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 9 月 24 日までの報告

Rev. 1.1

Last update 10/10/2005 nextEDGE Technology

この技術白書は、2005 年 3 月 11 日から 2005 年 9 月 24 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 9/24 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 80%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	45,101	アドウェア
Gator	19,343	アドウェア
About Blank	16,524	アドウェア
BonziBuddy	15,471	アドウェア
Alexa Toolbar	12,907	データマイナ
Internet Optimizer	10,990	アドウェア
CoolWebSearch	10,691	アドウェア
ISTbar	10,454	アドウェア
SyncroAd	6,986	アドウェア
n-Case	6,458	アドウェア
Cydoor	6,222	アドウェア
QuickSearch Search Bar	6,072	アドウェア
EliteBar	5,512	アドウェア
DashBar	5,461	アドウェア
Windupdates	4,944	アドウェア
Search Assistant	4,712	アドウェア
BDE	4,678	アドウェア
Media Pass	4,133	アドウェア
XDialer	3,974	ダイヤラ
Wareout	3,770	アドウェア

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。

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	3,359	トロイの木馬
Trojan.Desktophijack	1,036	トロイの木馬
Bamer Trojan	1,020	トロイの木馬
eXact Downloader	400	トロイの木馬
Trojan.Win32.FTP Attack	366	トロイの木馬
Prutect	310	トロイの木馬
Topconverting	307	トロイの木馬
Trojan.Puper	276	トロイの木馬
Conscorr	249	トロイの木馬
Ghost	211	トロイの木馬
Trojan-Clicker.Win32	165	トロイの木馬
Trojan Krepper-G	151	トロイの木馬
Trojan.StartPage	139	トロイの木馬
ICQ Trojan	135	トロイの木馬
StartPage	113	トロイの木馬
ABox	101	トロイの木馬
MagicControl	101	トロイの木馬
Backdoor.Thunker	88	トロイの木馬
Small-RN	68	トロイの木馬
Trojan Relaid	57	トロイの木馬

最近の傾向:

a. IRC(Internet Relay Chat)トロイの木馬を利用して、自動的に生成された悪意のあるリンクをクリックすることで感染(インストールされる)するスパイウェア技術が新しく報告が多くなっています。

例:**Career12**

http://www.shareedge.com/spywareguide/product_show.php?id=2193

b. 同様に、Rootkit と呼ばれるステルス機能を持つトロイの木馬への対応も必要です。

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 9/1 から 9/22 までの間に追加/更新されたスパイウェアの件数は、98 件。1 日 4.5 件。この数字は、ウィルスの更新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

2248	Maxsearch	2005-09-22 13:25:58
2137	Shorty	2005-09-22 11:58:52
2265	Downloader-RF	2005-09-22 11:07:06
2264	Downloader-BR	2005-09-22 10:33:07
1387	Ciador	2005-09-21 11:47:11
2262	NTRootKit-H	2005-09-21 08:24:04
2261	NetVision	2005-09-21 07:56:31
1102	Quick Keylogger	2005-09-21 01:06:04
647	764 Dialer	2005-09-20 12:12:04
1814	4Arcade PBar	2005-09-20 11:55:21
1763	ErrorGuard	2005-09-16 15:17:27
1284	404Search	2005-09-16 13:57:22
2193	Career12	2005-09-16 13:54:22
2253	DT.dl-VR	2005-09-16 13:50:43