Programy, które niszczą - wirusy i robaki komputerowe

Wprowadzenie

Programy, które niszczą - uwagi wstępne

- Cecha podstawowa - oprogramowanie opracowane by automatycznie (bez kontroli atakującego) i anonimowo zadawać straty
- Skuteczność wymagała opracowania mechanizmów samopowielania i automatycznego rozprzestrzeniania się.
- Motywacje - 'broń informatyczna', odwet, wyzwanie, test, kawał ...
- Początek problemu: 1981 - pierwszy 'typowy' wirus - wierszyk (Apple)
- 2001 - szacunkowa liczba znanych wirusów i robaków - ok. tysięcy, prawdopodobnie każdy z nas padł (i padnie) ofiarą infekcji ...

Klasyfikacja - kryterium: metoda powielania

- Wirusy - rozprzestrzenianie za pośrednictwem innych programów, do których dołączany jest 'niszczycielski' kod
- Robaki (bakterie?)

Wprowadzenie

- Kod związany z konkretnym procesorem (inny dla PC niż MAC)
- Inne klasyfikacje (pomieszanie kryteriów)
  - Robaki i wirusy
  - Konie trojańskie
  - Bomby logiczne, ...
- Inne rodzaje szkodliwego oprogramowania
  - Niszczenie zasobów lub zawieszanie pracy bez samoreplikacji
- Cel niszczycielskiego kodu - zadanie maksymalnych strat
  - Skuteczne rozprzestrzenianie (masowe i szybkie) i infekcja
  - Skuteczna infekcja
  - Skuteczne działanie - niezawodne wyrządzenie zamierzonej szkody
  - Skuteczne ukrycie
- Rozprzestrzenianie niszczycielskiego kodu
  - Kanały masowej komunikacji - poczta elektroniczna, internet

Rozprzestrzenianie - poczta

- Psychologia i proste triki
  - Psychologia + maniera domyślnego ukrywania rozszerzenia

I Love You	Załącznik - plik o nazwie LoveLetter.txt.vbs. Bez rozszerzenia to pozornie tekst, a nie skrypt VBS
Szkody	Rozsyłanie na adresy z książki, nadpisywanie JPG, JS, VBS, ..., MP3 - atrybuty 'ukryty', zmiany ustawień IE,...

  - Psychologia - wykorzystanie atmosfery strachu przed wirusami

```
From: support@Symantec.com Re: Virus ALERT!!!
Dear Customer,
We begun receiving reports regarding worms I love you.
...
To examine your system open the attached help file.
Attachment: Virus Protection Instructions.vbs
```

  - Psychologia + wykorzystanie trybu HTML poczty

```
Dear Customer, ...
If you wish to remove your name from our mailing list, click ...
```

Rozprzestrzenianie

Robak Nimda - rozmaite drogi rozprzestrzeniania

- Poczta - załącznik (plik README.EXE, robak rozsyła się na adresy z książki)
- Przeglądanie zarażonych stron oferowanych przez IIS
  Na końcu strony znajduje się kod JS, którego wykonanie (przez nie zabezpieczoną przeglądarkę) instaluje wirusa.
- Umiejscowienie kodu
  Dodaje się do listy skompilowanych zasobów (resources) programów, uaktywniając się po uruchomieniu programu
- Szkody Wymazywanie uruchomionego programu

Konie trojańskie - psychologia darmowego produktu

- NetBus - popularny koń trojański
  Program dający zdalną kontrolę nad komputerem ofiary - geneza: narzędzie administracyjne (podsłuch i monitorowanie systemu, otwieranie dostępu do systemu - 'backdoors')

Infekcja

Mechanizm infekcji

- Infekcja bezwarunkowa lub uzależniona od innych czynników - data, akcja użytkownika (otwarcie pliku), sekwencja zdarzeń (nieregularne infekowanie utrudnia wykrycie)

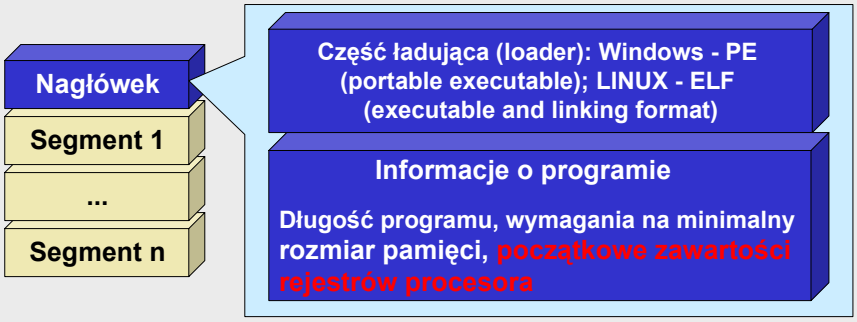
Wprowadzenie wirusa do pamięci operacyjnej (uruchomienie zainfekowanego programu, start systemu,...) i uaktywnienie wirusa (wykonanie kodu) → Monitorowanie systemu i infekowanie otwieranych i/lub uruchamianych programów

