



# Virus informatici

## Approfondimenti tecnici per giuristi

---

Ciclo dei seminari  
Informatica nei laboratori del CIRSFID

Facoltà di Giurisprudenza  
Università di Bologna



# Argomenti trattati

---

- Malware
- Virus
- Struttura dei software antivirus
- Falsi positivi ed errori di valutazione
- Esempi pratici



# Malware - definizione

---

Software, meglio definito come “Programma malvagio”, creato con il solo scopo di causare danni ad un computer o ad una rete di computer dove viene eseguito.



# Malware, funzionano sempre?

---

Domanda: Se io eseguo un file per Windows, e i software antivirus mi classificano quel file come malware, su un computer che utilizza come sistema operativo Mac OS X o Linux, cosa succede?

Risposta: **NULLA!**

I malware sono "scritti" per funzionare solo su architetture ben definite e non generiche.

(Eccezione virus scritti in Java)



# Malware - categorie

---

- Virus
- Worm
- Trojan horse
- Backdoor
- Spyware
- Dialer (errato)
- Hijacker (errato)
- Rootkit



# Malware - Worm

---

Programmi che sfruttano vulnerabilità del sistema operativo o delle applicazioni utilizzate per diffondersi e per eseguire codice "maligno" all'interno del sistema attaccato.

Esempio: Il worm Blaster sfruttava una vulnerabilità di Windows XP e 2000 che permetteva l'attaccante di riavviare il computer senza l'autorizzazione dell'utente utilizzatore del pc.



# Malware – Trojan horse

---

Conosciuto come “cavallo di Troia”, è un tipo di malware che se eseguito permette l'intrusione dall'esterno nel sistema da parte dell'attaccante.

Esempio: Sub Seven, famoso cavallo di Troia che seminava il panico ai tempi di Windows 95/98 e della totale disinformazione in materia di software antivirus.



# Malware – Backdoor

---

Letteralmente “porta sul retro”, sono dei programmi nascosti all’interno di altri programmi che permettono l’accesso ad un sistema nella totale inconsapevolezza dell’utente utilizzatore.

Esempio: Tutti i trojan horse nascondono backdoor che permettono l’accesso da parte dell’attaccante per prendere il controllo del sistema.



# Malware - Spyware

---

Programmi utilizzati per la raccolta e trasmissione di informazioni del sistema dell'utente su cui è installato.

Le informazioni acquisite possono andare dalle abitudini di navigazione dell'utente fino alle password utilizzate e memorizzate nei vari profili.



# Malware - Dialer

---

Programmi che gestiscono connessioni tramite normale linea telefonica analogica o digitale (56k o isdn) per fornire servizi di connettività (spesso a pagamento).

**Generalmente non sono malware.** Spesso però vengono definiti tali date le non chiare condizioni di utilizzo dei servizi da parte dei gestori.



# Malware - Hijacker

---

Programmi che alterano il funzionamento di browser (ad esempio Internet Explorer) per consentire l'apertura automatica di popup, spesso pubblicitari, recando disagi durante la navigazione.

**Generalmente non sono malware**, a meno che il programma non alteri in modo permanente l'utilizzo del browser aprendo popup all'infinito anche in siti diversi da quello visitato che ha "installato" l'applicazione.



# Malware – Virus

---

Programmi che si diffondono “copiandosi” all’interno di altri software o all’interno dei file del sistema infetto in modo tale da essere eseguiti nel maggior numero di volte possibili.

I virus attuali si diffondono anche tramite reti di computer locali o Internet.



# Malware – Virus

---

Non sempre un virus reca un danno “visibile” al sistema come ad esempio la cancellazione di file vitali al sistema.

Esistono virus creati con unico scopo di rallentare le funzioni del computer occupando risorse inutilmente.



# Malware – Virus del 2000

---

La maggioranza dei virus informatici, si moltiplicano e diffondono utilizzando le vulnerabilità dei client di posta elettronica (ad esempio Outlook Express), diffondendosi utilizzando gli indirizzi e-mail memorizzati all'interno dei client.



# Antivirus - definizione

---

Software sviluppato per l'identificazione, riparazione o eliminazione di malware informatici atti al danneggiamento del sistema.

- Northon
- Sophos
- Panda
- Antivir
- Avg



# Antivirus - funzionamento

---

2 metodi per l'analisi del file:

- Ricerca euristica: consiste nell'analisi del comportamento dei vari programmi cercando istruzioni sospette perché tipiche del comportamento dei virus (esempio: alterazione del contenuto di un file di sistema)
- Ricerca dello schema: consiste nell'analisi della struttura del file associando il file analizzato a tutti gli schemi conosciuti presenti nella lista virus del software antivirus.



# Antivirus – falso positivo

---

Può capitare che un antivirus considera dei file o programmi come virali (potenzialmente infetti) anche se in realtà non lo sono.

Tutto questo è dovuto al fatto che un insieme di istruzioni che compongono un virus (od una sua parte) può essere presente anche in programmi e file "normali" o possono essere ottenuti come combinazione casuale in un file di dati salvati non in formato testo.



# Antivirus – falso positivo

---

Si ha un falso positivo quando un software antivirus definisce “virale” un file o un programma quando in realtà non lo è.

Spesso è un errore di valutazione che alcuni software antivirus compiono; con molta probabilità, un file considerato potenzialmente virale da un antivirus X può essere considerato diversamente (non infetto) dall'antivirus Y.



# Antivirus – falso positivo

---

Perché accade?

- Gli algoritmi usati per la classificazione dei file sono diversi a seconda del software antivirus che si sta utilizzando. Essi sono proprietari e sviluppati dalle rispettive software house che non rendono pubblici i loro metodi di rilevazione
- Non esiste un ente che regolamenta la classificazione dei virus e che “metta d’accordo” le aziende
- Le software house che producono antivirus non collaborano tra di loro.



# Antivirus – caso pratico

---

Scenario: viene fatta una denuncia al soggetto X per danni ai soggetti Y per aver diffuso un file sul proprio sito Internet che, a dir della polizia postale, è un virus perchè al momento della scansione, il software antivirus l'ha rilevato come tale.

Come deve intervenire un avvocato per difendere il cliente X?



# Analisi forense - definizione

---

Disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova.



# Analisi forense

## Rilevanza della perizia informatica

---

Le software house che producono software antivirus non possono essere considerate come "enti certificatori", pertanto i report delle scansioni di sistema che segnalano la presenza di virus non hanno alcun valore probatorio "certificato" se non verificato tramite l'analisi forense del file sospetto.



# Analisi forense

## Rilevanza della perizia informatica

Per determinare se un file o un programma classificato come virus da un software antivirus sia veramente un virus, bisogna verificare ed analizzare, in un ambiente "asettico", il funzionamento del programma.

Come?



# Analisi forense

## Rilevanza della perizia informatica

---

Una possibile soluzione consiste nel creare uno scenario dove viene verificata la veridicità dell'accusa simulando il download dell'applicazione testandola su una macchina creata appositamente per verificare e monitorare il funzionamento del file preso in esame.



# Riferimenti

---

- [http://www.dm.unibo.it/~maioli/docs/fti\\_informatica\\_3009.doc](http://www.dm.unibo.it/~maioli/docs/fti_informatica_3009.doc)
- <http://it.wikipedia.org>
- [http://it.wikipedia.org/wiki/Virus\\_%28informatica%29](http://it.wikipedia.org/wiki/Virus_%28informatica%29)

