OUCH! | 2015 年 01 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
- アプリの取得
- 権限
- アプリの更新

モバイルアプリをセキュアに利用するには

はじめに

タブレットやスマートフォンなどのモバイルデバイスは、業務やプライベートを問わず利用される主要なテクノロジーになりました。モバイルデバイスが万能であるという理由は、様々な機能を多くのアプリから取捨選択して利用できるカスタマイズ性にあります。これらのアプリを利用することで生産性を上げたり、他の人とコミュニケーションを取ったり、情報を共有したり、学んだり、楽しんだりすることができます。しかし、これらモバイルアプリはリスクも伴いますので、モバイルアプリをセキュアに利用および管理するためのステップをご紹介します。

ゲストエディター

クリストファー・クローリー氏は、コンサルタント業を営むかたわら、SANS認定講師として講義を担当するほか、コースの著者でもあります。ツイッター（@CCrowMontanceChrisCrowley）やGoogle+（+ChrisCrowley）で積極的に情報発信をしています。

アプリの取得

最初のステップは、アプリを信用できる安全なソースから取得することです。誰でもモバイルアプリを作成することが可能であることを念頭に入れて、アプリを取得するソースには気を付けなければなりません。サイバー犯罪者は、あたかも正規のアプリに見える感染されたモバイルアプリを作成し、配布する技術に長けてきています。これらの感染されたアプリをインストールしてしまった場合、サイバー犯罪者によってデバイスを乗っ取られ、メールを読まれてしまったり、通話を盗聴されたり、アドレス帳から情報を取得されたりしてしまいます。広く利用され、かつ信頼できるソースからのみアプリをダウンロードすることによって、感染されたアプリをインストールしてしまう可能性を減らすことができます。気づいていないかもしれませんが、モバイルデバイスの種類によってダウンロード可能なソースは異なります。

iPadやiPhoneのようなApple製の機器の場合、Apple App Storeと呼ばれるAppleが管理している環境からのみモバイルアプリがダウンロード可能です。この利点は、Appleがモバイルアプリおよび開発者に対して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開発者および感染されたアプリを見つけることができるわけではないですが、このようなアプリ管理下にあることで、ユーザが感染されたモバイルアプリをインストールしてしまう可能性を低くしています。また、Appleによって感染していると疑いのあるモバイルアプリが発見された場合、そのモバイルアプリは速やかに削除されます。ちなみにWindows Phoneでも似たような手法を使って、モバイルアプリを管理しています。

Androidのモバイルデバイスは上記とは異なります。Androidは、極めて自由度が高いため、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することが可能です。この自由度が高い分、ユーザは自分で自分を守る責任が伴います。もちろん、すべてのアプリがレビューされている訳ではないため、ダウンロード・インストールするモバイルアプリの取捨選択により一層気を付けなければなりません。Googleによってモバイルアプリを管理する環境と

モバイルアプリをセキュアに利用するには

しては、Google Play があり、AppleのApp Storeと良く似ています。それはGoogle Playからダウンロードできるモバイルアプリは基本的なチェックが行われたものだということです。そのため、Androidデバイスで利用するモバイルアプリは、すべてGoogle Playからダウンロードすることを推奨します。他のウェブサイトからAndroid用のモバイルアプリをダウンロードすることは控えてください。なぜなら、サイバー犯罪者だけではなく、誰でも悪意あるモバイルアプリを作成、配布、そしてモバイルデバイスへインストールさせるように誘導することが可能だからです。追加の防御としては、モバイルデバイスにアンチウイルスソフトウェアをインストールすることも検討してください。

モバイルアプリを安全に利用するための鍵は、信頼できるソースからのみアプリをインストールし、アプリが最新の状態であることを確保しつつ、適切な権限が与えられていることを確認することです。

さらなるリスクの軽減策として、ダウンロード数が少ない新しく公開されたアプリや、評価が低い、コメントが少ないアプリは避けましょう。一般的には、アプリが長く公開されていて、評価が高いコメントが多ければ多いほど、信頼できる可能性は高くなります。また、必要としていて利用するアプリのみをインストールするようにしましょう。インストールする前に、「このアプリは本当に必要なのか？」と自問自答してみてください。また、すべてのアプリには、脆弱性が含まれている可能性があることを理解するだけではなく、プライバシーの問題が付随することを忘れないでください。そのため、アプリの利用を停止した場合は、モバイルデバイスから削除するようにしてください。（改めて必要になった場合は、またインストールすることができます）

最後に、モバイルデバイスを脱獄（JAILBREAK）またはルート権限を取得したくなることもあるかと思います。脱獄（JAILBREAK）またはルート化と呼ばれる一連のプロセスでは、デバイスをハッキングし、承認されていないアプリをインストールしたり、既存の機能を変更したりします。ここでは、モバイルデバイスを脱獄またはルート化することは推奨できません。なぜなら、モバイルデバイスに組み込まれているセキュリティ機能を無効にしたり回避できるようになったりしてしまう可能性があるからです。さらに、これを行うことによって保証やサポートなどの保守契約を無効にしてしまう可能性が高いのも理由です。

権限

信頼できるソースからモバイルアプリをインストールした後のステップは、プライバシーを守るために正しく設定できていることを確認することです。モバイルアプリをインストールおよび設定するためには、特定の権限を与える必要があります。アクセスを承認する前に、本当にアプリはそれらの情報へのアクセス権を必要とするのかを考えてみてください。例えば、いくつものアプリは位置情報を利用します。そのアプリにいつでも位置情報にアクセスできる権限を与えた場合、アプリの開発者に行動パターンを把握されてしまう恐れがあり、その情報を他者に売られてしまう可能性もあります。アプリが必要としている権限を与えたくない場合は、自身のニーズにあった他のアプリを探すことができますので、たくさんの選択肢があることを覚えておいてください。Appleデバイスは、位置情報へのアクセスなど、いくつかの権限の設定画面からいつでも変更可能です。WindowsおよびAndroidのモバイルデバイスは、少

モバイルアプリをセキュアに利用するには

し違っており、全て許可か全て拒否かのアプローチのみ提供しています。必要としているすべての権限を与えない限り、そのアプリをインストールすることができません。

モバイルアプリの更新

コンピュータやモバイルデバイスのOSと同様に、モバイルアプリも適切な更新を必要とします。犯罪者は、常にアプリの弱点を探索しています。そして弱点を発見すると、その弱点を突くための攻撃手法を作成するのです。アプリの開発者は、モバイルデバイスを守るために、これらの弱点を修正するためのアップデートを作成し、リリースしていますので、アップデートの有無を確認しインストールする頻度が高ければ高いほど安全だと言えます。多くのプラットフォームでは、アップデートの有無を自動的にチェックし、インストールするように設定することが可能ですから、モバイルアプリの自動更新設定にすることを推奨します。この設定にできない場合は、2週間に一度はモバイルアプリのアップデートの有無を確認することを推奨します。また、アプリがアップデートされた後で、新たに追加された権限を確認することも忘れないようにしてください。

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。http://www.securingthehuman.org

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、国内最大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。

リソース

ソーシャルエンジニアリングについて:	http://www.securingthehuman.org/ouch/2014#november2014
携帯端末の処分方法:	http://www.securingthehuman.org/ouch/2014#june2014
タブレット端末の安全な使い方:	http://www.securingthehuman.org/ouch/2013#december2013
良く使われるセキュリティ単語集:	http://www.securingthehuman.org/resources/security-terms
SEC575: モバイル機器セキュリティコース:	http://www.sans.org/sec575

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

