ここで紹介しているスパイウェアに関する情報は、japan.internet.com にて Web テクノロジーで連載中のコラムです。

タイトル:スパイウェアの定義

はじめに

“スパイウェア”という言葉をよく、インターネット上で製品や技術、特にセキュリティの分野で見る機会が多くなった思います。

多くの人とスパイウェアについて語るうち、私自身“スパイウェア”という言葉がある意味において、ウィルスという従来の概念を、技術的にもまた社会現象的にも超えたものであると理解するようになってきました。スパイウェアについての見解を説明しながら、そうした目に見えない部分についても紹介できればよいと思います。

まず最初に、“スパイウェア”の定義について説明したいと思います。

説明の中で聞きなれない用語などもありますが、スパイウェアガイドを参照してください。

狭義のスパイウェアと広義のスパイウェア

スパイウェアという用語は、よく知られているように曖昧な用語です。従って、それを使う場合には、必ずそれが狭義のスパイウェアなのか広義のスパイウェアなのかを、お互いに意識しておく必要があります。

スパイ ソフトウェア

では狭義のスパイウェアとは何か？　狭義のスパイウェアとは、スパイ行為をするソフトウェアということになります。単にスパイ行為をするソフトウェアと言っても、多くの種類や方法が存在します。例えば、キーロガー、バックアドア、リモートアクセスの機能を持つソフトウェアなどがその代表的なものです。これらのソフトウェアでは、ユーザーの操作記録を盗んだり、遠隔地からコンピュータを操作することができます。

スパイウェアの定義が立場によって違ってくる論点の一つの例として、広義のスパイウェアに含まれる、広告を目的としたソフトウェア、“アドウェア’”呼ばれるソフトウェアをスパイウェアなのかどうかがあります。

アドウェアとは、一般にポップアップ広告を表示することを目的としたソフトウェアです。つまり、アドウェアだからスパイウェアではないという主張なのです。ある意味正しいようですが、こうした論争になると、間

違った理解や定義になってしまうことに気づかれると思います。

実際スパイウェアをスパイウェア、アドウェア、パラサイトウェアなどと機能を基づいて分類することができます。しかし、アドウェアだから脅威は無いとは言えません。純粋にアドウェア機能のみを持つソフトウェアであればセキュリティへの脅威は少ないといえますが、多くの悪意を持ったスパイウェアは、例えばアドウェア機能とバックドア機能と共に持っているなどと、複合化されていることを無視しています。

そのため、アドウェアとして分類可能なソフトウェアも、その危険度を考えるとさまざまにレベル分けされます。実際、アドウェアと呼ばれるソフトウェアでもさまざまの技術が利用されているからです。

アドウェア

アドウェアを代表する手法として、ブラウザヘルパーオブジェクトとして IE にインストールされ、検索キーワードを他のサイトにリダイレクトし、関連した商品の広告や、購入サイトへのリンクを表示したり、関連商品のポップアップ広告を表示するものがあります。

多くの場合、IE の開始ページや検索ページ、さらにお気に入りにリンクを追加します。

これらはまた、高速検索機能としてうたったものもあります。検索キーワードは、固有の識別子（IP アドレス）とともに、その制御サーバーに送られます。

IP アドレスから個人情報に関連つけることは困難ですが、インストール時にそうした情報を入力するような仕組みを持つことで、簡単に可能になります。

悪意のあるものは、ブラウザ ハイジャックやポップアップを利用して、ユーザーを特定の Web ページに巧妙に誘導します。悪意のある Web ページを開くと、非常に危険なことが予想されます。

例えば、開いたと同時に Active-X ドライブバイダウンロードとばれる方法で、ソフトウェアをユーザーに見えないうちにインストールしたりします。常にインターネット接続を経由して、制御サーバーから新しい広告（ユーザーの嗜好に合わせた）を表示する機能を有したものもあります。

また、アップデータと呼ばれる機能を有しているものは、インターネットに接続できる環境で、自分自身を制御サーバーから常にアップデートしたり、他のソフトウェアをダウンロードしたりすることもできます。

実はスパイウェアの脅威とは、こうした技術や手法を複数組み合わせた攻撃が簡単にできてしまうことにあります。これらスパイウェアは、侵入時点では直接悪意を持ったソフトウェアとして振舞うことはなく、単

にバックアドア、トロイの木馬として機能します。この時点では、まだユーザーには、何かが起きていることは分かりません。

スパイウェアの定義

こうした、アドウェアの技術を利用した悪意のあるソフトウェアも存在することが理解できれば、単にアドウェアはスパイウェアではない、という論争が無意味なことが分かると思います。

では、広義のスパイウェアとはなにか？　広義のスパイウェアは、その機能からではなく、むしろユーザーの視点で、それがどんな行為をするかという観点から、以下の 3 つで定義します。

●ユーザーが知らない間にインストールしたり、ユーザーの知らない（認知しない、または承諾しない）行動をするソフトウェア
●ユーザーの情報をユーザーの知らない間に、外部に送信するソフトウェア
●インストール後、容易にアンインストールや削除ができないソフトウェア

参考までに、このような定義を用いることになった資料を紹介します。2004 年春に開催された FTC（米国 Federal Trade Commission）主催のスパイウェアワークショップでの議論をまとめた、2005 年春の報告書です。

『FTC 2004 年スパイウェアワークショップ報告』

ぜひ、多くの関係者に参考にしていただきたいと思います。

このワークショップの内容については、弊社とパートナシップを持つ Xblock Systems 社の CEO、Wayne Porter もアンチスパイウェア ベンダーのパネラーとして参加していたため、私自身その内容について直接訊いたりしていました。報告書となって発表されている内容は非常に興味のあるものなので、翻訳を紹介しています。そちらも参考してください。

第 2 回

スパイウェアはウィルスより複雑

要約

アンチウィルス ソフトウェアでは世界中どこでもどんな環境でも同一のシグネチャファイルで望まれないプログラムを検出できるが、アンチスパイウェアではそれができない。

シグネチャファイル

スパイウェアの定義が困難な理由のもう一つの側面として、使われている場所、人によってそれがスパイウェアになったり、管理ソフトウェアになったりすることです。例えば、高いセキュリティ レベルの要求されるオフォス環境では、誰が、どのコンピュータから、いつ何をアクセスしたかの記録を残す目的で、キーロガー機能を持つソフトウェア(商用リモート管理ソフトウェア)を導入している場合があります。一方同じソフトウェアが、家庭内のコンピュータや、そうした監視を行っていないオフィス環境で見つかったとしたら、それは除去すべきソフトウェアということになるからです。

前回紹介したスパイウェアの定義の1番目を、**”認知しない行為をするソフトウェア”**としているのもこうした理由からです。もはやスパイウェアは機能から定義することができないということです。

つまり、アンチウィルス ソフトウェアのように、世界中どこでもどんな環境でも同一のシグネチャファイル(ワクチンファイル)を利用して望まれないプログラムを検出する方法が、アンチスパイウェアでは利用することができず、環境や利用者に応じたシグネチャ ファイルを準備する必要があるということになります。

シグネチャファイルの質?

シグネチャファイルは、アンチウィルス ソフトウェアでいうワクチンファイルなどのような役割をします。アンチウィルスの業界ではシグネチャをワクチン、アンチウィルス ソフトウェアを注射器というように、非常に理解しやすい呼び方をしています。そしてアンチウィルス ベンダは、より多くのワクチンをより早く提供できるかで品質を競い合ってきました。

しかしアンチスパイウェアで利用されるシグネチャファイルは、ワクチンという位置づけとは少し違っているように思われます。第一に、あるスパイウェア モジュールに関する情報は、パターンマッチングによるファイルを検出するためのパターン情報だけではなく、それがインストールされた状態でどのように痕跡(フットプリント)を残しているかに関する情報や除去のための情報など、ひとつのスパイウェアに対して多角的な情報を定義しています。そしてそれらがひとつのスパイウェアに対して複数準備されます。複数準備されるのは、各種のソフトウェアにバンドルされているスパイウェアの場合、インストールの痕跡がそれぞれ存在することになるからです。これらの情報によって検出、除去が行われることになるため、シグ

ネチャファイルは単なるデータの情報と言うよりも、スパイウェア検出や除去のためのスクリプト、またはエンジンの役割を果たすことになります。

このようにスパイウェアに見られる新しい脅威を検出、除去するためには、シグネチャファイルもそのように対応、進化が必要になっているのだと思われます。

EULA (ソフトウェア使用許諾書)

"ユーザの知らないうちにインストールしたり、認知しない行為をするソフトウェア"に関連して、EULA に記述しているから、していないから、スパイウェアではない、などという説明もありますが、これらは作成者/配布元の言い分でしかありません。これに反論する意見としては、ユーザーが子供だった場合、EULA を読んだとしても理解することはできない、外国語で記述されている EULA を正しく理解するのは困難である、などの理由で、EULA への'同意'は事実上'同意'ではないと考えるほうが現実的だと思われます。

しかし、これはソフトウェアの提供者側からすると、ユーザーがソフトウェアの機能を理解した上でソフトウェアをインストールしたかどうかを確認するための重要な手順でもあります。
EULA や、アプリケーションの説明を無視してインストールすることで結果的に被害に遭ってしまうことを考えれば、ユーザーはやはり読むべきではないかと考えます。冗談のような技術として、この EULA を読み込んで解析し、スパイウェアの危険性を通知する仕組みも導入されつつあります。また、ユーザーの許可した以外の行為がアプリケーションにより実行された場合に、感知して警告を表示するようオペレーティングシステムを機能強化する要望などもあります。
実際こうした不明な EULA を利用してユーザーがアプリケーションのインストールを承諾した場合、悪意のあるソフトウェアはさらにアンインストールを困難にしていることがあります。つまり、ユーザーが利用を停止しようとしてもそれを困難にする手法です。
後で紹介しますが、SPY ACT(H.R.29)法案では、なんらかの情報収集を行うプログラムでは、通知や開示方法を明確に行うよう勧告しています。

