが愛用するモバイル端末、特にスマートフォンは、ほぼ全ての端末がカメラ、マイク、GPSを搭載している。また、常にネットワークにつながり、何らかの通信を行っている。ユーザーが自ら登録したアプリが常にバックグラウンドで動き、個人情報や個人の所有する金融情報が端末にひも付けられている。

そのため、モバイル端末は攻撃者にとって格好の標的だ。Lookoutの調査によれば、「全てのエンタープライズ向けモバイル端末で平均3%がマルウェアに感染している」（カックリル氏）というのだ。



エンタープライズ向けモバイル端末は、平均3%が何らかのマルウェアに感染している（Lookout調査による）

特に感染率が高いのは金融業だ。同業界においては、7%のデバイスが何らかのマルウェアに感染しているという（Lookout調べ）。「もし、企業のPCの7%がマルウェアに感染していると分かったら、その会社のIT部門は全員クビになるでしょう。そのくらい深刻な数字です」（カックリル氏）。

しかもこれは、正規のエンタープライズ向け端末――つまり、企業から従業員に貸与され、あるいは店舗などに設置されている端末、企業がしっかりと安全対策をしているはずの端末での割合だ。

従業員の中には、個人の所有するモバイル端末を無断で「活用」して、個人情報や業務に関する機密情報を扱っている者もいるだろう。機密情報をスマートフォンのカメラで撮影して端末に保管している者や、カフェや空港などで、通信が暗号化されていないフリーWi-Fiを使って企業のWebシステムにログインしている者もいるかもしれない。これらの「シャドーIT」がどのような脅威に晒（さら）されているかは、誰にも分からない。

「モバイルへの攻撃が少ないのではありません。企業がモバイル端末を狙う脅威について、きちんと見通せていないのだと思います」（カックリル氏）

モバイル端末への攻撃は、ターゲットを特定個人に絞って実行されるため、被害の詳細が明らかになりにくい。その結果、モバイルへの脅威の実態が把握しづらくなっているのではないか、と同氏は見ている。

大体の攻撃はフィッシングから始まっている

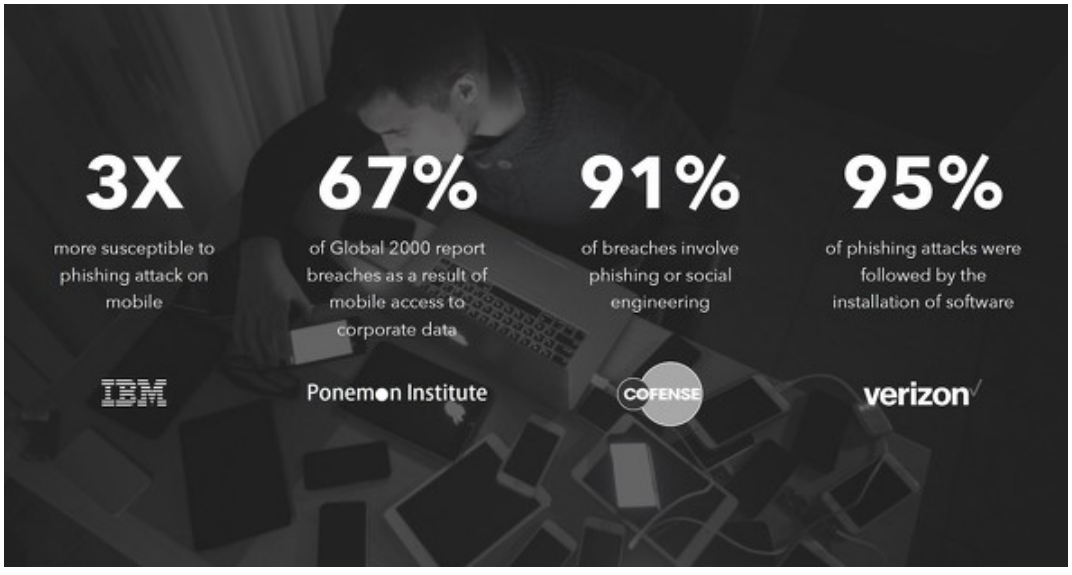
では具体的に、特定の個人をターゲットとする攻撃がどのように実行されるのか。それはほとんどの場合、ソーシャルエンジニアリングで始まる。つまりフィッシングだ。

攻撃者はまず、ユーザーに対して「マルウェアをインストールさせる、パスワードを入力させる」などの行為を誘う。そこで得たログイン情報を使って企業システムへのアクセスを試みるのだという。

「個人の端末への攻撃がきっかけだったとしても、企業に被害が出たとき、ニュースになるのは、例えば“X社で5億レコードの情報が流出した”という情報だけ。誰の端末がどのように攻撃を受けて情報漏えいのきっかけが生まれたのかは報道されません」（カックリル氏）。

