UN BUON VACCINO SCACCIA VIRUS

DEI VIRUS INFORMATICI SI PARLA MOLTO, ANCHE A SPROPOSITO. IL PERICOLO C'È: TRE COMPUTER SU 100 VENGONO INFETTATI OGNI ANNO, MA ATTUARE UNA CORRETTA PREVENZIONE RIDUCE ENORMEMENTE LE POSSIBILITÀ DI CONTAGIO.

DI CARLO ROSSI

A leggere le cifre ufficiali tremano i polsi: lo scorso anno, in Italia, l'attività dei virus informatici è aumentata del 35 per cento e, tanto per fare un esempio, negli ultimi tre anni sono state perse quasi 65.000 ore di lavoro per rimediare ai guasti provocati da questi "microbi in bit". Panico e terrore? Chiudiamo il PC in cassaforte e lo usiamo solo a Natale? La realtà non è così tragica: è chiaro che i virus sono un problema reale, ma l'allarmismo è giustificato fino a un certo punto. In fin dei conti lo scorso anno, secondo le stime, è stato infettato il 3 per cento dei personal italiani (circa 4.400.000), molto probabilmente soprattutto quelli collocati in aziende e istituzioni. E poi sarebbe sbagliato trascurare che non mancano misure preventive attive e passive, esattamente come per i virus "veri" si può ricorrere alla vaccinazione oppure evitare le fonti di contagio. Accorgersi che il PC è stato infettato è apparentemente semplice perché, dicono tutti, appaiono sul monitor cose strane. Però ci sono casi in cui i virus non c'entrano.

IL MICROBO IN BIT

Basta un tasto della tastiera bloccato ed ecco che lo schermo impazzisce. Oppure appaiono strani messaggi di errore del tipo "No ROM basic resident" e la colpa non è di un misterioso aggressore, ma del fatto che il coprocessore matematico si è parzialmente sfilato dallo zoccolo a causa di eccessive manipolazioni (fatto accaduto a chi scrive). Vediamo allora come si manifestano realmente i virus. La cosa, tra l'altro, non manca di essere divertente, come ci dimostra Gianfranco Tonello, ricercatore antivirus e autore di VirIT, il più completo programma scaccia microbi tricolore.

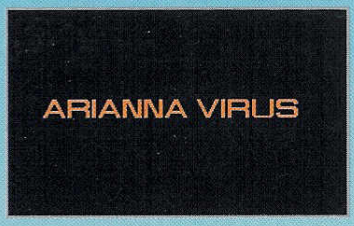
Un virus o codice virale è un programma che è in grado di autoreplicarsi e, oltre a produrre copie di se stesso, produce effetti desiderati dall'autore del virus e/o degli effetti collaterali, che si possono manifestare durante l'utilizzo del calcolatore. «Gli effetti voluti sono variabili da virus a virus, e sono legati agli scopi più o meno "goliardici" dell'autore del codice virale» spiega Tonello. «Nel panorama italiano, si possono incontrare virus che si limitano a visualizzare frasi a video come il virus Vota_DC.591, codice virale a sfondo politico, che visualizza a video nel mese di aprile: "Messaggio promozionale: Vota DC!". Altro codice virale "politico" è il Berlusconi virus, noto anche come Berlusca o Slavery virus, che il 27 marzo di ogni anno visualizza a video il messaggio: "Freedom is Slavery: Berlusconi ti guarda" accompagnato dal noto inno del Polo. Altri autori, invece, si sono cimentati creando codici a sfondo amoroso, come l'Arianna virus (scritto presumibilmente a Bari) che, dopo il quattrocentesimo boot, visualizza a video la scritta: "ARIANNA VIRUS". Stesso tema per Rebelbase, dove l'autore decanta il suo amore per Kaori, la ragazza simbolo della nota pubblicità di formaggi, e per tutte le ragazze giapponesi. Rebelbase si attiva il 16 aprile visualizzando la frase: "Happy Birthday KAORI! Dedicato a tutte le meravigliose ragazze giapponesi (C) BitLabs (The RebelBase) 1993, N. Italy". Oltre a questi codici virali che si limitano a manifestarsi senza creare danni, ci sono virus, come il Marzia (presumibilmente scritto a Pisa) che nei giorni 30 e 31 dei mesi che vanno da maggio a dicembre riscrive i primi 7 settori di tutte le tracce dei disco fisso. November_17th.855, un altro virus molto noto, dal 17 novembre fino alla fine del mese sovrascrive alcuni settori del disco fisso. Gli effetti collaterali generati dai virus» conclude Tonello «sono invece imputabili a conflitti in memoria con alcune applicazioni, conflitti che si generano con maggior frequenza quando i codici virali utilizzano funzioni non documentate, che possono portare al crash del programma e/o al successivo blocco del computer».

