

セキュリティ最前線 (2009年2月3日号)

目次:

- | | |
|-------------------------------------|-----|
| 1. 不正プログラムをもたらす“偽 LinkedIn プロファイル” | P.1 |
| 2. 経済停滞期の脅威とは | P.4 |
| 3. 2009 年の脅威からあなたと PC を守る行動指針トップ 10 | P.6 |

1. 不正プログラムをもたらす“偽 LinkedIn プロファイル”

どのような脅威か

2009年1月中旬、ソーシャルネットワーキングサイトの「LinkedIn」において、偽のプロファイルがいくつか掲載されていることが、トレンドマイクロのウイルス解析技術者により確認されました。偽プロファイルは、著名なセレブリティのプロファイルを装っており、ヌード写真を含め何枚かの写真も掲載され、ビヨンセ、ヴィクトリア・ベッカム、ケイト・ハドソン、サルマ・ハエックといったセレブリティたちが利用されていました。本来、「LinkedIn」は、企業にかかわる人々がビジネス関係の人脈を築くために利用するサイトです。そこにセレブリティのゴシップを好む人々向けのワナを設けるとは、意表をつく仕掛けではありません。

これらの偽プロファイル内には、リンクが貼られており、クリックすると、閲覧しているブラウザがリダイレクトされ、最終的に不正プログラム、「TROJ_DLOAD.ML」(※1)に導かれます。この不正プログラムは、実行されると、自身の亜種(「TROJ_DLOAD」)をダウンロードし、さらに偽セキュリティソフト、「TROJ_FAKEAV.GDS」(※2)をダウンロードしてインストールします。また、リダイレクト先のドメイン名(全て同一のIPアドレスにホストされています)は、いかにもどこかで聞いたような記述になっています。このため、ユーザは、正規のURLと誤ってしまいます。

「LinkedIn」を狙った攻撃としてはこれが初めてではありません。このソーシャルネットワーキングサイトを狙った攻撃は、2008年7月にも発生しました。有名な419詐欺(ナイジェリアを舞台にEメールを利用した国際詐欺。ナイジェリア刑法第419条の抵触に由来し「419詐欺」と呼ばれる)と似た手口でユーザの個人情報入手しようとしていました。この手口の場合、ユーザは、大きな利益が得られる一種の投資を促されるのです。ただこの手口も、最近は巧妙化が進む中、新たな脅威として再び注目され、「LinkedIn」にとどまらず、他のソーシャルネットワーキングサイトにまでその勢力を伸ばしつつあります。

“マイクロブログ”として知られる「Twitter」もサイバー犯罪者の攻撃に見舞われたようです。この場合の手口も、偽プロファイルでユーザを騙し、不正プログラムへと導くことです。現在、69名の“フォロワー”が攻撃にあったとのこと。この数は、既に数百万にも及ぶ「Twitter」のユーザ数に比べると、まだごく少数ではあります。しかしながら、「Twitter」や「LinkedIn」に対する一連の攻撃から、以下の2点が明らかになったといえるでしょう。

まず1つは、サイバー犯罪者たちは、今後もソーシャルネットワーキングサイトを標的にやりたい放題するだろうという点です。不正プログラム作成者たちは、喜んで手の込んだ脅威をもたらしてくるでしょう。特にそうしたサイトでのメンバー数の増大は、この傾向をもたらす大きな要素となります。「Facebook」は、最もよく狙われるサイトですし、「Bebo」や「Hi5」、「Friendster」、「Classmates.com」といったサイトも、この数ヶ月間で、不正プログラムやスパムメールによる攻撃が注目を集めたところです。

さらに重要なもう1つの点としては、こういったソーシャルネットワーキング関連の脅威の場合、“偽プロフィール”が非常に重要な役割を果たすという点です。サイバー犯罪者たちは、この手口を駆使して多くのユーザを騙し、不正なリンクをクリックさせます。この場合、「ソーシャルネットワーキング内にまさか偽のプロフィールがあり、このような場所がハッキングされるとは思いもよらない」というユーザの心理につけ込んでいるのです。また、トレンドマイクロのウイルス解析技術者も、ハッカーの集う地下のオンラインフォーラムでそうした“偽プロフィール”がセットで売られていたのを、偶然発見したようです。こうした点から、いわゆる「CAPTCHA」のセキュリティ機能がもはや確実ではなくなったことも理解できます。この機能は、歪んだ文字列を判断させることで、サイトへのツールによる自動ログイン等を避ける役目を果たしていたわけですが、いまや、サイバー犯罪者たちがツールを利用して、「CAPTCHA」を簡単にすり抜け、さらにソーシャルネットワーキング内へのログインも、自動で行えるようになったわけです。

