2005年および2005年第4四半期におけるスパイウェアの現状

ウェブルートソフトウェア株式会社
野々下　幸治

1. 概要

ここ近年日本でも、オンラインのビジネスの伸びと同時にオンラインでの詐欺がその数とともに内容も進化を遂げている。2004年は日本語のフィッシングメールが出現し、実際に被害者が発生する事件が発生し、フィッシングがオンライン詐欺の新たな手口として話題になった。2005年はオンライン銀行をターゲットとしてスパイウェアの事件がついに日本でも発生し、被害者が出ると共に、今年に入ってその犯人が捕まり、スパイウェアへの関心が高まった。

スパイウェアについては、ウイルス対策ベンダーとスパイウェア対策ベンダーとで定義が異なり、銀行の事件に利用されたキーロガーもウイルスベンダーは広義のウイルスに分類し、スパイウェアベンダーはスパイウェアと呼んでいる。

そもそも、コンピュータウイルスとスパイウェアは分類を行う観点が異なっている。

広い意味でのコンピュータウイルスはいわゆるマリシャスウェアとよばれ、ユーザーにとって悪意および害のあるソフトウェアをいい、その分類は感染方法によってウイルス、トロイの木馬、ワームに分類されている。

一方広い意味でのスパイウェアはユーザーの適切な同意なしにインストールされ、コンピュータの設定を変更したり、情報を勝手に送信したりするものをいい、その分類はウイルスと異なり、その目的によって基本的に分類されている。たとえば、広告を表示する目的のアドウェア、システムの状態を監視するシステムモニターなど。

したがって、そもそもキーロガーの機能を有するトロイの木馬は両方に分類されることになる。

ただし、ウイルス対策ベンダーは先にマリシャスウェアとしての分類分けを行った上で、スパイウェアの分類を行うので、トロイの木馬として届けられるキーロガーはスパイウェアの分類には入らず、商用のキーロガーなどがスパイウェアに分類される。

一方、スパイウェア対策ベンダーはそのような縛りがないので、たとえば、キーロガーは商用またはマリシャスの区別なくスパイウェアとして扱っている。

よって、ウイルス対策ベンダーはスパイウェアをマリシャスウェアに入れないが、スパイウェア対策ベンダーのスパイウェアにはマリシャスウェアも含まれている。この分類の違いがスパイウェアの定義において混乱をきたしていると思われる。

なお、よく、スパイウェアが金銭目的で、ウイルスは愉快犯との分類もするが、上記のようにウイルスの分類に愉快目的か、金銭目的かの分類はない。これまでの歴史を見れば、金銭目的は少なかったというだけで、現実にウイルスに分類されるトロイの木馬は、金銭目的の物が増えている。よって、これも当てはまらないと思われる。また、同様にウイルスは捕まえやすく、スパイウェアは捕まえにくいというのも同様に誤解である。

一口にスパイウェアとよんでいるが、人によってはキーロガーの問題であったり、アドウェアの問題であったり、その対象が異なっていることがある。今日、ブロードバンドの広がりと共にアドウェアのビジネスによる被害が増加し、キーロガーによるオンライン詐欺の被害もほぼ同時に増えたため、両方ともに代表されるスパイウェアが、コンピューティングの安全性にとって最重要な脅威になった。

ウェブルートはこのようなスパイウェアの問題の拡大に対して、その実際の状況を知り、適切な対策がおこなえるように、2004年より“State of Spyware”という報告書を出している。

この“State of Spyware”はPhileasと呼ばれる、インターネットを巡回し、スパイウェアの発見するシステムとSpy Auditと呼ばれるオンラインのスパイウェアの検査システムからのデータを元に分析されている。

今回、その“State of Spyware”の2005年の年間と第4四半期に関する最新の報告書が公開されたので、それを元にスパイウェアの現状を報告したい。

多くの企業や消費者はセキュリティの脅威に対処するために、すでにさまざまなセキュリティ対策製品を導入している。しかし、セキュリティ対策の導入の利用率が進んでいるにもかかわらず、新たな感染、新種のマルウェア、大規模なセキュリティインシデントが年間を通して業界ニュースを賑わした。

2. ニュースとインシデント

セキュリティアナリストから見れば、2005 年はデータセキュリティにとって最悪の年といえるかもしれない。米国ではさまざまなセキュリティ侵害が合計 130 件以上発生し、個人情報の盗難の可能性など、広範な不正行為の危険にさらされた被害者は 5,500 万人以上にのぼった。

