di Raffaello De Masi

Febbre da virus

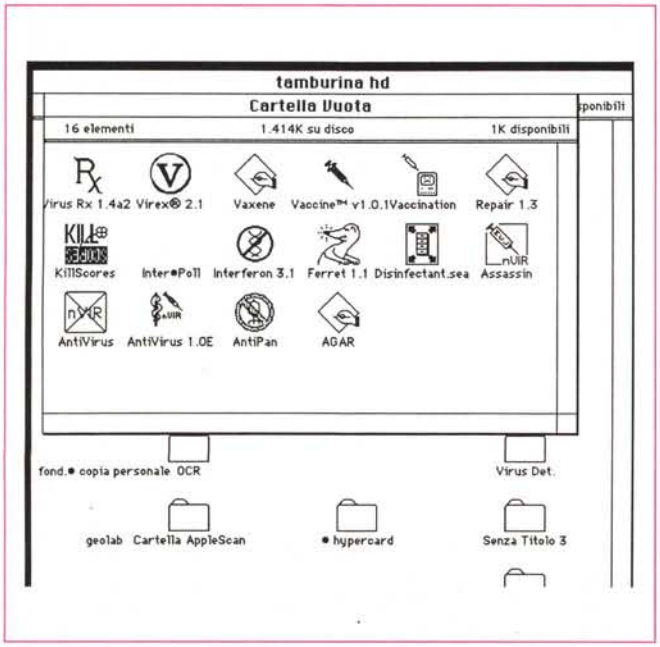
seconda parte

Una panoramica sui virus presenti nel mondo Mac: la terapia e la guarigione

La prima parte dell'articolo l'ho aperta con un detto di mia nonna; adesso ce ne sta bene un altro, che fa proprio alla bisogna, e che suona «Quando o' miedico sturea, o' malato se ne more!». Perciò, per evitare la parte del medico che parla, parla, senza dare soluzioni valide, credo che sia il caso, a un mese di distanza, di cominciare a fornire qualche chiarimento sulle cure da adottarsi quando ci ritroviamo nel bel mezzo di un'infezione selvaggia

In linea pregiudiziale è possibile affermare che, con un poco di pazienza e con i «ferri» adatti anche le applicazioni più attaccate possono essere ricuperate, a patto che non siano state sovrascritte da quel tipo di virus, piuttosto raro, che si moltiplica senza ritegno sovrapponendosi a tutto quello con cui viene a contatto. Sebbene molti virus siano stati descritti come operanti in tal modo, all'atto pratico la stragrande maggioranza di essi attacca solo l'header, la directory del disco. Una opportuna riparazione di questa «resuscita», come per incanto, file che si era dati per dispersi o completamente perduti. Anche applicazioni che sembravano irrimediabilmente compromesse possono essere facilmente ricuperate se si interviene correttamente su non più di un paio di tipi di risorsa. L'importante è sapere cosa fare e/o avere i mezzi adatti per fare il necessario.

Il mercato mette a disposizione molti programmi ad hoc per la cura e la eliminazione dei virus presenti su un sistema. Si tratta, alcune volte, di prodotti commerciali, come i notissimi SAM e Virex, ma nella maggior parte dei casi i prodotti vengono distribuiti gratuitamente o, attraverso le reti, in forma shareware («se ti piace manda un piccolo compenso, altrimenti butta via tutto»). Proprio in questa tipologia di prodotti abbiamo trovato un tool dalle caratteristiche eccellenti, che probabilmente supera tutto quello che la concorrenza mette a disposizione.

