特集：セキュリティリポート裏話（9）：

2018年も「金銭狙い」で変化続けるフィッシング、最新の手口は

http://www.atmarkit.co.jp/ait/articles/1811/28/news026.html

世の中で知られるようになってから10年以上が経つが、いまだに被害が減るどころか、スマートフォンの普及によって新たな手口が登場しているフィッシング。月次・年次で報告をまとめているフィッシング対策協議会に最近の動向と対策を尋ねた。

2018年11月28日 05時00分 更新

[高橋睦美，@IT]

フィッシングに関する情報収集や注意喚起、対策支援を行っているフィッシング対策協議会では、利用者や関連事業者から寄せられる通報を元に月次報告をまとめ、公開するとともに、毎年6月前後にフィッシングに関する年次レポートを公開してきた。

2018年全体の動向がまとまるのはやや先の話になるが、同協議会事務局 証明書普及促進ワーキンググループ副主査の駒場一民氏によると、最近のフィッシングには「金銭目的ということに変わりはないが、手口が多様化してきている」という特徴が見られるという。

公的機関や民間企業のふりをして、「アカウントが危険な状態にあります」といったメールやSMS（ショートメッセージングサービス）を送り付けて本物そっくりに作られた偽のWebサイトに誘導し、「安全のために必要です」などといった文面でIDやパスワード情報を入力させ、裏側でその情報を盗み取る「フィッシング」という手口が世の中で知られるようになってから10年以上経つが、いまだに被害は減らない。年によってはフィッシングメールや誘導先のフィッシングサイトの報告数に増減はあるが、常に一定数が流通している形だ。

2018年も、これまでにまとめているのは9月までの数字だが、過去4年間で最悪のペースでフィッシングメールに関する報告が寄せられているという。

注目したい傾向は、狙いの変化だ。正確には、「金銭狙い」という大きなトレンドに変わりはないが、「詐取しようとする情報が変わっている」と駒場氏は述べる。2014年から2015年にかけて主流だった、金融機関をかたって銀行口座情報とパスワードを詐取するフィッシングメールがぱったりとやみ、代わりに、クレジットカード番号を盗み取ることを目的としたフィッシングメールが幅を利かせるようになっているという。

背景としては、金融機関側の対策が功を奏したことが挙げられるだろう。2014年以降、インターネットバンキングを狙ったフィッシングが増加し、それに伴って被害額も急増。大手金融機関だけではなく地方銀行や信用金庫、ネット銀行をかたるなど手口が広がり、被害額は2015年度で30億円を超える規模に達した。が、事態の深刻さを踏まえて警察や金融機関側が業界を

挙げて対策に取り組み、ログイン時の認証方法を強化したり、一般利用者に向けて時に大げさに見えるほどの注意喚起を行ったりする他、金融機関間での情報共有を進めてきた。

この結果、フィッシング詐欺を仕掛けるサイバー犯罪者にとって、オンラインバンクをかたるフィッシングのコストは高くなった。

代わって彼らが着目しているのが、「比較的手間もコストもかからず、かつ追跡されにくい、主に海外のメジャーブランドをかたったフィッシング詐欺だ」（駒場氏）。特に、海外の事業者からドメイン名を取得し、サーバも海外に置いている場合などは、「初期投資」が少なくて済む割に、事業者や関連機関を通じてWebサイトのテイクダウン（閉鎖）をしようとしても時間がかかり、詐欺師によって割のいい方法になっているという。

ソフトバンク、佐川急便……メジャーブランドをかたるフィッシングが増加

2017年のレポートでも触れられている通り、金融機関をかたったフィッシングメールの代わりに増加しているのが、AmazonやApple、楽天といった、オンラインで広く利用されている「メジャーブランド」をかたったフィッシングメールだ。会員ページを模したサイトに誘導し、ユーザーのIDやパスワード、さらにはクレジットカード番号などをだまし取ろうとする手口が主流だ。

この記事を書いている2018年11月にも連続して、Appleの名前をかたり、Apple IDとパスワードの他、クレジットカード番号を入力させるWebサイトに誘導するフィッシングメールが増加し、フィッシング対策協議会をはじめ関係組織が注意を呼び掛けている。

