

セキュリティ最前線 (2009年2月13日号)

目次:

- | | |
|--------------------------------------|-----|
| 1. 「Waledac」は、新たな「Storm」となるか? | P.1 |
| 2. サイバー犯罪の脅威傾向:バレンタイン詐欺に騙されないために | P.4 |
| 3. セキュリティスポットライト:ボットネットとは何か、なぜ注意すべきか | P.7 |

1. 「Waledac」は、新たな「Storm」となるか?

どのような脅威か

今回の大統領選挙では、バラク・オバマ氏の任命からキャンペーン活動、そして最後の当選まで、そのすべてが歴史的な出来事といえるものでした。が、残念ながら、これらは同時にサイバー犯罪者たちにとっても、ソーシャルエンジニアリングのための絶好の機会でした。オバマ氏に関する偽ニュースは、無防備なユーザを騙すために利用されます。騙されたユーザは、不用意にリンクをクリックし、ファイルのダウンロードや Web サイトの閲覧等を行ってしまうのです。いずれも、不正プログラム感染へとつながります。

オバマ氏の大統領就任式は、数百万の参列者やそれを上回る数の見物人で溢れかえるイベントでしたが、その数日前から、これに便乗したスパムメールも現われていました。メールの内容は、「オバマ氏は大統領就任を拒否する」というもの。こうした内容の様々なバリエーションがスパムメールとして発生し、どのメールにも「この信じがたい、歴史的な大統領就任拒否の詳細はリンク先を参照」といったリンクが貼られてありました。むろん、この種の手口自体は、スパムメールの手法をよく知るユーザからすれば、別に目新しいものではありません。なお、これらのリンクをクリックすると、オバマに関する偽の Web サイトに導かれる仕掛けになっていました。そうした偽サイトのいくつかは、公式のオバマ氏キャンペーンサイトや支持者のサイトとそっくりのものもあったようです。

さほど目新しくない手口でありながら、この脅威がセキュリティ専門家たちの関心を惹いたのは、上述の偽サイトからもたらされるワームが、いずれも、「Waledac」という同一のファミリーによるものだったからです。それらは、「WORM_WALEDAC.KAX」(※1)や「WORM_WALEDAC.AH」(※2)、「WORM_WALEDAC.AL」(※3)といったワームでした。この「Waledac」に関しては、2008年12月から既に、偽電子カードを利用したスパムメールにおいて、その存在が確認されていました。そしてこの「Waledac」による攻撃は、ボットネットの「Storm」に関連したものであると、セキュリティ専門家たちは考えたようです。つまり、「Waledac」とは、新たなサイバー犯罪シンジケートが登場し、そこから発生した全く新種の「Storm」であるか、もしくは、旧来の「Storm」作成者が新たに改良したものを世に送り出したか、いずれかのケースだろうと考えたわけです。というのも、「Storm」と「Waledac」との間には、以下のような特筆すべき類似点が見られるからです。

- 双方ともファストフラックス (fast-flux) によるネットワークを用いている点。ファストフラックスとは、ドメインやネームサーバを次々と変えていくことにより、プロキシとして活動するホスト・ネットワークが絶えず変化する中、不正プログラムの活動を隠ぺいしようとする手法です。
- 「Storm」は、通常、休暇や祝日の出来事を利用した偽電子カードを用いる攻撃で知られていますが、この「Waledac」も、その作成者は、昨年12月の偽電子カードスパムメールに始まり、同様の手口を新年やバレンタインデー関連の不正活動にも用いているようです。
- 「Storm」と「Waledac」の双方とも、関連する不正プログラムは、自身を拡散させる機能を備えています。いずれの場合も、ひとたび感染すると、スパムメール送信用ボットとして外部から不正リモートユーザにより操作されるようになります。この点、双方とも次の手順で特徴的です。つまり、まず感染したコンピュータ内の複数のシステムドライブを検索し、メールアドレスが含まれたファイルを見つけ、そこからメールアドレスを収集します。そして収集した情報をファイルに保存し、そのファイルを暗号化します。暗号化されたファイルは、世界中に分散した複数の IP アドレス宛に HTTP ポストを介して送信します。また、双方とも、ランダムなポートを開き、外部の不正リモートユーザからのコマンドも待機します。

