Qualche lineetta di febbre...

L'altra sera mia moglie si è portata a casa una riunione di non so quale associazione benefica, e quindi il salotto buono (per la verità è solo quello) era indisponibile (io, la sera, mi sdraio sul divano, in compagnia di certi panini con la mortadella da far venire un collasso a persone meno allenate, e mi vedo un paio di film di fila). Ignobilmente espulso dopo una presentazione telegrafica (una delle rare volte in cui mia moglie mi ha detto: "Ma come, tieni tanto da fare con i tuoi computer!"), e prono alle mia innata inclinazione di rispetto altrui, mi sono messo a spiare dal buco della porta e ho notato come le professioni di filantropia si alternavano a certe passate di dolcetti da far impallidire Scaturchio (per chi non lo sapesse, è una delle più famose pasticcerie di Napoli; se passate per San Domenico Maggiore, sopra Mezzocannone, fateci una visitina e provate un "diplomatico" o una sfogliata riccia, dicendo che vi mando io); e io..., manco il tempo di fare una visitina al frigorifero.

Visto che le belle signore si erano messe comode e non parevano molto intenzionate ad alzare... i tacchi, ho cominciato a pensare a come passare la serata: mettermi a leggere con questo vuoto nello stomaco, manco a dirlo, scendere in studio nemmeno (dovrei passare nell'ingresso, e dare a quegli angeli di carità la soddisfazione di "Prende qualcosa con noi?" , meglio un calcio in pancia!). Ormai in redazione non c'era più nessuno, altrimenti davo un colpo di telefono ad Andrea o a Rino per l'aggiornamento sulle ultime barzellette. L'unica è di mettersi a scrivere l'articolo di ABC, così, almeno stavolta, lo consegno puntualmente.

di Raffaello De Masi

Ed ecco la tegola...

Me ne vado in camera di Anja , dove ho anche il PC, accendo e mi accorgo subito che c'è qualcosa che non va. Il boot è insolitamente lungo, nonostante la macchina sia stata spenta regolarmente, e, anche dopo l'apertura, noto una strana attività, apparentemente inconcludente, del disco rigido. Qualcosa non va per il verso giusto, e lo noto anche aprendo la cartuccia su cui conservo copia di tutti gli articoli. Fare due più due è semplice e improvvisamente mi ritornano alla mente certi strani blocchi di sistema, certe improvvise chiusure di documenti, apparentemente inesplicabili, e il rallentamento generale del sistema che da un po' di tempo sta affliggendo la mia macchina.

Il mio PC si è beccato qualche virus, e speriamo sia semplicemente quello di un banale raffreddore. E' arrivato il momento di far intervenire il medico; il vantaggio, per le nostre macchine, sta nel fatto che non è necessario fissare appuntamenti o aspettare l'arrivo del dottore. E' sufficiente avere semplicemente a disposizione la medicina adatta che, fortunatamente, è unica per tutte le sindromi: un buon antivirus. Lancio il mio buon prodotto antivirus (per adesso non facciamo nomi) ed ecco , preavvisata da una valanga di beep e di messaggi catastrofici, la diagnosi. Siamo infetti, e il nostro PC si sta portando dentro un mostro, del genere di Alien, che lo sta divorando da chissà quanto tempo.

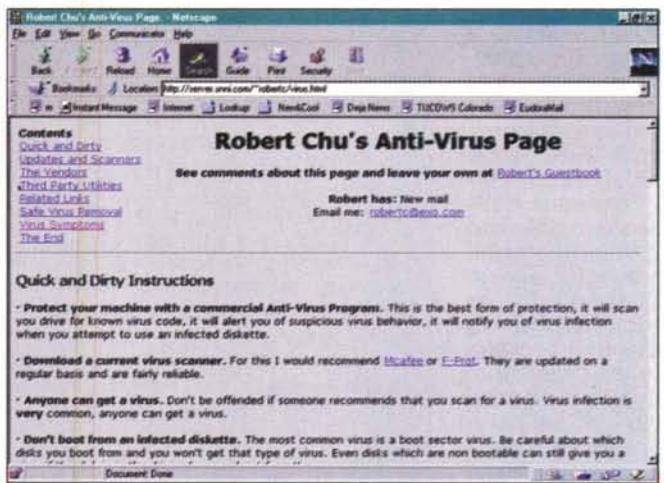
Beh, insomma, non è proprio così. Con un poco di pazienza e senza farsi prendere dal panico il nostro PC (o Mac) lo salviamo, senza neppure uscire con le ossa troppo rotte. L'importante è agire con chiarezza di idee, mirando bene e colpendo forte. Se è vero che il mondo è infestato da qualche diecina di migliaia di virus, è pur vero che abbiamo a disposizione gli antibiotici adatti (con il vantaggio che questi antibiotici, al contrario di quelli del mondo reale, contro i loro virus avversari sono veramente efficienti).