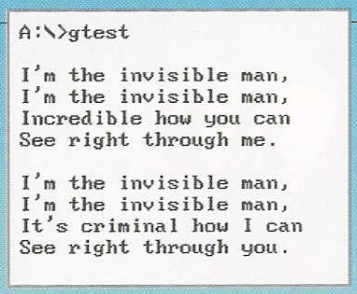
Come si propagano i virus

Le principali vie di contagio sono due: i programmi eseguibili e i settori di boot dei dischi o dischetti. Nel primo caso si installa sul PC il programma infettato e, ogni volta che lo si usa, questo si replica in altri file eseguibili (EXE, COM, BAT eccetera) ma non nei documenti (file di testo, di immagine e via di questo passo). Poi ci sono i virus del boot sector, che alterano il programma presente nel primo settore (il boot sector, appunto) di qualsiasi dischetto formattato DOS. Il contagio avviene quando si avvia il computer mentre è inserito un dischetto infettato nel drive A: il PC legge il settore incriminato ed esegue il codice virale; poi riprende il normale processo di avviamento, solo che intanto è stato infettato anche il boot sector o il Master Boot Record (la parte della prima traccia che contiene le informazioni sulla partizione) del disco fisso, così come sarà infettato, in molti casi, qualsiasi floppy non protetto dalla scrittura usato o formattato nel PC. E Internet, la posta elettronica o i BBS sono fonti di contagio? Gianfranco Tonello è abbastanza scettico: «Attraverso i BBS e INTERNET si possono prelevare file, cioè programmi che potrebbero essere infetti. La possibilità di contagio esiste, ma dai dati sulla diffusione dei codici virali in Italia, si è riscontrato che i virus più diffusi nel nostro paese si trasmettono attraverso il boot sector dei floppy disk, quindi con lo scambio di dischetti tra utente ed utente. Questa tendenza è confermata anche a livello mondiale. I virus del boot sector, tenuto conto della tecnica di contagio che utilizzano, non possono viaggiare attraverso i BBS o INTERNET». Però qualche eccezione, anche curiosa, non manca: «In Italia, in questi ultimi anni, si sono avute tre massicce diffusioni di virus informatici. La prima sembra essere avvenuta a opera del televideo RAI (RAI di tutto di più...), il quale grazie al servizio telesoftware ha distribuito ai propri utenti un programma denominato DIETA che aveva accodato un programma in grado di autoreplicarsi. Dopo accurata analisi ho potuto ri-

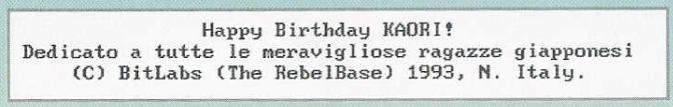
scontrare che si trattava di un nuovo virus, presumibilmente di origine italiana, chiamato Bloody_Warrior. Nel settembre del 1994 una rivista d'informatica ha diffuso attraverso un floppy allegato il virus Junkie.1027 e, nel novembre 1995, lo stesso è accaduto con il virus Bye». Per quanto riguarda il contagio attraverso posta elettronica, questa è oramai diventata una paura diffusa negli utenti di computer che si collegano a INTERNET, ma secondo il nostro esperto si tratta di una leggenda metropolitana, che si è diffusa grazie alla notizia-burla (hoax in gergo) del virus Good Times che si trasmetterebbe attraverso l'e-mail. «Queste notizie "bomba", prima di essere diffuse dovrebbero essere giustificate tecnicamente dall'assertore o diffusore della bufala» commenta Tonello.

Quali misure di protezione attuare? «L'unica precauzione per evitare in assoluto il contagio è non utilizzare floppy disk e, in generale, alcun software importato dall'esterno. Però questa è una pratica improponibile, quindi si deve utilizzare software di provenienza lecita, evitando di copiare illegalmente software di provenienza incerta. La curiosità verso i software shareware è un dato di fatto ma purtroppo questi, passando di mano in mano, possono venire "arricchiti" da sorprese sgradite. Per cercare di evitare questa situazione è consigliabile l'utilizzo di uno o più software anti-virus. Naturalmente, questi devono essere regolarmente acquistati oppure registrati nel caso di programmi shareware» dice Tonello, perché se si registra il proprio anti-virus shareware, o se ne compra uno regolarmente, è possibile usufruire del servizio di consulenza: insomma, quando l'anti-virus segnala la malattia si può prendere il telefono e chiedere indicazioni su che cosa fare (se si usa un programma taroccato, no!!!).





