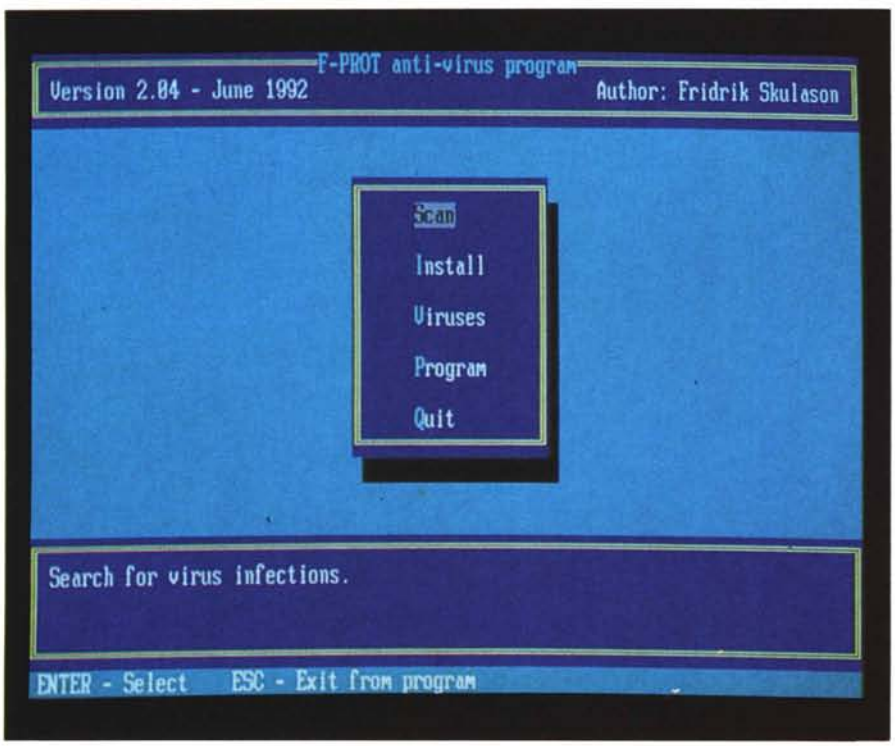
L'antivirus che viene dal freddo

di Stefano Toria



Anche in questo numero presentiamo un prodotto antivirus, e anche stavolta si tratta di un prodotto shareware. Ma il basso costo (il protagonista di questo mese è addirittura gratuito per chi ne fa uso privato, non professionale) non è sinonimo di bassa qualità: anzi, tutt'altro

Fuori dai circuiti internazionali

L'Islanda per il grande pubblico è un paese semisconosciuto. Se si eccettua il nostro Enrico Ferrari, che è innamorato di qualsiasi zona della Terra che abbia una temperatura media prossima allo zero, ben pochi possono affermare di conoscerla; negli ultimi anni è stata protagonista delle cronache soltanto per aver ospitato alcuni incontri diplomatici, e una ventina d'anni fa per una spettacolare eruzione vulcanica.

Giunge quindi un po' inaspettata la notizia che F-PROT, uno dei migliori prodotti antivirus disponibili oggi sul mercato, è opera di un islandese. Ma per chi si occupa di virus il nome di Fridrik Skulason («Frisk», come lui stesso si soprannomina) è tutt'altro che sconosciuto. E i lettori più attenti forse rammenteranno che l'anno scorso parlammo di lui in occasione della scoperta dell'autore del virus «Den Zuko».

In realtà l'Islanda è molto meno fuori dei circuiti internazionali di quanto si possa ritenere superficialmente. Nello specifico ambito dei virus, oltre a Frisk operano in quel paese anche alcuni personaggi ben diversamente intenzionati, se si vuole prestare fede a chi afferma l'origine islandese di quei due o tre ceppi virali che vanno appunto sotto il nome di «Icelandic». Ma procediamo all'esame del prodotto.

