

T13: マルウェアの基礎知識と 検知、防御技術

二木真明 (住商情報システム)
渡辺勝弘 (理化学研究所)

マルウェアと対策 ~ その変遷と最近の動向 ~

Internet Week 2005
T13: 不正プログラム対策と侵入検知、防御技術

二木真明(住商情報システム)

マルウェア (Mal-ware) って？

□ Malicious Softwareの合成語

- 「不正プログラム」もしくは「不正ソフトウェア」
 - ウイルス、ワーム、トロイの木馬、スパイウェア、ボット……
- コンピュータや利用者に害をあたえる(あたえうる)ソフトウェアの総称
 - 実害がなくても、利用者に伏せて何かを実行してしまうようなものは、すべて「灰色」
 - たとえば、利用者に断りなく、その挙動などの情報を他人に知らせてしまうようなマーケティング目的の「アドウェア」なども「灰色」。

「コンピュータウイルス」という言葉

- 本来の意味
 - コンピュータプログラムに寄生するマルウェア
 - 寄生されたプログラムを利用者が実行することで、OSや他のプログラムにも感染を広げるもの
- 近年の使われ方
 - コンピュータに「感染」するマルウェア
 - ワーム等も含む = マルウェア全般
 - ごく最近、「スパイウェア」が言葉として分離されつつある…
- 多様化により単純な分類が困難に
 - 新しい総称が必要に マルウェア

マルウェア機能別分類と形態別分類

- 感染形態別
 - ウイルス
 - ワーム
 - トロイの木馬
- 機能別
 - 大量メール送信
 - 脆弱性探索と攻撃
 - 情報持ち出し(スパイウェア)
 - バックドア作成
 - システム改竄(rootkit導入など)
 - 他のマルウェアの導入(Dropper / Downloader)
 - 遠隔制御(ボット)
 - その他……
- コード種別
 - バイナリ
 - マクロ/スクリプト

感染形態別の分類

- ウイルス
 - 他のプログラムに寄生(感染)する
 - 感染したプログラムの実行でその実行環境や他のプログラムに感染を広げる
- ワーム
 - コンピュータ内で独立したプログラムの形態を取る
 - 他のプログラムを介さず単独で伝搬、増殖するもの
- トロイの木馬
 - 特定の目的をもったプログラムに意図的に組み込まれた不正処理
 - たとえば、ネットで入手した便利なソフトウェアを入れたら、バックドアが仕掛けられていた……など

機能別の分類

- 大量メール送信
 - 感染したコンピュータが保持するメールアドレスを探索し、それらの宛先に対して、自分自身を添付した電子メールを送信するような感染行動を伴うもの
- 脆弱性の探索と攻撃
 - ネットワークを経由した探索を行い、発見したコンピュータに存在する特定の脆弱性を攻撃して侵入するような感染行動を伴うもの
- 情報持ち出し
 - コンピュータ内に存在する、もしくはコンピュータを経由する情報を記録、外部に送信するようなもの(たとえばキーロガーやP2Pソフトウェアを悪用するようなウイルス)

Copyright (C) FUTAGI, Masaaki

7

機能別の分類

- バックドア作成
 - 正規の認証を回避してコンピュータを利用できるような迂回路を作成するもの
- システム改竄
 - コンピュータのシステム(特にOS等の基盤)に不正な改竄を加え、本来の機能を阻害したり、不正な機能を追加するようなもの全般。たとえば、rootkitの導入による侵入隠蔽など。
- 他のマルウェア導入
 - 自分以外のマルウェアをダウンロードし、インストールしてしまうもの
- 遠隔制御
 - 外部からPCを制御できるような手段を提供するもの。単なるバックドア作成ではなく、特定の(もしくは一連の)作業をコマンドひとつで実行可能なようなもの。能動的に、外部の不正サーバに接続して指令を待つようなもの。

Copyright (C) FUTAGI, Masaaki

8

コード種別

- バイナリ
 - コンピュータの実行形式(機械語命令)でプログラムされたマルウェア
- マクロ/スクリプト
 - コンピュータ上の特定のアプリケーションが持つマクロ言語、スクリプト言語などでプログラミングされたマルウェア(VBAマクロ、VBスクリプト、Javaスクリプト……)

マルウェアの変遷(黎明期)

- コンセプトは1970年代に既に存在
 - SF小説などに登場(Tape Worm...)
- 1980年代前半:研究の存在
 - 自己複製型プログラムの研究や実証実験
- 1980年代後半:基本的な技術の確立
 - 1986年 Brain Virus

マルウェアの変遷(黎明期)

