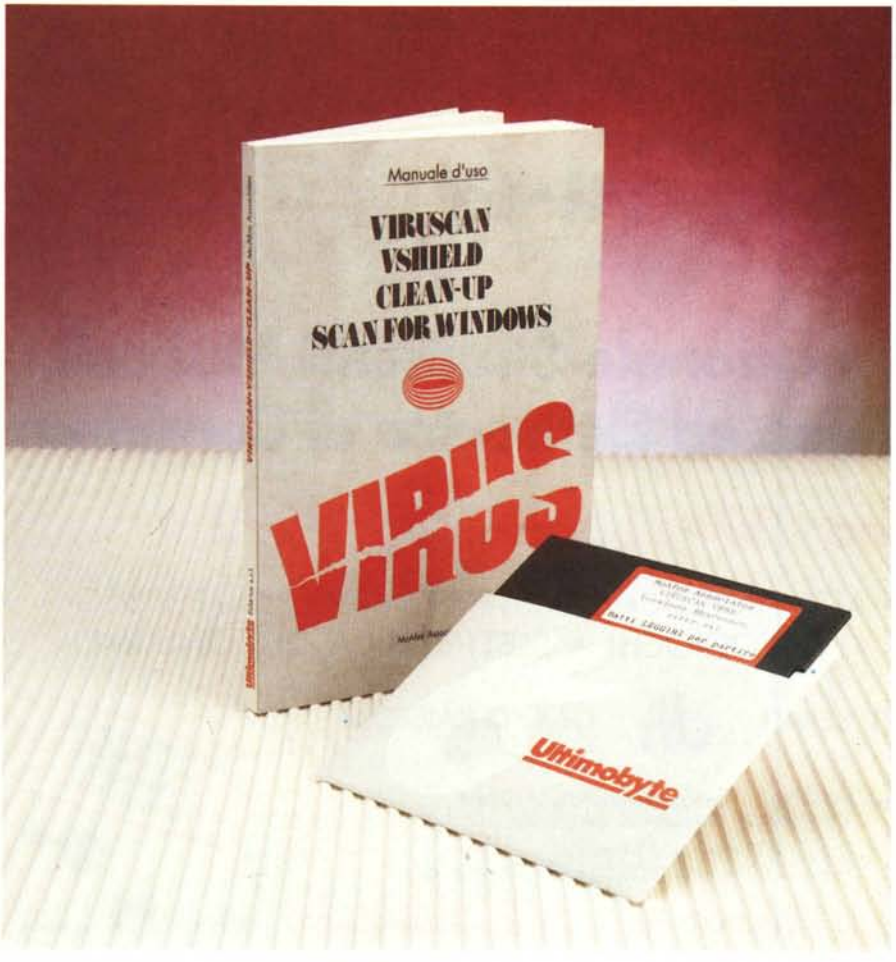
VIRUSCAN e i suoi colleghi

di Stefano Toria

Questo mese diamo uno sguardo al pacchetto antivirus che ha avuto il maggior successo; di fatto è in assoluto il secondo pacchetto shareware in termini di diffusione, subito dopo il PKZIP di Phil Katz. Stiamo parlando della serie di programmi antivirus di John McAfee, come i nostri lettori avranno certamente intuito: un punto di riferimento per chiunque si occupi di virus. Con qualche riserva, come vedremo



Componenti del prodotto

La versione 91, che viene recensita in questo articolo è stata prelevata personalmente dal sottoscritto dal BBS «The Homebase», il sistema telematico che la McAfee Associates mette a disposizione dei propri utenti e in genere di chiunque abbia bisogno di informazioni o di software specifico in materia di virus. Il prodotto che appare nella foto di apertura è quello che viene distribuito, completo di documentazione in italiano, dall'agente unico per l'Italia; peraltro il pacchetto è reperibile con la formula dello shareware (si è tenuti cioè a pagare il prezzo al produttore del software soltanto se lo si utilizza al di là dell'iniziale periodo di prova) praticamente su tutti i sistemi telematici: su MC-link curiamo di mantenere aggiornate le versioni dei cinque programmi di cui si compone il pacchetto.

Il distributore italiano fornisce il pacchetto in tre diversi formati: due versioni ad uso dei privati, rispettivamente l'una per DOS e l'altra per Windows; e una per aziende. Quest'ultima comprende anche le funzioni di scansione di server di rete locale, che non vengono distribuite ai privati.