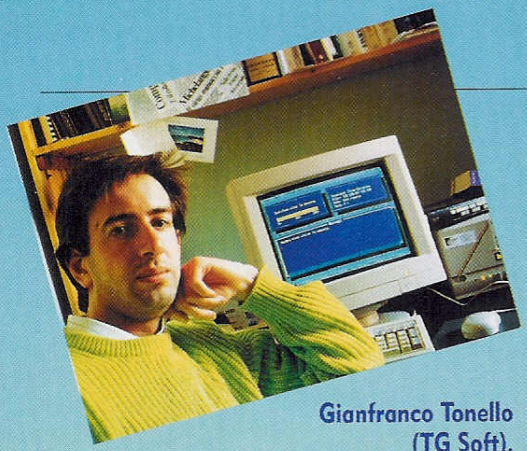
I virus informatici sono sovente accompagnati da scritte o messaggi di vario genere che lasciano intuire la nazionalità dell'autore del virus stesso e, talvolta, il motivo della sua creazione. Nelle schermate a sinistra vediamo qualche esempio di messaggio virale.



Altre raccomandazioni utili sono quelle di non avviare mai il PC con un dischetto inserito, a meno che non sia un dischetto di avvio controllato e protetto. Meglio ancora, se il PC lo consente, si deve modificare la sequenza di boot del computer, in modo da escludere che vada a cercare i dati per avviarsi nel dischetto. Questa operazione si compie attraverso il setup del BIOS ed è facilissimo riportare tutto come prima il giorno che servisse utilizzare il floppy per l'avvio. Fatte salve queste minime indicazioni, però, la difesa più efficace consiste nel corretto impiego dell'anti-virus, quindi non soltanto sul proprio computer, come routine, ma anche su tutti i dischetti che si vanno a utilizzare: i più prudenti dicono addirittura anche sui dischetti che si acquistano già formattati.

L'altro capitolo fondamentale è che cosa fare quando il computer è stato infettato. Si è sparsa la voce, per esempio, che l'ideale è formattare il disco fisso: si cancella tutto e, di conseguenza, anche il virus. Ma le cose non stanno proprio così: in generale questa pratica è sconsigliabile e permette, al più, di ottenere una soluzione temporanea. Il codice virale, vecchio o nuovo che sia, si troverà ancora annidato in qualche floppy, che prima o poi, l'utente avrà la malaugurata necessità di utilizzare reinfettando la macchina. Un'altra misura discutibile è l'uso del comando DOS FDISK/MBR, dove MBR sta per Master Boot Record. Questo comando dovrebbe scrivere nel settore del nuovo codice pulito, eliminando così eventuali virus. Tuttavia è una manovra che molti esperti sconsigliano, in quanto può portare alla perdita dei dati, e quindi va eseguita solo se si sa con esattezza che può servire per quel tipo di virus. Insomma, ancora una volta è fondamentale l'aiuto dell'esperto.

A ben pensarci, in conclusione, per i virus informatici vale lo stesso principio delle malattie virali umane: ammalarsi non è così facile se si ha un minimo di prudenza e, soprattutto, per le cure è meglio affidarsi al medico.



Gianfranco Tonello (TG Soft).

Un buon farmaco funziona così

A chi affidare la difesa del nostro prezioso personal? Quali sono le caratteristiche di un buon programma anti-virus? Secondo Gianfranco Tonello, per essere efficace il software deve avere almeno due moduli: un programma di scansione e di rimozione (per la bonifica dei calcolatori infetti); un programma residente in memoria (TSR), per l'identificazione dei virus prima che infettino il calcolatore. Ma un programma adeguato deve anche rendere disponibile un servizio di assistenza per risolvere in tempi accettabili eventuali problematiche derivanti da virus di nuova generazione non intercettati. È infatti totalmente inutile un software anti-virus che riconosca migliaia di virus, ma che non sia in grado di intercettare il virus che ha colpito l'utente. Inoltre, siccome i virus sono in costante evoluzione come tutto il mondo dell'informatica, bisogna anche pensare all'aggiornamento, ma anche qui senza esagerare: «In Italia, sebbene alcuni esperti asseriscano che ogni mese vengano prodotti nel mondo circa 200 virus, circolano più o meno 70 virus distinti all'anno (50 nel '94 e 64 nel '95). Quindi sembra sufficiente aggiornare il proprio anti-virus ogni 4-6 mesi» conclude Tonello.