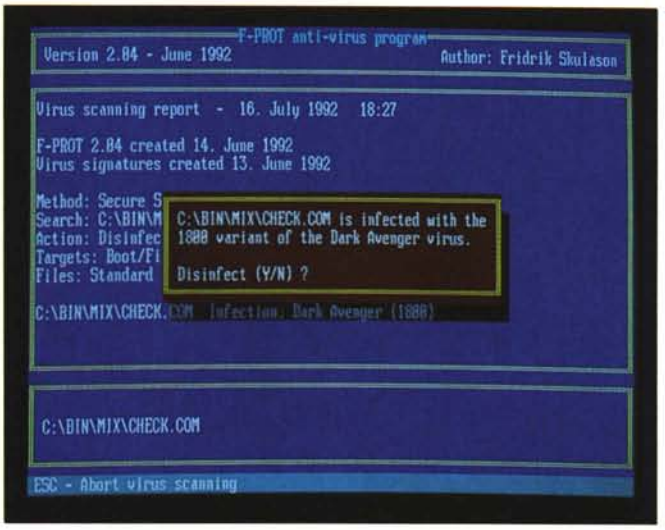
F-PROT

Produttore:
Fridrik Skulason, Frisk Software International, Postholf 7180, IS-127 Reykjavik, Iceland. Tel.: +354-1-694749 — fax: +354-1-28801 — Internet: frisk@complex.is
Prodotto reperibile tramite i normali canali dello shareware (su sistemi telematici nazionali ed esteri)
Prezzi di registrazione:
Per l'utente privato il programma è gratuito. L'utilizzo in aziende, enti e organizzazioni richiede il pagamento annuale di $1 per ciascun computer sul quale viene utilizzato F-PROT, con un minimo di $20 l'anno.

Le componenti

Come tutti i prodotti antivirus che appartengono alla categoria degli scanner, anche F-PROT viene aggiornato con frequenza. La versione in nostro possesso è la 2.04, rilasciata verso la metà di giugno; la successiva dovrebbe essere disponibile salvo imprevisti alla metà di agosto. Tutto ciò che compone il programma è compresso in un singolo archivio, FP-204.ZIP. Le funzioni del programma sono quasi tutte contenute in un unico eseguibile, F-PROT.EXE; fanno eccezione VIRSTOP.EXE, un piccolo TSR di sorveglianza che può essere utilizzato come strumento di allarme (v. riquadro), e F-TEST, un minuscolo programma che verifica la presenza in memoria di VIRSTOP.

F-PROT ha identificato un virus.



Prima della disinfezione viene chiesta conferma all'utente.

Fanno da corredo ai tre eseguibili alcuni file di supporto e configurazione, e una nutrita serie di documenti di testo, che vanno dal manuale d'uso delle funzioni principali del programma a un breve testo illustrativo sul fenomeno dei virus con alcune indicazioni su come comportarsi, fino alla descrizione del metodo euristico di analisi e ricerca di virus, una caratteristica esclusiva di F-PROT che approfondiamo a parte.

Installazione e uso

Installare F-PROT è semplicissimo: è sufficiente estrarre le componenti dell'archivio, inserendole per comodità in una directory specifica se lo si desidera.

Non ci stancheremo mai di rammentare come sia sempre opportuno tenere su un dischetto di sistema una copia degli antivirus che si sono scelti; F-PROT non fa eccezione a questa regola, e pertanto la prima cosa che si dovrebbe fare una volta spacchettato l'archivio è fare una copia del suo contentuto su un disco che contenga una versione pulita del DOS.

La prima impressione che si ricava avviando il sistema (è sufficiente il comando F-PROT senza alcuna ulteriore specifica) è che nel passaggio alla versione 2 dalla precedente versione 1, che avemmo occasione di vedere alcuni anni or sono, Frisk abbia speso un certo quantitativo di tempo nel progettare un'interfaccia utente degna di questo nome. La vecchia versione di questo antivirus infatti si componeva di più programmi diversi, con funzioni che in parte si sovrapponevano e un'interfaccia utente atroce, tutta fatta di comandi e switch da utilizzare di volta in volta.

All'avvio della versione 2 ci si trova di fronte a un gradevole menu con le funzioni del programma ben poste in evidenza, e una finestra nella parte bassa del video con i messaggi di aiuto contestuale. Tutte le funzioni sono state integrate in questa interfaccia unica, che peraltro risulta anche particolarmente robusta: l'abbiamo maltrattata in tutti i modi possibili ma non siamo riusciti a trovarle alcun difetto, salvo alcune scelte di impostazione che avremmo realizzato diversamente, ma si tratta di gusti personali.

