JNSA ワーキンググループ紹介

不正プログラム調査WG

不正プログラム調査WGリーダー
株式会社アークン
渡部　章

■ はじめに

近年、トロイの木馬、スパイウェア、リモートアクセスツールなど、不正アクセスを目的にしたハッキングツールが増加しています。また、ウイルス、ワームも同様に近年では不正アクセスを目的としたものも少なくありません。実際の不正アクセス技術ではこれらのツールを組み合わせて利用するケースが多くなっています。これらの現状を踏まえ、本ＷＧは、不正プログラムとその対策の調査研究を実施し、その成果を普及させるために発足しました。

■ 活動の目的

本ＷＧでは、様々な不正プログラムを分類化し、その利用目的を明らかにし、各分類における代表的な不正プログラムと、昨今話題となっている不正プログラムのメカニズムを説明できるような資料を作成公開します。これらのプログラムの中には、ネットワーク管理ツールとして正規に使用しているものも多く、使用目的や使用者によっては、不正プログラムになってしまうグレーなプログラムも多くあるため、両刃の剣といえます。そのために既存のセキュリティ技術では対象とされていなかったり、脅威として意識していないユーザも多いようです。そこで、本ＷＧでは具体的な対策方法も示して、この種の技術に関する正しい知識を広めていきます。また、既存のセキュリティ技術のこれら不正プログラムによる侵入、攻撃に対する有効性を検証します。

■ 現在までの進捗

本ＷＧが発足した平成14年度は、SQL Slammerワームが大量発生し、インターネットのインフラに多大な被害を出しました。その時、本ＷＧのメンバー達は平成13年に猛威を振るったCordRedの被害からの教訓を何故生かせなかったのかについて、大きな疑問を抱きました。そこで、初年度の調査・研究として「メモリ感染型のワーム」について、構造、被害状況、対策について「メモリ感染型ネットワーク・ワームの脅威とその対策」というタイトルで取りまとめました。その成果として、2003年6月2-3日に東京国際フォーラムにて実施されたNSF2003 springにてＷＧ活動発表を実施しました。
http://www.jnsa.org/result.html

また、平成15年度は、不正プログラムの定義、分類、構造、対策について、「不正プログラム対策ガイドライン」というタイトルで取りまとめました。

■ 今後の予定

今後本ＷＧは、基本的に隔月の会合を実施し、年一回の合宿にて成果物を取りまとめていきます。

平成16年度は、近年話題になっている、不正なアクティブ・コンテンツについて調査していきたいと考えています。これらの不正なプログラム・コードは、Javaアプレット、ActivXコントロール、Javaスクリプト、Visual Basicスクリプトなどで作成されており、

不正プログラム	好意的な使用	悪意ある使用
スパイウェア	システムの稼動監視、ユーザサポート支援	重要情報の不正取得
キーロガー	ユーザの動向監視	パスワードの不正取得
パケットアナライザ	ネットワーク管理支援、トラブル対応	パスワードや重要なデータの不正取得
脆弱性検知ツール	セキュリティレベルの管理	攻撃対象の選定

Web閲覧時やHTML形式のメールによって、ユーザの意図しない危害を与える可能性があります。不正なアクティブ・コンテンツのことを各対策ベンダーでは、Malicial Mobile Cord、もしくは、Vandal Cordと呼んでいます。

また、将来は、ユーザが不正プログラムの脅威について、わかりやすく理解できるように、ウイルスやトロイの木馬、また不正なアクティブ・コンテンツを擬似体験できるWebサイトの構築も検討しています。

■ おわりに

ウイルスによる被害は、他のセキュリティ被害に比べて圧倒的なもので、これは今後も継続するに間違いないでしょう。ただし、ウイルス対策ソフトウェアなどの既存セキュリティ技術では対策が十分ではない「メモリ感染型のワーム」による感染や、キーロガーなどのトロイの木馬や、スパイウェアなどによる情報漏えいの被害は、新しい脅威として、間違い無く多大な被害をユーザや社会に与えるでしょう。これらの背景から本ＷＧは、不正プログラムをウイルスだけに留めず、広範囲にその現況と対策について調査研究を実施していきます。