アンインストール

例えば、アンインストール用のプログラムやアンインストールのためのエントリをプログラムの追加と削除に準備していたとしても、完全にファイルを除去するのではなく、先のアップデータ機能部分をプロセスとして、または BHO やスタートアップ エントリに残したままにして、次回コンピュータの起動時や、ブラウザの起動時に設定やファイルを自動的に復元する手法が使われます。このようなスパイウェアの攻撃をうけてしまうと、そのコンピュータはほとんど乗っ取られた状態になってしまいます。
アンインストールを困難にする手法として、ステルスモードという手法があります。実行そのものを隠してしまうことです。ファイルが実行されていることを分からなくしています。ユーザー インターフェイスを持た

ないウィンドウ プロセスとして実行する方法が利用されます。

情報の外部流出

ユーザーの情報をユーザーの知らない間に外部に送信するソフトウェアでは、さまざまな方法で収集したデータを外部に送信します。収集する対象として、アドレス帳などのファイル、実行中のアプリケーションのタイトル名やスクリーンショット、キーロガーの保存したログファイルがあります。これらの情報をユーザーのメールクライアントを利用したり、自身の SMTP プロトコルを利用してあらかじめ設定したメール アドレスに送信したり、HTTP POST、FTP サーバーに送信する手法があります。これらの送信された情報を元に、スパイ(悪意を持った侵入者)は、被害者となるユーザーがいつどのアプリケーションのどの画面に何を入力したかをそのまま再現できることになります。

スパイウェアは、好ましくないソフトウェア

スパイウェアを定義する場合、単に機能からそれをスパイウェアと呼ぶことが困難なほど、多くの方法が同時に使われていることが理解できたと思います。用語としてのスパイウェアは、もはや元のスパイ ソフトウェアの意味でなく、いわゆるユーザーにとって好ましくないソフトウェアの総称として使うべきではないかと思います。

悪意のあるソフトウェアを総称してマルウェアという呼び方もありますが、ここでは、悪意のあるなしに係わらず不必要という意味も含め、または好ましくないものとしてスパイウェアという用語を利用しています。また好ましくない、不要などの判断はユーザーに委ねられることになります。
今後、ソフトウェアは自分自身がスパイウェアでないことの証明として、ユーザーがそれを不要と考えた場合、完全にアンインストールできることが要求されるようになるでしょう。
しかし、ユーザーは、不要な場合にアンインストールできるからと言って決して安心はできません。正統なソフトウェアは、完全なアンインストール機能を提供しますが、悪意を持ったソフトウェアは、こうした基準は守ってはくれません。
スパイウェアの定義として 3 つ目にあげた、**インストール後、容易にアンインストールや削除ができないソフトウェア** には、こうした理由があります。

スパイウェアはソフトウェアだけでない

ここで思い出したことがあります。スパイウェアをソフトウェアとして限定するのも、正しい認識ではありません。例えば、キーロガーでは、市販されているハードウェア タイプのキーロガーが存在します。キーボードとコネクタ間に接続したり、USB としてコンピュータに接続することで、キーボードの信号や入力データを記録するものです。これらハードウェア タイプのキーロガーは、現在のアンチスパイウェア ソフトウェアでは検出することはできません。

経済活動におけるシステムの進化とスパイウェア

そもそもスパイウェアが爆発的に増加したのは、P2P，マルチメディア、ツールバーに代表されるフリーソフトウェアへのバンドルです。近年におけるインターネットを利用した経済活動の発展の結果、ソフトウェア開発者がそのソフトウェアをライセンスする代償としてユーザーからソフトウェアの代金を徴収するよりも、広告代理店と契約し、広告のためのソフトウェア（アドウェア）をバンドルすることで、広告の表示回数や、クリック課金などのシステムにより直接広告代理店から徴収する方式が確立されました。ソフトウェアの作成者は、無料にすることでユーザーに利用される機会を増やすことができ、かつ確実に報酬が回収でき、それを次の開発に投資できます。利用するユーザー側も優秀なソフトウェアを無料で利用することができます。広告会社は各分野のソフトウェアを新しい広告媒体として利用し、投資することになります。このような方式は、ソフトウェアの開発、販売方法としては、シェアウェア(TBYB － Try Before You Buy）（参考文献: http://www.shareedge.com/public/article/WhatIsShareware.htm)と云う方式に続く、画期的な方法であるといえます。

しかし、この方法が短期間の間に乱用された結果、アドウェアにスパイウェアという悪いレッテルが貼られてしまったことは残念なことです。
また、インターネットを利用した経済活動システムをささえるアフィリエイト システムを狙ったものとして、ロイアリティウェアと分類されるアフィリエイト紹介料を横取りする目的のものも存在します。

そして、ダイヤラーと分類されるスパイウェアでは、ダイアルアップ接続をユーザーが知らない間に高額レートの回線を利用するように変更され、高額な請求が発生するような悪質なものも存在します。

同時に、用語としての”スパイウェア”は、DoubleClick 社のような Web 広告会社がデータマイニングを目的とした追跡クッキー技術を乱用してプライバシーを侵害する危険性があることから注目され、そこからスパイウェアへの関心が増大しました。
クッキーにつては、後ほどもう少し詳しく説明してみたいとおもいます。
スパイウェアの周囲には、最新のオペレーティング システム、インターネット、およびプログラミングの技術の進化だけでなく、アドウェアやロイヤリティウェアのようにインターネットを利用した経済活動システムの進化もあり、これらにも関係があることを注目すると、より理解し易くなるのではないでしょうか。

第三回

スパイウェアによって何が起こるか？

要約

スパイウェアにより被害をセキュリティへの侵害と、コンピュータへの障害の 2 つに分類しましたが、ここではもう少し詳しくその被害について説明します。

スパイウェアの脅威について議論する場合、スパイウェアが何をするかについて知っている必要があります。スパイウェア = アドウェア として捉えている人にとってスパイウェアは単に広告ツールとしか捉えられません。しかしここではスパイウェアの定義で説明したように、広義のスパイウェアが何をするか？ということを説明したいと思います。スパイウェアによって起こる問題として大きく 2 つに分けられます、ひとつは、セキュリティの侵害、もうひとつはパフォーマンスの低下、システムが不安定になったり、ハイジャッカなどのために操作が困難になるなどのコンピュータへの問題があります。

スパイウェアの存在を理解することを難しくしているのは、コンピュータにある問題が発生した場合、その現象が特定のスパイウェアで原因あることに気が付かないことが多いからです。
当然、スパイウェアのことについて知らない人にとっては問題の原因がスパイウェアであると考えるのは困難です。
例えば、アンチウィルス ソフトウェアがインストールされているにもかかわらず、コンピュータがウィルスに完全に汚染されるという報告があります。これはウィルスソフトウェアが検知できなかったことが原因でしょうか? またはそれが新種のウィルスだったためでしょうか?

セキュリティ ソフトウェアへの攻撃

スパイウェアによっては(トロイの木馬機能を持つソフトウェアなどで多く見られます)、セキュリティ ソフトウェアを攻撃するものがあります。一旦これが実行されると、コンピュータ上で実行されているセキュリティ ソフトウェア、例えばアンチウィルス ソフトウェアやファイヤウォールのプロセスの停止を試みます。また最近では、アンチスパイウェア ソフトウェアを攻撃するものがあります。特に有名なのは、Spector http://www.shareedge.com/spywareguide/product_show.php?id=20 と呼ばれるスパイウェアです。こうしたセキュリティ ソフトウェアを攻撃するスパイウェアは、さまざまな方法で実行されているセキュリティ ソフトウェアを妨害しようとします。例えば簡単にプロセスの停止を試みるものもあれば、さらにユーザーに偽のシステムエラー ダイアログ ボックスを表示し、セキュリティ ソフトウェアの問題のためのエラーである趣旨のメッセージを表示し、ユーザーにセキュリティ ソフトウェアを一旦停止するように促すものまで、

手法はさまざまです。一旦、アンチウィルスなどのセキュリティ ソフトウェアが停止されると後は何が起こるかわかりません。この場合、結果的にウィルスが原因でコンピュータは停止しますが、それを引き起こしたのは、セキュリティ ソフトウェアを攻撃するスパイウェアだったことになります。しかし、このような状態に遭遇した場合、スパイウェアが原因であったと的確に解析できる技術者はまだ少ないと思われます。
ファイヤウォールを攻撃するスパイウェアもまた危険です。多くの場合、その後リモート制御のためのソフトウェアなどのイントールや、コンピュータ内の情報の盗難につながります。
問題の真の原因を突き止め、対処しない限り再発の可能性は残ります。

ブラウザのセキュリティ設定に注意

セキュリティ ソフトウェアを攻撃するのと同じように、コンピュータのセキュリティ設定を変更するスパイウェアも存在します。多くの場合、BHO(ブラウザ ヘルパ オブジェクト)を利用したもので、Internet Explorer のセキュリティ設定を変更してしまいます。つまり、ブラウザのセキュリティ設定がいつの間にか'低'に変更されたり、悪意のある Web サイトを信頼済みのサイトとして知らない内に登録してしまうものです。ブラウザのセキュリティ設定など、一旦設定すると、普段設定が変わっていないかなど確認することは通常ありません。そのため、これを契機に 2 次被害を呼び込むことになり、その結果、真の原因は不明のままコンピュータが利用できなくなります。

コンピュータのリソースを喰い尽す

アドウェアと分類されるスパイウェアもコンピュータに深刻な問題を引き起こします。アドウェアによっては、鬱陶しい広告を出すためにコンピュータに常駐し稼動するためメモリや CPU リソースを消費するものがあります。1 つのアドウェアが深刻にメモリやプロセッサを消費してしまうものもありますが、多くの場合、複数のアドウェアが同時に動作することでコンピュータに多大な負荷が掛かり、マウスさえも思いどおりに制御できなくなったりします。また、広告を表示するために頻繁に制御サーバに接続するため、インターネット(ネットワーク) バンドを消費してしまうことになります。

インターネットにつながらない?

