

# セキュリティ最前線 (2009年4月14日号)

## 目次:

- |                               |     |
|-------------------------------|-----|
| 1. “身代金”も要求する偽セキュリティソフト       | P.1 |
| 2. サイバー犯罪の脅威と傾向: 税金関連詐欺の季節    | P.4 |
| 3. セキュリティスポットライト: 税金関連詐欺の見分け方 | P.6 |

## 1. “身代金”も要求する偽セキュリティソフト

### どのような脅威か

新たな手口を駆使する偽セキュリティソフトが現われたようです。サイバー犯罪者たちが偽セキュリティソフトを利用して、コンピュータ内のファイルを使えないようにしてしまうという手口です。これは、偽セキュリティソフトの初期の不正活動に比べると“革新的”な手法ではあり、1つの新たな脅威とも位置づけることができるでしょう。現実世界でも行われる“恐喝行為”をオンラインの世界にも適用し、その狙いは、もちろん現実世界と同じく、ユーザから金をゆすり取るということのようです。

偽セキュリティソフトは、ここ数年間、ユーザたちを苦しめ、多くの被害者たちを生み出してきました。このはた迷惑なソフトウェアは、通常、Web を介してコンピュータに侵入し、様々なソーシャルエンジニアリングの手口を駆使してユーザを騙し、自身をインストールさせます。一度インストールされると、この偽セキュリティソフトは、様々な警告を表示し、使用中のコンピュータに何か(感染等の)問題が発生したのではないかと、ユーザに思わせます。警告の種類は多岐に及び、エラーメッセージや、ダイログボックス、さらには偽の「ブルースクリーン(画面が青くなって操作不能になること)」、「青い壁紙を表示してユーザに(偽の)感染を知らせる」といったものまであります。そしてこの偽セキュリティソフトは、「ウイルススキャンを実施します」、「ウイルスを駆除します」、「不正プログラムを削除します」等のメッセージも表示します。ただし、「このためには、完全バージョンを購入する必要があります」とのメッセージも忘れずに表示し、ユーザに支払いを促すのです。

2009年3月、この偽セキュリティソフトに関し、新たな手口を駆使する“新世代型”の存在が確認されました。この新型は、いわゆる“ランサムウェア”の機能が備わっているようです。ランサムウェアといえば、かつてサイバー犯罪者たちにより次のような手口で利用されていました。感染したコンピュータ内の特定のファイルを暗号化でロックしてしまい、ユーザが開くことができないようにします。こうしてファイルを“人質”にした上で「ロックされたファイルの暗号を解読して開きたければ、金を払え」と身代金(ランサム)を要求するわけです。「“人質”と引き換えに解読キーを提供する」とサイバー犯罪者が通知するのが、この典型的なパターンでした。

トレンドマイクロでは、このランサムウェア型の偽セキュリティソフトを「TROJ\_FAKEALE.BG」(※1)として検出、そしてトレンドマイクロの解析エンジニアにより、2種類の不正活動(恐喝)を行うことが確認されています。偽セキュリティソフトによる“偽感染”だけでなく、ランサムウェアによる“人質ファイル”でも、ユーザを脅すというわけです。

### ランサムウェアの活動

不正プログラムの DLL ファイルが、“マイ ドキュメント”フォルダ内にある次のファイルを暗号化でロックしてしまいます。DOC、DOCM、DOCX、DOTM、DOTX、JPEG、JPG、MDB、MP3、PDF、PNG、POTM、POTX、PPAM、PPSM、PPSX、PPT、PPTM、PPTX、PST、WMA、XLAM、XLS、XLSB、XLSM、XLSX、XLTM、XLTX といった拡張子のファイルタイプです。これらのファイルは、通常、文書や画像、音楽、プレゼンテーション用資料、表計算等に利用され、重要な情報である可能性が高いばかりか、頻繁に使用されるファイルです。これらが暗号化によりロックされてしまうと、ユーザは、もはや関連アプリケーションを利用しても、これらのファイルにアクセスすることが不可能になります。

### 偽セキュリティソフトの活動

不正プログラムの EXE コンポーネントがこの活動を行います。上述の DLL が暗号化によるファイルのロック、「ランサムウェアの活動」を行った後、不正プログラムは、メッセージボックスで(ロックされたファイルを開こうとしているユーザに対して)「このファイルは損傷しているため開くことができません」などと告げます。同じエラーメッセージはタスクバーにも表示されます。さらに「ファイルの修復方法」と称するメッセージがボタンと共に表示され、ユーザがボタンをクリックすると、Web サイトにリダイレクト。そこから「FileFix Professional 2009」と称するソフトウェアが入手できるようになっています。

