OUCH! | 2014 年 5 月号

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

OUCH!

今月のトピック...

- はじめに
- 確認項目
- 対処方法

ハッキングされてしまったら？

はじめに

多くの人々がコンピュータや情報の安全を考慮しており、さまざまな対策をしています。しかし、車の運転と同じで、いくら気をつけても事故に遭わないとは限りません。今月号では、コンピュータがハッキングされているか判断する確認項目や、ハッキングされた場合の対応方法を説明します。結局のところ、コンピュータがハッキングされたら、なるべく早く検出し、なるべく早く対処することが被害を最小限にくい止めることになります。

ゲストエディター

ジェイク・ウィリアムズ（Jake Williams：malwarejake.blogspot.co, @MalwareJake）は、CSRgroup Computer Security Consultants社の主任科学者で、SANSのFOR526：Memory ForensicsとFOR610：Malware Reverse Engineeringの共同執筆者です。

確認項目

まず、コンピュータがハッキングされているかを判断する手順は、多くの場合一律ではありません。一般的な兆候がいくつかあり、その兆候が明確な場合、コンピュータがハッキングされていると判断できます。いくつか例を挙げます。

- ウイルス対策プログラムから感染を警告された。警告メッセージに、感染ファイルを削除または隔離できなかったと表示された。
- ブラウザのホームが知らない間に変更されていた。ブラウザが自分の意図しないWebサイトを訪問した。
- コンピュータに見覚えのない新しいアカウントがある。
- インストールした覚えのない新しいプログラムが起動している。
- コンピュータが頻繁にクラッシュする。または動作が非常に遅い。
- アプリケーションのインストールや更新をしていないのに、コンピュータからシステム変更の承認を求められる。
- 見覚えのないプログラムがインターネットへのアクセス許可を求めていると、ファイアウォールから警告が表示される。

対処方法

コンピュータがハッキングされたと判断したら、なるべく早く対応しましょう。職場から支給されているコンピュータや仕事用のコンピュータの場合、自分で修復作業をしないでください。さらに電源も切らないでく

ハッキングされてしまったら?

ださい。自分ではよかれとして行ったことも、損害を大きくする可能性があるだけでなく、解析調査に役立つ重要な証拠を破壊する可能性もあります。最善の方法は、ヘルプデスクやセキュリティ担当者、上司に連絡をとり、コンピュータが侵害されたことを報告することです。やむを得ず会社に連絡がとれない場合や、遅れが心配される場合は、コンピュータをネットワークから切断し、スリープ状態か休止状態にしておきます。自分でハッキングされたかわからない場合でも、念のため報告しましょう。多くの企業では、このような状況に対応する部門が設置されており、処理手順が決められているため、担当者に任せましょう。

あなたのコンピュータはいつ侵害されるかわかりません。早期発見、早期対応が一番の対策です。

個人用のコンピュータの場合、自己対処できる手順はいくつかあります。

- **バックアップ**：最も重要なのは、事前にバックアップをとっておくことです。具体的には、定期的にデータをバックアップし、バックアップからのファイルの復旧が可能なことを確認しておいてください。コンピュータがハッキングされた場合に考えられるのは、システムのハードドライブを初期化し、オペレーティングシステムを再インストールすることや、場合によっては新しいコンピュータを購入することになります。いずれにしても、個人のデータをバックアップし、復旧することが必要になります。
- **パスワードの変更**：全てのパスワードを変更してください。コンピュータやモバイル機器上のパスワードだけでなく、オンライン上の全てのパスワードを含みます。感染していない安全だと思われる別のコンピュータから全てのオンラインのパスワードを変更してください。
- **ウイルス対策**：ウイルス対策ソフトウェアが感染ファイルを警告している場合、ソフトウェアが推奨する手順に従ってください。通常、感染ファイルの隔離、駆除、削除が可能です。ウイルス対策ソフトウェアのほとんどは、感染ファイルについて詳細情報を提供しています。不審に感じたら、ファイルを隔離することです。不可能な場合はファイルを削除してください。
- **再インストール**：ウイルス対策のソフトウェアでマルウェアを駆除できない場合の最も安全な復旧方法は、コンピュータをゼロから再構築することです。まず、ネットワークからコンピュータを切断し、製造元の指示に従います。オペレーティングシステムの再インストールとは、ほとんどの場合ビルトインのリカバリパーティションを使います。リカバリパーティションが見つからない場合や、破損している場合、汚染している場合には、製造元に連絡してリカバリDVDの送付を依頼してください。バックアップからはオペレーティングシステムを再インストールしないでください。バックアッ

ハッキングされてしまったら?

プには、以前悪用されたのと同じ脆弱性が存在する可能性があります。バックアップを使う必要があるのは個人データの復旧のみです。さらに、コンピュータが古い場合、再構築に時間を費やすより、新しいコンピュータを購入する方が簡単（おそらく割安）です。

- **専門家の支援**：自分で修復するスキルや知識がない場合は、専門家にコンピュータを渡して修復することも検討してください。考えられる状況としては、ハッキングされてから、バックアップが古かったり不完全であることがわかり、写真、文書、ビデオなどの重要なファイルを感染マシンから新しいマシンへコピーする必要がある状態です。このような状況で安全な方法は、認定資格を持った専門家に依頼することです。専門家は、マルウェアが転移しないように安全にファイルを復旧し、マルウェアも新しいコンピュータにコピーされる危険を防ぐことができます。

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

OUCH! バックアップ:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! パスワード:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! マルウェアについて:	http://www.securingthehuman.org/ouch/2014#february2014
ディテクティング Evilポスター:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 坂 恵理子, 関取 嘉浩