スパイウェアガイド スパイウェア検出統計情報の分析
2005 年 3 月 11 日から 2005 年 11 月 17 日までの報告

Rev. 0.1

Last update 11/17/2005 nextEDGE Technology

この技術白書は、2005 年 3 月 11 日から 2005 年 11 月 17 日の期間におけるスパウェアガイド（ www.spywareguide.jp)で収集した日本国内におけるスパイウェア検出統計情報を分析し、まとめたものです。

統計情報の対象:

3/11 から 11/18 の累計ダウンロード数: 447,590 件（ある日のダウンロード数 3,034 件 8/26(金)）
検出件数 321,032 件　検出率 78%

3/11 から 9/20 の累計ダウンロード数: 412,449 件（ある日のダウンロード数 3,034 件 8/26(金)）
検出件数 321,032 件　検出率 78%

最も多く検出されているスパイウェアの分析::

検出件数での統計情報では、アドウェアと分類されるスパイウェアのみが見られます。これは、スパイウェア検出全体の 86%近くがアドウェアであることからも理解できます。以下に、これらのスパイウェアに関する個々の解説を記述しました。

- CnsMin は日本でのみ目立って見られるスパイウェアです。JWORD により配布されているプラグインに含まれています。多くのウィルス対策ソフトウェアのスパイウェア検出ではこのモジュールの検出は除外されています。

  除去するか、利用するかについての判断はユーザまたは企業の IT 管理者に任せる必要があります。日本では最近一部の PC メーカがこれをプリインストールして出荷していることも広がりの要因の1つと思われます。

  セキュリティの脅威はありせんが、プライバシ侵害の可能性があります。

- Gator 米国の広告会社 Claria により世界的に配布されているアドウェアです。

  セキュリティの脅威はありせんが、ポップアップや PC の性能低下を引き起こします。

- About Blank, ISTBar は、ブラウザハイジャカです。ブラウザだけでなくコンピュータの操作もハイジャックし、ユーザが思うように操作できなくなります。

除去が非常に困難です。

- Alexa Toolbar は、実際 Alexa ツールバーをインストールしていない環境でも検出されます。恐らくレジストリ情報の痕跡のみを検出しているケースです。

- CoolWebSearch は、もっとも悪名の高いスパイウェア(ハイジャッカ)です。CoolWebSearch を利用して多くのスパイウェアが配布されるため、異形が多く存在します。CoolWebSearch により配布されるトロイの木馬も存在します。
  除去が非常に困難です。時に、セキュリティの脅威があります。

表 1 最も多く検出されているスパイウェア

スパイウェア名	検出通知数	危険度
CnsMin	67,608	アドウェア
Gator	27,329	アドウェア
BonziBuddy (↑)	23,871	アドウェア
About Blank	19,947	アドウェア
Internet Optimizer (↑)	19,009	アドウェア
ISTbar (↑)	14,771	アドウェア
CoolWebSearch (↑)	14,702	アドウェア
Alexa Toolbar (↓)	14,403	データマイナ
Cydoor (↑)	8,439	アドウェア
SyncroAd	8,285	アドウェア
180 Search Assistant	8,036	アドウェア
DashBar (↑)	7,272	アドウェア
BDE (↑)	6,724	アドウェア
BHO.NovoPops(New)	6,458	アドウェア
QuickSearch Search Bar	6,177	アドウェア
EliteBar	6,099	アドウェア
Windupdates	8,903	アドウェア
Search Assistant	4,712	アドウェア
Media Pass	5,726	アドウェア
XDialer	5,262	ダイヤラ

カテゴリ別分析

トロイの木馬は、アドウェアのダウンロードなどにも使われますが、リモートアクセスのためのバックドアを準備したりするものもあり、セキュリティ脅威としてはすべて高いレベルのものであると考えられます。

特に注目するのは、Srv.SSA-KeyLogger は、新しいもので、また多く検出されています。セキュリティ ソフトウェアを攻撃するもので、非常に危険です。

表 2. トロイの木馬検出ランキング

スパイウェア名	検出通知数	危険度
Win32.Dyfuca.a	4,652	トロイの木馬
Trojan.Desktophijack	1,637	トロイの木馬
Bamer Trojan	1,072	トロイの木馬
eXact Downloader	647	トロイの木馬
Prutect (↑)	508	トロイの木馬
Trojan.Puper (↑)	447	トロイの木馬
Srv.SSA-KeyLogger (New)	377	トロイの木馬
Topconverting (↑)	375	トロイの木馬
Trojan.Win32.FTP Attack (↓)	368	トロイの木馬
Topconverting	375	トロイの木馬
Conscorr	341	トロイの木馬
Trojan-Clicker.Win32	222	トロイの木馬
StartPage (↑)	217	トロイの木馬
Ghost	212	トロイの木馬

最近の傾向:

a. Dropper.BallonPop, WinFixer に見られるような、スパイウェアをダウンロードするトロイの木馬が多く見られますこれらのスパイウェアがインストールされてしまうと、さらに複数のスパイウェアを呼び込むことになり、除去も困難になります。

b. スパイウェア Aurora は、アドウェアですが、これも除去が非常に困難なスパイウェアとして対応に難航しました。

c. 海外では、新規のスパイウェア対策ソフトウェアが増加しています。これに便乗して、スパイウェア対策を名乗った悪質なアドウェア機能を持つソフトウェアや、偽のスパイウェア検出警告と表示し、除去するために有料でソフトウェアを購入させるものまであります。

最近追加されたスパイウェア

例えば11/1から11/18までの間に追加されたスパイウェアの件数は、20件。1日 1.2件。この数字は、ウィルスの新規追加数を超えるものです。

表 3 最近追加更新されたスパイウェア

NeededWare	2005-11-17
Powwabar	2005-11-17
enBrowser	2005-11-17
SpyBot-CY	2005-11-17
Downloader-MSB	2005-11-17
Sexxxpassport	
Plug-in	2005-11-16
Dropper.BallonPop	2005-11-14

その他

新しいバージョンのウィルス対策ソフトウェアがスパイウェア対策機能を強化して発表になり、出荷が開始されました。残念なことに、パターンマッチングに依存した、ウィルス対策ソフトウェアが誤検出をしているという報告がユーザからありました。

例：

eTruct PestPatrol 11/03 シグネチャが X-Cleaner(日本語版)インストーラを"Zango"として誤検出

X-Cleaner インストーラを Trojan.Win32.Dialer.hc として誤検出