Come è fatto un programma antivirus

seconda parte

di Stefano Toria

Nello scorso numero abbiamo descritto il funzionamento del tipo più comune di programma antivirus, quello che esamina il disco alla ricerca delle impronte digitali dei virus. Proseguiamo questa analisi con uno sguardo alle caratteristiche dei programmi «da guardia», che combattono il rischio-virus tenendo d'occhio le funzioni pericolose. Daremo inoltre uno sguardo ai dispositivi hardware che svolgono funzioni antivirus

Una catastrofe annunciata (e mancata)

Mentre scrivo questo articolo (il 15 marzo) la polvere sembra essersi definitivamente assestata. Mi riferisco al nuvolone sollevato dal secondo cataclisma mondiale annunciato, o per essere più chiaro e comprensibile al virus Michelangelo. A un mese di distanza, cioè quando uscirà la rivista, i lettori non ne potranno più di sentirne parlare, o forse se ne saranno già completamente dimenticati. Mi rifiuto di pensare che uno solo dei lettori di MCmicrocomputer sia stato danneggiato da questo puerile e stupido virus; è la mia vanità che me lo fa ritenere, perché penso che tutti ovviamente mettano in pratica i miei consigli.

Nei giorni immediatamente precedenti il 6 marzo la mia scrivania si è progressivamente riempita di uno strato di comunicati di agenzia, provenienti dai quattro angoli del mondo, contenenti notizie, allarmi, timori, e soprattutto imprecisioni. Una soprattutto mi ha fatto particolarmente imbestialire: quasi tutti hanno scritto che il solo fatto di essere collegati a una rete di posta elettronica possa costituire causa di contagio. Al di là della falsità tecnica di questa affermazione, c'è la cattiva luce che viene gettata sui sistemi telematici di conferenza, che mi infastidisce particolarmente in quanto oltre a studiare i virus mi occupo del marketing di MC-link, la rivista telematica che i lettori di MCmicrocomputer conoscono ormai da anni grazie agli articoli di Corrado Giustozzi, e che in occasione del Grande Allarme del 6 marzo si è rivelata utilissima diffondendo informazioni corrette e precise (non mi sto facendo pubblicità gratuita: la conferenza sui virus è frequentata da tecnici di prima qualità).

In ogni caso, la stampa d'informazione e la televisione hanno fatto la massima confusione possibile; senza curarsi di informarsi meglio hanno messo insieme pezzi di informazione non necessariamente correlati, come nell'esempio che ho fatto qui sopra: il fatto che il virus si sia servito come veicolo dei dischetti che contenevano il programma «E-Mail» della DaVinci Systems ha fatto balzare alla conclusione che il virus era arrivato... «con la posta elettronica»; non del tutto errato ma nemmeno rigorosamente esatto.

A volte mi dico che bisogna rassegnarsi a una simile imprecisione nella stampa non specializzata, ma non riesco a convincermi del tutto; anche perché mi viene fatto di pensare che se trattano in questo modo un argomento che conosco bene, chissà quali e quante corbellerie mi vengono periodicamente rifilate su argomenti scientifici e tecnici che non sono in grado di controllare a fondo.

Tuttavia un servizio utile la stampa l'ha fatto: ha attirato l'attenzione del pubblico su una data pericolosa, e ha fatto fare qualche backup in più (che non fa mai male). Molti utenti di PC, preoccupati per il giorno del destino, si saranno informati meglio, attrezzati o rivolti a un esperto; e questo livello di attenzione al problema senz'altro non guasta, anche se rischia di restare episodico. Il risultato è stato tutto sommato positivo: ben lungi dal risultare una catastrofe, il venerdì 6 si è risolto in un piccolo fastidio; qualcuno avrà perso qualcosa, ma nel complesso il disastro non c'è stato. Contentissimi sono stati soprattutto i produttori di software antivirus, che hanno assistito a un incremento strepitoso delle loro vendite nei giorni precedenti il 6.

Ci sarebbe una considerazione da fare: cioè che l'attenzione del pubblico è stata attratta anche troppo sul fenomeno virus. In questo modo si rischia di dare eccessivo risalto a quello che è

soltanto uno degli aspetti del più vasto problema della sicurezza, e sul quale conto di dilungarmi prossimamente.