Dagli all'untore...

Come nel caso di un'infezione del mondo reale, non si può agire all'impazzata, senza capire come l'attacco è arrivato e da dove. Molto probabilmente si tratta di un problema meno grave di quanto s'immagini, e in ogni caso c'è sempre possibilità di metterci rimedio. L'importante è agire con criterio, evitando di spiegare in battaglia tutti i nostri mezzi, che potrebbero risultare inutili e inefficaci.

L'attacco in forze contro un nemico astuto, subdolo e agguerrito non raggiunge quasi mai l'effetto desiderato, come tutte le battaglie combattute dal genere umano hanno dimostrato. Ne hanno avuto prova gli americani in Vietnam che conducevano gli attacchi contro aree di giungla con il sistema cosiddetto "a saturazione". I Valkyrie sparavano con le Gatling allo spaventoso ritmo di 6.000 colpi al minuto, ma le perdite , tra i vietcong, erano esattamente pari a quelle che questi infliggevano ai marine con l'uso dei cecchini. Lo dice anche il colonnello Douglas Mortimer nel film 'Per un dollaro in più': "Quando due reggimenti attaccano la stessa posizione, finiscono inevitabilmente per spararsi addosso". Ne sanno qualcosa i russi, che in Afghanistan stavano rimettendoci le penne, contro i mujaidhin armati di kalashnikoff fatti in casa. Perciò pianifichiamo bene la nostra strategia, prima di dare avvio alla tattica.

La prima cosa da fare, quando si sospetta una infezione da virus, è quella di non fare nulla. Robert Chu, nella sua bella pagina di tutorial sui virus, consiglia di mettersi comodi e di non farsi prendere dal nervosismo, visto che questo può provocare ben più danni del virus stesso. Partiamo dal principio che la maggior parte dei nostri indesiderati ospiti può essere rimossa senza perdita di dati, e avremo già fatto il primo passo giusto.



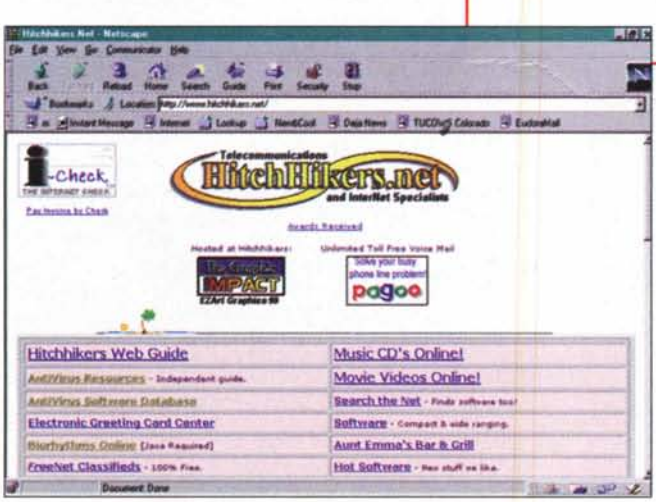
la home page di Robert Chu, un ottimo sito per imparare a conoscere i virus

