エグゼクティブ サマリー

人の心理や行動を悪用するハッキング

Raj Samani ー EMEA CTO

Charles McFarland ー シニアMTISリサーチエンジニア

intel Security

多くのサイバー犯罪でソーシャル エンジニアリングの手口が利用されています。ソーシャル エンジニアリングは、攻撃対象を騙して行動を起こさせ、マルウェアに感染させたり、重要な情報を盗み出そうとします。

攻撃を受けた場合の対応としては技術的な修復が中心となりがちで、人的な側面では攻撃を受けた側の責任が追及され、さらなるセキュリティ意識の向上を求める声が上がるだけです。企業の大半は攻撃を受けた理由を深く追求せず、今後の攻撃を回避するために注意喚起以外に何を行うべきかを考えようとしていません。

ソーシャル エンジニアリングは次のように定義されています。

> 人を騙して秘密を暴露させたり、結果として秘密が公開されるような行為を行わせる詐欺行為

ソーシャル エンジニアリング攻撃を受けた被害者は、自分の行為が有害であることに全く気づいていません。攻撃者は標的の悪意ではなく善意を悪用します。ソーシャル エンジニアリングは次の2つに分類できます。

- ハンティング型。攻撃対象とのやり取りを最小限にして情報を収集します。この場合、接触は1回だけで、攻撃者は情報を収集するとコンタクトを止めます。
- ファーミング型。攻撃者と関係を築き、長期にわたって情報を収集します。

通常、電子メールを使ったソーシャル エンジニアリングでは、ハンティング型の攻撃が実行されますが、例外もあります。たとえば、「ナイジェリアの手紙」では資金を調達するため攻撃が長期的になります。いずれの場合も、ソーシャル エンジニアリングは次の4つ段階で行われます。

1. 調査: 攻撃対象に関する情報の収集。調査は実行されない場合もありますが、次の段階を成功させるため、攻撃対象の趣味、職場、取引銀行などの情報を収集します。
2. フック: 攻撃を成功させる準備として、攻撃対象に接触し、きっかけを作ります。心理学者のRobert Cialdiniは、人を動かす要因として次の6つを挙げています。
   - 返報性: 恩義を受けた場合、それを返そうとする。
   - 希少性: 希少価値を感じるものに惹かれる。
   - 一貫性: 信頼を失わないため、一度約束したことは守ろうとする。
   - 好意: 好意を持つ人物に従いやすい。
   - 権威: 権威的存在から影響を受け入れやすい。
   - 社会的証明: 他人の行為をまねしやすい。
3. 実行: 攻撃の実行。攻撃対象に情報の開示、リンクのクリック、送金などの行為を実行させます。
4. 終了: やり取りの終了。ファーミング型の多くは、相手に疑いを持たせずに接触を終わらせようとします。たとえば、クレジットカード情報を盗み出す場合、被害者がカードの紛失や盗難を報告しないように、攻撃対象が不審を感じないように振る舞います。しかし、ソースコードや他の個人情報の場合、攻撃対象が不審を抱いても盗まれたデータを取り戻すことはできません。

ソーシャルエンジニアリングは単独で行われるとは限りません。大規模な攻撃の一段階で関連情報を収集する場合もあります。1回の攻撃で情報を収集して終わる場合もあれば、何度もハンティング攻撃を行い、収集した情報でファーミング攻撃を開始する場合もあります。

攻撃の経路

ソーシャル エンジニアリングは様々な経路で実行されます。

- Web サイト: ソーシャル エンジニアリングでは、攻撃の経路として不正なWebサイトがよく利用されます。『2014 Verizon Data Breach Investigations Report』(Verizon 2014年度データ漏洩/侵害調査報告書)によると、スパイ活動を目的とした攻撃の20%はWebサイトに侵入してマルウェアを散布しています。
- 電子メール: 電子メールを利用したソーシャル エンジニアリングの大半はフィッシング詐欺や標的型のスピアフィッシング詐欺です。電子メールはサイバー犯罪の効果的な手段です。Verizonのレポートによると、ユーザーの18%がフィッシング詐欺メールのリンクをクリックしています。
- 電話: 情報ブローカーがよく利用する手段です。
- 訪問: 従業員が騙されて情報を聞き出される可能性があります。
- 郵便: あまり利用されていませんが、現在でも郵便によるソーシャル エンジニアリング攻撃が報告されています。
- FAX: オンライン決済サービスを装うメッセージなどが送信されています。

