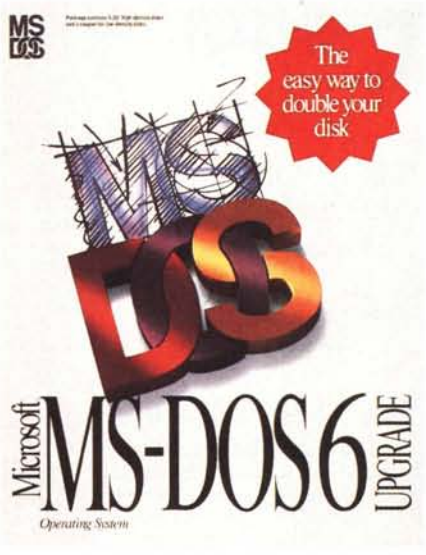
# Vecchio e nuovo

*«Smettere di fumare è facilissimo: io stesso ci sono riuscito molte volte». La citazione (a memoria, quindi imprecisa) è di Mark Twain; personalmente ho smesso di fumare più di sei anni fa e non ho mai più avuto voglia di ricominciare, ma non è per questo che l'ho riportata. Gli è che il mese scorso avevo scritto che non avrei più recensito antivirus, e questo mese invece parliamo di MSAV, l'antivirus incluso nel Dos 6. Non si può non parlarne, data l'importanza che deriva dal fatto che di Dos 6 presumibilmente ne verranno installate alcune decine di milioni di copie nel mondo in breve tempo, e che pertanto MSAV diventerà il numero 1 come base installata. Soltanto in Italia tra breve ce ne sarà oltre un milione di copie in circolazione: è una stima prudenziale, largamente per difetto, ma rappresenta la punta massima di diffusione di un antivirus nel nostro Paese da quando è scoppiato il fenomeno dei programmi autoreplicanti*

***di Stefano Toria***

Sempre in Italia restiamo con un riquadro d'attualità: abbiamo visto (con una certa preoccupazione, non lo nascondiamo) aumentare rapidamente il numero di virus apparentemente scritti in Italia. Proprio in questi giorni abbiamo terminato l'analisi di un virus scritto in una Università italiana, almeno stando a quanto afferma il suo autore; si tratta di un oggetto piuttosto pericoloso, ma non è né l'unico né l'ultimo. Abbiamo pensato quindi di parlare brevemente dei virus presumibilmente originati nel nostro Paese, con l'avvertenza che si tratta di una classificazione di comodo e non funzionale: la telematica ha abbattuto le frontiere della comunicazione, e un virus scritto in un luogo può iniziare a diffondersi a migliaia di chilometri di distanza anche dopo pochi minuti. Se facciamo un discorso a parte sui virus italiani è perché alcuni di essi hanno avuto una certa diffusione locale in tempi brevi, il che fa pensare all'attività di qualche gruppetto di vandali; non certo perché riteniamo che in Italia il pericolo dei virus derivi esclusivamente da virus italiani: sarebbe un'idea sciocca e priva di fondamento. L'attenzione dell'utente medio va rivolta indistintamente a tutti i virus, non solo a quelli provenienti da un certo luogo o che si attivano in una certa data. L'unico modo per salvarsi è di non abbassare la guardia, mai.

Da un paio di mesi non si parla d'altro che del Dos 6. Gli utenti più avanzati fanno confronti tra le capacità di compressione di DoubleSpace e di altri prodotti analoghi, o tra le funzioni di allocazione di memoria di MemMaker e quelle di altri gestori di memoria estesa o espansa. Gli utenti meno orientati alle dispute tecnologiche si interrogano sull'opportunità di passare al Dos 6 o se non sia preferibile rimanere fedeli alla




collaudata versione 5.

Vogliamo aggiungere il nostro personale contributo a questo fermento di idee; con la versione 6 dell'ultradecennale sistema operativo viene (finalmente?) dato il crisma dell'ufficialità al problema dei virus, perché se la Microsoft arriva a includere nell'ultima versione del proprio «cavallo da tiro» un antivirus allora vuol dire che il problema è serio. Così almeno penserà una larga parte dell'utenza.

