

コラム：スパイウェア対策を考える

「存在する不要なプログラムの種類と、ポリシー、ベストプラクティス、システム要件を理解し、その侵入を最小化すれば、スパイウェア対策の負担は軽減される。」

テリー・スウィーニー (Terry Sweeney)

「汝の敵を知れ」と忠告したのは、中国の兵法家、孫子でした。オンラインの有害なスパイウェアが一種の PUP (Potentially Unwanted Program: 不審なプログラム) として急速に拡大している今、この忠告は紀元前 500 年と同じように現在にも当てはまります。不審なプログラムが広く蔓延している状況に対処するためには、どのような問題に直面しているのか、そしてそれをどのような方法で回避したり、解消できるのかを知ることが重要です。また、ソフトウェア市場の現在の動向を理解し、堅固で長期的な防御を提供する最適なベンダーをお客様が選択できるようにすることも重要です。

「スパイウェア」は、トロイの木馬などの従来のマルウェアや、PUP の特徴をより多く備えたプログラムを含む包括的な用語となっています。PUP は、多くの場合ユーザに気付かれることなくステルス的に動作するソフトウェアです。害のない PUP も一部ありますが、大部分の PUP は、プライバシーやセキュリティに対して意図的または意図しない影響を持っています。

あるソフトウェアが望ましいものか潜在的に不審なものかの境界はどこにあるのでしょうか。McAfee® のグループマーケティングマネージャー、ジョン・ベドリック (John Bedrick) は次のように述べています。「その区別するのはお客様です。ユーザはインスタントメッセージにスマイリーアイコンを使いたいと思うかも知れませんが、その PC を所有している企業には、このような要望を却下する権利があります。お客様は、プログラムが各社の環境に必要な必要でないかを自ら決定できるソリューションを求めているのです。」

PUP についての基礎知識

PUP にはさまざまな種類があり、良い目的にも悪い目的にも使用される可能性があるため、変化しやすい性質を持つことがあります。ここでは、一般的な PUP について簡単に紹介します。

- **アドウェア**：ポップアップ、ポップアンダー、バナー広告などの広告を表示する PUP です。アドウェアは Web 閲覧の習慣を追跡する場合があります。アドウェアは通常、他のソフトウェアとともにインストールされ、ユーザはインストール時に、インスタントメッセージ (IM) などのフリーソフトウェアと引き換えに広告を受信することに同意します。アドウェアは一般的に大きなセキュリティリスクとはみなされませんが、コンピュータの処理速度を低下させる場合があります。
- **スパイウェア**：アドウェアと同様に、スパイウェアも、通常はフリーウェアやシェアウェアとともにインストールされたり、ポルノサイトをクリックすることでインストールされます。しかし、アドウェアとは異なり、スパイウェアはユーザや企業が知らないうちにデータを収集し、第三者に送信します。
- **ホームページハイジャッカー**：これは、ユーザのブラウザ設定を変更して新しいホームページ、検索ページ、またはエラーページ (ポルノ関係の場合が多い) を表示させる仕組みです。これらの PUP によって、ユーザのブラウザのお気に入り一覧も変更されることがあります。それ自体はセキュリティ脅威ではありませんが、お客様や同僚の目の前に変更されたページが表示されるのは厄介な問題です。従業員がわいせつに近いカレンダーやポスターを掲示したことで会社が訴訟を受けたり罰金を科されたケースがあることから、この「ハイジャック」ソフトは多くの企業が回避したい法的リスクの未対応領域となっています。
- **Cookie**：Web 閲覧の習慣や好みを追跡するために使用される簡単なテキストファイルです。無数の Web サイトのなかから Amazon.com を例に挙げると、このサイトは Cookie を使用することで、ユーザの次の訪問時に過去の検索や購入内容に基づいてお勧めの情報を表示します。この場合、Cookie は必ずしもセキュリティ脅威であるとは言えません。
- **キーストロークロガー (キーロガー)**：電子メール、IM の会話、Word 文書、オンラインバンキングなど、入力されたすべてのキーストロークを記録するソフトウェアです。このようなソフトウェアが知らないうち

にマシンにインストールされた場合、個人や企業は大きな問題を抱えることとなります。このような PUP の不正な側面は明白ですが、警察当局が証拠収集のために使用したり、企業が社員の挙動を監視するためにインストールする場合があります。

