JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

不正アクセスとハッカーツール

渡部　章

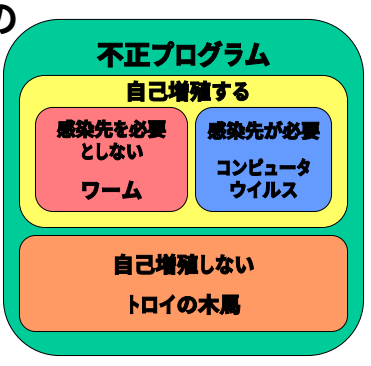
不正プログラム調査WG
株式会社アークン

2002 年 11月12日

不正プログラムの分類

JNSA

- 自己増殖するもの
  - 感染先を必要とせずネットワーク中で自分自身をコピーして増殖するもの
    - ワーム
  - 感染先を必要とするもの
    - コンピュータ･ウイルス
- 自己増殖しないもの
  - トロイの木馬
    - ハッカーツール等



不正アクセスを行うウイルス

2002年10月のウイルス届出

全ウイルス（ワームを含む）	：49種類、	1,521件
不正アクセス行為を行うもの	： 9種類、	440件、29%
攻撃行為を行うもの	：12種類、	104件、 7%

W32/Bugbear(バグベア)　323件、新種

このウイルスに感染すると、受信トレイや送信トレイ、及び特定の拡張子のファイル（tbb,eml,mbx,nch等）からメー ルアドレスを収集して、取得できたすべてのアドレス宛に、特定の内容のメールを送信する。また、以下の特徴がある。

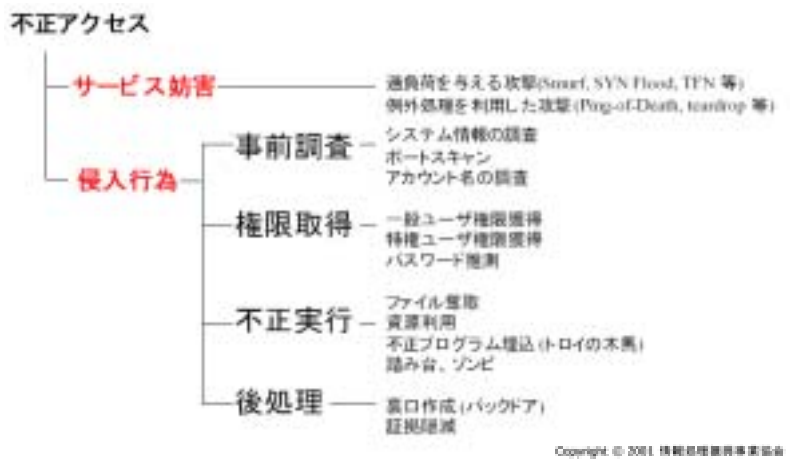
- 差出人アドレスを詐称する。
- ネットワークで共有されているパソコンに感染を拡大。
- ワクチンソフトやパーソナルファイアウォールなどの機能を停止。
- バックドアが仕掛けられ、外部から侵入される可能性がある。

このウイルスは、Windows95/98/ME/NT/2000/XPで動作する。

その他：　W32/Nimda(57件), W32/Badrans(49件), W97M/Marker(4件), W32/Gibe(2件), Linux/Slapper(2件、新種), Solaris/Sadmind(1件), W32/CodeRed(1件), W97M/Melissa(1件)

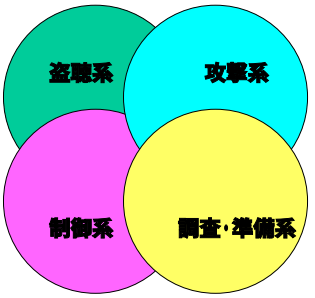
出典：http://www.ipa.go.jp/

不正アクセスの分類



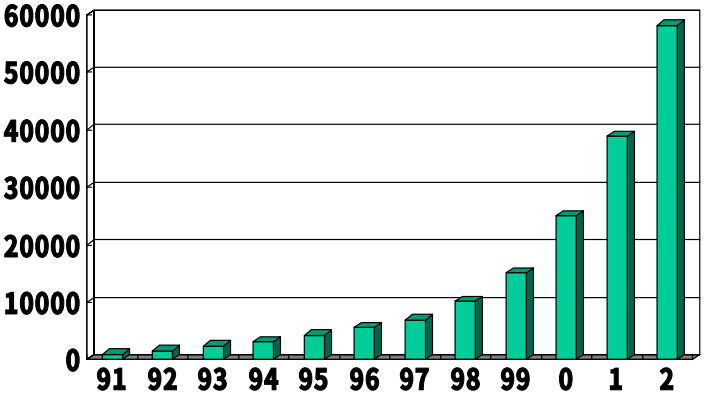
ハッカーツールの分類

- **調査･準備系**
  - ポートスキャナ、Warダイアラー、パスワード･キャプチャ、パスワード辞書攻撃、キーロガー、スプーファ
- **攻撃系**
  - クラッキングツール、Nuker、メール爆弾、SPAMツール、DDOS攻撃
- **盗聴系**
  - スニファ、アドウェア、スパイウェア
- **制御系**
  - RAT (リモート･アクセス･トロジャン)