「FileFix」は、その名称からも想像できるように、損傷したファイルを修復するツールのように見えます。実際、ユーザは、このツールでロックされたファイルを開くことができます。ただし、解読によりロックを解除して開くことができるのは、ファイル1つだけです。この時点でユーザは、「全てのファイルを解読し、ロックを解除するためには、FileFix の有償バージョンをダウンロードしてください」と告げられるわけです。一見、正規の手続きのようですが、ファイルのロックを解除するために 50 ドルを要求するツールなど、胡散臭いと思わすべきでしょう。

さらなる調査によると、この偽セキュリティソフトのホスト先のドメインは、トレンドマイクロが2007年に確認していたクリック詐欺やその他のペイパークリック(Pay-per-click)詐欺にも利用されていたことが判明しました。

また、同じドメインが、「Storm」や「Waledac」ボットネット関連の最近の亜種もホストしていたことが確認されました。こうした事実からも、このドメイン自体が、かなり前から数々のサイバー詐欺に利用されていたことが理解できます。そして今回のような「偽セキュリティソフト・ランサムウェアの組み合わせ」は、オンラインユーザにさらなる新たな脅威をもたらすことを意味します。実際、ユーザは、コンピュータ内に自分で保存している文書ファイルや、画像、音楽ファイル等は何の注意もせずに関開くものです。また、そうしたファイルは、ユーザの個人的な思い出に関するものや、仕事上の重要資料である場合がほとんどであり、それらがいきなり開けなくなれば、感染の危険性などは思い当たらず、とにかく早くファイルを開きたい一心となり、ロック解除のツール(実際はワナ)に金を払うことなど厭わないでしょう。

### どのようなリスクにさらされるか

現在、偽セキュリティソフトの手口は、既にネットユーザの間でもよく知られており、その手口も強く印象付けられています。初期の手口では、何も知らないユーザにウイルス対策ソフトを装って偽の感染警告を知ら

せ、完全版の購入を促しお金を巻き上げるというものでした。今回は、単にコンピュータへのセキュリティで脅すだけではなく、コンピュータ内のファイルを“人質”にとって脅すという意味で、この脅威のリスクが、再び勢いを盛り返した事例だといえます。今回のような被害を受けたユーザは、“ファイルの解読ツール”購入のためにお金をサイバー犯罪者に支払ってしまう羽目に陥ります。またそれにより、新たな被害を招くことにもなるでしょう。サイバー犯罪者たちは、ツールに購入によりお金を巻き上げるだけでなく、支払いの際にユーザが入力した個人情報も収集し、それを闇のフォーラム等で売りさばくからです。

### 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即座に自動的に保護されます。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。デスクトップでは、「ファイルレピュテーション技術」が、ユーザのコンピュータに知らない間にダウンロードされてくる全てのファイルが信頼のおけるものかどうかを検証し、アンチウイルス対策製品により、「TROJ\_FAKEALE.BG」の亜種や、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\_FAKEALE.BG

[http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ\\_FAKEALE.BG](http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEALE.BG)

## 2. サイバー犯罪の脅威と傾向: 税金関連詐欺の季節

どの国でも確定申告の時期に忙しそうにしているのは会計士ですが、どうやら忙しいのは彼らばかりではなく、サイバー犯罪者たちも、収集した社会保障番号などを駆使し、偽の確定申告の送付作業に忙殺されるようです。納税者が本物の確定申告を完了する前に、この作業を完了しなければならないため、サイバー犯罪者たちにとっても、その忙しさも尚更なのでしょう。

### 景気刺激策給付金に関する詐欺

ここ数ヶ月の事例を振り返ってもわかるように、サイバー犯罪者たちは、グローバル経済危機を利用して自分たちの金儲けを行っています。最近の事例では、米国の景気刺激策関連の給付等に関する情報を装ったスパムメールが出回ったところでした。上述の確定申告に関しても、米国の納税者であれば、2008年の確定申告さえ行っていれば何も問題はないはずなのですが、この機会を利用して様々なWebサイトが登場し、政府機関のサイトを装って納税者の手続きをサポートすると見せかけ、詐欺的行為を行うようです。

何も疑わないユーザは、そういった種類のスパムメール内のリンクを安易にクリックし、結果として、サポートが得られるどころか、スパイウェアを受け取る羽目に陥ってしまいます。また別の同じような例では、スパムメール内のリンクをクリックして、さらに複数の不正サイトにリダイレクトされたというケースも報告されています。

