Corso di Informatica

Utilità

2–I virus informatici

Prerequisiti

- Concetto intuitivo di applicazione per computer
- Uso pratico elementare di un sistema operativo

Introduzione

La sicurezza informatica è un requisito che deve essere garantito, specialmente quando i dati sono riservati o importanti.

Data la grande diffusione di **virus informatici**, è importante conoscere gli strumenti per proteggere i proprio computer da attacchi o infezioni di varia natura.

Pertanto, è importante disporre di appositi **software antivirus**, per la protezione dei sistemi. In questa Unità vediamo alcune di queste applicazioni.

Cosa è un virus informatico

In prima approssimazione, possiamo dire che i **virus informatici** sono programmi che si insediamo nel software presente sul computer (dati o programmi) e che hanno finalità di disturbo, di furto di informazioni o di danneggiamento.

Spesso hanno la capacità di autoreplicarsi, ossia di riprodursi, e quindi diffondersi nel computer, ogni volta che viene aperto il file infetto.

La diffusione può avvenire attraverso la rete, i CD-ROM la pen drive o altri drive esterni e può provocare danni a volte irreparabili ai dati o al funzionamento del computer.

Gli effetti dei virus

Un **virus** (dal latino = *veleno*) è scritto intenzionalmente per alterare il funzionamento del computer, senza che ciò venga autorizzato o rilevato dall'utente.

Un virus, oltre a replicarsi, può causare:

- comportamento anomalo del sistema e danni hw e/o sw;
- causare spreco di risorse (RAM, CPU, spazio su disco), con peggioramento delle prestazioni del sistema;
- causare confusione, come visualizzare messaggi inutili.

I danni da virus informatici

I danni più comuni sono:

- intasamento del server della posta
- eliminazione o modifica di file e archivi
- perdita di informazioni riservate
- danneggiamento di programmi o del sistema operativo
- formattazione degli hard disk
- surriscaldamento della CPU
  - aumentando a dismisura la frequenza del clock (**overclocking)**
  - arrestando la ventola di raffreddamento

Tipi di virus

Esistono molti tipi di virus, ognuno caratterizzato da:

- modalità di trasmissione,
- grado di invasività
- gravità dei danni che può generare.

Ad oggi ne sono stati classificati diverse decine di migliaia, ma ogni giorno ne vengono creati di nuovi

Tipi di virus

Esistono molti tipi di virus, ognuno caratterizzato da:

- modalità di trasmissione
- grado di invasività
- gravità dei danni che può generare

Ad oggi ne sono stati classificati diverse decine di migliaia, ma ogni giorno ne vengono creati di nuovi.

Tipi di virus

I virus, in generale, appartengono alle seguenti categorie:

- **worm**
- **trojan**
- **dialer**

e la fonte più comune di contagio odierna è Internet.

Tipi di virus
1) worm

Un **worm** (letteralmente "verme") è una particolare categoria di virus in grado di autoreplicarsi, ma, a differenza dei comuni virus, non necessita di legarsi ad altri programmmi eseguibili per diffondersi.

Il termine deriva da un romanzo di fantascienza degli anni '70 di John Brunner: alcuni ricercatori, notarono le somiglianze tra il loro programma e quello descritto nel libro e ne adottarono il nome.

Tipi di virus
1) worm

Uno dei primi worm diffusi in rete fu **Internet Worm**, creato agli albori di Internet nel 1988, da Robert Morris, figlio di un dirigente della **NSA** (*National Security Agency*) e riuscì a colpire tra le 4000 e le 6000 macchine (il 4-6% dei computer collegati a quel tempo in rete).

Tipicamente, un worm altera il computer che infetta, in modo da essere eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente.

Tipi di virus
1) worm

Si diffonde principalmente:

- con allegati di posta elettronica;
- sotto forma di *crack* di programmi costosi;
- condividendo file in rete
- *bug* del software

Tipi di virus
1) worm

I danni possono essere:

- *danni diretti* (manomissione diretta del computer)
  - interferenza con softqware installato (*antivirus*, *firewall*);
  - creazione di punti di vulnerabilità (*backdoor*, *keylogger*) da parte di *cracker* o altri virus;
  - alterazione del sistema operativo (spegnimento o riavvio forzati;
- *danni indiretti* (tecniche di intralcio):
  - intasamento della rete locale;
  - spreco di risorse del sistema;
  - intasamento delle caselle di e-mail;
  - invasione delle reti locali.