Il software ci è pervenuto sotto forma appunto di cinque file archiviati con PKZIP. Ecco i nomi e le lunghezze dei file:

SCANV91.ZIP	129268
CLEAN91B.ZIP	141141
VSHLD91.ZIP	107574
WSCAN91.ZIP	182569
NETSC91B.ZIP	116543

Ciascuno dei cinque componenti svolge una funzione specifica, e in particolare:

— **SCAN** è il nucleo centrale del pacchetto; contiene le funzioni di analisi dei programmi eseguibili per la determinazione della presenza di virus. È in grado di determinare la presenza di virus conosciuti nelle seguenti aree di un PC: la memoria, il master boot sector, il boot sector di partizione, il boot sector di un dischetto, i file eseguibili sia su disco fisso che su dischetto; in mancanza di

VIRUSCAN

Produttore:
McAfee Associates, USA. BBS: (001) 408-988-4004
Agente esclusivo per l'Italia:
Ultimobyte Editrice s.r.l., Via Aldo Manuzio 15, 20124 Milano, tel. (02) 6555306
Prodotto reperibile tramite i normali canali dello shareware (su sistemi telematici nazionali ed esteri)
Prezzi di vendita ai privati *(IVA inclusa)*:
Versione per DOS
L. 98.000 + L. 6.000 per spese spedizione
Versione per Windows
L. 118.000 + L. 6.000 per spese spedizione
Prezzi di vendita alle società:
Sono disponibili condizioni particolari per licenze di gruppo, a prezzi che vanno dalle L. 250.000 per un massimo di 5 licenze fino a oltre L. 25.000.000 per 3.000 licenze. Telefonare al distributore per informazioni.

specifica da parte dell'utente vengono considerati eseguibili i file con estensioni .APP, .BIN, .COM, .EXE, .OV?, .PGM, .PIF, .PRG, .SWP, .SYS, e .XTP. SCAN funziona indifferentemente sia su un PC isolato che su un cliente di una rete locale; per la verifica del contenuto di un server va utilizzato NETSCAN (v. oltre).

— **WSCAN** consiste sostanzialmente in uno shell che consente di lanciare l'esecuzione di SCAN sotto Windows. Anziché dover ricordare ogni volta tutti gli switch necessari all'attivazione o disattivazione delle varie funzioni (scansione delle sotto-directory, della memoria, aggiunta o controllo dei codici di convalida, etc.) l'utente può specificarli mediante due comode dialog-box; il programma provvede a memorizzare le scelte dell'utente, in modo da eseguire le successive scansioni nelle stesse condizioni fino a diversa specifica dei parametri.

— **NETSCAN** è il programma di scansione da utilizzare per il controllo di server su una rete locale gestita da uno dei seguenti software di rete: 3Com 3/Share e 3/Open, Artisoft Lantastic, Novell NetWare, Banyan VINES, DEC DECNet, Microsoft LAN Manager, PC/SA, NFSNet e in genere qualunque software compatibile con IBMNET o NETBIOS. La documentazione suggerisce di rivolgersi direttamente alla McAfee Associates per informazioni sulla compatibilità di NETSCAN con altri software di rete.

— **VSHIELD** è un programma residente di controllo antivirus. Esegue sostanzialmente le stesse funzioni di SCAN, ma si attiva ogni volta che viene richiesto al DOS il caricamento e l'esecuzione di un file eseguibile. Se il file richiesto risulta infetto da un virus, l'esecuzione viene impedita e l'utente viene avvertito.

— **CLEAN** è il programma di riparazione dei guasti da infezione.

I cinque archivi sono strutturati più o meno allo stesso modo. Oltre al relativo eseguibile ciascun archivio contiene i seguenti file:

— una documentazione specifica per l'utilizzo del programma contenuto nell'archivio;

— il programma VALIDATE.COM che consente di verificare se l'eseguibile è giunto all'utente in condizioni integre, e la relativa documentazione;

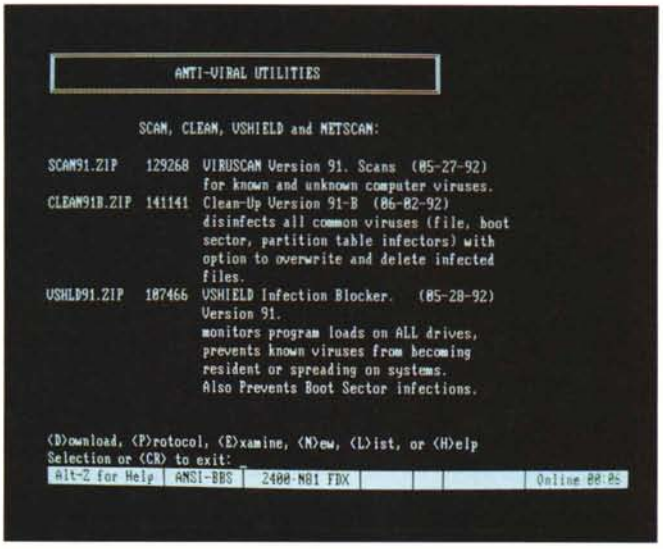
— un elenco dei rappresentanti della McAfee Associates in tutto il mondo;

— le istruzioni per la registrazione del programma direttamente presso la McAfee Associates;

— una tavola sinottica dei virus conosciuti, con la descrizione codificata delle caratteristiche di ciascuno di essi;

— un'offerta di abbonamento a CompuServe del valore di $15, per l'accesso al VIRUSFORUM gestito dalla McAfee Associates.

