

Virus del Settore di Avvio

Realizzata da Monteforte Carlo

Prof. Alfredo De Santis

Anno Acc. 2001 / 2002

Virus

Il termine **Virus**, nel senso più generale possibile, indica un qualsiasi frammento di codice, di lunghezza variabile, che penetrando nel sistema si dimostra potenzialmente in grado di danneggiarlo.

Si può parlare allora di *malware* cioè malicious software.

Classificazione

Sotto questo aspetto, un *codice nocivo* può essere così classificato:

- trojan horse (cavallo di troia)
- worm (verme)
- virus propriamente detto (veleno)

Trojan horse

Programma distruttivo pronto a esplodere.

Lo scopo principale è di danneggiare esplicitamente il sistema infetto.

Il nome deriva dal fatto che vengono spesso distribuiti sotto false spoglie (in programmi ambiti all'utenza).

BAT-trojan

Un semplice esempio di cavallo di troia è quello che si nasconde nei file *Batch* di MS-DOS. Esempio:

```
@FORMAT C: /AUTOTEST oppure
```

```
@DELTREE /y C:\*.*
```

/AUTOTEST è una back door di FORMAT

@ nasconde l' echo sul video

Worm

Programma che prolifera sulle reti. Si rigenera da solo sfruttando *bug* del sistema operativo.

E' un frammento di codice che esiste solo in memoria; consuma le risorse di sistema e si auto-propaga.

Non necessita di un programma portatore.

Worm

Famoso quello di Robert Morris.

Il suo verme contagiò i sistemi Unix il giorno 2 Novembre 1988.

Sfruttava un *buffer overflow* presente nei programmi finger e sendmail per irrompere nelle macchine che adottavano il s.o. Berkeley Unix.

Virus

Sequenza di istruzioni il cui scopo è di inglobarsi e confondersi tra le istruzioni di altri programmi, modificandoli.

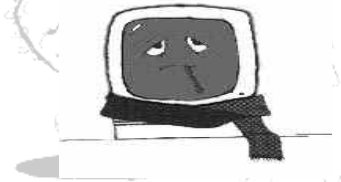
Attende il verificarsi di particolari condizioni.

Possono essere:

- distruttivi (sovrascrivono l' hard drive)
- innocui (fanno comparire un messaggio)

Virus

Una prima classificazione si può ottenere se si guarda in modo specifico il funzionamento.



Vediamo una possibile suddivisione.

Floppy Boot e MBR virus

Si installano nel Boot sector o nell'MBR del disco fisso.



A volte cambiano l'indirizzo di avvio in modo da farlo corrispondere a un nuovo settore modificato e dannoso.

File virus

Infettano file eseguibili.

Sostituiscono del codice o semplicemente ne aggiungono di nuovo.

Sfruttano il file system del sistema operativo per propagarsi.

Macro virus

Stragrande maggioranza dei virus in circolazione. Sono la moda del momento.

Prendono di mira fogli elettronici e database dei pacchetti software di largo consumo (Office).

Si propagano con le Macro, cioè procedure automatiche presenti nei documenti.

Macro virus

Documento originale

Header
Dati di sistema
Testo
Fonts
Macro
Altro

Documento infetto

Header
Dati di sistema
Testo
Fonts
Macro
Altro

**Macro
Virus**
←

Virus Multipartito

Virus di categoria avanzata. Tenta attacchi verso diversi oggetti:

- MBR + file eseguibili
- floppy + MBR + file
- file + macro
- file eseguibili DOS + file eseguibili WINDOWS

Caratteristiche

Una regola comune di tutti i virus è di avere un algoritmo di lavoro che gli consenta di entrare nel sistema.

In base alle caratteristiche di cui dispongono, si possono individuare diverse classi di virus.



Virus Companion

Semplici e facili da rimuovere, sfruttano i buchi offerti da MS-DOS.

Sostituiscono un file eseguibile con uno con lo stesso nome, ma estensione .COM. La maggiore priorità gli consente di avere un'esecuzione non voluta dall'utente.

TSR

Terminate and Stay Resident.

Lasciano una loro parte nella memoria RAM e intercettano le system call per diffondersi.