- 初期のマルウェア
 - ウイルスが中心
 - オフラインメディアによるプログラム授受で感染
 - PC環境の破壊、操作妨害(直接、間接)などの被害が中心
 - 技術誇示的、愉快犯的動機による製作、散布

マルウェアの変遷(インターネット普及期)

- 1990年代: PC、インターネット普及に伴いウイルスが一般化
 - マクロウイルス(非バイナリウイルス)の登場
 - メール媒介、感染型ウイルスの登場
- ネットワークワームの登場
 - 最初の登場は1987年 Morris Worm (Internet Worm)
 - CERT/CC創設のきっかけに
 - 再来は2001年(Code red)
 - そして、Nimda, Blaster.....

マルウェアの変遷(インターネット普及期)

□ 普及期のマルウェア

- 自動感染型ワームの登場
 - 感染に人手を介さない…(コンピュータの速度で拡散)
- ネットワークを利用して拡散
 - 電子メールによる大量複製、配布
 - 脆弱性探索、攻撃による短時間の自動感染
- 実害よりも、感染拡大による被害(業務停止、駆除のためのコスト)が中心
- 依然として、技術誇示的、愉快犯的動機が中心

マルウェアの変遷(成熟期!?)

□ スパイウェア、ボットなどの登場

- マルウェア感染技術・手法の成熟と、それらを基盤に特定の目的を持った機能を強化したマルウェアが登場

□ スピア(ターゲット攻撃)へのマルウェア応用

- 大規模拡散を意図しないマルウェアの開発
- 特定の目標を集中的に狙う形のマルウェア攻撃が顕在化(中央省庁宛のマルウェア添付メール配布など)

マルウェアの変遷(成熟期！?)

□ 成熟期のマルウェア

- 目的別に分化して機能を強化
- 大量拡散せず、感染後潜伏、顕著な症状を示さない(発見が困難)
- マルウェア撒布の自己目的化は、ほぼ終結。具体的な目的の「道具」としてマルウェアを利用する傾向
- 営利、犯罪行為やテロ目的のマルウェア利用が危惧される

最近のマルウェア関連トピックス

□ ボットネットによるSPAMとDDoS攻撃

- 大量のボット感染PC(ゾンビ)を統括するボットネットからのSPAM送信、DDoS攻撃の脅威
- ボットによるSPAMがマフィアの収入源にも...

□ Antinny による情報漏洩の頻発

- 亜種にウイルス対策ソフトが追いつけない典型
- ネットワーク統制機能がない野放しP2Pソフトウェアはマルウェアの格好の餌食になるという典型
- マルウェア自身がP2P技術を取り込んでいく可能性も高い(P2Pボットネットの報告もある)

新しいマルウェアのコンセプト

- Rootkit技術で自己を隠蔽するマルウェア
 - OSの管理機能を改竄し、ユーザに対してマルウェア感染と実行が一切見えないように隠蔽する技術
- 仮想化マルウェア
 - MPUの仮想化機能を悪用して、自分自身がホストOSとなり、本来のOSをゲストに追い出してしまうことで、自分をOS上から検知不可能にする技術。

新しいマルウェアのコンセプト

- Web系アプリケーションへのマルウェア攻撃
 - Webアプリケーションに存在するXSS(クロスサイトスクリプティング)脆弱性等を悪用したスクリプトベースのマルウェア
 - SNSワーム
 - 2005年10月 MySpace.com
 - あるユーザのプロファイルを見た全ユーザのプロファイルに不正なスクリプトが導入され、連鎖的に感染が拡大した。
 - 表面上は気付かない形での感染拡大
 - XSRF(クロスサイト・リクエスト・フォージェリー)攻撃
 - スクリプト型マルウェアを使ったイントラネットへの攻撃可能性もある
 - 社内ポータルを開きっぱなしのユーザが感染したら・・・

意外と簡単なマルウェア送り込み

- たとえば・・・フィッシングメールによる方法
 - フィッシング詐欺と同様の手法。添付ファイルではなく、マルウェアを仕込んだWebにアクセスさせる方法。ソーシャルエンジニアリング的要素が強い。
 - 自分の会社で「誰もひっかからない」と言い切れるだろうか。
 - ターゲット攻撃ならば、感染者は一人でも十分！？

そこで・・・本日のテーマ

- 通信という面からみたマルウェアの挙動と、検知のための技術
 - 侵入検知技術のおさらい
 - 捕まらないマルウェアを追いつめる方法
- マルウェア対策はどのように運用していくべきか
- 実際にマルウェアに侵入された場合の対応、そのための準備や体制