«The Homebase», il BBS della McAfee Associates.



Installazione e primo uso

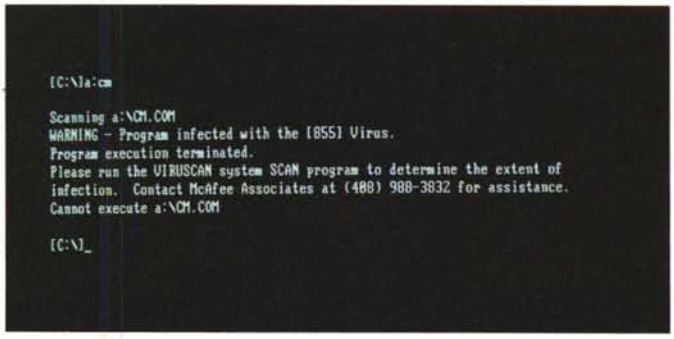
L'installazione dei programmi consiste semplicemente nell'estrazione dei file da ciascun archivio. Se lo desidera, l'utente può creare una directory specifica per ciascuno dei programmi, ma non è indispensabile.

La documentazione, scritta in inglese, è chiara e concisa. A differenza di altri prodotti, che abbiamo già presentato o presenteremo ai lettori di MCmicrocomputer, le istruzioni di uso dei programmi non si dilungano nello spiegare all'utente cosa sia un virus o come ci si debba comportare in caso di contaminazione. John McAfee infatti ha destinato sin dall'inizio i propri programmi al circuito dello shareware, il cui bacino di utenza è costituito da persone che presumibilmente sono già a conoscenza delle nozioni fondamentali sui virus, o sono in grado di ottenerle altrimenti. Inoltre lo shareware viene spesso prelevato da sistemi telematici; poiché in questo caso l'utente deve sopportare i costi telefonici di prelievo dei programmi, è opportuno che questi siano ridotti al minimo indispensabile, lasciando da parte le documentazioni aggiuntive che possono essere prelevate separatamente da chi le desideri. Coerentemente con questa impostazione, infatti, il BBS di McAfee offre una vasta gamma di testi illustrativi e didattici sulla natura dei virus e sul comportamento da tenere in presenza di una infezione.

Peraltro la documentazione fornisce alcune indicazioni indispensabili, come ad esempio il suggerimento di eseguire qualsiasi funzione connessa ai virus soltanto dopo aver spento il computer e averlo riacceso avviando il sistema da un dischetto integro.

L'uso di SCAN è semplicissimo: basta dare il comando SCAN C: e il programma parte con le opzioni di default. Già se eseguito in questo modo è in grado di scoprire la presenza di eventuali infezioni.

Naturalmente è opportuno seguire l'indicazione che abbiamo sempre dato



Un virus intercettato da VSHIELD.

ogni volta che se ne presentava l'occasione, e almeno la prima volta far partire SCAN soltanto dopo aver avviato il DOS da un dischetto di sistema certamente privo di infezioni.

Le funzioni dei programmi

In questa descrizione, per comodità, tratteremo il solo SCAN, con l'avvertenza che quanto detto vale anche (salvo diversa specifica) sia per NETSCAN che per WSCAN. Quest'ultimo in particolare non è che uno shell per l'esecuzione di SCAN, e pertanto l'unica differenza tra i due sta nel modo di specificare le opzioni: con degli switch sulla linea di comando per SCAN, con delle selezioni in una dialog-box per WSCAN.

Come abbiamo detto, SCAN è in grado di scoprire la presenza di tutti i virus conosciuti dal gruppo di ricerca della McAfee Associates alla data di rilascio del programma, cioè al 27 maggio 1992. Si tratta di 586 differenti ceppi virali, per un totale di 1.302 varianti diverse.

Questo numero comprende sia virus parassiti, che si trasmettono cioè servendosi di file eseguibili, sia virus che si avvalgono di un boot sector per la propagazione (NETSCAN non esegue il controllo del boot sector).

La scoperta della presenza dei virus viene effettuata servendosi delle «firme» dei virus. Abbiamo già trattato questo argomento, e in parte vi accenniamo in un riquadro in questo stesso articolo. È evidente che l'affidabilità di un programma di scansione dipende dalla qualità del lavoro effettuato per l'identificazione delle «firme». Sotto questo punto di vista SCAN non sembra particolarmente attendibile: infatti versioni successive dello stesso prodotto danno luogo a una diversa identificazione dello stesso virus nello stesso, identico file.