Operazioni a rischio:

- apertura di file
- esecuzione di file
- accesso a disco

Stealth virus

"C'è ma non si vede."

E' una tecnica che consente a un virus di diventare invisibile, cioè di scomparire se qualcuno ne va a verificare la presenza.

Si intercettano le letture / scritture del sistema operativo per infettare altri oggetti.

Stealth – Size hiding

Possibile scenario:

File originario = 100 byte

Virus = x byte

File infetto = 100 + x byte

Il virus in *listening*, si accorge dell'esecuzione di comandi tipo DIR e da come output

(100 + x) – x byte

Polimorfici

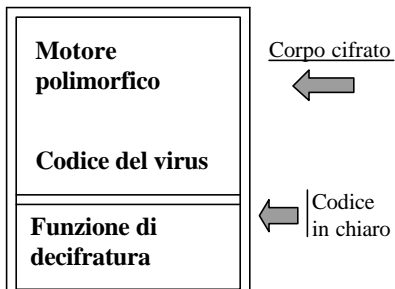
Un virus è polimorfico se riesce ad infettare un oggetto con un codice virale sempre differente.

Sfruttano un *polymorphic engine* per cifrare le istruzioni.



Polimorfici

Virus = corpo cifrato + corpo in chiaro.

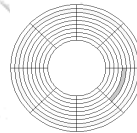


Boot virus

Il virus contagia il primo settore del disco fisso (MBR) o il primo settore del dischetto (Boot sector).

Questi settori sono deputati a contenere codice che serve per l'avvio della macchina (Boot loader).

Problema: il settore è lungo solo 512 byte.



Il Bootstrap

E' il nome che si da alla procedura eseguita per il riavvio o per l'accensione a freddo della macchina. Tale processo coinvolge il Bios

Basic Input / Output System

La lettura dei dati è all'indirizzo

traccia 0,

testina 0,

settore 1.



Il Bootstrap

Il Bios legge il codice e lo pone all'indirizzo 0:7c00h.

Il codice potrebbe essere danneggiato e il disco sarà marcato come non *bootable*.

Se tutto è andato a buon fine, compresi i controlli hardware, il sistema operativo sarà portato sulla RAM.

Il Bootstrap

Come sono strutturate le istruzioni del Boot sector ?

Poiché il sistema operativo non è ancora disponibile, le chiamate di sistema sono limitate.

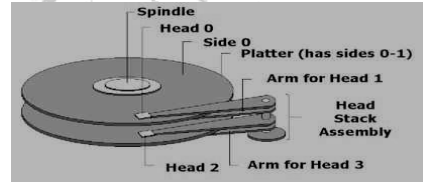
Si può disporre di:

- interrupt
- strutture offerte dal Bios

MBR

Acronimo di

Master Boot Record.



Oltre al codice di avvio include la tavola delle partizioni.

MBR

Struttura della partition table

- max 4 entrate
- ogni *entry* dispone di 16 byte
- è indicato dove inizia e finisce la relativa partizione
- una sola partizione attiva

Il Boot generico

Ogni partizione su disco può contenere un diverso sistema operativo.

Come si fa a caricare il sistema in memoria ?

Chiaramente ogni partizione riserva spazio per conservare il codice vero e proprio per lanciare il sistema operativo.

Chiamiamo tale spazio Boot di partizione.

Il Boot generico

Oltre al codice, tale settore contiene la FAT – File Allocation Table - e una serie di informazioni che la riguardano

dal terzo al trentunesimo byte.



Boot floppy

E' l'mbr relativo ai dischetti.

Corrisponde sempre al primo settore.

La struttura è la stessa del Boot di una partizione.

File system differente.



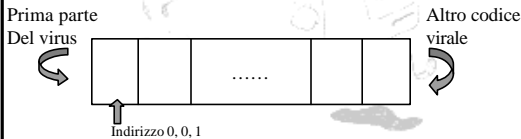
Non c'è spazio

Il virus deve stare nel settore di avvio per infettare il sistema, quando questo viene acceso.

Ma se non c'entra ?