I patiti della command line potranno invece attivare tutte le funzioni del programma mediante dei switch all'atto del suo lancio, evitando quindi del tutto di entrare nella sessione interattiva.

Le funzioni

All'avvio il programma esegue i soliti controlli: una verifica su se stesso per escludere l'ipotesi di essere stato modificato in qualsiasi modo, e una verifica della memoria alla ricerca delle tracce di eventuali virus residenti. L'utente si trova quindi di fronte alla scelta tra cinque diverse opzioni: Scan, Install, Viruses, Program e Quit.

SCAN richiama una dialog box nella quale l'utente può specificare le modalità di esecuzione della scansione. (Per semplicità illustreremo tutte le caratteristiche del programma facendo riferimento all'interfaccia guidata dai menu, ma tutte le funzioni attivabili da menu e dialog box sono perfettamente gestibili, come abbiamo detto, mediante dei switch sulla linea di comando).

L'utente può quindi scegliere il metodo di scansione, decidendo se avvalersi del «quick scan», rapido ma poco preciso, del «secure scan» più lento, ma ben più affidabile, oppure dell'analisi euristica. Va detto comunque che in questa versione si riscontra un sensibile aumento nella velocità della ricerca effettuata con il metodo sicuro, rispetto alla precedente versione che impiegava molto più tempo in tale funzione. Ai fini pratici quindi risultano talmente simili le velocità dei due metodi da far risultare inutile il «quick scan», che rimane esclusivamente a beneficio di utenti in possesso di PC molto lenti come gli originali XT.

La stessa modalità rapida di ricerca viene utilizzata da VIRSTOP, la controparte residente di F-PROT; in questo caso è accettabile che l'identificazione del virus sia imprecisa, poiché l'obiettivo di un programma come VIRSTOP è di bloccare l'esecuzione di programmi infetti, rimandando a una successiva analisi l'approfondimento della causa dell'infezione.

L'oggetto della ricerca può essere esteso all'intero hard disk o circoscritto a uno specifico file, directory o gruppo di file; si può indirizzare la ricerca verso un dischetto inserito nel drive, ovvero può essere indicato un drive logico di una rete locale.

L'utente ha il pieno controllo anche sul tipo di azione che il programma dovrà intraprendere nel caso in cui venga riscontrata un'infezione. Nel caso della ricerca veloce o dell'analisi euristica l'u-

F-PROT e l'analisi euristica

Una caratteristica interessante di F-PROT consiste nella possibilità di basare l'analisi dei file eseguibili, e la conseguente determinazione della presenza o assenza di virus, non già sul confronto con una stringa, ma sul comportamento del codice eseguibile.

Teoricamente si tratta di un approccio infallibile. Con un pizzico di fantasia anzi si può ravvisare in questo metodo una specie di applicazione pratica (e limitata) di uno degli eterni sogni dell'uomo, e cioè leggere il pensiero altrui.

Ma vediamo come si svolge il lavoro del ricercatore antivirus. Quando egli si trova di fronte a un programma che sospetta contenere un virus, la prima cosa che fa è cercare di comprenderne il funzionamento osservando il suo comportamento: in un ambiente opportunamente isolato viene eseguito il programma e si guardano i risultati.

Ad esempio, potrebbe darsi che qualcuno degli altri eseguibili viene modificato, oppure che cambia il boot sector o qualche variabile di sistema nella memoria.

A questo punto viene il lavoro più difficile: studiare il codice del programma per separare il corpo del virus dal resto del programma, e quindi andare a leggere una per una le istruzioni del virus per capire cosa voleva fare il programmatore che l'ha realizzato.

Detto così sembra facile, ma in realtà è un compito mostruoso, che porta via centinaia o migliaia di ore uomo perché già di per sé non è un lavoro semplice, ma bisogna moltiplicarlo per i trenta, cinquanta o cento nuovi virus che escono ogni mese.

Leggendo la sequenza di istruzioni previste dall'ignoto programmatore, il ricercatore ricostruisce la sua volontà, il suo pensiero, ed è in grado di rendersi conto al termine dell'analisi esattamente cosa succederà quando il virus verrà eseguito. È a questo tipo di lavoro che dobbiamo le informazioni precise, ad esempio, sul fatto che il virus Michelangelo si attiva il 6 marzo e distrugge il contenuto del disco fisso, ovvero che il Dark Avenger infetta i file eseguibili anche quando vengono aperti per una semplice lettura.

