

2009年11月17日

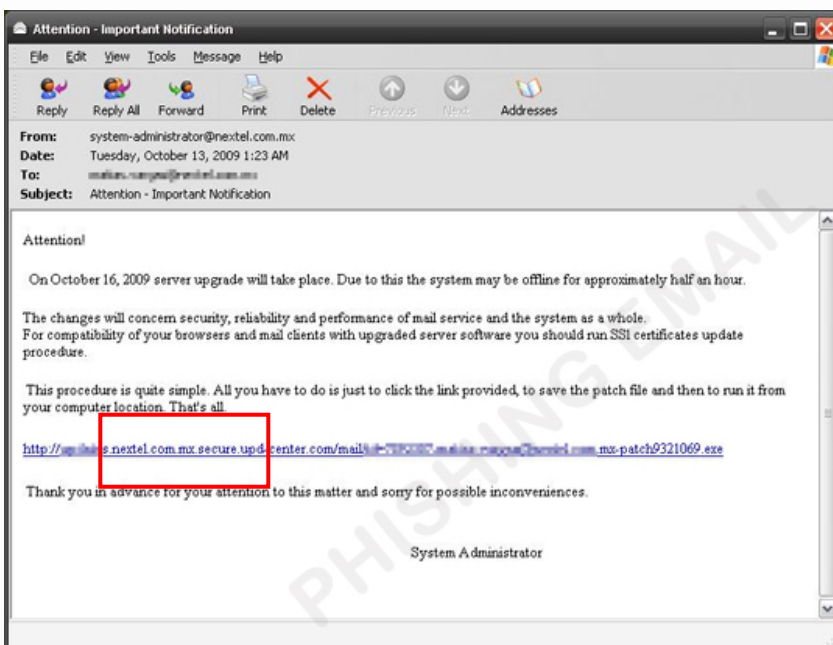
## サブドメインを自在に変化させた URL でボットネットに参加させる

トレンドマイクロのウイルス解析チームは、最近、オーダーメイドのスパムメールを用いる攻撃を確認しました。これらのメールは、特定の企業数社の社員を標的にしています。メール内のリンクをクリックした社員は、「TROJZBOT.CYX」をダウンロードすることになりました。この不正プログラムは、「ZBOT」の亜種で、ユーザのキー入力操作情報を収集し、リモートサーバに送信します。また、「ZBOT」の亜種に感染したコンピュータは、悪名高いボットネット「ZeuS」<sup>(※1)</sup>の一員になってしまいます。

### どのような脅威か

#### つい信用してしまうサブドメインが最新「ZBOT/ZeuS」攻撃の鍵

トレンドマイクロのウイルス解析チームは、複数の企業の社員をランダムに狙ったスパム活動を調査しました。標的となった企業の多くの社員は、社内のシステム管理者から送信されたように見えるお知らせメールを受信しました。メールには、「最近、サーバのソフトウェアが更新されたので、メール内のリンクをクリックし、社員がそれぞれのコンピュータを更新するように」と書かれていました。しかし、それぞれの会社の異なったシステム管理者が送ったはずのメール内のリンクは、同一のIPアドレスに変換されるサブドメインが用いられていました。これらのリンクをクリックすると、「ZBOT」の亜種「TROJ ZBOT.CYX」<sup>(※2)</sup>がユーザのコンピュータにダウンロードされます。



▲画面1 Nextelの社員に送信されたスパムメール。URLにnextelの文字列が入っている

これらの攻撃を分析すると、メール内のリンクが正規で無害であるようにみせかけるために、サブドメインがカスタマイズされていることがわかります。セキュリティに関するコンサルティングを目的としたドイツの第三者機関「BFK」が開発したDNSサーバ再現ツールを用いてテストすると、これらのURLは、危険なファイルをダウンロードさせるURLのドメインの下にある「ワイルドカード化されたサブドメイン」であることが判明しました。