## Aprendo la scatola

Il Dos 6 è arrivato in redazione sotto forma di Upgrade. Continuando nella politica che aveva inaugurato con la versione 5 la Microsoft ha dato per scontato che una larga parte degli utenti delle versioni precedenti del sistema volesse passare alla nuova versione senza troppi problemi; pertanto ha previsto una procedura di aggiornamento automatico, che consente un passaggio relativamente indolore dal vecchio al nuovo sistema. Non sta a noi, nella nostra rubrica, trattare delle varie opzioni della procedura di passaggio, né discuterne pregi e difetti.

Ai virus sono dedicate quindici pagine nel corpo del manuale, più una breve appendice sull'uso del BBS da cui possono essere prelevate le firme dei nuovi virus. Ma procediamo con ordine.

Cosa sono i virus del computer?

Si intitola così il primo paragrafo che il manuale dedica all'argomento. In poche righe, e con qualche approssimazione, vengono fornite all'utente alcune nozioni di massima sul fenomeno.

Apprendiamo quindi come effettuare la scansione, cioè la ricerca dei virus, con la possibilità di rimuovere i virus identificati. Le due operazioni possono essere effettuate sia direttamente dal Dos che sotto Windows.

Inoltre si può rendere automatica la scansione ad ogni avvio del computer, inserendo l'apposito comando nell'AUTOEXEC.BAT.

All'avvio il programma mostra il messaggio di copyright in favore della Central Point Software; il Microsoft Anti-Virus infatti non è che una versione personalizzata di un prodotto commerciale molto noto, il Central Point Antivirus.

Una serie di opzioni consentono di personalizzare il funzionamento dell'antivirus. Due esempi di opzioni configurabili: l'utente può attivare il controllo di integrità dei file eseguibili, basato su valori di checksum preventivamente calcolati dallo stesso programma e archiviati in un file specifico; è possibile attivare un dispositivo anti-stealth, per

combattere cioè quei virus che si mimetizzano in modo da evitare di essere rilevati.

Il prodotto contiene una lista dei virus che è in grado di riconoscere (circa 800 al momento del rilascio).

La documentazione cartacea, piuttosto stringata, è supportata da un esauriente help on-line che offre spiegazioni dettagliate sul significato e sull'uso di ciascun comando.

VSafe

L'antivirus fornito con il Dos 6 si compone di una parte richiamabile dall'utente e di una parte che può essere installata residente, per rendere automatico il processo di controllo ogniqualvolta viene richiesta l'esecuzione di un programma.

Secondo il manuale VSafe richiede 44 Kb di memoria per rimanere residente, e può essere gestito da un sistema di controllo di cui esistono due versioni, l'una per Dos e l'altra per Windows.

### *Impressioni e commenti*

Il Microsoft Anti-Virus appare a prima vista un prodotto realizzato in fretta per poter affermare di aver fatto qualcosa per il problema dei virus, piuttosto che il tentativo di realizzare un vero strumento robusto per la difesa dai programmi aggressori. Ne avevamo il sospetto, e ne abbiamo avuto facilmente la prova: senza nemmeno doverci scomporre a sottoporre il prodotto alle solite prove che i nostri lettori conoscono, abbiamo semplicemente preso un file eseguibile infetto da un banale virus e lo abbiamo fatto esaminare dalle due versioni del prodotto, quella per Dos e quella per Windows. La prima ha rilevato il virus, la seconda no. E il fatto, di per sé sconcertante, appare piuttosto grave se si considera che il virus utilizzato nella prova è il Pogue, uno tra i primi virus sviluppati con il Dark Avenger Mutation Engine, apparso oltre un anno fa.