大きく報じられたこれらの侵害事件は、引き続き消費者の財布に影響を及ぼしている。信用調査会社 ChoicePoint は、2005 年初めに個人情報の流出の事件を起こしたが、セキュリティ侵害に伴う費用をまかなうために、第 2 四半期の利益を調整しなければならなかった。さらに同社は、FTC との和解のために罰金 1,500 万ドルを支払うことに同意した。

そのようなセキュリティ侵害に伴う、ビジネス上の損失を被ったのは米国では ChoicePoint 1 社だけではない。そのほか、以下の組織や企業が被害を受けた。・H&R Block ・ BJ's Wholesale Club ・ DSW Shoe Warehouse・University of California・MasterCard ・Ford Motor Company・Sam's Club

上記の企業名は、顧客や消費者の個人情報が流出したため、年間を通してマスコミで大きく取り上げられた。しかし、これは全体の中の一握りのセキュリティ侵害に過ぎない。

日本においても、個人情報保護法の施行を受け、オンラインショッピングサイト等でのクレジットカードの情報流出等の事件が数多く報道された。

Sony BMG は猛反発と集団訴訟を受けて、不正コピー防止のためにルートキット技術を組み込んだ CD 数百万枚を回収した。問題のソフトウェアは、顧客のコンピュータをハッカーやウイルスに対して無防備にすると報じられている。訴訟では、Sony BMG は内密にスパイウェアを CD に組み込んだと申し立てられている。

このスキャンダルに続いて、マイクロソフトは、ハッカーに悪用されるとコンピュータに対するアクセスや乗っ取りが可能になる重大な脆弱性、WMF 欠陥を公表した。この独特の脆弱性は、Web ページの閲覧のような単純な行為でさえ安全でなくなるため、特に危険性が高かった。多くの技術系 Web サイトでは、セキュリティ脅威の進化を解説するために、この欠陥と関連するハッカーの行動を引き合いに出した。

3. インターネットの上のスパイウェアの配布状況

ウェブルートは Phileas という自動巡回ロボットによって、インターネット上のスパイウェアの配布状況や新しいスパイウェアを常に調査・研究している。その Phileas のデータによれば 2005 年にウェブルートはスパイウェアの配布サイトを 40 万以上検出した。

また、スパイウェア配布元として第 4 四半期は US が 30.54% と相変わらずトップであるが、第 2 位の中国が 30.31% とほぼ US の数に近づいてきている。

スパイウェア業者やスパイウェア作者にとっては 1 年を通して、検出と除去の回避が中心的な関心事になった。

そのためスパイウェア作者は、セキュリティ脆弱性を攻撃し、ポリモーフィックコードのような高度な技法を採用して、感染ユーザー層を拡大し続けている。

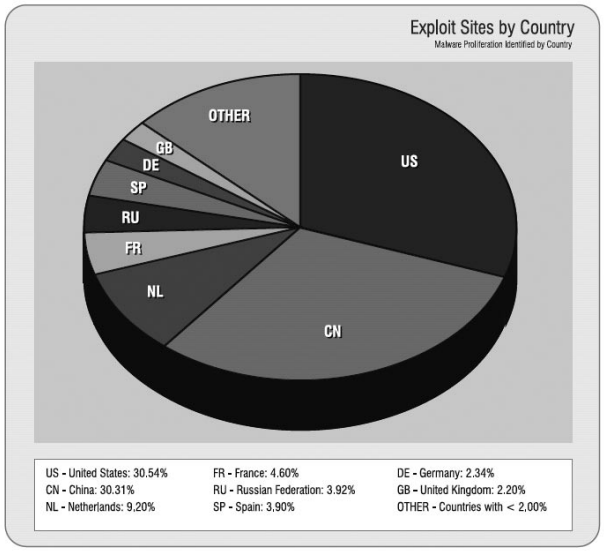
スパイウェア業者はより強力で除去しにくいプログラムの作成に努めており、ドライバベースの技術を使用したスパイウェアが増加した。

このようなプログラムは OS の最下位に入り込み、初期のスパイウェアよりもコンピュータの奥深くに自らを埋め込むもので、ユーザーの OS に広範なダメー

ジを与えることができる。

現在のスパイウェアの開発では、検出を回避するためにスパイウェアをユーザーから隠すだけでなく、自動更新技術を実装することにも力を注いでいる。

脅威は絶え間なく進化しており、スパイウェア対策業界は片時も目を離さないことが求められる。



今回、上位にランクインした脅威の以下のリストから、圧縮アルゴリズムと暗号化アルゴリズムが依然として使用されていることがわかる。トロイの木馬コード、ウイルスのインストール、ポリモーフィックエンジンをベースにしたスパイウェアでは、脅威の先手を打つために、新たな検出･除去手法が必要になる。