「Waledac」は「Storm」であるという認識は、上記のとおり、複数の解析結果や関連不正プログラムの動作・活動等から判断されたものです。また、「Storm」で使用されていた IP アドレスの多くが、現在は「Waledac」にも使用されているという点にも着目すべきでしょう。

実際、この2つが深く関連しているものであるならば、「Waledac」とは、「Storm」の新種、もしくは「Storm」が大幅にアップグレードしたものと考えべきでしょう。「Waledac」は、次の2点で「Storm」が改良されたものだといえます。1つは、「Waledac」がP2Pネットワークではなく、HTTPを利用している点です。「Storm」の場合、このP2Pの利用を手がかりにして検知していましたが、「Waledac」は、HTTPを利用しているため、この点でより巧妙に自身の動作や活動を隠ぺいすることができます。もう1つは、「Waledac」も、「Storm」と同様、ボット同士の通信を暗号化により隠ぺいしますが、「Waledac」の暗号化システムの方が「Storm」よりも性能が向上しているという点です。旧来の暗号化システムは、セキュリティ専門家でも簡単に解読することが可能でした。

どのようなリスクにさらされるか

今回の事例で感染数が最も多かったのは、北米地域、特にアメリカ合衆国でした。これは、不正なオバマ関連サイトがからんでいる点、当然といえるでしょう。また、感染数が多かった国の第2位に日本があがっている点も、興味深いといえます。これは、バラク・オバマ大統領がいかに“グローバルな人物”であり、彼に関することなら何でも、グローバルな影響を及ぼす可能性があることを雄弁に物語っているともいえるでしょう。オバマ関連の不正プログラムといえば、今のところ、「Waledac」による大規模な“キャンペーン”という様相を呈しています。このボットネットは、既に10,000台とも言われるゾンビPCによるネットワークを形成し、その数はさらに増加する勢いです。クリスマスや新年に続き、バレンタインデーを利用したスパムメール活動も既に始まっているようです。これらの出来事を利用した偽電子カードの手口は、上述のオバマ関連の手口ほどのインパクトは及ぼさないでしょう。ただ、かつての「Storm」の“キャンペーン”と同様、こうした攻撃が続くことで、無垢なコンピュータがどんどん“ロボット”に変えられていき、不正なネットワークが形成されていきます。季節の出来事や話題を利用したスパムメールが送信され、クリックを促されたユーザたちは、少しずつ「Waledac」ボットネットのメンバーへとになってしまうのです。

ボットネットの一部となってしまうと、事実上、ユーザは自分のコンピュータのコントロールをボットマスターに明け渡したことになります。ボットマスターは、こうしてコントロールを奪い取ったコンピュータを操作し、不正活動を行うわけです。この時点で行われる不正活動は様々であり、スパムメールの送信から、新たな感染対象のコンピュータ取得、(DoS攻撃やDDoS攻撃、EDOS攻撃といった)各種のサービス拒否攻撃、さら

には、サイバー犯罪のための情報収集活動やフィッシング活動にまで至ります。

トレンドマイクロからのソリューションとアドバイス

SPN(Smart Protection Network)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。「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。「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ます。SPN は、これら技術を連携(コリレーション)させることで、すべてのエントリーポイントを防御し、ボットネットが勢力を拡大しようとする活動も阻止することができます。不正なメールは、もはやインボックスにも至らず、危険と判断された IP アドレスも事前にブロックされ、さらに不正なファイルも事前に検知され、ファイル実行が阻止されるわけです。デスクトップでは、アンチウイルス対策製品により、「WORM_WALEDAC」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 WORM_WALEDAC.KAX

