添付資料

【今月の呼びかけ】

「 ウイルスを使った新しいフィッシング詐欺に注意！ 」

先月の呼びかけでは、SpyEye ウイルスによるインターネットバンキングでの不正利用事件を取り上げました。その SpyEye ウイルスはキーボードで入力した内容を盗むウイルスでしたが、IPA では 2011 年 9 月、異なる手口でインターネットバンキングのログイン情報を盗む事例を確認しました。

その手口は、既存のフィッシングの手口にウイルスを組み合わせた新しい手法です。銀行を装った偽のメールにウイルスが添付されており、ウイルスを実行するとログイン情報や乱数表の内容の入力を促す画面が現れ、メールの指示に従って入力してしまうと悪意ある者にその情報が渡ってしまう、というものです。実際にこの手口により銀行口座から総額数百万円を引き出される被害が発生しています。

IPA では実際の偽メールを入手しウイルスを解析しました。その解析結果から、ウイルスの概要と、実行されるとどのような動作をするのかを示すとともに、被害に遭わないための対策を紹介します。

（1）フィッシングとは？

フィッシング（Phishing）とは、金融機関（銀行やクレジットカード会社）などを装ったメールを送り、電子メールの受信者に偽のウェブサイトにアクセスするよう仕向け、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為のことをいいます。

以下に、典型的なフィッシング被害の一例を説明します（図 1-1 参照）。

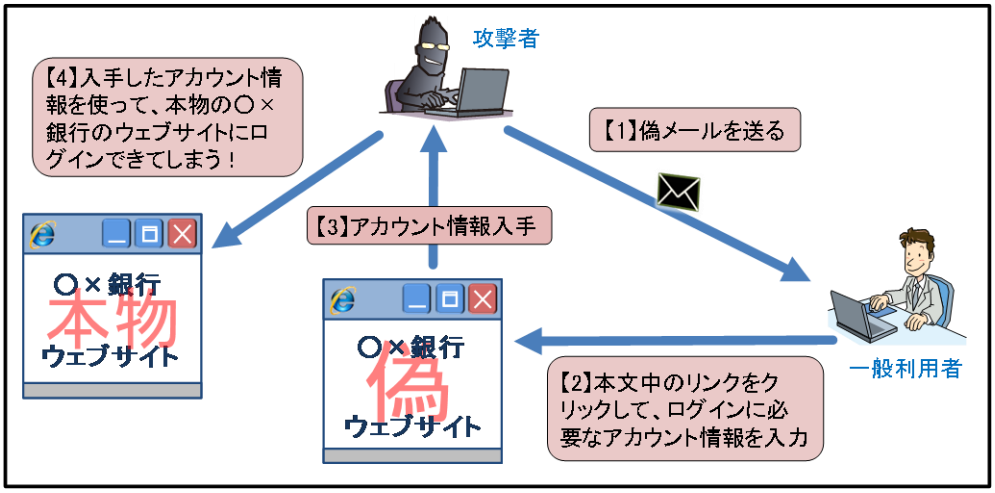

図 1-1：フィッシング被害の一連の流れのイメージ図

【1】攻撃者が偽メールを送信

攻撃者が、正規のウェブサービスや金融機関など実在する会社を装ったメールを無差別に送信します。

【2】利用者がメール本文中のリンクをクリック

メール受信者が、そのメールを信用してメール本文中の URL をクリックすると、事前に用意された偽のウェブサイトに誘導されます。

【3】攻撃者がログイン情報を入手

偽のウェブサイトと気付かずにログイン情報（ID やパスワードなど）を入力してしまうと、そのアカウント情報が攻撃者に渡ってしまいます。

【4】攻撃者が実際のウェブサイトにログイン

攻撃者は、入手したログイン情報を使い、利用者になりすまして本物のウェブサイトにロ

グインします。

(2) ウイルスを使った新しいフィッシング手口の概要

以下に、IPA で確認したウイルスの挙動と一連の手口を解説します。

【1】きっかけとなるメール（フィッシングメール）

国内の大手銀行を装った文面で、ウイルスが添付されたメールです（図 1-2 参照）。

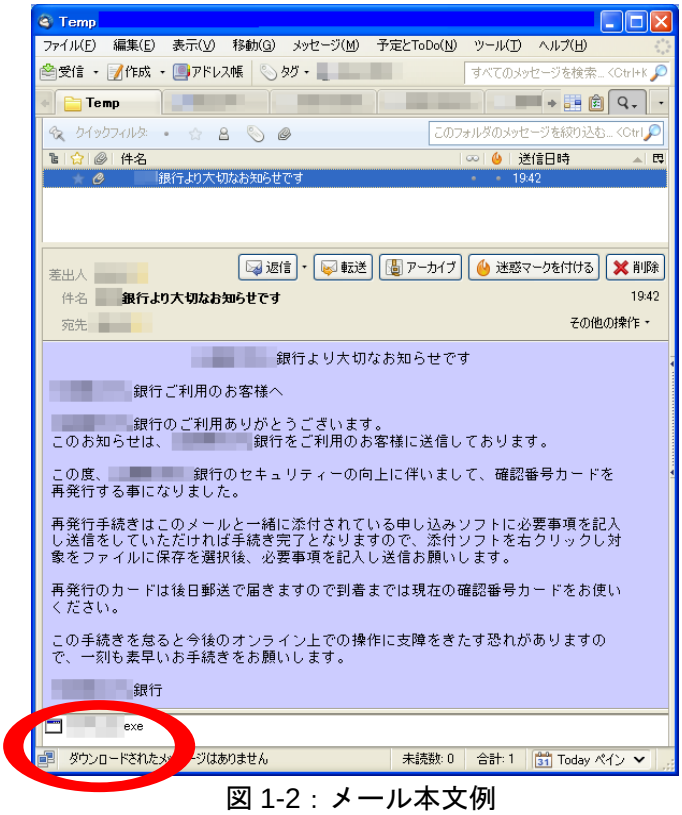

図 1-2：メール本文例

該当メールの添付ファイルを調査した結果、「Banker」や「Jginko」と呼ばれるウイルスの一種でした。アイコンの見た目が実在する銀行のロゴマークと同じもので、これは受信者がついクリックしてしまう効果を狙っていると思われます（図 1-3 参照）。

