OUCH! | 2017 年 03 月

コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

OUCH!

今月のトピック...

- はじめに
- モバイルアプリの取得
- 権限
- アプリの更新

モバイルアプリを安全に利用するには

はじめに

タブレット、スマートフォンや時計などのモバイルデバイスは、仕事およびプライベートにおいて利用されているメインのテクノロジーとなっています。モバイルデバイスが万能な理由は、利用可能なアプリが無数にあるからです。これらのアプリを使うことで、生産性を上げたり、すぐに他人と情報を共有したり、コミュニケーションが取れたり、トレーニングや教育をしたり、はたまた単純にゲームなどで楽しむことも可能になります。しかし、これらのモバイルアプリが提供する力には、リスクが伴います。このニュースレターでは、モバイルアプリを最大限活用しつつ、安全に利用する方法を紹介します。

ゲストエディタ

ジョシュア・ライト氏は、Counter Hack社のテクニカルディレクターとして活躍する傍ら、SANS Instituteのシニア講師を務めており、SEC575コース、Mobile Device Security and Ethical Hacking, and Hacking Exposed: Wireless の著者でもあります。また、ツイッター(**@joswr1ght**)を通じて連絡を取ることができます。

モバイルアプリの取得

最初にできることは、モバイルアプリを安全で信頼できるところからダウンロードすることです。サイバー犯罪者は、正規のアプリに見せかけた悪意あるアプリを作成し、配布することをマスターしています。この悪意あるアプリをインストールしてしまった場合、犯罪者はそのモバイルデバイスを完全に乗っ取ることができてしまいます。アプリを良く知られている、信頼できるところからのみダウンロードすることで、悪意あるアプリをインストールしてしまう確率を減らすことができます。そして、気付いていない人もいるかもしれませんが、モバイルデバイスの種類によってアプリダウンロードのオプションが変わります。

例えば、AppleのiPadやiPhoneは、Apple App Storeからのみモバイルアプリをダウンロードします。利点は、アプリが提供される前にAppleがセキュリティチェックを行うことです。Appleは、すべての悪意あるアプリを見つけることはできませんが、この管理された環境によって悪意あるアプリがインストールされる確率を劇的に減らすことが可能になっています。さらに、Appleはストアで公開しているアプリで悪意あるものを発見したら、そのアプリを素早く削除します。Windows Phoneも似たような手法でアプリの管理を行っています。

AndroidのモバイルデバイスはAndroidは、インターネット上のどこからでもモバイルアプリをダウンロードできる柔軟性を提供しています。この柔軟性が提供されていることによって、責任も重くなります。すべてのアプ

モバイルアプリを安全に利用するには

リがレビューされていないため、どのモバイルアプリをダウンロード、インストールするかをきちんと確認する必要があります。Googleは、Google Playと呼ばれる、Appleと類似の管理されたモバイルアプリストアを管理しています。Google Playからダウンロード可能なモバイルアプリは、基本的なセキュリティチェックを通っています。そのため、Androidデバイスを利用している場合は、Google Playからのみモバイルアプリをダウンロードするよう推奨します。Androidのモバイルアプリを他のウェブサイトからダウンロードするこはしないでください。なぜなら、サイバー犯罪者を含む世界中の誰でも悪意あるモバイルアプリを作成、配布し、そして自身のモバイルデバイスを感染させるために騙すことが可能です。追加の保護として、モバイルデバイスにアンチウイルスソフトウエアをインストールすることを推奨します。

モバイルアプリを安全に利用するための秘訣は、信頼できるところからのみアプリをインストールし、更新は利用可能になったら適用し、必要な権限のみを与えることです。

どのモバイルデバイスを使っていてもできることとして、新しいアプリやダウンロード数が少ないアプリ、または肯定的なコメントが少ないアプリをダウンロードしないことが挙げられます。アプリの利用可能な期間が長ければ長いほど、多くの人が利用しており、肯定的なコメントも多く、そのアプリを信用できる可能性が高くなります。また、必要性があって、実際に利用するアプリのみをインストールしてください。自分自身に「このアプリは必要か？」を聞いてみてください。アプリが増えるごとに脆弱性のリスクが増えるだけでなく、プライバシーの問題もあります。アプリを実際に利用しなくなったら、モバイルデバイスから削除してください（必要になったらいつでも再度追加できます）。最後になりますが、モバイルデバイスを脱獄またはルート化しないでください。これは、許可されていないアプリをインストールしたり、既存の作り込まれた機能を変更したりするためにデバイスをハッキングする行為です。これによってモバイルデバイスに作り込まれたセキュリティ機構をバイパスまた取り除くだけでなく、サポート契約や保証を無効にしてしまうことになることが多いです。

権限

信頼できるところからモバイルアプリをインストールしたら、プライバシーを保護するために安全な設定を行ってください。モバイルアプリにアクセス権を与える前に一度考えてください。アプリが欲している権限を与えたいか？そして、アプリにその権限は必要なのか？例えば、アプリの中には位置情報を利用するものがあります。アプリに位置情報を常に知らせている場合は、アプリの作者に自身の行動をトラッキングすることを可能にするだけでなく、この情報をアプリの作者によって売られる可能性があります。その権限を与えたくない場合は、拒否する、または要件を満たす別のアプリを探してみてください。たくさんのアプリがあることを覚えておいてください。

モバイルアプリを安全に利用するには

アプリの更新

パソコンやモバイルデバイスのオペレーティングシステムと同様に、モバイルアプリも更新が必要です。犯罪者は、常にアプリの脆弱性を探索し、発見しています。アプリの開発者は、これらの脆弱性を修正し、デバイスを保護するためにアップデートを提供しています。アプリの更新があるか否かを確認し、インストールする頻度が高ければ高いほど良いです。多くのデバイスでは、モバイルアプリの更新を自動的に行うよう設定できます。この設定を有効にすることを推奨します。これができない場合は、最低でも2週間に一度は、モバイルアプリの更新があるか否かを確認するよう推奨します。最後にアプリの更新が終わったら、新たに必要となった権限など無いか、確認してください。

詳しくは

毎月発行のセキュリティアウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティアウェアネスソリューションのサイトをご覧ください。
securingthehuman.sans.org/ouch/archives

日本語版翻訳チーム

日本語版翻訳－NRIセキュアテクノロジーズ株式会社

NRI セキュアテクノロジーズは、国内でも有数の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションなどの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。http://www.nri-secure.co.jp

リソース

ソーシャルエンジニアリングについて:	https://securingthehuman.sans.org/ouch/2017#january2017
モバイルデバイスを安全に破棄する:	https://securingthehuman.sans.org/ouch/2016#december2016
タブレットを安全に使用するには:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH! アーカイブと翻訳:	https://securingthehuman.sans.org/ouch/archives
Mobile Device Security Course:	https://sans.org/sec575

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Translated By: 内山　貴之, 時田　剛