コンピュータウイルスの動向

鈴木直美●フリーライター

相次ぐゼロデイ攻撃、正規サイトに感染の罠 Stormワームが年間通じ猛威、Winny情報流出も止まず

コンピュータウイルス(トロイの木馬やワーム、スパイウェアなども含む)もまた、金銭を得るための手段のひとつとして定着し、パスワードを盗み取ったり、システムを乗っ取るなどの犯罪指向の強いものが主体となっている。国内でのサイバー犯罪には、一部専門知識を必要とする部分が残っているが、海外では分業化が進んでおり、闇市場では個人情報の売買やボットネットのレンタルと並んで、専門知識を必要としないウイルス作成キットやフィッシングサイト構築キットなどが販売されているという。コンピュータウイルスの作成もまた、手段を選ばない犯罪者たちの日常的なツールのひとつになりつつあるようだ。

相次ぐゼロデイ攻撃で国産アプリも次々標的に

2006年から頻発していたソフトウェアの未修正の脆弱性を悪用する「ゼロデイ攻撃」は、数の上ではやや減少したものの、2007年も大きな脅威をもたらした。特にOSやブラウザー、ウェブで使われるプラグインなどのネットがらみの脆弱性は、サイトに誘導するだけで悪質なプログラムを実行できるため、攻撃者の格好のターゲットとなっており、Windowsのアニメーションカーソルや「RealPlayer」の脆弱性は、修正後も長期にわたって悪用が続いている。国産ソフトを標的としたゼロデイ攻撃も、2006年の2件から3件に増え、ワープロソフトの「一太郎」、フリーの圧縮解凍ソフト「+Lhaca」「Lhaz」を狙うトロイの木馬が出現した。

正規サイトに仕掛けられたウイルス感染の罠

ウイルス対策やスパム対策が進んだメール環境を反映してか、メールの添付ファイルを使った攻撃は少なくなり、言葉巧みにサイトに誘い出し、ウェブ上で攻撃を仕掛ける添付ファイルなしのウイルスメールが増加した。企業などの正規サイトを改ざんし、攻撃サイトに誘導する手口も急増。世界中のウェブサイトで改ざん被害が起き、不正なIFRAMEタグが埋め込まれた。特に下半期には、国内でも企業や自治体の正規サイトが多数改ざんされ、閲覧者がウイルス感染の危機にさらされる事例が多数報告されており、「怪しいサイトを開かない」だけでは、もはやウイルス攻撃を防げない状況となってきた。

Stormワームが感染を広げ巨大なボットネットに

欧州の暴風雨に便乗し、ニュースを装う大量のスパムメールで感染を広げたStormワームが、1年を通じて猛威をふるった。当初は実行ファイルを直接添付するスタイルだったStormも、6月ごろからはメールのリンクをクリックさせて攻撃サイトに誘導する手口へと移行。手を変え品を変え襲いかかる波状攻撃の向こうからは、やがて感染パソコンによって形成された巨大なボットネットの存在が浮かび上がってきた。ボットは、外部からの命令で操られるロボットのこと。Stormに感染したパソコンは、外部からの指示で意のままに動かされるロボットと化し、スパムメールの送信や悪質なプログラム、偽サイトのホスティングといったことに悪用されていたのだ。後期のStormには、ボットネットを切り分ける機能も搭載され、レンタルや切り売りの可能性も指摘されている。

リムーバブルメディアを狙うウイルス復興

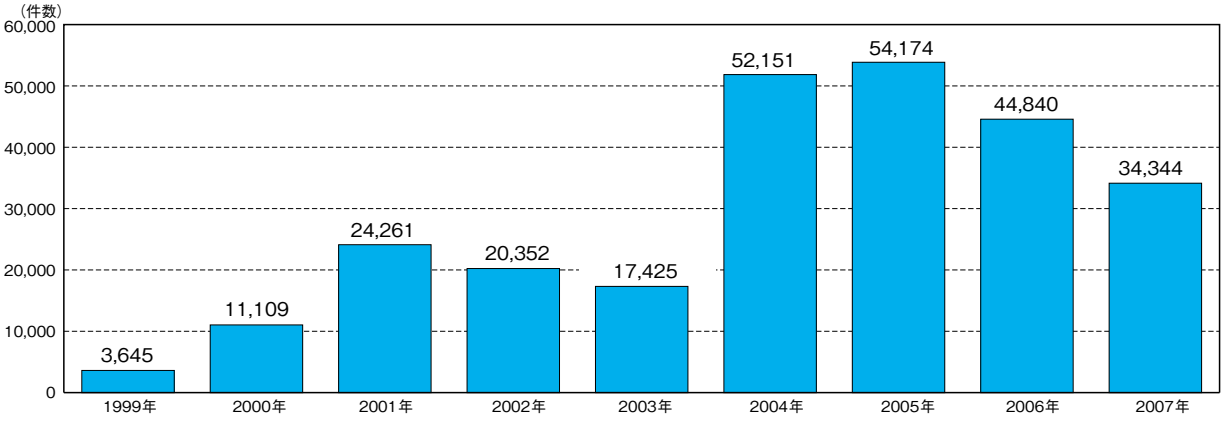
フロッピーディスクとともに衰退したリムーバブルメディアを介して感染を広げるウイルスが、USBメモリーやポータブル機器の普及を受けて再び活発に動き出した。もちろん、フロッピー時代のそれとは異なり、挿入時にメディア上の任意のプログラムを自動的に実行するオートラン機能を悪用したタイプである。感染パソコンに接続したネットワークドライブやほかのリムーバーブルメディアには、ウイルスが同様の仕組みを仕込んでしまうため、感染は、自宅と会社のようにネットワークなどでつながっていないパソコン間にまで拡大するおそれがある。