報道されるのは、図の右端（企業が攻撃されてどうなったか）のみ

世界企業ランキングリスト「Global2000」のレポートによれば、情報漏えいを経験した企業の67%が「おそらく、モバイル端末への不正アクセスがきっかけ」と考えているという。また、COFENSEの調査によれば、91%の情報漏えいが、フィッシング／ソーシャルエンジニアリングに関連している。



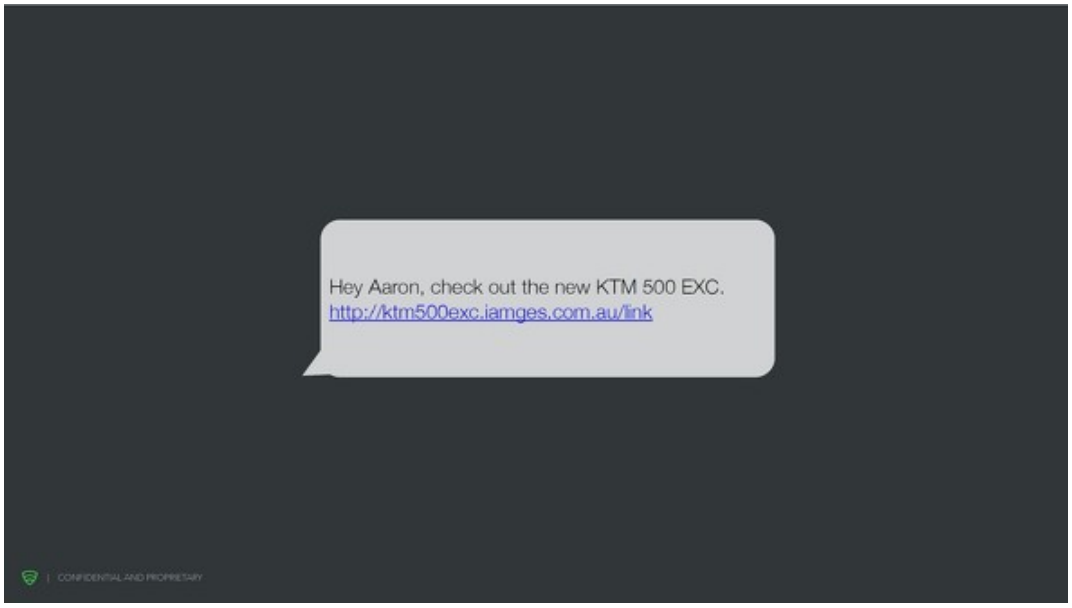
モバイル端末が狙われている

また、2011年にIBMがフィッシング攻撃に使われているサーバを特定し、その中身を分析したところ、**モバイル端末はPCの3倍フィッシングの被害に遭いやすい**という結果が出た。

モバイル端末のほうがフィッシングの被害に遭いやすいのはなぜか

モバイル端末のほうがフィッシングの標的にされやすい理由として、カックリル氏は「UIの違い」を挙げた。

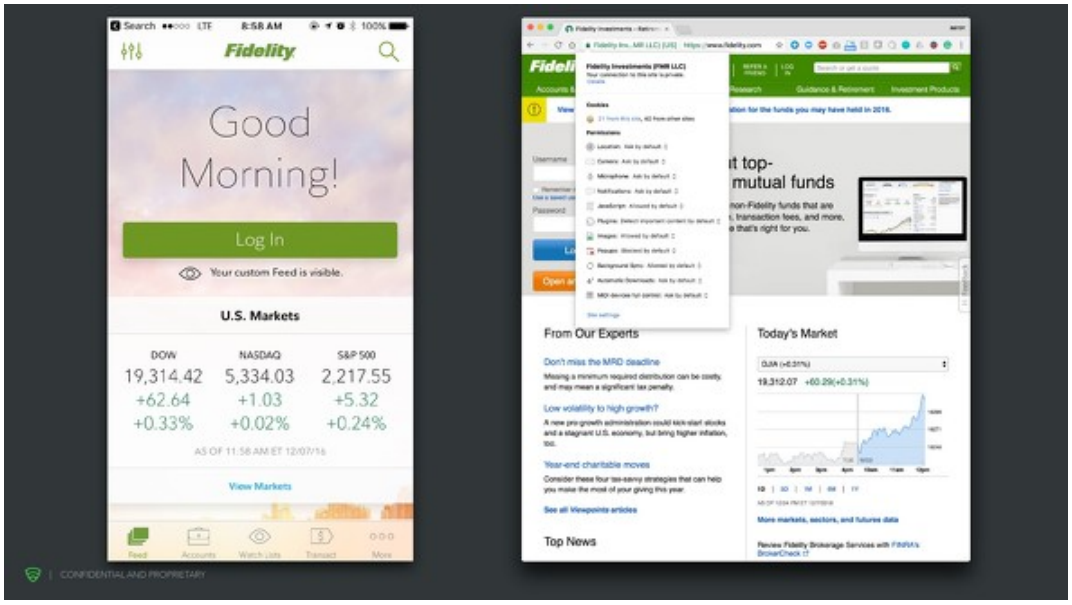
「例えば、私と兄弟は、バイクに乗っています。兄弟になりすました犯罪者からこのようなメッセージが送られてきたとします」（カックリル氏）