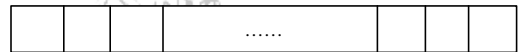
Solo 512 byte

Tipicamente il settore *target* contiene solo la prima parte del codice. Il resto va in altri settori.

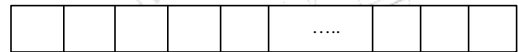


Non c'è spazio

Disco non infetto



Disco infetto



Non c'è spazio

Ovviamente il virus deve stare attento a dove scrive il suo codice.

Una cattiva scelta potrebbe essere fatale.

Due possibili metodi.



Non c'è spazio - 1

Si abbassa la misura dei drive logici.

Il virus sottrae i numeri necessari dai campi corrispondenti del BPB Boot sector e dalla tavola delle partizioni dell' hard disk.

Cioè si sottrae la memoria disponibile al sistema vista dal Bios, dello spazio necessario.

Non c'è spazio - 2

Si registrano i dati fuori dalle partizioni fisiche dell' hard disk.

Il codice è allora messo fuori dai bordi dello spazio visto come disponibile.

deve essere permesso dall' hardware

Coesistenza

Il settore di avvio è seguito direttamente dal virus.

Alcuni parassiti come *Brain* e *Ping-Pong* marcano i cluster che hanno occupato per memorizzare tali informazioni come *Bad cluster*.

Si deve accedere alla FAT

il sistema non li riscriverà

Residenza

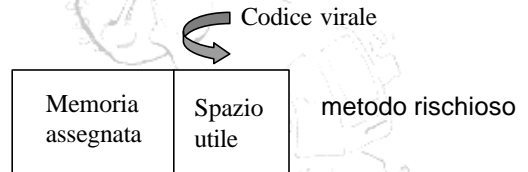
Per entrare in memoria, il virus deve ingannare il sistema.

E' necessario allora diminuire la misura della memoria che il sistema prevede.

La quantità di memoria è posta all'indirizzo 40h:13h e se si riscrive questo numero della giusta misura, si ottiene il posto dove copiare le istruzioni.

Residenza

Alternativamente si può utilizzare la memoria non ancora assegnata, oppure si rimane in memoria fino all'avvio del sistema operativo.



Hooking

Per replicarsi, il codice virale deve intercettare le chiamate a scritture / letture su dischetti o dischi.

Si tratta dell' hooking (aggancio) verso le system call più importanti.

Particolarmente utile l'interrupt *int 13h*.

Hooking, ma non troppo

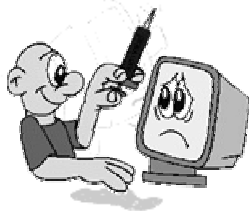
Intercettare tutte le chiamate a scritture o a letture verso dispositivi lenti (floppy) può essere controproducente.

Troppi accessi ai file possono insospettire l'utente.

L'infezione

L'ultima fase.

Si deve constatare se il bersaglio è già stato infettato e in caso negativo si porta avanti l'attacco.



L'infezione

```
Infect_boot( )
do
  signature = get_string();
  while (1234567 not in first_line);
insert_code();
```

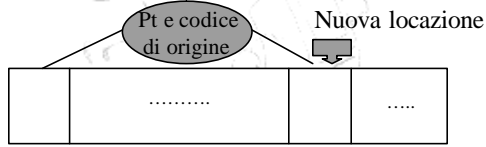
1234567 è l'ID del codice virale

Una funzione permette di avere la firma del virus. Se questa non c'è allora inizia l'*iniezione* del codice.

L'infezione

E' spesso utile salvare alcune informazioni quando si riscrive l'mbr.

Potrebbe essere necessario ad esempio copiarsi la tavola delle partizioni, oltre al loader originale.



L'algoritmo

- il virus libera una certa quantità di memoria
- copia se stesso sulla memoria libera
- legge il resto dal disco (se c'è)
- intercetta i necessari vettori degli interrupt
- esegue operazioni aggiuntive dipendenti dal particolare virus
- passa il controllo al Boot sector originale salvato e gli dà il controllo

L'algoritmo

Esistono virus di Boot non residenti.

All'avvio infettano l'mbr dell' hard disk o dei dischetti.

