2008-5-15

混沌とした中から

第92号
発行責任者　稲崎義明

最新ウィルステクノロジー（３）

前回からの続きですが、ウィルスが実験環境だと自分を消去してしまうということですが、どうやって実験環境を判断するのでしょうか。実験環境とはどういうことかからウィルスが判断するようです。つまり、解析用のツールがインストールされているや仮想化ソフトがインストールされている、さらに感染を広げないようにインターネットに接続されていないなどですが、ウィルスはそれぞれを判断するようです。ソフトをチェックしたり、特定のポートにデータを送って反応を調べたり、インターネットについては実際にサイトにアクセスしたりして調べるようです。

「攻撃を遮断されない」ですが、これは「ボット」と呼ばれるウィルスの場合です。「ボット」は2004年ごろから登場したウィルスで、感染したＰＣを攻撃側が乗っ取って特定の攻撃対象に対して複数の乗っ取られたＰＣが一斉に攻撃するもので、感染したＰＣはボットネットと呼ばれるグループを構成するのが特徴です。このボットネットは攻撃者からの攻撃の支持を中継サーバが中継し、ボットネットを構成する感染したＰＣに支持を与えることによって一斉に攻撃をするのですが、中継サーバを経由するためにこの中継サーバを閉鎖されるとボットネットとしての攻撃ができなくなります。これがボットネットの弱点なのですが、すでに対策が採られているようです。これが「攻撃を遮断されない」となるわけですが、まずとっているのが中継サーバの冗長化で、複数の中継サーバに同じボットネットに対する指示を中継させることにより1台が閉鎖されても攻撃が遮断されることはありません。また、中継サーバが閉鎖された場合ボットネットでこれまで指示を受ける立場であったＰＣが中継サーバに昇格する仕組みも用意されているようです。また、中継サーバ無しにボットネット内で相互に指示を出し合うことによって攻撃者が1台の感染したＰＣにだけ指示を出せばボットネット内全体に支持が伝わるような機能を持ったものも出てこようとしているようです。また、ボットネットでのデータのやり取りがＩＲＣというチャット用のプロトコルを使っているのが一般的であったことから、企業ファイアウォールではこの企業としては必要のないチャットのプロトコルのＩＲＣをブロックすることによってボットの動きを封じていましたが、これもＨＴＴＰやＨＴＴＰＳなどを利用するものが登場してきているようです。

最後が「新種を生み出す工夫」です。これに関して次のようなデータがあります。ドイツのウィルス検査機関が2007年に入手したウィルスが550万件で、2006年が97万件で5倍以上に急増したそうです。これは、凝ったウィルスが簡単に作れるツールが出回ったことが原因のようです。このウィルスを作るツールにも種類が2つあり、1つは新種のウィルスを作るもの、もう1つが既存のウィルスを改変するものです。インターネット上で入手できるこのようなツールは以前からありましたが、初期のものはメールを使って感染を広げることが主目的であり、現在のようなＰＣを乗っ取ったり情報を盗み出すようなものではなかったようです。現在のものは高機能化になり盗み出す情報の種類、例えばアプリケーションのパスワードを盗み出すといったことができます。また、盗み出した情報を管理するようなツールまで用意されています。このようなツールは当初ネット上で公開されもちろんフリーでしたが、このぐらい高機能になるとツールもフリーではなく商品として売買されています。ネット上の無料版は機能限定版で宣伝し、高機能のものは有償となり技術サポートさえ受けれるようになっているようです。

（次回へ続く）

（今週の情報誌から）

○日経エレクトロニクス　５月５日号

解説　小型ＰＣ騒乱　勝ち残りの条件

→小型軽量のパソコン、７インチとか８インチの液晶がついているパソコンは今までもいくつかあったが、これまでのものは普通のＰＣをただ小さくしたもので、遅い、高い電池が持たないなどいろいろな問題からたくさん売れるものではなかった。しかし、利用方法を割り切ったり、インターネット専用など企画力で新しい市場を形成しようと治している。

○日経パソコン　５月１２日号

特集　迷惑メールの「なぞ」を解く

→たくさん送られてくる迷惑メール。何の目的で、どうしてアドレスがわかっているのか。迷惑メールには出会い形、内職紹介、商品販売、架空請求、ウィルス添付、ウィルスサイトへの誘導などがある。また、アドレスはまずサーバのアドレスを採集して作ったり、Ｗｅｂサイトのものを収集したり、懸賞サイトから入手したりする。