Ma non è solo per questo che la nostra opinione sul prodotto è negativa. In fondo, si potrebbe obiettare, il Pogue non è né diffuso come il Form o il Cascade, né violentemente infettivo come il Dark Avenger, né pericoloso come il Datacrime o il Michelangelo. L'unica cosa notevole al suo riguardo è che è stato scritto con il famigerato Mutation Engine. È un virus da laboratorio, presente soltanto nelle collezioni di qualche ricercatore: che pericolo può costituire?

Il ragionamento è sbagliato, e ne spieghiamo le ragioni in un apposito riquadro. Ma non è ancora tutto: il manuale contiene diverse imprecisioni e alcune indicazioni fondamentalmente errate, come quella secondo cui in caso di rilevamento di virus occorre riavviare il computer servendosi della sequenza ctrl+alt+del: l'autore di questa indicazione forse ignora il fatto che questa sequenza può essere tranquillamente intercettata da qualsiasi virus, e di fatto ve ne sono diversi che lo fanno (due esempi: Den Zuko e Fu Manchu, entrambi scoperti nel 1989).

Uno dei messaggi di segnalazione emessi dal programma, e riportato dal manuale, ci ha fatto rabbrividire. Ne riportiamo la traduzione in italiano:

«Il virus xxxxxx infetta i file di DATI oltre ai file eseguibili. Pertanto è necessario controllare tutti i file su questo disco. Per vostra comodità l'opzione Controllare Tutti Files verrà automaticamente attivata quando avrete letto questo messaggio. Quando questa opzione è attiva, Microsoft Anti-Virus verificherà tutti i file sul disco, inclusi i file di dati».

Per chi ci segue da pochi numeri, preciseremo che l'idea che un virus possa «infettare» i file di DATI è risibile. Tecnicamente è possibile, in quanto nulla impedisce a un virus di scrivere una copia di se stesso in coda a qualsiasi oggetto, ad esempio questo articolo che sto scrivendo. Ma poiché per definizione non potrò mai far eseguire questo articolo dal microprocessore, perché non è codice eseguibile, quand'anche un virus perda tempo a «infettare» questo articolo (o qualsiasi altro file di dati) avrà per l'appunto perso tempo.

### *«Finalmente, è finita con questi virus!»*

Ma la causa delle nostre perplessità è ben più profonda. Inserire un antivirus, e in particolare questo antivirus, nella release più recente del più diffuso sistema operativo al mondo è un'operazione

## Bisogna ammazzarli tutti

Ci accade sovente di leggere o sentir dire che è importante che un programma antivirus sia in grado di rilevare i virus più diffusi e/o i più pericolosi, ma che non è un problema se qualche raro virus scappa fuori dalle maglie della rete. Qualcuno spinge il discorso fino ad affermare che per ragioni di efficienza vanno ricercati esclusivamente i virus in effettiva circolazione ed esclusi dalla ricerca quelli sperimentali o di laboratorio.

Questo ragionamento è sbagliato per due ragioni. Innanzitutto le statistiche (quelle poche disponibili) dimostrano che la diffusione dei virus ha caratteristiche fortemente regionali. Patricia Hoffman classifica come «raro» il virus 855, che abbiamo visto quale diffusione abbia in Italia. In Inghilterra è molto diffuso lo Spanish Telecom, che personalmente ho visto piuttosto di rado dalle nostre parti. Chi stabilirà quale virus è diffuso e quale non lo è? E in base a quali statistiche? Tipicamente le cause della diffusione di un virus prescindono dalla volontà dell'autore o dalle caratteristiche tecniche del virus; spesso anzi si tratta di un colpo di «fortuna» (dal punto di vista del virus), come avvenne con il Michelangelo. Che succede se da un giorno all'altro un virus sperimentale viene riprodotto in centinaia di migliaia di copie e spedito in giro per il mondo?

