Qualche lineetta di febbre...

Le gentili signore stanno ancora in salotto, e io, da persona perbene, sto spiando dal buco della porta (chi non capisce di cosa sto parlando non ha letto la prima parte di questo articolo; male, molto male!). La serata di beneficenza si sta trasformando in bivacco (dal buco riesco a veder solo una signora, più o meno del cretaceo superiore, modello Triceratopo, stravaccata sulla mia poltrona buona con un piatto in ciascuna mano).Beneficenza, quanti delitti si perpetrano in tuo nome!
E' quasi mezzanotte, l'allegra brigata non pare disposta a sciogliersi così facilmente, e la gozzoviglia pare destinata a durare ancora a lungo. Nessuno che si fosse degnato, nei miei confronti, di un "Gradisca", e pure che di copie carbone della ciclopica figura felliniana ne vedo circolare (sempre dal buco) diversi modelli, a due e tre volumi. Il mio stomaco si è trasformato in un buco nero, una stella a neutroni che sta divorando se stessa, ma con la strada verso la cucina bloccata, c'è poco da stare allegri. Ho trovato, nello zainetto della scuola di Anja, due bomboloni e un mandarino, ma è stato come gettare benzina sul fuoco (e poi mi sono sentito come un ladro in chiesa); come snack hanno perfettamente funzionato (tenete presente che, per aperitivo, io uso la pasta e fagioli!) ma adesso, a questo mostro inferocito che è il mio apparato digerente, bisogna assolutamente dare qualche soddisfazione. Penso a una treccia di cacciatorini che ho visto in frigo, se solo riuscissi ad arrivarci! Il computer in camera di Anja è acceso, se avessi un paio di panini con la mortadella (modestamente ho anche inventato una ricetta in proposito, pubblicata su una puntata di "Avvisi ai Naviganti") chi se ne importerebbe più delle signore in salotto. Sostengono che Vittorio Alfieri dimenticasse di mangiare quando studiava, ma evidentemente non teneva nella pancia il verme solitario che alloggia, dalla nascita, nella mia, e cui, lo confesso, sono fortemente affezionato. Allora ritorno al computer e, con l'ascetismo di un monaco tibetano, m'impongo di lavorare (oppiando così la fame). Rino mi ha raccomandato di non tardare oltre domani per la spedizione dell'articolo di ABC, occorrerà che mi dia da fare. Di cosa stavamo parlando? già, di virus! Hiii, che allegria. Se solo mi attaccasse il virus dell'inappetenza, quante cose risolverei! E magari riuscirei anche a venderlo come specialità medicinale. Ve lo immaginate i soldi che farei?