攻撃に使用されているドメインは、サブドメインをワイルドカード化、つまり自由に指定しカスタマイズすることができません。URL内に、自社のドメイン名などが入っているため、ユーザは疑いなくクリックしてしまいがちです。しかし、今回のスパム活動で用いられたドメインがワイルドカード化機能を備えたものであるという事実は、この攻撃の最も重要な特徴ではありません。このスパム活動がもたらす最大の危険は、関連するドメインが、次々に変化し続ける（「Fast-Flux」手法）ボットネット「Avalanch」に組み込まれており、新しいドメインが用いられるたびに即座に様変わりするという事です。それに加え、これらのドメインにはワイルドカード化機能があるため、ある攻撃から次の攻撃へ容易に移行していきます。例えば、1日のうちに何度も標的に合わせてサブドメインをカスタマイズし、セキュリティソフトの偽更新、「Outlook Web Access」の偽更新、そして金融機関が用いるSSLの偽証明書と、



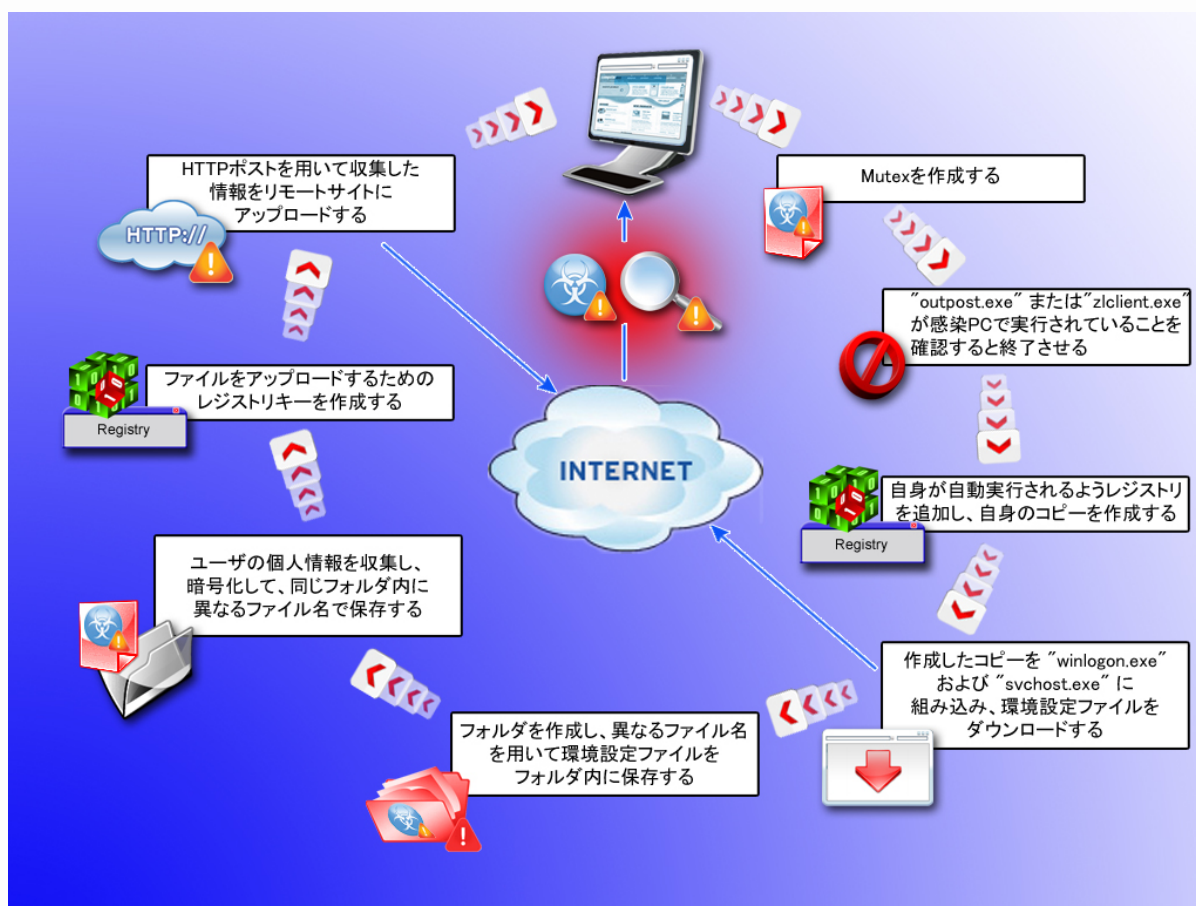
# セキュリティ最前線

「Webからの脅威」の最新事例を毎月2回トレンドラボからお届けします

姿を変え、攻撃を仕掛けることが可能なのです。

画面1のスパムメールのサンプルを見ると、サイバー犯罪者は、危険なURLに対し、サブドメイン「nextel.com.mx.secure」を作成したことがわかります。この攻撃では「Nextel」社が標的であったため、ダウンロードに用いるURLは、Nextelの社員にとって馴染みがあるように見えました。このようなソーシャルエンジニアリングの手口を用い、サイバー犯罪者は、感染を拡大させます。

「TROJ\_ZBOT.CYX」は、実行されると、Webサイトにアクセスし、「どこで自身のコピーのアップデートファイルがダウンロードできるか」、「収集した情報をどこに送信するか」といった情報を含む環境設定ファイルをダウンロードします。このファイルはまた、不正プログラムが情報を収集するために標的とする金融機関関連Webサイトのリストを含みます。