Uno strumento di protezione non sempre efficace

Nello scorso numero abbiamo visto come funziona un programma di ricerca di virus. Si tratta del tipo più comune di programmi antivirus, data la relativa facilità con cui può essere realizzato e mantenuto in costante aggiornamento. Tuttavia questo tipo di programmi soffre di una limitazione inerente: sono in grado di dare l'allarme esclusivamente sui virus conosciuti. E purtroppo non è detto che un virus conosciuto da qualcuno sia necessariamente noto a tutti gli sviluppatori di prodotti antivirus. In teoria tra i diversi gruppi di ricercatori c'è la massima cooperazione, e si mantengono in stretto contatto servendosi della posta elettronica; in pratica questo non è vero, e ne ho avuto personalmente le prove quando ho riscontrato, ultimamente, che un virus segnalato da quasi un anno dal «Virus Bulletin», la più autorevole pubblicazione internazionale sull'argomento, viene ignorato da alcuni tra i più noti programmi di ricerca di virus. Sembrerebbe di poter concludere che anche nel mondo degli antivirus valgono le regole della più accanita competizione commerciale. Che in questo caso si arricchirebbe di un elemento perverso: se ciascun prodotto fallisce l'identificazione di qualche virus, l'utente si troverebbe teoricamente costretto ad acquistarli e usarli sempre tutti. Su MC-link ci stiamo avviando a seguire questa strada, perché dobbiamo essere assolutamente sicuri di aver fatto tutto il possibile per evitare di diffondere virus con il software che mettiamo a disposizione dei nostri abbonati; spero di non dover arrivare a suggerire la stessa pratica anche ai lettori.

Come abbiamo visto lo scorso mese, la scansione funziona sia in fase preventiva (con l'analisi del contenuto di ciascun file alla ricerca di impronte di virus) che in fase operativa (con la stessa analisi compiuta su ciascun eseguibile nel momento in cui ne viene comandata l'esecuzione).

Il principio teorico di funzionamento di questo mezzo di difesa è semplice: se l'impronta corrisponde allora il programma in esame contiene il virus; il fatto viene segnalato all'utente che deciderà cosa farne, p.es. lo rimuoverà dal disco oppure lo consegnerà a un esperto per ulteriori analisi (sarà bene accertarsi che l'esperto sia veramente tale, dato il rischio insito nel far circolare programmi aggressori. La migliore pratica consiste sempre e comunque nel distruggere i virus, in ogni caso).

Ma non sempre la scansione è la migliore arma contro un virus. L'identificazione di un virus può portare a false sicurezze; ad esempio, l'utente che scoprisse di essere infetto da un virus della famiglia «1701» (conosciuto anche come «Cascade»; è il virus «dei caratteri che cadono») potrebbe concludere che si tratta di un virus innocuo e astenersi da ulteriori azioni; ma non tutte le varianti del «1701» sono innocue, ve ne sono anzi alcune che formattano il disco fisso.

Inoltre è sempre possibile che un virus venga modificato in modo da apparire identico al programma di scansione ma diverso nei suoi effetti, e ogni volta che mi è possibile cerco di risvegliare l'attenzione su questo fatto. Nulla vieta ad esempio che un hacker modifichi un «Den Zuko» in modo che invece di far apparire sul video la nota schermata grafica distrugga alcuni settori a caso sul disco fisso. L'utente che passa il suo antivirus e si ritrova il «Den Zuko» rimanda il lavoro di pulizia del disco, poi inavvertitamente riavvia il PC e si ritrova distrutta parte del proprio lavoro.

Infine c'è sempre il rischio di un virus effettivamente sconosciuto. Fino a qualche tempo fa ci ritenevamo lontani dai luoghi in cui ferve l'attività di sviluppo di virus: Europa orientale, Israele, Stati Uniti, Asia. Ma negli ultimi tempi c'è stato il boom della produzione nazionale (non che ne sentissimo il bisogno, in verità); e sono ben 21 i virus che Patricia Hoffman (v. riquadro) dichiara di origine italiana. A questo punto il rischio di contrarre un virus sconosciuto a tutti gli antivirus diviene elevato, e nessun programma di ricerca di impronte di virus potrà segnalarne la presenza.

