2003-10-15

H．P．Report

第82号

発行責任者　稲崎義明

ハッキングの仕方（4）

メールによるウィルスの感染ですが、前回書いたようにウィルスはマシン内のexeファイルに感染したファイルを実行するたびに感染してしまいます。ということは、メールの添付ファイルがよく知っているファイルであっても、exeファイルの場合はウィルスに感染してしまっている可能性があることになります。つまり、進入したウィルスはまずマシン内のexeファイルに進入を開始し、知らないうちに感染したファイルを知り合いに送ってしまうとそのマシンも感染してしまうということです。これがウィルスのウィルスたるゆえんです。

ウィルスに似たもので、「Ｂａｃｋ　Ｄｏｏｒ」というプログラムがあります。バＢａｃｋ　Ｄｏｏｒはその名前のとおり裏口です。本来の正面ではなく、裏口から進入しようとするもので、このプログラムによって遠隔操作することができるようになります。遠隔操作して何をするかといえば、たとえばきているメールの内容を読んだり、どのようにパソコンを操作しているかがわかりますし、相手のマシンを経由してハッキングを行うこともできます。このＢａｃｋ　Ｄｏｏｒのプログラム自体は非常に小さくて、相手に発見されないように実行するため、仕掛けることができればまず発見されることはありません。ハッキングとしては個人データの読み出しのほかに、多数のマシンに感染することによって、一箇所に一度に攻撃を仕掛けるようなＤｄｏｄ（分散負荷攻撃）を行うことができ、攻撃されたサーバをダウンさせることもできます。Ｂａｃｋ　Ｄｏｏｒの総数は種類別にしても約400種類以上あり、アンチウィルスソフトも完全に対応していないのが現状です。ＭＥＧＡ　ＳＥＣＵＲＩＴＹというサイトがあり、ここから現在存在するＢａｃｋ　Ｄｏｏｒのほとんどをダウンロードすることができます。

メールを使ってするハッキングに「メールボム」があります。メールボムは大量のメールを送信することによって受信者を攻撃しようとするもので、個人攻撃に使われるのが主です。といっても普通にメールを出すと、ReceivedやMessage-idなどといったアクセス情報がメールとともに送られています。ヘッダ情報を表示させるようにすると表示することができ、この情報を元に誰から送られたものかプロバイダでは調べることができます。これはフリーメールを使っても同様で、誰が使うためにフリーメールのページに入ってきたかの情報は必ず残っているので、匿名というわけにはいけません。ではどうすればよいかというと、E-Mailerといった匿名メール送信システムがあり、このソフトで送ると匿名にすることができます。メールボムは大量のメールを送るものですが、それだけではなく、受信したメールが自動的に容量を増やしハードディスクをパンクさせてしまうこともできます。そうなったらWindowsでは対処できず、Dosプロンプトで不必要なファイルを削除しなければならなくなります。

ところでウィルス対策ソフトですが、買ってきてそのままインストールというわけにはいかないようです。というのも、ウィルスにすでに感染してしまったマシンに入れることができないということです。そのために、事前にチェックプログラムによってまずマシンのスキャンを行い、感染していないことを確認したうえでのインストールということになっています。これば、アップデートも同じで、ちょっとの差で最新のウィルスに感染してしまうと、あとからアップデートしても何の役にも立たないことがあるということになります。そのためにも、こまめにアップデートが必要となるわけです。

（次回に続く）

(情報誌トピックス)

○日経エレクトロニクス　１０月１３日号

特集　ＳＣＯショック

→ＳＣＯはＵＮＩＸの知的財産権を所有する。このＳＣＯがＬｉｎｕｘを中心に事業展開しようとしているＩＢＭを著作権侵害で訴えた。これは、対岸の火事ではなく、Ｌｉｎｕｘを利用しているメーカ、一般ユーザに対しても影響してくる。もともとはフリーのＬｉｎｕｘであっても、追加、回収された部分に著作権侵害が認められた場合、フリーでなくなる可能性が高い。

解説　「脱３原色」に走り出すデジタルカメラとプリンター

→色の再現性を高めるために、これまでの３原色から多色化が始まっている。デジタルカメラでは、これまでの赤・緑・青に加えてエメラルドを加えたものが登場し、プリンタでは、シアン・マゼンダ・イエローに赤と青を追加する。どちらもより忠実に色を再現しようとするもので、この流れはディスプレイにも波及し始めている。

○日経パソコン　１０月１３日号

特集　思い出のデジタル化「史上最大の作戦」

→これまでのたまってしまっておき場所に困る昔の写真、音楽テープ、レコードなど。だんだん劣化してしまわないうちにデジタル化してＣＤやＤＶＤにしまえば問題解決。写真はついでにきれいに、音楽テープなどはノイズをとってデジタル化。整理のためのノウハウ満載。

特集　知っておきたい「１０大」技術トレンド

→今後のパソコンの進化を知るうえで欠かせない「１０」の技術（無線通信、バッテリ、ＣＰＵ、メモリ、ハードディスク、光学ドライブ、Ｗｉｎｄｏｗｓ、バス、ディスプレイ、筐体）について知る。

特集　ネット探索力をもっと鍛える

→インターネットを使って調べるにも、言葉がはっきりしないものはそれなりのテクニックが必要。「Ｇｏｏｇｌｅ」のサイトを使って探索するテクニックの紹介。

○Ｎ＋ＩＮＥＴＷＯＲＫ　１１月号

特集　無線ＬＡＮ設計講座

→使うと便利な無線ＬＡＮ。ところがセキュリティに問題があったり、思うほど速度が出なかったり、途中で切れてしまったりする。「電波」、「セルとチャネル」、「セキュリティ」、「製品」の４つのポイントを軸に設計・構築方法を解説する。

特集　内部情報漏洩実践防御術

→内部情報は、故意にもらすこともあるが、知らないうちにもある。漏洩ポテンシャルの実態を理解し、その危険性を把握し、具体策を立てなければならない。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　１１月１日号

特集　全理解！ＨＤＤ最新性能

→とどまることなく進化するＨＤＤ。高速回転、６４ビットＰＣＩ環境、ＲＡＩＤ性能など最新ＨＤＤテクノロジーを探る。

企画　すぐ始めるバックアップの３ステップ

→バックアップには「データのバックアップ」、「システムのバックアップ」、「ＨＤＤのミラーリング」の３ステップがある。ＨＤＤの破壊、ファイル破壊型ウィルス、人為的ミスなどからシステムを守るために必要なバックアップ。可能な限り「手間いらず」、「ローコスト」、「素早い復旧」のバックアップを考える。