

4W-3

インターネットのスパイウェア汚染度に関する予備調査と分析

岡崎 創十 棟上 昭男十
東京工科大学メディア学部メディア学科十

1. はじめに

技術は日々進歩し、インターネットからアクセスできる Web サイトは、とても便利である。さまざまな悪事を働く人おり、インターネット社会の脅威となっている。その一つとされているのが、スパイウェアの存在である。

スパイウェアとは、他人のコンピュータに無断で侵入し、勝手に個人情報を漏洩するなど、悪質な動作を行うプログラムである。

インターネットの Web サイトを閲覧したときに一体どのようなスパイウェアが、どの程度コンピュータに侵入するのかを調査したので、報告する。

2. スパイウェア(Spyware)

スパイウェアは、不特定人物や不特定な存在が、コンピュータの使用者あるいは、所有者に知られることなく、それらのコンピュータに個人情報を漏洩するように仕向けるなど、悪質な動作に利用される可能性のあるソフトウェアである。[1]

スパイウェアには、次のような種類のものがある[2]。

- ・アドウェア(adware)
- ・ブラウザチェンジャー(browser changer)
- ・ブラウザプラグイン(browser plug-in)
- ・バンドルウェア(bundleware)
- ・キーロガー(keylogger)
- ・ダイヤラー(dialer)

3. Web サイトにおけるスパイウェアの調査

3.1. 調査環境

VMware Workstation5.5 を用いて、仮想コンピュータシステムを実現した。その上に、WindowsXP HomeEdition SP2 を搭載した。

アンチスパイウェアとしては、フリーソフトの

Spybot-Search&Destroy!を用いる[3](図1)。

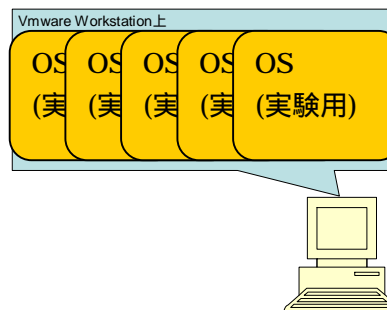


図1 調査環境

3.2. 調査対象の Web サイト

インターネットには、さまざまなサービスを提供している Web サイトがある。本研究では、1種類のサービスごとに100サイトずつ調査を行い、目標10種類のサービス、合計1000サイトを目標に調査を行う。なお、1000サイトは、スパイウェアが潜んでいそうなサイトを選んだ。現在、Screensaver サイト、Game サイト、Music サイト、Software サイトの4種類のサービスにおいて、調査が完了した。

3.3. 調査手順

Web サイト閲覧時にどれくらいのスパイウェアがコンピュータに侵入するかを検出する。図2のような調査手順で行った。

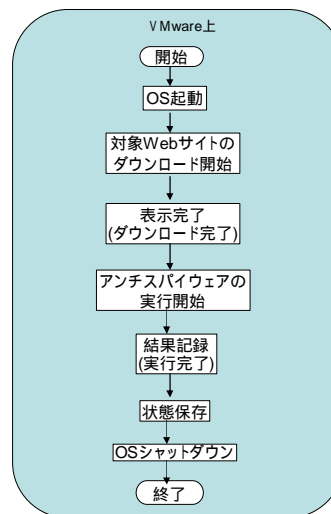


図2 調査手順

3.4. スパイウェアの検出調査

現在、Screensaver サイト100サイト、Game サイト100サイト、Music サイト100サイト、

Software サイト100サイトの調査を完了している。Screensaver サイトは、100サイト中34サイトからスパイウェアの侵入が見られた。また、Game サイトは、100サイト中36サイトからスパイウェアの侵入が見られた。Music サイトと Software サイトに関しては、100サイト中24サイトからスパイウェアの侵入が見られた。

