SANS SECURING THE HUMAN
NRI SECURE TECHNOLOGIES

OUCH! | 2014 年 4 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...

- 概要
- 狙われる理由
- 被害に遭わないようにするには

あなたも狙われています

概要

多くの人は、サイバー犯罪者に狙われることはないと考えています。そんな誤解をしている人は、自分のコンピュータには犯罪者が狙うような価値がないと思っているからです。これは大きな勘違いです。コンピュータ、携帯端末、オンラインアカウント、メールアドレス、クレジットカードのいずれかを持っていれば、誰もがサイバー犯罪者に狙われます。サイバー犯罪者にとっては、そのどれもが金銭価値があるのです。今回は、なぜ狙われるのか、どのように攻撃されるのか、被害に遭わないようにするにはどうすべきかを説明します。

ゲストエディター

エリック·コンラッドはBackshore社の社長兼CTOで、CISSP Study Guide第2版とEleventh Hour CISSP第2版の筆頭執筆者です。また、SANSのSEC511：Continuous Monitoring and Security Operations（6日間コース）の共同執筆者でもあります。

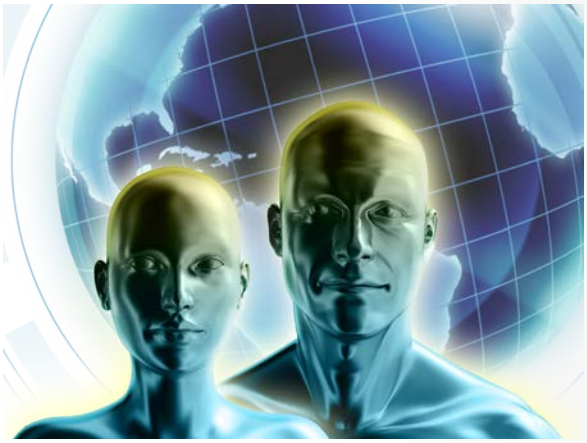
狙われる理由

詐欺、個人情報の盗難、恐喝といった犯罪行為は新しいものではなく、現代社会においては日常的に発生しています。犯罪者の目的は、簡単でリスクを負わずに、できるだけ多額の金銭を入手することです。以前の犯行は、犯罪者自身の居場所に限定され、狙った相手と物理的に接触する必要がありました。つまり、狙う対象も限定されると同時に、犯罪者自身もリスクを負う必要がありました。しかし、インターネットやオンライン技術の発達によって、犯罪手口は劇的に変化しました。現在、サイバー犯罪者は低コスト低リスクで世界中の人を狙うことができます。さらに、高度で組織的になり、非常に効率化されるようになりました。

サイバー犯罪は、より多くのクレジットカードを盗み、より多くの銀行口座をハッキングし、より多くのパスワードを侵害することで、金銭的見返りが高くなるといえます。そのため、サイバー犯罪者はインターネット利用者をできるだけ多くハッキングしようと試みます。世界中の何百万人といった人々を大量にハッキングすることは至難の業のように思われがちですが、自動化ツールを使って作業をすれば驚くほど簡単です。例えば、数百万件のメールアドレスをデータベースに登録すれば、自動化ツールを使って大量のフィッシングメールを送信できます。メールを送信するときにハッキングした他人のコンピュータを使えば、費用もほとんどかかりません。つまり、あなた自身は何も価値がないと思っているコンピュータでも、このような理由から狙われる可能性があるわけです。犯罪者にとって、メール攻撃の被害者は誰でもかまいません。メールを大量に送信すれば、誰かがだまされるからです。また、犯罪者は、ハッキングできそうなコンピュータや端末を探すた

あなたも狙われています

め、インターネットに接続されているコンピュータを手当たり次第スキャンしています(このスキャンもまたハッキングしたコンピュータを使用しています)。犯罪者は特別だからという理由で狙っているわけではなく、無差別に可能な限り多くの人に攻撃を仕掛けているのです。したがって、その中にあなたが含まれていることも十分にあるわけです。



気づいてください！　あなたのコンピュータや情報は世界中のサイバー犯罪者から狙われています。

被害に遭わないようにするには

サイバー犯罪者が世界中の人に対して大量ハッキングを試みる場合、比較的単純な手口を用いています。そのような攻撃に対しては、簡単な手順で防ぐことができます。以下の手順を参考にしてください。

- **自己意識**：あなたをサイバー攻撃から守るのはあなた自身です。多くの場合、あなたをだますことから始まります。例えば、メールに感染したファイルを添付して送信し、添付ファイルを開けるように仕向ける、または電話でパスワードを教えるように誘導します。常識的に考えて、怪しいまたはあり得ない話だと思ったら、攻撃であると思った方がよいでしょう。

- **更新作業**：利用する全てのコンピュータや携帯端末が完全に更新され、最新の状態であることを確認してください。これは、オペレーティングシステムだけでなく、利用しているアプリケーションやプラグイン全てにおいて重要です。システムやアプリケーションを常に更新された最新の状態に維持することで、一般的な攻撃を防ぐことができます。

- **パスワード**：アカウントごとに強固な個別のパスワードを設定してください。そうすることで、利用しているWebサイトがハッキングされ、そのサイトのパスワード全てが侵害されても、他のWebサイトのアカウントまでその影響を受けることはありません。また、利用している端末も、強固なパスワードやPIN（暗証番号）、ロック機能により保護してください。多数のパスワードを安全に維持するには、パスワードマネージャを利用してください。

- **クレジットカード**：カード利用明細書を、少なくとも週単位(月単位では十分ではない)でチェックしてください。クレジットカードの不正取引を見つけたら、直ちにカード発行会社へ連絡してください。金融機関によっては、普段の利用と異なる不審な高額利用が発生すると、電子メールやショート

あなたも狙われています

メッセージで警告してくれるサービスを提供しています。その場合は、ほぼリアルタイムで確認することができます。

- **自宅ネットワーク**:自宅ネットワークのWi-Fiアクセスポイントには、強度のある管理者パスワードを利用し、Wi-Fiネットワーク参加には、パスワードを必須にしてください。さらに、自宅ネットワークに接続する機器を全て把握し、更新されている状態であることを確認してください。

- **ソーシャルメディア**:多くの情報をオンラインに投稿することで、犯罪者から攻撃されやすい状態になります。サイバー犯罪者は投稿された情報を使ってだまそうとするだけでなく、だまされやすい人間であると特定されることもあります。

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! パスワードマネージャ:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! 自宅ネットワークを安全に:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! フィッシング攻撃:	http://www.securingthehuman.org/ouch/2013#february2013
ポスター: ターゲットはあなたです:	http://www.securingthehuman.org/resources/posters

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