こうしてリダイレクトされたサイトでは、たとえば、景気刺激策関連の給付等に関するサポートを装い、アクセスした者に対して、サポートを受けるために、氏名・職業・給与額、銀行の口座情報といった個人情報を入力するように促すのです。こうした個人情報の入力手続きは、あたかも受給資格を質問項目で確認していく作業のように巧妙に行われます。しかし実際は、こうして収集された個人情報は、サイバー犯罪者により、銀行やその他のオンライン金融口座のハッキングに悪用されたり、オンラインの闇マーケットで売り飛ばされたりします。こうした不正サイトの中には、各種の有名ニュースネットワークのロゴを使ったり、オバマ大統領の写真を使ったりして、ユーザに対して「給付金というタダでもらえるお金を早く手に入れよう」などと煽ったりもしています。

「この種の詐欺はこれからも続くだろう、ユーザは十分に気をつける必要がある」と、トレンドマイクロのセキュリティリサーチ・マネージャ、Jamz Yaneza は注意を促しています。そしてさらに、「こうした給付金関連の詐欺は、どんどん増加し、米国やその他の国で確定申告関連の期限が近づくにつれ、ますます増加していくでしょう。こういった詐欺の方法は、犯罪のために個人情報をどうしても必要とするサイバー犯罪たちの強い要求から、当然のようにして発生してきた手口なのでしょう」と説明します。

### 税金関連のフィッシング詐欺

税金関連の詐欺では、フィッシングも主要な手口となります。ユーザを騙し、個人情報を収集する必要があるからです。収集された個人情報は、銀行口座への侵入やクレジットカードの不正利用に使われ、さらに借金や貸付を行う際の名義に利用されたりもします。フィッシング詐欺は、通常、正規の機関からのメールを装い行われます。この場合に利用される正規の機関とは、主に米国の国税庁、IRS (Internal Revenue Service) などです。実際、IRSによると、昨年納税に関してこれまでに3万3000通ものフィッシングメール (IRSからのメールを騙ったメール) が転送されてきており、その種類も1500に達するといえます(※1)。

毎年開催されるBlack Hatセキュリティコンファレンスの2007年度の会議では、米国連邦官による発表があり、その中でそうして政府機関を騙ったフィッシング活動が、2007年だけでも倍々の増加が12回も続いたと報告していました。事実、2003年および2004年に報告された件数は、それぞれ1つずつのフィッシング

サイトだけでしたが、2008年には、IRSが閉鎖させたフィッシングサイトの数は1,630にも及び、その数はまだ増え続けているといわれています(※2)。

### グローバルレベルでの税金関連詐欺

税金関連の詐欺は、むろん米国に限ったことではありません。前述の Jamz Yaneza は、「税金関連の詐欺は、もちろん世界中で発生するものですが、特に件数が多い国としては、電子ファイリングやオンライン銀行といった方法が既に広く利用されている国、例えば、米国、ブラジル、カナダといった国々がそうです」と述べています。

2009年2月、トレンドマイクロの専門家は、オーストリアの納税者を狙ったスパムメールを確認しました。このスパムメールは、オーストラリア税務局(Australian Taxation Office)からを装い、受信者に対して申告を通常よりも早めに行うように促しています。このメール内のリンクをクリックすると、あるフィッシングサイトに導かれ、そこでクレジットカードの名義・番号・有効期限、さらに CVV コードを入力するように指示されます。また、本人の生年月日や住所・旧姓の入力も指示されます。実際、このフィッシングサイトは、検索ボックスやページリンクにいたるまで、オーストラリア納税局の本物そっくりであり、実に巧妙に作成されていたといえます。

さらに2009年3月には、ブラジルの財務省、Ministerio da Fazendaも、フィッシング詐欺の標的となりました。この政府機関からを装ったメールがブラジルの消費者宛に送信され、「あなたの所得税がまだ納められていません」などというメッセージが記されていたそうです。そして「確認のため」と称して、メール受信者はさらにメール内のリンクをクリックするように促されます。が、実際にクリックすると、不正なダウンロードが開始されます。トレンドマイクロの専門家によるさらなる調査では、不正プログラムが複数、ダウンロードされることが確認されています。

このようにどの国に限らず、税金関連の詐欺に関する注意は、グローバルレベルで必要です。「通常、税金関連詐欺のメールは、冷静に見れば怪しいとすぐ分かるはずです」と、Jamz Yanezaも説明します。こういった種類のメールが怪しいを見極めるためにも、日頃から次項目のようなセキュリティ情報を理解しておく必要があります。

注:

※1 "Social Networking Explodes Worldwide as Sites Increase their Focus on Cultural Relevance Facebook and Hi5 More than Double Global Visitor Bases During Past Year," ComScore, August 12, 2008, <http://www.comscore.com/press/release.asp?press=2396>

※2 Robert Lemos, "IRS Taxed by Phishing Attacks," SecurityFocus.com, February 20, 2008, <http://www.securityfocus.com/brief/684>