di Raffaello De Masi

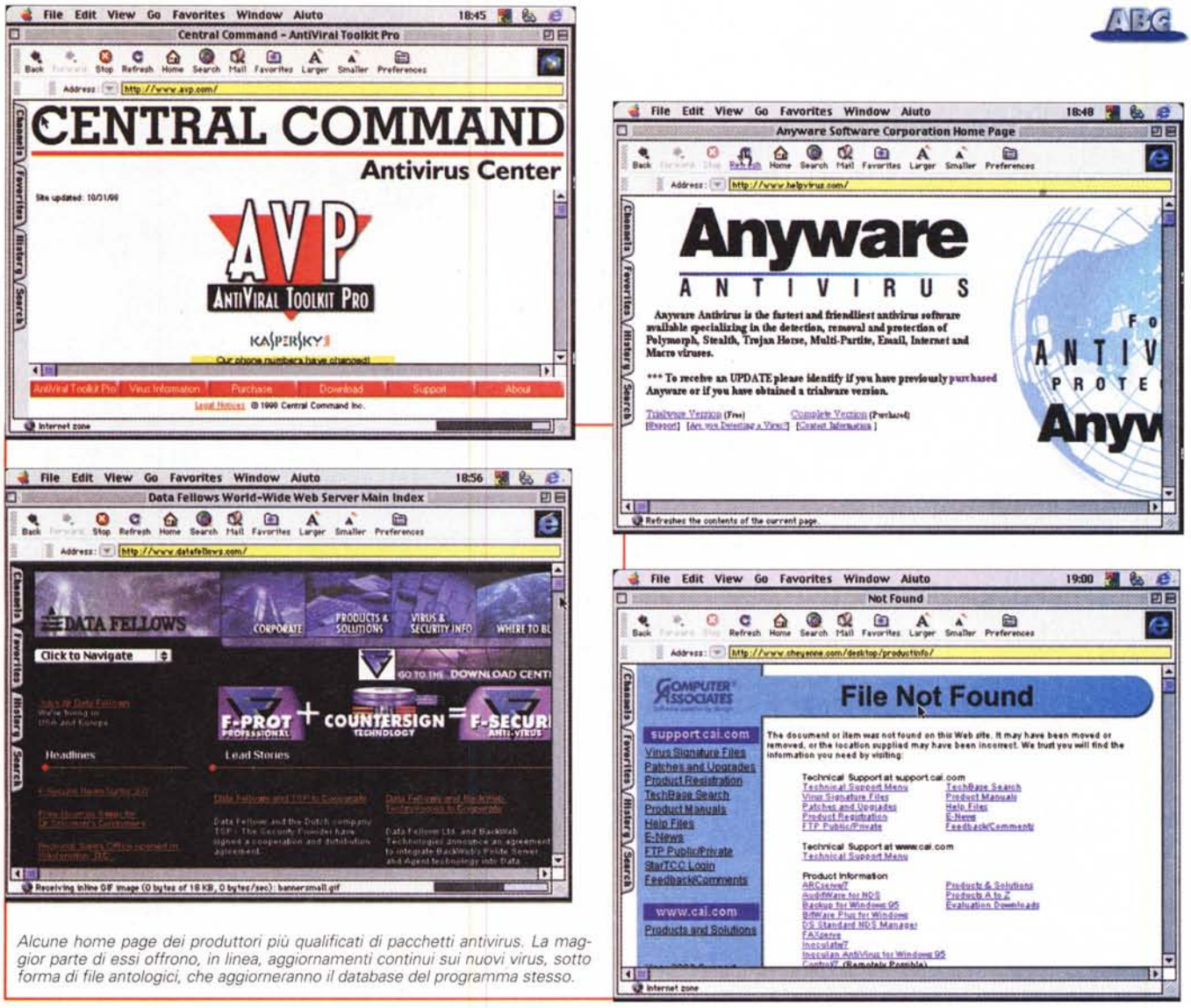
Seconda parte

Ma cosa è un virus?

E soprattutto, come fa ad essere così disastroso per le nostre macchine? Occorre premettere che la pericolosità dei virus è ampiamente diversificata. Ne ricordo uno, inoffensivo, che circolava sul Macintosh agli albori dell'era virus che apriva il giorno di Natale una finestrina con la scritta "Peace in the World", ricordo la famiglia di virus scoperta da don Zucchini (i famigerati virus ZUC) che oggi fanno sorridere per la loro ingenuità; insomma di acqua virale, sotto i ponti, n'è passata parecchia.

Un virus è, per definizione una pièce di programma che copia se stesso e, sovente, in aggiunta, esegue anche una serie di altre operazioni, più o meno dannose. Il termine non è dei più felici, visto che nessuno di essi fa ammalare la macchina; sarebbe stato forse meglio chiamarle, come qualcuno tentò di definirle all'inizio, "weed", malerba, nome che oltre tutto rende molto meglio anche l'idea della loro azione. Tanto per un minimo di buona educazione, anche nel linguaggio, ricorderemo che virus, in lingua italiana, fa al plurale virus e non viruses (vocabolo che denota il rispetto delle regole del plurale inglese, ma dimostra la scarsa conoscenza della grammatica italiana); "viri" e "virii", vocaboli spesso presenti in molte pubblicazioni, non esistono in alcuna lingua.

Dicevamo che, oltre a copiare se stessi, possono anche eseguire opera-



Alcune home page dei produttori più qualificati di pacchetti antivirus. La maggior parte di essi offrono, in linea, aggiornamenti continui sui nuovi virus, sotto forma di file antologici, che aggiorneranno il database del programma stesso.

zioni aggiuntive. In base a quello che fanno, essi prendono nomi diversi. Generalmente l'operazione aggiuntiva non è dannosa né immediatamente evidente, e il motivo è ovvio; se facessero qualcosa di strano o di grave, darebbero immediatamente segno della loro presenza.