La documentazione di SCAN afferma che il prodotto è in grado di scoprire anche la presenza di virus sconosciuti. Ciò è vero in parte, o meglio è vero sotto particolari condizioni. Il programma offre infatti la possibilità di appendere a ciascun file eseguibile un codice di convalida, che esso stesso può controllare in un secondo tempo. Se il valore calcolato all'atto del controllo differisce da quello archiviato nel file, è da sospettare l'azione di un virus che abbia modificato il file in cui risulta la discrepanza. Lo stesso lavoro può essere fatto sul

Scoperta e identificazione

Nello scorso numero abbiamo descritto le procedure di riparazione del danno causato dalla propagazione di un virus. Continueremo a ripetere fino alla nausea che la riparazione è sempre un'alternativa di ripiego, da utilizzare soltanto quando sia assolutamente impossibile ripristinare i programmi infetti prelevandoli da una copia originale, ma tuttavia sia altrettanto assolutamente indispensabile continuare a utilizzarli. Abbiamo già fatto alcuni esempi di casi in cui si verifichi una condizione di questo genere: tipico il caso di un'azienda che si serva di programmi amministrativi (contabilità, fatturazione, magazzino, etc.) sviluppati ad hoc da una software house non più reperibile, e che siano stati consegnati installandoli direttamente nei computer dell'azienda, senza che ne venisse consegnata anche una copia originale su dischetto. Se un programma di questo genere si dovesse infettare, l'unica via praticabile è la disinfezione.

Abbiamo visto come questa sia una pratica dall'esito variabile, dato che sostanzialmente dipende dalla natura del virus responsabile dell'infezione. Se si viene colpiti da un virus che «si comporta bene», eseguendo la procedura di infezione in modo reversibile, non ci sono particolari problemi; se per contro il virus in cui si incappa esegue delle modifiche irreversibili, allora non c'è modo di riportare i programmi allo stato precedente l'infezione.

Il presupposto della corretta disinfezione è quindi la corretta identificazione del virus. Nello scorso numero abbiamo soltanto accennato a questo problema, che vogliamo ora approfondire.

Ceppi e varianti

Chiunque abbia una minima dimestichezza con la denominazione dei virus (basta aver dato una scorsa alla documentazione che accompagna qualsiasi software antivirus) saprà che di alcuni virus esistono diverse varianti. Alcuni tra i più diffusi hanno anche alcune decine di varianti: Jerusalem, Vienna, Cascade, Stoned.

Come nasce una variante? Sostanzialmente ad opera di un ignoto hacker che desidera sviluppare un virus ma non possiede la sufficiente esperienza di programmazione in Assembler. Costui non farà altro che procurarsi un virus esistente e gli apporterà qualche piccola modifica, in modo da generare un nuovo virus. Particolarmente popolari sono le modifiche che determinano una variazione nell'azione del virus una volta che si innesca la condizione; ad esempio non è molto difficile modificare un virus che scrive qualcosa sul video, ottenendo che anziché scrivere sul video vada a sporcare il disco fisso. Lo abbiamo ripetuto innumerevoli volte, precisando anche che per questo motivo non ci si può permettere di sottovalutare un'infezione da un qualsiasi virus, anche se risulta all'apparenza un virus non aggressivo.

Il nostro hacker quindi rimedierà un virus già scritto, e non è molto difficile procurarsi una copia di 170X o di Ping-Pong, data l'enorme diffusione di questi virus. Servendosi di strumenti di analisi alla portata di tutti (quasi sempre il DEBUG) andrà a dare un'occhiata all'interno del virus, identificherà un punto in cui sia possibile fare una modifica senza scomporre troppo il resto del codice, farà la modifica e poi cercherà di diffondere la sua «creatura», esattamente come se si trattasse di un nuovo virus.

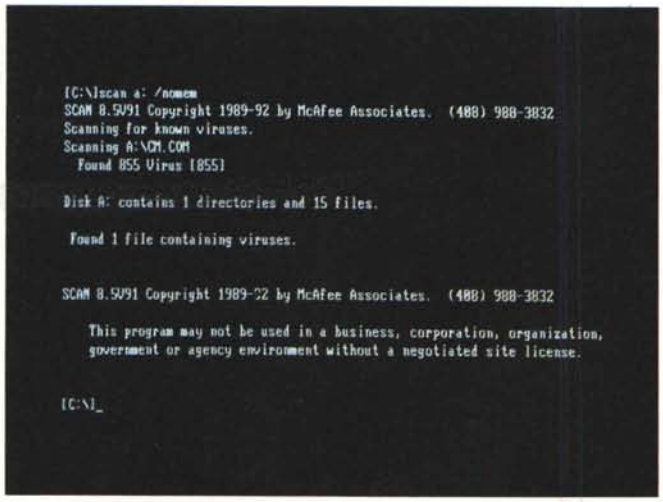
Il nuovo virus, che in realtà sarà relativamente «nuovo», sarà molto simile a quello da cui è stato ottenuto, ma non perfettamente identico. Magari l'ignoto hacker anziché modificare il virus con il DEBUG potrà disassemblarlo e quindi riassemblarlo dopo aver aggiunto alcune istruzioni; in questo caso, se si tratta di un virus che si trasmette accodandosi ai programmi eseguibili, sarà variata anche la lunghezza del codice che viene aggiunto in coda al programma vittima dell'infezione. Celebre fra tutti il caso del virus Cascade, che si chiama anche 170X perché in origine ne esisteva una variante da 1701 byte e una da 1704.

