OUCH! | 2014 年 11 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...

- ソーシャルエンジニアリングとは
- ソーシャルエンジニアリング攻撃を検知する・止めるには
- 今後のソーシャルエンジニアリング攻撃を防ぐためには

ソーシャルエンジニアリングについて

はじめに

一般によくある誤解として、サイバー攻撃者が、高度なハッキングツールやテクノロジーのみを使用してアカウントを奪取したり、パソコンやモバイルデバイスに侵入したりすることが上げられます。これは、はっきり言って間違いです。サイバー攻撃者は、必ずしも高度なハッキングツールやテクノロジーを駆使して個人情報を盗んだり、あなたのパソコンをハッキングするよりも、あなたと話をして騙すことが一番簡単な手法であることを知っています。このニュースレターでは、ソーシャルエンジニアリングと呼ばれる人間への攻撃がどのような攻撃であるかを理解し、どのようにして自分を守ることができるのかについて解説します。

ゲストエディター

アリッサ・トーレス氏は、コンピューターフォレンジックとインシデントレスポンスに強みを持つSANS 認定インストラクターです。インストラクター業務をする傍ら、インシデントハンドリングやデジタルフォレンジックなどを担当しています。ツイッターは@sibertor です。

ソーシャルエンジニアリングとは

ソーシャルエンジニアリングは、心理的に働きかける攻撃の一種で、攻撃者が意図する行動を取るように被害者を誘導するものです。ソーシャルエンジニアリングは、数千年も昔から存在しているもので、人を欺いたり、騙したりすることは、今に始まったことではありません。しかし、サイバー攻撃者は、このテクニックをインターネット上で使用することが非常に効果的であり、一度に多数の人を標的にすることが可能だということを知っています。ソーシャルエンジニアリングがどのようにして行われるかを理解するには、実例を紹介するのが一番早いでしょう。

パソコンのテクニカルサポートを行っている企業、例えば、ISP やマイクロソフトのサポート担当だと自己紹介する人から電話を受けます。そして、パソコンがおかしな挙動を示していることを発見したと語り、インターネット上でスキャンを行っていることやスパムメールを送信しているなどと伝え、何かに感染していると言います。次に、上記のような不正アクセスに関して調査を依頼されたと語り、パソコンを安全にすることを助けると言います。その際、適度にテクニカルな用語を織り交ぜ、複雑な手順を踏みながらパソコンが何かに感染していると電話で言い聞かせるのです。

例えば、特定のファイルがパソコン上に存在するかを確認するための手順を示し、そのファイルを探させます。このファイルを見つけた時、攻撃者は、パソコンが何かに感染していることの証拠だと言い聞かせようと試みますが、これらのファイルは通常、パソコン上に存在するありふれたファイルに過ぎません。パソコンが感染していると言い聞かせた後、あるウェブサイトを訪れ、提供しているセキュリティソフトウェアを購入させるか、あるいは発生している問題を直すためにパソコンへのリモートアクセスを許可するように促します。ところが、この販売されているソフトウェアは、悪意あ

ソーシャルエンジニアリングについて

るプログラムなのです。このソフトウェアを購入してインストールしてしまったら、パソコンが悪意あるプログラムに感染するよう誘導されて騙されただけでなく、お金を払って感染してしまったことになります。問題を修正するためにリモートアクセスを許可した場合も、攻撃者はパソコンを乗っ取って感染させるだけです。

ソーシャルエンジニアリング攻撃は、電話だけで発生するものではないことに注意してください。攻撃者は、あなたを騙すためメールにフィッシング、SMS、フェイスブックのメッセージ、ツイッターの投稿やオンラインチャットといった様々な手段が使用されます。したがって、これらの攻撃を防ぐには、何に注意すればよいのかを理解することが重要なのです。

ソーシャルエンジニアリング攻撃を検知、止め、そして防ぐことが、自分を守るためにできる最も有効な手段の一つです。

ソーシャルエンジニアリング攻撃を検知する・止める

ソーシャルエンジニアリング攻撃を防ぐ一番簡単な方法は、常識的な行動を取ることです。何か不審なことを感じたり、違和感を感じたりしたならば、それはソーシャルエンジニアリング攻撃かもしれません。ソーシャルエンジニアリング攻撃を示す主な兆候は：

- 緊急性が高い状況を訴えている人がいる場合。あなたが、すぐに結論を出さなければならない状況を相手だけが訴えている場合、疑った方がよいです
- アクセスすべきでない、または既に知っているはずの情報を求められている時
- でき過ぎた話の場合。よくある例は、券を買っていないのにも関わらず、宝くじが当たったと連絡が来た場合

誰かが自分をソーシャルエンジニアリングの被害者にしようとしている疑った場合、直ちにその人とコミュニケーションを取るのは止めて下さい。電話の場合すぐに切って下さい。オンラインチャットの場合、すぐに接続を切って下さい。信頼できないメールの場合は、削除して下さい。攻撃が業務に関連している場合、社内のヘルプデスクやセキュリティチームに報告して下さい。

今後のソーシャルエンジニアリング攻撃を防ぐために

ソーシャルエンジニアリング攻撃から自分を守るための予防策がいくつかあります。

- **パスワードを共有しない**：パスワードを聞き出すために連絡してくる組織はありません。パスワード聞かれた場合は、ソーシャルエンジニアリング攻撃です。

ソーシャルエンジニアリングについて

- **可能な限り情報を共有しない**：攻撃者があなたの情報を集めれば集めるほど、攻撃者が意図した行動を取るように誘導しやすい存在となります。自分のことに関して些細なことを共有するだけで、攻撃者はあなたという人物像を作りやすくなりますので、ソーシャルメディア、製品レビュー、その他掲示板やメーリングリストなどで共有する情報を少なくすることで、攻撃を受ける可能性は低くなります。

- **相手を確認する**：銀行、クレジットカード会社、携帯キャリアや他の組織から、正当な理由で連絡を受けることもあります。求められている情報や事項に関して疑いがある場合、その相手の名前と電話番号を聞き出してください。その後、信頼できる情報源、例えば、クレジットカードの裏、銀行からの明細や企業のウェブサイト(この場合、自分でブラウザに直接 URLを打ち込んでください)から企業の電話番号を入手してください。その後、入手した番号に電話をかけた際に、先ほど話していた人と同一であるか否かを確認できます。少し面倒かもしれませんが、自分の身元と個人情報を守るためには欠かせません。

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

メールによるフィッシング攻撃:	http://www.securingthehuman.org/ouch/2013#february2013
安全なソーシャルネットワーキング:	http://www.securingthehuman.org/ouch/2013#march2013
詐欺を防ぐ:	http://www.onguardonline.gov/topics/avoid-scams

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