SANS SECURITY AWARENESS

OUCH!

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

CEO詐欺とBEC

CEO詐欺やBECとは何か

攻撃者は、CEO詐欺やビジネスメール詐欺 (BEC) と呼ばれるメール攻撃を展開し続けています。これらは、ターゲットに本来取るべきではない行動を取るように言葉巧みに騙す標的型のメール攻撃です。大半の事例において、攻撃の目的は金銭となっていますが、この攻撃の非常に危険なところは、攻撃者がターゲットとした人物について事前に調査をしているということでしょう。ウイルスを組み込んだ添付ファイルや悪意のあるリンクが検出されるわけではないため、こうした攻撃を防ぐことはセキュリティ技術をもってしても非常に困難となっています。

攻撃者は、インターネット上でターゲットとした人物とその周辺について調査します。例えば、あなたが標的となった場合、攻撃者はあなたの職場の上司に関する情報や、さらには住宅取得などで利用した不動産業者について調べることが考えられます。攻撃者は、調査が済むと関係者を装ってあなたにメールを送ってきます。メールの内容は緊急性を煽るもので、請求処理や支払先の変更、重要な文書の返送といったことを直ちに実行するよう要求してきます。こうしたメールは、攻撃者が思い描いた通りの行動をとるように、あなたにプレッシャーをかけるという点で効果的です。以下に、このような攻撃が成功し得る2つの例を示します。

振り込み：犯罪者の目的は金銭です。彼らはあなたが所属する会社について、買掛金を管理する部署の人物や、送金担当者の特定といった調査をします。その後で、調査した人物の上司や部署の幹部になりすまして、その人物にメールを送ります。メールの内容は、緊急事態が発生したため、新しく設定した口座に今すぐ送金する必要があるというものです。このようなメールはターゲットとなった人物にプレッシャーを与え、犯罪者への送金というミスを誘発させることを狙っています。

還付金詐欺：犯罪者は、税金などの還付金詐欺に利用できる個人情報を狙っています。そのような情報を入手する手っ取り早い方法の一つは、企業で働く従業員全員の情報を窃取することです。犯罪者は、人事部に所属する人物を調査し特定します。その後人事部の幹部や、あるいは法務部といった人物になりすまし、調査した人物に偽のメールを送ります。メールの内容は緊急事態の発生と、社員全員の税務処理に関する情報が今すぐ必要だということを告げるものです。人事部の社員は、重要な情報を含む文書を幹部に送っていると思い込んでいますが、攻撃者の手口に引っ掛かると、そうした文書を結果的に犯罪者に送ってしまうことになります。

自分の身を守る

あなたが身を守るためにできることは何でしょうか。それは、常識を持つことであり、常識こそが最大の防御となります。犯罪を見破るための、頼りになる常識的な手がかりは次のとおりです。

メールの内容が非常に短く（たいていの場合2〜3行のみ）、緊急性の高さが強調されています。また、携帯電話から送られたという署名がついていることがあります。

緊急性の高さが強調されており、企業のポリシーを無視あるいは回避するようプレッシャーを与える内容が記されています。メールがあなたの上司や部署の幹部から送られているように見えても、業務上のポリシーや手順には必ず従いましょう。

業務に関係のある内容のメールですが、@GMAIL.COMや@HOTMAIL.COMといった個人のアドレスを使用しています。

メールが部署のリーダーや同僚、あなたが知っているもしくは取引のあるベンダーから来ているように見えますが、文章のトーンや書き方が彼らのいつものものとは違います。

支払い方法が提示されていて、別の銀行口座に今すぐ送金するよう要求するといった、あなたが普段従っているものとは違う方法が示されています。

もし職場で標的になっているかもしれないと疑いを抱いたら、攻撃者とのやり取りを中断し、監督責任者である上司に報告しましょう。自宅で標的となった、もしくは被害に遭い、振り込み処理が完了してしまった場合は、すぐに銀行に連絡し、警察に届け出ましょう。

ゲストエディタ

ドン・キャベンダー氏（@don_cavender、https://www.linkedin.com/in/donald-cavender）は、元FBI特別捜査官であり、20年以上に渡りデジタルフォレンジックやサイバー犯罪に携わってきており、最近のものでは、ワシントンD.C.のBECコーディネータとして、サイバー犯罪組織を中心に捜査しているほか、デジタルフォレンジックとサイバー捜査の研究や、トレーニングの提供も行っています。

リソース

ソーシャルエンジニアリング:	https://www.sans.org/u/HE3
フィッシングを阻止する:	https://www.sans.org/u/HE8
マルウェアの侵入を阻止する:	https://www.sans.org/u/HEd
ログイン情報を保護する:	https://www.sans.org/u/HEi

 Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | **Translated by:** 小山 裕之, 時田　剛