脅威が続くフィッシング

多様化するフィッシング攻撃

- スピアフィッシング (spear phishing) - ホエーリング (whaling)
- クローンフィッシング (clone phishing)
- ビッシング (vishing)
- スミッシング (smishing) ... etc

どのような規模のビジネスにおいても、サイバーセキュリティは常にホットな話題となっています。
サイバーセキュリティにおいては、2019 年時点で、ワールドワイドにみてもフィッシング (phishing) による脅威が、依然として最も上位にランクされています。
セキュリティの分野で使用される「フィッシング」という言葉は、詐欺の罠に引っ掛かることが魚釣りの fishing に似ており、イメージし易いので広く知られるようになりました。
ビジネスにおいては、特定の個人や団体を狙った標的型のスピアフィッシング (spear phishing) が特に脅威となり、このうち、経営幹部、意思決定者、財務責任者等を標的とするものがホエーリング (whaling) と呼ばれています。典型的なフィッシングの形態は、不特定多数に対し大量にメール送信され、わずかでもひっかかればよいというパターンですが、特にホエーリングでは、もっともらしいスピアフィッシングメールを巧妙に作成し、なりすます送る側と受け取る側両方の肩書きや役職などの地位から個人的なことまで、SNS 等から調べ上げ標的を絞り込んで送りつけます。これは、ソーシャル・エンジニアリングの人間心理的な隙をつく手法を使っているわけですが、たとえば、裁判所や税務署を装って届くメールは、幹部にとっては、会社に何か起こっているのか心配になりかなりの確率で罠にかかり、添付された偽の公文書を開いてしまい、それでダウンロードされるのがキーロガーのマルウェアだったりする巧妙な攻撃パターンです。
また、多くの場合、フィッシングによる詐欺は、偽サイトの URL を案内して本物そっくりの偽サイトへのアクセスを誘導し、個人情報をフォームに入力させようとしますが、電話等の音声案内を通じて詐欺被害者を誘導しようとするビッシング (vishing) という手口もあります。これは、偽ドメインの URL よりも電話番号の方が怪しいと見破ることが難しいため、連絡先として偽の電話番号をメールに記述しておいて電話をかけさせ、音声応答システムを通じて個人情報を窃取しようとするパターンです。
最近では、電子メール以外にも、スマホなどで使用されている SMS に、銀行や有名企業を装ってショートメッセージを送り、偽のサイトへ誘導するスミッシング (smishing) の場合でも、音声が含まれたビッシングがあるようです。
かなり前であれば、中国語っぽい文章だったり、あきらかに疑わしいメールで、フィッシング詐欺も見分けが付きやすかったのですが、時代と共にますます巧妙になっているため、私たちも最新の情報を常に入手し気を付けることが大切です。

© CEC Customer Service Ltd.