報道関係者各位

2015 年 7 月 14 日

3 人の政治家が公衆無線 Wi-Fi での ハッキング被害を経験

（2015 年 7 月 9 日ヘルシンキ発 － フィンランド本社発表資料抄訳）

カフェやホテルなどの公共の場で無料の無線 Wi-Fi を使用した際に、E メールや金融、ソーシャルネットワーキングの情報などが簡単に盗まれてしまうことが実験で明らかになりました。

ロンドンで行われた調査で、公衆無線 Wi-Fi を使用しているターゲットから個人データが簡単にハッキングされることがあることが分かりました。セキュリティやプライバシー保護のソフトウェアを手掛けるエフセキュアは、侵入テストを専門とする Mandalorian Security Services と Cyber Security Research Institute と協力して、テストを行いました。テストは 3 人の政治家のデバイスに侵入するというものでした。

英国政界で大きな権力を持つ議会から選ばれた 3 人の政治家は、**デイヴィッド・デイヴィス下院議員、メアリー・ハニボール欧州議会議員、ストラスバーガー上院議員**です。3 人は、それぞれの議会において重要な地位にありがらも、正式なトレーニングを受けておらず、3 人全員が通常使用していると認める公衆無線 Wi-Fi の使用中にコンピュータが比較的簡単に攻撃される可能性があるという情報も知らされていないと認めました。調査は 3 人の政治家の許可を得て行われました。

自分の E メールにアクセスされたデイヴィス議員は、「正直に言って、かなり恐ろしいです。抜き取られたのはとても厳重なパスワードです。多くの人が使っているものよりも厳しいパスワードでした。これでは全く『パスワード』とは言えません」とコメントしました。驚くべきことに、パスワードはどんなに厳重なものであっても破られてしまいます。公衆無線 Wi-Fi は本質的に安全ではないのです。ユーザ名とパスワードが無線 Wi-Fi のアクセスポイントの裏側に普通のテキスト形式で表示され、ハッカーは簡単に盗むことができるのです。

リスクを分かりやすくするために、エシカルハッカーの Mandalorian は、英国独立党へのくら替えを表明する E メールの下書きを作り、全国紙向けに発表予定の下書きフォルダーに入れました。その後、Mandalorian のペイパルのアカウントが不正アクセスされます。Gmail と同じをユーザ名とパスワードを使ったからですが、これは広く行われていることです。

ストラスバーガー議員の場合には、ホテルの部屋でのボイス・オーバー・インターネットプロトコル（VoIP）の通話が傍受され、インターネット上で無料で使え、しかもマスターするのも比較的簡単なテクノロジーで録音されました。ストラスバーガー議員は、「とても心配です。非常に強力な技術です。初心者が短時間で使えるようになると考えると本当に心配です。（テクノロジーを利用する際には）もっと知っておく必要があることがこれで証明されたと思います。最終的には、自分の面倒は自分で見なければならないのです。他の誰かがやってくれるわけではなく、自分の問題なのですから」と述べました。

欧州議会で「We Love Wi-Fi」キャンペーンを担当しているメアリー・ハニボール欧州議会議員には、カフェでインターネットにアクセスしているときに、フェイスブックから送信したように見える、タイムアウトしたため自分のアカウントに戻るように指示するメッセージをエシカルハッカーが送信しました。ここから、どのようにして同議員が知らないうちに自分のログインパスワードをハッカーに知られ、それを使ってフェイスブックのアカウントにアクセスされたかが明らかになりました。

ほんの数日前に欧州議会のテクノロジー担当者から支給されたタブレットを使っていたハニボール議員は、アドバイスがなかったことを特に懸念しています。「みんなパスワードですべて心配がなくなると思っているのですから、何か手を打つべきだと思います。私はいつもパスワードがポイントだと思っていました。驚きましたしショックです」と述べました。