Poi passano il controllo al loader primitivo e vanno ad influenzare le operazioni di sistema.



Stealth

Perché salvare il vecchio settore di avvio ?

Se un antivirus andasse a controllare tale spazio, si accorgerebbe dell'inganno.

Un gestore di interrupt rileva l'operazione di lettura e mette appunto una *redirezione* verso il settore primitivo.

MBR STEALTH

tutto in regola

Istruzioni cianfrusaglia

Per confondere il software antivirus, il programmatore intermezza le istruzioni virali con altre inutili, ma fuorvianti.

Esempio:

```
050000 ADD AX, 0000
83C600 ADD SI, +00
83C500 ADD BP, +00
```

Si sta sommando 0 a un registro a 16 bit

Riparazione - 1

Caso semplice: si individua il settore originale e lo si ripristina.

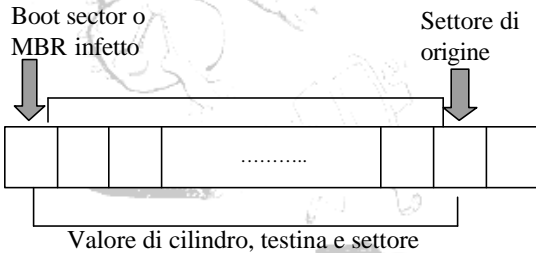
Boot sector o MBR infetto

Settore di origine



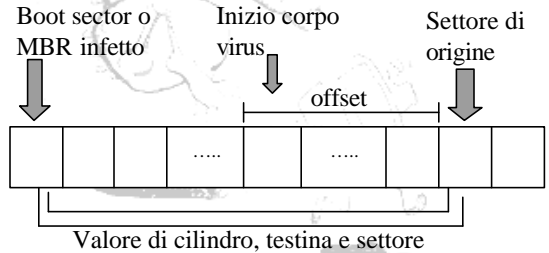
Riparazione - 2

Potrebbe essere necessario individuare l'indirizzo del settore (logico o fisico).



Riparazione - 3

L'indirizzo potrebbe puntare al primo settore del corpo del virus. E' necessario calcolare l'offset.



Diffusione

I Boot virus sono molto comuni.

A differenza dei virus residenti nei file, non hanno mai subito un rallentamento rimarchevole.



Come mai sono sempre stati attuali ?

Diffusione

Un raffreddore è un virus biologico geneticamente evoluto, se paragonato a malattie più dannose.

Boot virus ↔ Raffreddore

File virus ↔ Influenza

Diffusione

Il graduale passaggio dai sistemi DOS a quelli Windows, ha permesso ai virus di Boot di sopravvivere nonostante le nuove tecniche virali.

Questo perché Windows si è rivelato particolarmente resistente a tali virus, e viceversa non è in grado di essere operativo se contagiato da un virus residente nei file.

Diffusione

Dunque al pari di un raffreddore, un virus di Boot si presenta spesso come un semplice fastidio.

A volte l'utente si accorge dopo mesi di essere stato contagiato.

Se così, non ha alcuna ragione di debellare il male.

Michelangelo

Virus scoperto nei primi mesi del 1991.

Caratteristica peculiare:

se il sistema infetto è riavviato il giorno 6 Marzo di ogni anno, il virus sovrascrive l' hard disk con dati casuali.

il 6 Marzo è il compleanno del famoso artista

Michelangelo

Nei giorni che precedettero tale data, Michelangelo divenne l'evento di maggior attrazione.

Tutti ne temevano il potenziale distruttivo.

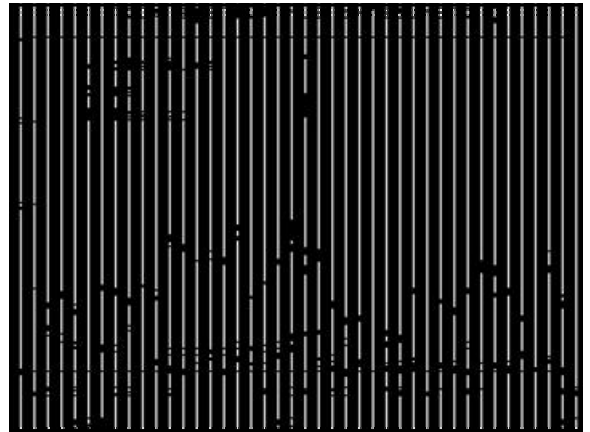
Allarmanti predizioni portarono a milioni il numero di sistemi che sarebbe crollato per il contagio.

