

I VIRUS

Cosa sono i virus

I virus informatici, al pari di quelli biologici, sono "entità" che creano danni. Si tratta di piccoli programmi che si infiltrano nel computer per distruggere dati, sabotare applicazioni e rubare informazioni. Proprio come accade a quelli biologici, i virus informatici hanno poi la capacità di autoriprodursi e di diffondersi per "contagio" da un computer all'altro.

Il mezzo di trasmissione dell'infezione può essere un'applicazione scambiata tra due o più PC mediante un qualsiasi supporto di memorizzazione e comunicazione come dischetti floppy, CD, reti locali, posta elettronica e Internet. In particolare esistono alcuni tipi di e-mail che sfruttano le "falle" (**Bug**) del sistema operativo per inserire il virus direttamente nel nostro PC senza bisogno di utilizzare alcun allegato.



Come funzionano i virus

Ogni virus appartiene a una specifica categoria e utilizza una precisa tecnica di trasmissione e infezione. In Windows, i virus sono dei programmi eseguibili e quindi dotati di una estensione di tipo *EXE*, *BAT*, *COM* o *PIF*. Anche i file compressi, con estensioni *ZIP* o *ARJ*, insieme agli *SCR* dei salvaschermo, possono essere utilizzati per diffondere il contagio. **Il funzionamento di un virus prevede solitamente le cinque fasi di letargo, attivazione, trasmissione, riproduzione e degenerazione.** Una volta che il virus arriva sul PC da infettare, rimane inattivo per un periodo di tempo più o meno lungo. In questa fase di letargo, il virus controlla e cataloga ogni operazione e attività del sistema operativo e dei programmi fino a quando non avviene uno specifico evento che ha il compito di attivarlo. Una volta risvegliato, il virus infetta uno o più file del computer nel quale si trova per poi replicarsi e trasmettersi su altri PC tramite rete oppure nel trasferimento dati. Nell'ultima fase, quella di degenerazione, il virus svolge il proprio compito danneggiando dati e programmi oppure impedendo il corretto funzionamento del computer.

Le "famiglie" dei virus

Ogni virus, pur essendo praticamente unico e differente da qualsiasi altro, rientra in una più generale classificazione nella quale sono contenuti tutti i software che hanno caratteristiche simili o che operano con le stesse modalità. Esistono virus di file residenti in memoria, di boot relativi all'avvio del sistema operativo, i Macro, i Trojan basati sul concetto del "Cavallo di Troia", i Worm, con cifratura di codice e polimorfici. Fra i più pericolosi, oltre a quelli di boot, ci sono i Trojan e i Worm. I primi, come suggerisce il nome, si nascondono all'interno di programmi innocui e si installano nel nostro computer per poi aprirne le "porte" tramite Internet a qualsiasi malintenzionato. I Worm, invece, utilizzano la Rete per diffondersi e propagarsi con velocità vertiginosa infettando in poche ore migliaia di computer. Alcuni virus, soprattutto i Macro, sfruttano la possibilità che offrono molti programmi di creare procedure automatiche per eseguire sui nostri dati delle operazioni ripetitive. Di solito vengono scritti con il linguaggio di programmazione Visual Basic e sono abbastanza semplici da individuare e da rimuovere.

I virus non sono uguali per tutti i sistemi operativi

Così come esistono differenti programmi che funzionano solamente in presenza di determinati sistemi operativi, anche la maggior parte dei virus viene sviluppata e realizzata per un preciso ambiente software. Esistono quindi virus che funzionano con i sistemi operativi Microsoft, virus per MacOS e virus che si diffondono sotto Linux. Partendo da questa considerazione è necessario però sottolineare alcune differenze. Windows è di gran lunga il sistema operativo più bersagliato sia a causa della sua grande diffusione sia per la presenza nel codice di alcuni "bug" che, se individuati, consentono ai virus un facile accesso alle risorse del sistema. I virus che minacciano Linux sono ancora molto pochi e sfruttano errori presenti solo in alcuni software; inoltre, la possibilità che hanno i virus di attivarsi automaticamente risulta meno presente in ambiente Linux e Unix.

Cosa sono gli antivirus

Gli antivirus sono speciali software che si preoccupano di controllare lo stato di salute del computer di proteggerci dagli attacchi dei virus. Anche se non esiste la protezione totale e perfetta, visto che i virus informatici nascono e si modificano con una rapidità enorme, grazie agli antivirus è possibile limitare considerevolmente il rischio di contagio. Non tutti gli antivirus offrono gli stessi livelli di sicurezza e di protezione. Per scegliere quello da installare sul nostro PC, dobbiamo **valutare sia la frequenza di rilascio delle nuove versioni sia la disponibilità in Rete di tempestivi aggiornamenti contro tutti i nuovi tipi di virus.** Fra le tante possibilità offerte dai differenti pacchetti antivirus ci sono il controllo della posta elettronica, con la scansione degli allegati, insieme alla verifica continua dei file di sistema del nostro PC. La maggior parte degli antivirus permette di pianificare tutte le operazioni di controllo e di aggiornamento, in automatico, nelle ore e nei giorni che preferiamo.

