SOPHOS

ソフォス統合脅威管理レポート

～世界のセキュリティ脅威傾向～

2006年上半期（1～6月）

ソフォス統合脅威管理レポート

2006年上半期（1～6月）

～世界のセキュリティ脅威傾向～

2006年上半期のセキュリティ脅威傾向

この文書では、2006年1月から半年間のセキュリティ脅威の動向についてレポートします。

2006年上半期は、2005年に引き続き、組織のネットワーク管理者にとって厳しい状況が続いています。人やコンピュータの脆弱性をついて企業の機密情報や金銭を窃取しようとするサイバー犯罪の被害は深刻化し、IT管理者が直面する課題も複雑化しています。

マルウェア（悪意のあるソフト）の数は従来に引き続いて増加していますが、特にユーザーが気づかないうちに侵入するマルウェアの増加が目立ちます。種類としてはスパイウェアやフィッシング詐欺が上位2位に上がりました。多くのユーザーに無差別に送りつけられるマスメール型のワームは減少し、特定のユーザーにターゲットをしぼってマルウェアを送信する方法がとられるようになってきています。そのため、送信者が検知される可能性も低下しています。

2006年6月にデロイト トウシュ トーマツ社が行った金融サービス業でのグローバルなセキュリティ調査によると、4分の3以上（78%、2005年の調査と比較して26%増）の企業が外部からのセキュリティ攻撃を受けた経験がある、と回答しています[1]。このレポートではサイバー犯罪を『21世紀の犯罪』と位置づけています。

2006年上半期の傾向

ソフォスが検知したマルウェアの数	180,000件以上
悪意のあるメールの比率	91件あたり1件
新規トロイの木馬検知数：ウイルスおよびワーム数	4：1
ランサムウェアが増加	

マルウェア増加の状況

マルウェアの数は増加し続けています。2005年6月にSophos Anti-Virusが検知、阻止したウイルス、スパイウェア、ワーム、トロイの木馬などのマルウェアおよびアドウェアやPUA（業務上不要なアプリケーション）の数は140,118件でしたが、2006年6月には180,292件にまで増加しています。

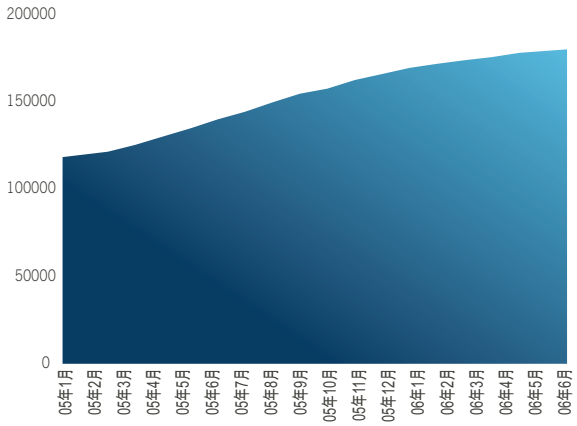

図1： マルウェア数増加の傾向

マルウェアの作成者はその手法を、大量に配信するマスメール型のワームから、特定のグループをターゲットにする方法に変えつつあります。ハッカーが金銭窃取を目的としている場合、大量のウイルスメールを送信して注目を集め、ユーザーに対策の必要性を感じさせるのは得策ではないと考えるのです。

同様にスパムメールの数も減少しています。アンチスパムソフトでは大量に一斉同報されるメールをチェックするなどの対策を行うため、検知を避けるのが目的です。

ソフォスの調査によると、2005年上半期にはウイルスメールは35通に1通の割合でしたが、2006年上半期には91通に1通にまで比率を下げており、攻撃の手法が変化していることを表しています。

マルウェアトップ10

グローバルでマルウェアの監視、解析を行っているソフォスラボの調査によると、2006年上半期のマルウェアトップ10は図2に示すとおりです。

2006年上半期にもっとも猛威を振るった脅威はSober-Zワームであり、ピーク時にはメール13通に1通の高比率で検知されました[2]。このワームは、FBIやCIAからのメッセージを装い、受信者が違法なWebサイトにアクセスしたと通知するものです[3]。2006年1月6日には対策が提供されているにもかかわらず、依然としてチャートの上位に挙がっています。

