

Virus informatici: cosa sono e come difendersi

Cosa sono

Iniziamo subito a parlare di cosa sono.

Un virus informatico (d'ora in poi solo virus), per essere definito tale, deve rispondere a certi requisiti; il più importante è la capacità di replicarsi, ovvero di copiarsi e di riuscire ad infettare con copie di se stesso, quanti più computer può.

Dopo aver completato la procedura di replicazione, di cui parleremo più avanti, normalmente il virus attacca il computer infetto, eseguendo le operazioni per cui è stato creato, che vanno dal semplice cambiamento delle icone di Windows fino alla formattazione dell'intero disco fisso, passando per il furto di dati personali.

Categorie

I virus dal 1984 (anno della creazione del primo virus), si sono evoluti (ad oggi esistono circa 65.000 virus) e sono stati pian piano raggruppati in categorie, vediamo quali esistono:

- + Worm: sono i tipi più diffusi, sfruttano problemi di sicurezza dei programmi di posta elettronica e di internet.
- + MacroVirus: si tratta di virus che sono scritti in linguaggio macro, un linguaggio usato nei documenti, come quelli di Word ed Excel
- + Trojan: o Troiani, sono dei virus che non fanno alcun danno ma permettono, attraverso internet, al loro creatore di accedere al computer e di prenderne il pieno possesso.
- + Vari: fanno parte di questa sezione tutti quei virus che magari, inibiscono il collegamento ad internet, oppure vanno ad infettare il record di avvio del computer (M.B.R., Master Boot record) e quindi non fanno caricare il sistema operativo, rendendo molto più difficile la loro rimozione.

Esistono poi caratteristiche che un virus può avere:

- + Polimorfici: un virus "evoluto" ha questa caratteristica, questi virus sono in grado di modificare la propria struttura, per non essere individuati dai programmi antivirus; fortunatamente esistono sistemi di scansione "euristici", che vanno a capire le azioni che un programma potrebbe compiere e avvertono se potrebbero essere dannose.
- + Retrovirus: i virus dotati di questa caratteristica, oltre al danno normale, va ad attaccare i programmi antivirus, facendoli funzionare male o rendendo impossibile la loro installazione.
- + Bombe a tempo (Timer Virus): un virus che è così definito, è progettato per avviarsi solo dopo una certa data, ora o azione, può per esempio essere programmato per avviarsi il 25 dicembre a mezzanotte e durare solo un minuto....sta alla fantasia del creatore.
- + Spyware: non è né una caratteristica né un virus, ma alcuni li considerano tali, sono dei programmi che non danneggiano niente all'interno del computer, ma una volta collegati ad internet, inviano informazioni personali ai loro autori.

Esistono poi altre caratteristiche meno importanti, le elenco:

Memory Resident, resta scritto nel computer anche in seguito alla cancellazione, per eliminarlo si deve eseguire la cancellazione ed il secure erase, un'operazione che cancella definitivamente i dati dal disco fisso.

Size Stealth, dimensioni nascoste, impedisce di sapere quali sono le sue dimensioni.

Full Stealth Encrypting, invisibilità piena, non viene visualizzato dal sistema operativo, viene però rilevato dai programmi antivirus

Encrypting, si cripta (codifica) per restare nascosto (simile al polimorfico).

Difesa

Come sempre la miglior difesa è la prevenzione, qualora questa non sia stata sufficiente, e ci ritrovassimo il computer infetto, dobbiamo contrattaccare.

Innanzitutto dobbiamo aver già installato ed aver aggiornato un software antivirus.

In commercio ne esistono tanti, si differenziano però dalla facilità d'uso e dalla richiesta di potenza.

Il numero uno, come è stato definito, è il Symantec Norton Antivirus, giunto all'edizione 2003.

Ma non sono da meno anche il McAfee Virus Scanner e il F-Secure.

Come prestazioni sono quasi uguali, F-Secure, è abbastanza buono e ha bisogno di poca potenza per funzionare.

Il McAfee, secondo al mondo, è ormai giunto ad essere quasi alla stessa stregua del Norton.

Se siete stati infettati, non fatevi prendere subito dalla preoccupazione, ci sono ottime speranze di rimettere tutto (o quasi) in ordine.