Il vero problema che coinvolge i virus è l'essere generalmente molto subdoli. Sovente sono costruiti per evidenziare la loro presenza solo quando si sono abbondantemente riprodotti e il danno è stato già fatto.

I virus possono essere divisi in classi, in base alle loro caratteristiche e, in particolare, all'ambiente in cui si annidano. Essi sono divisi in quattro categorie principali:

- ✔ file virus, che specificamente infettano le applicazioni (parassiti, il più comune tipo di attacco), creano duplicati di file (file compagni) o usano come veicolo file particolari di sistema (link virus);
- ✔ boot virus, che risiedono in un settore di boot del disco, o cambiano il puntatore al settore di boot stesso;
- ✔ macro virus, vere e proprie macro che viaggiano assieme a un documento (file di vari formato di wp, fogli elettronici, database, e, meno frequentemente, altri tipi di file);
- ✔ network virus, che usano come veicolo protocolli e comandi di un network o di una connessione via e-mail.

Manco a dirlo, esistono una serie infinita di combinazioni dei tipi principali; tutti i virus più "moderni" giocano le loro carte almeno in due campi diversi. Inoltre molte scuole di pensiero dividono i virus in base all'algoritmo operativo; TSR, Stealth, polimorfismo e non standard. I più subdoli sono il secondo e il terzo tipo. Lo Stealth (che vuol dire furtivo, nascosto) è un tipo di virus che riesce a nascondere le sue tracce, sovente intercettando le chiamate del sistema operativo alle tracce infette ed evitando che questo si accorga della loro distruzione (certi virus riescono, con una tecnica che ha del prodigioso, quando si accorgono che una chiamata del sistema operativo punta a un settore infetto o corrotto, a sostituire al volo la parte di codice distrutta).

I virus di tipo polimorfico sono i più "cattivi" e più difficili da snidare. Essi non hanno una "signature", vale a dire la stringa che ne permette l'identificazione, visto che riescono continuamente a cambiare il loro codice in maniera del tutto imprevedibile (due esempi dello stesso tipo di virus polimorfico possono essere completamente differenti, se comparati step-by-step).

La cattiveria dei cattivi

E infine i virus si possono classificare in base alla loro distruttività. Si va dai "joke", come vengono chiamati in

USA, a vere e proprie mine che possono distruggere un intero HD.

I virus più "docili" sono quelli "harmless", inoffensivi. Sovente sono anche definiti joke per il loro risvolto divertente. Qui, ovviamente, il discorso si fa particolare; non sempre, infatti, quello che può essere divertente per uno lo è per un altro. Tutto dipende dal senso dell'humour della persona. Ad esempio, uno comparso alcuni anni fa, apriva sullo schermo una finestrina che avvisava "... sto formattando l'HD!", anche se poi non lo faceva. Beh, non sempre si è nelle condizioni d'animo per ridere di una cosa del genere. Altri, come il "Peace in the world", aprono, a date stabilite o dopo un certo numero d'occorrenze, finestre con messaggi particolari. Ma oltre questo non sono particolarmente nocivi, non si riproducono più di una volta sulla stessa macchina e, sovente sono anche facili da estirpare.

La classe successiva è quella dei virus "not dangerous", non pericolosi. Generalmente non fanno altro che ricopiare se stessi sulla parte libera dell'HD, diminuendo progressivamente lo spazio disponibile. Sovente determinano variazioni nella visualizzazione della grafica e nella riproduzione del sonoro. L'anno scorso ne comparve uno, particolarmente divertente, che alla scadenza delle decine del mese scomponeva lo schermo in una scacchiera, iniziando una partita senza senso.

Al disopra di questi livelli il pericolo diviene significativo. Si va dalla modifica dei dati nei file alla loro corruzione completa, alla cancellazione di parti o di tutto l'HD a danni ancora più grandi, come cancellazione della PRAM o, addirittura interferenza con il firmware di gestione delle memorie di massa (secondo una leggenda metropolitana del mondo informatico, esiste un virus che, variando opportunamente la velocità di trascinamento dell'HD, ne determina la distruzione meccanica per effetto della risonanza che v'induce.

