OUCH! | 2017 年 01 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による攻撃を検知・阻止する方法

ソーシャルエンジニアリングについて

はじめに

サイバー攻撃者に関して、多くの人が誤解している部分として、彼らは高度なツールや技術力を使ってパソコンやアカウントをハッキングしていることが上げられます。しかしこれは、正しくありません。サイバー攻撃者たちは、情報を盗んだり、アカウントをハッキングしたり、システムを感染させたりするための一番簡単な方法は、間違いを犯すよう仕向けることだと学んでいます。このニュースレターでは、これらのソーシャルエンジニアリングと呼ばれる攻撃がどのようにして行われ、そして自分を守るためにできることを紹介します。

ゲストエディター

ジェームズ・リン氏は(**@jameslyne**)、SANSの認定講師であり、Sophos社で研究部門のGlobal Headとして、サイバー犯罪者が作成する最新のプログラムをリバースエンジニアリングしています。また、SANSが提供するMetasploit（SEC580）およびSocial Engineering（SEC567）コースの著者でもあります。

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、攻撃者が被害者に何かしてはいけないことをさせようと心理に訴える、精神的な攻撃です。ソーシャルエンジニアリングというコンセプトは、何も新しいものではありません。1,000年以上も前から存在しています。詐欺師やペテン師と同じだと思ってください。サイバー攻撃者にとって、現在のテクノロジーが有効である理由として、被害者となるあなたは攻撃者が物理的に見えないことが上げられます。そのため、攻撃者はあなたを含めた世界中の人々を標的に、どんな人や役をも演じることができます。さらに、ソーシャルエンジニアリング攻撃は、多くのセキュリティツールを回避してきます。このような攻撃がどのようにして行われ、そして自分を守るためにできることを理解するためにできる一番簡単な事は、以下にあげる2つの実例から学ぶことです。

パソコンをサポートする企業、例えばISPやMicrosoftのテクニカルサポートであると主張する人から電話がかかってきたとします。そして、あなたのパソコンがインターネット上でスキャン活動を行っていると説明し、何かに感染している可能性があるため、そのパソコンを安全にするための担当としてアサインされたと続けます。そこから様々な難しいテクニカルな表現を使い、さらに分かりづらいステップを踏みながらパソコンが何かに感染していると思い込ませます。例えば、特定のファイルがパソコン内に存在しているかを問い、そのファイルを探す方法を提示します。電話の発信者は、このファイルが存在していることが感染している証拠だと言い張ります。しかし、このファイルは、ほぼ全てのパソコンに含まれているシステムファイルです。パソコンが何かに感染していると説得に成功したら、セキュリティソフトウエアの購入を勧めてきたリ、修復のためにパソコンに対するアクセスを許可するように求めてきます。しかし、この販売しているソフトウエアは、悪意あるプログラムなのです。もし、これを購入してインストールしてしまった場合は、攻撃者は

ソーシャルエンジニアリングについて

あなたを騙してパソコンを感染させることに成功しただけでなく、お金を支払った上で感染しているのです。そして、リモートアクセスを許可してしまった場合は、パソコンを乗っ取った上でデータを盗み、そのデータを利益のために利用します。

多くのソーシャルエンジニアリング攻撃を特定し、止めるための最大の防御策は一般常識を持つことです。

もう一つの例は、主に職場で見られる CEO詐欺と呼ばれているメールを活用した攻撃手法です。サイバー攻撃者は、インターネットを活用してあなたが所属している組織について調査し、同僚または上司の名前を特定します。そして攻撃者は、その同僚または上司を騙ってメールを作成し、あなたに送付します。このメールでは、緊急を装って、急いで送金の手続きを行う、社員に関する機密な情報を送付するなど、急ぎでアクションを取るように要求してきます。多くの場合において、このメールには通常のセキュリティ手順を回避しなければならない緊急な事象があると語り、機密な情報を個人の @GMAIL.COMアカウント宛に送付するよう書いてあります。これらの攻撃が危険な理由は、サイバー攻撃者が事前に調査を行っていることです。また、アンチウイルスやファイアウォールでは、これらの攻撃を検知、阻止はできません。なぜなら、マルウエアや悪意あるリンクを活用していないからです。

一つ覚えておかなければならないのは、これらのようなソーシャルエンジニアリングの攻撃は、電話やメールだけを使用する訳ではないということです。攻撃は、携帯電話のテキストメッセージやソーシャルメディアを使うこともありますが、さらには攻撃者自身が直接会った時に行うこともあります。重要なのは、何に気を付ければ良いのかを知ることです。何よりも自分自身が最大の防御策なのです。

ソーシャルエンジニアリングによる攻撃を検知・阻止する方法

幸いなことに、これらの攻撃を阻止するのは、考えているよりも容易ですー一般的な常識を持つことが最大の防御策となります。何か疑わしきものがあったり、違和感があったりした場合は、攻撃の可能性があります。ソーシャルエンジニアリング攻撃である主なヒントは以下の通りです：

- 強い切迫感を作る人は、あなたが間違いを犯すように仕向けてきます
- アカウント情報などの本来知り得ない、または既に知っているはずの情報を求める人
- パスワードを求めてくる人。まっとうな組織はパスワードを聞き出すことはありません
- 仕事上で守るべきはずのセキュリティに関する手順や処理を回避（無視）するようにプレッシャーをかけてくる人

ソーシャルエンジニアリングについて

- 出来過ぎた話。例えば、応募していないのにも関わらず、宝くじまたは iPadなどのものが当たった連絡があった場合
- 友人または同僚から、普段と違う言葉遣いをしているおかしなメールを受信した場合。サイバー攻撃者がその人のアカウントをハッキングして、あなたを騙そうとしています。自分を守るために、直接会う、または電話をかけるなどの別の通信方法を使って、その友人または同僚とコミュニケーションを取ってみてください

もし、誰かがあなたを騙そうとしていると気付いた場合、その相手とのコミュニケーションは止めてください。攻撃が仕事で起きたものならば、社内のヘルプデスク、または情報セキュリティチームに報告してください。重要なのは、多くの場合は一般常識が最大の防御策であることを覚えておくことです。

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。
securingthehuman.sans.org/ouch/archives

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

フィッシングについて:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO詐欺:	https://securingthehuman.sans.org/ouch/2016#july2016
ランサムウエアについて:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Archives:	https://securingthehuman.sans.org/ouch/archives

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