以下のトップ 10 のプログラムのうち、Spyware-Strike と PSGuard の 2 種類はスパイウェア対策ソフトを装ったスパイウェアであることに注意していただきたい。

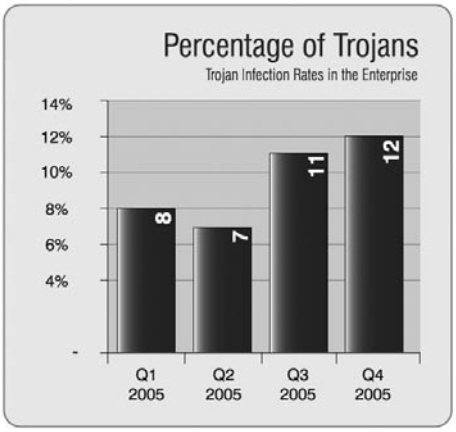
2005 年第 4 四半期のトップ 10

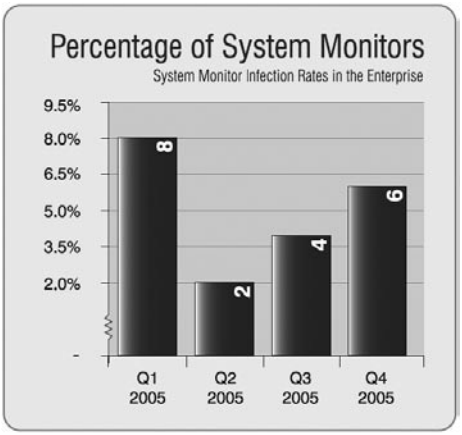
- 180 Search Assistant
- EliteBar
- PSGuard
- Apropos
- ISTbar
- SurfSideKick
- Virtumonde
- CoolWebSearch（CWS）
- DirectRevenue-ABetterInternet
- SpywareStrike

4. 企業についての調査結果

システムモニターやトロイの木馬などの悪意あるスパイウェアは、企業内の感染を広げている。

下図に示すように、2005 年第 3 四半期から第 4 四半期に、トロイの木馬は 9%増加した。第 2 四半期から第 4 四半期にかけては、システムモニターは四半期ごとに 50%ずつ増加した。





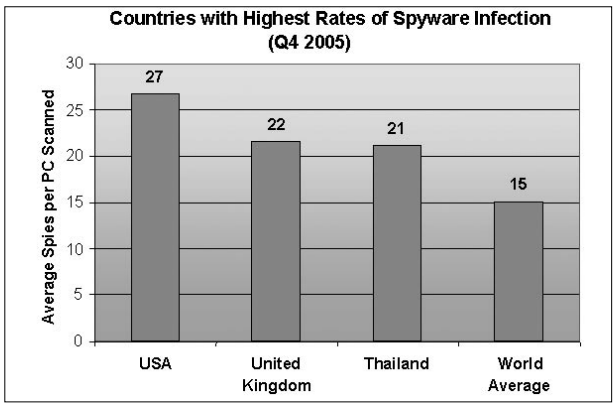
悪意あるスパイウェアはどんどん複雑化しており、旧来のウイルス検出および除去の手法では問題が生じる。

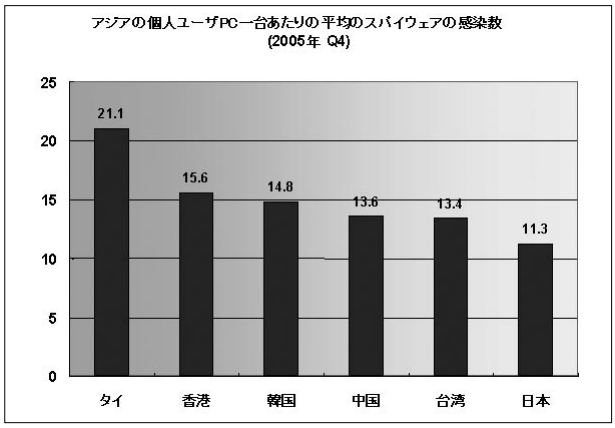
スパイウェアの場合、大半が旧来のウイルスよりも動作の変化が激しい。

ウイルス対策ソフトや無償のデスクトップ用ソリューションは、複雑で高度なスパイウェアに対しては効果的な保護と駆除が難しいことを認識することが重要だ。これらのプログラムで使われる検出・除去エンジンでは、ポリモーフィックコードやルートキット技術を使って検出を回避しようとする、悪質なスパイウェアを完全に除去することは難しい。