インターネットに接続できない、Web サイトが開けない、などの問題がルータやネットワーク機器が原因してる場合もありますが、スパイウェアが原因していることもあります。例えば、DNS キャッシュを操作するものだったり、多くの被害報告では hosts ファイルが改竄されていたことが原因でした。Hosts ファイルの改竄では、接続できなくなるばかりでなく Web サイトへのアクセスも見知らぬサイトに誘導されてしまいます。こうして誘導された悪意を持ったサイトを開くだけで、ドライブバイダウンロードによりさらに別の(次の段階の)ソフトウェアがインストールされることになります。

Active-X だけではないドライブバイインストール

ドライブバイインストール手法によるスパイウェアの侵入方法の多くは Active-X を利用しています。Active-X 利用したスパイウェアの侵入を回避するために、セキュリティ設定を変更したり(Microsoft Windows XP SP2 では、これらの危険性を回避するたに Active-X が自動的実行される際に警告が表示されるようになりました)、通常利用するブラウザとし IE ではなく、Firefox など、Active-X を実装していないブラウザに変えたりする方法があります。しかし、最近報告された手法では、Firefox で開いた Web サイトから Java Runtime をインストールし、Java アプレットが IE を起動、ユーザーに Active-X ブロックを解除することを要請し、その後ソフトウェアをインストールするというものでした。(スパイウェアガイド投稿を参照 http://www.spywareguide.com/articles/article_show.php?id=72) 。メールなどで見られるフィッシングのように偽ったメッセージで巧みにユーザーにセキュリティ設定を変更させるものまで存在します。

ハイジャッカの脅威

コンピュータの利用用途が Web サーフィングや電子メールの交換などインターネットでのサービスと密接になった今、ブラウザをハイジャックされることはコンピュータにとってもはや致命的とも考えられます。ユーザーは、常にブラウザを起動する環境にあるということは、ブラウザの起動をきっかけに動作するスパイウェアにとっては、格好のイニシエータとなります。ブラウザ ハイジャッカの多くは、BHO(ブラウザ ヘルパー オブジェクト http://www.shareedge.com/spywareguide/txt_terms.php#5)として侵入し、ブラウザの開始ページ、検索ページ、エラーページ、お気に入り、などを書き換えてしまいます。特に悪名の高い About Blank (http://www.shareedge.com/spywareguide/product_show.php?id=980)は、他のソフトウェアを呼び込みます。ブラウザを起動することでスパイウェアが活動を開始します。また、これら危険性度の高いスパイウェアは、起動するごとに自分自身を複数コピーすることで、除去を困難にしています。除去ができたとしても、ユーザーによりブラウザが起動されることで再び元の機能が回復したりします。また、たとえユーザーがブラウザを起動しないとしても、ある種のスパイウェアはブラウザを自動的に起動するようにオペレーティング システムを設定します。つまり、コンピュータを起動すると自動的にブラウザが起動され、Web サイトに接続し、Web サイトから次々とダウンロードが始まるような状態になります。

除去が困難

除去を困難にする手法として、こうして自分自身のコピーをいくつも作成して行くものあります。About Blank などに見られる、これらのハイジャッカでは、不用意にコンピュータを再起動するとさらに複製が作

られることになり事態がどんどん悪化します。また、ウィンドウズのスタートアップで起動し、必要なファイルが正しく揃っているかを確認し、必要であればアップデータを使ってインターネット経由で自分自身をダウンロードする機能を持つものもあります。先にも説明したように、一旦入り込めば次のレベルの侵略が始まります。

特に除去が困難なのは、複数のスパイウェアに感染しているような場合です。複数のハイジャカに感染されると、除去も一度では完了できません。

スパイウェアが何をするかについての分類は、上記の他に、ダイヤルアップを設定し、高額な回線を利用して接続するダイヤラ、ワームのように電子メールを勝手に送り自身は繁殖させようとするもの、トロイの木馬バックドアとしてリモート接続を許可することを目的とするものなどさまざまです。
(詳しくは、スパイウェアガイド プロパティ リストを参照してください。
http://www.shareedge.com/spywareguide/property_show.php、)

スパイウェアは最新技術と利用した脅威

このようにスパイウェアという脅威は単にそれが何かをし、それにより直接症状が出てくるといったものよりむしろ原因を引き起こす契機(イニシエータ)となるための、様々な手法をもった脅威であると捉えた方が良いと思います。そしてその手法が最新の技術を利用したものであることも感じて頂けたのではないかと思います。
また、こうした複数の攻撃技術を利用した脅威として rootkit (ルートキット)と呼ばれる、ハッキングのためのツールからの攻撃もあります。ルートキットからの攻撃を守る方法については、スパイウェアとは別の技術が必要になるので、詳細の説明を省略します。

Web サイト スパイウェアガイド (http://www.shareEDGE.com/spywareguide/) では、スパイウェアの脅威についての啓蒙と同時に、無料での検出と除去サービスを提供しています。同じサイトでは、検出されたスパイウェアの統計情報も公開しています。これらの統計情報は実際に日本国内で検出された情報です(*注意: ここで検出されたスパイウェアには、ブラウザ クッキーは含んでいません)。 これらの情報もスパイウェアに関して学ぶ上で大いに参考になると思われます。

どんなスパイウェアが報告されているか

内容を見ると、全体の約半分はアドウェアであることが分かります。次に多いのは、ブラウザハイジャッカで約 13%、データマイナ 12%と続きます。ここでのアドウェアは比較的、危険度が高いものは少ないよう

に思われます。しかし、ブラウザ ハイジャッカは当初考えていたよりも多いと感じています。ハイジャッカは、CoolWebSearch や About Blank などに代表されるように非常に除去が厄介です。スパイウェアとして、検出/除去する方法を思いつかないユーザーは、恐らくやむなくオペレーティング システムを再インストールしていると思われます。気をつけないといけないのは、たとえ再インストールしたとしても、原因を見つけ、対応しておかないと、再び同じ被害に遭ってしまうことです。

サイトでは、除去できないスパイウェアの相談や、スパイウェア除去のためのツールを紹介しています。ぜひともご利用ください。

第 4 回

スパイウェア対策 － 情報セキュリティ リテラシの向上

要約

スパイウェアを脅威として煽るだけでなく、何が脅威で何が脅威でないかについて消費者にも分かるようにするには何をすべきか?

スパイウェア対策について、ここでは 2004 年春、FTC 主催のスパイウェア ワークショップからの報告書を読みながら説明したいと思います。原文 http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf
スパイウェアガイドでは、部分的に日本語で紹介していますので参考にしてください。
http://www.shareedge.com/spywareguide/txt_articles.php?article=txt_20050318.php
“IV. スパイウェア危機に対するハイテク業界の対応”で提唱されているように、スパイウェアなどの最新の脅威に関する教育(情報セキュリティリテラシーの向上)は、特にハイテク業界が積極的に進めることが効果的です。消費者が自らこうした情報を常に集め、適切な対応をするのは、技術の進化速度を間あえると不可能なことです。ハイテク業界は、より最新技術を使った脅威の情報を多く持っています。それらの情報を元に的確な手法や対応方法などを企業や社会に公開し、最終的に消費者にまで教育が広がるような仕組みが必要です。また、行政などにも情報を提供しながら法的な整備を行い、悪質な業者を刑罰で対処できるようにすることで、抑止効果も得られることになります。いつものように被害があってからでは遅すぎます。幸運にもハイテク犯罪の場合、日本での犯罪は欧米を追って発生します。つまり、欧米で発生するハイテク犯罪は確実に上陸するし、その手法は全く分かったものであるということ考えると、実施することはそれほど難しいことではないようにも思えるのですがいかがでしょうか。

セキュリティ強化と利便性の低下

この場合、気を付ける必要があるのは、一方的に危険性のみが大げさに伝えられることです。またセキュリティを強化しようとすると、利便性を犠牲にすることになります。例えば、アンチスパイウェアの場合、ブラウザ クッキーをどう扱うかについての見解が良い例です。技術的に、クッキーはスパイウェアではありません。クライアント コンピュータに残るクッキーには、スパイウェアとなるプログラム コードやスクリプトは入っていないからです。しかし、アンチスパイウェアの多くは、クッキーをスパイウェアとして検出します。クッキーは現在殆どの Web サイトで使われている技術で、ユーザーのサイトでの利便性を高めたり、ユーザを見せたい情報に誘導するために欠かせない技術の一つです。しかし、技術的な知識のないユーザーがアンチスパイウェア ソフトウェアを使ってクッキーをスパイウェアとして検出したら、そのまま削除することになるでしょう。クッキーを削除したり、拒否することで利便性を犠牲にすることになります。