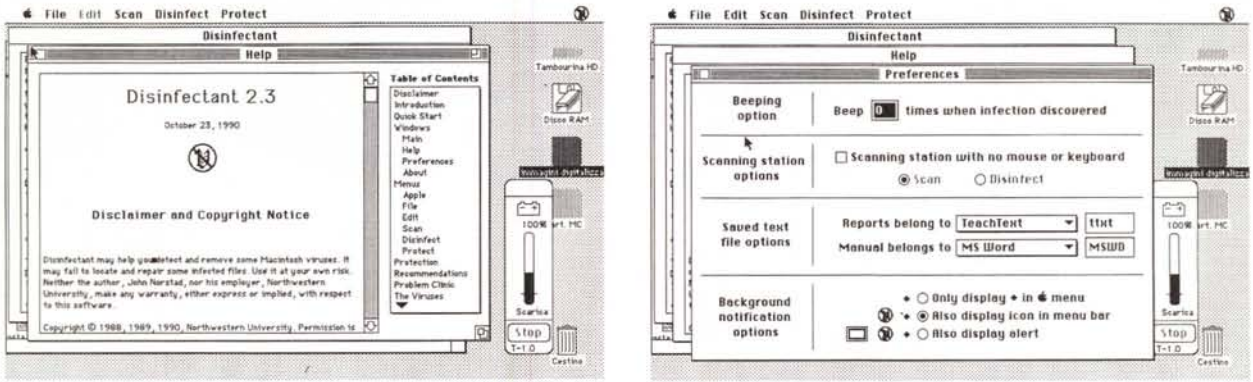


Una panoramica degli antivirus più diffusi.

I tipi di antivirus disponibili

Ma procediamo con ordine: gli antibiotici, per così dire, che possiamo fornire alla macchina possono essere raggruppati in due categorie fondamentali: quelli che distruggono semplicemente l'agente invasore, e quelli che tentano anche un parziale o totale recupero delle applicazioni (o dei file dati) avariati o comunque intaccati dall'agente.

I primi sono di più antica realizzazione e data, e rappresentano l'approccio più semplice al problema. Il loro meccanismo d'azione è piuttosto semplificato se si tien conto che essi sradicano dall'applicazione infetta l'agente, ma questa rimane comunque in possesso delle risorse guaste. L'applicazione, comunque, resta inutilizzabile (generalmente, al lancio, si ritorna quasi immediatamente al Finder) o possiede qualche bug che, nel momento meno atteso manda in bomba il sistema (tecnicamente parlando, questo avviene quando è chiamata in causa una risorsa che, per essere guasta, non riesce più a trovare il path principale dopo la sua esecuzione). Una



Disinfectant, l'eccellente programma di John Norstad, con le sue diverse opzioni.

variante al tema è rappresentata dagli antivirus (piuttosto semplificati anch'essi) che permettono di cancellare, direttamente da programma, le applicazioni sospette e non più sicuramente utilizzabili.

Gli antivirus più recenti ed efficienti permettono, oltre alla eliminazione dell'agente infettivo, anche il parziale o totale recupero delle applicazioni infette. Essi riescono a ricostruire in maniera abbastanza precisa le risorse rovinate, in modo da consentire l'uso di programmi (come quelli Microsoft Italia) protetti e installabili per una sola volta sull'hard disk). Anche qui, però il consiglio della maggior parte dei produttori (e della Apple stessa) è quello di reinstallare un'applicazione originale, per quanto sia possibile.

Vediamo a questo punto quali sono gli antivirus più diffusi, anche attraverso una breve cronistoria delle più importanti release esistenti sul mercato. Per una questione di principio, comunque, tratteremo poco o nulla dei programmi commerciali, e questo per due (crediamo buoni) motivi: primo perché esistono, come public domain software, programmi altrettanto (se non più) efficienti di quelli commerciali, secondo perché il voler speculare su una disgrazia capitata ad un altro rappresenta, a mio avviso, una non gratificante attività (si è arrivati all'assurdo, negli States, che un demo di un fantomatico programma veniva inviato gratuitamente; questo, appena lanciato, installava un virus di tipo completamente nuovo, il cui antivirus veniva poi fornito, a pagamento, dagli stessi fornitori del demo iniziale; bello stampo di imbroglioni!). Ben venga, quindi la tecnica dello shareware (che nel mondo della mela si chiama MacHonor): se utilizzi il programma o lo trovi degno della tua attenzione, per favore invia un compenso (generalmente pochi dollari) all'indirizzo XXXX YYYYY (alcuni autori, tra cui quello di uno dei più efficienti e potenti pacchetti antivirali attualmente in giro) chiedono di inviare il «compenso» ad associazioni benefiche o assistenziali.