Il cane da guardia

In queste situazioni l'utente dovrà valutare l'opportunità di affidarsi anche a un diverso tipo di strumenti di protezione: i programmi di monitoraggio delle funzioni pericolose.

Il principio di funzionamento di questi programmi è semplice: si basa sul fatto che qualsiasi aggressore debba servirsi di un'arma, nella fattispecie di una funzione del sistema operativo scelta tra un numero limitato e comunque identificabile con precisione; sarà sufficiente intercettare tutte le funzioni il cui utilizzo può influire sull'integrità del sistema, e controllare di volta in volta la legittimità del loro utilizzo.

La funzione che restituisce data e ora, ad esempio, oppure quella che fornisce il nome della directory corrente, non sono funzioni pericolose. Nessun programma potrà danneggiare l'integrità del PC che lo ospita semplicemente chiedendo l'ora.

La funzione che consente la formattazione di un disco è potenzialmente pericolosa. Lo sanno bene gli utenti che hanno formattato per errore un disco in luogo di un altro, e hanno distrutto dati o programmi essenziali.

Anche la funzione che richiede l'accesso a una rete locale è potenzialmente pericolosa, come quelle che agiscono sui dispositivi periferici, etc..

Il principio di funzionamento dei programmi di monitoraggio è di installare dei dispositivi di controllo che intercettino tutte le richieste di funzioni pericolose, verificandone — ove possibile — la legittimità e chiedendo conferma all'utente nei casi dubbi.

Questi dispositivi consistono nella maggior parte dei casi in piccoli programmi residenti, che si installano all'atto dell'esecuzione (tipicamente nell'ambito dell'AUTOEXEC.BAT) agganciandosi alle chiamate di sistema che possono essere utilizzate per accedere ai dischi: INT 26 per le funzioni di lettura/scrittura tramite DOS, INT 13 e INT 40 per gli accessi diretti al disco.

L'utente ha sempre la possibilità di scavalcare il controllo; ad esempio, dopo aver richiesto la formattazione di un dischetto non ha senso che venga segnalato il tentativo di esecuzione di un'istruzione pericolosa, perché l'utente lo sa da sé che la formattazione può distruggere dati; ma potrebbe essere ugualmente utile la segnalazione in quanto la funzione di formattazione potrebbe essere stata dirottata, all'insaputa dell'utente, verso un drive diverso da quello che lo stesso utente ha richiesto.

In occasione di una segnalazione l'utente dovrà aver preventivamente appreso come comportarsi; dovrà essere in grado cioè di comprendere se si tratta di un effettivo allarme o di una segnalazione ridondante. Dovrà quindi interrompere l'esecuzione del programma sospetto e verificare la effettiva sicurezza del programma.

Hardware antivirus

Tra coloro che si sono messi seriamente d'impegno a scrivere software antivirus, e coloro che si sono limitati a cavalcare la tigre, hanno trovato un proprio spazio i produttori di hardware antivirus. L'argomento utilizzato da costoro è semplice ma efficace: qualsiasi software antivirus si può infettare, aggirare, disattivare; l'hardware per definizione non si infetta, è difficile da aggirare e se opportunamente progettato entra in funzione prima ancora del BIOS previsto dal costruttore. Sembrerebbe il dispositivo di protezione ideale.

Nel giro di pochi mesi sono uscite sul mercato alcune schede antivirus, che si possono suddividere grosso modo nelle stesse due categorie in cui abbiamo ripartito il software: prodotti che scandiscono i dischi alla ricerca di firme, e prodotti che tengono d'occhio le funzioni pericolose segnalandole opportunamente all'utente.