Ma alla base dell'errore nel ragionamento c'è un altro fatto. Esistono da diverso tempo numerosi sistemi telematici (BBS) che si prefiggono come fine più o meno esclusivo quello di agevolare la comunicazione tra i singoli e i gruppi del cosiddetto «underground» dell'informatica, più o meno ispirato all'ideologia cyberpunk e ai suoi proclami sulla necessità di rendere libera e gratuita l'informazione. Gran parte di questi BBS offrono ai propri utenti una vasta collezione di virus, alla quale chiunque lo desideri può attingere liberamente. In modo indiretto alcuni di questi sistemi contribuiscono anche allo sviluppo del numero di virus esistenti, poiché impongono che chiunque desidera prelevare virus debba essere autorizzato, e la condizione per ricevere l'autorizzazione è di contribuire alla collezione con un virus originale.

Gran parte dei virus esistenti sono reperibili su questi «virus exchange BBS». Molti sedicenti esperti di virus collezionano e scambiano campioni di virus come farebbero con le figurine dei calciatori. Affermare che un virus non è diffuso è velleitario. Quanto tempo ci vorrà perché uno di questi virus scappi di mano a uno di questi incoscienti collezionisti? Non dimentichiamo che uno dei virus più diffusi al mondo, lo Stoned, si è diffuso proprio in questo modo.

Uno studente neozelandese lo aveva scritto per prova e lo teneva accuratamente al sicuro nel proprio computer. Il fratello minore ne prelevò una copia e infettò un computer della propria scuola, ovviamente in segreto, pensando che bello scherzo sarebbe stato. Ecco il risultato: milioni di copie di questo virus girano allegramente per il mondo.

Anche adesso, mentre sto scrivendo queste righe, potrebbe star succedendo la stessa cosa con il Pogue o con uno qualsiasi degli oltre millecinquecento virus teoricamente «da laboratorio». Qualsiasi programma antivirus degno di rispetto deve essere in grado di riconoscere perfettamente ciascuno di questi virus.

*Stefano Toria*

di marketing che nulla aggiunge alla soluzione del problema della sicurezza dei PC, e anzi contribuisce notevolmente ad aggravarlo.

Data l'attuale struttura del personal computer IBM (e compatibili) non esiste alcun prodotto al mondo, hardware o software, che possa risolvere definitivamente il problema dei virus. Ripetiamo ancora una volta che il problema si affronta (attenzione: si affronta, non si risolve) adottando sì le opportune misure hardware e/o software, ma educando preventivamente l'utente a conoscere il problema, a capire se un determinato comportamento è rischioso o meno, a riconoscere il sintomo di una potenziale infezione e a distinguerlo, per quanto possibile, da un banale problema di falsi contatti o di errori nel software.

Una delle domande che compaiono regolarmente ai seminari e alle conferenze sui virus è la seguente: «Ma non è possibile includere nel sistema operativo una difesa dai virus?». La risposta a questa domanda è regolarmente un no ben motivato. Cioè: no allo stato attuale delle cose. Sì se si riprogetta interamente il personal computer più diffuso al mondo, ignorando il fatto che forse là fuori ci sono novanta milioni di macchine tutte fatte allo stesso modo. Dato questo stato di cose è improponibile riuscire a includere in una futura versione di Dos, o di un simile sistema operativo, una misura efficace contro i virus.

Ma questo fatto è noto soltanto agli addetti ai lavori e ai pochi che hanno seguito corsi, seminari e convegni sulla sicurezza dei PC. Il grande pubblico questo non lo sa. Pertanto è facile prevedere che l'uscita di un Dos che comprende anche un antivirus sia vista da una larga fascia dell'utenza come il segnale che finalmente qualcuno ha messo le misure antivirus dentro al sistema operativo. Ma abbiamo visto che non è così, perché l'antivirus non è una parte del sistema operativo (e anche se lo fosse stato avremmo nutrito seri dubbi sulla sua efficacia): è un programma come tutti gli altri. Come i vari Scan, F-Prot, Sweep, ThunderByte AntiVirus, VI-Rex e tutti gli altri che abbiamo incontrato nel corso di questi anni.

E siccome tutto ciò è ignoto al grande pubblico potrebbe accadere che molti installino il Dos 6, abbassino la guardia sentendosi finalmente sicuri e si verifichi una recrudescenza del fenomeno.