どのようなリスクにさらされるか

「LinkedIn」にセレブリティのプロファイルがあるなど、一見すると怪しいことなのですが、一般の「LinkedIn」ユーザたちならば、本物のプロフィールと信じてしまう場合もあります。このサイトに「こうも簡単に偽物が掲載されるはずがない」と考えているからです。また逆にいえば、本来ならばビジネス関連のネットワーキングに利用されるこのサイトにセレブリティのプロファイルという事実自体が、ユーザの好奇心を十分に掻き立てることになります。かくして、ちょっとした好奇心に駆られたたった1回のクリックが、それが不正なリンクのクリックであるために、脅威にさらされる結果となるわけです。今回の攻撃は、まずコンピュータが感染させられ、その後（ユーザに感染を気づかせて）偽セキュリティソフトを売りつけて金を巻き上げるという手口のようなのです。このように、今回の攻撃は、ユーザたちがもう何ヶ月にも苦しめられてきた“偽セキュリティソフトのワナ”も仕掛けられた脅威でもあります。

「LinkedIn」は、今後もより多くのユーザを惹きつけるサイトとなるでしょう。2008年、「LinkedIn」は、メンバーの増加率が193%にも及び、メンバー増加率の高いソーシャルネットワーキングサイトの中では、第4位となりました。また、「Twitter」のメンバー増加率は、343%であり、これは2008年の第1位です。こうした新規メンバーも、既にメンバーであるユーザも、区別なく今回のような脅威にさらされているといえます。

「LinkedIn」のような被害にあったソーシャルネットワーキングサイトは、ユーザからの信頼を失ってしまうリスクにもさらされています。もしサイト内の“偽プロフィール”から直接に不正なWebサイトに接続されているとすると、こうしたソーシャルネットワーキングサイトは、すでにそれ自体が危険なサイトであると、ユーザが見なしてしまうからです。

トレンドマイクロからのソリューションとアドバイス

トレンドマイクロのスマートプロテクションネットワーク（SPN）は、従来のアプローチよりもさらに進んだセキュリティ対策で、新種の脅威がユーザを襲う前にこれをブロックします。このSPNは、トレンドマイクロの様々なソリューションおよびサービスの中で用いられ、トレンド独自の「クラウド技術」と「軽量クライアントアーキテクチャ」を組み合わせたもので、これにより、ユーザがどこで接続していてもその個人情報が入座に自動的に

に保護されます。また、この SPN は、攻撃全体から必要なセキュリティ対策を識別し、それらを「コリレーション技術」という相互関連づけにより、トータルな防御を可能にした唯一のセキュリティ技術でもあります。

SPN は、「Web レピュテーション技術」の防衛層では、危険な Web サイトを識別し、そのドメイン評価に基づき、ユーザのアクセスをブロックします。今回の場合、「LinkedIn」の偽プロフィール内にリンクが、この技術により既にブロックされているので、ユーザが不正な Web サイトにリダイレクトされるのを避けます。「Eメールレピュテーション技術」の防衛層では、関連したスパムメール等をブロックします。これにより、不正なドメインへのリンクが含まれたメールをユーザが受信するようなことはありません。「ファイルレピュテーション技術」の防衛層では、ユーザのコンピュータにダウンロードされてくるファイルが信頼のおけるものかどうかを検証します。デスクトップでは、アンチウイルス対策製品により、「TROJ_DLOAD.ML」や「TROJ_FAKEV.GDS」、その他の危険な脅威の検出と削除が行われます。

注：

今回ご紹介したウイルスの詳細情報は下記 Web ページをご覧ください。

※1 TROJ_DLOAD.ML

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ_DLOAD.ML

※2 TROJ_FAKEV.GDS

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEAV.GDS

2. 経済停滞期の脅威とは

経済の停滞につけこむ

グローバル経済が苦難に陥るほど、闇の地下経済は繁栄するようです。サイバー犯罪者たちは、ますます巧妙化された手口を用いて、消費者の個人情報を盗んだり、売り飛ばしたりしています。2009年はこの傾向がさらに多くのサイバー犯罪が発生するだろうと、トレンドマイクロのウイルス解析技術者も予想しています。

「現実世界の経済が停滞すると、地下のサイバー犯罪者たちは、そうした状況での人々の不安につけこむのです。つまり、銀行の合併や、抵当権失効、その他の不安を煽るようなニュースに関して注意を喚起するようなスパムメールを作成し、不安にかられた人々にクリックさせようとするわけです」と、トレンドマイクロのアドバンス・スレット・リサーチャーの Paul Ferguson は説明します。