Wprowadzenie wirusa do pamięci operacyjnej (uruchomienie zainfekowanego programu, start systemu,...) i uaktywnienie wirusa (wykonanie kodu) → Powielanie innymi metodami

- Monitorowanie przez wirus w RAM procesu uruchamiania programów i modyfikacja kodu programu ('slow infectors')
- Monitorowanie przez wirus w RAM operacji otwierania programów i modyfikacja kodu programu ('fast infectors')
  Zwykle podczas skanowania programami antywirusowymi (gdy uruchamiając skaner nie sprawdzono, czy w RAM nie ma wirusów)
- Infekowanie plików w trakcie pracy zarażonego programu (wirus nie przedostaje się na trwałe do pamięci operacyjnej)

Infekcja

Ogólny format pliku wykonywalnego



Uruchomienie programu

- wykonanie części 'ładującej' nagłówka - alokacja pamięci, ustawienie atrybutów właściwych dla systemu operacyjnego,
- ustawienie rejestrów procesora zgodnie z danymi o zawartości pliku zawartymi w części 'skorowidzowej' nagłówka (licznik programu, rejestry adresowe itp.)

Infekcja

Modyfikacja pliku

- Posiadanie odpowiednich uprawnień pozwala na zapis do pliku
- Korekta nagłówka pliku w celu zapewnienia uruchomienia kodu wirusa i zachowania spójności informacji o programie
- Dopisanie do pliku wykonywalnego kodu wirusa

Typowa procedura modyfikacji pliku (C)

- Otwarcie pliku `fopen(filename,"wrb+")`
- Odczytanie niezbędnych informacji z nagłówka pliku

`fseek(..,adres_header,...);` `fread(bufor,...,..,..);`

- Nadpisanie nagłówka

`fwrite(vir_header,...,...,..);`

- Dopisanie kodu wirusa i zamknięcie pliku

`fseek(.,adr_vir,.);` `fwrite(vir,..,..,..);` `fclose(.);`

Infekcja

Miejsca umieszczania wirusów

- Infekowanie programów (wirusy) - ukrywanie kodu w plikach wykonywalnych
- Infekowanie sektorów startowych komputera (MBR, DBR) - wirus rejestruje swój adres i ukrywa się na dysku, często zaznaczając zajmowany sektor jako uszkodzony
- Programy z celowo ukrytym kodem, pozornie wykonujące inne, zwykle pożyteczne funkcje - konie trojańskie
- Infekowanie plików zawierających makroinstrukcje - wykorzystanie luk istniejących w konkretnych aplikacjach - makro-wirusy
- Umieszczanie wirusów w plikach o tej samej nazwie co programy exe z rozszerzeniem com - preferowanym w odniesieniu do kolejności wykonania przez DOS - companion virus
- Modyfikacje tablic alokacji plików, tak by wskazywały na kod wirusa zamiast na kod uruchamianego programu - wirusy klastrowe (cluster v.)
- Atakowanie kodów źródłowych - istnieją wirusy poszukujące i modyfikujące pliki ASM, PAS itd

Niszczenie zasobów

Szkody wyrządzane przez wirusy i robaki

- Większość wirusów jest niegroźna (dowcipy)
- Część wirusów i robaków wywołuje nieodwracalne zniszczenia (del,...)
- Szkody mogą być niezamierzone - wadliwie napisany kod (w wirusie ‘Stoned’ nie przewidziano wprowadzenia dyskietek >360kB co, zamiast niegroźnego ‘dowcipu’, owocowało niszczeniem całego FAT dyskietki)

Stopień winy użytkownika za dokonanie zniszczeń

- Bez winy użytkownika - wykorzystanie błędów i luk oprogramowania - infekcja mimo przestrzegania ogólnych zasad bezpieczeństwa
- Z winy użytkownika - nieostrożne uruchamianie zainfekowanych programów - infekcja wskutek lekkomyślności
- Niszczenie zasobów przez użytkownika - użytkownik, wskutek ignorancji sam dokonuje zniszczeń

  Virus hoaxes - wykorzystanie strachu: zalewanie skrzynek pocztowych, doprowadzanie użytkowników do własnoręcznego zadawania sobie strat (rzekomy wirus - aby usunąć zrób ....)

Niszczenie zasobów

Uruchomienie ataku

- Wirusy wprowadzane do RAM podczas startu systemu / uruchomienia zainfekowanego programu
- Wirusy z plików wsadowych - podstęp, polegający na uruchomieniu wirusa przy użyciu odpowiednio spreparowanego komentarza

```
@ECHO OFF
:[komentarz - sedno ataku]
COPY nic.BAT C:\nic.COM > NUL
C:\nic.COM
[binarne dane]
```

Rzeczywista funkcja pliku

Spreparowany komentarz uruchamia zawartość pola danych - wirusa.