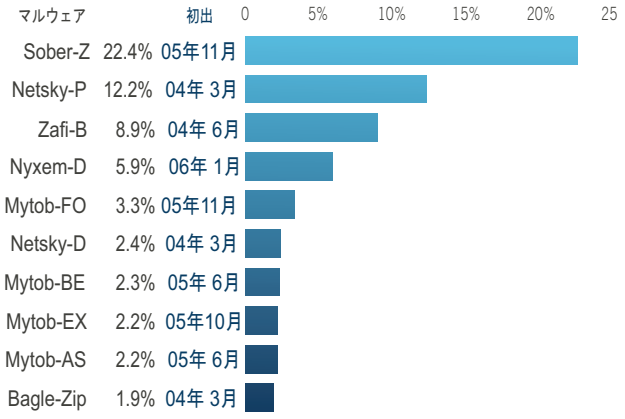

図2: マルウェア トップ10および
各マルウェアが最初に発見された時期

Nyxem-Dは、アダルトコンテンツを装うメールによって感染を拡大したワームで、カーマスートラ(性にかかわるインドの経典)ワームとも呼ばれています[4]。2006年に新規に発生したワームはこの1件のみです。このことからも、最近のセキュリティ脅威の傾向が、注目を集めることを避け、より少数を狙った潜行的な攻撃にシフトしていることがわかります。

トロイの木馬

2006年上半期の傾向では、マルウェアの作成者は、ウイルスやワームよりもWindowsに影響を与えるトロイの木馬を好む傾向が出ています。

2005年には、トロイの木馬と、ウイルスとワームの比率は2対1でしたが、現在では4対1に変わっています。

2006年上半期に出現したトロイの木馬の2分の1は、スパイウェアを含んでいました。スパイウェアは感染したコンピュータで、ユーザーのキー入力のログを保存したり、ユーザー名やパスワード、クレジットカード情報などの情報を窃取したりして第三者に売り渡すために使用されます。

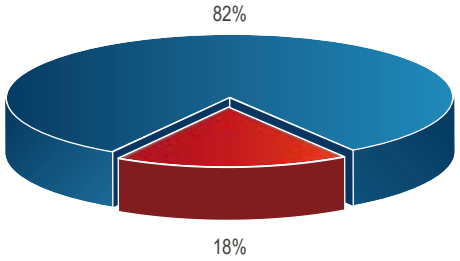

図3: 新規トロイの木馬(82%)とウイルス(18%)

トロイの木馬自体は感染手段を持たないため、作成者は、ユーザーにダウンロードさせたりマルウェアを実行させることなどによって感染を広げようとします。メールは、最も手ごろで感染速度も速いツールとして使用されます。最近では、メールにマルウェアを添付するのではなく、Webサイトのリンクのみを記載してユーザーにアクセスを促す手法が増えています。リンク先のWebページには悪意のあるプログラムが置かれています。

WindowsなどのOSの脆弱性が放置されていたり、ウイルス対策ソフト、ファイアウォールなどのセキュリティ対策が不十分な場合には、ユーザーが気づかないうちにマルウェアをダウンロードしてしまう危険性があります。

新規の脅威

ランサムウェア(Ransomware)

今年は、トロイの木馬の作成者が古い「ブラックメール」のスタイルをデジタルの世界に持ち込み、マスメールを使った攻撃ではなく、狭い範囲にターゲットをしぼって攻撃を行う傾向が強く見られます。ランサムウェアは多くの場合トロイの木馬の形式をとり、暗号化するなどの手段によってユーザーが自身のファイルにアクセスできない状況を作り出したうえで「身代金」の支払いを強要するものです。ソフォスラボでは多くの実例を把握しており、たとえば2006年5月に発見されたZippoと名づけられた例では暗号化したファイルを復号するための対価として300ドル50セントが要求されます。[5]

Ransam-Aは、Western Unionの送金サービスを使って10ドル99セントを支払え、支払わないと30分ごとにファイルを1つずつ削除すると脅迫するほか、アダルト画像や不適切なメッセージの表示などを行うものです[6]。エンドユーザーがトロイの木馬の実行を止めるためにCTRL+ALT+DeLキーを押すと、侮辱的なメッセージが表示されます。