このように、いわゆるプラットフォーマーやECサイトをかたった詐欺が目立った2018年だが、中でも特徴的な手口の一つが、ソフトバンクをはじめとする携帯キャリアの決済サービスを狙うフィッシングで、2018年2月、4月に多くの通報が寄せられた。

「最初は『なぜ、携帯キャリアの会員サイトにログインするためのIDとパスワードを盗むのだろう。ユーザーの月々の請求額が分かったところで、それほどうまみはないはずだ』と思わされたが、よくよく考えてみると、キャリア決済を用いることで、上限3〜4万とはいえ、換金可能なiTunes Cardなどを購入し、ギフトとして第三者に送付できてしまう。人によっては、月々の携帯電話の料金をあまり細かくチェックしないこともあり、発覚までさらに時間がかかることも目を付けられた要因だろう」（駒場氏）

さらに「これまでのフィッシングメールは受け取っても無視すれば済んだが、こうした手口に対しては、自分自身の携帯電話の設定を見直し、キャリア決済の上限額を低く設定する必要がある。それも、できれば今すぐに」とアドバイスした。

もう一つ注目したい手口が、2018年8月に急増した、佐川急便の名前をかたって不在通知を装って送られるSMSフィッシングだ。iOSの端末でアクセスするとフィッシングサイトに誘導され、Android端末でアクセスするとマルウェアをダウンロードさせようと試みる。万一このマルウェアをインストールしてしまうと、端末でやりとりされている情報が盗み見されたり、あらゆる操作が可能になったりする恐れがある。

佐川急便をかたるフィッシングは2018年9月にいったん落ち着いたものの、手を変え、品を変えながら継続しており、2018年10月に再び増加傾向を見せている。駒場氏は、日本語の表現がこなれている上、荷物の再配達という日本社会で広く利用されているサービスをかたることから、「日本人、あるいは日本の社会状況に非常に詳しい人物が犯行に関与しているのではないか」と推測している。

中には、佐川急便の名前を名乗りつつ、なぜかApple IDやパスワードを尋ねてくる不正サイトも報告されているという。冷静に考えれば、「荷物の配送にこうした情報が要求されるのはおかしい」と思えるかもしれない。が、「頭では分かっていても、疲れて夜遅く家に帰ってきたときなどにこうしたメールを見て、ふとクリックしてしまうこともあるだろう」と駒場氏は警鐘を鳴らす。特に、Android搭載端末は「提供元不明のアプリのインストールを許可する」の設定を無効にし、メッセージを受け取ってうっかりクリックしてしまった場合に備えることも有効だ。

大学生も標的に、学内IDを狙うフィッシング

もう一つ注意したいのが、大学の情報システム部門をかたった手法だ。「メールボックスの容量が限界に近づいている」旨の通知を装って偽のサイトに誘導し、学生が利用しているIDとパスワードを盗み取る手法だ。奪ったアカウントは、別の被害者に不正なメールを送付するのに悪用されたり、学内の情報収集、個人情報流出につながったりする恐れがある。クラウドサービスが企業だけではなく、大学をはじめとする教育機関で広く利用されるようになってきたことを背景に、引き続き注意が必要な手法だという。

フィッシングメールは、金銭狙いのものが圧倒的多数を占めるが、標的型攻撃の最初のトリガーとして用いられることもある。同一のIDとパスワードが使い回されていると、得られたIDとパスワード足掛かりにして別のシステムに侵入され、芋づる式に侵害範囲が広がる恐れがあるわけだ。「教育機関の場合、メールシステムだけではなく、大学の他のシステムでも学生番号などの同じIDとパスワードを利用している場合が多い」（駒場氏）ため、特に注意が必要だ。

ただ学生の場合、年齢が若いこともあって一般にリテラシーが低い。また、雇用関係にある企業とは異なり、セキュリティポリシーを強制させるのも難しい。駒場氏はさらに、「この先、成人年齢が18歳に引き下げられると、多くの学生がクレジットカードを手にできるようになる。そうなったときに、被害が広がらないかが懸念される」と指摘した。

こうした事態に備え、フィッシング対策協議会では、2018年から複数の大学と協力して学生向けのフィッシング啓蒙、啓発活動を開始した。まだ5〜6校程度だが、2019年度以降、より多くの大学に拡大していくという。

「気を付ける」だけではない対策とは

フィッシングへの対策となると「不審なメールは無視する」「不審なリンクはクリックしない」という心掛けがしばしば言われる。確かに注意を配ることは大切だが、それだけでは限界があるのも事実だ。