Dane binarne mogą być nie być wyświetlane (Ctrl-Z), aby podgląd pliku nie wzbudził podejrzeń (podejrzenia powinna wywołać rozbieżność rozmiaru pliku i rozmiaru wyświetlanego tekstu)

Uwarunkowania wykonania ataku

- Brak - atak następuje po uruchomieniu kodu wirusa/robaka.
- Uaktywnienie warunkowe - data, akcja użytkownika, sekwencja zdarzeń

Utrudnianie detekcji wirusów

Metody

- Szyfrowanie kodu wirusa - by uniknąć wykrycia na podstawie analizy sygnatury kod jest szyfrowany i umieszczany w infekowanym programie wraz z kluczem i procedurą deszyfracji. Deszyfracja jest pierwszą fazą działania wirusa
- Aktywne oddziaływanie wirusa na proces analizy zawartości pliku lub jego długości dokonywanej przez skaner (ang. stealth viruses)

  Śledzenie i przechwytywanie odwołań I/O oraz odpowiednie akcje:
  - żądanie odczytu długości pliku - odpowiednio spreparowana odpowiedź
  - Żądanie odczytu sektora z kodem wirusa - modyfikacja żądania z podaniem OS innego numeru sektora (np. z zapamiętanym wcześniej obrazem prawidłowego pliku)
- Retro-wirusy - wirusy atakujące programy antywirusowe
- Infekowanie okazjonalne (co pewien czas, tylko pliki spełniające pewne warunki - np. o rozmiarze mieszczącym się w określonym zakresie)

Utrudnianie detekcji wirusów

Metody c.d.

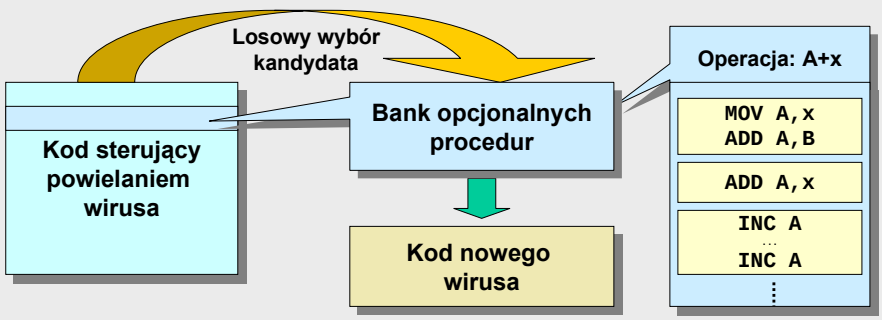
- Wypełnianie kodem wirusa istniejących w kodzie programu luk, nie powodujące zmiany rozmiaru infekowanego programu (luki w kodzie programu są dopuszczalne, jeżeli format pliku jest optymalizowany pod kątem np. szybkości uruchamiania - format PE dopuszcza istnienie luk bo oczekuje wypełniania kodem bloków o rozmiarze będącym wielokrotnością np. 512b)
- 'Tunelowanie' - technika polegająca na ustawieniu dla programu wirusa priorytetu w zakresie obsługi przerwań wyższego, niż posiadają antywirusowe programy monitorujące
- Wykorzystanie strumienia NTFS ADS (alternate data streams) - kojarzenie z plikiem dodatkowych danych w plikach ADS. Pliki ADS są niewidoczne dla większości narzędzi systemu. Uruchomienie programu powoduje automatyczne uruchomienie skojarzonego z nim pliku ADS, który może być wirusem

Bezpieczeństwo systemów informatycznych

Utrudnianie detekcji wirusów

Metody, c.d. - polimorfizm

- Zmiana kodu wirusa w kolejnych generacjach z zachowaniem jego zasadniczej funkcji.
- Metoda: żonglerka kodem nadmiarowym - pustymi instrukcjami (NOP), alternatywne stosowanie instrukcji o tym samym skutku, takich jak alternatywne warianty: MOV A,0, ADD B,A albo ADD B,0



Krzysztof Ślot © 2002

Metody detekcji wirusów

Skanowanie

- Przeglądanie plików w poszukiwaniu sygnatur znanych wirusów lub fragmentów sygnatur (zwiększenie odporności na polimorfizm)
  - ☺ Rzetelne sprawdzenie pod kątem detekcji większości znanych wirusów - konieczne częste aktualizacje
  - ☹ Kosztowne obliczeniowo, znajduje tylko znane wirusy, możliwe fałszywe alarmy