Spesso un'analisi così approfondita porta via troppo tempo, e per varie ragioni il ricercatore non ritiene opportuno andare più avanti.

Tuttavia è quasi sempre possibile determinare in breve tempo il tipo di meccanismo di cui il virus si serve per agganciarsi al sistema: trasferire il proprio codice in una diversa zona della memoria, inserire valori specifici nel vettore degli interrupt, andare alla ricerca di altri file eseguibili per modificarli, etc..

Un'analisi di questo genere si definisce «euristica» (gr. eurìsko = trovo, scopro). Si tratta di un metodo di ricerca non rigoroso, che consente di arrivare a risultati che dovranno poi essere verificati in maniera più scientifica, ma che nel caso dei virus offre il sostanziale vantaggio di consentire l'identificazione di virus che non sono stati ancora studiati.

E infatti il nostro virus sconosciuto, quello che abbiamo ricevuto da un lettore che l'ha sviluppato personalmente e che abbiamo conservato proprio per questo genere di test, viene inesorabilmente scoperto dall'analisi euristica di F-PROT, che dà la seguente indicazione:

«This program contains code to search for other executable files.
A normal program might need to do this, but this could also be a
direct-action (non-resident) virus».

Chiunque abbia un minimo di dimestichezza con i virus sa bene che un programma che va alla ricerca di altri file eseguibili va guardato con parecchio sospetto.

Descritto così, sembra tutto troppo bello per essere vero. Ma c'è ovviamente il rovescio della medaglia. L'analisi euristica che Skulason ha realizzato in F-PROT non funziona ancora perfettamente, tant'è che egli stesso nella documentazione sottolinea il fatto che si tratta di una funzione sperimentale, sulla quale l'utente non deve fare pieno affidamento. Infatti la metodologia adottata nella ricerca determina una serie di falsi allarmi e di false sicurezze.

La scansione dei duemilacinquecento e passa eseguibili che risiedono sul supervitaminizzato disco fisso del notebook dell'autore di questo articolo dà luogo ad alcune centinaia di segnalazioni.

La maggior parte di esse sono prive di significato; F-PROT non è in grado di effettuare un'analisi euristica sui programmi eseguibili compattati (ad es. mediante LZEXE, OPTLINK, PACK o simili), ed ogni volta che ne incontra uno segnala il fatto e procede oltre. Ma anche molti degnissimi programmi (PCSHELL, Microsoft Word, e alcune funzioni di QEMM tanto per citarne alcuni) vengono inflessibilmente bollati da F-PROT, che si accorge dell'insolito funzionamento di alcuni di essi.

Quasi sempre la segnalazione è corretta, e soltanto l'utente è in grado di distinguere il buono dal cattivo. È questo il caso di QEMM, forse il miglior gestore di memoria attualmente disponibile sul mercato, che tra le proprie funzioni offre la possibilità di spostare in memoria alta le aree richieste dai comandi di configurazione FILES, BUFFERS e FCBS. Per fare ciò si avvale di particolarissime funzioni non documentate del DOS, la qual cosa non sfugge a F-PROT.

Per contro, alcuni virus perfettamente conosciuti si comportano in modo talmente sporco e subdolo da sfuggire all'identificazione euristica.

E pertanto accade che un file che viene identificato con precisione come il dato ceppo e la data variante dallo stesso F-PROT utilizzato come scanner, venga per contro lasciato passare per buono in fase di analisi euristica.

Le prove che abbiamo effettuato confermano quindi che si tratta di una funzione che probabilmente potrà dare buoni risultati in futuro, se verrà affinata, ma che per il momento è opportuno lasciare agli specialisti, che siano in grado di interpretarne correttamente le segnalazioni.

S.T.

Un rapporto dell'analizzatore euristico. In realtà il primo dei due file è infetto, il secondo no.

nica azione possibile consiste nel generare un rapporto, in quanto una identificazione imprecisa del tipo di virus non consente di fare altro che di segnalarne la sospetta presenza. La determinazione precisa dell'origine dell'infezione, effettuata mediante il «secure scan», offre altre tre possibilità: la disinfezione, la cancellazione del file infetto e il cambio del nome.