Arhiveus(図4参照)はオンラインのドラッグストアから商品を購入するように要求します[7]。

今後の傾向

モバイル機器

1990年代後半以降、数社のウイルス対策ベンダーはモバイル機器でのウイルス大規模発生を警告しています。しかし、2006年上半期の現時点で深刻なマルウェアはまだ発生していません。携帯電話やPDAでの大規模な感染はなく、Windows環境でのウイルスと比較するとモバイル機器の危険性はさほど大きくはないといえるでしょう。

モバイル機器でのマルウェアが深刻な問題となっていない理由のひとつは、マルウェア感染による不当な利益を得ている犯罪組織が、モバイル機器よりWindowsでの効果に魅力を感じているからです。多様なOSが混在していてその違いに配慮しなければならない携帯電話の環境とは異なり、Windows環境であればウイルスを短期間で広範囲に感染させることができます。

モバイル機器を含めたユビキタス環境が推進され、OSが統一化されて普及すれば、それを狙った深刻なマルウェアの出現が増加すると思われます。

ただし、セキュリティベンダー各社はすでにモバイル機器を狙ったマルウェアへの対策テクノロジーを開発しはじめており、2006年中にはより多くのソリューションが提供されると思われます。

Windows Vista

2006年3月、マイクロソフト社は2007年までに次期OSであるWindows Vistaをリリースすることを発表しました。

Vistaではセキュリティ機能の強化が予定されており、そのリリースの遅れはユーザーにとって悪い知らせだといえます。

Windows Vistaにはホームユーザー用のスパイウェア対策のツールが含まれ、ハッカーによるゾンビ化への対策と期待されます。

また、多くのマルウェアやルートキットの阻止も期待されます。特に、OSの構造を利用した現在のルートキットはほぼ阻止できるものと思われます。しかし、Vistaを狙ったマルウェアやルートキットが作成されるのも時間の問題であり、より検知しにくいマルウェアの出現が懸念されます。

Macintosh

2006年2月には、Mac OS Xでの最初のマルウェアが検知されました。しかし、大規模な感染とはならず、その後もアップル社のOSを狙った深刻なマルウェアは出現していません。これはウイルス作成者がまだWindowsを主なターゲットとしているためだと思われます。そのため、今後も、Mac OS Xは比較的安全なOSであり続けると考えられます。

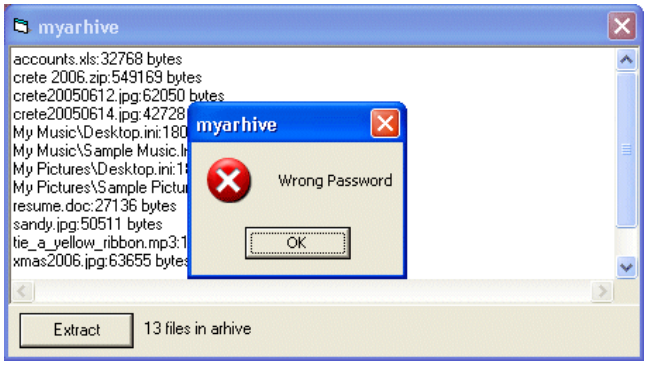

図4：ランサムウェアによる表示の例 – Arhiveusトロイの木馬

ルートキット(Rootkits)

ルートキットとは、第三者（不正な侵入者など）がコンピュータにハッキングした後に使用するソフトウェアツールをまとめたパッケージのことを指します。攻撃者によるアクセスの継続を支援することを目的としたもので、実行プロセスやファイルまたは改ざんしたシステムデータを隠してセキュリティソフトによる検知を回避します。ルートキットに関連しては、2005年ソニーが音楽CDの著作権を保護する目的で作成し、配布したプログラムが有名です。このプログラムには自身の存在を隠蔽するルートキットの手法が用いられていたため、多くの反発を招きました。さらに、プログラム自体のセキュリティ上の脆弱性がトロイの木馬などの攻撃対象となり、最終的にはソニーがユーザーからの損害賠償に応じざるを得ない事態にまで発展しました[8]。