La prima cosa che si deve fare, è sapere se si ha il controllo del computer, o meno.

se, come nella maggior parte dei casi, il computer, seppur infetto è nelle nostre mani, non preoccupatevi e seguite queste istruzioni: accertate che il virus non si autoavvii ogni volta che accendete il computer, per fare questo andate su: Start/Avvio -> Esegui -> Scrivete "Regedit" e date OK, vi si aprirà un programma, dalla colonna di sinistra individuate la stringa "HKEY_LOCAL_MACHINE" e successivamente "SOFTWARE" -> "Microsoft" -> "Windows" -> "CurrentVersion".

Da qui dovete controllare la stringa "Run" e "RunServices", se avete un sistema NT (Windows NT, NT Workstation, 2000, 2000 Server, XP Home, XP Pro, 2003 Server) anche le stringhe "RunOnce", "RunOnceEx".

Una volta cliccato su quelle stringhe vi comparirà nella schermata di destra delle "chiavi", in pratica delle stringhe cui sono assegnati dei valori. Cancellate ogni stringa che vi insospettisca, occhio ad avere buon senso.

Fatto ciò dovete chiudere Regedit e andare su Start/Avvio -> Programmi -> Esecuzione automatica, anche qui cancellate le voci sospette. Ora passiamo al contrattacco, fin qui infatti abbiamo prevenuto il reavvio dei virus.

Provate innanzitutto a far partire la scansione del software antivirus, qualunque esso sia; al termine della scansione, avrete un rapporto (report) di tutti i file infetti che l'antivirus ha rilevato nel vostro computer.

Se siete riusciti ad avere il report, soffermatevi sugli elementi riportati, il miglior rimedio sarebbe eliminare tutti i file infetti per scongiurare il pericolo; alcuni file però potrebbero esservi utili o addirittura necessari, magari il vostro curriculum è infetto o magari qualche componente di Windows stesso. Quindi la miglior cosa da fare è provare a riparare (fix, in inglese) i file infetti; purtroppo quest'operazione non sempre riesce e bisogna per forza ricorrere ad una cancellazione.

Se siete stati attaccati da un virus, cercate prima nei siti dei produttori, molto spesso, per i virus più diffusi i produttori, rilasciano piccoli programmi (tools), atti a rilevare e riparare la maggior parte dei danni fatti dal virus; attenzione però questi tools valgono solo per un certo virus.

Un'altra operazione che potete fare invece di cancellare i file è quella di mettere in quarantena i file infetti, in attesa di un (improbabile) sistema per ripristinarli correttamente.

Una credenza molto diffusa è che i virus possano rompere il computer; ciò è assolutamente falso, i virus in quanto software, non possono in alcun modo danneggiare a livello fisico il pc, possono al massimo cancellare tutto o formattare i dischi, ma non possono danneggiarli.

Prevenzione

Come tutte le cose, la difesa migliore oltre che alla prevenzione con Antivirus e Firewall, è affidata al vostro buon senso.

Un particolare riguardo all'antivirus, se sarete infettati o se sul vostro pc ci sarà mai un virus, lui sarà il vostro più caro amico.

Quindi cominciamo con l'elenco:

- + Installate un potente antivirus (Norton, McAfee, Panda, F-Secure, Trend, ecc.).
- + Mantenetelo aggiornato scaricando gli aggiornamenti dai siti dei produttori.
- + Installate un potente Firewall (Norton Personal Firewall, ZoneAlarm, Sygate Personal Firewall, ecc.)
- + Configurare con pazienza il Firewall (se non siete molto esperti, rivolgetevi a dei tecnici competenti).
- + Aggiornate in continuazione con le opportune "Patch" sia il programma per la posta elettronica (Outlook, Eudora, ecc.) che il vostro Web Browser (Internet Explorer, Netscape, Opera, Mozilla, ecc.)
- + Siate paranoici, scansionate qualsiasi cosa che deve essere immessa nel vostro computer, quindi scansionate qualsiasi cd prima di avviarlo, scansionate qualsiasi programma vi scarichiate da internet, scansionate qualsiasi e-mail che ricevete.
- + Non aprite allegati o e-mail "strane", magari è un e-mail di vostro padre, con un allegato tipo "Report.exe" e coll'oggetto in inglese, e magari vostro padre neanche lo sa l'inglese; vi sembra abbastanza strana?

I virus usano ogni mezzo per diffondersi, ultimamente però quello che viene sfruttato di più è la posta elettronica.

Quindi, controllate scrupolosamente tutte le e-mail.