ハッカーツールの現状

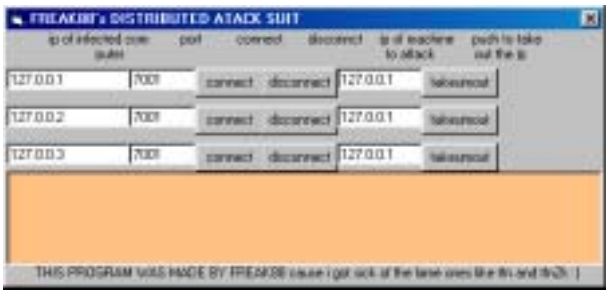
ハッキングツールの増加



58,169種類 (2002年8月現在)

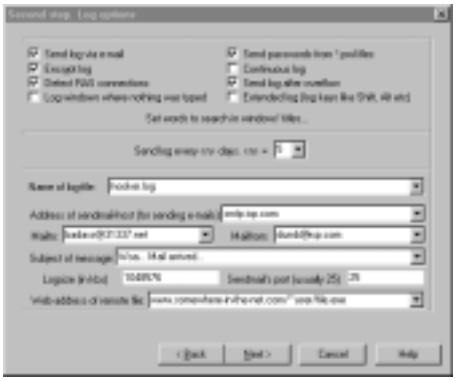
ハッカーツール例①

- **Freak88**
  - 分類：DDOS攻撃
  - 作成日：07/30/2000、危険度：高
  - このツールによって、攻撃者は、小規模なDDOS（分散型サービス不能）攻撃の調整をリモートで行える。



ハッカーツール例②

- **Hooker**
  - パスワード及びデータを盗み出すトロイの木馬。
  - Windows起動時に自動実行し、キーボードのコマンドを監視、RSA(Remote Access Server)のログインとパスワード、及びネットワークの情報(IPアドレス、パスワードおよびスクリプト)を獲得し、指定のメールアドレスに送信する。
  - 時限自爆機能を持っていて、ある一定の時間がくると自分自身をシステムから削除する。
  - Win32プラットホーム(Win95/98/NT)で動作。

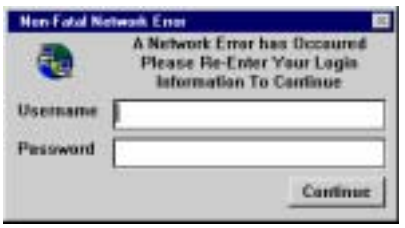


ハッカーツール例③

- **Illusion Mailer 0.05**
  - 匿名でEメールを送信できる。
  - Windows 95/98/ME/NT/2000で動作する。
  - 自動起動するようにレジストリを書き換える。
  - TCPポートの 2155と 5512を利用する。

ハッカーツール例④

- **Fatal Network Error**
  - “ネットワークエラーが出ました。継続するためにログイン情報を入力してください。”というプロンプト画面を表示する。
  - ユーザ名とパスワードを促し、Continueをクリックすることで、プレーンテキストでその情報をc:\os32779.sys に保存する。



ハッカーツール例⑤

- **SubSeven 2.2**
  - RATs(Remote Access Trojan)に属する代表的なハッカーツール。
  - バージョン2.2は2001年3月10日にリリースされたものである。
  - 情報収集機能
    メッセージ送信、チャット、スクリーンショットの取得、利用可能ドライブのリスト作成、
    PCの詳細情報取得、キー入力の盗聴、サウンドの録音、ファイルサイズの取得
  - リモート操作･設定機能
    ブラウザの開始、ターゲットマシンの再起動、
    CD-ROMの開閉、マウスの設定、
    サーバのパスワード設定、サーバ名の変更、
    オンライン通知のON/OFF 、
    アクティブ･ウインドウの操作、
    モニタのON/OFF、タスクバーの表示/非表示、
    ファイルの操作、壁紙の変更、
    実行ファイルのダウンロード/アップロード
  - 使用不能攻撃機能
    キーボードの使用不能、スピーカの使用不能、
    指定ウインドウと終了ボタンの使用不能、
    サーバを終了、スタートボタンを隠す

ハッカーツール対策

仕掛けられたハッカーツールを発見できますか？

- 不正アクセス技術はハッカーツールの組合せによる技術であると言っても過言ではない。
- ところが、VPN、IDS、ファイアウォール、ウイルス対策ソフトなどの既存のセキュリティ技術では、仕掛けられたハッカーツールや、その侵入を検出することはできない。
- 従って、常時接続している個人･企業では、今後ハッカーツールを検出･駆除･隔離するために PestPatrol などの専門ソフトウェアが必須となる。
  (http://www.pestpatrol.jp/)

ハッカーツール 三大侵入経路

1. 外部より第三者によって組み込まれる
2. ブラウジングやメール添付により
   ユーザが気付かずに組み込まれる
3. 内部ユーザによって組み込まれる
   (内部犯罪)

ハッカーツールのデモ

- Win-spy
  - フォルダの隠匿
  - パスワード調査
    - キーストローク
    - スクリーン・ショット
  - 証拠隠滅
  - 情報漏洩 (e-mail)

- 従業員管理に利用可能？！