Michelangelo

Il crollo totale non si verificò mai. La gente si armò infatti di prodotti antivirus di tutti i generi.

Di conseguenza, in quel periodo, furono dichiarate numerosissime infezioni, non a causa di un'esplosione incontrollata di virus, ma solo perché la gente fece più caso alla loro presenza.

Si parlò allora di *Michelangelo Madness*.



Come si comporta Windows

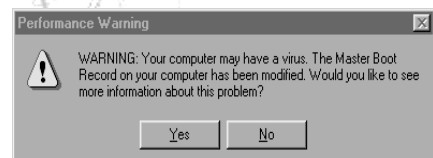
Windows non dispone di protezioni contro i virus di Boot.

Con la serie DOS 6.xx, la Microsoft ha affrontato la prima e l'ultima avventura nel mondo dell'antivirus.

Ha delegato terze parti per lo sviluppo di barriere antivirali.

Warning

Il sistema si limita ad avvertire l'utente che potrebbe essere stato contagiato.



Sintomi di infezione

- il computer non è in grado di avviare il sistema operativo
- il computer non può avviare dal disco rigido
- il sistema MS-DOS riferisce una quantità di memoria base non uguale a 640 kb
- nell'accedere a floppy o all' hard disk viene segnalato che il disco non è di sistema
- blocco della memoria o dei programmi in uso

Una semplice verifica

In MS-DOS un virus del settore di Boot può essere così rivelato:

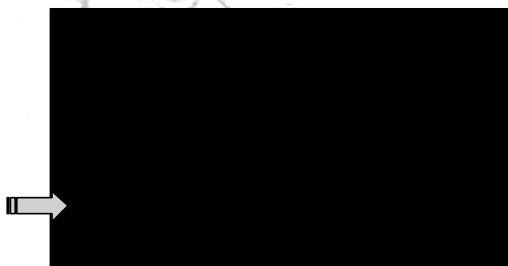
- si chiede il *prompt* dei comandi
- si esegue il comando CHKDSK
- la quantità di memoria complessiva deve essere esattamente 655.360 byte

$$640 * 1024 = 655.360$$

altrimenti è probabile un contagio

Una semplice verifica

L'output di CHKDSK:



Disinfestazione

Nei casi più gravi è necessario:

- formattare l' hard disk e reinstallare il sistema
- reinstallare i programmi da copie sicure
- ripristinare solo i dati dalle copie di back-up

gli eseguibili potrebbero essere infetti

Software antivirus

Un antivirus non deve limitarsi a rivelare ed eliminare solo i virus noti.

Tecniche polimorfiche renderebbero il prodotto inoffensivo.



Una classe avanzata di software antivirus dispone di scanner euristico.

Tecniche di rilevamento

Gli antivirus hanno sviluppato tecniche di rilevamento che, se usate contemporaneamente, garantiscono, con ottima probabilità, di rivelare un computer virus.

I prodotti antivirus si possono raccogliere in tre categorie.

Programmi di monitoraggio

Controllano attività sospette, come la richiesta di formattazione del disco rigido o l'accesso a zone privilegiate di memoria.

Utili come una prima linea di difesa.

facili da scavalcare

Scanner

Confrontano le firme contenute in un database interno con quelle eventualmente contenute nei file infetti.

Dispongono di tecniche euristiche che usano per file cifrati o sconosciuti.

Possono lavorare
in *background*

Programmi detection

Si basano su due tecniche:

- verifica dell'integrità, cioè calcolano un valore hash dei file, lo registrano e poi su richiesta effettuano un nuovo calcolo per verificare se i vecchi file hanno subito qualche modifica;
- tecniche euristiche, cioè salvano informazioni sufficienti per ripristinare un file, nel caso questo venisse danneggiato da un parassita.