スパイウェアの侵入
～情報漏洩の可能性～

八戸工業大学第一高等学校　情報科
○落合光仁、上野毅稔、沼尾敏彦、田名部俊成

ochiai@kodai1.ed.jp,t-uwano@kodai1.ed.jp,numao@kodai1.ed.jp,tanabu@kodai1.ed.jp

概　要　：本校では、DOS/V 機の製作実習を行っている。その様子を動画教材として授業に活用したいと考えていた。そのため高圧縮率で画像品質の高いコーデックを探していた。この時に「スパイウェア」の存在を知った。これが個人情報を洩漏してしまうプログラムであることが分かった。本校では「スパイウェア」に対しては未対策であったため、ウィルスと同等のレベルで全校をあげて対策に取り組んだことについて報告する。

１．はじめに

本校では情報システムコースでコンピュータを組み立てる授業を展開している。この作業手順やコンピュータを構成する部品などを撮影し、ストリーミングデータとして授業で活用したいと考えた。サーバのディスク容量などの問題から、高圧縮で比較的鮮明な画像が得られるビデオコーデックを探し、その導入作業を進めていた。作業の途中でスパイウェアの存在を知ることとなった。このスパイウェアを調べていくと、大変危険な要素を含んだプログラムであることが分かった。本校でも重要なセキュリティ対策の一つとし、全校をあげて対策に取り組んだことを報告する。

２．スパイウェアとは

スパイウェアはユーザーが知らないうちに勝手にコンピュータにインストールされ、特定のサーバに個人情報を送信するソフトウェアである。その多くは企業がホームページ閲覧者の閲覧履歴から、どのような情報に興味を持っているか探るなど、主にマーケティングのために利用されている。

例えば、知らない会社から電子メールが突然届いたり、画面にリクエストしていないホームページが勝手に開いた経験のある方もいると思う。このような場合、スパイウェアがパソコンに密かに侵入し、個人情報を悪意のあるユーザーに送信している可能性がある。

３．スパイウェアとウイルス

スパイウェアとウイルスはユーザーに迷惑行為をする意味ではほとんど違いがない。どれがスパイウェアでどれがウイルスなのか境界は灰色である。その大きな違いは、スパイウェアは二次感染せず、ウイルスは二次感染を繰り返し被害を拡大していくことである。最近ではスパイウェアもウイルスに近い動きをするものもあり、その存在を知らずにコンピュータを動作させインターネットに接続することは大変危険である。

４．スパイウェアの感染経路

■フリーウェアから感染

フリーウェア（特に外国製のものに多い）の中にはスパイウェアを含んでいるものがある。承諾画面が表示されインストールされるが、目立たないようにスパイウェアのことが書いてある場合が多い。多くのユーザーはスパイウェアの存在を意識せずインストールしてしまう。

例えば、DivXPro はMPEG-4 をベースにしたビデオコーデックである。このソフトウェアに広告会社 Gator 社(カリフォルニア州)のGAIN が同梱されている。

図1. GAINインストール

インストール時には図１のような画面が３種類表示され、それぞれ「ＧＡＩＮ の説明」「GAIN のプライバシーに関する説明」「GAIN のライセンス」が表示される。

GAIN の説明にはDivXPro がなぜ無料なのかや広告を画面に表示することなどが記載されている。

ＧＡＩＮ のプライバシーに関する説明には、クッキー情報を読むこと、その情報がサーバーに送られることが記載されている。

通常この文章を隅々まで読み納得してインストールしているユーザーは何人いるだろうか？

■ＡｃｔｉｖｅＸ を使用したインストール

ActiveX を利用してスパイウェアがインストールされる可能性がある。ＩＥ のセキュリティの設定が低い場合、ActiveX の付いているホームページにアクセスしただけで何の警告も無く勝手にインストールされる。

例えばCoolWebSearch と呼ばれるソフトなどはブラウザーを乗っ取る機能を持っている事が確認されている。非常に多くの変種が確認されているが、その多くに共通する動きは「coolwebsearch.com」の関連サイトを表示する機能やＩＥ の「信頼済みサイト」にデータを追加する機能がある。この機能により追加されたサイトからは、任意のコードを警告無しでダウンロードしインストールすることができるようになる。更に自分自身をバージョンアップすることも可能となる。また、多くのスパイウェアと同様に広告を表示する機能も併せ持っている。