La nostra opinione è che non si tratti di prodotti validi per un'ampia diffusione, sostanzialmente per due ragioni: innanzitutto qualsiasi prodotto hardware è più difficile da aggiornare rispetto a un software, e abbiamo visto come l'aggiornamento costante e tempestivo sia essenziale per una buona difesa dai programmi aggressori; inoltre questi di-

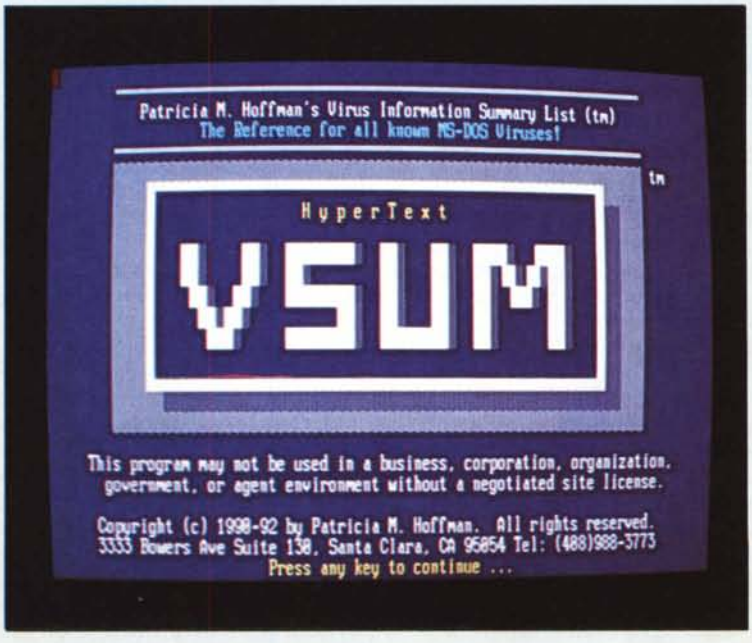
VSUM: un ipertesto tecnico sui virus

I virus conosciuti sono oltre 1.200 per il solo ambiente MS-DOS. Abbiamo ripetuto diverse volte che l'utente dovrebbe trattarli tutti allo stesso modo, cioè come potenziali distruttori, e sbarazzarsene quanto più presto e definitivamente possibile.

Ma l'esperto ha bisogno di avere maggiori informazioni su un virus, soprattutto quando viene chiamato ad intervenire in un ambiente in cui decine o centinaia di computer sono collegati in rete e le infezioni possono viaggiare a velocità considerevoli. In questi casi è indispensabile sapere con che genere di virus si ha a che fare, che effetti può produrre, e soprattutto qual è la condizione di attivazione. Un solo esempio basta a chiarire quest'ultimo punto: fino al 6 marzo chi sospettava di essere stato colpito dal Michelangelo è stato giustamente preoccupato per il rischio che correva di perdere il proprio lavoro; oggi il Michelangelo non fa più paura, perché si sa che c'è un periodo di tempo ragionevole per affrontarlo con calma, prima della prossima data di attivazione, il 6 marzo 1993. Ma se il virus fosse un Dark Avenger, che si attiva casualmente una volta su sedici, la procedura di emergenza sarebbe ben più urgente.

Tutte queste informazioni sui virus sono mantenute a cura di un gruppo di specialisti che fanno capo alla McAfee Associates, la società statunitense che prende il nome da uno dei massimi esperti tecnici sul fenomeno virus, e che produce quello che è tra i più diffusi programmi antivirus e cioè SCAN.

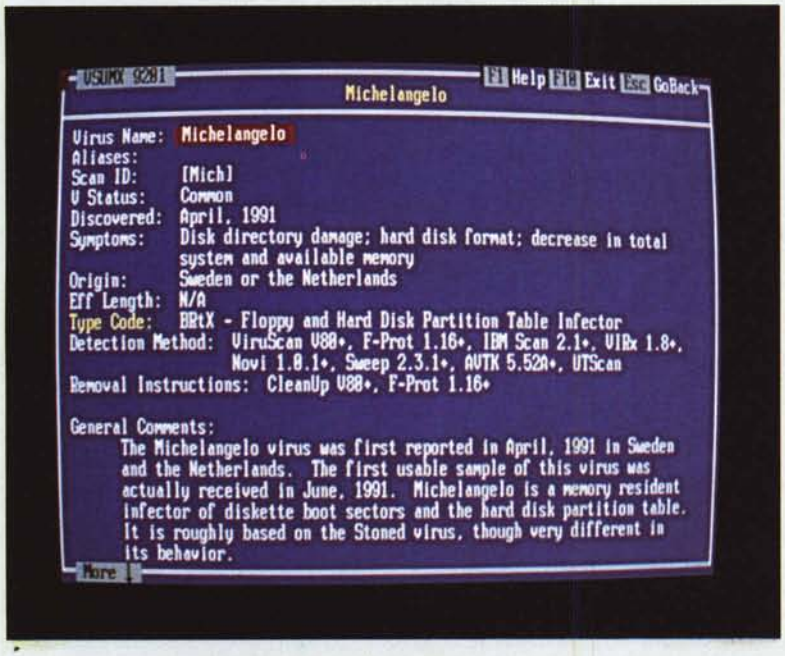
Il lavoro di costante aggiornamento sui nuovi virus, indispensabile per mantenere efficace SCAN, ha dato luogo a un utilissimo sottoprodotto: la lista VSUM. Curata da Patricia Hoffman, una collaboratrice di McAfee, la lista è nata inizialmente come lungo file di testo; successivamente, quando il numero di virus conosciuti si è ingigantito e si sono moltiplicati gli incroci di