銀行にとっての厄介なニュース

銀行は、今回のグローバル金融危機で大きな打撃をうけましたが、相変わらず、ソーシャルエンジニアリングによる詐欺の格好の標的のようです。例えば、2008年には、偽のデジタル証明書を利用した事件が多発し、このため、オンライン銀行におけるセキュリティの信頼性が失墜してしまいました。デジタル証明書は、オンラインでビジネスを行う上で信頼関係を維持するための、いわば“電子身分証明書”といえるものであり、多くの銀行において、オンライン業務のセキュリティ管理に重宝していました。

しかし残念ながら、ハッカーやフィッシング詐欺師たちは、この種のセキュリティならば簡単に適応してしまいます。2008年4月に発生したフィッシング攻撃では、バンク・オブ・アメリカ(Bank of America)の顧客を標的にしており、「Rock Phish gang」というツールで作成した偽デジタル証明書を顧客にインストールさせるという手口が使われました。そしてそれから2週間も経たないうちに、コメリア銀行(Comerica Bank)およびコロニアル銀行(Colonial Bank)を狙った別の偽デジタル証明書の存在が、トレンドマイクロにより確認されました。

従来のフィッシング攻撃の場合、まずフィッシング詐欺師がメールを送信し、それを介してユーザを偽のログインページに導くという手口がとられていました。しかし、コメリア銀行やコロニアル銀行への攻撃の場合、すでにスパイウェアがユーザのコンピュータに仕込まれているので、偽ログインページにユーザを導いてそこから個人情報を収集するという手間をかけずとも、そのまま収集活動ができます。この巧妙な手口により、無防備なユーザは、簡単に大量の個人情報が盗まれてしまいます。

スパイウェアによるフィッシング詐欺では、2008年9月、米国で第4位の規模を誇る金融機関、ワコビア(Wachovia)も標的にされました。この攻撃には、ルートキットも利用されていたようです。ルートキットは、感染したファイルやプロセスを隠ぺいさせる機能を持っており、これにより、感染したコンピュータ内で全く目立たないように不正活動を行うことができます。同種の攻撃は、当時、窮地に立たされていたメリルリンチ(Merrill Lynch)にも及んだようです。ちょうどその頃、メリルリンチは、バンク・オブ・アメリカからの買収行為でメディアからは大いに注目されていました。

この場合、偽のメリルリンチ関連のリンクをクリックすることにより、不正プログラムがダウンロードされました。この不正プログラムは、感染したコンピュータのセキュリティを改変するので、結果として不正リモートユーザによる遠隔操作が可能になります。ワコビアを標的にした攻撃も類似の手口が利用されています。ワコビア

への攻撃の場合、感染したコンピュータ内にトロイの木馬型のルートキットが作成されました。このルートキットが、不正活動を行うファイルやプロセスを隠ぺいしながら、それらのメモリ常駐を確保するのです。手口の類似性から、この2つの攻撃は、同一の不正プログラム作成者によるものだと考えられています。

“電子割引券”を集めて節約

2009年、サイバー犯罪者たちは、いわゆる“偽の電子割引券”を用いた手口も多用してくるだろうと、セキュリティ専門家たちは予想しています。この偽の電子割引券で“節約好き”な消費者をうまく騙すというわけです。実際、2008年には、マクドナルドの顧客を標的にしたこの種のフィッシング詐欺が発生しています。マクドナルドの顧客に「(偽の)メンバー向け顧客満足度調査アンケート」と称した偽のWebページを表示し、「回答すれば顧客の口座に75ドルが振り込まれます」などと説明。そしてアンケートに回答した後、顧客は、氏名、メールアドレス、クレジットカード番号、電子証明等の入力促されました。

偽のアンケート調査は、2008年、いくつかのフィッシング攻撃で利用されました。たとえば、上述のマクドナルドと似た事例として、2008年12月、コカ・コーラのプロモーションを装った攻撃が確認されました。この“偽プロモ”では、アンケート調査に回答すると、「無料のパハマ旅行」や「ソフトドリンク生涯無料券」が貰えるなどと説明していました。この種のアンケート調査は、回答者への特典が付きものですが、2008年に発生した数々の事例から、「特典を得たい」という消費者の心理を、サイバー犯罪者たちも巧みに利用していることが明らかになりました。

