Dr. Solomon's Anti-Virus Toolkit

di Stefano Toria

Dopo averlo più volte... «minacciato», diamo l'avvio con questo numero alle prove di alcuni tra i più diffusi prodotti antivirus. Il prodotto che abbiamo scelto per la prima recensione porta un nome blasonato: quello del Dr. Alan Solomon che è uno tra i più preparati tra coloro che combattono in prima linea la battaglia contro i virus

Il materiale

Il Toolkit viene fornito in una scatola che contiene il manuale in inglese, i dischi nei due formati (uno da 720K e due da 360K) e un ulteriore dischetto da 720K con la versione aggiornata all'ultimo momento. E proprio di «ultimo momento» sembra trattarsi, dato che i file contenuti in questo dischetto recano la data del 22 aprile, cioè pochi giorni prima che il materiale ci venisse inviato in redazione per la prova. Questo è un dato senz'altro positivo, in special modo per un software che serve a combattere un fenomeno che muta ogni giorno come quello dei virus.

Molto correttamente, il software viene distribuito su dischetti non utilizzabili per la scrittura. I due dischi da 5,25" sono privi di tacca, mentre al dischetto da 3,5" è stato rimosso lo sportellino che chiude la finestrella di protezione contro la scrittura (vedi foto di apertura). In questo modo è praticamente impossibile andare a scrivere sui dischi, e pertanto l'utente può stare certo di avere sempre a disposizione una copia originale del software, al riparo da qualsiasi attacco di virus.

(Ovviamente rimane sempre possibile scrivere su questi dischi, intagliando la tacca con una lametta sui dischi da 5,25" o chiudendo la finestrella con del nastro isolante su quelli da 3,5"; ma l'utente che faccia una cosa simile poi non può certo lamentarsi del proprio destino se si ritrova infettato).

Ci sarebbe piaciuto che anche il dischetto di aggiornamento fosse arrivato senza lo sportellino; confidiamo che l'importatore recepisca il suggerimento

e che i prossimi aggiornamenti del software siano distribuiti su dischetti non scrivibili.

Il pacchetto è completato da un volume separato che contiene il manuale in italiano, tradotto dall'importatore Siosistemi. Le ragioni per cui si è scelto di fornire le due versioni del manuale appaiono chiare esaminandone la suddivisione in capitoli. I primi due contengono rispettivamente una introduzione e le istruzioni per installare e configurare il programma; sono seguiti da un breve «trattato» sui virus del computer, piuttosto ben realizzato, chiaro e conciso, senza alcuna concessione al sensazionale. In questo capitolo, come d'altra parte nel resto del manuale, viene mantenuta una costante enfasi sulla necessità di evitare il panico in situazioni critiche.

Il capitolo 4 consiste in un voluminoso elenco dei principali virus conosciuti, che nella versione inglese occupa ben 252 pagine, e che la Siosistemi ha scelto di non tradurre in italiano. A nostro avviso si tratta di una scelta corretta, perché l'utente medio quasi certamente non avrà mai la necessità di conoscere nei dettagli il funzionamento di questo o di quell'altro virus, mentre lo specialista sarà senz'altro in grado di leggere la documentazione tecnica in lingua inglese, senza contare il fatto che esistono raccolte di informazioni tecniche ben più approfondite di questo manuale.

Traducendo i soli capitoli indispensabili per l'utilizzo del prodotto si è ottenuto invece un manuale snello e facile da aggiornare. I due capitoli successivi riportano rispettivamente una descrizione dettagliata di ciascuno dei programmi che compongono il Toolkit e un altro breve trattato sulla prevenzione dei virus, nello stesso stile del precedente.

Gli ultimi due capitoli contengono informazioni di carattere organizzativo e commerciale.

Il manuale nella versione inglese ci è piaciuto; di facile lettura, senza chiassosi allarmi o statistiche poco credibili, è un punto di riferimento per l'informazione sui virus. La versione italiana soffre dei problemi di traduzione che si riscontrano purtroppo molto spesso, e se il contenuto è identico a quello dell'originale non si può dire lo stesso per lo stile e la grafica, e soprattutto per la comprensibilità. In alcuni casi abbiamo dovuto consultare la versione inglese per chiarire alcuni punti che risultavano oscuri nella traduzione.