Alcuni hacker sono così maliziosi da scegliere, come bersaglio delle proprie modifiche, quelle parti del virus che sono state scelte da qualche ricercatore come «impronta digitale» del virus, e che consentono ai programmi antivirus di identificare il tipo di virus. E qui entriamo nel cuore dell'argomento di questo mese.

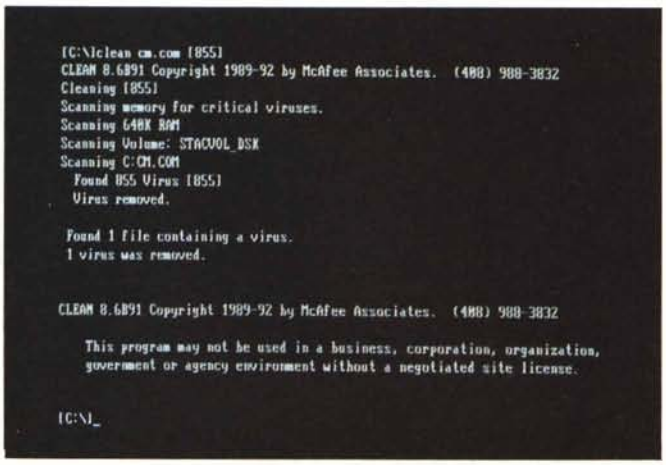
Scoperta dell'infezione

Accorgersi che un programma è stato infettato non è particolarmente difficile. In molti casi è sufficiente listare la directory in cui si trova il programma e confrontare la lunghezza del file eseguibile con il valore originario di tale lunghezza; se si riscontra una variazione, ecco scoperto un caso di infezione. Purtroppo non è possibile affidarsi completamente a una tecnica così elementare; chi ci segue assiduamente sa infatti che esistono i virus nascosti, i virus gemelli e comunque una serie di virus che non modificano la lunghezza del programma vittima, o che mimetizzano l'eventuale variazione di lunghezza.

Esistono almeno due diversi metodi per determinare con certezza se un dato programma sia stato infettato o meno. Il primo fa uso di un sistema di controllo dell'integrità; ne abbiamo parlato e non ripeteremo quanto abbiamo già detto, accennando soltanto al fatto che il controllo dell'integrità consiste nel confrontare un valore di riferimento (es. un CRC) calcolato sulla sequenza di byte che compone il programma eseguibile subito dopo la sua installazione con lo stesso valore calcolato dopo una sospetta infezione; se i valori differiscono bisogna approfondire il motivo di tale differenza, essendo probabile che si sia verificata un'infezione.



SCAN segnala la presenza del virus...



...e CLEAN lo rimuove.

Requisito essenziale per potersi servire di questo metodo è l'aver installato il sistema di controllo dell'integrità prima che l'infezione si sia verificata. In mancanza di questo requisito si potrà utilizzare il secondo metodo, cioè l'uso di un programma di scansione di virus. È in questo contesto che diventa rilevante la differenza tra scoperta e identificazione del virus.

L'uso delle «firme»

I programmi di scansione si servono di particolari sequenze di byte dette «firme» o «impronte digitali» per stabilire se il codice oggetto contenuto in un programma eseguibile consista in uno dei virus conosciuti. Ciascun produttore di software antivirus mantiene una propria collezione di virus, e si serve dell'opera di persone specializzate nel disassemblare virus per isolare la «firma» di ciascun nuovo virus che entra a far parte della collezione.