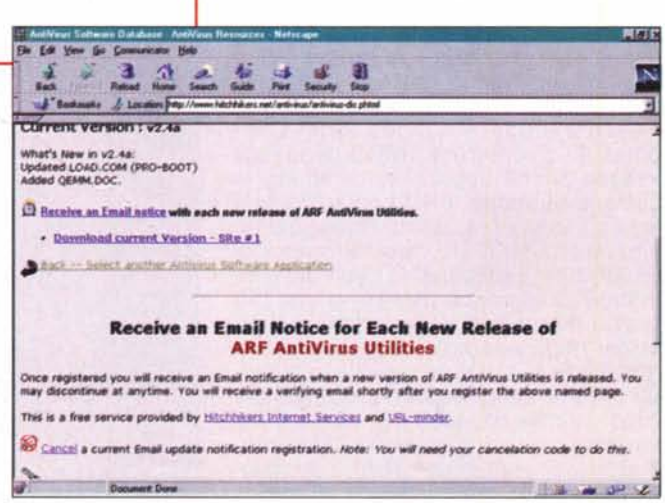
Innanzi tutto occorre precisare che, più spesso di quanto non si pensi, ciò che si scambia per un virus è ben altra cosa. Un file che non si apre più, un programma che si chiude inaspettatamente, un documento di videoscrittura che, improvvisamente, appare pieno di caratteri criptici, non sono necessariamente sintomi di un'infezione. E così è importante adoperare, fin dall'inizio, un minimo di discernimento, che rispetta alcune considerazioni di carattere generale, che non abbisognano di una cultura avanzata, nel campo dei calcolatori e della ricerca antivirus, per essere comprese.

Innanzi tutto non è detto che la diagnosi positiva eseguita da un pacchetto sia una condanna inoppugnabile. Nessun prodotto AV è infallibile e alcuni package possono fornire una indicazione falsa, per così dire, per troppa prudenza.

Il motivo è presto detto; gli AV funzionano cercando , nel file infetto, una sequenza particolare di byte; nello sforzo di individuare il maggior numero di virus, le stringhe oggetto di ricerca sono estremamente numerose. E' ovvio quindi che, per un motivo o per un altro, può verificarsi che una certa stringa di caratteri sia riconosciuta come segnale di un virus, mentre tutto questo non è. Un esempio, per chiarire immediatamente il caso; chi ha prodotto il virus ha, ovviamente, usato un compilatore; questo ha potuto inserirvi una pièce di codice che fa parte della runtime del compilatore stesso, e che, ovviamente, potrà far parte anche di un programma perfettamente regolare. In questo caso pacchetti prodotti con lo stesso compilatore potrebbero dare un falso allarme (in effetti molti produttori di virus usano questo trucco per mascherare meglio i propri "rampolli"). A

il sito Hitchhikers, contenente un aggiornatissimo database dei virus finora scoperti. I Db sono già organizzati per essere letti dai correnti antivirus, commerciali e shareware





complicare ancora di più le cose ci si mettono i virus polimorfi, che modificano la sequenza dei loro byte ad ogni successivo attacco; ovvio quindi che la loro ricerca diviene estremamente difficoltosa, e complessa da distinguere da file senza macchia.

Esiste una serie di indicazioni (come dicono in USA "Quick & Dirty") che, anche se non infallibili al 100%, permettono di orientare l'opinione della persona che teme di essersi beccato "l'influenza". Si tratta di falso allarme quando, all'analisi, un solo file appare essere infetto (i virus sono fatti per moltiplicarsi), o quando, sebbene sia diagnosticata un'infezione, il package AV usato non riesce a diagnosticarlo. Viceversa ci sono diversi indicatori dell'avvenuto contagio che sebbene non determinanti, lasciano pensare a probabili guai in vista. In questo caso, diversi prodotti AV diagnosticano lo stesso virus, molti file appaiono infetti allo stesso modo, diversi file .EXE e .COM appaiono più grandi delle loro dimensioni abituali e, cosa più importante, tutti più grandi della stessa lunghezza. Spesso quando si tenta di salvare un file Word l'opzione appare non disponibile (in Windows) o il sistema rifiuta di registrare sul floppy (Mac); sovente, ancora, W95 rifiuta l'accesso al disco/file a 32bit. Occhio, poi, al led dell'HD; una attività ingiustificata del disco rigido è spesso sintomo di guai, e altrettanto sospetta è lo strano aspetto di grafica sullo schermo o la forma delle icone (il diffusissimo virus CAP, una macro di Word estremamente infestante, modificava l'icona originale dei documenti (quella con la grossa W) in una con una freccia tratteggiata (quella dei modelli)). Ancora, il sistema non riesce a leggere il disco 2 del Windows su dischetti, il CMOS dimentica i setup anche dopo aver cambiato la batteria tampone, l'HD non può essere raggiunto eseguendo il boot dal dischetto, CHKDSK riporta meno di 655360 byte disponibili, l'HD dichiara inaspettatamente di non avere più spazio disponibile, si avvertono rumori strani negli altoparlanti battendo alla tastiera, e così via. In ogni caso, quando si teme di essersi beccato qualche virus, la cosa più saggia è inviare il file sospetto al servizio dei principali produttori , che, generalmente, rispondono nelle 24/48 ore.