### Il bersaglio immobile

E c'è ancora un'altra considerazione da fare. Tra i circa duemila virus conosciuti ve ne sono alcuni che nel proprio comportamento prendono specificamente in considerazione la possibilità di trovare installati nel sistema-vittima alcuni noti prodotti antivirus. È il caso del virus Peach, che prende di mira il Central Point AntiVirus, o dell'855 che va in cerca di SCAN o CLEAN; si potrebbero fare ancora altri esempi. (Detto per inciso è questa una delle ragioni per cui si suggerisce di non limitarsi all'uso di un solo antivirus, ma di utilizzarne almeno due o tre, e di non usare mai antivirus residenti se non in casi del tutto particolari).

Sono pronto a scommettere con i miei pazientissimi lettori che per la data in cui leggeranno questo articolo sarà già comparso il primo virus scritto appositamente per aggirare il Microsoft Anti-Virus. E che prima di Natale ve ne saranno in circolazione almeno una decina. Una rapida analisi del prodotto ha mostrato almeno un paio di punti di attacco per un virus che voglia ingannare questo antivirus, e abbiamo ragione di ritenere che l'attacco condotto in questi modi avrebbe pieno successo.

Personalmente non credo negli antifurti elettronici, e difendo la mia autovettura con una robusta sbarra di acciaio che blocca i pedali: per tagliarla occorre la fiamma e nessun ladro di auto va in giro con il cannello ossiacetilenico. Ma quand'anche volessi acquistare un antifurto elettronico l'ultimo che acquisterei sarebbe un modello del quale posso avere la certezza che tutti i ladri di auto ne possiedono uno. E senz'altro i primi a installare il Microsoft Anti-Virus saranno proprio i più incalliti autori di virus.

### L'assistenza

Un punto fondamentale per qualsiasi prodotto antivirus consiste nell'assistenza post-vendita. Per le proprie ca-

## Un sistema operativo antivirus

A botta calda mi rendo conto che nella recensione del Microsoft Anti-Virus ho fatto delle affermazioni che possono apparire un po' troppo kantiane. In particolare ho escluso che possa essere realizzato, sulla piattaforma PC IBM, un sistema operativo antivirus. Per supportare questa mia affermazione, e anche per soddisfare l'interesse e la curiosità di chi è un po' più addentro ai misteri della macchina, vorrei delineare quello che secondo me dovrebbe essere il progetto di un elaboratore a prova di virus.

*1. CPU a due stati*

Il presupposto di qualsiasi discorso di sicurezza dinamica consiste nella possibilità di distinguere tra le azioni condotte dal sistema operativo e quelle condotte da qualsiasi programma applicativo. La CPU dovrà essere in condizione di operare in stato privilegiato, nel quale accetterà di eseguire qualsiasi codice operativo, o in stato normale, nel quale rifiuterà di eseguire codici operativi che si riferiscono a operazioni sensibili o pericolose. La transizione dall'uno all'altro stato dovrà essere governata dal sistema operativo e non potrà mai essere ceduta a un applicativo.

*2. Specializzazione delle tipologie di file*

Nel concetto di protezione dai virus è implicito quello di protezione dei file eseguibili. Per ottenere una simile protezione è indispensabile una struttura estesa di attributi; il «tipo» di file non dovrà essere definito esclusivamente da una componente del nome (.COM, .EXE) ma da uno schema convenzionale di attributi. Questi ultimi dovranno essere sottratti al controllo diretto degli applicativi; ogni modifica agli attributi di un file dovrà essere soggetta all'approvazione del sistema operativo che dovrà valutare le circostanze.

*3. Esclusione di ogni operazione diretta sui file eseguibili*

In un sistema operativo protetto non deve essere ammessa alcuna operazione diretta sui file eseguibili tranne la creazione e la rimozione. In condizioni normali si tratta di un'operazione logica che non è mai necessaria, soprattutto in un contesto in cui la programmazione si svolge esclusivamente in linguaggi evoluti. E poiché non è necessaria non dovrà essere prevista (fanno eccezione le routine di modifica manuale del contenuto dei dischi, le quali tuttavia saranno per definizione sotto il controllo dell'utente, appunto in quanto manuali).

