月間セキュリティ啓発ニュースレター

個人を標的とした詐欺

はじめに

サイバー犯罪者は、人々をだますために独創的な手段を生み出し続けています。そんな中、個人にターゲットを合わせた詐欺という、新しい形の詐欺が有名になりつつあるのをご存知でしょうか。サイバー犯罪者は何百万人もの人々に関する情報を発見もしくは購入し、その情報を個人に合わせた攻撃に利用します。ここでは、そのような詐欺が行われる際の手口と、一般的な攻撃の例を紹介します。この新しい詐欺について知ることで、攻撃を検知したり防いだりすることが容易になるでしょう。

手口

メールや電話による詐欺は新しいものではなく、サイバー犯罪者は長年に渡り人々を欺く試みを続けています。例えば、「You Won the Lottery（宝くじに当選しました）」や、悪名高いナイジェリアの王子を騙る詐欺があります。しかし、これらの昔から存在する詐欺において、犯罪者は標的を絞っていませんでした。彼らは単純に、共通の内容のメールを作成し、何百万人もの人々に送りつけていたのです。こうした詐欺メールは同じ文章で構成されているため、詐欺であることが容易に判断できます。個人に合わせた詐欺は別物で、サイバー犯罪者はまず調査をし、それぞれの意図した相手（被害者）用の特別なメールを作成します。氏名やパスワード、電話番号、その他の詳細な情報が載ったデータベースを発見もしくは購入することで攻撃準備が可能となります。このような情報は、ウェブサイトのハッキングによって容易に入手可能であり、ソーシャルメディアや一般に公開されている政府の記録からも取得できます。その後犯罪者は、情報を入手した人物全員を標的に定めます。

サイバー犯罪者が使用する騙しのテクニックの代表例が、金銭の支払いを強要する脅迫や不安を煽る行為です。攻撃は、次のように展開されます。犯罪者は、ハッキングされたウェブサイトから入手されたパスワードを含むログイン情報を発見もしくは購入します。入手したデータベースに含まれるあなたのアカウント情報を探し出し、ハッキングされたウェブサイトで使用していたパスワードを含む、あなたに関する詳細な情報を載せたメールをあなた宛てに送ります。その際犯罪者はパスワードを、あなたのコンピュータや機器をハッキングした証拠として挙げます。もちろんこれは嘘です。その後犯罪者は、あなたのコンピュータをハッキングする過程で、あなたがオンラインでポルノ動画を閲覧していたことを突き止めたと主張してきます。さらに金銭を支払わない場合、家族や友人にオンラインでの恥ずかしい行いを共有すると脅迫します。

ここでのポイントは、このようなケースのほとんどにおいて、サイバー犯罪者があなたのシステムをハッキングしたことは無いということです。彼らはあなたが何者なのか、どのウェブサイトを閲覧したのかということすら知りません。犯罪者は単に、彼らが持っている数少ないあなたの個人情報を利用して、あなたのコンピュータや機器が実際にハッキングされたと思い込ませ、金銭を支払わせようとしているに過ぎないのです。悪い人たちは、電話での詐欺でも同様の手口を利用する可能性があることを覚えておいてください。

何をすればよいか

こうした内容のメールや電話は、詐欺であることを認識しましょう。自分自身の個人情報を他人が持っていたら、恐怖心を抱くのは当然です。しかし、送信者が嘘をついていることを思い出してください。あなたに仕掛けられた攻撃は、自動で大規模に展開されたキャンペーンの一部であって、直接あなたを狙ったものではありません。サイバー犯罪者が個人情報を発見したり購入したりすることは、日々容易になってきているので、個人に合わせた詐欺は今後増えることが予想されます。確認するべき手がかりを挙げておきます。

⚠

- **緊急度の高いメールやメッセージ、電話を受けた際は、特に用心しましょう。相手が恐怖や切迫感といった感情を出している場合、犯罪者はあなたにミスを起こさせようとしています。**
- **ビットコインやギフトカード、その他の追跡が難しい方法での支払いを要求された場合**
- **怪しいメールを受け取った場合、GOOGLEで検索し、他の人が同様の攻撃を受けていないか調べましょう。**

究極的には、常識があなたの一番の防御策となります。さらに、複数のオンラインアカウントでパスワードを共用せず、常にユニークで長いパスワードを付けることも推奨します。全てのパスワードを覚えておくことができませんか？そんな時はパスワードマネージャを使用しましょう。また、可能な限り二段階認証も有効化しましょう。

ゲストエディタ

レニー・ゼルツァー氏は、経験豊富なサイバーセキュリティー専門家です。彼はMINERVA LAS社で、マルウェア対策ソリューションを開発したほか、SANS INSTITUTEにおいてセキュリティに関する授業を担当しています。またゼルツァー氏は、マネージドセキュリティサービスや、コンサルティング業務にも従事した経験を持っています。ゼルツァー氏は、ブログ（zeltser.com/blog）やTwitter（@lennyzeltser）でも情報を発信しています。

リソース

ソーシャルエンジニアリングについて:	https://www.sans.org/u/MUU
フィッシングを阻止する:	https://www.sans.org/u/MUZ
インターネットで自分自身を検索する:	https://www.sans.org/u/MV4
パスワードマネージャ:	https://www.sans.org/u/MV9

 Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: 小山 裕之, 時田　剛