Ancora una volta ci troviamo quindi di fronte a uno strumento che offre di rimuovere l'infezione, fornendo all'utente la possibilità di fare ciò che abbiamo sconsigliato circa centomila volte di fare. Di F-PROT c'è da dire che le sue capacità di disinfezione appaiono molto buone; in attesa di poter effettuare un test a tappeto su questo tipo di funzioni, per il quale non è semplice attrezzarsi, abbiamo fatto alcune prove non rigorose dalle quali però emergono risultati che vanno a favore di F-PROT e che ci permettono senz'altro di considerarlo il male minore, nel caso in cui l'utente sia costretto malgrado tutto a disinfettare i propri programmi anziché reinstallarli..

L'utente può scegliere se includere o meno nella ricerca alcune categorie di oggetti e specificamente: i virus da boot sector, i virus parassiti, i più noti cavalli di Troia e scherzi, le stringhe di identificazione specificate dall'utente e i file eseguibili compattati. Di queste cinque opzioni soltanto la quarta è disattivata di default, e può essere attivata soltanto dopo che l'utente abbia inserito — se ritiene necessario farlo — le proprie stringhe di identificazione di virus, servendosi di una diversa funzione del programma.

Infine è possibile scegliere quali tipi di estensioni formeranno l'oggetto della ricerca: gli eseguibili standard (*.APP *.COM *.EXE *.OV? *.SYS), ovvero tutti i file o un gruppo di estensioni specificate dall'utente.

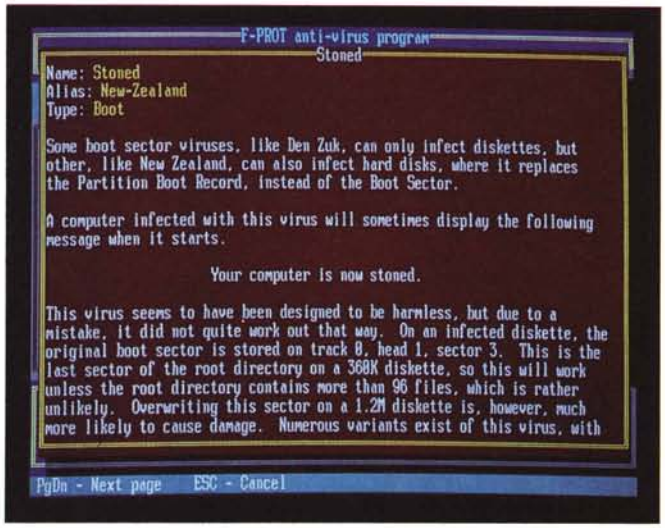
Le prestazioni

Una volta avviata, la ricerca è rapida. Sulla configurazione di prova, quella descritta nel riquadro, il tutto si esaurisce in una manciata di secondi anche perché il disco fisso è quasi vuoto. Sul sistema di confronto, il solito notebook 386sx con QEMM, Stacker, oltre 2.500 file eseguibili e per di più eseguito sotto Windows, F-PROT chiude i lavori in poco meno di tre minuti. Non abbiamo mai dato troppo credito a queste prove al cronometro, tanto che riteniamo superfluo fornire i secondi e i decimi; tuttavia è essenziale stabilire se i tempi di scansione sono accettabili o meno, perché in quest'ultimo caso l'utente si stancherà ben presto di utilizzare un programma che lo tiene inchiodato per ore davanti a un video con dei nomi che scorrono.

Sotto questo profilo F-PROT è più che valido. Se lo si esegue da un dischetto risulta in qualche modo più lento l'avvio, mentre la fase di ricerca viaggia sostanzialmente alla stessa velocità.

Nulla da eccepire per quanto riguarda la precisione: F-PROT fornisce indicazioni impeccabili in tutti i casi che gli abbiamo sottoposto. Non manca di rilevare nessuna infezione, specificandone con precisione il tipo e la variante; abbiamo inoltre esaminato i risultati di test condotti presso l'Università di Amburgo, che mostrano come F-PROT sia ora in grado di rilevare tutte le possibili permutazioni del Dark Avenger Mutation Engine, del quale abbiamo già avuto occasione di parlare.

Una scheda del database informativo sui virus.