*4. Registri di sistema*

Ciascuna operazione di un certo tipo (es. creazione di file eseguibili) dovrà essere registrata di modo che l'utente possa seguire una traccia cronologica delle operazioni svolte.

Già una corretta attuazione di queste quattro indicazioni determinerebbe un sistema operativo in cui scrivere programmi autoreplicanti in grado di sfuggire a una pronta identificazione sarebbe estremamente problematico. E vorrei precisare che non ho inventato nulla di nuovo: ho tratto libera ispirazione dalla struttura di alcuni dei sistemi operativi previsti per i mainframe della serie 370 della IBM, con i quali in passato ho avuto una certa dimestichezza. Alcune specifiche progettuali di quei sistemi avrebbero potuto benissimo essere riportate sui personal computer, ed è un peccato che ciò non sia avvenuto dieci anni fa.

*Stefano Toria*

# Un po' di folklore locale?

Uno dei miei primi contributi alla rivista, quasi tre anni fa, consistette nella classificazione dei virus per paese di provenienza. Rifare oggi quel lavoro sarebbe un'impresa piuttosto difficile, perché all'epoca usciva qualche nuovo virus ogni mese mentre oggi ne escono oltre cento, e star dietro a tutti è praticamente impossibile. Dove è stato scritto il Girafe? O il Tremor? Dove hanno fatto la loro prima comparsa le ultime dieci varianti del solito Jerusalem? Ormai non gli si riesce più a star dietro.

Nonostante ciò siamo riusciti a mettere insieme una tavola dei virus che risultano essere stati scritti in Italia. La pubblichiamo più per curiosità che per effettiva utilità, anche se poi sembra che alcuni di questi virus abbiano avuto una certa diffusione locale.

| Pseudonimo | Città | Virus prodotti | Data |
|---|---|---|---|
| GROG | Bari | E-Riluttanza<br>Enmity v1.0<br>Lor<br>Grog v3.1<br>Nocciola | Mar.- Apr. '93 |
| The Invisible Man | Salerno | Invisible Man | Apr. '93 |
| Aragorn | Roma | Aragorn | Nov. '92 |
| Cracker Jack | Milano | Enigma<br>Necrop<br>Lucifer<br>BadGuy<br>Ah<br>Interceptor | Febr. '91<br>Magg. '91<br>Magg. '91<br>Magg. '91<br>Magg. '91<br>Sett. '91 |
| Amissi dee Panoce | Padova | Cossiga | ? '91 |

La maggior parte di questi virus è già nota ai più diffusi tra gli antivirus. Ce n'è uno in particolare del quale abbiamo avuto da pochi giorni un campione, e che abbiamo analizzato con molta attenzione perché si tratta di un prodotto piuttosto pericoloso. Si tratta del virus «Invisible Man», al quale abbiamo attribuito questo nome perché uno dei suoi effetti consiste nel far apparire sul video le prime due strofe dell'omonimo brano dei Queen. Il virus è pericoloso, come dicevamo, perché è multipartito, polimorfo e ha caratteristiche di stealth e tunneling. Sembra che sia stato speso diverso tempo nello scriverlo.

Ad ogni modo, poiché nel giro di pochi giorni ce ne sono arrivati almeno due diversi campioni tramite MC-link, riteniamo di mettere in guardia i lettori. Il virus può essere identificato servendosi delle funzioni di analisi euristica di F-PROT e di TBSCAN; forniamo inoltre le stringhe di identificazione di questo virus, utilizzabili con il VIRUSCAN di McAfee:

Per rilevare l'Invisible Man nei file:
"0E*(6)1F*(6)BB*(8)B9*(8)BA*(8)81C1*(8)3097*(8)43*(6)00F2*(6)E2*(7)E9"

Per rilevarlo nel Master Boot Record:
"B92D00*(6)36807439*(7)46*(6)E2*(7)EB"

Analisi e elaborazione a cura di Paolo Monti.

ratteristiche un antivirus è un prodotto che si spera che non serva mai a niente, ma quando svolge il proprio compito di evidenziare la presenza di un virus pone l'utente in una situazione scomodissima: dover valutare le misure da prendere riguardo a un fenomeno che non ha alcuna possibilità di valutare in prima persona.

