SANS SECURITY AWARENESS

メッセージングアタック

はじめに

サイバー攻撃者が人々を騙したりだましたりする最も一般的な方法の一つは、電子メール(しばしばフィッシングと呼ばれる)や電 話で騙そうとすることです。しかし、テクノロジーが進歩し続ける中、悪者たちは常に新しい方法を試みており、それにはテキストメ ッセージ、iMessage/Facetime、WhatsApp、Slack、Skypeなどのメッセージングが含まれています。今月は、これらのメッセー ジを使った攻撃を特定/阻止するための簡単な手順をご紹介します。

メッセージ攻撃とは?

メッセージング攻撃(時にスミッシングと呼ばれる、フィッシングという言葉をもじった用語)とは、サイバー攻撃者がSMS、テキスト メッセージ、またはメッセージングのテクノロジを使用してユーザーに接触し、ユーザーがとるべきでない行動をとらせようとする攻撃です。最終的に悪質なリンクをクリックさせたり、電話番号を教えてもらうことで銀行情報を入手したいのかもしれません。従 来のフィッシングメール攻撃と同様、攻撃者は心の隙を突いてあなたに行動させようと誘導してくることが多いのが特徴です。しか し、メッセージング攻撃を非常に危険なものにしているのは、電子メールよりも形式張らない連絡手段なので、プライベートなやり 取りで油断をしてしまい被害に遭う可能性が高いということです。さらに、メッセージング攻撃は、電子メールと比べて情報が少な いので、疑わしいことに気付く手がかりも少なくなってしまうという特徴があります。奇妙なメッセージや不審なメッセージを受け取った場合は、まず、このメッセージに意味があるのか、メッセージを受け取った理由を自問するようにしてください。ここでは、一般的な手がかりをいくつか紹介します。

非常に強い切迫感があるメッセージの場合、誰かがあなたに行動を起こさせようとしている可能性があります。

メッセージの中に個人情報やパスワード、その他の機密情報へのアクセスを要求するものではないでしょうか。

あ るいは、そのメッセージはうますぎているような内容ではないでしょうか?あなたが買ったわけでもない宝くじに当選したりすることはありません。

同 僚や友人のアカウント・電話番号から送信されたように見えるメッセージであっても、それが本当に同僚や友人であるとい う保証はありません。少しでも不審なメッセージが同僚や友人から送られてきた場合、これらのアカウントは攻撃者に乗っ 取られて乗っ取られた可能性があります。あるいは、攻撃者がこれらのアカウントのふりをして、ユーザーをだましてアクション を起こさせようとしているのかもしれません。

あ なたが、今すぐにでも何かをしなければならないようなメッセージを受け取ったら、ちょっとだけ時間を置いて冷静に考え てから返信するようにしてください。

さらに、攻撃者は電子メールとメッセージング攻撃を組み合わせることさえあります。たとえば、ギフトカード詐欺は次のように振舞 います。ある日、友人や同僚を装って急ぎのメールが送られてきて、携帯電話の番号を聞かれます。その後、攻撃者に伝えてしまった携帯電話の番号宛てにメッセージを繰り返し送り、ギフトカードを購入するように促します。あなたがメッセージの執拗さに負け てカードを購入すると、攻撃者はカードの裏にあるコード部分をスクラッチし、コードの画像を送り返すように要求するのです。別のよくある攻撃としては、ビデオや画像を送りつけるというものです。(往々にして「信じられない!」あるいは「要確認」というコメント が添えられています)それはあなたの好奇心に訴えるものです。メッセージが知人からのものであるように見える場合は、実際に行 動を起こす前に電話で相手に確認すると良いでしょう。

公的機関から警告のメッセージが届いたら、直接その機関に確認するようにしてください。たとえば、銀行から銀行口座やクレジッ トカードに問題があるというテキストメッセージを受け取った場合、カード会社のWebサイトにアクセスするか、カードの裏面に記載されている電話番号を参照してカード会社に直接電話して確認してください。ほとんどの政府機関 (税務署や警察などの法執行機関) は、テキストメッセージではあなたに連絡するようなことはありません。

つまり、メッセージング攻撃に関しては、あなた自身の常識が最大の防御なのです。

ゲストエディタ

Jen For氏は、ソーシャル・エンジニアリングに関してDEF CON23のブラックバッジを保持するほどのキャリアを持ち、ドミノのセキュリティー・プログラム・スペシャリストとしてセキュリティー啓発活 動を行っています。彼の動向については、Twitterで@j_foxをフォローすることで確認できます。

リソース

ソーシャルエンジニアリング:	http://www.sans.org/u/XAQ
フィッシングを阻止する:	http://www.sans.org/u/XAV
電話による詐欺:	http://www.sans.org/u/XB0

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