È qui che si «pare la nobilitate» di un programma, o per meglio dire del suo produttore. Tanto più abile e precisa è l'opera dei ricercatori nell'estrarre una «firma» che consenta di identificare con assoluta certezza il virus distinguendolo da eventuali varianti, tanto più affidabile e preciso sarà il risultato del programma, non tanto nell'accorgersi della presenza di un'infezione quanto nello stabilire con estrema precisione la variante del virus responsabile dell'infezione stessa, e conseguentemente la corretta procedura da seguire per la disinfezione. Ciascun ricercatore infatti giungerà a risultati diversi nella ricerca di una «firma», basandosi sulla propria esperienza, sulle conoscenze e sulle informazioni che ha a disposizione. Due diversi programmi antivirus possono quindi identificare lo stesso virus in maniere diverse, e ne abbiamo avuto personalmente la prova quando un lettore ci ha inviato tramite MC-link un programma infettato dal virus 855, nel quale aveva modificato le istruzioni che danno luogo all'esecuzione del virus, segnalandoci le modifiche effettuate. Questo programma, sottoposto all'esame da parte di due diversi programmi di scansione, risultava infetto a uno dei due e sano all'altro. Dopo aver ripristinato le istruzioni modificate dal lettore rimettendole come le aveva lasciate il virus, entrambi i programmi identificavano il virus contenuto nel programma. Questo significa che i due programmi fanno uso di due diverse «firme» per l'identificazione del virus 855; una delle due contiene le istruzioni che il nostro lettore ha modificato, l'altra invece è prelevata da una diversa porzione del virus.

L'obiettivo della precisione assoluta non è tanto rilevante se l'utente è in grado di sostituire i programmi infetti con le copie originali: in questo caso sarà sufficiente anche un'identificazione rozza e imprecisa. Il problema assume rilievo se l'utente non è in grado di rimpiazzare i programmi infetti ed è costretto a ricorrere ai servizi di disinfezione del software antivirus. La riparazione del danno in alcuni casi può dare esiti peggiori dell'infezione, se viene eseguita senza tenere conto delle eventuali differenze nella procedura di infezione seguita da diverse varianti dello stesso virus. E abbiamo visto come, trattando di virus, sia prudente comportarsi come se «in alcuni casi» voglia dire «sempre».

La raccomandazione quindi è che se proprio non si può fare a meno di disinfettare i programmi colpiti, almeno si scelga il pacchetto antivirus che fornisce la massima garanzia di corretta identificazione delle varianti. L'utenza specializzata ha a disposizione diversi strumenti per compiere correttamente la scelta del migliore software antivirus; agli utenti normali suggeriamo di rivolgersi a un consulente che garantisca affidabilità e competenza. Approfondiremo questo argomento in un prossimo articolo.

Stefano Toria

partition boot record e sul master boot record.

È evidente come questa funzione possa essere utilizzata soltanto se vengono preventivamente installati i codici di convalida negli eseguibili presenti sul proprio PC.

Una funzione tecnicamente interessante consiste nella possibilità di installare, in ciascun file eseguibile, le informazioni per la disinfezione. Qualora questa funzione venga utilizzata, in caso di infezione il file potrà essere ripristinato con maggiore sicurezza da parte di CLEAN (v. più avanti).

La funzione di determinazione e controllo dei codici di convalida e ripristino, già presente nelle precedenti versioni del programma, è stata ulteriormente migliorata consentendo all'utente di scegliere di archiviare i codici in un file esterno, senza appesantire né modificare gli eseguibili. Infatti il codice di convalida aggiunge 10 byte a ciascun eseguibile, e le informazioni di convalida e ripristino ne aggiungono 54. Inoltre l'aver estratto tali informazioni dai file costituisce una ulteriore misura di sicurezza, in quanto un ipotetico sviluppatore di virus (categoria che, come è ormai noto, ne sa una più del diavolo) potrebbe deliberatamente modificare i dati di convalida generati da SCAN in modo da far apparire intatto un file che in realtà è stato modificato. Archiviando i codici in un file esterno su dischetto, invece, l'utente può conservare i dati di convalida su un supporto sicuro, che al limite potrebbe essere lo stesso dischetto con il sistema operativo «certamente pulito» da utilizzare per i periodici controlli antivirus.

Sempre con riferimento ai virus sconosciuti, SCAN è in grado di ravvisare all'interno dei due boot record la presenza di sequenze di istruzioni sospet-

te; in questo caso verrà segnalato un virus definito «Generic Boot Sector» o «Generic MBR».

Tra le funzioni avanzate di SCAN sono da segnalare la possibilità di utilizzare un file esterno di «firme», funzione utile a chi dovesse scoprire un nuovo virus e intendesse servirsi di SCAN per isolarne tutte le replicazioni; la disponibilità di un log della singola sessione di scansione oppure di un log incrementale per mantenere la storia dei controlli effettuati; e la possibilità di controllare le date di esecuzione delle scansioni.

VSHIELD è disponibile in due versioni, che differiscono tra di loro nei requisiti di occupazione di memoria. Rammentiamo infatti che VSHIELD è la controparte residente di SCAN, che deve contenere al minimo indispensabile lo spazio di memoria occupato per non sottrarre RAM ai programmi applicativi.