Gli antivirus commerciali

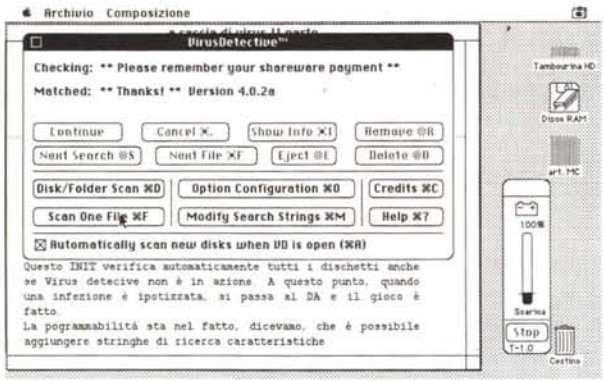
Vediamo, quindi cosa c'è a disposizione soprattutto in questa area. Per quanto attiene ai programmi commerciali le scuole, per così dire, sono due: quella che fa capo a Virex, e l'altra che gravita intorno a SAM. Il primo è un ben noto programma della HJC Software giunto oggi alla versione 2.7. Dotato di una interfaccia accattivante, semplice da usare anche da parte di un inesperto (basta lanciare e scegliere il tipo di operazione che si desidera effettuare: scansione del disco, solo ricerca dei file corrotti, o ricerca e riparazione) ha un solo grande difetto: almeno fino alla release nominata non può analizzare i file e i programmi in uso, come, ad esempio, il Finder-Multifinder, il Desktop, il System e così via! Occorre quindi eseguire la diagnosi partendo da un dischetto all'uopo costruito, e contenente solo i documenti di lancio e il programma stesso.

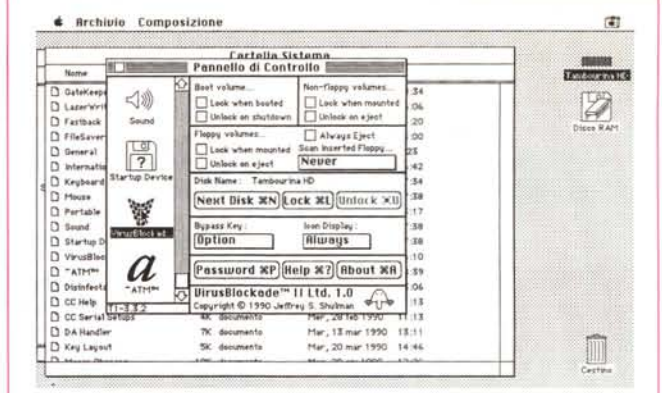
SAM è un programma di buona qualità e fattura; il principio e le tecniche di funzionamento sono le stesse, ma il problema dell'analisi delle applicazioni «busy» è superato; questo permette di eseguire immediatamente una analisi del sistema nel momento stesso in cui si ha un dubbio sullo stato di salute del sistema, magari intervenendo dall'interno di una applicazione, senza nemmeno chiuderla e lavorando anche in Multifinder. Un ottimo antivirus, anche se non è certo nato per questo motivo, è il blocco delle utility Norton; Lanciando il Disk Doctor il programma esegue una analisi completa del sistema, diagnosticando e fissando anche gli eventuali «buchi» nei programmi e nelle applicazioni. Ovviamente, proprio perché non è nata per questo motivo, l'applicazione non distingue tra infezioni da virus e difetti fisici del dischetto, ma il risultato è quello che conta; proprio per i motivi anzidetti, comunque, alcune categorie di virus sfuggono al controllo di queste utility.

