Spywareguide.com 日本語版
スパイウェア対策はスパイウェアを知ることから...

www.shareEDGE.com/spywareguide/

nextEDGE Technology, Inc.

Apr. 6 2005

Rev .1

スパイウェアガイド

スパイウェアガイド Webサイト
- 可能な限り商用目的を排除し、一般ユーザ向けにスパイウェア脅威に関する啓蒙と、スパイウェアへのユーザレベルでの対応を目的として運営

■ スパイウェア検出情報
- X-Cleanerから報告される検出結果をリアルタイムに集計、報告
- 唯一の日本国内でのスパイウェア検出統計情報

■ スパイウェア情報データベース – スパイウェア照会
- X-Cleanerで定義されているスパイウェア情報のデータベースを日本語で紹介(日本語作業中)

■ スパイウェア ノート
- スパイウェアに関する情報を、私見を含み提供

■ メンバーシップ(無料)
- 最新版Xcleanerのダウンロード、追加ライセンス販売(個人向け)
- メンバーのみの情報の提供

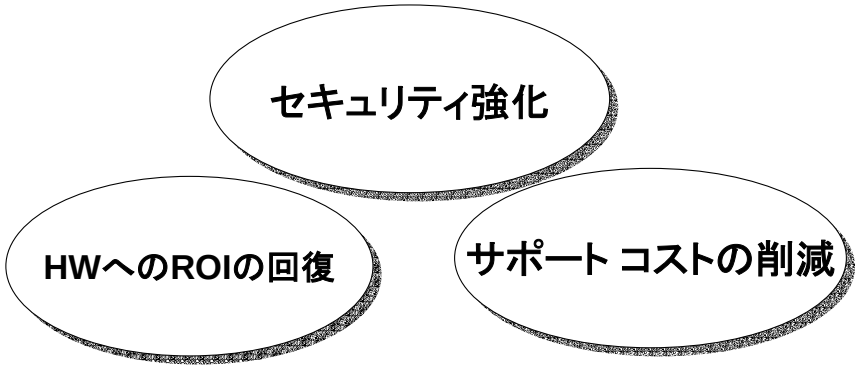
ウィルスとスパイウェアの違い

- 狭義のスパイウェアと広義のスパイウェア定義
  - ウィルスベンダの定義するスパイウェアは狭義のスパイウェア
  - BHO,アドウェア、ハイジャッカ、Active-Xコントロールを含まない
- アンチスパイウェア ベンダのスパイウェア定義
  - ユーザの知らない間に、インストールされ、知らないことを実行するソフトウェア
  - アンインストールが複雑なソフトウェア
  - ユーザのプロファイルを収集し、知らない間に外部に送信するソフトウェア
- アウパイウェア対策には
  - ウィルス対策とは全く違う検出、除去技術が要求される

スパイウェア対策の必要性

スパイウェア対策の必要性

スパイウェア対策ソフトウェアの導入による3つベネフィット



セキュリティ

インターネット盗難防止

キーロガーを利用してユーザのアカウント情報を盗み、さらにそのアカウントを利用して個人のインタネート上の資産が盗難される事件が多く発生しています。

- 検疫サービス - メンバー サイトなど個人情報へのアクセス前に、キーローガーなどがユーザのコンピュータに侵入していないかを簡単にチェックするサービス
- インターネットバンク
- クレジットカード情報の入力

キーロガーには、HWタイプも存在している
- VPN/SSL/暗号化しても、別のレベルで情報を盗難できる
-公共のネットカフェなどに、第3者が仕込む
-家庭内で、親が子供に、子供が親に…

アドウェアの被害としては、パーフォマンスの低下、システムの不安定化
企業にとっては、HWへの投資効果に影響する深刻な問題
企業内のPCは100%その能力を発揮しているか?

サポート コスト

ISP / IT管理 テクニカル サポートコスト

スパイウェアに関する知識を得て、また適切なツールを持つことでテクニカル サポートに掛かる経費を軽減することができます。

E. テクニカル サポート コールセンタでのスパイウェアに関わる費用（2004年FTCスパイウェアワークショップから)

- 問題が発生すると、消費者はISP、OS製造元、またはPC製造元のテクニカル サポート センターに連絡します。Dellの報告では、スパイウェアは、2003年終わりにはテクニカル サポート スタッフへの電話中で1番目のカテゴリとしています。同様に、McAfeeは、スパイウェアは大きなテクニカル サポートの問題であり、過去のウィルスを越えるものであるとしています。DellやMcAfeeではスパイウェアに関するコールは、テクニカル サポート コール全体の10％から20％に達しています。
- ISP関係者はこれらのコールへの対応に掛かるコストが実際にビジネスに影響を与えていると報告しています。1つの理由として、スパイウェアに関するテクニカル コールは一般に、通常のテクニカル サポート コールよりも時間が掛かることがあげられます。それは多くの場合、消費者は、スパイウェアが原因していることを知らないこと、その上でテクニカル サポートは問題の原因をトラブルシューティングしなければならないためです。あるパネリストは通常のISPへのテクニカル サポート コールおよそ5分掛かり、スパイウェアに関するコールの平均は約25分、これはコールに関わるコストを$15ほど引き上げています。なぜならISPのユーザは、標準的に$20から$40を月額インターネット アクセスに支払っていて、それらテクニカル サポート コールはISPのプロフィット マージンを深刻に減少させています。