Il campionario, nell'ambito di tutte le categorie, è vastissimo. Esempi famosi di virus di pericolosità diversa sono Form (uno dei più diffusi nel mondo; il 18 d'ogni mese si "accendeva" e rendeva inutilizzabile la tastiera, associando anche un suono al tocco di ogni tasto), Jerusalem (che ogni venerdì tredici cancellava ogni applicazione lanciata), Loose (che formattava l'HD), Dark Avenger (che alle sedici sovrascriveva un settore a caso nell'HD con la scritta "Eddie lives ... somewhere in time"). Qui il danno può essere davvero grave; premesso che occorrerebbe fare il backup del disco ad intervalli regolari, spesso ci accorgiamo del danno dopo molto tempo (il virus è fatto per agire in modo graduale e progressivo), e ritornare alla copia di backup è quasi sempre inutile, corrotta com'è anch'essa. L'immaginazione non ha limiti; Chheba, ad esempio, superava le difese di sistema operativo relative alla password di accesso al sistema, creando un nuovo utente con il massimo dei privilegi, con user name e password ovviamente inaccessibile.

Una categoria a parte di infezioni riguarda i Trojan Horse, i cavalli di Troia. Mutuando la loro dinamica dalla mitologia, i cavalli sono programmi che fanno qualcosa di più di quello che ci aspetteremmo lanciando un'applicazione. Un esempio, ormai divenuto classico nella letteratura, di cavallo di Troia è Aids Information Diskette. Nel 1989 ventimila utenti ricevettero una copia di questo file, che riassumeva le conoscenze sull'AIDS e le raccomandazioni per la profilassi e la prevenzione. Una volta aperto, il file installava sull'HD il cavallo, che si annidava in un settore di boot. Dopo la novantesima accensione della macchina i nomi dei file venivano tutti composti con caratteri criptici e appariva una finestra di messaggio che chiedeva il pagamento di una somma per ricevere il programma d'antidoto. Per chi desidera sapere come va a finire la storia, occorre precisare che le istruzioni che accompagnavano l'invio contenevano anche la procedura per ripristinare le condizioni iniziali, ma non tutti quelli comparsi successivamente sono stati così "buoni" (Arachnoid, comparso nel 1995, cambiava in modo assolutamente casuale le estensioni dei file, cosa particolarmente disastrosa per quelli di sistema). Generalmente, comunque, la maggior parte dei produttori di prodotti antivirus mostra una non eccessiva preoccupazione verso questi agenti patogeni.

Due parole, in stile ABC, su come e dove si attacca un virus (e magari, per i più bravi, dove andarlo a cercare...).

Desiderate conoscere, senza poter questo entrare in dettagli tecnici, dove e come s'insedia un virus? In due parole, ecco le risposte.

Il più semplice metodo di infezione è la sovrascrittura; il virus attacca un'applicazione o un file e sostituisce una parte del codice con se stesso. Ovviamente il file infetto diviene inutilizzabile e questo dovrebbe immediatamente avvisare l'utente del problema; ahimé, però non sempre è così, perché l'implementatore del virus fa spesso sovrascrivere aree dell'applicazione attaccata poco usate, così che l'infezione viene rilevata dopo diverso tempo, dando al virus tutto il tempo per propagarsi.

I virus parassiti non cambiano invece il contenuto dei file raggiunti, in modo che il loro contenuto appaia sempre in buono stato; essi possono agganciarsi in testa, in coda o nell'interno del file vittima (in questo caso spostando la restante parte del codice). Quest'operazione può avvenire in vari modi, ma il metodo più usato è quello di spostare una parte della testa del codice del file in coda al file stesso, per fare posto al codice del virus. Ovviamente il virus provvede anche a disciplinare i puntatori in modo che la modifica non sia visibile; la presenza del particolare codice estraneo in testa e in coda serve anche al virus stesso per riconoscere i file infetti e non.