La differenza tra le due versioni, VSHIELD e VSHIELD1, è sostanziale. VSHIELD esegue i controlli servendosi dello stesso database di «firme» utilizzato da SCAN. Se caricato normalmente occupa circa 37Kb; se viene attivata la funzione di trasferimento su disco nei periodi di inattività l'occupazione scende a circa 3Kb, mentre se viene caricato in memoria alta l'occupazione è minima: 416 byte. VSHIELD1 per contro occupa sempre uno spazio fisso pari a 6Kb, e per i controlli richiede che sia stato preventivamente applicato ai file eseguibili il codice di convalida, mediante l'apposita funzione di SCAN.

VSHIELD è corredato di un programma, CHKSHLD, che ne verifica la presenza in memoria; la documentazione ne consiglia l'uso preferibilmente su stazioni collegate in rete locale, piuttosto che su PC stand-alone. È presente nella documentazione anche un esempio di login script per Novell Netware, mediante il quale il supervisore di rete può imporre il caricamento di VSHIELD su tutti i PC al momento in cui accedono alla rete.

La riparazione del danno

Infine, CLEAN è la funzione di disinfezione dei programmi infetti. Oltre alle funzioni essenziali svolte da SCAN, limitatamente alla scansione dei file eseguibili, CLEAN tenta anche di eseguire al contrario le azioni che sono state attuate dal virus al momento dell'infezione. In molti casi questa operazione è possibile e consente di ripristinare il file colpito allo stato in cui si trovava prima dell'infezione. Quando il ripristino non è possibile, CLEAN segnala il fatto all'utente e gli offre la possibilità di rimuovere permanentemente il file infetto.

Le prove dei prodotti antivirus vengono effettuate in redazione su un PC Unibit 286 a 12 MHz con 640Kb di RAM, scheda Hercules e video monocromatico, disk controller ST-506, disco fisso Seagate da 60Mb e drive per floppy da 3,5" 1.44Mb.

Sul disco fisso sono installati i seguenti virus (il numero tra parentesi indica il numero di campioni differenti per i virus di cui sono presenti più copie e/o varianti):

512, 855, 1244, 1381, 1554, 4096, AIDS, AIDS-II, Alabama, Ambulance, Amoeba (2), Anarkia, Anthrax, Anti-Pascal (2), Anti-Pascal II (3), Attention, Bebe, Burger (3), Cascade, Crash, Dark Avenger (2), Darth Vader (3), Datacrime (2), Datacrime-2, Destructor, Devil's Dance, Fish 6, Flip, Fu Manchu, Icelandic (2), Invader, Jerusalem, JoJo, JoJo-2, June 16th, JW2, Kennedy, Leprosy, Liberty, Lisbon (2), Lozinsky, Murphy, Nomenklatura, Ontario, Oropax, Plague, Pogue, Polish 529, Saturday 14th, September 18th, Smack, Stupid, Suomi, Suriv-A, Sverdlov, Taiwan (3), Taiwan-3, Traceback, Typo-712, USSR-600, V801 (2), Victor, Violator, Old Yankee Doodle.

La collezione sperimentale di MCmicrocomputer, utilizzata per questa prova, contiene inoltre tre virus da boot sector: Stoned, Ping-Pong e Michelangelo.

La documentazione afferma che CLEAN è in grado di rimuovere anche virus sconosciuti, purché gli eseguibili colpiti dal virus siano stati preventivamente corredati delle informazioni indispensabili alla disinfezione. Abbiamo sperimentato questa funzione servendoci di un virus che ci è stato inviato qualche tempo fa in redazione e che certamente non è conosciuto ad altri ricercatori, anche perché lo abbiamo conservato (con la massima cautela) proprio per poter eseguire controlli di questo genere. Si tratta di un virus piuttosto «pulito», che si trasmette agli eseguibili .COM lasciando le cose ben in ordine. CLEAN non ha avuto problemi nel rimuovere questo virus, ripristinando il file nello stato in cui si trovava prima dell'infezione.

Teniamo tuttavia a mettere i lettori in guardia contro i facili ottimismi: non tutti i virus si comportano così «educatamente» come il nostro, anzi è molto più probabile inciampare in virus ben più agguerriti, che modificano in modo irreversibile il file che scelgono come bersaglio dell'infezione.

Le prestazioni

Da quando il fenomeno dei virus si è affermato come argomento di interesse generale, non più limitato ai laboratori di ricerca specializzata, John McAfee si è conquistato il titolo di «guru» dei virus, e i suoi programmi la fama di completa affidabilità. Confermano questa situazione anche i milioni di copie di VIRUSCAN diffuse in tutto il mondo.