キーロガーには、HWタイプも存在している
- VPN/SSL/暗号化しても、別のレベルで情報を盗難できる
-公共のネットカフェなどに、第3者が仕込む
-家庭内で、親が子供に、子供が親に…

アドウェアの被害としては、パーフォマンスの低下、システムの不安定化
企業にとっては、HWへの投資効果に影響する深刻な問題
企業内のPCは100%その能力を発揮しているか?

ハードウェアROIの回復

ハードウェアへのROIの回復

たとえ、最新のコンピュータをビジネス環境に導入したとしてもスパイウェアによりその本来の性能が100％発揮されていないとしたら、それはハードウェアへの投資効果は結果的に100％得られていないことになります。スパイウェアを除去することでパフォーマンスを回復することは、ハードウェアへの投資効果を回復することをいえます。

(FTCからの報告より)

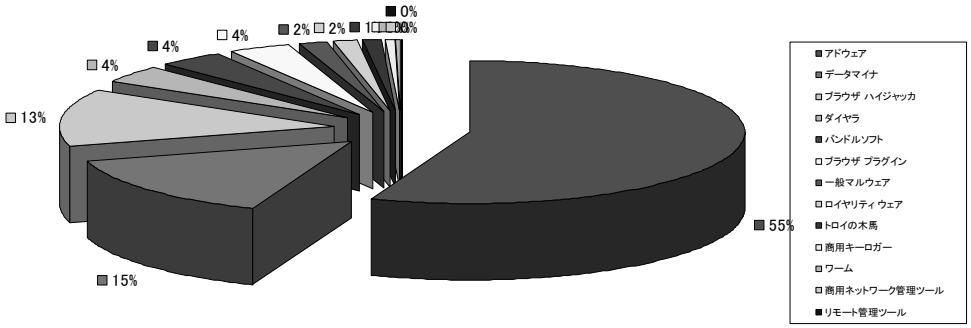
- スパイウェア プログラムは、しばしばシステム動作性能に多大な影響を及ぼします。コンピュータの動作性能を過大に低下させる現象は、最も多いスパイウェアに関連した被害の苦情は、コンピュータ製造メーカ Dellの受けたもので、すべてのスパイウェア関連の苦情の1/4以上あったと2004年4月時点での結果でした。スパイウェアは、またコンピュータをクラッシュさせることがあります。Microsoftでは50％のユーザのコンピュータ クラッシュはスパイウェアに起因したものであると報告しています。パネリストによると、あるスパイウェアは、多くのシステム リソースを消費し、ユーザはもはやマウスを使ええなくなったり、カーソルがフリーズした状態に陥ってしまうと報告しています。

キーロガーには、HWタイプも存在している
- VPN/SSL/暗号化しても、別のレベルで情報を盗難できる
-公共のネットカフェなどに、第3者が仕込む
-家庭内で、親が子供に、子供が親に…

アドウェアの被害としては、パーフォマンスの低下、システムの不安定化
企業にとっては、HWへの投資効果に影響する深刻な問題
企業内のPCは100%その能力を発揮しているか?

