

セキュリティ最前線 (2008年5月16日号)

目次：

- | | |
|-------------------|-----|
| 1. 多様化するフィッシング詐欺 | P.1 |
| 2. フィッシング詐欺を見破るコツ | P.4 |
| 3. 最新のロックフィッシュ攻撃 | P.6 |

1. 多様化するフィッシング詐欺

「フィッシング詐欺」とは、ユーザを騙して個人情報を収集する手法です。フィッシング詐欺は通常、インターネット詐欺と関連し、サイバー犯罪者はユーザのクレジットカード番号、社会保障番号、ユーザ ID、パスワード等を盗もうとします。例えば、特定の Web サイトへのリンクをクリックするよう促すメールをユーザが受信します。Web サイトは通常、銀行や保険会社のホームページ等によく知られたサイトに似せたものです。この偽の Web サイト上で、ユーザはセキュリティコードを含む個人情報を入力するよう求められます。Web サイトは本物そっくりですが、これはユーザを騙すためにサイバー犯罪者が作成した偽の HTML ページです。

フィッシング詐欺では通常、メールが利用されますが、その他のコミュニケーション手段も用いられます。ユーザがインターネットの使用に成熟するにつれて、フィッシング詐欺のテクニックも巧妙さを増し、新しい手口が次々を編み出されています。今では「ビッシング (vishing)」と呼ばれる手法を用いるサイバー犯罪者もいます。これは、偽の Web サイトへのリンクの代りにインターネット電話 (VoIP) を使用するテクニックです。メールを利用する代わりにインターネット電話システムを利用し、特定地域のユーザを対象とします。例えば、「お客様のクレジットカードに問題が発生しているため、次の番号まで至急ご連絡ください。」等と告げる録音されたメッセージをユーザは電話で受けます。もちろん、示された連絡先は保険会社のもではなく、サイバー犯罪者につながります。

トレンドマイクロ 脅威研究プロジェクトマネージャ ジャムズ・ヤネザによると、フィッシング詐欺は通常、金銭を盗み取ることを初めとしたさまざまな悪質な目的で行われます。2007 年、高

高齢者を対象としたフィッシング詐欺で「2007年生活費更新版」と題したメールが送信されました。メールの件名通りの内容であれば、4千9百万人の社会保障受給者に対し、保留となっている給付金増加に関する情報を提供するはずですが、実際は受信者を、社会保障サイトを装った偽の Web サイトにリダイレクトし、社会保障番号、銀行口座番号、クレジットカード情報等の提供を促しました。[*1] また、サイバー犯罪者がリモート操作するボットネットを構成する目的で、多くのユーザーのコンピュータへのアクセスを狙ったケースもありました。

ジャムズ・ヤネザによると、通常のフィッシング詐欺では大規模な消費者グループが標的とされるのに対し、ターゲットを絞った「スパイ（槍型）フィッシング詐欺」と呼ばれる攻撃は、小規模ながらより多くの利益をもたらす対象者をターゲットとしています。スパイフィッシングでは、大企業で働くプロフェッショナル、信用組合員、特定地域の人々等が狙われます。会社重役等の大きな獲物を標的としたフィッシング詐欺者は、大きな儲けを狙っています。企業の CEO らをターゲットにした詐欺者は、彼らの高収入とネットワークアクセスに目を付け、組織のネットワークに侵入して企業全体にスパムメールを送信するための大量のメールアドレスを収集します。

数週間前に発生した大規模なスパムメール攻撃では、2万人の会社重役が標的にされました。これらの会社重役は、裁判所からの召喚令状を装ったメールを受信しました。このメールでは、受信者の本名、会社名、電話番号が正しく記載されていました。詳細内容を見るためにメール内のリンクをクリックした受信者は、リダイレクトされた先の Web サイト上で、文書を読むためのブラウザをダウンロードするよう指示されます。ここで「Yes」をクリックした場合、バックドアおよびキーロガーがインストールされ、金融機関の Web サイトでユーザーが入力した個人情報が収集される仕組みになっています。[*2]