スパイウェアに限らず、セキュリティの脅威への対策においては利便性とのトレードオフが不可欠です。例えば P2P や、IM(インスタント メッセージ)、および Skype など利便性の高い多くの技術がセキュリティへのリスクを理由にビジネス環境への実装が否定される傾向にあります。しかし、本来向かうべき方向とは、利便性を犠牲にするのではなくこうした‘Graynet’(グレーネット)を効率よく管理して行くかという部分にセキュリティ ビジネスが発展し、便利なものを安全に使えるようにするということであり、それを実現する技術支援と、社会的な支援が重要になって来ると考えます。

クッキーはスパイウェアではない

時々、アンチスパイウェア ベンダーは製品販促を優先するためか無実のものも脅威としてユーザーの恐怖心を煽っているように感じます。例えば、ベンダーは、クッキーをスパイウェアとしてシグネチャ データベースに登録することでシグネチャファイルを簡単に大きくすることができます。アンチウィルスのデータベースのデータ登録件数を多く見せる方法に加えて、クッキーをシグネチャに追加することで多く見せることは簡単です。つまり、”xx社のアンチスパイウェア製品は xx 万のデータベースがあります。”と優位性を見せることができます。先にも説明したとおり、アンチスパイウェア用のシグネチャ データベースにとって重要なとは量よりも質であるということを思い出してください。インターネット上の Web サーバを巡回し、クッキーを自動的に収集することはそれほど難しいことではありません。しかしこれは、スパイウェア対策という面では、あまり効果的な方法とは思われません。

追跡クッキーは、プライバシーの侵害であるから、スパイウェアという意見もあります。あるアンチスパイウェア ベンダーは、この追跡クッキーのことを”スパイウェアクッキー”と呼んだりしています。これは間違いです。そしてこれはよりユーザーのスパイウェアへの誤解を招いてしまいます。クッキーは、クライアントに保存される単純なテキストファイルです。このファイルには、プログラム コードも、またユーザーID やパスワードなどの情報は、一切含まれていません。従って、クッキーがコンピュータの情報を盗む、外部に漏らす、コンピュータ障害を引き起こすなどはありません。一方、そのクライアント コンピュータ上に残るクッキー ファイルが盗まれることでセキュリティのリスクが発生するのは確かです。

追跡クッキー/サードパーティ クッキー

このようにクッキーは技術的には、スパウェアではありません。しかし、クッキーがスパイウェアとみなされていたことには、理由がありました。

クッキーは本来、唯一それを設定したサイトからのみアクセスが可能です。これは利用者が1つのサイトから他のサイトに移動している間も、元のサイトでの情報を保存しておくためです。しかしこの技術がある種有名な DoubleClick 社によって乱用されました。その手法は、彼らのサーバーからさまざまなバナー広告を表示し、それらのサーバーからクッキーを設定、読み込むことでユーザーのサーフィングを追跡することです。これらのクッキーは、サードパーティ クッキーと呼ばれるもので、ユーザーが表示している Web サーバーから設定されるファーストパーティ クッキーとは違って、見えない間に、バナー広告に埋め込まれた Java スクリプトなどを利用して設定されます。DoubleClick 社は、数千もの Web サイトに広告

を持っていて、それらの各広告は自身のサーバーから呼び出され、クッキーを設定、読み込みを繰り返すことで、ユーザーがどこにいるかを把握することができるシステムを構築することができました。
先にも述べましたがクッキーは、スパイウェアではありません。しかしクッキーの技術を乱用したこうしたシステムは、ユーザーの嗜好の監視であり、プライバシーの侵害です。つまり、プライバシーの侵害がスパイ行為であることから、追跡クッキーが、さらにクッキーがスパイウェアのように見なされていました。

プライバシーを守るためのブラウザの設定

しかし、こうしたことから自身を守る方法はすでにあります。
以下に追跡クッキー(サードパーティ クッキー)を回避するためのブラウザの設定を紹介しておきます。

Mozilla や Netscape では 編集> 設定で
プライバシーとセキュリティ -> クッキーで"文書がある Web サイトから送信されてくるクッキーのみ受信する"を選択します。これによりサードパーティのクッキーがブロックされます。クッキーの期限や他のプライバシー設定を行い、クッキー、ダウンロード マネージャ、サーフィング履歴を調整することができます。

最新バージョンの Internet Explorer では、ツール -> インターネット オプションで "プライバシー"タブをクリックし、"詳細設定" ボタンを押します。
"自動 Cookie 処理を上書きする"をチェックし、サードパーティ クッキーにある"ブロック"をチェックします。

ユーザーへより詳しい解説も必要

情報セキュリティ リテラシの向上を図る上で重要なのは、やはり正確な情報を提供することではないかと思います。例えば、"コンピュータの情報が盗まれる"といった場合にどんな情報がどのような方法で盗まれるかについての説明も正しく提供してあげる必要があるのではないでしょうか? スパイウェアの定義に関してこのコラムで解説しようとしているのですが、これは逆に、実はスパイウェアが定義できないものであることも説明しようとしています。例えば、"スパイウェアによってあなたのクレジットカードの情報が盗まれる!"といっても実際は、"スパイウェア"というクレジットカードの情報を盗み出すソフトウェアが存在するのではなく、リモートアクセスツールもしくは、キーロガー、または BHO などのソフトウェアを利用されることでそれが可能にるわけです。そしてそうした行為をするソフトウェアのことをスパイウェアと呼んでいるのです。この辺りのことを一般消費者に明確に説明することでスパイウェアだけでなく、情報セキュリティリテラシの向上が図られるのではないかと考えています。何でも脅威として、販促目的で恐怖心だけを煽る方法は、ユーザーのセキュリティ意識を高めることはできますが、本来のリテラシの向上とは違うのではないかと思います。実際大きなセキュリティ関連ベンダーでもこうした行為をしていることも見られるのは残念なことです。

また、大手のベンダーではありえませんが、インターネット上には悪意のある偽のセキュリティ ベンダーに遭遇する場合もあります。例えば、アンチスパイウェアと名乗るスパイウェア製品、セキュリティ製品と名乗る、マルウェアやトロイの木馬も実際に存在します。こうした二重スパイと呼ばれるセキュリティ製品にダウンロードに慣れた個人ユーザーが被害に遭うことがあります。またスパイウェア除去サービスを名乗る詐欺サービスも報告されています。恐らくクッキーでも削除してスパイウェアを除去したと報告したりしていたのでしょう。

企業内におけるスパイウェアに関する教育もまたセキュリティ リテラシの向上のために有用です。また学生など若い世代への教育も必要です。新しいもの好きで、色んなことに興味を持つ若い世代にこうしたセキュリティ リテラシに関する教育がより必要であることは明らかです。便利であるインターネットやコンピュータの利用の裏に、こうした危険性もあることを知っておくことは重要です。

法の整備

次に、日本よりも少し進んだ米国の例を見てみます。先日下院を通過した SPY ACT 法(H.R. 29)の内容について見てみましょう。 原文への URL も紹介しておきます。

http://thomas.loc.gov/cgi-bin/t2gpo/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr032.109.pdf

ちなみに、SPY ACTとは、SECURELY PROTECT YOURSELF AGAINST CYBER TRESPASS ACT の略です。

この法案で興味あるところは、”スパイウェア”を定義してそれを違法とするのではなく、各種の行為を挙げてそれを違法としていることです。長い間FTCは積極的にスパイウェアを定義するために時間を費やしてきました。しかし、昨年のスパイウェア ワークショップでの結果に見られるようにスパイウェアを定義することはできませんでした。

スパイウェアを定義し、それを違法であるとする代わりに、この法案では多くの具体的な行為を違法としています。それらは、前回のスパイウェアが何をするか? で説明したことが含まれています。ここでは便宜上スパイウェア用語を使っていくつかを紹介して見ます。(カッコ内が原文の対応するセクションと項目を表しています。)

いわゆるハイジャッカ行為の禁止(SEC 2.(a) (1))

コンピュータを制御して情報を盗む行為(A) –ブラウザ ハイジャッカ(B)、ダイヤラハイジャッカ(C),悪質なアドウェア(E)

コンピュータの設定の変更に関して(2)、ホームページ ハイジャッカ(A)、検索エンジンハイジャッカ(B)、お気に入りへの書き込み(C),セキュリティ設定の変更(D)

キーロガーの行為に関して(3)、フィッシングなどで見られる偽の Web サイト(4)、紛らわしい表現の禁止、インストールに関して、強制的にインストールする行為を禁止(5)

セキュリティ ソフトウェアへの攻撃を禁止に関して(9)、

データ収集に関して(SEC3)、個人情報を収集、送信することを禁止、閲覧したWebページを集め、広告表示に利用することを禁止(B)
サードパーティ クッキーの乱用についての禁止を連想されることとして、唯一読んでいるWebページのみが情報を集め、特定のWebサイト内でのみこれを利用できる
情報収集するプログラムは、その機能に応じて適切なメッセージをユーザーに明示するように勧告しています(C)。
例えば、”このプログラムはあなたに関する情報を収集し、送信します。利用に関して同意しますか?”
“このプログラムは、あなたの訪問した Web サイトに関する情報を収集し、その情報を利用してあなたのコンピュータに広告を表示します。利用に関して同意しますか?”
“このプログラムはあなたに関する情報を収集し、送信します。また、あなたの訪問したWebサイトに関する情報を収集し、その情報を利用してあなたのコンピュータに広告を表示します。利用に関して同意しますか?”

法による規制でどんな効果があるか?