Le altre funzioni

La ricerca di virus è supportata da altre funzioni accessorie, e in particolare:
— *Install*, che consente di installare o aggiornare il programma partendo da un dischetto, ovvero di predisporre le scelte di default o di personalizzare i messaggi in una lingua diversa dall'inglese. È inoltre possibile attivare VIRSTOP, la sentinella antivirus residente;
— *Viruses* fornisce un piccolo database di informazioni sui virus, sul genere di quello gestito da Patricia Hoffman (del quale abbiamo parlato alcuni mesi fa), ma più stringato e senza funzioni ipertestuali; mediante questa funzione inoltre è possibile gestire il proprio archivio di stringhe di identificazione di virus;
— *Program* fornisce alcune informazioni sul programma: il costo, le modalità per ottenere il programma o gli aggiornamenti (v. più avanti), le prestazioni e come contattare l'autore.

Dove si trova F-PROT

Per chi è in possesso di un modem e ha dimestichezza con sistemi telematici e BBS, ovvero per chi fa parte di club informatici o gruppi di utenza, l'approvvigionamento dello shareware non costituisce un problema. Ma gli altri utenti possono incontrare alcune difficoltà nel procurarsi un prodotto che apparentemente è molto buono, ma che non può essere acquistato nel solito negozio sotto casa, o magari ordinandolo presso uno dei vari mail order che ormai hanno preso piede in Italia come oltre oceano. Vediamo quindi come si può fare a procurarsene una copia.

La versione che abbiamo recensito l'abbiamo prelevata direttamente da una fonte attendibile. A differenza di McAfee, Skulason non gestisce in proprio un sistema telematico; si avvale per contro di alcuni centri di distribuzione di shareware raggiungibili tramite la rete Internet, definiti FTP-sites. Lo stesso autore provvede ad inviare a un certo numero di FTP-sites, noti per la loro affidabilità, le nuove versioni del prodotto. Chi ha accesso alla rete Internet non avrà quindi alcun problema nel procurarsi il programma. Per gli altri esistono due possibilità: collegarsi a uno dei tanti sistemi telematici (come il nostro MC-link) che lo mettono a disposizione dei propri utenti, se si ha a disposizione un modem; oppure richiederlo direttamente all'autore.

Le conclusioni

F-PROT è un programma che ci è piaciuto. Snello ma completo, potente

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 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.

ma facile da utilizzare e oltretutto costa anche molto poco: il costo di una telefonata via modem per procurarselo, a cui vanno aggiunte alcune decine di migliaia di lire se si intende utilizzarlo in ambiente professionale anziché per uso personale. Mantiene ovviamente i limiti tipici dei programmi di scansione, ma nella propria categoria resta uno tra i migliori e più affidabili strumenti di protezione contro i programmi aggressori.

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

I programmi antivirus residenti

Quasi tutti i programmi antivirus offrono tra le proprie funzioni la possibilità di installare un residente che tenga d'occhio tutti i programmi che vengono eseguiti, in modo da impedire che vengano caricati in memoria programmi infetti da qualche virus conosciuto.

Molti utenti hanno visto di buon occhio questa possibilità, considerandola un po' troppo semplicisticamente una soluzione radicale al problema dei virus.

In realtà questi programmi trovano un'applicazione precisa, al di fuori della quale non è del tutto prudente utilizzarli.

La limitazione non è tanto inerente ai programmi stessi quanto al modo in cui molti utenti se ne servono, ossia delegando ogni funzione di protezione a questi programmi e magari tralasciando di aggiornarli.

Un limite strutturale dei programmi residenti consiste nel fatto che non sono in grado per definizione di impedire un'infezione da boot sector.

Se si fa il boot da un dischetto infetto il programma residente non partirà, presumibilmente perché viene avviato dall'AUTOEXEC.BAT presente sul disco fisso; ma quand'anche partisse, dato il modo in cui avviene la sequenza di boot si ritroverebbe con il virus già eseguito e forse installato in memoria. Per ovviare a questo problema i residenti antivirus solitamente effettuano all'avvio una scansione dei boot sector del disco fisso, per verificare se sono infetti.

La combinazione di questi due fattori limitanti (trascuratezza dell'utente nell'aggiornare il prodotto e impossibilità di prevenire l'infezione del boot sector) può provocare effetti interessanti.