■ＩＥのセキュリティホールを突くもの

Microsoft では次々に新しいセキュリティホールが見つかるため、WindowsUpdate だけでは１００％ 安全ではない。現状ではWindowsUpdate を迅速・確実に行うことが最善の策といえる。

５．スパイウェアの危険性

現在のところ、スパイウェアは違法ではない。DivXPro の様にソフトによっては、インストール時にスパイウェアが入ることを明記し、ユーザーに同意を求めている。

しかし、多くのユーザーは内容を読み飛ばしている。「説明が英語でよく理解できない」「読むのが面倒」などの理由で、知らないうちに導入されている。

スパイウェアを取り巻く問題を難しくしているのは、単なる「広告」からユーザーのタイピングを記録する「キーロガー」に至るまで、非常に幅広い範囲のプログラムが存在し、ユーザーの個人情報や会社情報の漏洩問題がクローズアップされている。

６．感染した場合の動作

①Web ブラウザが勝手に起動し広告を表示
②WebブラウザでHP を閲覧していると、別のインスタンスが開き広告が表示される。
③Web ブラウザのホームページが変更されている。
④[お気に入り]フォルダに勝手に登録されている。
⑤新しいツールバーがWeb ブラウザに追加されている。
⑥プログラムが起動できない。
⑦Windows やプログラムが機能しなくなる。
⑧無断で特定のソフトウェアを削除する。

ここに記述した主なスパイウェアの動き以外にも凶悪な物が存在する可能性がある。

７．その他のソフト

■Ｆｌａｓｈｇｅｔ（ダウンロード支援ソフト）

Cydoor が添付しオンラインで消費者の趣味や嗜好を追跡し，広告を流し込んでいることがある。

■Ｂａｂｙｌｏｎ（有名な翻訳ソフト）

Ｃｙｄｏｏｒ が添付しＣｙｄｏｏｒ を削除すると、Babylon が正常に作動しないことがある。

■GlobalDivX（ムービープレイヤー）
SaveNowが添付し、一般に「バグだらけで、通信を不安定にする」と言われている。オンラインユーザーのアクセス先を監視し，その後ターゲット広告や特別サービスなどを掲載した別のブラウザウィンドウをポップアップする動きがある。
■RadLight（マルチメディア再生ソフト）
インストールすると、スパイウェア駆除ツールとして有名なAd-awareを、ユーザーに無断でアンインストールする。

８．スパイウェア駆除

スパイウェアの駆除には非常に難しい問題がある。主な理由の一つは、インストール時にユーザーの承諾を得ているため、スパイウェア対策ソフトで簡単に駆除することができない。

現在、スパイウェア対策ソフトで検出されたスパイウェアはユーザーの判断で駆除できる様になっている。しかしソフトの配布者は「配布者とユーザーが契約してインストールしたソフトを、スパイウェア対策ソフトが駆除することは、契約行為を妨害するもの」として厳重に抗議している。

これに対し、スパイウェア対策ソフトの作者側は「一般ユーザーが簡単にアンインストール出来ない反社会的ソフトである」と主張している。この主張を受けて最近のスパイウェアはアンインストールができるものが出てきている。

日本の例では、NECが採用した「JWord」というツールバーがあるが、このソフトも最近では[プログラムの追加と削除]でアンインストール出来るようになっている。

今後、スパイウェア対策ソフトの作者側は、スパイウェアを削除し続けると損害賠償の訴訟を受ける可能性が出てきている。

このような事情からスパイ対策ソフトで駆除できないスパイウェアも存在するようになってきた。そこで専用の駆除ツールが必要になるが、無料で高性能な駆除ツールとして「Spybot-S&D」と「Ad-aware」がある。簡単に言えば「Spybot-S&D」は狙い撃ちタイプ、「Ad-aware」はパターンサーチタイプである。この駆除ツールはお互いに得意不得意があり駆除の時には両方の駆除ツールを使いスパイウェアを駆除する必要がある。また、CoolWebSearchは「Spybot-S&D」や「Ad-aware」では対応しきれない悪質なスパイウェアで「CWShredder」という専用の駆除ツールが存在する。