Tipi di virus
2) trojan

Un **trojan** o **trojan horse** (*Cavallo di Troia*), è un tipo di virus che deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto.

Gli effetti, in genere, non si manifestano subito (da cui appunto il nome) per dare modo al virus di replicarsi attraverso il disco, per cui quando esso si manifesta, potrebbe aver già infettato tutto il disco.

Tipi di virus
2) trojan

I trojan non si diffondono autonomamente come i *worm*, ma dietro un intervento diretto dell'aggressore per far giungere l'eseguibile maligno alla vittima.

A volte agiscono insieme: un worm viene iniettato in rete con l'intento di installare dei trojan sui sistemi.

Spesso è la vittima stessa a scaricare un trojan sul proprio computer, dato che i *cracker* amano inserire queste "trappole" ad esempio nei videogiochi piratati, che in genere sono molto richiesti.

Tipi di virus
2) trojan

Vengono in genere riconosciuti da un antivirus aggiornato come tutti i **malware**.

Se il trojan in questione non è ancora stato scoperto dalle software house degli antivirus, è possibile che esso venga rilevato, con la scansione euristica, come probabile malware.

Dal 2001 i *trojan* furono utilizzati sistematicamente per:
- invio di messaggi spam
- rubare informazioni personali (numeri di carte di credito o indirizzi email
- bloccare l'aggiornamento di antivirus

Tipi di virus
3) dialer

Un **dialer** è un programma per computer di pochi *kilobyte* che crea una connessione ad Internet, a un'altra rete di calcolatori, o semplicemente a un altro computer, tramite la comune linea telefonica o un collegamento ADSL.

Un **dialer virus** connette l'utente ignaro ad utenze telefoniche con elevata tariffazione, spesso nascondendo frodi e truffe, di cui l'utente verrà a conoscenza solo al momento della fatturazione dei consumi, in bolletta.

Trasmissione di virus

I mezzi più comuni di trasmissione di un virus sono:

- allegati alla posta elettronica**.** Può avvenire:
  - volontariamente
  - inconsapevolmente, il mittente non sa di aver inviato un allegato infetto
  - in modo trasparente all'utente, la e-mail parte autonomamente
- scambio di supporti infetti (floppy disk o pen drive)
- programmi di messaggistica immediata
- scaricamento di file o programmi infetti durante la navigazione in Internet (anche semplicemente visitando un sito web infetto)

Come funzionano i virus

Un virus è un programma composto da un numero molto ridotto di istruzioni e che usa le minime risorse del sistema (RAM, CPU, dischi) in modo da rendersi il più possibile invisibile.

Tuttavia, un virus di per sé non è un programma eseguibile: per essere attivato, deve infettare un programma ospite (in genere, i programmi eseguibili, quindi scritti in binario).

Come funzionano i virus

Spesso, un virus funziona nel seguente modo:

- inserisce una copia di sé stesso in fondo al programma ospite;
- pone, tra le prime istruzioni del programma ospite, un'istruzione di salto alla prima linea della sua copia;
- alla fine della copia esegue un altro salto all'inizio del programma ospite.

In questo modo quando un utente lancia un programma infetto, viene dapprima impercettibilmente eseguito il virus, e poi il programma.

L'utente vede l'esecuzione del programma e non si accorge che il virus è ora in esecuzione in memoria e sta compiendo le varie operazioni di disturbo contenute nel suo codice.

Il software antivirus

Affinché il proprio sistema sia protetto da virus è necessario installare un software **antivirus**.

Un software antivirus è in grado di:

- individuare i virus conosciuti fino a quel momento (e presenti nel suo database)
- in alcuni casi, di riconoscere comportamenti anomali riconducibili alla presenza di virus non ancora conosciuti.

Il software antivirus

In pratica, è opportuno:

- installare un programma antivirus e mantenerlo costantemente *aggiornato*;
- usare programmmi antivirus *specifici per reti locali*;
- usare programmi antivirus *specifici per Internet* (*Internet Security*).

Come agisce un antivirus

L'antivirus attivo esegue automaticamente la scansione dei file utilizzati dall'utente, con particolare attenzione:

- ai file provenienti da Internet
- ai file provenienti da unità disco esterne
- ai programmi di messaggistica.