Il software di pubblico dominio e shareware

Ma passiamo alla parte più interessante. Dal 1988 a oggi numerosi programmatori si sono cimentati nel realizzare applicazioni (e talora pacchetti) destinati a combattere questo flagello. Tracceremo di seguito una piccola cronistoria delle applicazioni più efficienti, realizzate nel corso di questi tre anni, per poi fare il punto su quelle che attualmente offrono le maggiori garanzie di efficienza e sicurezza. I pacchetti sono elencati in ordine alfabetico, con la release più recente (alcuni di essi sono ormai fuori mercato e superati — vengono citati solo per dovere di cronaca) e su ognuno di essi viene espresso un giudizio generale sulla sua efficienza e un commento.

- ***AntiPan (1.5) di M. Hamel.*** Specifico contro gli nVIR. Legge dischetti e hard disk, rimuove le infezioni e ripara i file. Individua anche i cloni di nVIR. Cosa estremamente interessante, dop l'operazione di «pulizia» esegue una rie di operazioni che «vaccinano» stema da successive infezioni, re

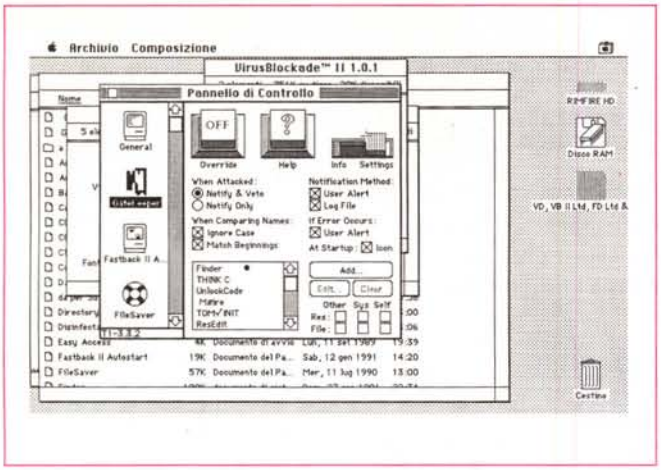




Ancora un altro campione, Virus Detective, che va opportunamente abbinato a Virus Blockade per la migliore opera di prevenzione.

dolo del tutto resistente. Si tratta di un programma piuttosto efficiente, ben supportato dall'autore, che fornisce anche informazioni dirette sull'uso, in tempi ragionevolmente brevi.