９．本校での取り組み

本校では、ウイルス対策と同レベルで対応が必要と判断し、全校あげて対策に取り組んでいる。校内ネットワークに接続しているコンピュータは全てウイルス駆除ツールとスパイウェア対策ソフトの導入を義務づけている。しかし、スパイウェア対策ソフトはユーザーが起動させ駆除するタイプである。このためユーザーが意識的に使いスパイウェアの発見、駆除をしなければならない。

写真１．　教職員向け講習会風景

本校では校内ネットワーク利用者にスパイウェアの存在を知ってもらうため、教職員対象の講習会を開いた。全教職員にスパイウェアの存在を認識し、その対策を理解してもらうよう働きかけた（**写真１**）。

本校のコンピュータをAd-awareで確認した結果、あるコンピュータからは162個のスパイウェアらしきオブジェクトが確認された。本校では平均５０個ものスパイウェアらしきオブジェクトが確認されその数の多さに驚いている。また個人のノートパソコンからも最大４４個のスパイウェアらしきオブジェクトが確認されている。

スパイウェアはバックグランドで動作していることが多く、スパイウェアが動作したときの動きを確認するために動作、駆除実験を行った。

図2. Ad-aware で確認

スパイウェアはDivXPro についてくるGAIN をインストールする。インストール時には図1 の様にデータをサーバーに送る事の書かれた承諾書が表示される。

図3. DivXPro のインストール

実際にインストールした後にＩＥ を使いインターネットを閲覧していると図４ の様に宣伝ページが表示された。

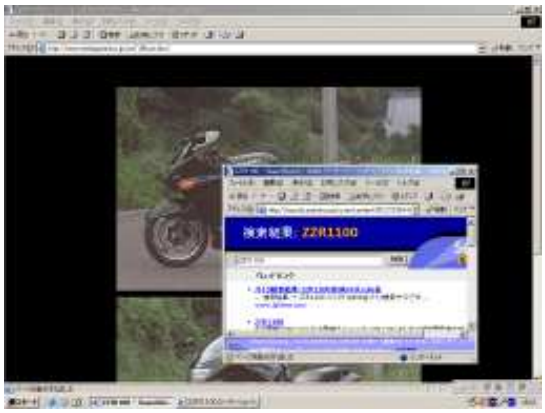

図4. GAIN の起動

その後「Spybot-S&D」と「Ad-aware」でスパイウェアの確認をしたところＧＡＩＮ が確認することができた。その後ＧＡＩＮ を駆除したところＤｉｖＸＰｒｏ による圧縮編集ができなくなっていた。

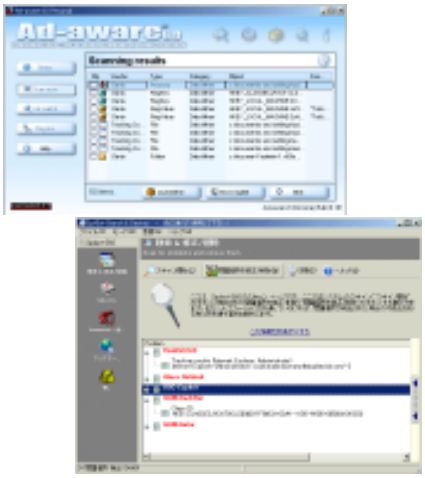

図5. GAIN の確認

１０．まとめ

ビデオコーデック選定作業からスパイウェアの存在を知り、その対策に全校を上げて取り組んだ。教職員に対しては研修会を実施し、研修会前には「スパイウウェアって何？」「こんなにスパイウェアなどが氾濫していてはコンピュータを使えなくなる」との声も聞かれたが、研修会後には「正しい知識と対策方法を知っていれば問題ない」との声に変わっていた。また、実際にコンピュータにスパイウェア対策ソフトを導入し「数十個スパイウェアが入っていたよ」と報告を受ける場面も生まれている。また生徒に対しては、ネットワーク技術や実習などの授業を通して、その恐ろしさを考えさせている[2]。

今後も新しい凶悪ソフトウェアが出現すると思うが、情報を収集し教職員や生徒に還元していく必要性を強く感じた。

参考文献

[1]スパイウェア関連のトピックス
http://higaitaisaku.web.infoseek.co.jp/menu5.html
[2]ASAHI パソコン2004.2/15 号,P74
[3]青森県高教研工業部会発表資料，落合他
2004.1