ソーシャル エンジニアリングを防ぐ対策

人、プロセス、技術をコントロールすることで、ソーシャル エンジニアリングのリスクを回避できます。これらの要素がすべてではありません。また、すべての組織に該当するとは限りません。

人

- 明確な境界: 情報の公開に関するポリシーを徹底させ、ポリシーに違反する依頼が発生した場合のエスカレーション パスを明確に定義する必要があります。
- トレーニングの継続的な実施: セキュリティ意識向上プログラムを実施し、従業員に対するトレーニングを継続的に行う必要があります。McAfeeフィッシング詐欺クイズなどのツールを使用して、攻撃でよく利用される手口を理解させてください。
- 確認の徹底: 問題がないように思える依頼に対しても確認を怠らないようにスタッフを指導する必要があります。直後侵入を試みる人物には注意が必要です。
- 情報の重要性: 電話番号など、重要に見えない情報でも攻撃に利用される可能性があります。
- 人を責めない文化: ソーシャル エンジニアリングの攻撃対象は被害者です。騙された従業員を罰すると、他のスタッフも情報漏えいを認め難くなります。騙された人物が攻撃者から脅迫される可能性もあります。

プロセス

- 不審な電話の報告: 不審な電話を受けた場合、やり取りの詳細を報告する必要があります。これは調査に役立ちます。
- ブロック通知ページ: 従業員が不正なWebページにアクセスしたときに、ブロック ページを表示し、アクセスできない理由を通知しましょう。リスクを事前に通知するだけでなく、攻撃元の特定にも役立ちます。
- 顧客への通知: 顧客が情報へのアクセスを拒否された場合、顧客にその旨を通知し、顧客に情報を利用する資格があるかどうか確認する必要があります。また、顧客との通信方法も検討する必要があります。PayPalでは、電子メールが偽物かどうかを見分ける方法として次のようなガイドラインを提示しています。「弊社から電子メールでお客様の銀行口座、クレジットカード、デビットカードの情報を確認することはありません。また、お客様の氏名、アカウントのパスワード、PayPalセキュリティの質問に対する答えを電子メールで確認することもありません。」

McAfee Labsのリンク

- エスカレーション ルート: スタッフが詐欺メッセージを受信したときの報告経路を明確に定義する必要があります。
- 抜き打ちテスト: 複数の攻撃手段を使用してソーシャル エンジニアリングに対する従業員の意識を定期的に確認しましょう。トレーニング プログラムの効果を判断できます。

技術

- 通話の記録: 着信を記録することで調査がやりやすくなります。
- 不審な電話番号: 不審な電話番号を監視用の番号に転送します。
- 電子メール フィルタリング: 既知または新しいマルウェアを含む不正なメールを削除します。
- Webフィルタリング: 不正なWebサイトへのアクセスをブロックし、マルウェアを検出します。
- 強力な認証: 多要素認証を利用しても、ソーシャル エンジニアリングのリスクを排除できるわけではありません。ユーザーが騙され、認証情報を漏らしてしまう可能性もあります。新たな攻撃者を阻止するのは容易ではありません。

サマリー

ソーシャル エンジニアリングの脅威は蔓延しています。サイバー犯罪者は、ソーシャル エンジニアリングで不正に情報を入手し、犯罪行為に利用しています。この脅威に対処するには、ソーシャル エンジニアリングの特性をよく理解する必要があります。攻撃者、手口、リソースなどを把握し、リスクを回避するための手段を講じる必要があります。

このレポートの完全版については、www.mcafee.com/hacking-human-osをご覧ください。

Twitter@Raj_Samani

Twitter@CGMcFarland

1. http://www.verizonenterprise.com/DBIR/2014/
2. https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ

McAfee. Part of Intel Security.
東京本社 〒150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウエスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店 〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所 〒460-0002 愛知県名古屋市中区丸の内 3-20-17 中外東京海上ビルディング 3F TEL 052-954-9551（代）FAX 052-954-9552
福岡営業所 〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com