Negli ultimi tempi, tuttavia, negli ambienti specialistici cominciavano a circolare notizie sempre più insistenti su una pretesa ridotta affidabilità di SCAN. Il fatto non deve sorprendere: mantenere perfettamente efficace ed efficiente un programma di scansione di virus non è cosa semplice, soprattutto al crescere del numero di virus in circolazione. Far coesistere la precisione di identificazione, la velocità di esecuzione e il basso costo è praticamente impossibile: lo abbiamo già fatto presente dalle righe di questa rubrica e abbiamo già ipotizzato alcune clamorose uscite dal mercato, sulle quali anche cominciano a circolare voci.

Ad ogni modo abbiamo voluto verificare personalmente l'attendibilità di tali voci. Abbiamo quindi predisposto il consueto test con la collezione ridotta già utilizzata nello scorso numero, ma con alcune minori variazioni. Si tratta di 77 campioni diversi di file infetti, in cui sono presenti diverse varianti degli stessi virus e/o diverse replicazioni della stessa variante.

Dell'identità dei virus siamo certi: li abbiamo analizzati personalmente e confrontati anche con le indicazioni fornite da altri due centri di ricerca; tutte le identificazioni di ceppo e variante concordano pienamente tra di loro.

Il test di corrispondenza ha fornito risultati modesti: VIRUSCAN ha identificato correttamente soltanto 43 file, pari al 55,8%; altri 19 (il 24,7%) sono stati identificati genericamente come appartenenti al proprio ceppo ma senza precisazione della variante, mentre dei rimanenti 15 (19,5%) l'identificazione era imprecisa in alcuni casi, totalmente errata in altri e in un caso veniva considerato sano un file in realtà infetto dal virus «September 18th».

Pertanto SCAN risulta uno strumento efficace per scoprire la presenza di virus in un sistema, ma non per identificare correttamente il virus responsabile dell'infezione. Abbiamo visto già nel numero scorso come la corretta identificazione di un virus sia il requisito essenziale per una corretta disinfezione.

I risultati confermano la convinzione che più volte abbiamo espresso: cioè che non ci si debba mai affidare, per quanto possibile, a un software per la rimozione del virus, ma si dovrà ricorrere sempre alle copie originali, eliminando completamente le copie infette e sostituendole con una nuova installazione: MC

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

L'ESTATE COMPUTER

CON I NOSTRI PREZZI NON C'E' BISOGNO DI RINUNCIARE ALLA VACANZA PER ACQUISTARE UN COMPUTER

286/27L dx 699000
386/33L sx 847000
386/33L dx 947000
386/40/71L cache 997000
486/99L SX 1047000
486/33/170 CACHE 1549000

1MB RAM+HD 45 MB+DRIVE (1,44-1,2)+S.VGA COLORE +2 SERIALI+PARALL.+JOY+ TASTIERA 102 TASTI+MOUSE TRE TASTI+CABINET+DOS 5 + MANUALI ITALIANO

MONITOR

MONOCROMATICO VGA L 179000
VGA COLORE 14 POLLICI L 389000
MULTISCAN 1024X768 L 489000
1280X1024 17P 0,26 L 1499000

Amiga 600 1.3 garanzia commodore, 3 manuali in italiano, +mouse+joystick.
L. 569.000

GVP•POINT
Schede accelleratrici, hard disk, accessori, ultime novità

Notebook CHAPLET 386/25 sx, hd 60, 2 mb ram, drive 1,44 mouse tre tasti completo di borsa.
L. 2.249.0000

48 ORE DI PROVA PRIMA DELLA CONSEGNA, ASSISTENZA IN SEDE GRATUITA IN 15 MINUTI.

VENDITA RATEALE DA 6 A 48 MESI SENZA ACCONTO SENZA CAMBIALI.

STAMPANTI

STAR LC 20 80 COL 180CPS	L289000
STAR LC 24/20 24A 216 CPS	L399000
STAR LC 200 COLORI 222C	L359000
STAR INKJET	L459000
NEC P20 24 AGHI 80 Col. 216cps	L499000
NEC P30 24 AGHI 136Col. 216cps	L729000
HP LASERJET II P PLUS	L1299000
LC 24/200 COLOR 24A. 222C	L580000

ACCESSORI

SCANNER GENIUS OCR	L199.000
SCANNER COLORI GENIUS	L549.000
SOUND BLASTER VER. 2.0	L219.000
SOUND BLASTER PRO	L349.000
MIDI PER SOUND BLAST	L 49.000
MODEM 2400 BAUD VTEL	L149.000
MODEM FAX EST MOFAX	L299.000
TAVOLETTA GRAF.12X12	L279.000

In Via GUIDO CASTELNUOVO 33
(Ponte Marconi)
00146 Roma
Tel. 06/5566219
Tel. 06/5592835
Fax. 06/5594161

computerage

Tutti i giorni dal lunedì al venerdì
dalle 9:30 alle13:00-15:30 alle 19:00

I PREZZI SONO AL NETTO D'IVA