### 3. セキュリティスポットライト:税金関連詐欺の見分け方

#### 1. 偽物メールや添付ファイルに注意すること

今日、金融関係機関がメールを送りつけるようなことはほとんど皆無と聞いていいでしょう。ですから、金融関係機関からそのようなメールを受信した場合、ほぼ偽物と考えて問題ありません。実際、米国 IRS サイトでも「IRS が納税者と E メールで連絡を取ることはありません」と説明しています。カナダの税務局、CRA (Canada Revenue Agency)も同じ説明を掲載しています。このことは、暗証番号やパスワード、さらには、クレジットカードや口座情報やその他の金融機関の個人情報に関して同じです。こうした情報の連絡に E メールが使用されることはありません。もし仮に税務局と称するところからメールが送られてきて、添付ファイルを開いたりリンクをクリックしたりするように促された場合、そのようなメールは無視することです。添付ファイルには不正コードが含まれており、リンクはフィッシングサイトに飛ばされ個人情報が収集されるというワナがあるに違いありません。もし仮に、納税局があなたの個人情報が必要というのであれば、その場合は、納税局に直接電話をかけることです。

#### 2. Web サイトの URL をチェックすること

多くの不正 Web サイトの URL は、正規 Web サイトのそれに比べて、スペリングが異なっていたり、ドメイン名が違っていたりと、いくつか特徴的な点があります。また偽 URL のいくつかは、不自然に長かったり、該当機関の名称が含まれていなかったりと直ぐに判別できる場合もあります。たとえば、IRS (米国税庁) の場合、この Web サイトの URL は、かならず「<http://www.irs.gov>」で始まります。ただし、もし仮に閲覧しようとしているサイトが正規かどうか判別に迷う場合は、直接その該当機関や会社に連絡してみることです。なお、そのように直接連絡する際も、その(偽物かもしれない)Web サイトに記載されている連絡先は利用しないことです。別の信用のおける場所に記載された連絡先を利用してください。

#### 3. 自分の預金明細や請求書をチェックすること

米連邦取引委員会 (FTC: The U.S. Federal Trade Commission) では、個人情報や銀行情報を盗まれたかもしれないと思う方は、必ず自分の預金明細、クレジットカード明細をしっかりとチェックし、身に覚えのない請求書などないかも確認するようにと注意を促しています。実際、個人情報や銀行情報が盗まれて悪用されていても、そうしたチェックを怠っていたために、数年間も気づかなかったケースもあったといえます。また別の場合では、IRS (米国税庁) から W-2 フォーム (税金の明細書) が届いて初めて気がついたというケースもあったそうです。

#### 4. 怪しいメールに関しては、しかるべき機関に報告すること

もし怪しいメールが届いて被害を受けた場合は、まずは、(悪用された) 正規の機関に報告することです。そうすれば、直ぐに調査を行ってくれます。米国の場合ならば、怪しいメールや怪しい URL が米国税庁 (IRS) を騙っている場合は、本当の米国税庁 (IRS) の宛先である「[phishing@irs.gov](mailto:phishing@irs.gov)」に報告してください。あるいは、米連邦取引委員会 (FTC) 関連の場合は、本当の米連邦取引委員会 (FTC) の Web サイトである「[www.ftc.gov](http://www.ftc.gov)」にて苦情フォームに記入してください。カナダの場合は、そうした苦情は、カナダ王立騎馬警察 (Royal Canadian Mounted Police) の「[info@phonebusters.com](mailto:info@phonebusters.com)」宛になります。オーストラリアの場合は、オーストラリア税務局の「[ReportEmailFraud@ato.gov.au](mailto:ReportEmailFraud@ato.gov.au)」宛になります。

その他の国に関しては、その国の税務局のオンラインサイトからセキュリティや詐欺に関する項目を探して、しかるべき宛先に報告してください。こういったサイトには、フィッシング詐欺等に報告を受ける際の宛先が必ず記されているはずで、怪しいメールを転送する場合は、必ずメールのインターネットヘッダーも含んでください。この箇所には、送信者を特定できる情報が記載されている可能性があります。また、怪しいメールの転送後、その怪しいメールそのものも忘れずに削除しておいてください。

## 5. セキュリティソフトをインストールすること

セキュリティソフトは、ご使用のコンピュータのスキャンを行い、感染の有無を知らせてくれます。シグネチャや定義に基づいたパターンファイルが、既存の不正プログラムやその他の脅威を明らかにしてくれるからです。不正プログラムの作成者は、絶えず新しい不正プログラムを作成して攻撃を繰り返してきます。セキュリティソフトに関しても、絶えず最新の定義をインストールしておくことが重要です。

たとえば、「ウイルスバスター2009」、また企業向けには「ウイルスバスター コーポレートエディション」等は、不正プログラムやスパイウェアの脅威からご使用のコンピュータを守り、安全なインターネット閲覧活動を保証してくれます。

- ※ 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/>>