Installazione e primo uso

L'installazione dei programmi non comporta alcuna particolare difficoltà:

Dr. Solomon's Anti-Virus Toolkit

Produttore:
S&S International Ltd., Uk
Distributore:
Siosistemi s.r.l., Via Cefalonia 58, 25124 Brescia. Tel. (030)2421074
Prezzi *(IVA esclusa)*:
Toolkit completo
L. 250.000 (con aggiornamenti trimestrali)
VirusGuard
L. 150.000 (con aggiornamenti mensili)
FindVirus
L. 150.000 (con aggiornamenti mensili)
VirusGuard+FindVirus
L. 200.000 (con aggiornamenti mensili)

basta inserire il dischetto, attivare il drive, scrivere install e premere invio. All'utente viene chiesto di prendere poche semplicissime decisioni: in quale directory installare il programma, e se debba essere inserito nell'autoexec.bat il programma di sorveglianza antivirus.

Il dischetto di aggiornamento sostituisce interamente l'originale, e va utilizzato in sostituzione di esso. Questo fatto non è riportato da nessuna parte, ma si deduce logicamente esaminando il contenuto dei dischetti.

Ad ogni modo l'installazione consiste semplicemente nel trasferimento nella directory specificata dei file che compongono il pacchetto, e nell'eventuale aggiornamento dell'autoexec.bat con la chiamata al programma di sorveglianza. Ha funzionato senza particolari problemi sia sul PC di prova installato in redazione (v. riquadro), sia su una macchina un po' più... complessa, cioè un notebook 386sx con QEMM 6.0+, Stacker, e per di più eseguendo i programmi sotto Windows.

Le componenti del programma

Il toolkit si compone di ben sedici funzioni diverse, gestite da un'interfaccia con menu a tendina piuttosto semplice da utilizzare, con semplici comandi da tastiera o con il mouse. Per ciascuna funzione l'utente deve compilare un modulo con le opzioni desiderate; premendo F10 viene avviata l'esecuzione del programma richiesto.

È possibile eseguire anche i singoli programmi sotto forma di comandi DOS; in questo caso l'utente deve specificare tutti i parametri che sarebbero stati contenuti nel relativo modulo nel sistema a menu, e pertanto questa possibilità è quasi esclusivamente riservata all'utilizzo in ambiente batch, ad esempio per un controllo all'avvio del sistema inserendo l'opportuna istruzione in autoexec.bat.

Per contro non è consigliabile l'utilizzo dei programmi dalla riga di comando in modo interattivo, poiché in questa modalità l'interfaccia non brilla per chiarezza e coerenza.

La funzione centrale del pacchetto è quella denominata «FINDVIRUS». Come il nome suggerisce, si tratta di un programma di ricerca di firme. Nonostante le riserve che abbiamo più volte espresso riguardo ai programmi di ricerca di firme, riteniamo che si tratti di una funzione comunque indispensabile, per il semplice motivo che la maggior parte delle infezioni segnalate provengono da un gruppo limitato di virus e pertanto un buon programma di scansione è in grado di compiere un'opera preventiva che, pur non garantendo il 100% della protezione, riduce comunque il rischio in modo apprezzabile.

