OUCH!
月間セキュリティ啓発ニュースレター

あなたは狙われている

はじめに

多くの人は、自分自身や自身が保有するシステム、またはアカウントに大した価値が無いと思っており、自身はサイバー攻撃の標的ではないという誤った考えを持っていますが、これは事実とは全く異なる考えです。どのような形であれ、自宅、職場に関わらず、テクノロジーを使用しているのであれば、犯罪者から見るとあなた自身には間違いなく価値があります。しかし、あなたはラッキーです！あなたは既に、あなた自身というサイバー攻撃に対する最大の防御策を持っているのですから。

なぜ狙われているのか

今日インターネット上には多くのサイバー攻撃者が存在しており、攻撃者それぞれが様々な動機を持って活動を展開しています。では、なぜ彼らはあなたを攻撃したいと考えるのでしょうか。理由は、あなたに対するハッキングが、攻撃者にとって目的を達成する手助けとなるからです。以下に2つの一般的なサイバー攻撃者の例と、攻撃者があなたを狙う理由をご説明します。

⚠ **サイバー犯罪者**：彼らの目的は多くのお金を稼ぐことであり、彼らにとってインターネットの利点とは、ボタンをクリックするだけで簡単に、世界中のユーザを標的にすることができることにあります。そのため、犯罪者があなたからお金を稼ぐ方法は数多く存在します。例えば、あなたの銀行口座や、退職後に使うお金を積み立てておくための口座からお金を盗んだり、あなたの名前でクレジットカードを作ってあなた宛てに請求をさせたり、あなたのコンピュータを踏み台にして他の人にハッキングを仕掛けたり、あなたのソーシャルメディアやゲーム用のアカウントをハッキングして、そのアカウントを他の犯罪者に売ったりするなど、あなたを利用して犯罪者がお金を稼ぐ方法は、ほぼ無限に存在します。多くの人たち（この中にはあなたも含まれます）を、一日でハッキングすることを目的にするサイバー犯罪者が、数十万人も存在するのです。

☆ **標的を絞った攻撃者**：彼らは高度な技術を有するサイバー攻撃者であり、大抵の場合政府や犯罪組織、またはあなたを標的としている競争相手に雇われて活動しています。あなたは自分の仕事があまり注目されないものと考えているかもしれません。しかし、実際は違うのです。

- あなたが職場で扱う情報は、他の企業や政府にとって非常に大きな価値がある可能性があります
- 標的を絞った攻撃者は、あなたをハッキングするためではなく、あなたの同僚や他のシステムをハッキングするためであり、職場でのあなたを狙う可能性があります
- 攻撃者は、あなたが仕事で付き合いのある、または協力関係にある企業のために、職場でのあなたを狙う可能性があります

アンチウイル製品を使用していれば安全か

自身が標的であることは問題ないとしましょう。しかし、アンチウイルス製品とファイアウォールをコンピュータにインストールすれば、保護されるので大丈夫と考えていませんか。残念ながら、そんなことはありません。多くの人はセキュリティ対策ツールをインストールすればセキュアであると考えていますが、これが全面的に正解とは言えないのです。サイバー攻撃の手口は日々進化を続けており、現在の攻撃手法の多くがセキュリティ技術を容易に回避してしまいます。例えば、攻撃者はよく、アンチウイルス製品が検知できないような、特別なマルウェアを作成します。そうしたマルウェアは、メールフィルタをカスタマイズされたフィッシング攻撃によって回避したり、あなたに電話をかけて騙したり、あなたのクレジットカードやお金、パスワードを利用した詐欺行為に及んだりします。テクノロジーはあなたを守る上で重要な役割を果たしますが、究極的には、あなた自身が最大の防御策なのです。

幸い、セキュアな状態になることはそう難しいことではありません。常識と基本的な行動こそが最大の防御策です。不自然な、または怪しい緊急のメールやメッセージ、電話を受けたら、それは攻撃である可能性があります。コンピュータや機器がセキュアな状態であるようにするためには、最新の状態を保ち、自動アップデート機能を有効化しましょう。最後に、個々のアカウントに強力でユニークなパスフレーズを設定してください。サイバーセキュリティについて普段から意識しておくことが、究極的には最大の防御策となります。何から始めたら良いか迷っている場合はsans.org/ouchで公開している、月刊OUCH!ニュースレターの購読を検討してください。

ゲストエディタ

マット・ブロマイリー氏（@mbromileyDFIR）は、インシデントレスポンスやデジタルフォレンジックの専門家として8年以上の経験を有しており、世界中の組織やインシデントを相手に仕事をしてきました。ブロマイリー氏はさらに、SANS FOR508とFOR572のインストラクターとして、デジタルフォレンジックとインシデントレスポンスの楽しさを伝え続けています。

SANS SECURITY AWARENESS

リソース

マルウェアの侵入を阻止する:	https://www.sans.org/u/L1J
ソーシャルエンジニアリングについて:	https://www.sans.org/u/L1O
電話攻撃と詐欺:	https://www.sans.org/u/L1T
パスフレーズについて:	https://www.sans.org/u/L1Y
ポスター - You Are a Target:	https://www.sans.org/u/L23

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