悪名高いナイジェリアの 419 詐欺（この種の詐欺を罰するナイジェリアの刑法 419 から命名）は、最もよく知られたフィッシング詐欺の一つと言えます。サイバー犯罪者はこの詐欺で苦境にあるナイジェリアの公務員を装い、アメリカの銀行口座からの送金を求めるメールを送信しました。このメールの受信者は、銀行口座への一時的アクセスを許可するか送金するよう促され、見返りに多額の謝礼を約束されます。しかし実際は、受信者の銀行口座情報および現金がフィッシング詐欺者により盗み取られます。

フィッシング詐欺およびその他のターゲット攻撃が及ぼす経済的影響は、かなりのものです。消費者報告書では、アメリカの消費者が過去 2 年間にウイルス、スパイウェア、フィッシング詐欺の攻撃により 70 億ドル以上の損害を被ったと推定しています。[*3] 企業ユーザおよび個人ユーザの双方が、今日さらに勢いを増しているフィッシング詐欺に関してさらに知識を得る必要があります。ガートナー（Gartner）の調査によると、2006 年 8 月から 2007 年 8 月の間に 360 万人のアメリカ人がフィッシング詐欺による被害を報告しました。これは前年の被害者 230 万人から増加したことになります。[*4] さらに英国 APACS（銀行共同支払決済機構）は、イギリスにおけるフィッシング詐欺が今年第 1 四半期中に倍増したと報告しています。[*5]

参考：

- [*1] By Annys Shin, "The Checkout–Social Security Scam,"
http://blog.washingtonpost.com/thecheckout/2006/11/scammers_who_keep_up_with_the.html November 13, 2006.

- [*2] Dan Goodin, "Fake Subpoenas Harpoon 2,100 Corporate Fat Cats,"
http://www.theregister.co.uk/2008/04/16/whaling_expedition_continues/, April 16, 2008.

- [*3] ConsumersUnion.org, "U.S. Consumers Lose More Than \$7 Billion to Online Threats," Consumer Reports,
<https://secure.consumersunion.org/site/Advocacy?JServSessionIdr007=jkjuzxl2t1.app43a&cmd=display&page=UserAction&id=1799>, August 6, 2007, 2007.

- [*4] Gartner Survey Shows Phishing Attacks Escalated in 2007; More than \$3 Billion Lost to These Attacks,
http://www.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20071217005365&newsLang=en, December 17, 2007.

- [*5] Matthew Broersma, "UK Phishing Attacks Double," TechWorld, November 13, 2006.

2. フィッシング詐欺を見破るコツ

人々が依然としてフィッシング詐欺の犠牲となっている中で、一体どのような対策が有効でしょうか。「その第一段階として、フィッシング詐欺がどのような外見を伴っているかを人々に認識してもらう必要があります」トレンドマイクロ 脅威研究プロジェクトマネージャ ジャムズ・ヤネザはこのように言います。「どのようなメールや電話が怪しいのか認識できれば、騙される人は減ります。」以下に、フィッシング詐欺を見分けるための典型的な特徴および詐欺の犠牲にならないためのアドバイスをいくつか挙げます。

スペルミスや誤った文法

フィッシング詐欺は通常、メールから始まります。これらのメールのほとんどはアメリカのユーザを対象としていますが、メールの送信者は多くの場合、英語を母国語としていません。したがってメールの英語には、スペルミスや誤った文法が見受けられます。「ただし、これは話半分に聞いておいてください。サイバー犯罪者は今やプロのライターやデザイナーにメール内容の構成を外注していますから。私が見たうち 70%がプロとは言えない内容で、このパーセンテージは急速に減少してきています。したがって、正規のメールとスパムメールを見分けることは次第に難しくなってきました。」

