統合脅威管理によるスパイウェアの阻止

Sophos Positioning Paper
August, 2005

ここ数ヶ月間のスパイウェアの急激な蔓延により、組織が直面するセキュリティ脅威の被害も、ネットワークへの損害や機密情報の窃取、漏えいだけでなく、組織の信頼性の損失にまでつながるなど、深刻化しています。

このポジショニングペーパーでは、スパイウェアが組織に浸透する手段とその被害を食い止めるための対策を紹介します。また、セキュリティ分野で 20 年以上の経験と実績を持ち、数多くのアワードを受賞しているソフォスが提供する、スパイウェアを始めとするウイルス、トロイの木馬、ワーム、フィッシング詐欺、スパム、ポリシー違反などに対抗する技術をご紹介します。

スパイウェアとは？

スパイウェアは、組織の機密情報を搾取、破壊したり、ネットワークに侵入口を作ってより深刻な攻撃を加えるための体勢を作るなど、継続的で重大な被害をもたらす、悪意を持ったソフトウェアです。ユーザーを巧みに騙して、あるいはユーザーが知らないうちに自らをインストールさせてユーザーのコンピュータに侵入し、第三者に情報を送信させます。

アドウェアはポップアップメッセージなどによってユーザーのコンピュータに特定の広告を表示するものであり、スパイウェアとは異なるものとして扱われます。ユーザーの生産性とシステムの効率性を低下させるという問題点はありますが、あるユーザーにとっては必要な情報かもしれません。

「スパイウェアはセキュリティを脅かす不当なソフトウェアです。アドウェアは生産性を脅かす刺激物だといえます。ソフォスはスパムを 100%阻止します。将来的には Sophos Anti-Virus でアドウェア阻止の機能も提供する予定です。」
Sophos CTO（最高技術責任者）Richard Jacobs

急激に拡大する脅威

スパイウェアは、急激に蔓延し、新しい技術により常時拡大を続けます。

スパイウェアの脅威には以下が含まれます。

- **パスワード等の情報搾取**
  パスワードその他、個人情報を窃取します。
- **キーロガー**
  パスワードなどの情報を搾取する目的で、ユーザーのキー入力を監視します。
- **バンキングトロイの木馬**
  銀行の Web フォームなどへの接続を監視し、バンキング情報を窃取します。
- **バックドアトロイの木馬**
  システムを無防備化してハッカーによる侵入を可能とするバックドアを作るトロイの木馬。パスワード搾取、キーロガー、バンキング情報の搾取などを行う目的で使用されます。
- **ボットネットワーム**
  リモートで制御される複数のコンピュータを作り出すワーム。バックドアトロイの木馬のネットワーク。スパイウェアを感染させたり、ゾンビネットワークとしてスパムを配信したりするのに利用されます。
- **ブラウザハイジャッカー**
  ブラウザの設定を勝手に変更し、ユーザーを悪質な自動ダウンロードサイトに誘導したり、ブラウザのセキュリティ設定を緩和したりします。
- **ダイヤラー**
  高額な有料ダイヤルや国際電話に無断で接続させます。主にアダルトサイトへの接続が行われます。
- **ダウンローダー**
  ユーザーが気づかないうちにコンピュータに悪質なプログラムをインストールします。

組織にとっての脅威

スパイウェアはビジネスの連続性を多様な方法で脅かすため、組織にとって大変深刻な問題となります。

データ搾取

スパイウェアは重要な機密情報を搾取します。たとえば、パスワード情報窃取、キーロガーの特性を持つ Progent-A と呼ばれるトロイの木馬は、一度インストールされると、次にそのコンピュータがオンラインに接続されたときに情報送信を開始します。このようなスパイウェアは、金融情報やスプレッドシート、個人の記録、銀行口座番号とパスワード、その他感染したコンピュータに入力された情報などを搾取します。これによる被害としては、信頼性の損失、金銭の損失または競争力の低下、他者から訴訟されるリスクなどが考えられます。

ハッキング

スパイウェアはデータを窃取するだけでなく、ハッカーのために脆弱なコンピュータを生み出し、提供します。Feutel-L のようなバックドアトロイの木馬に感染すると、ハッカーによるリモート制御を許します。プロジェクトプランの消去、在庫情報の改ざん、アダルトコンテンツのダウンロード、マウスやキーボードの制御などがハッカーによって行われます。この種のセキュリティ攻撃では、何が行われるか予測がつかないため、IT 管理者にとっては、ウイルス以上に頭の痛い問題となります。

> *「全コンピュータの 67%がなんらかのスパイウェアに侵されていると考えられる。多くのマシンでは複数のスパイウェア亜種が発見されている。」*
> *IDC, Worldwide Spyware 2004-2008 Forecast and Analysis, 2004 年 11 月*