スパマー（スパム作成者）

医薬品関係のスパム（性的魅力の向上、ダイエットなどの効用を訴えるもの）やポルノなどのアダルトコンテンツを含んだスパムが相変わらず出回っています。また、株価を操作することを目的としたスパムも成功を収めています。2006年6月中旬、Southern Cosmetics社の株式購入を促すスパムキャンペーン（同じ目的のために複数の手法や文面を用いて配信される一連のスパム）が出現し[9]、広範囲に配布されました。これはSouthern Cosmetics社が、カントリーミュージック歌手ナオミ・ジャッドがプロモーションに参加するコスメティクス企業Naomi LLcとのビジネス提携を行うとして株の購入を勧めるもので、スパム対策ソフトを回避するために画像データが使用されていました。ソフォスはこのスパムキャンペーンを検知し、阻止しています。Southern Cosmetics社の株価はこのスパムメールが配布された後、急上昇し、同社の調査では、1株1セント未満だった価格が6.6セントにまで跳ね上がったといいます。

図5は、同様の被害を受けた他の企業の株価をソフォスがモニタリングしたものです。4月21日にスパムキャンペーンメールが配布されると、40万株近くの取引が発生し株価は74%の上昇を見せ

ました。その後もスパムが配布され、1週間後にはさらに高値がつきました。このようなスパムは通常、週末に配信されます。週末にはリサーチャが分析を行っていないために新しいスパムルールの作成や適用が行われる、スパムに対して無防備になる企業が多いからです。なお、ソフォスでは週末を含め、24時間365日、セキュリティ脅威の分析と最新の対策の配布を行っています。

この詐欺の手法は、インターネット以前から存在しているものです。スパマーは(多くの場合、犯罪組織に属し)低価格で株を購入し、スパムメールを使って株の購入を誘導し、株価が上がるのを見計らって売りにだします。スパムに踊らされた購入者の手元には不当に高値で購入した株が残り、ターゲットにされた企業は財政的な混乱に陥り、スパマーだけが大金を手にすることになります。

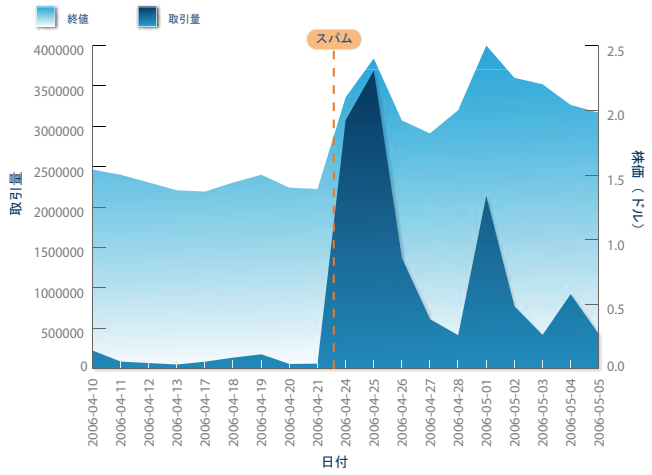

図5: Pump-and-dump詐欺(株価操作詐欺)にあった企業の株価および取引量の推移

ソーシャルエンジニアリング

現在では多くの人が添付ファイルをクリックすると脅威に感染する危険がある、という認識を持つようになりました。そのため、ソーシャルエンジニアリングはより巧妙な手口に進んでいます。政治的な問題、話題のニュース、魅力的な話題はユーザーを強く惹きつけるためスパムメールに使用されており、スパムによる詐欺の阻止を図る組織のセキュリティ対策担当者にとっては大きな負担となっています。

ソフォスではこの種の電子メール詐欺を継続的に検知し、阻止しています。2006年6月にソフォスが検知し、阻止したStinxトロイの木馬は「ジョージ・W・ブッシュ大統領とトニー・ブレア首相が中東の石油価格高騰に関与している」という内容を[10]、Sixenワームはワールドカップを題材にして感染を狙うもので、「裸のワールドカップに参加するサッカーファンの画像」などの内容を含んでいました。[11]

スパム送信国

スパムの数は増加し、世界的な問題となっています。スパマーは、自分自身がいる場所に関係なく、セキュリティ対策が不十分なPCをボット化するなどによって、世界中のどこからでもメッセージを配信することができます。