Tre lettere, due risposte

Fino al Natale scorso la posta che i lettori mi inviavano era generalmente incentrata sul Macintosh , visto anche che sono quindici anni che ne parlo sulle nostre pagine. Poi Rino Nicotra mi passò le redini di questa rubrica, e la mia casella, nella maggior parte delle volte per mio demerito, si è riempita di lettere di genere diversissimo.

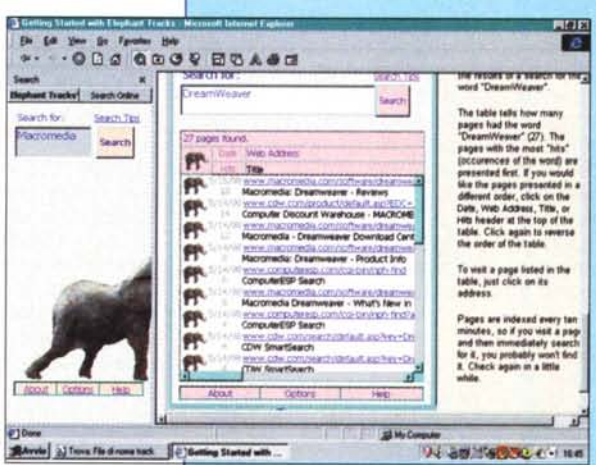
Così ABC pare debba essere divenuto, nell'immaginario dei nostri lettori, una specie di "manuale delle Giovani Marmotte", in cui trovare risposta a tutto quel che si cerca. Lo so , certo, di essere enciclopedico come Mr. Belvedere o "L'uomo di bronzo", e mi fa certo piacere che la rubrica sia divenuta, in barba alla sua giovane età, cotanto punto di riferimento, ma credo che diverse persone , nella rivista, siano più qualificate di me nel rispondere a certi quesiti.

Quando, comunque, non reindirizzo ad altri le lettere, rispondo sempre a tutti i lettori che mi scrivono. Devono avere solo un po' di pazienza, se non lo faccio proprio lo stesso giorno o quello successivo.

Invece pare che la fretta sia la musa ispiratrice di Davide G. , di La Spezia, che mi ha scritto quattro volte in due giorni per pormi un solo quesito semplice, ma di non facile soluzione. E' possessore di un Macintosh e di un PC e ha sempre apprezzato , nel primo, la possibilità di comandare, allo startup, il lancio di diversi gruppi di programmi in autorun, come si sa, schiacciando la barra spaziatrice. Davide mi chiede se (senza per questo caricare utility non di sistema operativo) è possibile fare la stessa cosa in ambiente Windows 95 (non 98).

Caro Davide, dalle mie parti non si può paragonare la lana alla seta (e giù, adesso mi aspetto un'altra valanga di PCisti inferociti! a minor onta vorrei precisare che questa possibilità del Mac è solo recente, mentre prima era affidata a una utility di NowSoft). Davide chiede di poter fare ciò in casa, senza cioè ricorrere a utility esterne; vediamo come fare.

Premesso che, con solo ciò che pone a disposizione il sistema operativo, quello che il lettore chiede non è realizzabile, la soluzione almeno parziale del problema c'è. Si può creare una cartella dove trascinare , dalla "esecuzione Automatica" i programmi non desiderati, e lanciare questi quando servono. Ma una soluzione più elegante è data dalla creazione di una cartella nella stessa cartella di Startup; chiameremo questa con un nome acconcio (es. No Startup o In Attesa di Partenza) e vi trascineremo i programmi o le utility non sempre necessari. Gli elementi contenuti in essa non partono automaticamente allo startup, ma la cartella , al boot, si apre, mostrando il suo contenuto, in modo che , in caso di necessità, si può accedere al programma desiderato.



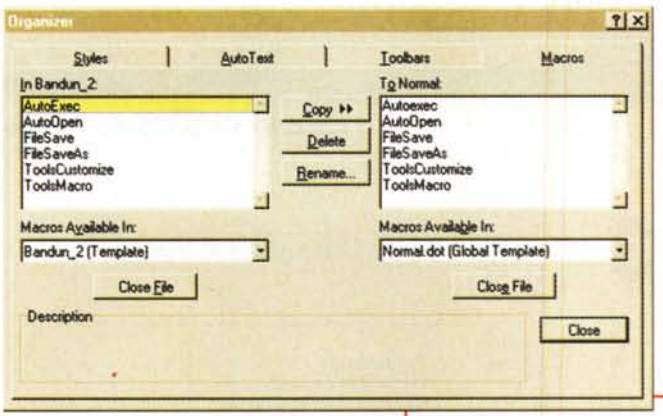
Per i non Pico...