FINDVIRUS è uno scanner rapido ed efficiente. Non crediamo che la qualità

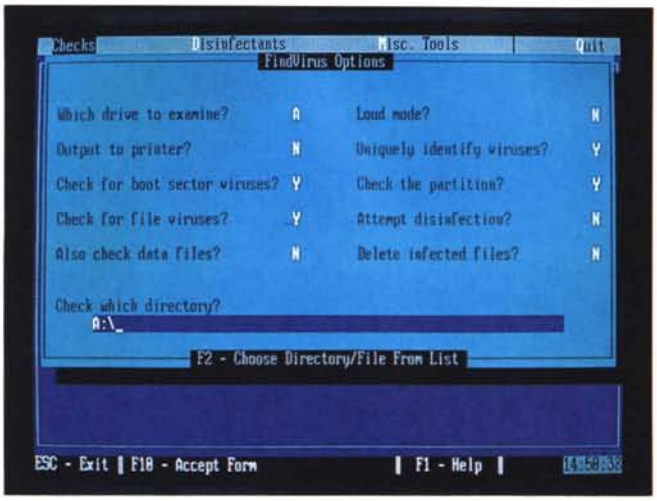
L'ambiente di prova

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

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

512, 855, 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, RMIT, Saturday 14th, Smack, Stupid, Suomi, Suriv-A, Sverdlov, Taiwan (2), Taiwan-3, Traceback, Typo-712, USSR-2144, USSR-600, V2P2, V801, Victor, Violator, Yankee Doodle.

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



Il modulo delle opzioni di FINDVIRUS.

di un antivirus possa essere misurata semplicemente con una prova al cronometro, ma in ogni caso questo programma ha dimostrato delle prestazioni soddisfacenti: oltre 80 Mb sono stati esaminati in poco più di un minuto sul notebook, e sul PC in redazione il controllo di una decina di Mb (tra cui si trovavano oltre settanta programmi infetti) è stato completato in meno di mezzo minuto. Anche la scansione di un dischetto è un'operazione che si conclude in una manciata di secondi.

Abbiamo verificato il funzionamento di FINDVIRUS sulla collezione sperimentale di virus di MCmicrocomputer. Essa consiste attualmente in 76 diversi file che rappresentano 65 diversi virus parassiti, cioè che si trasmettono servendosi di file eseguibili come mezzo di diffusione. In aggiunta abbiamo tre dischetti che contengono altrettanti virus da boot sector: Stoned, Ping-Pong e Michelangelo. FINDVIRUS ha identificato correttamente tutti i virus; sebbene la denominazione utilizzata da Alan Solomon differisca in alcuni casi da quella adottata da altri ricercatori (John McAfee, il gruppo del Virus Bulletin) l'importante è che il programma sappia bene con quali virus ha a che fare. Abbiamo già accennato a questo requisito, e ne parliamo più diffusamente in un altro riquadro.

CHECKVIRUS è una funzione di verifica di integrità dei file eseguibili. Il principio di funzionamento di questo programma è del tutto analogo a quello di altri integrity checker: viene calcolato un valore numerico che è funzione del contenuto di ciascun file eseguibile, secondo una formula che permette di ottenere valori sensibilmente diversi anche in presenza di piccole variazioni dei file; se a un successivo controllo, effettuato rieseguendo il calcolo e confrontando il risultato ottenuto con quello precedentemente archiviato, si riscontrasse una differenza, l'utente verrebbe avvertito della possibilità che il file eseguibile sia stato contaminato da un virus.

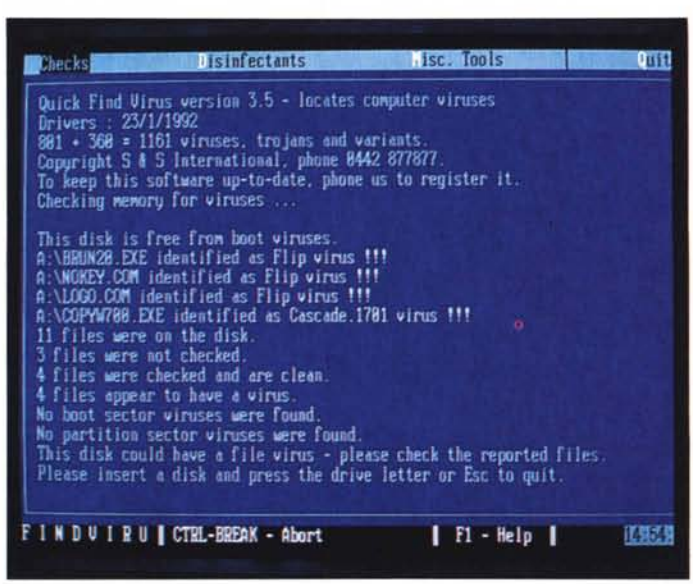
È un controllo piuttosto elementare e non efficiente al 100%, che non tiene conto ad esempio dell'esistenza dei virus «gemelli» («companion virus» in inglese), cioè di quei virus che in presenza di un file .EXE creano un file invisibile con lo stesso nome ma con l'estensione .COM, in modo che il DOS esegua quest'ultimo anziché il corrispondente .EXE.