È inevitabile che nella valutazione di un prodotto antivirus si tenga in considerazione la qualità dell'assistenza fornita dal produttore. Purtroppo dobbiamo rilevare la carenza del Microsoft Anti-Virus in questa direzione: né il manuale né i testi on-line riportano nominativi, indirizzi o telefoni a cui rivolgersi nel caso in cui si incontri un virus; e l'unica forma di assistenza consiste nel piano di aggiornamento delle firme dei virus.

Prescindiamo dalla considerazione che i prodotti antivirus più affermati e validi stanno via via abbandonando la tecnologia della ricerca di stringhe in favore di una più efficiente ricerca algoritmica. L'aggiornamento delle stringhe può essere richiesto per posta, sottoscrivendo un abbonamento a un piano di invio periodico di nuove firme, ovvero chiamando un BBS.

Quest'ultima forma di aggiornamento, che sarebbe senz'altro la più comoda, è ovviamente preclusa a chi non sia in possesso di un modem. Ma anche per chi lo possiede la vita non è resa più facile: l'unico numero telefonico disponibile è negli Stati Uniti, nell'area di prefisso 503. A questo numero, secondo il manuale, sarebbe collegato un sistema attivo 24 ore al giorno per 7 giorni alla settimana (ma quando abbiamo provato noi a chiamarlo squillava libero e non abbiamo ottenuto alcuna risposta). Francamente un solo numero, e negli Stati Uniti, per qualche milione di utenti potenziali in tutto il mondo sembra un po' pochino.

## *Conclusioni*

Ci è piaciuta l'idea che la Microsoft abbia preso coscienza del problema dei virus. A voler sparare veramente lontano, si potrebbe forse affermare che una tale diffusione dei virus è in parte «colpa» proprio della Microsoft, perché se il Dos fosse stato progettato in un altro modo... ma non amiamo molto ragionare con i «se», e questa presunta «colpa» è più un paradosso che qualcosa in cui crediamo veramente. I virus ci sono, e i responsabili dei virus sono i loro autori: e basta.

Ci è piaciuto un po' meno il modo in cui la Microsoft ha pensato di affrontare il problema dei virus. Da una casa con le dimensioni e le possibilità della Microsoft, e non ci riferiamo soltanto a possibilità economiche, ci saremmo aspettati un po' più di attenzione nella scelta del partner. Non tutti hanno la vocazione di scrivere software antivirus; è un'operazione noiosa, porta via un sacco di tempo per stare appresso a tutti i nuovi virus che escono ogni mese (siamo a quota centocinquanta) e richiede lunghe ore passate a disassemblare il lavoro di gente che spesso non sa nemmeno cosa voglia dire fare un buon programma Assembler. Non ci sorprende quindi il fatto che l'antivirus del Dos 6 non sia prodotto a casa Gates.

Ma proprio per questo avremmo apprezzato molto di più che la Microsoft si fosse scelta un partner in grado di confezionarle un prodotto di alta qualità, sia nel software vero e proprio che nella documentazione. Francamente dispiace vedere come una buona occasione sia stata sprecata: si poteva fare qualcosa per sensibilizzare veramente gli utenti alle necessità dell'informatica sicura, e invece ci si è limitati a mettere un cappello su una sedia per dire «ci siamo». Peccato. Sarà per la prossima volta (ma ci sarà, una prossima volta?).

MC

*Stefano Toria è raggiungibile tramite MC-link alla casella MC0170 tramite Internet all'indirizzo MC0170@mclink.it*