Consideriamo il caso di un computer in cui sia stato installato, nel gennaio 1991, un residente antivirus successivamente mai aggiornato.

Nel corso del 1991 sul computer viene inavvertitamente effettuato il boot di un dischetto contenente il Michelangelo, che come noto è stato scoperto nell'aprile 1991 e si è attivato per la prima volta nel marzo 1992. L'utente, che si crede al sicuro «perché tanto ci ha l'antivirus», la mattina del 6 marzo accende il computer e...

Ma anche se l'utente si preoccupa di aggiornare regolarmente il suo antivirus non è comunque una buona idea delegargli il compito di difendere la macchina, come ultima sentinella contro l'invasione degli alieni.

L'utente non deve mai abbassare la guardia, non deve trascurare i backup e non deve tralasciare di controllare personalmente il software che si procura e i dischetti che riceve.

Ecco quindi che l'utilità dei residenti antivirus viene considerevolmente ridimensionata. Ma allora a cosa servono in realtà?

È presto detto: servono nel caso in cui si verifichi un'infezione che viene scoperta con mezzi tradizionali, e vanno usati per il controllo successivo alla disinfezione. Rivediamo brevemente quali sono le fasi della disinfezione:

— si avvia il sistema con un dischetto pulito e si fa una scansione per determinare l'estensione dell'infezione;
— si fa un backup supplementare dei dati;
— se necessario, si ripartizionano e riformattano i dischi fissi e si reinstalla il sistema operativo;
— si rimuovono sistematicamente tutti i prodotti infetti e li si reinstalla partendo dai dischi originali; meglio ancora sarebbe reinstallare tutti i prodotti software, infetti o meno;
— si va a caccia di tutti i dischetti che possono essere stati infettati e si verificano e/o riformattano.

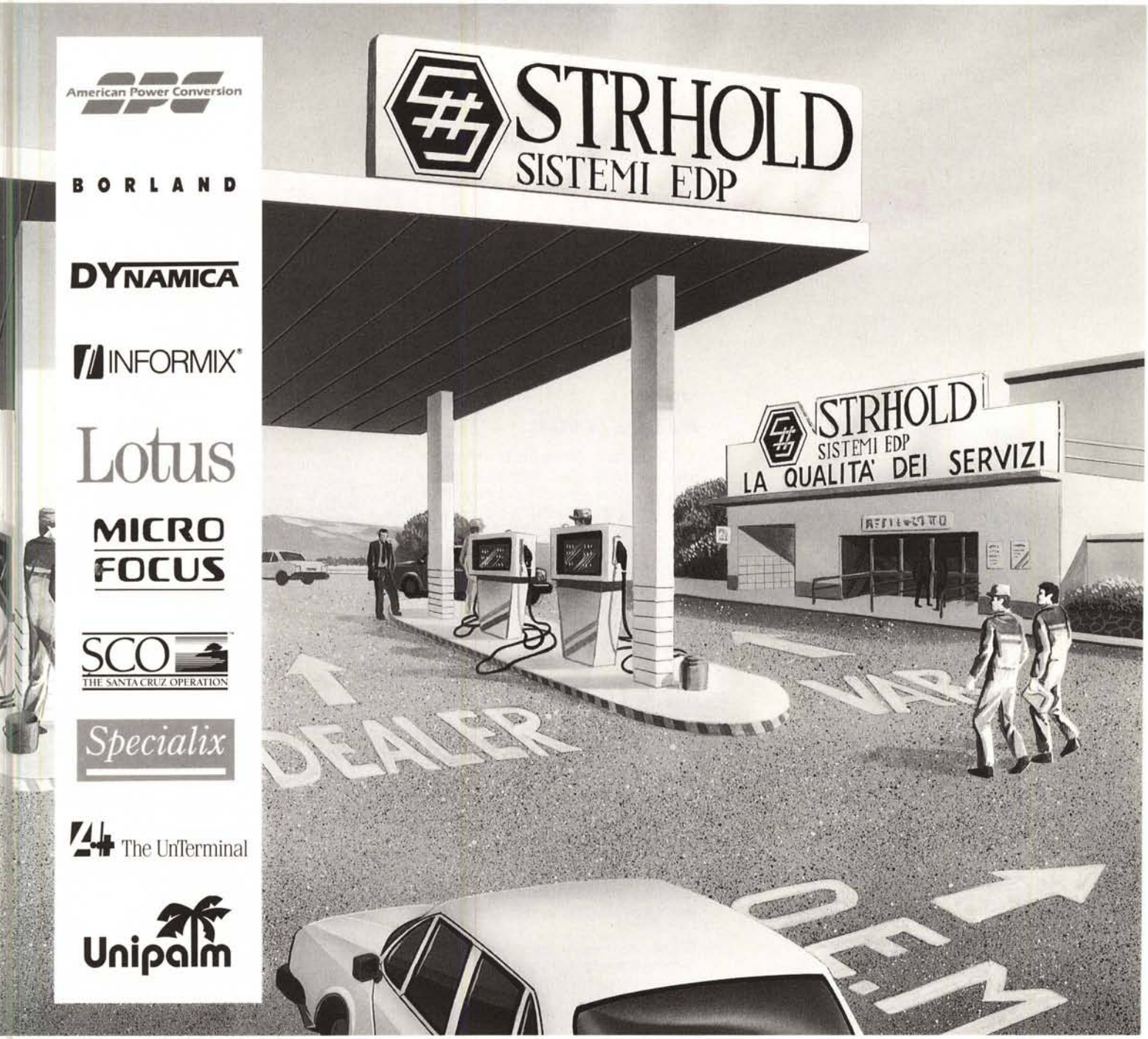
È in quest'ultima fase che i programmi-sentinella dimostrano tutta la propria utilità. Nel caos che segue la scoperta di un'infezione, specialmente se è molto diffusa in un ambiente aziendale con centinaia o migliaia di computer, quasi certamente si scatena la caccia al dischetto, si smuovono pile di carte che giacciono da mesi su scrivanie polverose alla ricerca del disco sepolto.