製品の製造段階で感染パソコンを使用したため、出荷された製品にウイルスが混入するという事例も相次いでおり、新品の外付けハードディスクやUSBメモリー、オーディオプレーヤー、フォトビュワーなどから、ウイルスが見つかっている。

インターネット白書／ ©1996-2012 Impress R&D

届出数・感染数ともに減少

資料2-2-5　コンピュータウイルスの届出件数の推移



出所　IPA「2007年のコンピュータウイルス届出状況」（2008年1月）

ウイルスの届出は、前年の4万4840件から3万4334件へと大幅に減少。実害のあった感染数も同様に減少し、前年と同じ0.2%となった。届出数は2005年をピークに、感染数は2002年以来減少傾向を示しているが、ウイルスベンダーの年間レポートとは大きな乖離がある。たとえばウイルス感染による「Winny」や「Share」からの情報流出だけでも年間に157件が公表されているのに対し、IPAに届け出たウイルスの感染数はその半分以下という現実から見ても、届出制度そのものが正常に機能していない可能性が高い。

自身を添付するマスメーリング型は出現せず

資料2-2-6　届出ウイルスの種別

ウイルス名称	検出数	届出件数
W32/Netsky	5,566,319	7,352
W32/Stration	236,768	1,879
W32/Mytob	234,695	2,662
W32/Nuwar	204,122	583
W32/Sober	159,171	74
W32/Looked	155,860	374
W32/Sality	148,575	2,098
W32/Bagle	105,750	2,960
W32/Mydoom	62,627	2,242
W32/Mywife	43,712	1,713
その他のウイルス	223,780	12,397
合 計	7,141,379	34,334

出所　IPA「2007年のコンピュータウイルス届出状況」（2008年1月）

自身を添付した大量のメールを送信し、感染を広げるマスメーリング型のワームは、わずかな感染者がいる限り永遠に検出され続ける。2004年に登場したNetskyや2005年に登場したMytob、Soberが2007年も相変わらず上位に位置し、前年に登場したStrationとNuwarがこれに加わった形だ。Nuwarは、一般にはStormの名で知られており、年間を通じて大量のウイルスメールが送られた。が、下半期にはウェブベースの攻撃に移行したため、ウイルス本体が添付ファイルとして送り込まれ検出されるというケースはなくなっている。IPAへの届出も2月をピークに、上半期だけで98%を占めており、ウェブベースの攻撃は、実害を与えられず検出だけされるという状況を回避することにも奏功している。

今年も止まらなかったWinny情報流出

ウイルス感染による「Winny」や「Share」などのファイル共有ソフトを介した情報流出は、前年に大きな社会問題にまで発展したが、国をあげての自粛要請もむなしく、2007年も止まることなく続いた。公表・報道されたものだけでも、その数157件。うち134件には計84万人の個人情報が含まれていた。警察関係では、1万件を超える捜査情報が流出した警視庁など5件の情報流出が発覚し3名が懲戒免職に。防衛省からも、陸上自衛隊で3件の流出が発覚した。教育関係では19件が発覚し4万人を超える生徒らの個人情報が、医療・福祉関係では12件が発覚し2万人を超える患者情報などが流出した。自治体関係では、委託先から5自治体の住民情報7万2000名分を含む55万件の情報が流出したほか、職員らによる21件のウイルス感染で、3万7000名の個人情報や行政情報が流出した。

インターネット白書／ ©1996-2012 Impress R&D

Internet White Paper ARCHIVES
インターネット白書
ARCHIVES
1996,1997,1998,1999,2000

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp

©1996-2012 Impress R&D, All rights reserved.