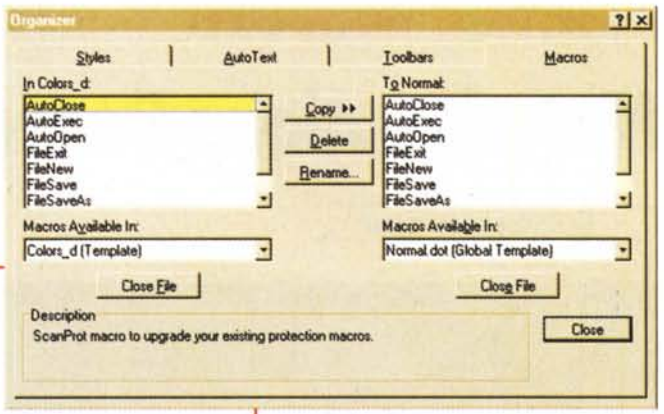
La seconda risposta è rivolta a Remo U. di Catanzaro, e Alfonso F. di Aosta, che, con termini diversi mi pongono lo stesso problema. Che poi sarebbe, in termini ridotti all'osso, questo: "Ricordo di aver trovato, qualche giorno fa, correndo su Internet, una notizia riguardante una nuova ricetta sui tortellini alla panna (o su una associazione di collezionismo, o sulla convention mondiale degli Amici di Naomi). Purtroppo non ho salvato il bookmark, e neppure la history del browser mi fa capire molto – forse è andata persa o cancellata. Come posso fare?"

La risposta sta in un pacchetto originalissimo della Elephant Software , http://www.elephant-software.com che ha , come descrizione delle sue funzioni, tre domande e una risposta: "Ti è capitato ultimamente di aver perso un sacco di tempo cercando di ritrovare una pagina WWW che ti interessava? – la lista dei tuoi bookmark è diventata più lunga di un braccio? – ci sono pagine di cui hai solo un confuso ricordo e che non riesci a ritrovare? immagina di poter ritornare, ad un semplice tocco, a tutto quello che in una maniera o nell'altra hai letto o intravisto su WWW; adesso smetti di immaginare, e lascia che Elephant Tracks ricordi per te!"

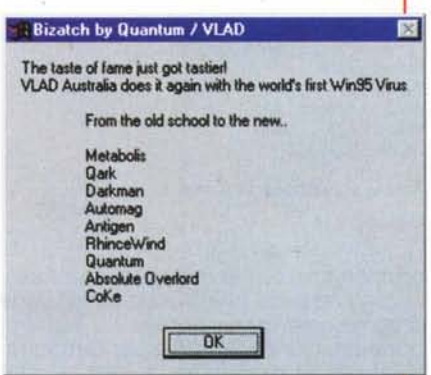
Elephant Tracks, questo il nome del pacchetto, è una utility di browser che "ricorda" praticamente ogni parola di ogni pagina scorsa nelle nostre "navigate". In altri termini ET lavora come un motore di ricerca, ancorché personale; basterà battere in una apposita casella la parola cercata per avere una lista di indirizzi, precedentemente visitati, in cui questa parola compariva (sono ammesse ricerche con operatori). Il vero vantaggio rispetto alla semplice cache del browser (che poi non sempre fa quello che noi diciamo!) sta nel fatto che ET non "ricorda" le pagine, ma solo le parole in esse contenute , e le conserva , oltre tutto, in forma compressa, così da richiedere, mediamente, circa 2 K per pagina (una diecina di mega, usualmente lo spazio riservato alla cache dei browser, conterrebbe ben cinquemila pagine) Il pacchetto permette anche il setup dei parametri di "conservazione", permettendo ad esempio di stabilire la cancellazione automatica dopo un certo tempo.