カテゴリ別スパイウェア

報告されているスパイウェアの55%はアドウェア



2005年4/6日集計

最も多く報告されているスパイウェア

最も多く検出されているスパイウェア トップ20

- Alexa Toolbar データマイナ (最終報告日付:2005/04/05 12:01:04)
- CnsMin アドウェア (最終報告日付:2005/04/05 12:01:20)
- QuickSearch Search Bar アドウェア (最終報告日付:2005/04/05 12:03:47)
- Gator アドウェア (最終報告日付:2005/04/05 12:02:25)
- About Blank ブラウザ ハイジャッカ (最終報告日付:2005/04/05 11:58:07)
- CoolWebSearch ブラウザ ハイジャッカ (最終報告日付:2005/04/05 11:42:43)
- EliteBar アドウェア (最終報告日付:2005/04/05 12:01:38)
- Bearshare バンドルソフト (最終報告日付:2005/04/05 11:59:11)
- ISTbar ブラウザ ハイジャッカ (最終報告日付:2005/04/05 12:00:33)
- DashBar アドウェア (最終報告日付:2005/04/05 09:07:32)
- BonziBuddy アドウェア (最終報告日付:2005/04/05 11:57:59)
- Cydoor アドウェア (最終報告日付:2005/04/05 12:03:00)
- XDialer ダイヤラ (最終報告日付:2005/04/05 08:11:26)
- Internet Optimizer アドウェア (最終報告日付:2005/04/05 12:01:20)
- n-Case アドウェア (最終報告日付:2005/04/05 12:02:42)
- WebRebates ロイヤリティ ウェア (最終報告日付:2005/04/05 11:47:44)
- BDE アドウェア (最終報告日付:2005/04/05 10:54:47)
- SyncroAd アドウェア (最終報告日付:2005/04/05 12:04:49)
- Precision Time アドウェア (最終報告日付:2005/04/04 23:36:07)
- DownloadWare アドウェア (最終報告日付:2005/04/05 12:01:32)

危険度の高いスパイウェア

危険度の高いスパイウェア トップ20

- FreeWire バンドルソフト (最終報告日付:2005/04/03 15:22:03)
- CoolWebSearch ブラウザ ハイジャッカ (最終報告日付:2005/04/05 11:42:43)
- Forbot トロイの木馬 (最終報告日付:2005/04/04 08:30:30)
- ICQ Trojan トロイの木馬 (最終報告日付:2005/04/03 12:45:33)
- ComputerSpy 商用キーロガー (最終報告日付:2005/03/24 18:47:44)
- NetSky ワーム (最終報告日付:2005/04/04 22:01:40)
- Album Galaxy バンドルソフト (最終報告日付:2005/04/02 07:06:28)
- Sysupd ダイヤラ (最終報告日付:2005/03/29 20:48:28)
- MarketScore データマイナ (最終報告日付:2005/04/02 07:14:31)
- Blaster Worm ワーム (最終報告日付:2005/04/04 22:36:15)
- xxxtoolbar アドウェア (最終報告日付:2005/04/03 12:09:30)
- Websearch アドウェア (最終報告日付:2005/04/03 20:27:51)
- Trojan.Win32.FTP Attack トロイの木馬 (最終報告日付:2005/04/05 02:04:19)
- AdBreak アドウェア (最終報告日付:2005/03/26 22:17:27)
- Small-RN トロイの木馬 (最終報告日付:2005/04/02 14:27:08)
- Sidefind アドウェア (最終報告日付:2005/04/05 11:47:31)
- About Blank ブラウザ ハイジャッカ (最終報告日付:2005/04/05 11:58:07)
- BadTrans.B ワーム (最終報告日付:2005/04/04 18:44:16)
- Sub Seven トロイの木馬 (最終報告日付:2005/03/30 13:40:32)
- ??rvices.exe Trojan トロイの木馬 (最終報告日付:2005/03/27 09:24:25)

多く報告されている問題

- **プラウザ ハイジャッカ About:blank**
  - **除去できない**

Backup

X-Cleaner概要

- **X-Cleanerの特徴**

1. 個人利用から企業、ISP、セキュリティ コンサルテーションまでの幅広い製品ラインナップを提供
2. スパイウェアガイド www.shareEDGE.com/spywareguide/ と共に多くの情報を提供
3. 日本独自のスパイウェアにも柔軟に対応

X-Cleanerターゲット市場

ターゲットとしている市場(優先順)

企業	X-Cleanerだけでなく、ブロックリスト、将来のSPTやエンタープライズ版の販売 コンサルテーションや、シグネチャのカスタマイズなどさらに追加サービスを販売する可能性大
ISP / Webサービス	未だ日本では実装されていない。しかし、米国の例からニーズは大きいことは明らか
OEM	PCベンダ- プリインストール データベース/エンジン技術の提供
コンシューマ	パッケージ化と販売

X-Cleaner製品ラインアップ

製品	ISP Pack	企業 Pack	OEM	概要
X-Cleaner Micro-Scanner	✓			Quick Scan, Deep Scan Deep Scanの提供は、契約から2週間後になります
X-Cleaner Deluxe		✓	✓	プロフェッショナルなスパイウェア駆除が行えます。
X-Cleaner Command		✓		コマンドラインにより実行可能、スパイウェアの検出と、駆除が可能
X-Cleaner Enterprise		✓		企業ユーザ向けのソリューションを提供します。 *日本語版は4月以降(新しいバージョン以降)
X-Cleaner Block List		✓		Block Listを使って、既知のスパイウェアの活動を防ぐことができます。
SPT		✓		Block Listをさらに発展させActive-Xだけでなく、スパイウェアモジュールを封じ込めるためのセキュリティ テンプレート *日本での提供は4月以降
スパイウェアデータベース			✓	www.spywareguide.com で提供されるスパウェア情報データベース

1. 10大Spyware by Webtoot

アダルト関連サイトからの悪質なプログラムが多い.

