COSA SONO I “VIRUS” INFORMATICI

In generale, qualsiasi software che invece di essere utile all'utente si esegue a sua insaputa con lo scopo di provocare gravi danni.

Nell'ambito dell'informatica un **virus** è un software, appartenente alla più ampia categoria dei **malware***, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente.

Non sono programmi eseguibili e per avviarsi devono infettare un programma ospite, inserendo il codice nocivo tra le prime istruzioni: in questo modo quando l'utente lancia il programma infetto, viene dapprima eseguito il virus in modo impercettibile e poi il programma richiesto dall'utente.

L'utente quindi vede solamente l'esecuzione del programma e non si accorge che il virus è stato attivato ed **è in esecuzione nella memoria RAM** e sta compiendo le operazioni in esso contenute. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.

Una volta eseguito, il virus è in grado di riprodursi e fare copie di se stesso. Può anche avere altri compiti come quello di aprire una **backdoor**, un **keylogger** o un **dialer**.

Un virus **danneggia solo il software** del computer ma non l’hardware.

***Malware**: *un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Nell'uso comune il termine virus viene frequentemente ed impropriamente usato come sinonimo di malware, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio **worm**, **trojan**, **dialer**, ….*

DIFFERENTI TIPOLOGIE DI VIRUS

Virus di BOOT
E' un tipo di virus ormai quasi inutilizzato che infetta i settori di avvio degli hard-disk o dei floppy-disk e che quindi si attiva al momento dell'accensione del PC.

Virus POLIMORFICI
Effettuano una mutazione ad ogni infezione, in modo da risultare meno rilevabile da parte degli antivirus.

Virus METAMORFICI
Sono ancora più potenti dei virus polimorfici: riescono a mutare completamente il proprio codice e a dividerlo in più parti all'interno del file infetto, diventando davvero difficilmente rilevabili da parte degli antivirus

MACRO Virus
Sfruttano la capacità di eseguire particolari istruzioni, denominate **macro***, messe a disposizione da alcuni software di uso comune, come ad esempio Microsoft Word, Excel o PowerPoint e trasformano un innocuo file in un programma pericoloso.
Fortunatamente tutte queste applicazioni segnalano l'eventuale presenza di Macro in un file e quindi per evitare l'infezione basta controllarle e cancellare tutte le Macro che non sono state scritte personalmente!

Virus INNOCUI
Sono tutti quei "programmino" innocui cha una volta avviati si spacciano per virus e fanno apparire effetti grafici e scritte sul monitor. Sono comunque fastidiosi per l'utilizzatore.

***Macro**: piccolo programma che viene creato per automatizzare una serie di operazioni ripetitive.

ALTRI TIPI DI MALWARE

Sono di seguito riportati altri pericoli informatici che però non sono classificati come veri e propri virus.

Worms
E' un malware in grado di diffondersi, autoreplicarsi e causare danni proprio come un virus ma, a differenza di un virus, non necessita di un programma ospite per funzionare perché, una volta eseguito, modifica il sistema operativo della macchina ospite in modo da essere eseguito automaticamente. Utilizza la rete internet per propagarsi e di solito il suo effetto è quello di influenzare negativamente le prestazioni del PC con operazioni inutili o dannose.

Trojan
Non si replicano autonomamente ma sono file eseguibili come normali programmi. Per contagiare il PC devono essere manualmente aperti dall'utente e quindi per fare ciò si spacciano con nomi ed icone fittizie per programmi utili e richiesti dall'utente (proprio come per i worms).
Essi sono il mezzo più diffuso per l'installazione dei backdoor. L'unico modo per essere contagiati è aprirli direttamente e per questo bisogna prestare particolare attenzione a quello che si scarica dalla Rete (soprattutto dai software P2P), a ciò che arriva per posta e diffidare sempre di ciò che non si conosce.