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_WALEDAC.KAX

※2 WORM_WALEDAC.AH

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_WALEDAC.AH

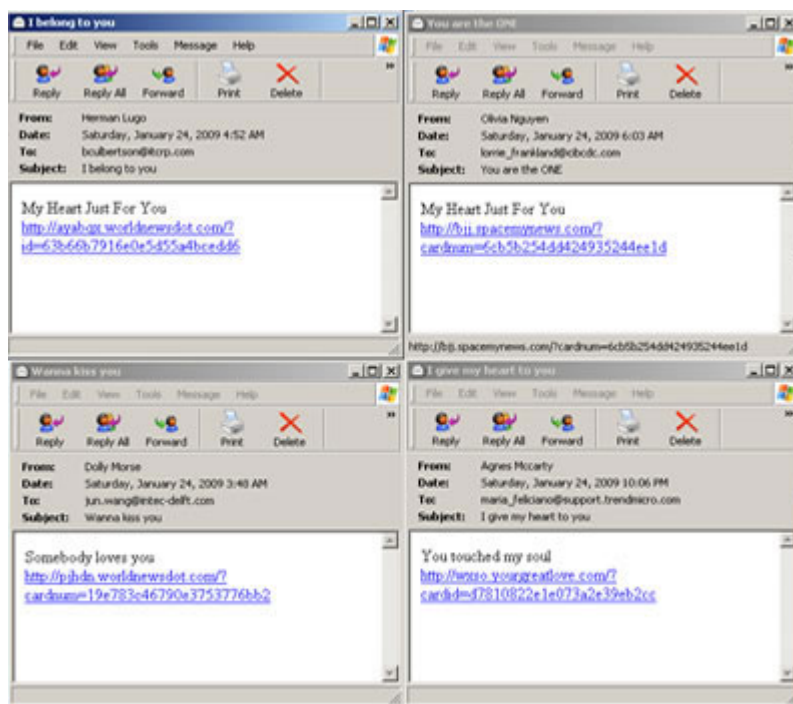
※3 WORM_WALEDAC.AL

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_WALEDAC.AL

2. サイバー犯罪の脅威傾向：バレンタイン詐欺に騙されないために

ワームがもたらす恋愛事情

「私の心を受けてください(I give my heart to you)」、「キスさせて(Wanna Kiss You)」、「あなたこそ、理想の人(You are the ONE)」等、最近のスパムメールの件名は、何かと刺激的でワクワクさせてくれるものばかりのようです。「いったい誰がそんなに私のことを想ってくれているのだろう」という好奇心がわいても不思議ではありませんが、そうした浮ついたユーザに対して、トレンドマイクロのウイルス解析技術者たちは「そのようなメールは絶対に開いてはいけない」と、きっぱり警告しています。もし開いてしまったら、「Waledac」という名の“かわいいワーム”に感染し、“危険な恋”におちてしまうことでしょう。



バレンタインの挨拶を装ったメール

ただし、このワームが本当に“恋している”のは、あなたではなく、スパムメールを介した大量感染活動なのです。「Storm」と同様、「Waledac」も、休日や祝日の出来事に便乗し、数週間も前からそれに乗じたスパムメールの送信を行っています。こうして、バレンタインデーに関しても、既に“ロマンチック”なメールがユーザの受信トレイに溢れて始めているわけです。この場合、どのスパムメールにも、「誰かがあなたに恋している(Somebody loves you)」や「私の気持ちを受け取って(My heart just for you)」などと、危険な誘惑に満ちたメッセージが含まれています。そしてそのようなメール内のリンクをユーザがクリックしてしまうと(むろん不正なリンクなわけですが)、浮ついたユーザは、別のサイトにリダイレクトされてしまいます。このリダイレクト先のサイト内にあるリンクをクリックすると、「WORM_WALEDAC.AR」(※1)として検出される不正なファイルのダウンロードされてしまうわけです。このワームは、他の「Waledac」の亜種と同様、感染したコンピュータのセキュリティを脅かします。ワームは、ランダムなポートを開き、サードパーティからのコマンドを待機します。このサードパーティが、ボットネットを操作者であると考えられています。

