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

ハッキングされているかも？

はじめに

どれだけあなたがセキュアな環境にいようと、車の運転のように事故を起こす可能性があるでしょう、あるいは事故に巻き込まれるかもしれません。以下にハッキングをされているか見極める手がかりと、ハッキングされている場合にするべきことを挙げていきます。良くない事態の発生を検知するタイミングが早ければ早いほど、問題を修正できる可能性は高まります。

ハッキングされている可能性を示す手がかり

- 使用しているアンチウイルス製品が、システムのウイルス感染を示す警告を表示している。その警告が、あなたを騙してある番号に電話をかけさせたり、何か別の製品をインストールさせたりするウェブサイトからのポップアップ表示ではなく、間違いなくあなたが使用しているアンチウイルス製品から発せられていることを確認しましょう。はっきりとはわかりませんか？使用しているアンチウイルス製品を開いてみてください。
- あなたのパソコンが暗号化され、ファイルを取り戻すために身代金を支払う必要があると脅すポップアップが表示されている。
- 使用しているウェブブラウザが、あなたの意志とは関係なく様々なウェブサイトを開いてしまう。
- あなたのパソコンやアプリケーションがしばしばクラッシュし、知らないアプリのアイコンが表示されていたり、怪しいウィンドウが突然現れたりする。
- 間違えていない確信があるにも関わらず、あなたのパスワードが機能しない。
- 送信していない確信があるにも関わらず、あなたの友達から、なぜスパムメールを送り付けてくるのかと質問される。
- クレジットカードの請求が届いていたり、操作した記憶が無い銀行口座からの引き落としが発生していたりする。

どのように対応すれば良いか

ハッキングされているかもしれないと疑念を抱いたら、すぐに行動に移るべきです。ハッキングが仕事と関係ある場合、自分で解決しようとせず、すぐに関係者に報告してください。個人のシステムやアカウントの場合は、次に挙げる項目を試してみてください。

パスワードを変更する：あなたのコンピュータやモバイル機器のパスワードだけでなく、オンラインで使用しているアカウントのパスワードも含みます。パスワード変更の際は、ハッキングされたコンピュータを使わず、セキュアであることが判明している別のシステムを使用しましょう。多くのアカウントを保有している場合、最も重要なものからパスワード変更を開始してください。全てのパスワードを管理しきれないのであれば、パスワードマネージャを使用してください。

金融関係：クレジットカードや銀行口座に関わる問題の場合、すぐに銀行やクレジットカード会社に電話しましょう。電話をかける際は、クレジットカードの裏や利用明細に掲載されている電話番号を利用し、もしくは信頼のできるコンピュータから、金融機関のウェブサイトにアクセスしましょう。また利用停止の手続き（米国の場合、信用調査会社でクレジットフリーズの手続きを実施しましょう）を検討するべきです。

アンチウイルス製品：使用しているアンチウイルス製品から、ファイルのウイルス感染が報告された場合、その製品が推奨する行動に従いましょう。大半のアンチウイルス製品には、特定のウイルス感染への対処法について学べるページへのリンクがついています。

再インストール：ウイルス感染したコンピュータを修復できない、もしくはより確実なシステムの安全性を求めたい場合、オペレーティングシステムを再インストールしましょう。バックアップからの再インストールは控えてください。バックアップは個人ファイルの復旧にのみ使用するべきです。再構築が面倒だと感じるのであれば、専門のサービスを利用することを検討しましょう。あなたのコンピュータや機器が古いものであれば、新しいものを購入したほうが良いかもしれません。最後に、システムの再構築や新しいコンピュータの購入後、アップデートが完了していることを確認し、可能な限り自動アップデートを有効にしておきましょう。

バックアップ：あなた自身を守る上で鍵となる対策は、日常的にバックアップを取ることで、事前に準備をしておくことです。多くのサービスでは、自動で毎日、さらには毎時間バックアップを取得してくれます。どのサービスを利用するかに関わらず、バックアップ後のファイルが復旧可能であることを定期的に確認しましょう。多くの場合において、バックアップデータの復旧が、ハッキングの被害から復活する唯一の方法となります。

法執行機関：何らかの理由で脅迫されていると感じる場合、インシデントの発生を地域の法執行機関に報告しましょう。なりすましの被害に遭った場合、警察への被害届の提出、国民生活センターや弁護士への相談が有効です。（米国在住でなりすましの被害者である場合、こちらのページを訪問しましょう。HTTPS://WWW.IDENTITYTHEFT.GOV）

ゲストエディタ

ヨハネス・ウルリッヒ博士（@johullrich）は、SANS Technology Instituteの主席研究員としての肩書きのほか、SANS Internet Storm Centerのセンター長であり、SANS特別会員でもあります。ウルリッヒ博士は、共同センサネットワークであるDShieldを開発した実績を持ち、Internet Storm Centerにおいてネットワークセキュリティニュースのポッドキャストを毎日配信しています。

リソース

バックアップと復旧について: https://www.sans.org/u/JGP
パスフレーズについて: https://www.sans.org/u/JGU
パスワードマネージャ: https://www.sans.org/u/JGZ
マルウエアとは: https://www.sans.org/u/JH4
クレジットフリーズ: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

 Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Translated by: 小山 裕之, 時田 剛