法案ができ、刑罰が定義されてもスパイウェア犯罪が減ることはないと思います。しかし、法の整備は必要です。これら法の整備がもたらす効果として、悪意を持っていない製作者がこれに確実に準拠すること(抑止力)、またユーザーは何が悪質で何が正統かをこうした法に照らし合わせて識別できるようになること、またユーザーがこれらの製品や Webサイトを見つけた場合、その製作者やそれを配布しているサイトに対し、ソフトウェアの配布停止やサイトの停止を訴えることができることではないでしょうか?
こうした法の整備や情報収集(報告の受け口)のために IPA などが積極的に活動すべきと思いますが、声が届かないのは残念なことです。

第 5 回

スパイウェアの侵入経路と対策について

要約

スパイウェアがどのように侵入して来るかについて紹介し、どんな対策が可能かについて考えてみます。

スパイウェアの侵入経路について説明する前に、利用されるコンピュータの環境について分類しておきます。ここでは、公共アクセス PC、ホーム PC、および企業内 PC と大きく分類してみました。

公共アクセス PC が危ない

公共アクセス PC とは、ネットカフェや、ホテル、Kinko's などコンピュータの貸し出し、など公共アクセス端末として利用されている PC(パブリック アクセス端末)を意味します。恐らく公共アクセス PC が最もスパイウェアの脅威にさらされている PC ではないかと考えられます。

これらの PC に、スパイウェアが侵入する方法として、以下の経路があります。まず、商用リモート アクセス ソフトウェアのインストールによるものがあります。これには、RAT(Remote Access Tool)などは、コンピュータの管理者やユーザーによりインストールされる場合、第三者によりインストールされる場合、ドライブバイ インストールなどの方法でユーザーの知らない内にインストールされる場合があります。

商用というのは、一般に市販されているソフトウェアのことを意味します。多くの場合、コンピュータの監視や管理を目的としたソフトウェアで、誰でも入手することができるものです。また、こうしたソフトウェアはウィルス対策ソフトウェアではインストールを検出したり除去したりされることはありません。

第三者によるキーロガーやリモート管理ソフトウェアのインストールは、企業内ではオフィスの監視やデータアクセスを記録など管理目的で管理者によりインストールされるものがあります。一方、公共端末 PC は、スパイ行為を目的としてリモートアクセスや、キーロガーなどがコンピュータの利用者や所有者が知らない間に悪意を持った第三者によりインストールされる場合があります。例えば、ファイルを印刷するサービスを提供する PC にリモート管理ツールを仕込むことで、大切な文章ファイルがそのまま第三者にネットワークを経由してコピーされる可能性があります。

キーロガーによりユーザーID が盗まれる

また、インターネットカフェなどでは、悪意を持った第三者によりキーロガーが仕込まれ、オンライン ゲームユーザーのゲーム アカウントを盗み出し、その ID を利用してゲームアイテムを盗み出して売買するような事件は、日本よりもネットカフェ ユーザーを多く持つ韓国や中国では多く発生していました。そうした事情から韓国や中国では日本よりも早くアンチスパイウェア ソフトウェアが多く紹介されていました。

では、不特定多数のユーザーに利用されるこうした公共のアクセス端末をどうやってスパイウェアなどの脅威から保護することができるでしょうか? 最も有効な手段としては、アンチスパイウェアを含んだセキュリティ対策を適用した上で、さらにユーザーが利用する毎に、コンピュータを初期化することが有効だと

思われます。
また、セキュリティ テンプレートなどを利用してユーザーがプログラムをインストールできない、システム設定を変更できない、ブラウザの設定を変更できない、など利用範囲を制限する設定はサービスを提供する側で提供する必要がありますが、利用する側も、利用する前に、オンライン スキャン サービスなどの Web サービスを利用して、一旦確認してから操作を始めるなどの注意も必要かも知れません。
先にも紹介したように商用キーロガーには、ハードウェア タイプのものも存在しています。ハードウェアキーロガーはスパイウェア対策ソフトウェアでも検出することはできません。従ってセキュリティ対策のチェック項目としてハードウェアの検査も含めることが必要になります。ハードウェアタイプのものはキーボードコネクタ間に挿入されるものです。通常目視で確認することができます。
こうした公共アクセス端末を使ってプライバシーや情報盗難の被害に遭った場合、誰が責任を持つべきかについてなどの議論の解決は困難です。実際、こうした公共アクセス端末を提供している側からすればこのような PC にセキュリティ対策への投資を最小限にしたいと考えます。従って、問題があれば交換、再インストールなどの対応がされているのでしょうが、利用者に損害が発生したとしても、保障することなどまさに想定外になっていると思われます。

情報セキュリティ リテラシ向上のための良い循環構造とは

例えば、クレジット カード ID やオンライン バンクの ID 情報の盗難により消費者に被害が場合でも、米国などの例では、クレジット カード会社や銀行などが責任を持つというシステムが既にありました。このため消費者を守るために、企業側が IT 情報セキュリティに投資を惜しまない、また消費者へのスパイウェアなどの新たな脅威に対するリテラシ向上のための教育活動に貢献するという良い循環が自然生まれる構造になっているのではないかと思います。最近日本でのクレジットカードのスキミングなどによる犯罪行為で預金者の預金を銀行が守れなかった場合に、銀行が預金者の預金を保障する法的な動きも、結果的にこのような新しい脅威に対して迅速に対応できる良い循環を生む原動力となることを期待したいものです。

ホーム PC への脅威

家庭で利用している PC がスパイウェアに感染する経路として、公共アクセス PC での侵入経路である第三者によるインストールよりも多くの可能性があるのは、やはり Web サイトへのアクセスやインターネット上のソフトウェアのダウンロードによる感染です。特に海外の Web サイトからドライブバイ インストールによる感染には注意が必要です。危険なサイトにアクセスしないことも被害を軽減することになりますが、フィッシング メールや URL の入力間違によって誘導されることを避けるのは困難です。また最近では、フィッシング メールによりユーザーを Web サイトに誘導し、サイトをアクセスすることでドライブバイ インストールする手法が多く見られます。スパムやフィッシング メールへの対策や Web サイトへのアクセスをフィリタリングすることである程度危険度を軽減することが可能です。ドライブバイ インストール対策として考えられる方法は、ウィルス対策ソフトウェアの導入とパーソナル ファイヤウォール、ブラウザの脆弱性、ポ

ップアップの禁止など対応に加え、Internet Explorer をブラウザとして利用している場合、Active-X の停止やブロック リストによる Active-X の制御も効果的です。

ブロックリストの活用

スパイウェア対策専用のソフトウェアでは、各社の持つシグネチャ ファイルから生成したブロックリスト機能を提供しているものがあります。プロックリストは既知の Active-X コントロールを利用したスパイウェアを Internet Explorer から実行できなくする方法です。これにより、既知のスパイウェアについては、実行を抑止し、また侵入を阻止することができます。リアルタイムで検出する方法に比べ、システム リソースを一切消費しないで効果的にスパイウェアから守ることができます。ブロックリストで利用している技術についての詳細は、Microsoft 社の技術情報を参照してください（参照 http://support.microsoft.com/kb/q240797/）。ブロックリストを提供しているスパイウェア対策ソフトウェアを利用している場合、そのスパイウェアシグネチャファイルの更新と共に最新のブロックリストを定期的に適用することで常に新しいスパイウェアへのブロックリストによる対応が可能です。ブロックリストの入手や追情報は、スパイウェアガイド http://www.shareedge.com/spywareguide/blockfile.php を参照してください。

その他スパイウェア対策専用ソフトウェア機能の活用

逆にユーザーがインターネット上のソフトウェアを故意にインストールすることによる感染もあります。プラグインや無料ソフトウェアなどにバンドルされているものです。多くの検索機能を提供するブラウザ プラグインでは、検索キーワードを一旦特別な Web サーバーに送信し、結果を表示します。ソフトウェアにバンドルされるスパイウェアにはさまざまなものあります。広告を目的としたアドウェアであっても、アップデート機能を持ったものは、ユーザーの知らないうちにさらに他の広告表示のためのソフトウェアをダウンロードしたり、自分自身の最新版のダウンロードを試みるものがあります。インストール時にインターネットにアクセスする場合が多いので、パーソナルファイヤウォールでそれを検出したり、情報の流出や他のソフトウェアの自動ダウンロードを拒否することはできます。除去には、同時に提供されるアンインストーラを使用すると良いのですが、上記のように他のソフトウェアをインストールしたりしていると、アンインストーラでは完全に除去はされないままになります。

ホームPC では、ハイジャッカの被害が多く報告されています。また、ハイジャッカは、除去が非常に困難な場合が多く、除去が可能なスパイウェア対策ソフトウェアが必要になります。感染に気づいたら、早期にスパイウェア対策ソフトウェアでの除去が必要です。ハイジャッカでは、ブラウザの開始ページや検索ページが変更されていることで、感染に気付きます。スパイウェア対策ソフトウェアの多くは、そうしたブラウザ設定の変化を検出する機能が提供されているので、それらの機能を利用すると早期に発見することができます。非常に複雑な場合が多く、手動ではなく、ソフトウェアでの除去が必要になります。多くの場合、コンピュータの起動毎に自分自身をコピーしながら増えて行くので、コンピュータの挙動がおかしい

からと思って安易にコンピュータを再起動していると感染が重症化してしまいます。

さらに個人ユーザーのコンピュータの被害としては、LSP(Layered Service Provider)の置き換へ、hostsファイルの改竄なども報告されています。スパウェア対策ソフトウェアでは、未知のスパイウェアによるこれらの情報の変更を検出する機能が提供されています。

企業内コンピュータは、本当に守られているか?