5. コンシューマーについての調査結果

スパイウェアに対する意識の高さにもかかわらず、望ましくないプログラム、特にトロイの木馬やシステムモニターのような悪意あるプログラムに感染される消費者は増加している。米国、タイ、英国の家庭用コンピュータのユーザーは依然として感染率がトップクラスだった。日本は平均 11.3 と世界の平均 15 よりも低い。これは多くのスパイウェアが英語圏をターゲットとしており、日本語のスパイウェアが少ないためだと思われる。しかし、最近は日本語のインストール用の Web ページを用意するなど、日本人をターゲットにしてきているので、今後は日本の感染が増える可能性も考えられる。





スパイウェア感染率が上昇する原因を 1 つに特定するのは難しいが、セキュリティアナリストは、パソコンの低価格化と、低料金化やアクセス増加によるブロードバンドの普及率の高まりを指摘する。コンピュータの価格が手頃になるにつれて、1 世帯で複数台のコンピュータを所有する傾向が強まる。

さらに、検出を回避するために、スパイウェア作者はプログラムを頻繁に変更する。家庭ユーザーが新種のスパイウェアから身を守るには、定義が頻繁に更新されるスパイウェア対策ソフトを使うことが必要だ。残念ながら、スパイウェア対策ソフトをインストールしても定義やバージョンを更新しないでいると、頻繁に更新を行う場合のような保護は得られない。

6. 米国における法規制

US においては、特にアドウェアのアフェリエイトのビジネスモデルが消費者の PC にいろいろな問題を起こしているために、SPAM と同様、法による規制が進んできている。2004 年 10 月にスパイウェア業者を相手に初のスパイウェア訴訟を起こした FTC は、2005 年には取締活動を強化し、スパイウェアや偽のスパイウェア対策ソフトの配布元とみられる業者に対して数件の訴訟を起こすとともに、FTC によれば顧客データを適切に保護できなかった企業に対して

も提訴に踏み切った。

その中でスパイウェアの配布元は、2005 年に議会を通過した新たなスパイウェア規制法案の重圧を感じ始めている。米国の多くの州がこのような業者の提訴に踏み切った。米国政府レベルでも米連邦取引委員会（FTC）が、自作のスパイウェアをスパイウェア対策ソリューションと偽って配布しようとした複数のスパイウェア作者を提訴した。

2005 年に、コンピュータユーザー数名が自分たちの手で問題を処理すべく、スパイウェアを欺瞞的に広めたとして複数の企業に対する集団訴訟を起こした。このアプローチは比較的目新しいため、これをきっかけに訴訟が急増するかどうか、業界では訴訟の成り行きを注意深く見守っている。

2005 年末までに、米国の 12 州でスパイウェア法案が可決された。そのうち 11 法案はすでに施行されており、ネバダ州については 2007 年 1 月 1 日から施行される。これらの新法はアラスカ州、アリゾナ州、アーカンソー州、カリフォルニア州、ジョージア州、アイオワ州、ニューハンプシャー州、テキサス州、ユタ州、バージニア州、ワシントン州で施行されているが、今後その効力が明らかになるだろう。2006 年会期のために州議会が招集されるため、米国では今後さらに多くの州でスパイウェア法案が検討される可能性は高い。

スパイウェアの脅威が加速する中、この災いの種からシステムを守ろうとする人々にとって 2006 年はどう展開するだろうか。

スパイウェア作者は審議中の米国政府法案に注意を払っており、悪意あるプログラムを配布する場合は、起訴の困難な中国やルーマニアなどの外国を経由するのを常套手段にしている。高度な暗号化技法をルートキット技術と合わせて使用することで、さらに悪質なタイプの望ましくないソフトウェアが引き続き蔓延するだろう。

2005 年に消費者と企業は、スパイウェアとその増大する影響についての認識を深めた。ユーザーはオンライン対策ツールの 1 つとして、スパイウェア対策ソフトを導入し始めている。ただし次のステップとして、導入した対策で問題を確実に解決し、対策ソフトを常時最新に保ち続けることを徹底しなければならない。

2005 年版「State of Spyware」に記されているように、スパイウェアの標的になるユーザーは増え続けており、オンラインセキュリティに対する脅威全体は飛躍的に増大している。