またCleanerを装ったうそのソフトウェア CoolWebSearch.

2. Marketscore ステルス ソフト (Web閲覧高速化そふと)

3. By Webroot ファイヤウォールやアンチウィスルだけでは十分でないことを証明

4. 2003年 1200万ドルから2008年 3.500億ドル

5. デル スパイウェアに関する問題 ユーザのクレーム

Spy Act法案 スパイウェア製作者が処罰

Spyware診断 – 構成図

スパイウェアの脅威に対して、現状を把握するための診断システムをオンサイト、またはnextEDGE側に簡単に設定することができます。

ステップ1

特別仕様のMicro-Scannerを配布します。（インターネット上に設定も可能）

ステップ2

ターゲットとなる環境のそれぞれのPCでMicro-Scannerを実行します。

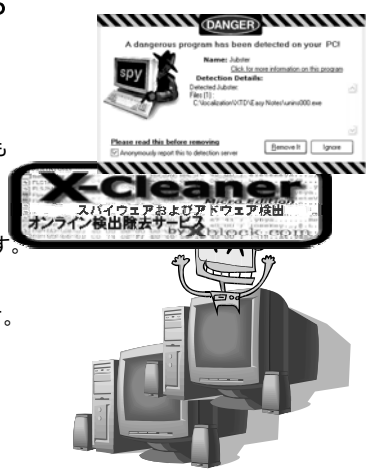
ステップ3

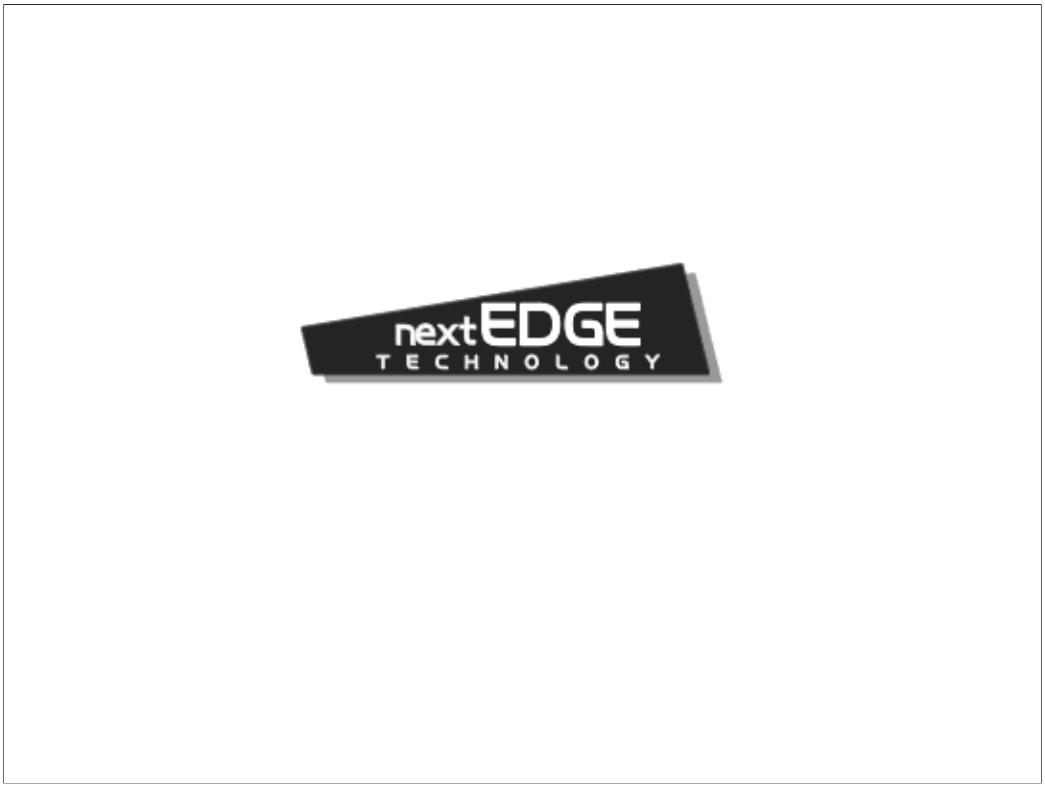
検出結果は、インターネットにあるnextEDGEサーバに収集されます。

ステップ4

検出結果、診断結果レポートを提供します。

補足: データ収集は2,3週間実施します。




nextEDGE
TECHNOLOGY