企業内コンピュータへのスパイウェアの侵入経路や方法は、特に他の例と違ったものはありません。先日のイーバンクでの事件のように、個人を狙ったさまざまな騙しのテクニックによる侵入の可能性は他の環境よりも高いのかも知れません。騙しのテクニックでは、フィッシング メール、IM (インスタント メッセンジャー)や、チャット機能を利用して、感染リンクからソフトウェアをインストールさせてしまう方法です。大企業など、外部と社内ネットワーク間でセキュリティが装備されている企業内でのコンピュータにはその利用用途やインターネットなど外部ネットワークへの接続がある程度制限されている環境では、スパイウェアによる被害も少ないかも知れません。SOHO や中規模になると外部との接続に関する安全確保は、家庭での利用とさほど変わらないケースもあるでしょう。しかし、大企業であってもネットワーク環境が多くの制限事項により安全だと思い込んでしまうことは非常に危険ともいえます。これは例えば、”自分は健康に気をつけているから病気にならない。”と過信して、定期健診もしない、ただ自分で思い込んでいるような人に似ています。企業内においてはスパイウェアもその侵入や、インストール場所を管理してこそはじめて安全といえます。スパイウェアを管理するということは、具体的には、企業内のコンピュータにインストールされているスパイウェアをアプリケーション ソフトウェアの管理と同様にインベントリを作成して管理しようというものです。

グレー ソフトウェアの管理

その理由として、まず、キーロガーやリモート アクセスなどをスパイウェアではなく、監視ツールとしてインストールしているコンピュータでは、これらの活動がスパイウェア対策ソフトウェアにより妨害されないように管理する必要があります。また、ブラウザプラグインも種類によっては、企業で推奨したものをインストールしている場合もあります。そしてどれを残して、どれを除去するかは、つまり、スパイウェア ポリシーの管理がコンピュータを利用している個々のユーザーではなく、管理者により各グループ毎にコントロールされることが必要になります。そのためにも企業内コンピュータのスパイウェア対策では、スパイウェア インベントリの管理が必要ということになります。これを利用して管理者は、どのコンピュータにどんなスパイウェアがインストールされているかを常に把握します。悪質なものや有害なものは、最初に除去しるとして、ここで管理するスパイウェアとは悪質なものではなく、よりグレーなソフトウェアということになります。また、ユーザーの介在なしにリモートから除去できるような仕組みも必要です。こうした面から考えると、スパイウェア対策とウィルス対策では、大きくその目的が違っていることがお分かりになると思います。スパイウェア対策で要求されるのは、企業内のグレーなソフトウェアを如何に管理するかということではな

いでしょうか。ウィルス対策ソフトウェアでは、グレーソフトウェアという概念は存在しません。白か黒かと判断し、黒の侵入を完全に排除することがその目的であり、期待されている役割です。一方スパイウェア対策はというと、グレーソフトウェアの存在を認め、それらを企業ポリシーに沿って管理してゆくとことが期待されるべき機能と役割ではないかというのが、私の考えです。残念ながら、スパイウェアの存在や定義も曖昧な現時点において、ここで説明した機能と役割を持ったスパイウェア対策ソフトウェアは、市場には存在していません。しかし、皆無ではありません。スパイウェア対策ベンダーの製品で企業用として、エンタープライズ機能を持った製品がこれらの要望をある程度満たしていると思います。
しかし実際製品化について、色々と話をしていると、スパイウェア対策ソフトウェアのエンタープライズ版の導入を求める企業は少ないように思われます。これは、セキュリティに対してさらなる投資を必要とするからです。最小限の投資でこうしたシステムを企業ユーザーに提供する方法や製品開発に関して、現在私達は、いくつかのソフトウェア ベンダーと協議を始めましたので、そちらもご期待ください。

スパイウェアは感染しない?

グレーソフトウェアの管理という概念を企業情報セキュリティ管理に導入することは、スパイウェア対策だけでなく、その他の新たなセキュリティの脅威への対策という面から非常に有効です。
例えば、スパイウェアの定義に関しての説明でよく見かける表現として、”スパイウェアは感染しない“を定義している場合があります。これはウィルス対策ソフトウェア ベンダの定義する狭義のスパイウェアになります。つまり、感染機能を持つソフトウェアは、ワームとして分類されますが、スパイウェアでもワームとして分類するスパイウェアが存在します。”スパイウェアは感染しない”とスパイウェアを定義したり、その前提でスパイウェア対策を考えようとすると、何が起こるかといえば、ウィルス対策ソフトウェアでも検出されない、感染する悪意のある、または不要な広告を表示するソフトウェアには対策しない、できないということになります。前回のコラムの米国の Spy ACT について紹介したように、スパイウェアを機能から定義することが現実的でないことが簡単に理解できると思います。ここでいう感染機能を持つスパイウェアとは、その感染方法(技術)もウィルスとは違っていたりします。

セキュリティ ポリシー テンプレートの活用

また、スパイウェアを検出、除去する方法とは違う方法があります。これは、XBlock Systems 社により特許申請されている技術で、Microsoft Windows 2000/XP のセキュリティ ポリシー テンプレート機能を利用した、SRP（ソフトウェア制限ポリシー テンプレート）http://www.shareedge.com/spywareguide/articles/SRP_ja.pdf)を利用する方法です。ブロックリストと同様に、常に最新のスパイウェアからコンピュータを守るために、最新のセキュリティ テンプレートを適用することになります。これによりコンピュータは、既にインストールされているスパイウェアを除去することもなくその活動を封じ込め、また新たな侵入からも防ぐことができます。大きなメリットは、OS で提供されているセキュリティ機能を利用するだけなので、コンピュータへの負荷(CPU や、メモリの消費)が一切ないことです。最近では、ウィルス対策ソフトウェア ベンダーからの製品はより多くの機能を統合した形式でセキュリティ スイート化されて提供されてきました。しかしその多くは、システムへの負荷が増大し、実際利用しているとその動作性能の低下に困惑することが多いのではないでしょうか?

しかし、こうしたセキュリティテンプレートでの対応は、システムへの負荷の軽減だけでなく、その他多くの利点があります。まず、ファイルを削除したりすることが無いため、誤検出や、除去の不具合によるシステムへの障害がなくなります。また、既存の検疫システムや、データやプログラムの配信システムに容易に統合することができます。

企業でのスアイウェア対策

スパイウェア対策を企業で考える場合、重要な点としては、グレーなソフトウェアを管理する概念と仕組みうい実現すること、また、導入においては、以下のステップで実装できるかどうかとではないかと考えます。

1. 調査(インベントリ作成)、
2. コンサルテーション（分析）
3. インプリメンテーション（実装）
4. 運用メンテナンス(シグネチャ、セキュリティテンプレートのカスタマイズと配信)
5. テンプレートのカスタマイズと配信)

その後、このコラムか以下の表題と共に継続される予定です。

■ 今後の新たな脅威にどう備えるか

第 6 回

スパイウェア対策の導入がなぜ困難か

要約

スパイウェア対策の導入を困難にしている要因について解説し、改善のための取り組みの実例や、方法論について紹介します。

スパイウェアの存在や感染を認識すること

ウィルスとスパイウェアを比較して説明する場合、ウィルスは、破壊活動を目的として開発され配布されるプログラムであるのに対し、スパイウェアは経済活動を目的としたプログラムであるといえます。スパイウェアの開発者、配布者はその行為により金銭的に収益があることを期待してプログラムを開発配布しており、確実にその成果を得ているとすれば、その収益を次の製品開発に投資することでより高度で効果的なプログラムを作り出すことができます。一方ウィルス プログラムの開発は、かける費用も少なく、対投資効果もほとんどないという構造になっています。このように開発にかけるリソースが全く違ってくるわけで、スパイウェア技術の進化はウィルスの進化をはるかに超えているということが簡単に想像できます。

また、スパイウェア プログラムは破壊活動ではく、プログラムは自分自身を感染 PC により長い間侵入したままユーザーに知られること無く活動することを重要な目的としています。スパイウェア プログラムが実際コンピュータ内に存在しているかどうか分からない、認識できないということもスパイウェア対策導入の遅れの原因の 1 つであり、それはスパイウェア検出ソフトウェアがまだ一般に普及していないからでもあります。実際に企業の IT 管理者の方々と話しをしていて分かったことですが、ウィルス対策ソフトウェアベンダーの提唱するスパイウェアの検出機能が、広義のスパイウェアを検出しないことをユーザーに明確に通知されていないために、既存のウィルス対策ソフトウェアに付加されたスパイウェア検出機能でスパイウェアに十分対応できていると勘違いしてしまっていることも大きな要因です。

悩める現場の技術者達

2005 年に入って、スパイウェアの脅威への対応を掲げた多くのウィルス対策ソフトウェアは、実質まともな対応ができないままでした。しかし、実際の企業の IT 管理者の方々と話しをしていると、企業や個人ユーザーの多くは、大手ウィルス対策ソフトウェア ベンダーの言及のままにしかスパイウェア対策を行っていないことが判ってきました。それでいて、こうした現場の技術者の方々は、無料や有料のスパイウェア対策専用のソフトウェアを独自に駆使しながらスパイウェアに関する勉強もしているため、現在の対策で十分とはいえないことも実感しているわけです。まさに現実と虚構の落差をどう埋めるべきかの方法を模索している技術者達です。なぜこんなことが起こってしまったかは、このコラムのテーマでもあるスパイウェアの定義がウィルス対策ソフトウェア ベンダーとスパイウェア対策ソフトウェア ベンダーで違っているからであり、またそのことがユーザーに正しく通知されていないからです。これから将来新たなバージョ

ンアップなどを加えることで広義のスパイウェア対策機能が実装されるとも考えられますが、このことが結果的に日本の IT 業界全体に本格的なスパイウェア対策の導入を遅らせることになった大きな要因であると考えています。

すべてのスパイウェア対策を信じることはできない?

