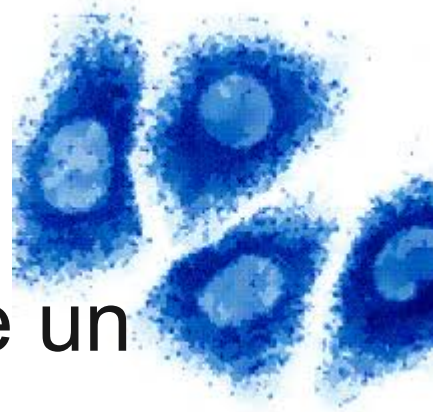


Cos'è un VIRUS?



E' un elemento software, in più specifico è un **malware** (software maligno):

- un programma (un eseguibile, quindi con estensione .exe, .bat, ecc..)
- delle sequenze di istruzioni maligne che si appiccicano a un vostro programma.

Questi virus sfruttano le debolezze dei nostri programmi (BUG) per poter fare ciò che vogliono.



Curiosità: "virus" in latino significa veleno.

Copyright by Francesco Pesecco - www.pesecco-francesco.com



Capacità distruttive



A seconda del tipo di danni causati, i virus si classificano in:

- **innocui**: se comportano solo una diminuzione dello spazio libero sul disco senza nessun'altra alterazione delle operazioni del computer (spesso il loro fine è quello di spiarcì);
- **non dannosi**: se comportano solo una diminuzione dello spazio libero sul disco, col mostrare grafici, suoni o altri effetti multimediali (spesso pubblicitari).
- **dannosi**: possono provocare problemi alle normali operazioni del computer (ad esempio, cancellazione di alcune parti dei file, impedirci l'uso di internet, ecc);
- **molto dannosi**: Causano danni difficilmente recuperabili come la cancellazione di informazioni fondamentali per il sistema (formattazione di porzioni del disco) e in alcuni casi (rarissimi) anche danni hardware.

Comunque non abbiate paura: anche nei casi più disastrosi c'è spesso il metodo per recuperare i vostri dati importanti.

La vita di un virus

I virus informatici presentano numerose analogie con quelli biologici per quello che riguarda il ciclo di vita, che si articola nelle fasi seguenti:

- * **creazione**: è la fase in cui lo sviluppatore progetta, programma e diffonde il virus. Di solito i **cracker** per la realizzazione di virus ottengono codice virale di pochi centinaia di byte.
- * **incubazione**: il virus è presente sul computer da colpire ma non compie alcuna attività. Rimane inerte fino a quando non si verificano le condizioni per la sua attivazione.
- * **infezione**: il virus infetta il file e di conseguenza il sistema.
- * **attivazione**: al verificarsi delle condizioni prestabilite dal cracker, il virus inizia l'azione dannosa.
- * **propagazione**: il virus propaga l'infezione, riproducendosi e infettando sia file nella stessa macchina che altri sistemi.
- * **riconoscimento**: il virus viene riconosciuto come tale e viene individuata la stringa di riconoscimento, ossia la firma che contraddistingue ciascun virus.
- * **estirpazione**: è l'ultima fase del ciclo vitale del virus. Il virus viene eliminato dal sistema (grazie all'anti-virus).

Come si diffondono

Sono molti i modi con la quale possono trasferirsi da un computer all'altro.

Ogni virus lavora in maniera differente, ecco alcuni esempi:

- scambiandosi i file infetti portandoli sul pc con chiavette di memoria, cd, dvd o simili.
- via INTERNET, sicuramente la strada più efficace
 - Per e-mail sotto forma di allegati;
 - Utilizzando browser poco sicuri si scaricano senza che nemmeno ce ne accorgiamo;
 - Scaricando e aprendo file da siti web poco affidabili;
 - Attraverso chat i nostri amici già infettati ci possono mandare file infetti;
 - Ecc..



Più bravo e ingegnoso è stato lo sviluppatore e più possibilità di successo di diffondersi avrà.



Attenti al virus



Se i virus sono già noti (quindi hanno già mietuto sufficienti vittime) allora gli sviluppatori degli antivirus saranno corsi ai ripari rendendo i loro antivirus capaci di resistere all'attacco.

**Morale della favola: TENETE IL VOSTRO ANTIVIRUS
SEMPRE AGGIORNATO!!!**

Inoltre è bene tenere aggiornati anche tutti i nostri programmi (SO compreso) perchè di solito se il bug viene riconosciuto verrà successivamente sistemato.



Scontato sarebbe dire di tenere comunque sempre gli occhi bene aperti e non cadere nelle trappole dei cracker, perchè spesso il migliore antivirus siamo proprio NOI!!

Come debellarlo



Se il virus è comunque riuscito a passare c'è spesso la possibilità di eliminarlo adoperando specifici programmi di rimozione.

I risultati non sempre però sono quelli sperati, infatti la soluzione più radicale ma sicuramente efficace è quella della formattazione (ovvero eliminazione totale dei contenuti del pc per ripartire da zero) e conseguente ripristino del sistema operativo.

Non sono tutti virus

Virus è un termine utilizzato spesso in maniera generica, vedremo che esistono varie tipologie di malware:

- **Exploit:** tecnica per prendere il controllo di un computer sfruttando le debolezze (bug) del sistema operativo o di altri programmi che accedono ad Internet (ad esempio da Windows utilizzando Internet Explorer).
- **Rootkit:** programmi che permettono ai virus di "nascondersi" nel computer.
- **Trojan:** o "cavallo di Troia" sono genericamente software malevoli (malware) nascosti all'interno di programmi apparentemente utili, e che dunque l'utente esegue volontariamente. Il tipo di software malevolo che verrà silenziosamente eseguito in seguito all'esecuzione del file da parte dell'utente può essere sia un virus che un qualunque tipo di minaccia informatica poiché permette al cracker che ha infettato il PC di risalire all'indirizzo IP della vittima.

Altri metodi per fregarvi

Oggigiorno però fare “virus” non è più di moda, e senza dubbio non rende! La cosa più intelligente è rubare informazioni “sensibili” (credenziali del conto corrente, carta di credito, ecc..)!!



Ecco alcuni metodi utilizzati:

- **Ingegneria sociale:** tecnica di studio di un bersaglio per carpirne la fiducia ed entrarne in contatto.
- **Keylogger:** software che una volta eseguito su di una macchina memorizza in maniera trasparente all'utente ogni tasto premuto in un proprio database. Solitamente viene installato tramite virus o backdoor, e viene programmato in modo che ritrasmetta via rete i dati memorizzati.
- **Phishing:** tecnica di ingegneria sociale per ottenere informazioni riservate al fine del furto di identità e di informazioni personali, ad esempio facendovi entrare in siti fasulli uguali agli originali nel quale inserite la vostra username e password.
- **Sniffing:** o "annusare"; tecnica per intercettare i dati in transito in rete e decodificarli.