- ***AntiVirus (1.0 E) della SoftHansa Gmbh***. Ripara dischetti infetti da nVIR e previene successive infezioni con un meccanismo di vaccinazione piuttosto simile a quello di AntiPan. Non subisce aggiornamenti da molto tempo, ma è ancora piuttosto efficiente.
- ***Assassin (2.0) di Peter Gontier***. Gratuito: ancora dedicato alle infezioni nVIR, è piuttosto semplice da usare e fornisce buoni risultati. È molto veloce nelle operazioni; dà qualche problema con Multifinder. Sebbene si tratti di un programma di grande qualità, è stato a un certo punto abbandonato dall'autore, che ha invitato i suoi clienti ad utilizzare Disinfectant (vedi appresso).
- ***Disinfectant (2.3) di John Norstad***. Gratuito: la prima versione è del lontano marzo 1989: si tratta di uno dei più potenti ed efficienti antivirus presenti sul mercato; è accompagnato da una documentazione tecnica notevole e l'autore (professore alla NorthWestern University dell'Illinois) lo ha immesso in tutte le reti più diffuse negli States, in modo che possa essere acquistato da chiunque lo desideri: ne parliamo in seguito.
- ***Eradicat'em (1.0) di Dave Platt***. Gratuito: si tratta di un altro ottimo programma, che permette l'eliminazione di s del tipo WDEF e CDEF. Si presen- me un documento di startup di si- , che sradica automaticamente le ni appena queste danno segno di binato a programmi come Gate- e/o Disinfectant permette una e molto efficace del sistema.
- ***'1.1) di Larry Nedry***. Gratui- di una delle più vecchie rea- stenti sul mercato, e il la- namento non è stato molto seguito. Elimina infezioni di tipo Scores, ma dimostra di essere datato dando qualche problema nella individuazione e nella eliminazione di ceppi recenti.
- ***GateKeeper (1.1.1) di Chris Johnson***. Gratuito: prodotto eccellente, efficiente e di gran qualità, si tratta di un INIT che protegge il sistema da infezioni di tipo WDEF e CDEF. Possiede come ideale complemento GateKeeper Aid (1.1.2). Sebbene non offra protezione contro virus del tipo WDEF e CDEF (è il suo tallone d'Achille) ha il pregio di essere estremamente efficiente, facile da usare (basta installarlo nella cartella Sistema) ed è ben supportato dall'autore. Ne parliamo un po' più ampiamente in seguito.
- ***Interferon (3.1) di Robert Woodhead***. Intercetta infezioni di Score e nVIR, ma non permette la riparazione dei file. Si tratta di una delle più vecchie realizzazioni e il suo uso non è privo di pericoli (può smembrare le directory di un HD). Lo stesso autore raccomanda di non più usarlo (anche se ci pare un consiglio interessato, visto che Woodhead è l'autore di Virex, un programma commerciale dei più diffusi e venduti).
- ***KillScores (1.0) di Mark Pack e Apple Corps di Dallas*** (con la collaborazione di Howard Upchurch). Gratuito: ripara e rimuove infezioni di virus Scores. Efficiente e quasi del tutto trasparente.
- ***KillVirus. (1.72) di Mathias Urlichs***. Gratuito: noto anche col nomignolo di KillnVIR, è un potente distruttore di questi agenti patogeni. È un INIT, e ripara fin dal lancio tutte le applicazioni, compreso il System, il Finder e il Multifinder. Inoltre aggiunge una risorsa del tipo «nVIR 10 Inibitor» al System File, che permette di prevenire ulteriori infezioni; peccato che abbia due difetti: l'inibitore implementato viene talora confuso, da altri pacchetti antivirus, come una infezione, e ancora è completamente trasparente per cui rimuove tutto quello che presume essere una infezione senza avvisare l'utente.
- ***N.O.M.A.D. (1.55) di Bill Pierce***. Rimuove infezioni nVIR, ma non dal System dal Finder.
- ***Quick Scores (1.8) di Antony Tuorto.*** Gratuito: è un desk Accessory che permette di identificare ed eliminare infezioni da Scores. Non ripara le applicazioni.
- ***Repair (1.5) di Steve Brecker***. Gratuito: dedicato agli nVIR non esegue la scansione di tutto il disco. Occorre indicargli volta per volta il file da analizzare. Questo suo difetto lo rende poco utilizzabile, specie data la concorrenza di pacchetti molto più efficienti.
- ***RezSearch (1.0b) di Wade Blomberg***. Gratuito: si tratta di un tool professionale, essendo configurabile per eseguire ricerche finalizzate di stringhe, caratteristiche di infezioni virali. Non è di uso facile né ovvio.
- ***RWatcher (1.0) di John Norstad***. Gratuito: uno Startup che offre una protezione combinata contro Scores e nVIR. Configurabile. Sebbene si tratti di un sistema altamente professionale è stato abbandonato dall'autore, che consiglia di utilizzare Disinfectant e GateKeeper.
- ***Vaccination (1.1) di Mike Scanlin***. Ripara da infezioni nVIR. Anche esso ha il difetto specifico di Repair (occorre indicargli, volta per volta il file da analizzare). Non può riparare un System file. In complesso ha prestazioni piuttosto modeste.
- ***Vaccine (1.0.1) CE Software***. Sebbene distribuito da una organizzazione commerciale, è gratuito ed è presente su molte reti! Si tratta del sistema ufficiale Mac inizialmente adottato contro le infezioni; monitorizza attività sospette, ma non è efficace contro tutte le infezioni. È stato abbandonato e non è più



GateKeeper facilissimo da usare; occorre indicare i file da monitorare.

efficace contro diversi nuovi ceppi.