インターネットを介して情報を送信しないこと

銀行やその他の企業がインターネットを介して顧客に個人情報の提示を求めることはあり得ないと認識している消費者は少ないようです。また、銀行が顧客に電話をして口座情報や社会保障番号を尋ねることもありません。メールや電話で個人情報を聞かれても決して教えないということを消費者自身が肝に銘じておく必要があります。相手の身元がはっきりと確認できる場合に限り、情報提供を行います。社会保障番号を聞かれた場合、最後の 4 桁のみを教えます。通常、電話会社が顧客のアカウント情報を確認する場合、その他の身元証明があれば社会保障番号は最後の 4 桁のみで間に合います。

クリックに注意

スパムメールそのものはそれほど危険ではありません。スパムメールを受信した後のユーザの行動によりフィッシング詐欺は引き起こされます。例えばスパムメールを受信したユーザが、メール内に設けられたリンクをクリックしたとします。問題はここから発生します。メール内に組み込まれたリンクをクリックしないことで、フィッシング攻撃を回避することができます。「銀行やその他の組織がユーザにソフトウェアのダウンロードを求めることはあり得ません」とジャムズ・ヤネザは言います。「銀行がブラウザヘルプ用ツールバーのダウンロードを求めることはたまにありますが、これも今日のフィッシング攻撃の増加を受けて稀になってきています。」

援助をもとめる策略に騙されないように

多くのボランティア団体がメールを介して募金のお願いをしてきます。その場合、該当の団体に

直接電話をして募金願いが本当のものであるかどうかを確かめることが最良です。先の 419 詐欺の例でも見たように、困った人を助けるための懇願を装ったフィッシング攻撃は多くあります。

メールを介した請願は転送しないこと

チェーンメールやオンラインの請願書は、ほぼすべて正規のものではないと言ってよいでしょう。これらは、多くの人々の電子メールアドレスリストを容易に収集することを目的とした詐欺者によるものです。不幸にも友人や家族にこれらのメールを転送した人々は、サイバー犯罪者の手助けをしてしまうこととなります。請願書の中には、名前、住所、メールアドレスが明記されているものがあります。しかしよく見るとこれらのチェーンメールでは、取り上げている問題を解決するための具体的な行動等が記されていない場合が多々あります。例えば、MADD (Mothers Against Drunk Driving) からの請願メールを装ったチェーンメールでは、目標 5 千人の署名が集まった後にどのような活動が行なわれるのか等が記されていません。[*6] スпамメール送信者は、収集したアドレスリストをフィッシング詐欺やインターネット犯罪に利用します。

油断しないこと

フィッシング詐欺から身を守るための第一手段は、消費者自身が常に用心することです。メールの添付ファイルは、その出所が明確であるもののみを開くようにし、その他の迷惑メールや怪しげなメールは削除します。知っている企業や Web サイトからメールが来た場合、同じ Web サイト上でホストされているリンクのみをクリックします。他の Web サイトにリダイレクトされる場合、メールが正規のものでない証拠とも言えます。

技術的な解決策

フィッシング詐欺から身を守るための最大の防御策としては、すべての可能なエントリーポイント (インターネットの入り口、メッセージの入り口、エンドポイントクライアント、エンドポイントサーバ、ネットワーク) における保護機能を備えた総合的なフィッシング対策ソリューションを利用することです。トレンドマイクロでは、個人ユーザおよび中小企業向けにそれぞれのニーズに沿った多様なフィッシング対策ソリューションを提供しています。さらに、すべての OS、ブラウザ、デスクトップアプリケーション、インスタントメッセージアプリケーション等を常に最新の状態にアップデートしておくことをお勧めします。

フィッシング攻撃から身を守るためのその他の手段や情報に関しては、トレンドマイクロの Web サイト (<http://us.trendmicro.com/us/threats/enterprise/threats-summary/phishing/>) (英語) をご参照ください。

参考：

[*6] Snopes.com blog entry "Somebody Should Have Taught Him,"
<http://www.snopes.com/inboxer/petition/drunk.asp>, December 18, 2007.

