Corso di Sistemi di Eleborazione
Prof. N. Mazzocca

Attacchi alla sicurezza e Sistemi Anti-Intrusione

Valentina Casola

Introduzione

- PARTE 1:
  - Definizioni e tassonomia di attacchi:
    - Virus,
    - Worm
    - Trojan Horse.
- PARTE 2:
  - Sistemi anti Intrusione (IDS)
    - Tipologie
    - Architetture di riferimento

PARTE 1

Tassonomia degli attacchi e virus

Intrusione: definizione

- Un attacco malizioso è costituito da un insieme di attività che violano le politiche di sicurezza di un sistema.
- An **intrusion** is an attempt to bypass security mechanisms or compromise confidentiality, integrity or availability of systems and data;

Tassonomia degli attacchi

- DARPA taxonomy includes [DARPA 2000]:

  - **DOS** (denial of service) are designed to disrupt a host or network;
  - **R2L** (Remote to local) attackers who do not have an account on a victim machine and try to gain access;
  - **U2L** (User to root) a local user trying to gain privileges as a superuser;
  - **PROBE** programs to scan the network and gain information.

Tassonomia degli attacchi

Other taxonomies include also virus/worms activities:

- A **virus** is a program that inserts itself into one file and then performs some (possible null) action.

- A **worm** is a variant of the virus that can spread itself automatically over the network from one computer to the next. Worms take advantage of automatic file sending and receiving features found on many computers.

Virus

- Un virus è un programma in grado di attaccare uno o più file ed eseguire delle azioni non permesse.
- È possibile dunque individuare due fasi di azione:
  - nella prima fase il virus si attacca ad un file (insertion phase);
  - Nella seconda fase il virus agisce a tutti gli effetti (execution phase).

Pseudo-codice di un virus

- **Beginvirus:**
  - **If** spread-condition **then begin**
    - **For** a set of target file **do begin**
    - **If** target is not infected **then begin**
      - Determine where to place virus instruction, copy them and alter target file to execute added instructions
      - **End; end; end;**
  - Perform some action
  - **Goto** beginning of infected file
- **Endvirus:**

- Alcuni tool per scrivere un virus “semplice”: VCS, VCL e MPC

Tipi di virus: Boot sectors infectors

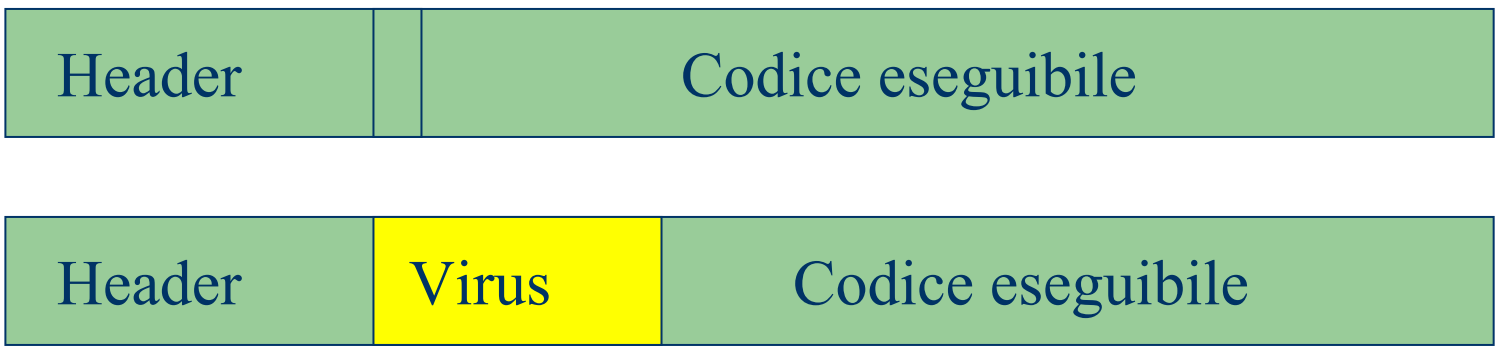
- Attaccano i settori di boot di un disco (floppy o hard drive) e/o il Master Boot Record (MBR) di un disco ;
- I settori di boot sono una parte del disco usati per avviare il sistema o montare un disco; il codice in esso contenuto viene eseguito quandi il sistema vede il disco per la prima volta;
- Se in esso è presente un virus, questo verrà eseguito (tipicamente sposta il codice di boot in un altro settore)

Virus Brian: un esempio di boot sector infector

- Quando il sistema parte da un disco infettato, il virus viene caricato.
- Il virus modifica il vettore delle interruzione del disco facendo in modo che appena viene inserito un disco l'interruzione punti al virus in memoria che viene così attivato copiando se stesso in altri settori del disco (si replica).

Executable infectors

- Un virus eseguibile attacca un programma eseguibile (tipicamente con estensioni COM o EXE):



Jerusalem: un esempio di executable infectors

- Jerusalem viene attivato (trigger) quando un programma infetto viene eseguito.
- Modifica un registro di sistema e si sostituisce al servizio delle interruzioni del clock, verifica l'anno e la data se non è un giorno prefissato non fa nulla ma risiede in memoria, se è Venerdi 13 del 1987 attiva un flag di "distruzione" ed ogni volta che viene chiamato un file con estensione .com o .exe questo viene infettato.

Multipartite Virus

- A un virus che può infettare file di boot o eseguibili.
- E tipicamente composto da due parti, ognuna capace di infettare una specifica parte del sistema (implementano più strategie di attacco).

TSR Virus

- “Terminate and Stay resident”
- Virus che rimangono attivi in memoria anche dopo che l’applicazione è terminata;
- I virus che non sono TSR vengono attivati solo quando l’applicazione attaccata viene eseguita.

Stealth virus

- Tentano di essere invisibili; intercettano chiamate al sistema operativo; quando un achiamata cerca di prendere attributi o leggere il file, il virus non agisce restituendo i valori ed il comportamento reale, quando il file infetto viene eseguito, il virus si attiva.
- Ecco perché molti anti-virus devono essere avviati da un floppy “pulito” e fidato.

Macro virus

- È un virus composto da una sequenza di azioni che viene interpretata e non eseguita direttamente;
- Ad esempio il virus Melissa attacca file Word97 attivandosi con le Macro di Word (copiava se stesso nel template del documento, invocava un client di posta ed inviava copie di se stesso ad indirizzi presi dalla rubrica).
- Tipicamente usano programmi specifici, non attaccano tutti….

Worm

- Un worm è un programma che copia se stesso da un computer ad un altro, non ha bisogno di attaccarsi ad un file per diffondersi.
- Tipicamente utilizzano programmi di file sharing per diffondersi da un PC all'altro connessi in rete.

Trojan Horse

- Un trojan Horse è un programma con un duplice effetto:
  - Il primo effetto è visibile e noto,
  - Il secondo effetto è inaspettato.
- Esempio: il programma NetBus permette di controllare da remoto un sistema Windows NT su cui è stato installato un server (NetBus) che viene avviato in fase di avvio dal SO.

Anti Virus

- I meccanismi antivirus più popolari sono basti su file-scanner che cercano “file modificati”.
- In particolare gli antivirus utilizzano un database di virus-signature che viene aggiornato costantemente,
- Altri antivirus usano degli integrity scanner in grado di determinare se un file è stato modificato ma non sono in grado di riconoscere l’attività di un virus.