- ***Vaxene***. Anonimo gratuito; non esegue la scansione completa del disco. Non ripara le applicazioni infette. È la classica beffa del programmatore, visto che, nella finestra delle informazione appare un messaggio che avvisa che l'autore è lo stesso del virus Scores.
- ***VCheck 1.3 di Albert Lunde***. Gratuito. Esegue uno «snapshot» del System e lo compara con il precedente ad intervalli regolari. L'utilità è solo relativa.
- ***Virus Blockade II (1.0) di Jeffrey Shulman***. Un INIT che, tra le numerose altre caratteristiche, ha anche quelle di eseguire la scansione automatica dei dischetti inseriti.
- ***VirusDetective (4.3) di Jeffrey Shulman***. Desk Accessory che può essere configurato. Non può riparare applicazioni infette, ad eccezione di quelle da WDEF e CDEF. Possiede una configurabilità totale, che lo rende un tool efficace e distruttivo nei confronti di quasi tutti i virus, a patto di essere in mano a uno specialista. Grazie a questa configurabilità spinta, Virus Detective è uno dei più potenti pacchetti sul mercato, in quanto basta intervenire sui suoi setup per configurare l'applicazione a nuovi tipi di infezione presenti. Tanto per fare un esempio, quando comparve il virus WDEF Virus Detective fu l'unico capace di fronteggiare la situazione in attesa delle release aggiornate degli altri pacchetti. Inoltre il servizio di supporto e aggiornamento fornito dall'autore è di eccezionale qualità e rapidità. Ne riparliamo appresso.
- ***Virus RX (1.6) di Apple Computer***. Gratuito: riesce ad individuare praticamente tutti i virus presenti. Sebbene non permetta la riparazione dei file infetti, è forse il tool diagnostico più potente esistente sul mercato.
- ***Virus Warning (1.0) di Mike Scanlin***. Gratuito: è un documento di startup che lancia un messaggio di avvertimento quando si verifica una infezione da nVIR; non previene l'infezione ed è di scarsa utilità.
- ***Warning (1.1) di William Lipa***. Gratuito: funziona pressoché allo stesso modo di Virus Warning e ne possiede gli stessi difetti.

Un'occhiata più da vicino ai migliori tool

E adesso diamo uno sguardo più da vicino ai pacchetti più interessanti, sempre nell'ambito dello shareware e del free software. Tra i molti abbondantemente disponibili sul mercato abbiamo scelto quelli che, in forma diversa, assolvono a compiti almeno in parte complementari e che rappresentano una dotazione minima, ma completa, di difesa contro gli attacchi batteriologici al cuore, pardon, al chip del nostro Mac.

Disinfectant

Come d'altro canto si intendeva anche da quanto detto in precedenza, uno dei package più efficienti è Disinfectant, di cui, nell'ottobre scorso è stata messa in circolazione la versione 2.3 . L'autore, John Norstad della Academic Computing ad Network Services della North Western University di Evanston dell'Illinois, mette a disposizione il pacchetto completo, rappresentato dal codice oggetto e da un manuale di istruzioni (sotto forma di file testo) completo ed esauriente.

Il programma è piuttosto sostanzioso (circa 340 K, anche se in questi sono contenuti un help in linea di gran pregio); il package ha un unico neo, ma di scarsa importanza; si tratta di un programma a sé stante, non di un INIT, CDEV o DA. Come mostrato anche da una suggestiva animazione corredata di musichetta «acchiappafantasmi», Disinfectant è efficace (individua, cancella i virus e ripara le applicazioni guaste) del tipo Scores, nVIR, INIT 29, ANTI, MacMag, WDEF, ZUC, MDEF, Frankie e CDEF (praticamente tutto lo scibile in fatto di virus).