3. 最新のロックフィッシュ攻撃

フィッシング詐欺の猛攻撃の裏には、「ロックフィッシュ (Rock Phish)」として知られる特定のテクニックが次第に普及してきていることがあります。洗練されたロックフィッシュ技術の手を借りて、サイバー犯罪者はフィッシング詐欺におよびます。ロックフィッシュは、本格的に人々を騙すことを目的とし、フィッシング詐欺のサイトを何としてでも隠します。また、長期間に渡りフィッシング詐欺のサイトを有効にしておくために「ファストフラックス」を使用します。ファストフラックスとは、フィッシング詐欺のサイトを隠すために利用される DNS 切り替え技術です。

フィッシング詐欺対策グループ (APWG) がサイバー犯罪研究者サミットで行った報告によると、ロックフィッシングは、記録されているフィッシング攻撃のうちほぼ半数に加担しています。ファストフラックスが実際に使用されているのであれば、フィッシング詐欺サイトはより多くのユーザを誘い込もうと比較的長い期間有効にされているはずであると APWG は言います。

トレンドマイクロ 脅威研究プロジェクトマネージャ ジャムズ・ヤネザは次のように言います。「ロックフィッシュの Web サイトはウクライナでホストされている可能性があり、そのインターネットサービスプロバイダーはロシア、コントローラはエストニアに位置しています。セキュリティ専門家や法律の履行を以ってもこれらの Web サイトを早急に取り除くことは困難で、多くの人々がフィッシングメールを受信し、フィッシング詐欺サイトにアクセスしてしまいます。」

トレンドマイクロのコンテンツセキュリティ Web ブロッキングチームの推定によると、ロックフィッシュの Web サイトは一日で 2 万から 6 万に上るといいます。この数はさらに増加しています。これらの Web サイトのほとんどは、同じ IP アドレスでホストされています。

ロックフィッシュキットに加えて、フィッシング詐欺者は「universal man-in-the-middle phishing kit」を販売しています。このキットを利用することにより、詐欺者は偽の URL を設定してユーザに正規の Web サイトにアクセスさせ、より多くの個人情報を収集します。ロックフィッシュと同様に「universal man-in-the-middle phishing kit」も Web ベースの GUI 画像を提供し、ターゲットとしている正規の Web サイトに類似した Web サイトを用意します。フィッシング詐欺者が作成した Web サイトは、正規の Web サイトと交信し、そのオリジナルページをロードします。ユーザがその正規の Web サイトに接続している間に、詐欺者はフィッシング詐欺サイトを介してうまくユーザの個人情報を収集します。

ごく最近では、ロックフィッシュを利用した新しい情報漏えい型不正プログラム (別名「Zeus」) が生み出されました。この攻撃でユーザは、銀行のオンラインログインページ (実際はロックフィッシュにより作成されたページ) にアクセスするための「電子証明書」をインストールするよう指示されます。トレンドラボのコンテンツセキュリティチームは、複数の「不正な証明書」を発見し、これらを「TSPY_PAPRAS.AC」および「TSPY_PAPRAS.AD」として検出対応しています。これ

らの不正プログラムは、アメリカ銀行とコロニアル銀行を標的にしました。

典型的なフィッシング攻撃では、特定の機関や企業のログインページを装った偽の Web サイトにユーザを誘導するためにメールを利用しています。一方ロックフィッシュ攻撃では、ユーザを偽の Web サイトにログオンさせる必要なしに、詐欺者は情報を収集します。これは、ユーザのコンピュータにスパイウェアを埋め込むことにより、ユーザのコンピュータ操作がリモートサーバに送信される仕組みによるものです。したがって、セキュリティ保護されていないユーザの個人情報は危機にさらされています。

最近のこれらの脅威からも分かるように、メール内のリンクのクリックには警戒すること、およびウイルス対策製品を常にアップデートしておくことが今一度ユーザに強く求められます。

※ セキュリティ最前線は、米国トレンドマイクロで発行しているニュースレター「[First Line Of Defense \(FLOD\)](#)」(英語)を元に翻訳したものです。

※ お申し込み：[「F.L.O.D. Threat Watch Newsletter Signup](#)」(英語)

[<http://us.trendmicro.com/us/newsletter/>](http://us.trendmicro.com/us/newsletter/)