Come funzionano gli antivirus

Per riconoscere i possibili programmi contagiati, gli antivirus confrontano "pezzi" del codice di tutti i file presenti nel nostro PC, o in una specifica cartella, con una tabella contenente le "impronte" di tutti i virus noti. In pratica, **verificano se fra le parti del codice di un qualsiasi file si nascondono altre parti di codice che potrebbero appartenere al software di un virus.** Il confronto avviene tramite suddivisioni e verifiche del codice, basate su procedure matematiche, estremamente variabili tra i diversi antivirus. In ogni caso, per essere sicuri che la tabella contenente le definizioni dei virus sia effettivamente utile, è necessario aggiornarla periodicamente tramite il sito del produttore. Quando un antivirus trova un file infetto, ci avvisa della sua presenza ed eventualmente ci propone la rimozione della parte virale del codice. A volte quest'ultima operazione non è consentita e quindi possiamo solamente spostare il file contenente il virus in una speciale cartella chiamata *Quarantine Zone*, ovvero "*zona in quarantena*". I file in quarantena, in alcuni casi, possono essere recuperati con successivi aggiornamenti della tabella di definizione dei virus. In caso contrario, devono essere eliminati.

Come prevenire gli attacchi dei virus

Grazie alla possibilità che hanno tutti i nuovi antivirus di aggiornare in tempo reale la propria tabella di definizione dei virus, un unico programma può controllare e in alcuni casi prevenire il contagio di migliaia di differenti tipi di virus. Se utilizziamo quotidianamente connessioni di rete e accesso Internet, le probabilità di incontrare un virus sono molto alte e si rende indispensabile un controllo costante e continuo da parte di un antivirus. Per questo motivo, ogni antivirus può lavorare in due differenti modalità: in *realtime* ovvero "*in tempo reale*" e in Scan cioè "*a scansione*". La modalità in tempo reale, chiamata anche "*monitoraggio*", effettua la verifica di qualsiasi file venga aperto, letto, modificato, inviato oppure ricevuto durante la nostra sessione di gioco o di lavoro. **Purtroppo il PC, a fronte di una maggiore sicurezza, subisce una brusca diminuzione delle prestazioni.** La scansione, attivabile manualmente oppure automaticamente mediante una pianificazione, offre una protezione meno tempestiva ma può essere lanciata quando il computer non sta lavorando.

Come si protegge PC durante la navigazione sul Web

Rispetto ai primi programmi per navigare su Internet, i browser attuali come Internet Explorer6.0, Netscape Navigator7.1, Mozilla 1.5.1 e così via offrono una sicurezza quasi totale nei confronti dei virus che viaggiano in Rete. Il "*quasi*" è motivato dalla necessità che hanno questi stessi programmi di essere continuamente aggiornati per mantenere elevato il livello di guardia nei confronti dei nuovi virus. Così come gli antivirus necessitano dell'aggiornamento continuo della tabella della definizione dei virus, anche **per salvaguardare la nostra sicurezza mentre utilizziamo la Rete è necessario aggiornare costantemente il nostro browser e, in alcuni casi, l'intero sistema operativo.**

Proteggere la posta

L'E-Mail è attualmente uno dei principali mezzi di diffusione dei virus. Capita molto spesso che nella nostra casella di posta vengano recapitati messaggi "*spam*" provenienti da mittenti inesistenti che pubblicizzano prodotti di varia natura, a volte con allegati potenzialmente pericolosi. È sufficiente uno sguardo per capire che quei messaggi devono essere subito eliminati; tuttavia in alcuni casi è meglio ricorrere alla scansione preventiva da parte del nostro antivirus. Norton Antivirus, McAfee VirusScan e simili dispongono di una speciale opzione, da abilitare o meno a seconda delle nostre esigenze, per eseguire automaticamente questo compito. Gli stessi programmi di posta elettronica, come Outlook o Outlook Express, prevedono la possibilità di non scaricare gli allegati che rientrano nelle categorie a rischio. Se, inoltre, desideriamo ancora una maggiore tranquillità, possiamo attivare l'opzione che permette di scaricare solo l'intestazione dei messaggi dal nostro server di posta. In questo modo decidiamo con tranquillità quali messaggi eliminare e quali invece scaricare completamente.

Gli Antivirus più famosi

Ecco quali sono attualmente gli antivirus più diffusi:

- Symantec Norton Antivirus 2004, disponibile nella versione Standard e Professional;
- McAfee VirusScan 7.0, nelle due versioni Home e Professional;
- Kaspersky Labs Antiviral Toolkit Pro, in versione Standard e Professional;
- TrendMicro PCCillin 9, disponibile in varie versioni;
- Panda Antivirus, disponibile in numerose versioni per utilizzo personale e aziendale.