È scritto in MPW, l'ambiente di sviluppo Mac di cui parliamo anche nelle note relative alla programmazione strutturata. Oltre al programma vero e proprio, al lancio può essere installato, nella cartella sistema, un INIT che permette di monitorare tutte le attività e di evidenziare quelle sospette.

Non si tratta di una opzione sempre desiderabile. Il gran difetto degli INIT o dei programmi che monitorano l'attività del disco è che essi non distinguono tra interventi «cattivi» e «buoni». Così anche la semplice aggiunta al System di un set di caratteri fa scattare le difese (l'INIT monitora una attività illecita a danno delle risorse del sistema o del Finder) e il tutto può rappresentare una gran seccatura, in fondo.

Disinfectant fornisce anche una serie di opzioni e, dopo aver eseguito le sue operazioni di verifica crea un report che può essere stampato o scritto in un file testo. Ciononostante è consigliabile sopportare il fastidio, ma assicurarsi una vita tranquilla. Infatti l'applicazione principale non difende dall'infezione, cancella solo quelle già esistenti e ripara (alla perfezione) le applicazioni intaccate.

Di grande interesse è infine la serie di opzioni avanzate disponibili; tra le altre abbiamo trovato utili quelle che permettono la scansione di reti AppleShare e dischi pubblici su reti TOPS, anche se è senz'altro più facile accedere ai file direttamente attraverso la macchina che materialmente li contiene. Ancora Disinfectant può essere installato su un server e usato da più di un utente simultaneamente. Nonostante la sua poten-

Virex Guard; sebbene sia estremamente efficace è piuttosto fastidioso nell'uso.

za, il programma non individua infezioni presenti su archivi Stuffit, BinHex, Packit o altri meno diffusi programmi di compressione. Ancora, la versione 2.3 non funziona su dischi Rodime Cobra.

Disinfectant è distribuito gratuitamente, ma solo attraverso network: i parametri di accesso sono i seguenti: BitNet: jln@nuacc. Internet : jln@casbah.acns.nwu.edu. AppleLink : a0173. Compuserve: 76666,573. Attraverso queste reti è possibile colloquiare anche con l'autore.

Virus Detective

Altra applicazione degna di nota è Virus Detective, giunto alla versione 4.03. Si tratta di un prodotto shareware, e l'importo da inviare è abbastanza modesto (40$, compresi gli upgrade). L'autore mette a disposizione un pacchetto, per così dire, complementare, Virus Blockade, di cui diremo tra poco.

Nella sua implementazione principale, Virus Detective è un DA; esso va installato con DAMover. Usando il gergo pittoresco dell'autore esso fa la guardia e annusa virus attivi e inattivi e cavalli di Troia. Il grandissimo pregio di Virus Detective, che ne fa un pezzo davvero unico, è che esso è programmabile. In che modo? Semplice: ogni virus è caratterizzato da una stringa di caratteri. Quindi, la base del programma è sempre la stessa; l'autore invia periodicamente agli utenti registrati l'elenco delle stringhe necessarie per intercettare nuovi virus. La vera forza del pacchetto è comunque l'abbinata con Blockade, un INIT/cdev venduto anche esso in shareware, che autolanciandosi elimina completamente qualsiasi problema o preoccupazione circa la presenza di virus.

Questo INIT verifica automaticamente tutti i dischetti anche se Virus Detective non è in azione. A questo punto, quando una infezione è ipotizzata, si passa al DA e il gioco è fatto.

A dispetto del prezzo (non si può certo avere tutto gratis) questo antidoto-medicamento è molto efficace e rappresenta, grazie alla sua (non proprio facile) programmabilità un buon investimento. Sia Detective che Blockade possono essere richiesti a Jeffrey S. Shulman, P.O. Box 521. Ridgefield, CT 06877.