100サイト中36サイトと4種類のサービスのうちもっともスパイウェアが検出された Game サイトのスパイウェアの結果が、図3である。

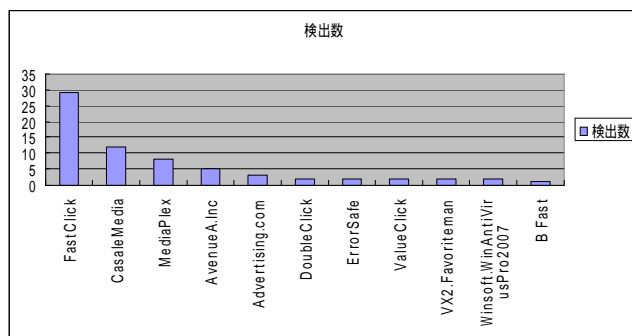


図3 Game サイトから検出されたスパイウェア

Game サイトだけで総数68個のスパイウェアが検出された。Software サイト以外からは、Spybot-Search&Destroy!の場合、ファストクリック(FastClick)というスパイウェアがもっとも多く検出された。

ファストクリックとは、マーケティングのために一般ユーザのネットサーフィンの習慣についての情報を貯えるトラッキングクッキー(Tracking Cookie)である。ファストクリックのクッキー(Cookie)は、本来有害でないが、容易に開発され、誤用することができる。機密情報を集めるときのセキュリティ問題を提起する可能性がある[4]。

トラッキングクッキーは、クッキーの中でも悪質な動作をするものに分類される。スパイウェアとして定義される悪質な動作をするクッキーのことをスパイウェアクッキー、トラックウェアクッキー、トラッキングクッキー、追跡クッキーなどとも呼ばれている。スパイウェアとして定義されるクッキーは、クッキーを複数のサイトで利用し、一般ユーザの個人情報を収集することを目的として、複数の無関係なサイト間で共有されるクッキーのことである。このクッキーは、異なる多くのWebサイトを閲覧するユーザの嗜好を追跡し、マーケティング目的に利用される。このクッキーによって収集された情報により、広告配信会社が一般ユーザに向けて、配信する広告をコントロール

する場合などに用いられている[4]。

そもそもクッキーとは、インターネットのWebサービスにおいて、WebブラウザとWebサーバの間での暗黙の情報交換を行うための仕組みである。Webサーバからの指示によって、Webクライアント側で作成され、保存される。このときクライアント側に保存されるデータは、クッキーの名前と値、クッキーの有効期限、有効ドメインパスである。一見すると便利なクッキーだが、クッキーの情報はクライアント側に暗号化されずに記録されるので、一般ユーザが改竄することは容易で、これを悪用すれば、他人になりすましてWebサーバにアクセスできてしまうという問題がある。

トラッキングクッキーの対策としては、Internet Explorer の設定によるクッキー制御や定期的に全てのクッキーの削除があげられる。

4. 考察

Webサイトを閲覧調査した結果、多くのスパイウェアがコンピュータに侵入していることが分かった。ほとんどのスパイウェアが、トラッキングクッキーであり、ユーザの嗜好を分析し、ユーザの好むポップアップ広告を表示するというアドウェアの一種である。これは、コンピュータのパフォーマンスを著しく低下させるものではないようだが、油断はできない。トラッキングクッキーの侵入を防ぐのが今後の問題であると考えている。

本研究では、現在400サイト調査を完了した。全国大会当日までに残り600サイト、6種類のサービスについて調査をしたい。

5. 参考文献

- [1] Roger Thompson: Why Spyware Poses Multiple Threats to Security, Comm.ACM, Vol.48, No.8, pp6-8 (2005)
- [2] Sudhindra Shukla AND Fiona Fui-Hoon Nah: Web Browsing AND Spyware Intrusion, Comm.ACM, Vol.48, No.8, pp50-57 (2005)
- [3] The home of Spybot-S&D!
<http://www.safer-networking.org/>
- [4] Anti-Spyware101
<http://www.anti-spyware-101.com/japanese/>