「Storm」が流した噂

「Storm」に関わるサイバー犯罪者たちも、消費者の金融に関する不安につけこむような活動をしています。2008年7月、サイバー犯罪者たちは、そうしたスパムメールを送信しました。メールには、「現在の世界金融状況に関する詳細説明」などと称して、「AMERO通貨が実施される可能性」といった内容を紹介するリンクが貼られていました。「AMERO通貨」とは、「北米通貨統合(North American Currency Union)」といった架空の組合による北米統一通貨構想のこのように、好奇心から思わずリンクをクリックしたユーザは、不正なWebサイトへと導かれ、ここで「Storm」の亜種による被害をうけることになります。むしろ、「AMERO通貨」も「北米通貨統合」も実在しないのですが、米国・カナダ・メキシコの間でこのような協定が結ばれる噂はよく知られており、ユーザは思わず興味を抱いてしまうわけです。2008年、AMERO通貨による米財務証券が発行されたとの報告があったようですが、これも直ぐに事実ではないことが判明したようです。

企業に対する脅迫メール

経済停滞が相変わらず続く中、いわゆる“脅迫メールによる攻撃”が、2009年後半から増えているのではないかと、トレンドマイクロのウイルス解析技術者たちは予想しています。そしてこの攻撃では、個人のホームユーザよりも、中小企業の方が標的にされるだろうとも見えています。中小企業は、それなりに高額な金銭をゆすりとることができる規模がある一方、IT関連を破壊するといった脅迫に対して独自に対応できるほどの設備はありません。特に経済的にも問題のある時期はなおさらでしょう。そしてこの攻撃は、DDoS攻撃(分散型サービス拒否攻撃)の手口が使用されるはずですが、これならば、こういった中小企業の電子商取引のサイトをダウンさせることもできます。また、企業の重要ファイルを暗号化でロックしてしまい(「解除してほしければ金を出せ」と)、恐喝に使うこともできるでしょう。現在の経済危機のもと、多くの中小企業は経費削減に苦勞しており、そのような中で(「業務を麻痺させてほしければ、金を払え」などという)“脅迫メール攻撃”を受けてしまうと、“体力”のない企業は、サイバー犯罪者からの高額請求といった恐喝に屈服してしまうかもしれません。

3. 2009年の脅威からあなたとPCを守る行動指針トップ10

トレンドラボでは、「2009年に発生する脅威から、いかに自分自身とコンピュータを守るか」という点について、下記のような「行動指針トップ10」をまとめました。そのいくつかは既に馴染みのあるものでしょうし、また、意外に思われるものもあるかもしれません。いずれにしても、これらの正しい行動を実践することで、2009年も安全にインターネットを利用することができます。

1. ご利用のアプリケーションやオペレーティングシステムを常に最新にしておくこと

「自動更新・インストール」といった機能を用いれば、更新プログラムや修正パッチがリリースされると、それが直ぐ自動的にご利用のアプリケーションやコンピュータに適用されます。これにより、コンピュータの設定も常に最新化され、更新プログラムが完全にインストールされた状態を維持することができます。企業の場合、IT部門の担当者が、脆弱性チェックのスクランを社内ネットワーク上で少なくとも1週間に1回の頻度で行うべきです。また、ほとんどのプログラムは、自動更新の機能が備わっていますが、それでも念のため、自動更新の設定を見て、どの程度の頻度で更新されるかをチェックしておくことです。できれば、「毎日」に設定するのがよいでしょう。自動更新の機能のないソフトウェア等の場合は、そのソフトウェアの発売元のWebサイトに行き、適正な修正パッチのダウンロードを定期的に行う必要があります。

2. ご利用のセキュリティソフトを最新化しておくこと

定期的に更新されるウイルス対策製品を最新化しておくことで、脆弱性を利用する脅威からご使用のコンピュータを守ることができます。たとえば、「トレンドマイクロ ウイルスバスター2009」は、脆弱性利用の防止やファイアウォール、コンテンツフィルタリングといった機能を総合的に備えています。企業などの大きな組織の場合、「トレンドマイクロ脆弱性診断サービス (Vulnerability Assessment)」をご利用いただくことも可能です。これを「トレンドマイクロ Control Manager」と一緒にご利用いただくことで、現状のネットワーク・セキュリティレベルを診断・報告し、潜在的に発生するセキュリティ上の脆弱性を識別することもできます。また、ご利用のセキュリティソフトで、お使いの各種プログラムのスクランも行ってください。新たなプログラムをインストールする際には、「使用許諾契約書」を注意深くお読みください。その中に該当のプログラム以外のものをダウンロード・インストールするなどの記述があった場合は、直ちにインストールを中止してください。