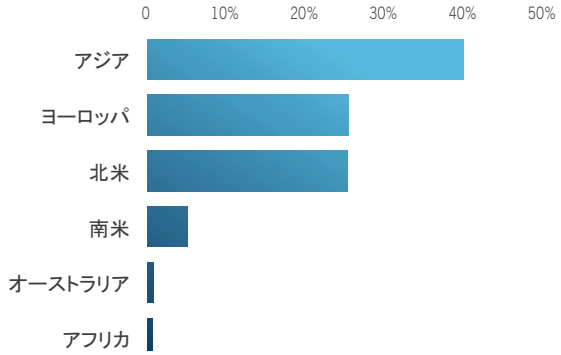

図6: 地域別スパム送信比率

2006年上期のスパム送信国第1位にはアメリカであり、全スパムの23.4%がアメリカから送信されています*。しかし、アメリカではスパマーへの実刑判決、法令の強化、セキュリティ対策の強化など多様な要因により、2004年以来、その比率は減少し続けています。かわって比率をあげているのが中国(20.5%)と韓国(8.7%)です。地域別の統計ではアジアからのスパム送信が多くを占め、北米を大きく超えています。

セキュリティ対策の必要性

人手を介さず、ソフトウェアの脆弱性をついて感染を広げるマルウェアが増加しているため、十分な対策が適用されていないコンピュータはこれまで以上により多く、短い間隔で攻撃を受け続けることになります。ユーザーがセキュリティパッチを適用するまで、またはOSやアプリケーションのベンダーがセキュリティパッチをリリースするまでの間隙をついて攻撃を加えるマルウェアが増加しています。

たとえば、Oscar-Bトロイの木馬はMicrosoft Wordを狙ってデイゼロ攻撃を仕掛ける脅威です。Wordファイルが開かれると感染します[11]。

まとめ

2006年後半には、新しい脅威の増加、感染拡大の高速化、ネットワークを守る手段の複雑化が、ビジネスに大きなインパクトを与えると思われます。サイバー犯罪が巧妙化、マルウェア検知を回避するための手段が次々と生み出される中、組織がシステム、重要な機密データ、ビジネスの連続性を守るためには、多様な手法が組み合わされている脅威を統合的に解析する専門技術と製品を提供するセキュリティソリューションの採用が必須です。

* ここに記載されている比率は、送信されているスパム(ボット化されたマシンから送付されたものを含む)の数に基づいて算出したものであり、スパムがどの国の言語で記述されているかを示すものではありません。

出展

1 Global Security Survey, Financial Services Industry and Deloitte Touche Tohmatsu, June 2006

2 The latest news on the Sober-Z worm outbreak, 1 in 13 emails are now infected by the Sober worm
www.sophos.com/pressoffice/news/articles/2005/11/soberz.html

3 Sober-Z worm poses as bogus messages from FBI or CIA
www.sophos.com/pressoffice/news/articles/2005/11/soberfbi.html

4 Obscene Kama Sutra worm spreads via email
www.sophos.com/pressoffice/news/articles/2006/01/nyxemd.html

5 Zippo Trojan horse demands $300 ransom for victims' encrypted data
www.sophos.com/pressoffice/news/articles/2006/03/zippo.html

6 Ransom Trojan horse demands money with menaces
www.sophos.com/pressoffice/news/articles/2006/04/ransom.html

7 Devious Arhiveus ransomware kidnaps data from victims' computers
www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html

8 Refunds for music fans hit by Sony DRM rootkit
www.sophos.com/pressoffice/news/articles/2006/05/sonysettlement.html

9 Cosmetics company's stock price rises sharply following spam campaign
www.sophos.com/pressoffice/news/articles/2006/06/stockspam.html

10 Spammed Trojan claims Bush/Blair Middle East oil cover-up
www.sophos.com/pressoffice/news/articles/2006/06/stinxw.html

11 Nude World Cup worm spreads via email
www.sophos.com/pressoffice/news/articles/2006/06/sixem.html

12 Trojan horse exploits zero day Microsoft Word vulnerability
www.sophos.com/pressoffice/news/articles/2006/05/oscorb.html