- **リモート管理ツール**：これらのツールを使用すれば、PC やサーバを乗っ取ることができます。これは、たとえばユーザが問題を抱えている場合に IT スタッフがその PC を制御してすばやく診断テストを実施できるといった状況では役立ちますが、ハッカーがコンピュータの制御を奪い、機密データにアクセスしたりマシンをスパム送信ネットワークに組み込んだりした場合は極めて危険です。

PUP 対策

まずは防御から

このような不審なプログラムの防御は、定期的なエンドユーザ教育、厳しい利用ポリシー、および企業の境界フィルタリングによって実現できます。「最初のステップは、最前線で防御することです。あなた自身がこのようなプログラムの入手を止めれば、あとから駆除について悩む必要はありません」とベドリックは述べています。

もう 1 つの効果的な防御手段は、ポリシーの実施です。これはユーザが自由に必要なプログラムをインストールしたり、好きなサイトをブラウズできるようにするよりもむしろ、ユーザの権利を一部制限することになります。企業は手始めにオペレーティングシステムの制限を有効にすることもできますが、McAfee Desktop Firewall、McAfee Intercept などのデスクトップファイアウォールやホストベースの侵入防御ソフトウェアを検討する必要があります。ベドリックは、「これらのソフトウェアは、設定したポリシーに基づいてマシンを確実にロックすることができる」と説明しています。

このような努力にもかかわらず、一部の PUP はそれでも検知を逃れて侵入するでしょう。ここで、ウイルス対策市場をリードするマカフィー製品がスパイウェア対策ソリューションをスマートに補完するのです。「ウイルス対策ソフトの最新のシグネチャファイルとスパイウェア対策プログラムを使用すれば、多数のプログラムをインストールされないようにブロックできる」とベドリックは述べています。企業は、個人やホームユーザができないこと、つまり境界防御の設置を実行できます。「それでもなお境界防御を通り抜ける PUP があるため、階層的なアプローチが必要である」と同氏は補足しています。

企業向けの設計

マカフィーのソリューションと多くの他社ベンダーのセキュリティパッケージとの違いは、ここにもあります。これらの多くは、個人やホームユーザを対象としています。ベドリックは次のように説明しています。「コンシューマ製品を採用し、いくつかの管理ソフトウェアを継ぎはぎして魔法の杖を振り、それをビジネスグレードのスパイウェア対策だと唱えても、満足のいくセキュリティを期待することはできないでしょう。企業のニーズは、その規模を問わず、事後ではなくソフトウェアの開発時に考慮に入れなければなりません。」

ベドリックは、セキュリティ管理コンソールを利用してスパイウェア対策製品やポリシーを管理することを企業に提案しています。これは特に、企業がウイルス対策ソフト、ファイアウォール、およびホストベースの侵入防御ソフトを導入している場合に有効です。「1 台で、これらのスイートすべてをシームレスに統合して管理でき、多数のアイコンが表示されることもない」と同氏は述べています。

中規模および大規模企業では、セキュリティ管理コンソールで、コンプライアンス管理、不正なマシンの検知、ポリシーの実施といったその他の関連機能も処理したいと考えるでしょう。本当にビジネスグレードのセキュリティと認められるためには、スパイウェアを含むすべてのセキュリティエージェントが自動的にアップデートされなければならないとマカフィーは確信しています。

「本当にビジネスグレードのセキュリティ製品を使用すれば、IT 部門は管理コンソールからエンドユーザにプッシュ型でアップデートを配信できる」とベドリックは述べています。このように、企業はエージェント駆動のアップデートを管理コンソールから起動して実行し、クライアントベースとシステムベースの両方をカバーすることができます。このようなアップグレードやアップデートの際には、ユーザに再起動やその他の操作を要求するべきではありません。

マカフィーは、本格的なオンアクセススキャン、アラート通知、および PUP ブロック機能を提供しています。さらに、24 時間 365 日のテクニカルサポートを提供し、5 大陸 13 か国に研究者を擁する世界有数のウイルス対策研究機関、AVERT (Anti-Virus Emergency Response Team: アンチウイルス緊急対策チーム) も配備しています。ソフトウェア市場のあらゆる分野が整理統合されている状況において、企業は、協業するベンダーが長期にわたってセキュリティ市場に存在するかどうかを判断する必要があるでしょう。