愛の嵐(Storm)を巻き起こす

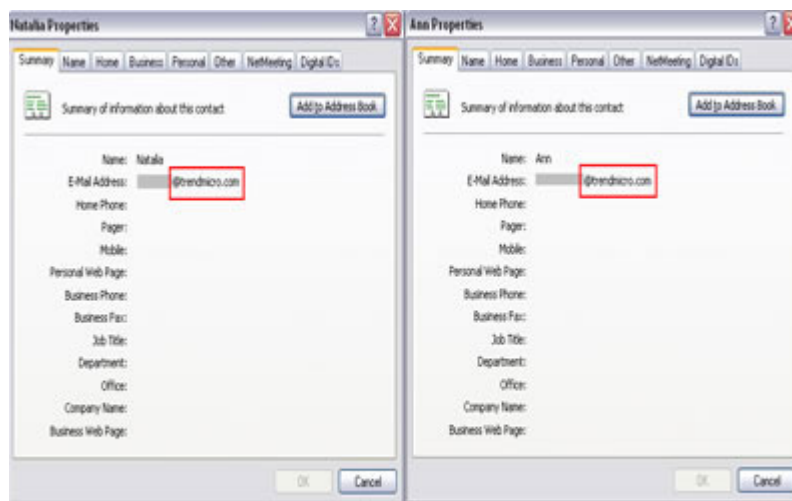
実際、セキュリティ専門家の説明によると、「Waledac」は、ボットネットの「Storm」によく似ているといえます。この「Storm」は、2007年から2008年にかけてユーザを悩ましたボットネットとして有名ですが、「Waledac」フ

アメリカも、「Storm」と非常によく似た特徴や動作を示しているのです。とりわけ、バレンタインデーなどのイベントに便乗してスパムメールを送信する手口などがそうです。

「Storm」は、巧妙なソーシャルエンジニアリングの手口を使用することでもよく知られており、その手口は、特に休日や祝日の出来事をテーマにしてユーザを騙そうとするものでした。他にも、ファストフラックス (fast-flux) という攻撃方法でも、「Storm」と「Waledac」は似ています。これは、DNS を次々に変えていき、不正なサイトの検出を逃れようとする手法です。また、「Waledac」は、1 つのドメインに複数のサーバ名を使用します。これも、「Storm」と同じ手口です。さらに「Waledac」は、“ecard.exe”や“postcard.exe”といった「Storm」と同一のファイル名も使用しています。場合によっては、偽のアンチスパイウェア製品を騙しの手口としてインストールしますが、これも双方に共通する特徴です。

出会い系スパムメールの増加

「Waledac」によるスパムメールの他に、ユーザの“恋愛願望”につけ込んだいわゆる「出会い系スパムメール」も増加傾向にあります。こうした「出会い系スパムメール」の中には非常にユニークなものがあり、驚くべきことにトレンドマイクロからの誘いを装ったメールさえ確認されました。こうしたメールは、メール内の「From」の欄を操作し、スパムメールのファイルタリングを逃れます。また、スパムメール送信には、“辞書攻撃”という手口が使用されます。この手法は、特に一定のドメインからランダムに大量送信する際に用いられます。簡単な文字列を(まさに辞書のように)どんどん組み合わせながら言葉をつくり、こうして大量に作り出された言葉の中に実際のメールアドレスに使用されているものもあるに違いないという予想から送信が行われます。作り出されたメールアドレスが有効か無効かは、送信エラーの発生や実際の返信等で確認し、有効とみなされスパムメール送信者のリストに追加することになります。こうして追加されたメールアドレスは、さらなるスパムメール活動にも利用されることになるという仕掛けです。



トレンドマイクロ関連のメールを装ったスパムメール

ただしここに予想外の展開であることがトレンドマイクロのウイルス解析技術者にも確認されています。この展開は、ある意味、滑稽とさえ言うてよいでしょう。ここでは「From」の欄が偽装されているため、実際にスパムメールを受信したユーザが返信しても、または送信エラーが発生しても、本来の送信者(スパムメール送信者)に戻ってこないというのです。彼らスパムメール送信者にとっては、とんだ無駄骨というわけです。