▲図1 「TROJ\_ZBOT.CYX」の動作のサイクル

## 不正プログラム「ZBOT」ファミリーが危険な理由

ボットネット「ZeuS」は、様々なコンポーネントで構成されています。これらのコンポーネントは、トレンドマイクロでは「ZBOT」ファミリーのトロイの木馬型不正プログラムおよびトロイの木馬型スパイウェアの亜種として数か月に渡り検出しています。「ZeuS」は、中小企業を狙ったオンラインバンキング攻撃を仕掛けることでよく知られています。専属のITまたはセキュリティ担当者をもたず、1人か2人で銀行口座や給与口座を担当しているような中小企業が「ZBOT」作成者の標的です。

「ZeuS」の悪評が広まるにつれ、「ZBOT」ファミリーは、これまでで最も危険な情報収集型不正プロ



# セキュリティ最前線

「Webからの脅威」の最新事例を毎月2回トレンドラボからお届けします

グラムと認識されるようになりました。精巧なフィッシングページを簡単に作成できるキット「Rock Phish」<sup>(※3)</sup>を開発したことで知られるサイバー犯罪集団(犯罪組織も「Rock Phish」と呼ばれる)が2009年4月頃始めて「ZBOT」を用い、「Rock Phish」関連のフィッシング攻撃を成功に導きました。「ZBOT」は、通常、メール<sup>(※4)</sup>または脆弱性<sup>(※5)</sup>を用いて感染活動を行います。関連不正ファイルの多くは圧縮されているので、分析の際にコード解読を困難にしています。実際、最新の「ZBOT」は、より複雑になったパッカー(圧縮ツール)を用いて圧縮されています。

「ZBOT」ファミリの不正プログラムは、ルートキット機能を持ち、自身が作成したフォルダやファイルを隠蔽することができます。また、多くの場合、自身のコードをシステムのプロセスに組み込むので、ユーザは、不正なプロセスを容易に終了させることができません。不正プログラムはまた、ファイアウォールおよびセキュリティソフトに関連するプロセスを終了させて自身の検出および削除を避けます。