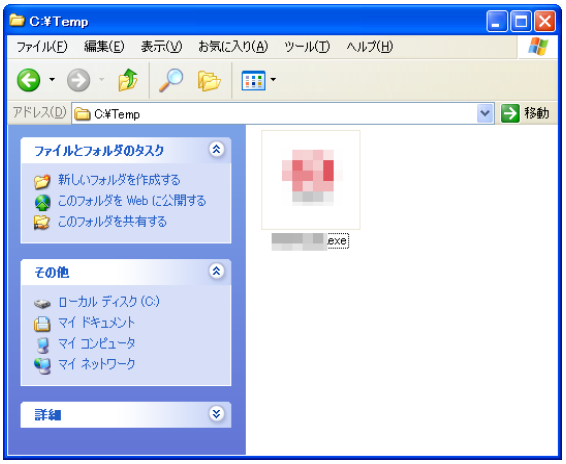

図 1-3：ウイルスのアイコンを表示したイメージ

【2】ログイン情報入力画面

メールの文面に従い、添付ファイルを開くと、送金手続きの際などに必要な契約者番号やパスワード、乱数表の情報全てを入力するように促す画面が現れます（図 1-4 参照）。**通常、このような依頼がメールで来ることはあり得ません。**

図 1-4：情報入力を促す画面のイメージ（表示内容はウイルスによって異なります）

【3】ログイン情報を送信

情報を入力し「送信」ボタンをクリックすると、外部のサーバーに、情報入力済みの画面を画像データとして送信しようとします。

外部サーバーへの接続に失敗した場合には、文字化けしたメッセージが表示されます。日本語環境で文字化けするこの文字列は、中国語簡体字として表示すると「连接失败」となり、これは「接続の失敗」を意味します。このことから、このウイルスは中国語を理解する人物によって作成された可能性があります。

図 1-5：接続失敗時のエラーと思われるメッセージ

【4】悪意ある者がログイン可能に

結果的に、契約者番号、複数のパスワード、乱数表に書かれた全ての情報が相手に知られるため、これらのアカウント情報を基に、悪意ある者がインターネットバンキングサイトにログインし、送金手続きなどをすることが可能になります。

（3）対策

従来のフィッシングの手口では、悪意ある者が偽のウェブサイトを開設し、その上で利用者を偽サイトに誘導する必要がありましたが、今回のケースでは、メールの添付ファイルそのものにアカウント情報を入力させる仕掛けが施されており、仕組みとしては単純といえます。

単純であるが故に、基本的な対策を確実に実施することが大切です。

【i】フィッシング対策

① メールの真偽の確認

金融機関等から来たと思われるメールでも、内容を慎重に確認してください。そもそも**カード番号や暗証番号を入力するような依頼がメールで届くことはありません**。もしそのようなメールが金融機関等から届いた場合は、送信元に電話で問い合わせたり、ウェブサイトのお知らせ欄を見たりして、その情報（メール）の真偽を確認してください。電話で問い合わせをする時は、メール本文に記載されている連絡先ではなく、口座開設時に送付された書類を見る等、正しいと確証が持てる連絡先に電話してください。

② メール記載のリンクに注意

メール本文内にあるリンク先に不用意にアクセスしないことも重要です。当該銀行等のウェブサイトを確認する場合は、メール中のリンクからアクセスするのではなく、ブラウザの「お気に入り」や「ブックマーク」に正しいアドレスを登録しておき、常にそちらからアクセスすることを勧めます。

（ご参考）

フィッシング対策協議会

http://www.antiphishing.jp/

【ii】ウイルス対策

① 添付ファイルの取扱い

メールに添付ファイルがあった場合は、常にウイルスの可能性を疑ってください。普段やり取りのある送信者からのメールでも用心し、少しでも不自然だと思うメールであれば、相手に確認を取るか、メールそのものを読まずに削除してください。

② ウイルス対策ソフトの活用

ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入したウイルスの駆除ができます。前述の事例におけるウイルスについても、ウイルス対策ソフトが導入済であればメール受信時や添付ファイル保存時、またはファイルを開く際にウイルスとして検出することができます。

【iii】事後対応

万一、インターネットバンキングの不正利用の被害に遭ってしまった場合は、当該銀行への問い合わせをしてください。多くの銀行では、ウェブサイトのトップページから問い合わせができるようになっています。さらに、ウイルスに感染していない、自分自身が管理している安全なパソコンから、インターネットバンキングで使用しているパスワードを変更してください。**今回紹介した「Banker」や「Jginko」のように乱数表を入力するタイプのフィッシング詐欺に遭ってしまった場合は、乱数表の内容を既に知られてしまっているので、乱数表カードの交換や、口座を開設し直す、といった対処が必要です。**

なお、ID やパスワードの管理が本質的な対策の一つですので、それに関しては、2011 年 6 月の呼びかけを参照してください。

（ご参考）

IPA - 2011 年 6 月の呼びかけ「パスワード ぼくだけ知ってる たからもの」

http://www.ipa.go.jp/security/txt/2011/06outline.html