Non è utilizzabile da solo come misura antivirus, ma presenta tuttavia alcune caratteristiche interessanti, come ad esempio la possibilità di archiviare il file con i valori di controllo su un dischetto da tenere fuori del PC, in modo da evitare che i valori di controllo vengano alterati da un programma aggressore.

Un'altra particolarità che ha attratto la nostra attenzione consiste nella possibilità di specificare il nome di un file che contiene la lista dei file eseguibili da controllare. In questo modo l'utente ha il pieno controllo sui file da verificare, la qual cosa rende il sistema utilizzabile con successo anche in situazioni di grande mobilità dei file eseguibili come ad esempio gli ambienti di sviluppo di software. Un programmatore potrà quindi includere nella lista dei file da verificare tutto ciò che è stabile, e quindi editor, compilatori, link editor, programmi di utilità e componenti del sistema operativo, escludendone i programmi compilati da lui stesso, i quali variando di volta in volta potrebbero generare regolarmente falsi allarmi.

QCV (che sta per Quick Check Virus) è una funzione analoga a CHECKVIRUS, con la differenza che non vengono calcolati e archiviati dei valori di controllo per i file ma semplicemente la lunghezza di ciascun file. Questo è un metodo piuttosto sbrigativo per verificare l'eventuale presenza di un virus, basato sull'assunto che un virus parassita modifichi la lunghezza degli eseguibili a cui si attacca. È un assunto inesatto, perché esistono alcuni virus che mascherano la propria presenza conservando una copia dell'originale di ciò che hanno modificato; quando un programma antivirus va ad esaminare i file in cerca delle tracce dell'infezione il virus, presente in memoria, fornisce al programma i dati originali, così da far ritenere che non vi siano state modifiche, mentre in realtà i programmi sono stati modificati.

Esistono inoltre alcuni virus (p.es. il



FINDVIRUS ha identificato alcuni file infetti.

Lehigh) che non modificano affatto la lunghezza dei file eseguibili, ma si vanno ad inserire nei programmi sfruttando spazi non utilizzati.

VIRUSGUARD è la funzione di sorveglianza a cui abbiamo accennato in precedenza. Caricato residente nei 640K o in memoria espansa, a scelta dell'utente, sovrintende alle operazioni di caricamento ed esecuzione dei programmi, interrompendole nel caso in cui il programma da eseguire risulti infettato da uno dei virus riconosciuti dal programma stesso.

In questo non differisce dagli analoghi programmi residenti di controllo, già da tempo disponibili sul mercato. Ciò che rende VIRUSGUARD diverso dagli altri è il fatto che il controllo viene effettuato sui file eseguibili anche all'atto di una semplice lettura. Copiare un file infetto da un dischetto al disco fisso, ad esempio, diviene impossibile perché VIRUSGUARD segnala la presenza del virus e rende impossibile la lettura del file infetto.

Quando viene riscontrata un'infezione appare sul video una finestra in sovrimpressione, con le opportune segnalazioni. L'utente ha la possibilità di personalizzare questa finestra, ad esempio inserendo direttamente il nominativo e il numero telefonico della persona da chiamare in questi casi di emergenza. Un'azienda potrebbe fornire in questo modo ai propri dipendenti direttamente il nominativo del responsabile per la sicurezza informatica, addetto a gestire le emergenze da virus.

Una volta scattato l'allarme l'utente ha la possibilità di concludere il lavoro che stava svolgendo, salvando eventualmente i file, prima di spegnere il PC e intraprendere l'azione di emergenza. Anche in questo caso la documentazione è molto corretta, e sottolinea la necessità di ripartire servendosi di un dischetto DOS privo di infezioni prima di eseguire i controlli.