GateKeeper

Terzo (ma non per importanza) in questa rassegna è GateKeeep che generalmente offre i migliori risultati se abbinato con GateKeeper Aid. Sono ambedue INIT, anzi per essere precisi sono rispettivamente un CDEV e un INIT. Si tratta della classica utility fatta apposta per chi non è tagliato per giocherellare con le risorse e con tecniche approfondite di analisi dei file. Lo si mette nella cartella sistema e lo si dimentica; esso vieta qualunque operazione di modifica delle risorse presenti sulle memorie di massa.

Per la verità non si tratta di un toccasana. Ad esempio interferisce continuamente con l'eccellente FileSaver delle Norton Utility (che ha bisogno di aggiornare continuamente un suo file nascosto dove tiene traccia delle attività eseguite); ma non basta! Anche il semplice tentativo di aggiungere o togliere un font crea problemi. Inoltre è una dannazione per chi programma visto che, nella fase di compilazione, il linguaggio manipola spesso e volentieri le risorse del codice oggetto che sta formando. Per contraltare, se si sopporta un poco la sua onnipresenza, libera definitivamente dalla preoccupazione dei virus; inoltre, cosa da non sottovalutare, crea un report automatico di tutte le sue attività, che può essere analizzato alla ricerca delle applicazioni sospette.

Simile al precedente, ma meno articolato e un poco più ridotto nelle prestazioni è il ben noto VirexGuard, che monitora i dischetti ogni volta che vengono inseriti; non distrugge l'infezione, come il precedente, per cui va utilizzato con un buon antivirus; generalmente lavora meravigliosamente in combinazione con Disinfectant.

Infine potete vedere nelle figure una miscellanea dei programmi descritti nell'articolo; di essi non parliamo per motivi di spazio e anche perché sono superati da quelli che abbiamo descritto in maniera più dettagliata.

Conclusioni

I virus per il Mac, grazie anche alla particolare struttura del sistema operativo, sono costretti a seguire, nel loro attacco, non più di quattro o cinque vie obbligate. La chiave di accesso per la maggior parte dei virus è, senz'altro, quella delle risorse (è questo il motivo per cui i pacchetti prodotti dai programmatori meno scaltriti, che non fanno uso delle risorse stesse, sono «duri» da attaccare da parte dei virus). Così gli antivirus sono costruiti, essenzialmente, per tenere d'occhio questa via maestra d'infezione, e svolgono quasi sempre bene il loro compito.

Dopo averli usati in lungo e in largo ritengo i più validi essere Disinfectant (gratuito, efficientissimo, e con una documentazione superba, a dir poco), e Virus Detective (quest'ultimo, se ben programmato e abbinato con Blockade rende le memorie di massa virtualmente impenetrabili); Gate Keeper è fatto per essere montato e dimenticato, ma a volte è una presenza inopportuna; Virex (che bisogna comprare) ha il difetto di non analizzare i file in funzione (tipicamente Desktop, dove purtroppo si insediano la maggior parte degli agenti patogeni, Finder, System, DA Handler, i driver della stampante e le applicazioni in quel momento aperte); occorre costruirsi un dischetto di boot che contiene solo questo programma e lanciarlo per analizzare l'HD interno; in compenso è quello che più di tutti riesce a riparare meglio le applicazioni guaste.

Dan Littman e Tom Moran nel loro mensile report sui virus di nuova scoperta parlano addirittura di un virus che può provocare danni fisici alla LaserWriter: come ciò sia possibile sinceramente non lo so, ma la cosa certo non fa dormire la notte. Spero di non averci mai a che fare, in ogni caso ho montato sul mio FX Virus Detective, SAM, GateKeeper e Disinfectant, con FileSaver alle spalle che dà il suo contributo. Non sarà una gran prova di coraggio, ma, nel dubbio, come dicono i banchieri, meglio esagerare!

MC