La schermata introduttiva di VSUM.

spositivi possono essere installati soltanto su computer da tavolo dotati di slot di espansione, il che li taglia fuori dall'utilizzo da parte di quell'ampia parte dell'utenza informatica (compreso il sottoscritto) che si serve di laptop e notebook, che nella maggior parte dei casi non sono provvisti di slot di espansione, oppure ne sono dotati ma solo a condizione di servirsi di un box esterno, rendendo impossibile il controllo «al volo» di programmi eseguiti quando l'utente è fuori della propria sede: proprio quando invece ce ne potrebbe essere maggiormente bisogno.

Stefano Toria è raggiungibile tramite MC-link alla casella MC0170.



La scheda del "Michelangelo".

L'elenco dei virus di origine italiana secondo Patricia Hoffman.

referenze da un virus all'altro, il formato della lista è stato trasformato in un semplice ma efficiente ipertesto. Il programma è stato scritto appositamente per VSUM, senza servirsi di strumenti ipertestuali già disponibili.

Distribuito come «shareware», il programma si suddivide in quattro sezioni principali, corredate da alcune schermate informative sulle caratteristiche del programma, la cronologia delle successive versioni, le informazioni per la registrazione, etc.

Virus Index: i virus conosciuti sono elencati in ordine alfabetico. Ciascuna scheda informativa riporta il nome del virus, gli eventuali altri nomi con cui è conosciuto, il codice identificativo utilizzato da SCAN e CLEAN (es. [Jeru] per il Jerusalem, [170X] per il Cascade, etc.), la diffusione del virus, la data in cui è stato identificato o sottoposto ai ricercatori, i sintomi, il paese di origine, la lunghezza se si tratta di un parassita, la modalità di aggressione, il metodo di identificazione, le istruzioni per rimuoverlo e un commento discorsivo sulle caratteristiche del virus.

Relationship Chart: molti virus possono essere raggruppati in vere e proprie «famiglie». Queste informazioni, più utili a chi sviluppa programmi antivirus che al pubblico anche di tecnici, sono fornite in maniera più ampia e documentata nelle schede dei singoli virus; in questa sezione sono raffigurati gli alberi di parentela dei virus, utilizzabili con il sistema dell'ipertesto per scorrere le schede informative in ordine di parentela anziché alfabetico.

Cross Reference: consente di reperire la scheda informativa di un virus partendo da uno dei nomi con cui il virus è conosciuto.

Appendices: alcune funzioni secondarie sono raggruppate in questa sezione, e in particolare la ricerca delle schede informative per lunghezza del virus, per paese di origine, per data di attivazione e per tipologia di infezione; è riportato anche l'elenco dei virus più diffusi e un dizionario di conversione dalle denominazioni utilizzate dalla AVPD (Anti-Viral Product Developers) a quelle adottate nelle schede di VSUM.

VSUM
Virus Information Summary List
Patricia M. Hoffman
3333 Bowers Ave. Suite 130
Santa Clara, CA 95054
Tel. (408)988-3773
BBS: (408)244-0813
Costo shareware: $30 per un anno disponibile su MC-link all'uscita di ciascuna nuova versione