Backdoor
Si tratta di programmi di amministrazione remota che permettono al costruttore del backdoor di prendere il controllo del PC attraverso la rete. Non sono in grado di replicarsi in modo autonomo, ma hanno la caratteristica di tenere aperte delle porte che possono essere utilizzate per accedere ai dati e ai programmi del computer, inviare e ricevere files, cancellare archivi, veicolare virus all'interno del sistema. Generalmente sono installati da worm o trojan.

Spyware
Software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.

Rootkit
Non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.

Exploit
Tecniche per oltrepassare i sistemi di sicurezza che sfruttano le falle del sistema operativo o di altri software.

Keylogger
Software che memorizza le operazioni effettuate dall'utente (come la pressione dei tasti sulla tastiera, il movimento del mouse, i programmi utilizzati,…) e poi solitamente le invia tramite rete al costruttore del keylogger, in modo che possa risalire alle password e alle operazioni effettuate dall'utente. Non rallentano il PC e quindi passano totalmente inosservati.

Phishing
Programmi che creano false interfacce per l'accesso mediante Username e Password da parte dell'utente: una volta inseriti i dati, invece di effettuare l'accesso, il software li invia al costruttore dell'interfaccia. Questa tecnica è utilizzata soprattutto su Internet.

Dialer
Il termine indica generalmente programmi che si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati per truffare, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

ALCUNE REGOLE PER EVITARE "INFEZIONI"

⇨Per principio sottoporre a controllo qualsiasi di provenienza sospetta prima di eseguire uno qualsiasi dei files.
⇨Ridurre l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza.
⇨Proteggere in"scrittura" tutti i propri cd/dvd di sistema o contenenti programmi eseguibili.
⇨Non eseguire mai programmi di origine sconosciuta. Se proprio lo si dovesse fare, avvalersi di un programma antivirus in modo di rilevare la eventuale presenza di virus.
⇨Limitare la trasmissione di files eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computers in rete.

COSA FARE IN CASO DI INFEZIONE

Si possono ipotizzare due situazioni:

1. **danno già avvenuto**;
2. **infezione scoperta in tempo**.

Nel primo caso l'utente si accorge della presenza del virus in quanto ha notato malfunzionamenti di vario genere. L'unica cosa da fare è ripristinare il contenuto dell'hard-disk con i dati di un recente back-up, dopo opportuna opera di disinfestazione con antivirus.

La procedura di disinfezione nei casi più gravi comporta:

1. Formattazione dell'hard-disk e reinstallazione del sistema operativo.
2. Reinstallazione dei programmi a partire dai cd originali, protetti in scrittura e sicuramente non infetti.
3. Effettuazione di una copia dei soli dati a partire da una copia di back-up recente.
4. Se si sospetta un virus delle macro, prima di aprire i documenti sarà opportuno controllarli con dei programmi antivirus per verificare che non siano infetti.

Nel secondo caso, se l'infezione è invece scoperta in tempo, prima che provochi danni irreparabili, si possono fare numerose cose:

1. Spegnere il computer e riaccenderlo lanciando il sistema operativo da cd protetto in scrittura.
2. Eseguire dei controlli con antivirus atti a verificare la presenza del/dei virus.
3. Fare un back-up dei soli dati.
4. Formattare l'hard-disk, dopodiché ci si è ricondotti al caso del danno già avvenuto.

🔔 E' da **sconsigliare** in linea generale la **semplice disinfezione con i programmi appositi**: spesso essi nel tentativo di eliminare il virus alterano in maniera definitiva il programma disinfettato che, pertanto, deve essere, comunque, reinstallato.

Qualora si verifichi un'infezione, **è NECESSARIO controllare tutti i cd/dvd di cui si dispone** con un programma di scansione, perché l'infezione potrebbe ripetersi.

CURIOSITA'

☞*La diffusione di programmi dannosi risulta in continuo aumento. Si calcola che nel solo anno 2008 su Internet siano girati circa 15 milioni di malware, di cui quelli circolati tra i mesi di gennaio e agosto sono pari alla somma dei 17 anni precedenti.*