「ZBOT」は、ユーザの個人情報を収集し、他のサイバー犯罪者に売り渡します。地下経済の調査や公開されているケーススタディなどによると、「ZBOT」は、感染したコンピュータから個人情報を収集し、リモートサーバ(サイバー犯罪者)に送信することで、順調に利益を上げ続けています。「ZBOT」の亜種は、攻撃に利用するソーシャルエンジニアリングの手法を次々と変えることができるために、特に危険な不正プログラムですが、その多様性が目隠しとなり、このファミリが及ぼす被害の全体像は注目されないままです。

## どのようなリスクにさらされるか

「ZBOT」の亜種は、通常、フィッシング詐欺への警戒心が低く、その被害がどれほどであるかを認識していない無防備なユーザを狙います。例えば、今回の攻撃では、サイバー犯罪者は、複数のワイルドカード化したサブドメインを利用し、より多くの無防備なユーザを罠にはめ、不正なリンクをクリックさせました。

それぞれのユーザが受信したスパムメールは、そのユーザが勤める会社のシステム管理者から送られたように見えました。会社名が含まれ、正規を装ったドメインが用いられていたからです(画面1参照)。このため、ユーザがURLをクリック、コンピュータが感染し、結果として、サイバー犯罪者はクレジットカード等の個人情報を入手するという筋書きでした。収集された情報は、不正サーバに送信され、今後の不正活動に利用されたり、地下のオークションに出品されてより高い値段をつけた先に売り渡されたりします。

## トレンドマイクロからのソリューションとアドバイス

**Trend Micro Smart Protection Network (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**クラウド型技術**と**軽量の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。

今回の攻撃では、SPNの**「Webレピュテーション」技術**は、確認された不正なドメインおよびサブドメインにユーザがアクセスする前にブロックすることでユーザを守ります。また、**「ファイルレピュテーション」技術**は、不正ファイル「TROJ\_ZBOT.CYX」を検出し、この不正プログラムがユーザのコンピュータにダウンロードされる前にブロックします。さらに、**「E-mailレピュテーション」技術**は、この攻撃に利用されるスパムメールをブロックします。同様の攻撃がMacユーザを狙った場合でも、トレンドマイクロのMac対象製品がユーザを守ります。

トレンドマイクロ製品のユーザでない場合は、無料サービス「オンラインスキャン」<sup>(※6)</sup>の利用をお勧めします。オンラインスキャンは、ウイルス感染型、トロイの木馬型不正プログラムやワーム、不必要なブラウザプラグインなどを検索し、削除する高性能の人気スキャナです。



# セキュリティ最前線

「Webからの脅威」の最新事例を毎月2回トレンドラボからお届けします

今回の脅威に関するブログ(英語):

<http://blog.trendmicro.com/tailor-made-zbot-spam-campaign-targets-various-companies/>

関連情報

※1 マルウェア感染・侵入 実態は悪化の一途(トレンドマイクロ セキュリティブログ)

<http://blog.trendmicro.co.jp/archives/3089>

3 大危険ボットネットである ZeuS/ZBOT について

※2 TROJ\_ZBOT.CYX ウイルス情報(トレンドマイクロ ウイルスデータベース)

[http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ\\_ZBOT.CYX](http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ_ZBOT.CYX)

※3 Rock Phishers Up the Ante with More ‘Digital Certificates’ (Trend Labs MALWARE BLOG・英語)

<http://blog.trendmicro.com/rock-phishers-up-the-ante-with-more-digital-certificates/>

精巧なフィッシングページを簡単に作成できるキット「Rock Phish」について

※4 マイケル・ジャクソン死因騒動に便乗したスパムメール

<http://blog.trendmicro.co.jp/archives/2966>

マイケル・ジャクソン関連のスパムメールを使用する ZBOT

※5 “Critical Update” Leads to Critical Info Theft (Trend Labs MALWARE BLOG・英語)

<http://blog.trendmicro.com/critical-update-leads-to-critical-info-theft/>

脆弱性を使用する ZBOT

※6 オンラインスキャン

<http://www.trendmicro.co.jp/hcall/>