Sul PC della redazione VIRUSGUARD ha identificato correttamente i virus di cui si è tentata l'esecuzione. Sul notebook non c'è stato verso di risolvere una incompatibilità tra lo stesso VIRUSGUARD e QEMM, sebbene l'installazione sia stata effettuata seguendo le specifiche istruzioni contenute nella documentazione.

Una particolarità di VIRUSGUARD è il fatto di poter verificare a priori se un dischetto è accettabile o meno, servendosi di un codice di autorizzazione che un'altra funzione del Toolkit si occupa di inserire. AUTHOR consente di registrare su ciascun dischetto un codice di otto caratteri, che viene controllato da VIRUSGUARD al primo accesso al dischetto. Se un particolare dischetto è privo di codice o ne riporta uno differente da quello con cui è stato avviato VIRUSGUARD su quel dato computer, ne viene impedito l'utilizzo.

CHECKVIRUS segnala delle anomalie su un eseguibile.

La riparazione del danno

Alcune delle funzioni del Toolkit consentono di ripristinare allo stato primitivo ciò che è stato alterato da un'infezione.

Abbiamo scritto più volte che in linea di principio siamo contrari a questa pratica; tuttavia un approccio realistico al problema dei virus porta a constatare che in molti casi gli utenti non hanno a disposizione gli originali dei programmi che utilizzano quotidianamente, e pertanto può essere indispensabile tentarne un salvataggio, ancorché si tratti di una pratica pericolosa.

Una funzione di ripristino è insita nello stesso FINDVIRUS. Se viene rilevata la presenza di un virus FINDVIRUS è in grado di rimuovere l'infezione — sempre che ciò sia possibile, ovvero sempre che l'infezione sia derivata da un virus che non determina un danno irreversibile.

UNVIRUS consente la riparazione di dischetti colpiti da virus da boot sector, ripristinandoli allo stato iniziale.

Due ulteriori funzioni, CLEANBOOT e CLEANPART, si occupano di virus da boot sector o da master boot record. CLEANBOOT può essere utilizzata per «ripulire» il boot sector di un dischetto, mediante la sovrapposizione di un boot sector valido. Non è possibile utilizzare questa funzione per ottenere un dischetto di sistema utilizzabile; tuttavia si può essere certi che dopo CLEANBOOT un dischetto di dati sarà privo di infezioni.

CLEANPART offre alcune fondamentali funzioni per la gestione della sicurezza relativamente al master boot record. L'utente ha la possibilità di rimuovere un'infezione determinata da uno di quei virus, come ad es. lo Stoned, che modificano il primo settore fisico del disco; inoltre è possibile utilizzare CLEANPART per archiviare su dischetto una copia dei dati della CMOS, del master boot record e del record di boot della partizione principale, in modo da essere in grado di ripartire anche dopo che sia stato danneggiato uno di questi elementi vitali per il funzionamento del sistema.

Due funzioni di servizio, NOFLOPPY e NOHARD, consentono di controllare l'accesso rispettivamente al drive del floppy disk e al disco fisso, impedendo la lettura e/o la scrittura.

Una funzione piuttosto curiosa è RUN.

Si tratta di un programma-kamikaze, che viene utilizzato per lanciare l'esecuzione di altri programmi in modo che un eventuale virus infetti lo stesso RUN e non il programma che viene eseguito.

Non abbiamo condotto specifiche prove in merito, ma riteniamo che sia una funzione facilmente aggirabile da parte di un autore di virus sufficientemente smaliziato; pertanto non è di per sé da considerare misura di sicurezza. Gli stessi sviluppatori sembrano condividere questa opinione, e il manuale è onesto ed esplicito in proposito.

SHRED consente di distruggere un file, rendendone impossibile la riattivazione.

Completano il Toolkit alcune funzioni riservate agli utenti più esperti: CHECKMEM per esaminare il contenuto della memoria, PEEKA per esaminare il contenuto del disco; e due programmi di utilità generale, TKBATCH che contiene delle funzioni utili nei file batch e

BROWSER che consente di scorrere file di testo.

Conclusioni

Si tratta di un sistema di programmi studiati con cura, per un campo di applicazione in cui più che la presentazione o l'interfaccia vanno curate l'efficacia e l'efficienza.