これは企業ユーザーでも、個人ユーザーでも同じことが言えます。まずは、スパイウェア対策ソフトウェアによるスパイウェア検出を行い、現状を認識することをお薦めします。スパイウェアガイド(www.shareEDGE.com/spywareguide/)で無料のスパイウェア検出と除去を提供しているのは、こうしたスパイウェア対策の導入が進まない現状を改善するための 1 つの手段と考えるからです。よく検出だけは無料で提供するが除去はソフトウェアの購入を要求するソフトウェアがありますが、こうしたものでは、ユーザーの購買意欲を高めるためにクッキーをスパイウェアとして検出することで、より多くのスパイウェアに感染していると見せるものがあるので注意が必要です。

悪質なものでは、無料スキャン ソフトウェアとしてインストールされクッキーをスパイウェアとして検出し、これを除去するのに(クッキーを消去するのに) 数千円を請求するものまであります。しかし、クッキーの消去ツールに数千円払う必要があるでしょうか? しかしスパイウェアに関する知識のないユーザーにとってはそれが価値あることかどうかを判断することは困難なのです。

スパイウェア オンラインスキャン サービスを普及させる試み

現在私達の推奨しているオンライン スパイウェア検出と除去サービスを使っても、すべてのスパイウェアが確実に検出や除去が可能なわけではありません。実際、そこで使用しているクイックスキャン技術は、ハードディスク上のすべてのファイルをスキャンするのではないため、既知のスパイウェアを検出しようとしても完全ではありません。代わりに高速なスキャンが実現されているため、ユーザーはいつでも気軽に検出が可能になります。無料スキャン サービスの役割として期待されるのは、ユーザーにスパイウェアの存在を認識してもらうことにあります。

検出結果を見てみると、数ヶ月前のイーバンクでのスパイウェア事件を契機に検出報告数が急上昇したことがわかります。これは、スパイウェアが多くなったことが原因ではなく、スパイウェアを意識したユーザーが多くなったことを意味しています。スパイウェアに関心を持ち、検出サービスを実行するユーザーが多くなったということです。

スパイウェア オンラインスキャン サービスの役割

今後、こうした無料オンラインスキャンサービスの提供サイトを広げることでスパイウェアの存在を認識していただけるようにしたいと考えています。こうした活動がインターネット ユーザーのスパイウェアへの関心を高め、情報セキュリティ リテラシ向上に大いに貢献すると思われます。

しかし、スパイウェアの検出だけでなく、除去についても、こうしたオンラインスキャンの技術では、十分対応できないスパイウェアがあります。以前のコラムで解説したとおり、ある種のスパイウェアは、除去を

非常に困難に作成されています。こうしたスパイウェアの除去には、やはりスタンドアロン型の対策ソフトウェアを利用する必要があります。
つまり、軽度のスパイウェア感染への対応やグレーなプログラムの検出には、十分な機能が提供されているので、’健康診断’といった程度で利用することが可能になります。
これ以上の機能やその他の目的では、スタンドアロン型など別のソリューションが必要になります。

企業ユーザー向けスパイウェア インベントリ作成サービス

また、企業ユーザー向けとして提唱しているのは、スパイウェアのインベントリ作成サービスです。これは現在お問い合わせのあった企業ユーザー向けに、スパイウェア対策を導入する前に簡単に行えるサービスとして企業内 PC がどれほどスパイウェアに感染しているかを把握し、スパイウェア インベントリを作成しておくことで実際の導入時にこれをベースにスパイウェア対策ポリシーを定義するためです。
スパイウェアとは、同じプログラムが利用用途や利用場所によっては必要なソフトウェアであったり、不要なソフトウェアであったりすることから、このグレーなプログラムをインベントリとして管理運用するためです。

スパイウェア情報データベース

グレーなプログラムの存在を認識することで、スパイウェア対策をどのように展開して行くかが変わってきます。例えば、ウィルス対策はプログラムが悪性かそうでないか、白黒で判断することで悪いプログラムを徹底的にブロック、除去する方式や考え方を取り、そのプログラムが悪いものとした前提でその機能や感染方法などの情報が必要となります。スパイウェアなどグレーなプログラムの場合は、侵入経路や、その機能の情報はもちろん、さらにそのプログラムが必要なものか、不要なものか、またはどちらでもないものかなどの判断を助けるための情報が必要とされます。
それは常にエンドユーザーまたは企業の IT 管理者が除去/無視を判断する必要があるからです。ウィルス対策では、この除去/無視の決定がウィルス対策ソフトウェア ベンダーによって行われるのでエンドユーザーは必要か不必要かを全く意識する必要はありません。

アプリケーション データベースの提案

現在グレー プログラムに関する情報データベースは十分に提供されていません。スパイウェア データベースは、スパイウェアに関しての情報としては役立つと思われますが、グレー プログラムの情報には、十分ではありません。現在私達は、アプリケーション データベースのサービスを提供しようと試みを始めました。このデータベースには、悪いソフトウェアだけではなく、必要なもの、不要なもの、どちらでもよいものとプログラムを 4 つに分類してデータベース化したものです。エンドユーザーや IT 管理者が不審なプログラムを見つけたらこれらのデータベースを検索することでそのプログラムの要不要を判断するために役立つものと期待しています。データベースに存在していないプログラムの登録や、追加情報に関して、このデータベースの構築には利用者からの支援を期待しています。

(http://www.shareedge.com/modules/appdb/)

スパイウェア対策として、まず遅れているスパイウェアの存在の認知度を上げると共に、それをより正しく理解すること、次に従来型の白黒で判断する方式ではなく、白黒さらにグレーの存在を認識し、グレーな部分をどれだけ効率よく管理できるかの対策を実施してゆくことをではないかと私達は考えております。

第 7 回

一般消費者におけるスパイウェア感染の実態と新しい対策

要約

2005 年 10 月 12 日からサービスを開始したヤマダ電機 WEB.COM(www.yamada-denkiweb.com) での X-Cleaner マイクロスキャナを利用したスパイウェア検出除去サービスからの統計情報およびユーザーからの報告例を紹介します。また、最新のセキュリティ対策事情について紹介します。

一般消費者の PC における感染状況は、1 台に 1.8 件

2005 年 3 月からはじめたスパイウェアガイド www.shareEDGE.com/spywareguide/ で提供していた無料オンライン スパイウェア検出と除去サービスでは、インターネットに熟知していて、また’スパイウェア’の知識も若干持ったユーザーが中心であったのに対し、同年 10 月から開始したヤマダ電機 WEB.COM での同様の検出サービスでは、より一般のインターネット ユーザーが新たに加わったと考えられます。検出と除去サービスを行っているため、一旦除去されたコンピュータでの検出も行われていることから、検出率などを調べるには初めて利用されるユーザーのデータが重要になります。そこで対象にした、最初の 8,000 ユーザー(PC)をサンプルに計算すると、1 台当り約 1.8 件のスパイウェア感染があることが分かりました。

ここで、1.8 件という数字をどう見ることができるでしょうか？ 多いか少ないか。ここでのスパイウェアは、クッキーは含んでいません。また、オンラインスキャナでは、クイックスキャン機能での検出であることを考えると、実際はもう少しあると思われます。また、体験された方の報告などから想像できるのは、スパイウェアは PC 1 台につき最低 1 つという感染よりも、全く感染のない PC もいくつかあるが、感染している PC には、多くの場合複数の感染があるといった感染状況ではないかと考えています。

サポートセンター技術者への教育不足の実態

サービスの開始後、あるユーザーからの問い合わせがありました。そのユーザーが言うには、スパイウェアに対応した最新のウィルス対策ソフトウェアをインストールしてあるのにも関らず、コンピュータの調子が悪いので、加入しているインターネット プロバイダ(大手 ISP)のサポートセンターに電話したが、原因が分からないので OS を再インストールするように言われたため、コンピュータの製造元のサポートセンターに電話したが、結局、同様の回答しか得られなかったそうです。そこで、ニュース記事で見たヤマダ電機 WEB.COM での無料スパイウェア検出/除去サービスを試したいということで相談がありました。

実際に検出を実行してみると、そのコンピュータには、9 つほどのスパイウェア検出があり、中でも CoolWebsearch や IST Bar など、悪名の高いハイジャッカにも感染している状態でそれらスパイウェア

がコンピュータの不具合の原因であったことが考えられます。

スパイウェア対策とその脅威について啓蒙活動を広める上で、より一般ユーザーの目にすることになるような無料オンライン スキャナは非常に有効です。しかし、こうした例にあるように、ISP や PC ベンダーのサポート技術者への教育がされていない事実もあり、これは非常に残念なことです。米国の多くの ISP や PC ベンダーは、2004 年以降、こうしたサポートへの負荷を軽減したり、ユーザーのサポートに対する顧客満足度を上げる目的で積極的にスパイウェア教育が実施されていますが、日本の現状はまだまだなのかも知れません。