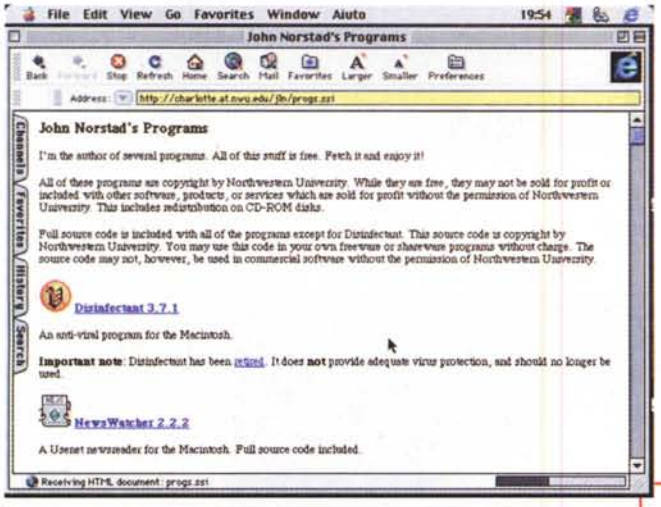
Incorporare un virus al centro del file vittima è un po' più complicato, ma il vantaggio sta nel fatto che sono meno visibili. Sovente questi virus "conoscono" la struttura del file da attaccare e, per nascondere la loro presenza, vanno a sovrascrivere aree non significative o inutilizzate, come la tabella di rilocazione degli indirizzi, gli header dei programmi, o aree del programma che non intervengono nell'esecuzione del programma stesso (ad esempio le aree di "info" o un comando che si prevede sarà poco usato dall'utente). Alcuni virus, più raffinati ed eleganti, addirittura comprimono la restante parte del codice per evitare modifiche della lunghezza, in modo da non essere intercettati dai checksummer. Questi virus, sovente, sono capaci di cambiare il punto di entrata in maniera casuale.

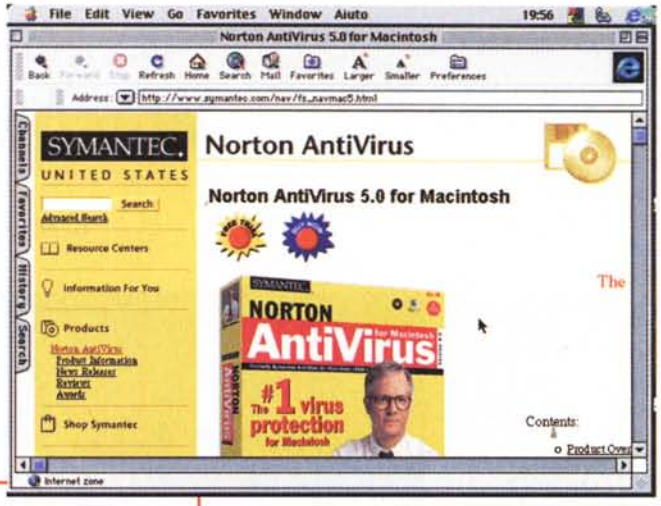
(continua ...)

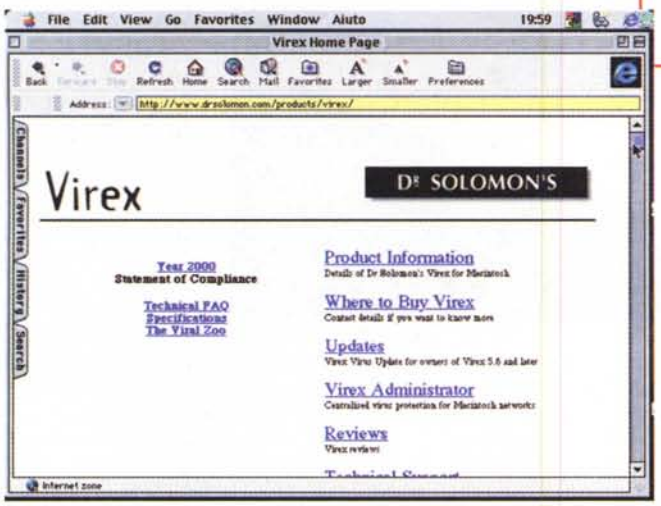
Ma dico io, questa gente che si mette a progettare e a costruire i virus, non tiene niente (per non dire altro...) da fare? Perché non impegna la materia grigia per qualche cosa di più produttivo?