Il Toolkit tuttavia è abbastanza soddisfacente anche sotto il profilo della presentazione: documentazione curata e interfaccia gradevole, unitamente a una costruzione robusta, a una notevole precisione e alla contemporanea disponibilità di scanner e integrity checker ne fanno un sistema adatto ad essere utilizzato sia dal privato sia soprattutto da ambienti lavorativi in cui la protezione di un patrimonio informativo distribuito su più personal computer sia elemento essenziale nella strategia aziendale. MC

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

La riparazione del danno

Quando un virus attacca un file eseguibile segue una procedura che generalmente è riconducibile a quattro distinte fasi. Esaminiamole in dettaglio.

1. Identificazione della vittima

La prima operazione svolta dal virus consiste nello stabilire quale sia il programma da infettare. (Ricordiamo che stiamo parlando di virus che attaccano file eseguibili e non virus da boot sector nei quali, per definizione, la fase di identificazione non esiste). Può trattarsi del programma di cui l'utente ha chiesto l'esecuzione, oppure di un programma scelto a caso nella directory corrente ovvero lungo il PATH. In ogni caso il virus ottiene il nome di un programma in cui replicarsi.

2. Replicazione

Una volta identificata la vittima il programma aggressore fa una copia di se stesso nel programma vittima. È qui che si determina la possibilità, o la impossibilità, di ripristinare il programma vittima al proprio stato originale. Alcuni virus sono scritti con cura, e badano bene a non andare a sovrapporsi a nessuna area vitale del programma. Si tratta di quei virus che spesso causano l'aumento della lunghezza del programma eseguibile, oppure che vanno ad installarsi in una parte del file eseguibile che contiene uno spazio lasciato disponibile per essere utilizzato dal programma stesso una volta che ne viene avviata l'esecuzione.

Altri virus sono scritti in modo più trascurato, oppure deliberatamente in modo da danneggiare il file eseguibile di cui si servono per la trasmissione. In questi casi il ripristino dell'eseguibile allo stato originario può risultare impossibile.

3. Aggancio

Dopo che il virus si è installato nel programma vittima dovrà modificare quest'ultimo in modo che quando esso verrà eseguito come prima cosa venga eseguito il corpo del virus anziché il programma stesso. Pertanto il virus, al termine dell'installazione, procederà a identificare il punto di accesso al programma (l'«entry point») e a modificare le cose in modo che le prime istruzioni eseguite siano nel corpo del virus, e che al termine dell'esecuzione del virus il controllo del PC passi alla prima istruzione del programma vittima. L'utente in questo modo non si accorgerà di nulla perché il programma vittima verrà sempre e comunque eseguito.

Anche in questa fase al virus si offrono notevoli possibilità di compiere danni irreversibili. Tuttavia molti virus lasciano il file vittima in uno stato tale per cui è comunque possibile ripristinarlo allo stato originario.

4. Esecuzione

Dopo aver terminato la replicazione il virus passa il controllo al programma che lo conteneva. La nuova infezione è completa, e un altro file eseguibile contiene ora una copia del virus.

La riparazione

Disfare il lavoro fatto da un virus non è mai né complesso né lungo. Se si conosce bene il meccanismo dell'infezione è spesso sufficiente rimettere al proprio posto le istruzioni iniziali del programma (sapendo dove andarle a riprendere, là dove il virus le ha nascoste), ripristinare l'entry point e troncare il file eseguibile.

Sono queste le funzioni svolte dai programmi di riparazione: lo stesso FINDVIRUS per il Dr. Solomon's Anti-Virus Toolkit ma anche CLEAN di McAfee, VIRex della Microcom, e molti altri.

Il problema nasce con quei virus che si comportano in modo sporco. In questi casi rimettere le cose a posto risulta impossibile, e l'utente apprezzerà la saggezza del consiglio di tenere sempre a disposizione una copia originale e intatta del software installato sul computer.

Un caso particolare: i virus «gemelli»

Abbiamo accennato nel testo ai virus gemelli. Poiché non ne abbiamo mai parlato prima, conviene spendere due righe sull'argomento.