Skanowanie z wirtualnym uruchamianiem podejrzanych plików

- Rozwinięcie idei skanowania w celu lepszej ochrony przed polimorfizmem - pliki są uruchamiane 'programowo' - program AV emuluje procesor i sprawdza efekty działania podejrzanych instrukcji (dalekich skoków, dostępu do procedur BIOS itp.)
  - ☺ Możliwa detekcja większości znanych wirusów - konieczne częste aktualizacje
  - ☹ Bardzo kosztowne obliczeniowo, detekcja tylko znanych wirusów

Bezpieczeństwo systemów informatycznych

Metody detekcji wirusów

Sprawdzanie rozmiarów plików wykonywalnych

- Dla programów w wersji oryginalnej zapamiętywane są ich rozmiary, służąc następnie jako kryterium weryfikacji oryginalności programu
  - ☺ Szybkie sprawdzenie, nie trzeba znać wirusa
  - ☹ Łatwe do oszukania - wpisanie kodu wirusa w program, wirusy FAT

Sprawdzanie integralności plików wykonywalnych

- Dla programów w wersji oryginalnej wyznaczane i przechowywane są funkcje skrótu ('odciski palca'), które służą do sprawdzenia czy pliki nie zostały zmodyfikowane
  - ☺ Trudne do oszukania - jedyny sposób to kontrola wirusa nad I/O i podsuwania programom sprawdzającym zachowanej wcześniej, oryginalnej wersji. Wykrywa dowolną zmianę - nie trzeba znać wcześniej wirusa
  - ☹ Kosztowne obliczeniowo, nie odróżnia zmian wywołanych przez wirusy i inne przyczyny

Krzysztof Ślot © 2002

Metody detekcji wirusów

Monitorowanie systemu

- Monitorowanie odwołań do procedur systemowych uznanych za niosące potencjalne zagrożenie (dostęp do dysków, przyznanie praw rezydowania na stałe w pamięci i inne) i odpowiednie reagowanie w razie ich wystąpienia (np. pytania do użytkownika o zgodę)

Ogólna metoda obrony

Nie ma gwarancji przechwytywania wszystkich odwołań do procedur systemu operacyjnego, monitory mogą stać się bardzo uciążliwe

Monitorowanie wybranych aplikacji

- Sprawdzanie poczty i innych aplikacji przy użyciu metod ogólnych lub specyficznych dla konkretnej aplikacji

Oprogramowanie AV

Cechy programów antywirusowych (AV)

- W obecnie dostępnych produktach standardem jest użycie kombinacji wymienionych technik detekcji - wszystkie oferują skanowanie, monitorowanie systemu, monitorowanie poczty. Większość stosuje dodatkowo sprawdzanie integralności plików
- Podstawowym sposobem sprawdzania jest skanowanie
- Każdy liczący się program zapewnia zdalną, ciągłą aktualizację baz danych wirusów
- Powszechnie stosowane programy: Norton, Panda, McAfee (MKSVir)
- Porównanie skuteczności programów - sytuacja zmienna

Ochrona przed wirusami

Ogólne zasady bezpieczeństwa

- Zachowanie szczególnej ostrożności w zakresie instalowania nowych programów i konfiguracji / używania poczty elektronicznej
- Sprawdzanie wersji instalacyjnych programów (przypadki infekowania fabrycznie nowych programów)
- Sprawdzanie programu po zainstalowaniu, przed pierwszym uruchomieniem (czy nie ma wirusów w rozpakowanych plikach)
- Ostrożność przy ograniczaniu typów sprawdzanych plików (odchodzenie od identyfikacji programów na podstawie ich rozszerzenia, szereg nowo powstałych formatów to pliki wykonywalne)

  ..., BAS (moduł VB), CPL (odmiana sterownika)
  FON - plik czcionki może zawierać fragment wykonywalny,
  SCR - wygaszacz ekranu - plik wykonywalny, SYS, VB, VBS, VXD ...

- Posiadanie awaryjnej dyskietki systemowej
- Regularne dokonywanie kopii zapasowych
- Dezaktywacja niepotrzebnych serwisów (np. WSH - Win Scripting Host)

Usuwanie skutków infekcji

Część strat jest nieodwracalna

Procedura usuwania wirusów infekujących pliki wykonywalne

- Izolacja systemu - odłączenie od sieci
- Doprowadzenie systemu do stanu, w którym z całą pewnością jest ‘czysty’ - uruchomienie z dyskietki z niezainfekowanym OS
- Uruchomienie skanera - sprawdzenie sektora startowego: usunięcie ewentualnych wirusów
- Normalne uruchomienie systemu i wykonanie procedury dezynfekcji dysków stałych, wymiennych
- Sprawdzenie wszystkich komputerów w sieci
- Zabezpieczenie komputerów programem antywirusowym stale monitorującym system
- Ciągłe uaktualnianie oprogramowania antywirusowego - baz danych wirusów i stosowanych technik przeciwdziałania infekcjom