バレンタインという恋愛のシーズン、こうした脅威から身を守るためには、フィッシング詐欺や、不正な電子グリーティングカード、出会い系サイトの偽プロフィール等に対して、十分に気をつける必要があります。フィッシング詐欺では、たとえば、恋人に花束やチョコレートを贈ったあなたを狙って、「ご注文の品が未配達となっています。ご確認のため、お客様のクレジットカード情報をご入力ください」というメールが舞い

込むかもしれません。また、電子グリーティングカードを受信した場合も、カードを見るために最新のマルチメディアプレーヤーのダウンロードが必要と指示され、実際にダウンロードしてみると、マルチメディアプレーヤーではなく、不正プログラムが入手できた、などということも起こりかねません。さらには、出会い系サイトでめぐり合った相手からは、“真実の恋愛”ならぬ、“深刻な脅威”がもたらされることもあるでしょう。もっとひどい場合は、出会い系サイトでめぐり合った“偽の恋人”と実際に会うこととなり、この架空の“偽恋人”があなたのもとに来るための航空券が必要、それをあなたが負担、などという羽目に陥るかもしれません。こうしたワナにはまらないためにも、ユーザたちは、メールを開けるときも、URL をクリックするときも、何らかのファイルをダウンロードするときも、浮ついた心ではなく、しっかりと冷静に頭を使うべきなのです。

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 WORM_WALEDAC.AR

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_WALEDAC.AR

3. セキュリティスポットライト：ボットネットとは何か、なぜ注意すべきか

ボットネットとは何か？ ボットネットとは、感染してボットと化したコンピュータの集合体のことです。そしてボットとは、不正なソフトウェアプログラムのことであり、これにより感染したコンピュータは、外部から不正にコントロールすることが可能になります。このように感染したコンピュータのことは、“ゾンビ PC”とも呼ばれます。ホラー映画のゾンビのように、誰かにコントロールされるだけの存在になりさがったことから付けられた名称のようです。またこの場合、外部から不正にコントロールする者(ボットネットを運営するサイバー犯罪者)は、ボットマスターとも呼ばれます。

ボットネットは、いわば、サイバー犯罪者たちの“兵器庫”であり、また、何よりも大量のスパムメール送信に利用される重要なツールなのです。ボットマスターたちは、自分たちのボットネットを別のサイバー犯罪者たちに貸し出しする場合があります。ボットネットを借りたサイバー犯罪者たちは、これを用いて、偽の薬局商品を売るスパムメールの送信や、不正プログラムやスパイウェアがダウンロードされるリンクがあるスパムメールの送信も行います。リンク先からは情報収集型の不正プログラムやスパイウェアがもたらされ、受信者の個人情報収集される仕掛けになっています。ボットマスターたちは、自分たちのボットネットを増殖させる際にもスパムメールを利用します。つまり、自分のボットネットを用いてスパムメールを送信し、そのスパムメールの添付やリンクからは、ボット作成型の不正プログラムがもたらされ、感染したコンピュータが次々にボットとなるといわけです。

今日、よく知られた巨大ボットネットとしては、「Storm」や「Rustock」、「Sribi」、「Kraken」、「Mega-D」、「Bobax」などがあります。いずれも、数千のボットにさらに数千のボットがつながった巨大ネットワークを誇っています。

なぜ注意すべきか？ 上述のとおり、バレンタインデーは、サイバー犯罪者たちにとっても、格好の“素敵な機会”だからです。彼らは、電子グリーティングカードのスパムメール、出会い系サイト関連のスパムメール、配達物の確認を装ったスパムメール、その他の様々な正規メールを装い、人々が浮き足立つこの時期、ユーザの目の前にひょっこりと現われるかもしれません。個人情報や貯金なりを失いたくなかったら十分に注意することです。

個人ユーザも企業も、こういった脅威から身を守るためには、オンラインのセキュリティを正しく実行する必要があります。これにより、1) スパムメールの受信、2) 受信したスパムメール内の不正リンクのクリック、3) そしてクリックすることでもたらされる不正プログラムやスパイウェアからの脅威を確実に阻止することができます。

※ 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:「*FL.O.D. Threat Watch Newsletter Signup*」(英語)
<<http://us.trendmicro.com/us/newsletter/>>