L'interprete dei comandi al DOS, COMMAND.COM, segue una precisa logica nell'interpretare i comandi. Quando l'utente scrive qualcosa per prima cosa il comando viene scisso in argomenti; il primo argomento viene poi utilizzato per stabilire cosa va fatto.

Tralasciando i dettagli, viene un momento in cui il DOS si mette a cercare sui dischi per prelevare un file contenente istruzioni eseguibili, file che abbia il nome corrispondente all'argomento specificato dall'utente. Nella sequenza di ricerca, supponendo che l'utente abbia dato il comando AVVIA, il DOS cercherà per primo AVVIA.COM e lo caricherà in memoria per l'esecuzione. Nel caso in cui non riesca a trovare questo file allora cercherà AVVIA.EXE sempre per eseguirlo.

Qualora siano presenti entrambi i file, verrà sempre e comunque eseguito soltanto il primo dei due. (Naturalmente l'utente ha modo di scegliere, specificando esplicitamente un'estensione per stabilire quale dei due voglia eseguire).

Questo meccanismo viene sfruttato da alcuni virus particolarmente «delicati». Sono pochissimi i virus di questo tipo di cui siamo a conoscenza; uno di essi, il Globe, è stato identificato grazie alla segnalazione di un abbonato di MC-link. Un virus gemello consiste in un breve file di tipo .COM il quale, quando viene eseguito, va alla ricerca di un file .EXE a cui non corrisponda un file con estensione .COM; una volta trovata la sua vittima, il virus si trascrive in un file con lo stesso nome della vittima e con estensione .COM, a cui provvede a impostare l'attributo di file nascosto, in modo che il file non appaia quando l'utente lista la directory. Il file .COM si conclude con una chiamata all'altro file, quello con lo stesso nome e l'estensione .EXE.

Una successiva esecuzione del programma vittima determina per prima l'esecuzione del virus, il quale provvede a replicarsi nuovamente prima di dar luogo all'esecuzione del programma effettivo, e così via.

In questi casi la disinfezione è semplicissima: è sufficiente rimuovere il file nascosto con l'estensione .COM, eventualmente servendosi di una utility per la visualizzazione dei file nascosti.

Stefano Toria

IL N°1 NEGLI U.S.A. ORA ANCHE IN ITALIA

CH products

I RIVENDITORI CH

PIEMONTE
ALEX COMPUTER
C.so Francia 333/4
Via Tripoli 169/B - TO
COMPUTER HOME
Via San Donato 46/D - TO
EUROCOM
Corso Francia 283/A - TO
IL COMPUTER SERVICE
Via Stradella 235/A - TO
AGARTHI
Via Montegrappa 112
Rivoli - TO
COMPUTER WORK
Via Rivoli 38/A
Orbassano - TO
PC
Via Guasco 54 - AL

LIGURIA
ELITE COMPUTER
Via Orsini 31/R - GE
PAGLIALUNGA SDF
Via Vico Liceri 6
Rapallo - GE

LOMBARDIA
ALCOR
Via P. Sarpi 7
Viale Gran Sasso 50
Viale Biggy 22 - MI
FLOPPERIA
Via Monte Nero 15 - MI
L'UFFICIO 2000 SRL
Via Ripamonti 213 - MI
NEWEL SRL
Via Mac Mahon 75 - MI
SUPERGAMES
Via Vitruvio 37 - MI
IL CURSORE DI NEGRI
P.zza Martiri della Liberta 7
Novate Milanese - MI
BIT LINE SAS
Via Corridoni 35 - Rho - MI
PENATI
Via Simone 49/D
Corbetta - MI
B&B COMPUTER SRL
Via Gaddini 6 - Gallarate - VA
LECCOLIBRI
Via Cairoli 46 - Lecco - CO
ELTRONGROS SPA
Via Leonardo Da Vinci 54
Barzanò - CO
VIDEO IMMAGINE
Via Bernocchi 11/3
Villa Carcina - BS
MEDIA MARKET
Via Fermi 1 - Curno - BS