Le fasi di azione di un antivirus sono:
- rilevamento
- riparazione o eliminazione in caso di riconoscimento

Disinfezione dei file

Un antivirus non è in grado di proteggere il sistema da tutti i virus esistenti, tuttavia l'utente che ne è sprovvisto è esposto a sicuro contagio.

La presenza di un virus nel sistema viene solitamente comunicata all'utente tramite una finestra di dialogo in cui sono riportati:

- nome del file infetto
- nome del virus.

Viene chiesto all'utente quale tipo di azione si desidera effettuare, se la riparazione o l'eliminazione, operazione detta disinfezione del file.

Disinfezione dei file

Un file non riparabile può anche essere messo in **quarantena**, ovvero può essere isolato dagli altri file per evitare un ulteriore contagio, in attesa che i futuri aggiornamenti del software antivirus lo mettano in condizione di disinfettare il file.

Proteggersi dai danni

Per garantire una buona protezione del sistema e dei dati presenti, sono sufficienti in genere, alcune precauzioni, adottando le quali, si possono scongiurare danni e disastri informatici.

In genere, è sufficiente:

- aggiornare periodicamente il software antivirus;
- scansionare periodicamente i vari supporti di memoria;
- accertarsi di utilizzare media affidabili

Proteggersi dai danni
1) Aggiornamento dell'antivirus

Da quanto detto, consegue la necessità di effettuare un aggiornamento continuo del software antivirus, per aggiungere le definizioni dei nuovi virus che ogni giorno vengono creati.

In genere, l'aggiornamento può essere fatto:

- scaricandolo dal sito del produttore dell'antivirus
- mediante una apposita funzionalità dell'antivirus per il *download* automatico via Internet.

È bene notare che non è consigliabile installare più di un antivirusa sulla stessa macchina, in quanto, oltre ad appesantire le operazioni, si rischia che uno di essi venga scambiato dagli altri come virus, con conseguenti conflitti e malfunzionamenti

Proteggersi dai danni
2) Scansione periodica dei dischi

Oltre all'aggiornamento, è indispensabile periodicamente far effettuare all'antivirus delle **scansioni periodiche** di tutte le unità disco e della memoria.

Proteggersi dai danni

3) Utilizzare media affidabili

È bene comunque:

- inserire nei drive (CD, DVD, penna, floppy) soltanto supporti di origine certa
- effettuare sempre una scansione con antivirus dei supporti sconosciuti
- non aprire mai messaggi di posta elettronica provenienti da mittenti sconosciuti
- effettuare sempre una scansione con antivirus degli allegati ai messaggi di posta elettronica

Virus e Linux

Linux (e quindi Ubuntu) può dirsi immune ai virus con una sicurezza che sfiora il 100% per vari motivi.

Gli “exe” di Windows (fortemente attaccabili) funzionano spesso tramite **Wine** (che emula le librerie Windows in ambiente Linux). Questi “exe” non si interfacciano quindi direttamente con Ubuntu (né possono farlo perché non ne sono ingrado), quindi il massimo danno può consistere nel dover reinstallare Wine.

Virus e Linux

Il malware per sistemi Unix esiste da quando esiste Unix; soprattutto per i server, ma è difficile "bucare" il sistema poiché:

- ha un rigido sistema dei permessi, che impedisce a chiunque l'accesso ai file di sistema (cosa che non vale per XP e per provarlo basta vedere quanto sia facile cancellare una cartella di sistema con effetti disaetrosi… meglio non provarci!)
- esiste una grande varietà di sistemi basati su Linux, ma diversi tra loro, per cui realizzare virus validi per tutti è effettivamente impresa scoraggiante.

Virus e Linux

Tuttavia, negli ultimi anni, sono venuti fuori anche antivirus molto potenti per il malware (raro) che colpisce i sistemi Unix.

In particolare

- **avast! Linux Home Edition**
- **Virus Scanner.**

Argomenti

- Cos'è un virus informatico
- Gli effetti dei virus
- I danni da virus informatici
- Tipi di virus
  1. worm
  2. trojan
  3. dialer
- Trasmissione di virus
- Come funzionano i virus
- Il software antivirus
- Come agisce un antivirus
- Disinfezione dei file
- Proteggersi dai danni
  1. Aggiornamento dell'antivirus
  2. Scansione periodica dei dischi
  3. Utilizzare media affidabili
- Virus e Linux

Altre fonti di informazione

- V. bibliografia