Hit parade degli aggressori più tenaci

Secondo i dati di Istinform, i 10 virus più diffusi sono Form (38,7%), Junkie (10,3%), November_17th.855 (10%), FaxFree (5%), Cascade 170X (5%), Bye (3,2%), Stoned (3,2%), Flip (2,4%), Crawen (2 %), Tequila (1,7 %). Nel 1995 le regioni più colpite sono state nell'ordine l'Emilia Romagna , col 24% degli incidenti segnalati, la Lombardia (14%), il Piemonte (12%) e il Lazio (11%). Qualche dato anche sui paesi produttori di virus: ovviamente non di tutti i 7.700 codici virali in circolazione è possibile definire la nazionalità, ma in prima approssimazione il maggior numero viene dalla Russia, seguita da Stati Uniti e Bulgaria (patria del mitico "Dark Avenger", nome di battaglia dietro il quale si nascondeva probabilmente un gruppo di matematici). Nemmeno l'Italia scherza, però, è settima nel mondo e quarta in Europa.

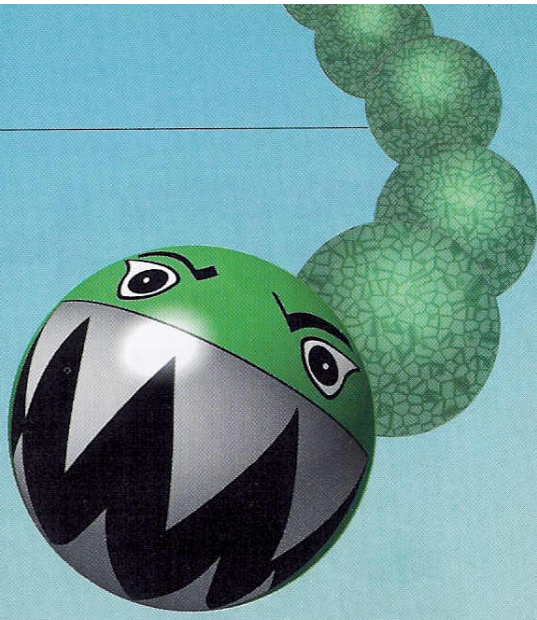
Faccio un codice infettivo perché son vivo..

Che cosa spinge una persona a scrivere un codice virale è difficile a dirsi, ma qualcuno sulla rete ha provato a domandarlo agli stessi autori. Senza pretesa di fare un sondaggio scientifico, ecco alcune risposte giunte al newsgroup alt.computer.virus:

- Perché non capiscono, o non vogliono capire, le conseguenze per gli altri.
- Semplicemente se ne fregano.
- Fanno una distinzione artificiosa tra scrivere/ideare un virus e distribuirlo.
- Traggono un'eccitazione più o meno conscia dagli atti vandalici.
- Credono di combattere in prima linea contro una certa forma di autorità.
- Gli piace sfidare i creatori di anti-virus.
- Per richiamare l'attenzione e ottenere una seppur minima considerazione, sia pure attraverso il nome del loro virus.

La giusta medicina on line

Cercare sulla rete informazioni relative ai virus e ai programmi che li tengono a bada è relativamente semplice. Per cominciare esiste un sito che ha link verso moltissimi altri siti dedicati all'argomento: l'indirizzo è "http://www.innet.net/~ewillems". Notizie sugli anti-virus, prove comparative, analisi, eccetera si trovano invece all'URL "http://www.first.org/virus/virevws". Un'altra ottima fonte di informazioni è il Virus Bulletin che si trova digitando "http://www.virusbtn.com/". Indagini mirate, invece, sono possibili al sito Virus Text Search, che è in pratica un motore di ricerca con accesso ad alcuni dei più completi archivi internazionali: "http://all.net:8000/cgi-bin/all-search-2". Chi cerca dati e notizie aggiornatissimi sui codici virali che effettivamente circolano in Italia farà bene a collegarsi con il BBS C.R.A.V. al numero 049/897596, aperta dal lunedì al venerdì dalle 8:30 alle 19.



Un acchiappa virus made in italy

Oltre che ricercatore e collaboratore di SecurityNet, l'ente che si occupa della sicurezza informatica delle banche, Gianfranco Tonello è l'autore di VirIT (TG Soft, tel. 049/631748). Questo programma anti-virus si presenta piuttosto allettante non solo per l'ottimo rapporto qualità-prezzo, ma anche per le sue caratteristiche di completezza non poi così comuni anche in prodotti più noti. Innanzitutto è in grado non solo di trovare i virus noti ma, grazie alla cosiddetta modalità euristica, può identificare il codice semplicemente sospetto, così da rintracciare eventuali nuovi virus. Il terzo "modulo" del software è invece un programma residente in memoria (VIRITTSR.COM) in grado di segnalare la presenza di virus prima che producano l'infezione del PC. Facile da usare (è scritto in italiano) VirIT è anche tarato in modo specifico sui virus effettivamente presenti nel nostro paese (e che spesso sfuggono ai prodotti stranieri) e consente di avvalersi di un servizio in linea preciso e rapido. ■