Questo articolo è apparso sul Corriere del Ticino di martedì, 3 marzo 1992 nella sezione Prima Pagina

Computer, attenti al virus “Michelangelo”

Qualche consiglio per il 6 marzo, data in cui è prevista l’apparizione di un germe distruttivo che colpisce I PC

Silvano Marioni **www.marioni.org**

C'è una certa attesa tra gli utilizzatori di personal computer per il prossimo 6 marzo. Per questa data è infatti prevista l'apparizione un nuovo virus che colpisce i personal computer MS-DOS con conseguenze distruttive. Il nuovo virus che si chiama "Michelangelo", si attiva solo in occasione del compleanno del grande artista rinascimentale, nato per l'appunto il 6 marzo 1475, e in questa occasione cancella buona parte dei dati presenti sull'hard disk. Il virus è stato scoperto nell'aprile del 1991 in Svezia e da allora sono già stati preparati dei programmi per identificarlo e renderlo inoffensivo. Questo non ha impedito ad alcune aziende statunitensi, leader nel settore dei personal computer, di spedire i loro prodotti sia software che hardware contaminati da questo virus, a loro insaputa. Nonostante le aziende abbiano ricontattato tutti i loro clienti informandoli su come rimuovere il virus, si teme che nel frattempo il contagio si sia diffuso soprattutto perché il virus è nuovo e non viene riconosciuto da tutti i programmi antivirus. A complicare le cose c'è il fatto che il virus ha un meccanismo di riproduzione molto efficiente e che non manifesta nessun segno della sua presenza se non in modo drammatico il giorno 6 marzo.

Anche se questi dati possono impressionare, bisogna precisare che "Michelangelo" non è che uno degli oltre 100 virus che si manifestano ad una data prefissata. John McAfee, uno specialista che dalla metà degli anni ottanta si occupa di virus, ha catalogato a tuttoggi oltre 480 virus principali e 720 varianti solo nell'ambiente MS-DOS. Anche se non tutti i 1200 virus hanno comportamenti distruttivi come "Michelangelo", essi restano pur sempre un grosso fastidio per chi utilizza il personal computer nel proprio lavoro. Che cosa si può allora fare per premunirsi e non dover fronteggiare situazioni spiacevoli ? Per poter capire quali sono le situazioni e i comportamenti potenzialmente a rischio è importante conoscere il principio che sta dietro al fenomeno dei virus . Un virus di computer è composto sostanzialmente da una serie di istruzioni di programma che, quando eseguite, hanno la capacità di autoriprodursi. Queste istruzioni, inserite in un programma infetto, vengono portate nella memoria del computer al momento in cui il programma viene eseguito. Al contrario del programma, che quando termina esce dalla memoria, le istruzioni del virus rimangono in memoria, pronte ad agganciarsi al prossimo programma che viene eseguito. In questo modo ogni programma eseguito diventa un programma infetto e a suo volta fonte di contagio. Questo inquietante meccanismo di infezione, che ha molte analogie con la patologia degli agenti infettivi negli organismi viventi, non è che una metà dell'attività del virus. L'altra metà consiste in una serie di istruzioni che definiscono il modo di comportamento del virus. E' attraverso questo comportamento che il virus si manifesta nei modi e nei tempi stabiliti dal suo autore, producendo danni di diversa gravità. Vi sono casi in cui creano solo fastidi come ad esempio il virus "Stoned" che si limita a mostrare sullo schermo "Your computer is now stoned - legalise Marijuana" oppure il virus "Cascade" che fa cadere ad una ad una le lettere presenti sul video. Esistono poi virus che producono danni più gravi ma pur sempre ricuperabili come ad esempio "Jerusalem", che ingrandisce i programmi ogni volta che vengono eseguiti fino al punto da non poterli più caricare in memoria. Vi sono infine virus che producono danni irreversibili come "Michelangelo" che cancella intere parti di hard disk senza lasciare nessuna possibilità di recupero.

Visto che i virus informatici possono moltiplicarsi e diffondersi da un computer all’altro solo attraverso l'esecuzione di un programma infetto, una prima regola pratica potrebbe essere quella di evitare di eseguire programmi provenienti da dischetti sconosciuti o sospetti. Se il dischetto dubbio è un dischetto di sistema, il solo avviamento del computer con questo dischetto è già sufficiente per trasmettere il virus.

Ma cosa fare se invece nella vostra attività dovete scambiare dischetti con altre persone ? Chi vi garantisce dello stato di salute dei loro dischetti ? Cosa può succedere ai personal computer collegati ad una rete locale ? Oggi la risposta più sicura a queste domande è data dai programmi antivirus. Questi programmi sono in grado di

identificare i programmi infetti sia sui dischetti che sull'hard disk e nella memoria del computer e nella maggior parte dei casi riescono ad eliminare i virus presenti. Il loro unico limite è quella di scoprire i virus solo in base alle caratteristiche memorizzate; è quindi necessario utilizzare sempre le ultime versioni dei programmi antivirus poiché, come stima Edward Wilding editore di Virus Bullettin, oggi compaiano circa 20 nuovi virus ogni mese. I programmi di identificazione sono in genere semplici da istallare e da usare, mentre una volta scoperta un'infezione da virus è consigliabile rivolgersi a uno specialista per verificare l'entità del danno subito e ricuperare le eventuali informazioni danneggiate. Un pregiudizio abbastanza diffuso è quello che il software scaricato dalle banche dati possa contribuire alla diffusione dei virus. Oggi, come conferma l'autorevole rivista PC Computing, i responsabili di questi servizi sono molto attenti al problema dei virus e verificano attentamente il software prima di renderlo pubblico. Inoltre le banche dati svolgono un lavoro molto importante nella diffusione dei programmi antivirus e dei loro aggiornamenti. Un esempio in Ticino è la banca dati dell'Associazione Ticinese Elaborazione Dati (ATED).che mette a disposizione di tutti informazioni e programmi antivirus aggiornati. L'utilizzo del servizio, che è gratuito, può essere fatto collegandosi via modem allo 091 23.95.28 - 1200/2400 baud 8 N 1.