攻撃者側も策を弄（ろう）しており、本物のサイトをそのままコピーしたり、本物のブランド名の一部を利用したドメイン名を多数取得して次々使い捨てたりしながら攻撃を仕掛けてくる。時には、電子証明書まで取得してユーザーをだまそうとすることもあり、「気を付ける」だけでは見抜きようがないことがある。

こうした手口も相まってか、残念ながら、フィッシングによるクレジットカード不正利用被害は増加している。日本クレジット協会の調査によると、いわゆるスキミングによる被害も微増しているが、それ以上に「番号盗用被害」が増加しており、2016年の88.9億円から、2017年にはほぼ倍増して176.7億円に達した。2018年もそのペースは衰えず、1〜6月の半年だけで92.8億円と過去最悪のペースで、その流出経路としてマルウェア（トロイの木馬）や企業サイトからの流出とならび、フィッシングが多いと思われる。

クレジットカード業界もフィッシング対策の必要性を感じており、3Dセキュアなどの対策を導入するケースも増えているが、「使いやすさとてんびんに掛ける必要があり、対策はこれからの課題だ」と駒場氏は指摘している。

企業としては、同協議会が公表しているガイドラインに沿ってサーバ証明書やDKIM（DomainKeys Identified Mail）/DMARC（Domain-based Message Authentication, Reporting & Conformance）を実装し、なりすましメールを見抜く手段を実装することが推奨される。だが、詐欺師が勝手にドメインを取得し、名前をかたったWebサイトを作ることまでは防げないのも事実だ。

「自社をかたるフィッシングサイトを見つけ次第自力で、あるいはサービス事業者を通じて通報、共有するとともに、ユーザーに対する注意喚起を行う地道な作業を続けていくことも、ブランドの価値を守るために必要だ。また、アナログな手段だけに忘れがちだが、問い合わせ用の電話窓口が用意されていれば、いざというとき直接尋ねることができ、顧客の安心材料の一つになる」（駒場氏）

一方ユーザーの側としては、まずはフィッシング対策業議会やJC3（日本サイバー犯罪対策センター）が提供している情報を参照して横行している手口を知り、受け取ったメッセージに対して「ひょっとしたら」という疑いを持つことが対策の第一歩になるだろう。また、事業者が用意しているならば極力、二要素認証や多要素認証を利用すべきだ。

メールやメッセージ、ソーシャルネットワークが使われる限り、フィッシングというものを絶滅させることは難しいだろう。「クレジットカード情報の不正詐取はもちろん、一見すると、金銭とは無縁のように思えるポイントや携帯キャリア決済を狙う手口など、何らかの形で金銭につながる情報を狙う手口はこれからも増えていくだろう」と駒場氏は警告する。引き続き、関連各機関と調整しながら注意喚起に務めていくため、ぜひそうした情報を参照してほしいとした。

特集：セキュリティリポート裏話

近年、効果的なセキュリティ対策を実施するには、脅威の最新動向を常にウオッチし、分析することが欠かせません。その成果の一部が多数のセキュリティベンダーから「リポート」や「ホワイトペーパー」といった形で公開されています。この特集では、そんな各社最新リポートのポイントを解説するとともに、行間から読み取れるさまざまな背景について紹介していきます。

セキュリティリポート裏話

特集：セキュリティリポート裏話

関連記事

国内でフィッシング詐欺が急増、クラウドサービスのアカウントが脅威対象に――トレンドマイクロ調べ

トレンドマイクロが発表した2018年上半期（1月～6月）のセキュリティ動向によると、国内では、クレジットカード情報やクラウドサービスの認証情報を狙う「フィッシング詐欺」が急増。また、「不正マイニング」などの仮想通貨を狙う脅威は、世界的に拡大傾向にあることが判明した。

5分で絶対に分かるフィッシング詐欺

「OWASP Top 10」をはじめ、業界標準ガイドラインの改訂相次ぐ

セキュリティ対策をまとめ、強化する際に役立つ資料がある。政府やコミュニティーがまとめた公開ドキュメントだ。経済産業省の「サイバーセキュリティ経営ガイドライン Ver 2.0」とOWASPの「OWASP Top 10 - 2017（日本語版）」を中心に内容を紹介する。

ITmedia Inc.