A colloquio con l'esorcista

Abbiamo parlato con Gianfranco Tonello un ricercatore anti-virus, un esorcista del mondo informatico. Ma tranquillizzatevi: i virus sono solo una trentina

Abbiamo chiesto a Gianfranco Tonello quale sia la situazione per quanto concerne i virus in Italia.

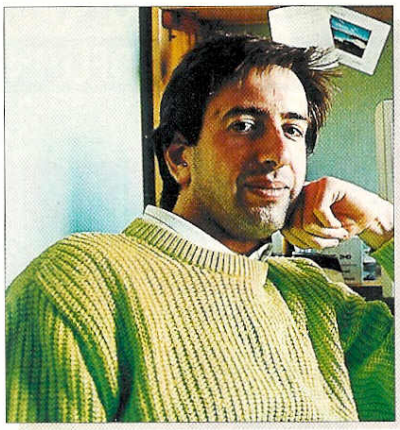
«Diciamo che in Italia c'è stato in questi ultimi anni un notevole produzione di virus locali.»

«Ad esempio ci sono state molte varianti del virus *Marzia* e anche del virus *Novembre 17* che sono pericolosi sia per gli impianti elettronici più grandi che per i singoli "consumatori" di informatica.»

Ma cosa fanno questi virus? «Una variante del virus *Marzia* si attiva il giorno 30 o il 31 del mese da marzo fino a dicembre. In tutti gli altri giorni il codice virale non dà problemi. Quando però il virus scatta sovrascrive il disco fisso eliminando i dati memorizzati. E lo fa solo in quel periodo dell'anno.»

«Ci sono poi numerose varianti. Ad esempio la più famosa è la 855 che si attivava dal 17 novembre fino al trenta dello stesso mese. Altri hanno cambiato anche data: ad esempio c'è il 768 che si attiva l'otto di luglio. Insomma ci sono state molte modifiche in questi ultimi anni.»

«Questi tipi di virus hanno effetti distruttivi: sovrascrivono delle informazioni sul disco rigido e chi è infetto perde i suoi dati. Poi ci sono altri tipi di virus come l'*Arianna* che è stato creato a Bari che si attiva dopo aver scritto il quattrocentesimo boot, il codice virale infetta un'area del disco fisso. Dopodiché quando uno ha riacceso il computer per quattrocento volte, improvvisamente appare sul video la scritta "Arianna virus". Si tratta, però di un virus simpatico perché non danneggia il disco fisso.»



«Un altro codice virale che si chiama *Rebel base* è stato creato nel 1994 e si comporta in modo simile all'*Arianna*: improvvisamente – nel bel mezzo del mese di Aprile – appare una scritta che dice *Come sono belle le ragazze giapponesi*. Un virus che è dedicato in particolare a Kaori, la ragazza della pubblicità del famoso formaggio industriale. Insomma alcuni virus sono pericolosi, altri sono carini.»

Quanti virus ci sono in circolazione? «Le fonti parlano di 5000, 6000 virus, però in circolazione nel mondo ce ne saranno duecento e in Italia ne girano una trentina che sono poi sempre i soliti.»

«Quindi non c'è un gran numero di codici virali pericolosi, ma c'è un aumento di produzione delle loro varianti. Per una protezione sicura bastano gli antivirus che sono in commercio. L'unico rischio sono le piccole produzioni locali. Può capitare che un codice virale venga prodotto e abbia una diffusione in una città e basta. Come è successo con il *Novembre 17 800* che si è diffuso solo a Bari. A Bari l'avevano tutti, ma lì si è fermato.»

«Tra i virus a produzione italiana ricordiamo *Invisble_Man.2926* (presumibilmente realizzato a Salerno) e il *Bloody_Warrior* (realizzato a Milano). Abbastanza diffuso è anche *Hllc.Crawen* del quale sono note due varianti attive in particolar modo nel Veneto e in Friuli Venezia Giulia.»

«Altri codici hanno una diffusione più limitata. Come è il caso del virus *Vota_Dc.591* in provincia di Padova e di *Rebel Base* in provincia di Venezia. Nella storia dei virus italiani il più famoso è certamente *Invisible_Man.2926* che è stato segnalato per la prima volta nel 1993. Questo tipo di virus infettava i file *Exe. Com* e il *Master Boot Record* ed è residente in memoria.»

Come funziona l'antivirus? «Per prima cosa l'antivirus cerca di evidenziare il codice virale. Si tratta di una fase di scansione.»

«Poi si ha una fase di rimozione dove – una volta trovati i dati per ogni virus – si cercano le informazioni per rimuovere il problema. Infine c'è uno scudo residente che serve a prevenire l'infezione; un programma che rimane sempre residente in memoria e controlla tutti gli accessi. Controlla i virus sconosciuti.»

«Quindi non solo curare, ma anche prevenire.»

Che tipo di virus è il cavallo di Troia? «Il cavallo di Troia non è un virus, ma un programma che non è in grado di replicarsi il suo solo scopo è quello di danneggiare o cancellare i file dell'utente».

«Ha questo nome perché spesso viene presentato in un modo accattivante, che invita chi usa i computer ad aprirlo. Ad esempio, potrebbe essere stato chiamato *Moana.exe*. Peccato solo che una volta che uno lo esegue vede sovrascrivere tutto il suo hard disk perdendo così tutti i dati.»

«Un virus è più pericoloso perché non solo può avere gli stessi effetti del *cavallo di Troia,* ma può anche replicarsi infettando il disco fisso, magari scattando in una particolare data.»

E cosa sono i worm? «I worm sono virus che vivono nel mondo *Unix* e hanno la capacità di riprodurre una copia di se stessi. Il più famoso è quello di Morris nell'89 che è entrato nella rete americana e ha creato una serie di gravissimi problemi.»

Dove lavora un "esorcista" antivirus? Io lavoro prevalentemente a casa visto che qui lo posso studiare con la calma necessaria.

Gianfranco Tonello (telefono e fax 049/631748) è uno specialista nella ricerca di virus e di antivirus e ha ideato diversi software per la protezione dei personal computer.

a cura di Andrea Becca

Type Mate anche in Italia

Ricordate l'articolo "Quante dita ha la tua tastiera?" (Pc Open n.2 pag.14)? Sappiate che il programma Type Mate si può acquistare in Italia da Middle Heart (039/9340128), oppure da Ediventi (02/2898035) a 10.000 lire.