「ねえ、この新型バイク見た？」

「……気付きましたか？　このリンク先、“images”のつづりが違うのです。でも、兄弟からのメッセージだと思い込んでいれば、きっとつづりの確認などせずに、リンク先に飛んでしまうでしょう。しかも現在、なりすましの方法は、少し検索するだけですぐ分かってしまいます」（同氏）

また、PCのブラウザであればSSLの詳細が表示されるが、モバイル端末のブラウザからでは、組織名しか見えない。そのため、正規のサービスに似せて作られたフィッシングサイトを見破るのは、PCよりモバイルのほうが難しい。

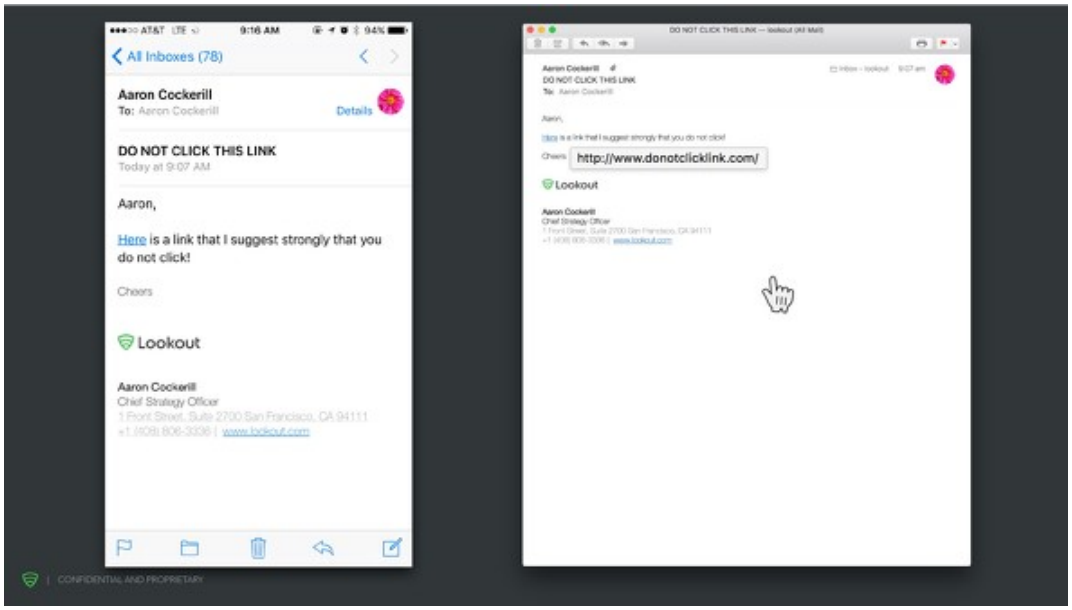


PCブラウザなら当たり前のSSL詳細表示がモバイルには無い

さらに、モバイル端末では多くのサービスをアプリ経由で利用している。しかし実は、アプリ内で信号が暗号化されているかは不明だ。そもそも使用しているアプリが、本当に正規サービスからリリースされたものかすら分からない。

【関連記事】Samsungとは無関係なアプリ「Updates for Samsung」がGoogle公式ストアで公開、日本でもユーザー獲得中

また、標的型メール攻撃を受けたとき、PCの場合はカーソルをホバリングすればリンク先が見える。しかし、モバイルに同様の機能は無い。



モバイルにはカーソルをホバリングしてリンク先を確認する機能が無い

そして、SNSのメッセージ機能でリンクを送るのは、会社のメールでリンクを送るよりはるかに簡単だ。

ドイツ、スウェーデン、フィンランドで発生した標的型攻撃は、Facebookのメッセージ機能を使ったものだった。ターゲットの元には、ある日URLと「見て！あなたがこの動画に写っているよ！」とだけ書かれたメッセージが送られてくる。**PCからアクセスするとYouTubeにつながるが、モバイルのブラウザからアクセスすると一瞬YouTubeのアプリが立ち上がり、その後すぐFacebookによく似たサイトに戻り、ログイン情報の入力を求めてくる。**これは、明らかにモバイル端末だけをターゲットにした攻撃だったという。

以上のように、モバイル端末は、われわれユーザーの心理的な弱さを狙った攻撃を受け続けている。個人の対策が弱ければ、その個人がアクセスするサービスが被害を受けてしまう。

それではなぜ、個人の端末を狙った攻撃をシステムで防ぎきれないのか？　その疑問に対し、カックリル氏は「正確には、個人の端末を監視する仕組みそのものは“違法”ではないのです」と答えた。（後編に続く）