3. Webサイト評価サービスを利用する

「Trendプロテクト」等、無料のWebサイト評価サービスの利用もお勧めします。こうしたサービスを活用すれば、迷惑な内容や危険な内容が含まれたWebページを避けながら、安全にインターネットを利用することができます。

4. スクリプト機能やウィジェット (widgets) を無効化しておくこと

Webを利用した多くの攻撃は、様々なスクリプト機能を使用し、ブラウザ上で感染プログラムを実行させます。また、ダウンロード機能のあるウィジェットを利用する場合があります。こうしたスクリプト機能は無効にしておき、またできればウィジェットも利用しないようにしておけば、ユーザは、こういった手口を用いる攻撃から身を守ることができます。

5. 用心深く、疑い深くいること

フィッシング攻撃の“最前線”で身を守るのは、ユーザ自身であり、それゆえに各人の判断は非常に重要です。その点で何よりも重要な行動指針としては、メールの添付ファイルに関しては、知っている相手・予期した相手からのメールのみ開くこと。迷惑なメールや怪しいメールはすべて削除すること。知っている企業のWebサイトからメールが届いた場合、メール内のリンクをクリック

する場合は、宛先がそのサイト内へのものだけにすること。つまり、リダイレクトにより別のサイトに飛ばされるようなリンクが貼られてメールは、まず不正なメールに違いないと見なすべきです。

6. 「個人情報を確認したい」というリクエストには応じないこと

銀行もその他の企業も、個人情報の確認をインターネット上で行うことは決してありません。この点を知らない顧客は意外と多いようです。また、銀行の場合、口座情報や社会保障番号 (Social Security Number) を電話で確認してきたりすることも決してありません。「メールや電話を介した個人情報の確認には絶対に応じない」と、決めておくといよいでしょう。仮に確認作業を行う場合は、相手側が自身の本人確認を、事前にしっかりと行ったときのみ限定すべきです。また、社会保障番号の確認を求められた場合も、相手に教えるのは下4桁のみとしておくべきです。たとえば、電話会社から電話があり、利用している電話のアカウント情報の照合で社会保障番号が必要です。と言われても、この場合でも、相手に伝える情報は、下4桁としておくべきです。

7. スпамメール内のリンクはクリックしないこと

危険は、スパムメール受信自体にあるのではなく、スパムメールを受信したユーザが何かをした際に発生します。ユーザがスパムメールを受信し、様々な誘い文句で、ユーザにメール内のリンクをクリックさせるように促します。そして思わずクリックしてしまうと、そこで問題が発生する訳です。スパムメール内のリンクは絶対にクリックしないこと。これにより、スパムメールがもたらすフィッシング攻撃や不正プログラムのダウンロードを防ぐことができます。

8. 怪しげな募金活動には注意すること

現在、多くのボランティア組織は、Eメールを利用して募金活動等を行っています。そのようなメールを受信した場合、確認のためこの募金活動が本当かどうか、該当のボランティア組織に電話するなどして確認することです。「419 詐欺 (ナイジェリアを舞台に Eメールを利用した国際詐欺。ナイジェリア刑法第 419 条の抵触に由来し 419 詐欺と呼ばれる)」等、慈善事業を装って金銭を騙し取る手口のフィッシング詐欺が非常に多くなってきています。

9. 署名活動のメールは転送しないこと

いわゆる“チェーンメール”やオンラインでの署名活動など、こうした活動のほとんどは偽物です。こうした活動に協力しても、結局のところ、スパムメール大量送付用のリスト作成に加担するだけです。残念ながら、この種のメールを受信したユーザは、親しい友人や家族に転送する傾向があり、彼らのメール情報がサイバー犯罪者たちの手に落ちてしまうこととなります。もっとも、こうしたメールは、ほとんどの場合、ユーザに何らかの行動を起こさせることはないようですが、それでも、署名活動等は、転送の際に氏名・住所・メールアドレスを記させる場合もあり、こうした情報は、最終的にスパム送信者たちの手に渡り、彼らのフィッシング活動やその他のインターネット関連の犯罪に利用されることとなります。

10. 業務上の行動指針：ガイドラインの作成と社員教育

どのデータには誰がアクセス可能かなどの社内ポリシーを作成すること。こうして明文化した文書をキーとなる社員に配布し、社内全体で情報漏えい防止を図ることです。企業での情報漏えいは事故で発生することもあります。他方、社員教育を通して重要情報の取り扱い方法の周知を徹底することでも防ぐことはできます。組織内でこうした部分での意識の高めることは、多層的な防御対策を行う上でも非常に重要です。

※ 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/>>