あるケーブルテレビ局(ISP)の試み

米国の最近の動向では、また、IT セキュリティへの脅威から総合的にユーザーを守るために、AOL などの大手のプロバイダは、セキュリティ センターとして、各種のセキュリティ対策を殆ど無料でユーザーに提供するようになりました。セキュリティ対策をエンドユーザーに代わって ISP が積極的に提供する仕組みはスパイウェアに限らず、今後の新しい脅威から守るためにも効果的な方法と思われます。
私自身の身近ではこうしたレベルでユーザーを IT セキュリティの脅威から守ったり、サポートしたり、また安全に、かつ有効にインターネットを利用できるような活動をしている地方のプロバイダがありました。それは大分県にあるケーブルテレビ局 CTB メディア(www.ctb.ne.jp) で、ケーブルテレビ加入者の 30%は同時にインターネット サービスも利用しているようです。話を聞いていてとても魅力的に思ったのは、サポートもすべて自社内でこなしているのはもちろんのこと、地方という強みからでしょうが、問題があったら電話での対応のみならず、お客様の家まで伺って対応することが定着していることです。こうした活動により、お客様からの要望や不満を直接吸い上げるだけでなく、インターネット セキュリティ リテラシ教育まで行うことができるという点です。設備や性能の点では、大手の全国規模のプロバイダ引けを取らない、こうした地方の CATV 局では、こうした顔をあわせたコミュニケーションによるサポートが充実することでお客様を十分引き付ける魅力を持っています。また、メールや掲示板による伝達だけでなく、顔を合わせながら接することで IT セキュリティ リテラシについての啓蒙活動が効率よく行われ、効果的に安全水準が高まるのではないでしょうか。インターネット上に都市も地方も無いわけですから。

ISP から提供されるセキュリティ サービスへの期待

米国では、ケーブルテレビ局はさらに電話サービスまで提供していて、ケーブルテレビさえあればテレビ、インターネット、電話、ビデオオンデマンドで好きなエンターテイメントがいつでも楽しめる状況です。こうしたサービスも技術的には日本でもできるのでしょう。新しいメディアとインターネットとの融合は、こうした先進的な地方 CATV に大いに可能性があるのかも知れません。

この CATV 局 CTB メディア(www.ctb.ne.jp)では、以前から提供していた無料のウィルスプロテクト サービスに加えて、会員向けに無料スパイウェアのオンラインスキャン サービスを 2006 年 2 月から開始す

ることになりました。ISP からの会員向けのオンライン スパイウェア スキャンサービスは、米国では既に多くの ISP が提供していますが、日本では、初めてのサービスであることということも注目に値するでしょう。今後、こうしたセキュリティ サービスが ISP から提供されることで、対策の遅れがちな一般のインターネット ユーザーの多くを新しいセキュリティの脅威から守ることが可能になると考えます。

第 8 回

スパイウェアを撲滅するには?

要約

スパイウェア被害はますます増える一方です。このスパイウェアを撲滅する方法は無いのか考えてみます。

スパイウェアにおける最近の動向に

昨年 12 月から、「スパイウェア対策を名乗る」スパイウェアによる被害報告が増えてきました。それらの多くは、アドウェアに分類されるものですが、中にはトロイの木馬に分類されるものもあります。スパイウェアが脅威であることが一般に知られて来たことと、一方でスパイウェアそのものがいったい何か定義できないことでこうした被害が増えてきているのかも知れません。今回のテーマを進める前に、これら最新の動向についても報告しておきたいと思います。

SpywareStrike, SpywareCleaner, UnSpyPC,Winfixer, SpyAxe などが代表的なものです。当初これらは、悪質な偽スパイウェア対策ソフトウェアをユーザーが自身でダウンロードしてインストールすることで感染すると考えられていましたが、それだけではなく、他の無料のソフトウェアにバンドルされていたり、特に多い感染方法としてドライブバイインストールがあるようです。

これらのソフトウェアはダウンロードを可能にするためのいくつかのアフィリエイトサイトを持っていること、またそれらのサイトには、ドライブバイインストールを可能にする ActiveX スクリプトが組み込まれていたり、ブラウザのセキュリティ脆弱性を利用してインストールを可能にしていることで広まっているのではないかと考えられます。これらのサイトはまた、日本語のページや日本語化されたソフトウェアも配布していることも日本での感染が増えている原因と考えられます。

以下の対策を確実にすることを強くお薦めします。

- ブラウザで IE を利用している場合は、SP2 の適用に関らずアクティブ スクリプトを無効にするか、または実行前にプロンプトを表示するよう設定
- Microsoft からの最新のセキュリティパッチを随時適用すること
- ブロックリストなどの技術で不正な ActiveX コントロールを不活性化する。

スパイウェアガイドでの統計情報でも、12 月以降 Winfixer の検出と被害報告が増えています。これらの「スパイウェア対策ソフトウェアを名乗るスパイウェア」では、スパイウェアとはあまり関係のない一時ファイル、リンク先のないリンクファイル、ショートカットキーやクッキー ファイルをスパイウェアのように表現してユーザーの恐怖心を煽り、製品を販売するだけでなく、他のアドウェアやトロイの木馬をユーザーの知らない間にダウンロードするもの、またはアンインストールしても、完全にインストールされずに、コンピュータにセキュリティの脅威があると警告し、再インストールさせようとするものなどがあります。

最近の調査では、Winfixer はアドウェアだけでなく Vundo と呼ばれるトロイの木馬とも関連していると思われています。
Winfixer から感染する Vundo は、おそらく現時点では自動除去が不可能なトロイの木馬の 1 つです。これは winlogon.exe の子スレッドとしてカーネルレベルで実行されています。
こうした種類のスパイウェアをフォイストウェア(Foistware
http://www.shareedge.com/spywareguide/category_show.php?id=43)として分類することができます。

スパイウェアの目的は経済活動である

スパイウェアを技術的に捉えて、それに対抗する技術によりスパイウェア対策を行うことは、永遠に続くいたちごっこも思われます。技術的な対策は、技術の専門家に委ねるしかありませんが、IT 業界全体、または行政レベルでの対応も効果的であると思われます。
残念ながら現在の日本の IT 社会ではこうしたレベルの取り組みは行われていません。そのためユーザーは、常に新たな脅威から自分自身を守るために時間やお金を費やすことになります。
いつも説明していることですが、スパイウェアとは経済活動を目的とした脅威です。これはスパイウェアに限らず最近の IT への脅威は、スパムメールなどに見られるように経済活動が背景にあり、そこで生まれる経済効果が新たな技術を開発するために再投資されるわけです。

スパイウェア行為の抑止

従って、その目的である経済活動を絶つことがまさに、これらを絶つための究極の方法であるといえます。そのための対策を IT 業界や政府レベルで提供することではないでしょうか? スパイウェアの製作者だけではなく、配布したサイトやバンドルしたソフトウェアの製作者、また接続先 Web サイトなどを取り締まる仕組みを確立し、さらに罰金による処罰を科すことで、スパイウェアの配布が経済的活動としてもはや有効でないことを明確にし、抑止力を高めることが可能と思われます。下記に掲載された最近の米国の事例は非常に有効に思われます。そこではスパイウェアを配布した業者は、それで得た売上げと同額の賠償金を支払うことになったとのことです。
http://japan.internet.com/ecnews/20060106/12.html
日本ではこれらの法整備などを含め非常に遅れているのが実情で、急速な対応が必要となるでしょう。

訴訟された偽スパイウェア対策ソフトウェア

2006 年 1 月 25 日は、SpywareCleaner を販売していた Secure Computer が Microsoft などから訴訟されました。ワシントン州法によりニューヨーク州の会社、Secure Computer が訴えられていることも面白いのですが、この訴訟で注目すべき点は、どんな手法で Secure Computer 社が Spyware Cleaner を販売していたかではないでしょうか。
関連記事: http://www.idg.co.jp/ghl/cs/30602.html,

スパイウェアノート:
http://www.shareedge.com/spywareguide/txt_articles.php?article=txt_20060127.php

まず、Spyware Cleaner そのものですが、ソフトウェアには、アドウェアがバンドルされていることで、インストールしたコンピュータには、ポップアップ広告が表示されるようになります。また、ソフトウェア自身も簡単にアンインストールするだけでは削除されず、スタートアップに登録されたプログラムが自分自身を復活させる機能を持っているようで、除去が困難なソフトウェアです。また、インストールされると、ユーザーのセキュリティ設定をユーザーの知らない間に変更します。

販売方法については、ダイレクト メールを使ってまるで Microsoft 社からの製品であるかのように紛らわしい広告を配信したり、高額の報酬率で多くのアフィリエイトを利用したりしていたようです。あるアフィリイトは、Google などに検索キーワードに"Microsoft Anti-Spyware"などで有料リンクを登録することで、消費者を騙して彼らの Web サイトに誘導して販売していたようです。また、MS
Web サイトを訪問すると"スパイウェアに感染している"と警告を表示してユーザーを脅かして商品を販売する方法も利用していました。
また、MSN メンバーには、"MSN メンバーのための特別なセキュリティ アラート"として製品を広告するメールが配信されていたようです。

スパイウェア行為の抑止
この例にあるように、スパイウェアというより高度に洗練されたインターネットを使った商法が使われているため、訴訟はそれぞれ違反項目毎に罰金が加えられるようです。恐らく訴訟されるもの製品の開発元だけでなく、アフィリエイトや、メール配信業者にも及びます。
アフィリエイトでは、75%の報酬率だったそうなので、アフィリエイト パートナーによっては販売意欲をそそられる製品だったことは間違いないでしょうが、果たしてその製品が消費者によってどんなに悪影響があるのか無知のまま配信に協力したのかどうかも争点となるかも知れません。
について知らなかったかどうか。
技術的な観点からいうと、スパイウェアを撲滅することは、不可能といえます。理由は、それが常に進化する技術が使われるために、永遠のいたちごっこであるからです。しかし、高度な手法を使った過剰な販売行為は、すでにインターネット上で蔓延しています。法整備などを急速に進める必要があると思われます。
例えばアフィリエイトという手法は、一般に普及していますが、やはり過剰と思われるものが多く見られます。アフィリエイト パートナーが扱っている品物が何かを熟知することなく報酬率で選択するようになると、悪意を持った製品も一気に広がってしまう要因が常にあります。意図したかしていないかに関らず悪意を持った製品の配布に協力した業者の刑罰の対象になるような法整備が必要ではないでしょうか?