OUCH! | 2016 年 04 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
・ハッキングに遭ったことを示す手がかり
・対応策

ハッキングに遭ったときの対応策は？

はじめに

自身のパソコンやモバイルデバイスを守ることは重要だと考えるから、安全にするために色んなことをしていることでしょう。しかし、どんなに安全にテクノロジーを利用しても、そのうちハッキングまたは不正アクセスの被害に遭う可能性はあります。このニュースレターでは、自身のパソコンやモバイルデバイスがハッキングの被害に遭ったかを確認する手段と、ハッキングされた場合の対応策を紹介します。最終的には、異常を早く検知し、素早く対応することで、サイバー犯罪者による被害を最小限に抑えることができることを覚えておいてください。

ゲストエディター

サマンサ・ダビソン（@sam_e_davison）は、Uber社の Security Awareness and Education Program Manager で、世界中350都市にい る従業員の教育をしています。

ハッキングに遭ったことを示す手がかり

ハッキングの被害に遭ったかを確認するのは大変困難です。なぜなら、一つのことを確認すれば良いという訳ではないからです。その代わり、ハッカーはいくつかの手がかりを残します。これらの手がかりはインディケータ（何かを示すもの）と呼ばれることが多いですが、自身のシステム挙動がこれらの手がかりと一致した場合、ハッキングの被害に遭った可能性が上がることになります。

- アンチウイルスプログラムから何かに感染したというアラートが発信された場合。特に影響を受けたファイルを隔離または削除できなかった場合
- ブラウザのホームページが知らないうちに変わった場合。または、ブラウザが勝手に様々なサイトに接続してしまう場合
- 自身が作成した記憶の無いアカウントがパソコンまたはデバイス上に存在する場合。また、インストールした記憶の無いプログラムが実行されている場合
- パソコンまたはアプリケーションのクラッシュが頻発する場合。または、知らないアプリに関するアイコンがあったり、見知らぬウィンドウがポップアップしたりする場合
- アプリケーションのインストールまたは更新を行っていないにも関わらず、プログラムによってシステムの変更を行うために認証を要求される場合
- パスワードが正しいと確信を持っているにも関わらず、システムやオンライン上のアカウントにログインしようとした場合にパスワードが間違っていると指摘された場合
- 友人や知人から送った記憶も無いスパムメールをなぜ送っているのかを尋ねられた場合
- モバイルデバイスが使用しているSMS番号に対して不正な請求があった場合

ハッキングに遭ったときの対応策は?

- モバイルデバイスが突然、大量のデータまたは電池を使用した場合

対応策

パソコンまたはデバイスがハッキングされたと思った場合、対応は早ければ早い方が良いです。被害にあったパソコンまたはデバイスが業務のために会社から支給されたものであれば、自身だけで問題解決を図らないでください。なぜなら、良い事よりも悪い事の方が起きる可能性が高いでなく、調査を行う上で重要な手がかりを破壊してしまう可能性もあるからです。そのため、まずインシデントがあったことを会社に報告してください。報告は通常、ヘルプデスク・セキュリティチームまたは上司を通じて行われます。何かしらの理由で会社に報告できない事情がある場合や、報告の遅れが気になる場合は、パソコンまたはデバイスをネットワークから切り離した状態でスリープ・サスペンドまたは機内モードに設定してください。ハッキングの被害にあったかどうか分からない場合でも、念のために報告しておくことが大事です。ハッキングされたパソコンまたはデバイスが会社貸与のものではなく私物の場合は、以下の対応策が考えられます：

利用しているパソコンまたはデバイスは、いずれハッキングされてしまう可能性はあるが、インシデントを早期に発見し、対応は早ければ早い方が良い。

- **パスワードを変更する** これは、パソコンやモバイルデバイスのパスワードだけでなく、オンラインアカウント用のパスワードも含めた全てのパスワードを変更してください。ハッキングの被害に遭ったデバイスを使ってパスワードの変更処理を行わないでください。代わりに安全だと思われる違うパソコンまたはデバイスを使って、それぞれのパスワードを変更してください。
- **アンチウイルス** アンチウイルスソフトウエアから感染したファイルに関する通知があった場合、アンチウイルスソフトウエアが推奨する対応策を実施してください。典型的な対応策の中には、ファイルを隔離する、ファイルを駆除するまたはファイルを削除する。　などがあります。多くのアンチウイルスソフトウエアは、その特定の感染に関する情報を提供しているリンクを示してくれます。対応に迷った場合は、ファイルを隔離してください。隔離できない場合は、ファイルを削除してください。
- **リビルドする** 感染による被害を修正できない場合、またはシステムが完全に直ったという確信を得たい場合は、安全な方法としてリビルドするという手法があります。パソコンの場合は、システム開発者が提供する手順に従ってください。多くの場合では、組み込まれているユーティリティを使って、オペレーティングシステムを再インストールすることになります。これらのユーティリティが無い、壊れている、感染してしまっている場合は、システム開発者に連絡するまたは、ホームページを訪問してみてください。この場合は、バックアップからの再インストールはしないでください。なぜなら、攻撃者が悪用した脆弱性がそのまま残っている可能性があるからです。バックアップは、データをリカバリする目的でのみ利用してください。モバイルデバイスの場合は、デバイスの開発者またはサービスプロバイダが提供する手順に従ってください。これらの手順

ハッキングに遭ったときの対応策は?

は、それぞれのウェブサイト上に記載されているはずです。多くの場合は、モバイルデバイスを出荷状態に戻すことになります。リビルドするにあたり不安な場合は、これらのサービスを提供する事業者に頼んでみてください。パソコンまたはモバイルデバイスが古い場合は、新しいものを買う方が簡単でかつ安いかもしれません。最後になりますが、パソコンまたはモバイルデバイスをリビルドした後、または新しいデバイスを購入した後は、最新のパッチやアップデートを適用し、自動アップデート機能も有効にしてから利用してください。

- **バックアップ** 自身を守るためにできる一番重要なステップは、定期的にバックアップを取ることです。バックアップの頻度が高ければ高いほど良いです。ソリューションやツールの中には、一時間おきに新しいファイルおよび変更されたファイルをバックアップしてくれるものもあります。バックアップを取る手法やツールに限らず、そのバックアップからファイルを復元できるか否かは確認してください。ハッキングの被害に遭った際、バックアップからのデータ復旧が唯一の復旧方法であることが多いです。
- **法執行機関** 恐喝に遭っていると感じた場合は、法執行機関に届出してください。

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

日本語版翻訳ー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。 http://www.nri-secure.co.jp

リソース

バックアップと復旧:	https://securingthehuman.sans.org/ouch/2015#august2015
パスフレーズについて:	https://securingthehuman.sans.org/ouch/2015#april2015
マルウエアとは:	https://securingthehuman.sans.org/ouch/2016#march2016
タブレットを安全に使用するには:	https://securingthehuman.sans.org/ouch/2016#january2016

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