Ma non è detto che la caccia riesca al 100%, e oltretutto i problemi delle aziende multilocalizzate crescono in modo esponenziale al numero delle sedi, soprattutto se sono frequenti gli scambi di dischetti da sede a sede.

Pertanto la caccia al dischetto prevede necessariamente l'installazione su tutti i computer aziendali di un residente antivirus, che a questo punto verrà puntualmente mantenuto aggiornato: si spera che la lezione sia stata imparata. Poiché il virus responsabile dell'infezione sarà stato identificato, e non vi saranno dubbi sulla sua natura, certamente l'antivirus residente sarà in grado di identificarlo su quel dischetto sperduto che in qualche modo è riuscito a sottrarsi alla furia della caccia dei primi giorni, e magari riemerge dopo tre mesi quando ormai i giorni del Grande Disastro del Virus sono un ricordo passato.

Stefano Toria

AREE DI SERVIZIO UNIX IN ITALIA



STRHOLD®
SISTEMI EDP

PRESENTI A SMAU
Pad. 25 Stand C32-B35

IMAGEWARE

PIU' DI UN DISTRIBUTORE

Reggio Emilia Via Cipriani 2 - Tel. 0522/792641 - Fax 0522/77846 - Tlx 531059 STRHOL I • **Milano** Via Dante 4 - Tel. 02/72002222 - Fax 02/72001474 • **Torino** Via Borgaro 49 - Tel. 011/2296949 - Fax 011/2296939 • **Vicenza** V.le Mazzini 123/125 - Tel. 0444/324292 - Fax 0444/545248 • **Roma** Via Pannonia 51 - Tel. 06/7004234 - Fax 06/7001673 • **Napoli** Via S. Alfonso de' Liguori 3 - Tel. 081/457084 - 290283 - Fax 081/290283 • **Bari** Via Resistenza 48/B - Tel. 080/228430 - Fax 080/5364437 • **Catania** Via Asiago 35 Tel. 095/376686 - Fax 095/381369 • **Palermo** Via G.Bonanno 73 - Tel. 091/301650 Fax 091/347451 • **Matelica** (MC) Via Circonvallazione 131 - Tel. 0737/787058 - Fax 0737/787200 • **Prato** (FI) V.le Montegrappa 183 - Tel. 0574/575656 Fax 0574/572532 • **Albisola Capo** (SV) C.so Ferrari 109/2 - Tel. 019/487272 - Fax 019/480047 • **ODTeam**® Consulenza e supporto per SCO Open DeskTop