ゾンビアタック

ボットネットなどのスパイウェアはスパマーがスパムを配信するための手段としてしばしば活用されます。Sober-Q のようなトロイの木馬では、スパマーが脆弱性のあるコンピュータまたは Web サーバーを利用し、正当な配信元を使ってスパムメッセージを配信することを許します。ハイジャックされたコンピュータは「ゾンビ」と呼ばれます。ソフォスの調査によると、スパムの 60%以上がこのようなゾンビマシンから配信されています。その多くは正当な組織のネットワークに属しています。

ネットワークの被害

ネットワークのパフォーマンスは、スパイウェアの攻撃により大きな損害をこうむる可能性があります。ビジネスにおいては、対策や駆除に時間をとられるだけでなく、業務の中断や生産性の低下に直結します。

スパイウェアの侵入

スパイウェアはウイルスを使って、あるいはユーザーがメールに含まれる Web リンクをクリックしたり添付ファイルを開いたりすることによってインストールされます。多くのスパイウェアはインストールされる際にユーザーの介在を必要とするため、P2P ソフトなど一見有効なソフトウェアを隠れみのにしてユーザーにダウンロードを促します。あるいは、ポップアップメッセージで、ユーティリティを使用するために必要不可欠なソフトウェアであると表示してユーザーを惑わし、ダウンロードさせるスパイウェアもあります。その他システム、たとえば Web ブラウザの脆弱性などを利用してスパイウェアがインストールされるケースもあります。ユーザーが特定の Web サイトを訪れるか、HTML メールに含まれるメッセージを見るだけでスパイウェアがインストールされてしまう場合もあります。このような手法は “drive-by download”（自動ダウンロード）と呼ばれています。

スパイウェアの防御

基本ステップ

いかなるセキュリティ脅威に対しても、以下を組み合わせた基本的な対策が必須です。

- **教育**
  すべてのエンドユーザーがセキュリティ対策の重要性を理解し、メール添付ファイルを開いたりソフトウェアをダウンロードしたりインストールする際には十分な注意が必要であることを認識するように指導しなければなりません。
- **ポリシー**
  未認証のダウンロードが行われないことや、パスワードの効果的な使用が徹底されるよう、組織内でインターネットポリシーを策定し、施行しなければなりませ

ん。

- **テクノロジー**
  ブラウザやOSに最新のセキュリティパッチを適用し、ブラウザのセキュリティを正しく設定し、セキュリティソフトを常に最新に保たなければなりません。

ソフォスが提供する統合脅威管理

上記に挙げた基本的なセキュリティに加え、組織には、エンドポイントとゲートウェイのすべてを防御する統合脅威管理ソリューションが必要です。多様化、複雑化するウイルス、ワーム、トロイの木馬、スパム、フィッシング詐欺、ポリシー違反などを個々の脅威として捉えるのではなく、統合的な脅威として管理し、対策を講じることは大変重要です。

大手独立系テスト団体 WestCoast Labs、ソフォスに『スパイウェア認証』を授与。
ソフォスはスパイウェアをすべて検出して「Checkmark」を獲得。

スパイウェア認証の受賞は、ソフォスのウイルス対策ソフトウェアが、個別の脅威に対応するだけでなく、スパイウェアその他を組み合わせたセキュリティ脅威を統合的かつ効果的に阻止する、信頼性の高いソフトウェアであることを意味します。また、Sophos Anti-Virus の次期メジャーアップデート版であるバージョン 6.0 では、アドウェアを阻止する機能が標準で装備されることが予定されています。

ソフォスは、お客様に対し、今後も継続的に統合脅威管理のソリューションをご提供します。ソフォスラボが、ウイルス、スパイウェア、スパムに対し、マルチレベルでの防御を24時間/365日年中無休で提供し、メールポリシーの違反を阻止します。

その他、ソフォス製品およびソフォス製品を使ってネットワークを防御する方法の詳細につきましては、ソフォスのサイトをご参照ください。
www.sophos.co.jp

ソフォスとは

ソフォスは法人向けセキュリティ対策ソリューションの世界的なリーディング プロバイダです。グローバル企業、SMB市場、製造業、金融業、政府機関、教育機関など、あらゆる分野、規模の法人・組織をセキュリティ脅威から保護します。全世界150カ国以上で3,500万以上のお客様にご導入いただき、その高品質な技術力とサービスは高い評価をいただいております。

ソフォス株式会社
〒231-0062　神奈川県横浜市中区桜木町1-1-8 日石横浜ビル15F
Tel. 045-227-1800　　E-mail. sales@sophos.co.jp

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.CO.JP