それぞれの侵入の事例では、ハッカーは簡単にパスワードで保護されたサービスを回避できるということだけではなく、いかにして個人データがさらなる攻撃に利用されるかも明らかになりました。「誰がどのスポーツチームのファンなのかということはハッカーにとっては役に立たない情報だと、普通の人は考えるでしょう」と Mandalorian のディレクターである、スティーブ・ロードは言います。「しかし、それが知られてしまうと、あなたが開封する可能性が高そうな、あなた自身やあなたの好きなものについてのフィッシングメールを、ハッカーは作ることができるのです。メールの中のリンク先をクリックするか、添付ファイルを開けてしまうと、つかまってしまいます。デバイスにマルウェアを入れられ、あなたの情報のすべてを与えてしまうことになるのです。それだけではなく、会社のネットワークにアクセスしているデバイスの場合には、会社の情報も与えてしまいます。」

エフセキュアのセキュリティ・アドバイザーの**ショーン・サリバン**は、公衆無線 Wi-Fi を使う人にこのようにアドバイスします。「公衆無線 Wi-Fi を使うことを恐れるべきではありません。これは素晴らしいサービスです。しかし、それにはリスクがあり、自分を守る責任は自分にあるということを理解しなければなりません。仮想プライベートネットワーク（VPN）というソフトウェアを使えばよいのです。電話やタブレット用にはアプリがあります。当社の Freedome VPN はデバイスからネットワークに送られるすべてのデータを暗号化しますので、ハッカーは使えるものは何も盗めないのです。オンにするだけで、公衆無線 Wi-Fi を使う場合でも、可能な限り安全に保護されますので、安全かどうかを心配せずに、自分のやりたいことに集中することができます。」

詳細情報:

The Great Politician Hack （ポッドキャストと動画）http://privacy.f-secure.com/2015/07/08/the-great-politician-hack/

Freedome https://www.f-secure.com/ja_JP/web/home_jp/freedome

エフセキュア株式会社 会社概要

http://www.f-secure.co.jp/

F-Secure – Switch on freedom

エフセキュアは、25 年以上にわたり世界中の数千万人もの人々をオンラインの脅威から守ってきました。弊社の受賞歴のある製品は、クライムウェアから企業を標的としたサイバー攻撃に至るまで、あらゆる脅威から人々と企業を守っており、40 カ国を超える国々に広がる 6000 以上のリセラー、200 以上の通信事業者から購入することができます。弊社の使命は、人々が周りの世界と安全につながることができるように支援することです。この動きに参加し、自由のために闘いましょう。1988 年創業のエフセキュアは、NASDAQ OMX Helsinki Ltd に上場しています。

エフセキュア株式会社は、エフセキュア社 100%出資の現地法人として設立され、以降、増収を続けながら順調に企業規模を拡大しており、2014 年 5 月に日本法人設立満 15 周年を迎えました。

会 社 名: エフセキュア株式会社
カントリーマネージャ: キース・マーティン
所 在 地: 〒102-0072 東京都千代田区飯田橋 3-11-14 GS 千代田ビル 5F
設 立: 1999 年 5 月
事業内容: セキュリティ関連製品・サービスの販売およびサポート

Mandalorian について

Mandalorian は、2005 年の創業以来、高品質かつ高価値のセキュリティ調査サービスを提供しています。専門領域コンサルタントである Mandalorian は、専門家や個人サービス向けに一貫性のある商業・技術サポートを提供し、できるだけ一緒に働きやすい存在であることを目指しています。その裏付けとなる Mandalorian の認定書が、さまざまなテストサービスを提供するための当社の技術力を証明しています。とりわけ、あらゆるデバイスやシステム、アプリケーションについてのカスタムメイドのテストを得意としています。Mandalorian は本拠を英国においていますが、防衛関係、政府機関、金融機関など、世界中の官民両方の分野にサービスをご提供しています。

さらに詳しい情報は、電話は+44(0)1256 830 146 に、E メールは info@mandalorian.com 宛てにお寄せくださるか、http://www.mandalorian.com をご覧ください。

本件に関するお問合せ先
エフセキュア株式会社
マーケティング部
Tel: 03-3556-6301 Fax: 03-3556-6295
Email: japan@f-secure.co.jp
〒102-0072 東京都千代田区飯田橋 3-11-14 GS 千代田ビル 5F
URL: http://www.f-secure.com
Blog: http://blog.f-secure.jp