VENETO
BIT SHOP
Via Daniele Manin 43 - PD
COMPUMANIA SRL
Via Carlo Leoni 32 - PD
COMPUTER POINT
Via Roma 83 - PD
GIANFRANCO MARCATO
presso "Centro Giotto"
Via Venezia 61 - PD
MEGABYTE 3 SRL
Piazza San Tomaso 10/11 - VR

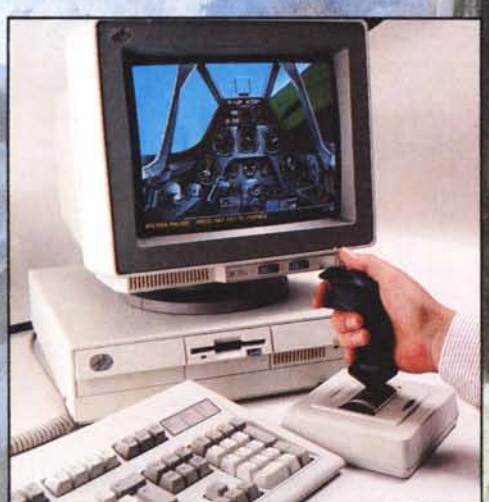
TRENTINO ALTO ADIGE
MUSIC CENTRE
Via Sopramassso 32/4
Gandolo - TN

EMILIA ROMAGNA
BOLOGNA INFORMATICA SAS
Viale Lenin 45/B - BO
GRANDE EMPORIO
STERLINO
Via Murri 73/D
Via Lombardi 43 - BO
ORSA MAGGIORE
Centro Commerciale
"I Portali"
Piazza Matteotti 20 - MO
ARGNANI
Piazza della Liberta 5/A
Faenza - RA
L'ASTEROIDE
di BOCCALI PAOLO
Via Cavour 155/A
Cesena - FO
GEMINI INFORMATICA SAS
Via Durante 6 - PC
CENTRO OFFICE
Via Lazzaretti 5/A - RE

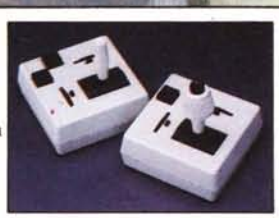
MARCHE
COMPUTER HOME
di MANNA RITA
sede di Fano
Via Garibaldi 108
sede di Pesaro
Via Vanzolini 7

LAZIO
COMPUTEL
Via Ettore Rolli 33 - Roma
D&D
Via Lungo Tevere
dei Mellini 38 - Roma
ELETTRONICA MILAZZO
Viale Nobiltore 16/22
Roma
METRO IMPORT
Via Donatello 37 - Roma

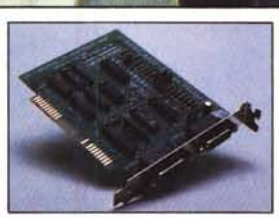
SICILIA
E.L.S.E.
Via Umberto 96
S.P. Clarenza - CT
HOME COMPUTER
Via delle Alpi 50 F - PA



MACH I
MACH I PLUS
- Nuovo design
- Elevate prestazioni
- Due pulsanti fire
- Funziona con migliaia di programmi



ROLLERMOUSE
- Mouse più veloce e più preciso
- Design esclusivo a 4 pulsanti
- Funzione di selezione e bloccaggio
- Compatibile mouse Microsoft
- Modelli: Serial, Bus, PS/2, Mac e Amiga



GAMECARD III AUTO
- Con regolazione automatica della velocità da 4,77 Mhz a 33 Mhz
- Velocità programmabile
- Due porte joystick
- Software in italiano per il test e la calibratura
- Modelli PC e Microchannel

MACH II/III
- Durata 100 volte superiore rispetto ai normali joystick
- Altissima precisione
- Grande affidabilità

FLIGHTSTICK
- Impugnatura sagomata: si ha la sensazione di impugnare una vera cloche
- Capacità grafica, può essere usato con CAD ed applicazioni grafiche
- Controllo assoluto, permette un controllo a 360 gradi del cursore
- Potenziometri lineari di lunga durata

DISTRIBUZIONE ESCLUSIVA
CTO