Virus & Antivirus

Virus

Nella sicurezza informatica un **virus** è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di se stesso

I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.

I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.

Che cosa è un VIRUS?

Un virus è composto da un insieme di istruzioni, come qualsiasi altro programma per computer. È solitamente composto da un numero molto ridotto di istruzioni, (da pochi byte ad alcuni kilobyte), ed è specializzato per eseguire soltanto poche e semplici operazioni e ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile

Un virus, per essere attivato, deve infettare un programma ospite, o una sequenza di codice che viene lanciata automaticamente. La tecnica solitamente usata dai virus è quella di infettare i file eseguibili: il virus inserisce una copia di sé stesso nel file eseguibile che deve infettare, pone tra le prime istruzioni di tale eseguibile un'istruzione di salto alla prima linea della sua copia ed alla fine di essa mette un altro salto all'inizio dell'esecuzione del programma.

Principalmente un virus esegue copie di sé stesso spargendo l'epidemia, ma può avere anche altri compiti molto più dannosi (cancellare o rovinare dei file, formattare l'hard disk, far apparire messaggi, disegni o modificare l'aspetto del video, ...)

Vecchi e nuovi VIRUS

Un virus è un frammento di codice che non può essere eseguito separatamente da un programma ospite, mentre un worm è un applicativo a sé stante.

Prima della diffusione su larga scala delle connessioni ad Internet, il mezzo prevalente di diffusione dei virus da una macchina ad un'altra era lo scambio di floppy disk contenenti file infetti. Il veicolo preferenziale di infezione è invece oggi rappresentato dalle comunicazioni e-mail e dalle reti di peer to peer (ad esempio eMule).

Il vecchio concetto di virus è stato sostituito con quello più moderno di worm. I worm sono scritti in linguaggi di programmazione di livello sempre più alto in stretta connivenza con il sistema operativo, nella quasi totalità dei casi Windows, e le sue vulnerabilità.

Questi nuovi tipi di infezioni penetrano nel sistema quasi sempre da soli sfruttando le vulnerabilità, non fanno molto per nascondersi, si replicano come vermi anziché infettare i file, che è un'operazione più complessa ed ormai in disuso.

Antivirus

Un **antivirus** è un software atto a rilevare e, eventualmente, eliminare virus informatici e altri programmi dannosi (noti come malware).

Un **antivirus** da solo, per quanto affidabile ed efficiente, non è una protezione totale contro il 100% dei virus informatici esistenti al mondo. Inoltre, un antivirus si basa su determinate regole e algoritmi scritti da esseri umani, e pertanto queste possono portare a errori (falsi positivi) e/o a decisioni sbagliate.

Il metodo delle signatures, ovvero delle firme, è forse ad oggi quello più utilizzato. Questo metodo, sostanzialmente, prevede il confronto del file da analizzare con un archivio in cui sono schedati tutti i malware conosciuti, o meglio le loro firme. Ovviamente l'efficienza di tale metodo si basa sulla completezza dell'archivio, diverso per ogni casa produttrice di software antivirus, e sulla velocità del software nell'eseguire il confronto tra il file e la firma.

Alcuni antivirus provano ad eseguire i file eseguibili e, tramite l'analisi del comportamento di tali eseguibili, riescono a capire se si tratti di eseguibili che contengono codice malevolo o meno. Questo metodo, se basato su buoni algoritmi, può essere molto preciso.

Che cosa è un ANTIVIRUS?

Uno dei principali metodi di funzionamento degli antivirus si basa sulla ricerca nella memoria RAM e/o all'interno dei file presenti in un computer di uno schema tipico di ogni virus . In pratica ogni virus è composto da un numero ben preciso di istruzioni (codice) che possono essere viste come una stringa di byte, il programma non fa altro che cercare se questa sequenza è presente all'interno dei file o in memoria.

Esiste anche un'altra tecnica di riconoscimento detta "ricerca euristica" che consiste nell'analizzare il comportamento dei vari programmi alla ricerca di istruzioni sospette perché tipiche del comportamento dei virus (come la ricerca di *file* o *routine di inserimento all'interno di un altro file*) o ricercare piccole varianti di virus già conosciuti (variando una o più istruzioni è possibile ottenere lo stesso risultato con un programma leggermente differente).

ANTIVIRUS & FIREWALL

Per quello che si è detto si capisce che per avere un sistema sicuro l'antivirus non è affatto sufficiente, occorre una protezione ulteriore: il firewall. Un firewall permette, se ben configurato ed usato correttamente, di bloccare i virus, anche se non conosciuti, *prima* che questi entrino all'interno del proprio computer e volendo permette anche di bloccare all'interno alcuni virus presenti nel proprio computer evitando così che essi possano infettare la rete a cui si è collegati.

Con l'avvento di internet l'antivirus è diventato uno strumento quasi indispensabile e quasi esclusivo per i sistemi operativi rilasciati da Microsoft, mentre gli altri sistemi risultano quasi immuni da virus; per questo motivo la maggior parte degli antivirus è realizzata per i sistemi operativi Microsoft.