Che fare?

Come in qualunque infezione del mondo reale o del bit, la prevenzione è sicuramente la migliore fonte di difesa. Premesso che occorrerebbe sempre







Anche Macintosh ha i suoi guai, e qualche angelo custode.

avere a disposizione una copia di backup del disco, il sistema migliore è quello di avere installati, sulla macchina almeno un paio di buoni prodotti antivirus. I programmi devono essere aggiornati all'ultima versione e devono poter accedere periodicamente alle librerie delle case produttrici per il download delle più recenti "antologie di stringhe d'identificazione dei virus; e questi pacchetti vanno usati più che regolarmente. Raccomandazioni ovvie (ma non banali) sono quelle di verificare ogni dischetto che passa attraverso la nostra macchina ed a questo può porre rimedio un tool antivirus, fratello minore dei veri e propri programmi, ma molto efficace in fase di prevenzione.

I tool AV sono di due tipi, gli scanner e i checksummer (verificatori di modifiche). I primi generalmente funzionano in modalità on-access; in altri termini eseguono una scansione delle memorie di massa (dischetti, ZIP, Syquest, HD portatili) quando queste vengono montate; VirusGuard, WinGuard o il vecchio Virex per Mac funzionano in questo modo; essi sono continuamente in funzione e vigilano qualunque cosa attraversi la porta della nostra macchina. Generalmente non occupano grande memoria (VirusGuard impegna solo 9K della memoria convenzionale DOS e WinGuard addirittura zero K) quando sono, per così dire, in standby. Queste utility, spesso, non sono completamente efficaci verso l'intero panorama virale (WinGuard, quello forse più noto, non rileva i virus macro) e apprezzabili prestazioni in tal senso offrono anche pacchetti non specifici, come Nuts&Bolts e Norton Utilities. Questi tool possono essere quasi sempre usati on-demand, vale a dire lanciati quando se ne riscontra la necessità; hanno una contropartita, vale a dire che sovente vengono disabilitati dall'utente che odia l'attesa di qualche secondo cui viene costretto durante l'accesso ai dischetti.

L'altra categoria, i checksummer, si basano su un principio: gli eseguibili, le applicazioni, i programmi, insomma, non possono cambiare di dimensione; il checksummer, appena montato, crea un database delle applicazioni, monitorando la loro grandezza. Se, ad una successiva verifica, si nota che un'applicazione ha mutato le sue dimensioni, qualche sospetto è più che giustificato. Il vantaggio di queste applicazioni sta nel fatto che non hanno bisogno d'essere updatate continuamente, quando nuovi virus appaiono sulla scena; lo svantaggio è che falliscono quando virus intervengono sul codice del programma senza modificarne le dimensioni. Attualmente la loro utilità e funzionalità si sta riducendo sempre più.

E arriviamo al piatto forte di questi articoli, i veri e propri pacchetti antivirus. E' su questi che dobbiamo basarci per mettere rimedio al guaio quando questo si è verificato. A quale rivolgersi, e quale utilizzare?

La risposta sarà brevissima, visto che dobbiamo rimandare alla puntata successiva, finale, l'analisi di questi pacchetti: usatene almeno un paio, congiuntamente, sia per monitorare l'ambiente sia per cancellare virus dalla vostra macchina. I motivi di questo consiglio sono diversi; l'enciclopedia virale sta divenendo man mano sempre più ampia, e, sebbene i maggiori produttori facciano a gara per mantenersi aggiornati, e mettano gratuitamente in linea le loro librerie di stringhe d'identificazione, il continuo proliferare di nuovi esemplari e la presenza di virus "cattivi" come i polimorfici rende sovente difficile l'individuazione di certe infezioni, specialmente quelle che gli specialisti chiamano "lente". La scelta è particolarmente ampia; molto materiale, di buona qualità, si trova anche nello shareware e le versioni demo dei pacchetti commerciali continuano a funzionare, anche se con qualche fastidio, anche dopo i fatidici trenta giorni. Perciò, bando alla pigrizia, e stiamo all'erta! MC