OUCH! | 2016 年 07 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...

- CEO詐欺とは？
- 自身を守るために

CEO詐欺

CEO詐欺とは？

サイバー犯罪者は卑劣な存在です。ー得たいものを得るため、常に新たな手法を彼らは編み出しており、彼らが考える最も効果的な手段は、一般ユーザを標的にすることです。しかし、サイバー犯罪者は、組織内で最も脆弱なのは意識の低い従業員だということを理解していても、OUCH! 読者のような意識の高い従業員が、組織を攻略する上で最も手強い相手になることを忘れているのでしょう。

ゲストエディター

アンジェラ・パパス氏は Thomson Reuters社で情報セキュリティトレーニングや意識啓発活動のディレクターを務めており、アンバサダープログラム、eLearningおよびフィッシングといったトピックで従業員に教育を行っています。

サイバー犯罪者は、CEO詐欺（CEO Fraud）、または偽の送金指示メール（Business Email Compromise、BEC）と呼ばれる新たな攻撃手法を編み出しました。この攻撃は、CEO や役員などに成りすまして、従業員に対し通常では行わないようなことをメールで指示してくるというものです。この攻撃の前には、攻撃を効果的にするために、組織のウェブサイトからオフィスの所在、役員の名前、どのような企業と取引をしているか、などの情報を下準備としておこなってから仕掛けてきます。この他にもLinkedIn、FacebookやTwitterなどから同僚に関する情報を仕入れ、組織の構造について分かった段階で特定の従業員を標的にするのです。この時、サイバー犯罪者の標的は、目的に合わせて選択されます。サイバー犯罪者の目的が金銭的なものであれば、経理部門の従業員を標的にしますし、税に関する情報であれば人事部を標的にするかもしれません。そして、データベースサーバへのアクセスが目的であれば、IT部門が標的になるでしょう。

サイバー犯罪者が得たいものに従って標的を選択すると、次は具体的な攻撃の準備に入ります。攻撃には、多くの場合スピアフィッシングという手法が用いられます。フィッシングは、攻撃者が多くの人に対して同時にメールを送り、悪意ある添付ファイルを開かせたり、巧妙に細工されたWebサイトなどにアクセスするように仕向けるものですが、スピアフィッシングの場合は、標的とする特定の人物に限定し、多くはカスタマイズしたメールを送る点で異なります。このスピアフィッシングで使われるメールは、上司や同僚から送られたメールであるように細工されており、社内で頻繁に使われる言いまわしや、会社のロゴ、署名なども場合によっては本物が使われる場合があるため、不審メールとして検知できないほど、本物と見分けがつかないようになっています。

© SANS Institute 2016

CEO詐欺

しかし、攻撃者によって偽装されたメールの場合は、緊急性を煽るような内容だけではなく、具体的に何らかのアクションを取るように求めるなどの特徴が多く見られます。また、他の誰にも言わないようにといった指示もあり、落ち着いて考えればスピアフィッシングによるメールを受信したユーザに、何らかの過ちを犯させるように仕向けていることは明らかです。以下に、一般的に見られる3つのシナリオをご紹介します：

CEO詐欺は、とても強力な攻撃で、多くのセキュリティ対策を回避することが可能です。最終的には、人が一番の防御策になります。

- **不正送金**: サイバー犯罪者が金銭をターゲットにしている場合、経理に関わる人またはチームを特定するために、あなたの組織を調査します。そして、上司になりすました偽装メールを送り、 さらに続いて緊急事態が発生したことを理由にして、特定の口座にお金をすぐに振り込むよう指示をしてくるというものです。

- **税金詐欺**: サイバー犯罪者が他人になりすまして税金詐欺を画策している場合、あなたの組織を調査し、社員情報を管理している部署、例えば人事部や相当する人物を特定します。そして、役員または法務部になりすまして偽装メールを送り、税務処理に関する書類などの情報をすぐに送るよう要求するというものです。

- **弁護士のなりすまし**: すべての CEO詐欺攻撃がメールで行わるとは限りません。別の手法、例えば電話が使われることもあります。このシナリオでは、まず役員になりすまして偽装メールを送ることから始まりますが、メールの本文において緊急の用件で弁護士から電話があることが伝えられます。その後、 サイバー犯罪者が弁護士になりすまして偽装電話をかけ、電話の中で時間的制約のある機密事項を話すことで、緊急性を煽っていきます。サイバー犯罪者は、この緊急性を煽ることで通常では考えられないアクションを起こすように仕向けるというものです。

自身を守るために

このような攻撃に対して、自分自身と組織を守るために何ができるでしょうか？ その答えは、一般常識が一番の防御策だと言えます。上司や同僚からメールを受信した時、違和感がある場合は、攻撃の可能性があります。ヒントとしては、緊急性の煽りがあるかどうかです。何か違和感があったり、通常使われるようなトーンではなかったり、呼称が通常と違うなどがきっかけで気づくことができます。また、別のヒントとして、攻撃者が見たことの

© SANS Institute 2016

CEO詐欺

ないメールアドレスや電話番号を使う場合もあります。この時、普段見る上司や同僚のメールアドレスと酷似しているものが使われることがあります。違和感がある場合は、信頼できる電話番号を使って送信者に電話する、直接会うなどして（メールでの返信はしないでください）、そのメールを送ったか否かを確認してください。また、既存のセキュリティポリシーや手順は必ず守るようにするのも防御策の一つです。多くの組織では、決められた手順に従って送金が行われたり、機密文書を送付しています。これらの手順を破ろうとする要求は、送信元が誰かであるかに関わらず、違和感を覚えるべきであり、具体的なアクションを取る前に確認してください。このような要求を受信した際、何をして良いか分からない場合は、上司、ヘルプデスクや情報セキュリティ担当者に連絡してください。

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

ソーシャルエンジニアリングについて:	https://securingthehuman.sans.org/ouch/2014#november2014
フィッシングについて:	https://securingthehuman.sans.org//ouch/2015#december2015
マルウエアとは:	https://securingthehuman.sans.org/ouch/2016#march2016
2段階認証について:	https://securingthehuman.sans.org/ouch/2015#september2015
SANS Security Tip of the Day:	https://www.sans.org/tip-of-the-day

OUCH!はSANS Securing The Human プログラムによって発行され、Creative Commons BY-NC-ND 4.0 licenseに従って配布されます。このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。翻訳その他に関しては、ouch@securingthehuman.org までお問合せください

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