2008-5-1

混沌とした中から

第91号
発行責任者　稲崎義明

最新ウィルステクノロジー（２）

コンピュータウィルスもビジネスになってくると作成者はいろいろなことを工夫します。確かにすぐにわかってしまうものや感染がうまくいかなければ商品にならないからです。いろいろな工夫の方法が有りますが、主なものとしては「感染を広げる」、「正体を隠す」、「攻撃を遮断されない」、「新種を簡単に作る」といったものがあります。

まず「感染を広げる」ですが、これまではメールで感染するものや、ＯＳを含むソフトウェアの脆弱性をついて感染するものが中心でしたが今は複合ワザです。例えばＷｅｂサイトにウィルスを置いてそれを使えるファイルであると装ってユーザにダウンロードさせる手口が増えています。中には検索サイトを悪用しＷｅｂサービスを使って感染サイトを探すウィルスもあります。どうやるかというと、まずソフトウェアの脆弱性を公表しているセキュリティ企業のＷｅｂサイトをアクセスして脆弱性の見つかっているソフトウェアの名称やそのソフトウェアに含まれるファイル名、脆弱性の種類などを取得して検索を実行します。検索で出てきたサイトでは脆弱性の有るソフトを使っている確率が高いということですから、そのサイトに対して脆弱性の合わせた攻撃を仕掛けて侵入を図ります。不正侵入できた場合そのサイトを改竄しウィルスを感染させるような仕掛けをすることになります。そうなるとこのサイトにウィルス対策が十分されていないユーザがアクセスするとウィルスに感染することになります。同じように検索サイトを悪用する手口としてはＳＥＯ（検索エンジン最適化）を使うものもあります。つまりＳＥＯを利用して検索した際に結果の上位に表示されるように工夫するということです。まずウィルスを感染させることを目的としてサイトを作ります。次に事前にウィルスを感染させ自由に操ることのできるようにしたパソコンを使って作ったウィルスサイトを宣伝します。具体的にどうやるかといえば、無料のブログサービスでアカウントを取得しウィルスサイトを宣伝するブログサイトを構築したり、既存のブログサイトのコメント欄にウィルスサイトのＵＲＬを書き込んだりして検索サイトによる評価を上げてウィルスサイトが検索の上位に来るようにします。ユーザは検索で上位に表示されれば人気の有るサイトとして何の疑いも無くアクセスすることになります。そんな簡単に検索の上位にウィルスサイトが来るものかと思いますが、現実２００７年になるとＳＥＯの利用がたくみになって表示されるようになってきたようです。

次が「正体を隠す」です。正体を隠す目的はウィルス対策ソフトのパターンファイルを作るために解析させないためです。ウィルス対策ソフトメーカは新しいウィルスが出るとまずそのウィルスを収集します。次に解析するわけですが現在のウィルスのほとんどは簡単に解析できない工夫が解かされています。その方法の１つはプログラムを暗号化などして読みづらくする「難読化」です。ウィルスはプログラムですから主にバイナリー形式です。これをわかり易いようにプログラムに戻すリバースエンジニアリング（昔アセンブラのときにあった逆アセンブルと同じ）をするわけですがこれをできなくしています。こうなると実際に実行してみないとウィルスの挙動がわからないことになります。しかしウィルスはここでも対策を採っています。つまり解析側は感染を拡大するわけに行かないわけですから実験環境で実行することになります。ウィルスはこれを判断し実験環境となれば自分自身の実行を中止してさらに自分自身を消去してしまいます。

（次回へ続く）

(今週の情報誌から)

○日経エレクトロニクス　４月２１日号

解説　「ライフ･レコーダ」の萌芽　あなたの１日を見守ります

→腕時計のように身につけた端末で一日の行動を見守り適切なアドバイスをくれる。そんな「ライフレコーダ」が作られ始めている。ライフレコーダは脈拍、皮膚温度、動きなどを計測し続けパソコンにデータを送る。パソコンは専用ソフトで解析し歩行数や活動量、睡眠時間などを推定し、必要なデータを記録し続ける。そのデータから活動量を測定し、健康管理、生活の質の向上、思い出記録、生産効率／品質管理のツールなどに拡大する可能性がある。

○日経パソコン　４月２８日号

特集　ＰＣユーザのためのケータイ活用術

→ケータイもいろいろ便利な機能がある。スケジュールをチェックしたり、指定時間に自分にメールを送ったり、ネットから情報をすばやく入手したりなど。ケータイはたくさんの機能を持っている、この特集から使えるものをピックアップして使ってみるのもいいのでは。

○日経ＳＹＳＴＥＭ　５月号

特集　忙しさから現場を救う　時間管理術

→対策を採らなければ仕事はたまるばかり。行き当たりばったりではどうしようもない。習慣化、段取り、一覧化で乗り切る。時間の使い方も例えば集中タイムを設定して仕事にメリハリを付ける等。