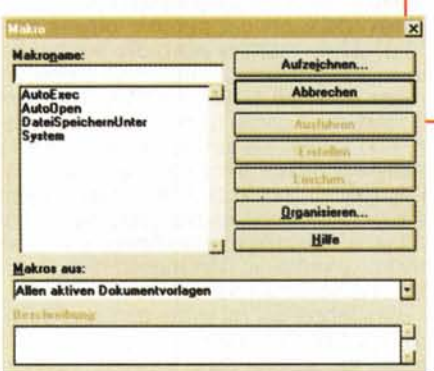
Elephant Tracks è disponibile per Internet Explorer 4 su macchine W95 e W98; al momento della disponibilità in edicola di questo numero sarà probabilmente disponibile anche la versione per Netscape 4.

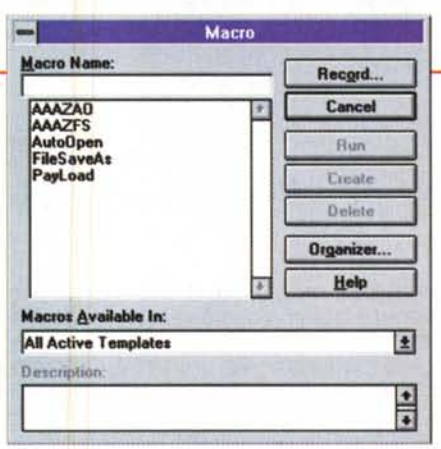


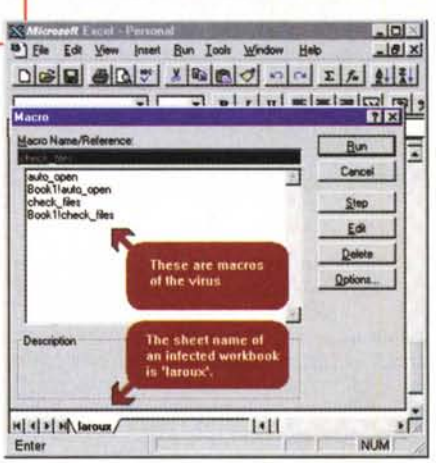


alcuni virus in azione; beh, se vi sta comparendo qualcosa del genere, potete cominciare a preoccuparvi!





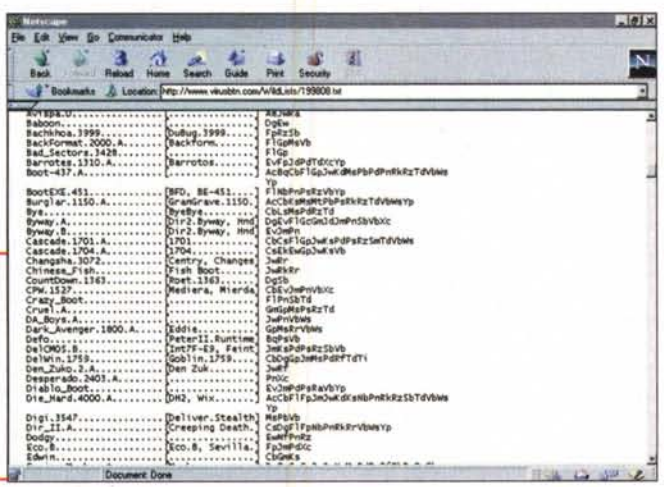




Conclusioni

In questa puntata preliminare abbiamo appena appena accennato al problema. Certo, da quando i virus sono comparsi sulla scena (il padre del primo virus è Joel McNamara, che lo presentò nel dicembre 1994 in un simposio al MIT, per scopi dimostrativi; il primo virus "commerciale" è dell'estate del '95) il panorama è molto cambiato, con esemplari sempre più numerosi e virulenti (alla fine del 1997 i virus noti erano quasi 2000, e oggi raggiungono i diecimila, con un ritmo di comparsa di qualche centinaio al mese – fonti MCAfee). Ma, fortunatamente, una sparuta schiera di Cavalieri di Camelot riesce a tener loro testa, sia attraverso pacchetti commerciali sia attraverso shareware che non ha molto da invidiare ai precedenti. Ma, come nella vita, la migliore difesa è la prevenzione; perciò rifornitevi, cari amici, di un buon package e installatelo immediatamente; la prossima volta vedremo come fare per usarlo al meglio.

MS



un esempio di database di identificatori di virus, con relative stringhe di ricerca; questo è l'elenco dei nuovi virus comparsi nel solo agosto 1998 (e ce ne sono più di trecentocinquanta) . Perciò, occhio!