Mac e virus

Nel mondo delle infezioni virali che stiamo esplorando si è arrivati anche alla specializzazione; per quanto attiene al Macintosh abbiamo quattro famiglie di virus diversi che, scherzosamente, definiremo con quattro diversi aggettivi.

— ***Virus «bonaccioni»***: si tratta di virus che non producono grossi danni; generalmente oscurano senza dare preavviso lo schermo ma non pregiudicano dati o il salvataggio della sessione corrente; talora fanno comparire inaspettatamente sullo schermo vermi o insetti in movimento che non scompaiono se non si resetta il sistema. Alla fin fine si tratta di una burla, se vogliamo, di buon gusto, e facilmente sopportabile.

— ***Virus «fastidiosi»***: si tratta ancora una volta, di virus che non producono un vero e proprio danno, ma solo inconvenienti talora non immediatamente rilevabili; il più famoso di questi è rappresentato da «fatman», un virus che «ingrassa file ed applicazioni fino a saturare i media, in particolare l'hard disk». Abbiamo eseguito una prova pilotata di questo virus su un HD presente in un SE e i risultati si vedono in figura 1 dove il file di questo articolo (circa 3000 battute-byte) si è più che decuplicato. Anche qui il fastidio è solo passeggero, ma questo virus ha il difetto di mandare, talora, in bomba il sistema, con perdita della sessione corrente e dei rispettivi dati.

— ***Virus «cattivi»***: si tratta di virus che attaccano subdolamente le applicazioni, rendendole parzialmente inservibili; ci si ritrova dopo un certo periodo, con l'HD semirovinato e bisognoso di un backup parziale; un esempio di questa famiglia è «Unable virus», peraltro poco diffuso.

— ***Virus s...***: ognuno aggiunga ciò che crede. Si tratta di una vera e propria piaga! Questi virus sono piuttosto «sporchi», in quanto, oltre ad avere lunghi periodi di incubazione, producono danni irreversibili alle applicazioni; un esempio è, appunto, «nvir» che rende le applicazioni che attacca praticamente mai più utilizzabili, in quanto, anche dopo una adeguata «cura» con «deviratori» come «Antibiox», «KillVirus» o «Virus Detective», l'applicazione è del tutto persa (lanciata, ritorna al «Finder»), almeno per un utente non specialista e profondo conoscitore di «Inside Macintosh». Tutto questo è causa di gravi fastidi, se si tiene conto dell'impegno che è necessario per ricostruire il contenuto di un hard disk, anche se sottoposto periodicamente a backup.

Diviene quindi necessario avere a disposizione le tecniche per essere capaci non solo di rimuovere il virus ma, nella bisogna, di poter tentare di recuperare o riparare una applicazione rovinata. La prima cosa da fare è di installare un virus detective, come quelli elencati precedentemente o come, ad esempio «Vaccine», e rilanciare il sistema. Se compare una bomba, o il sistema si inchioda, o, ancora, otteniamo un avviso dall'antivirus, il Finder è contaminato (si ricordi che, nella maggior parte dei casi, i virus non possono attaccare programmi che non siano stati fatti funzionare almeno una volta; anzi, generalmente, quelli più «azzannati» sono quelli più utilizzati; una volta ho trovato un MacWrite con addosso 35 «nvir»); occorre, a questo punto rilanciare di nuovo con un dischetto di sistema e sostituire il Finder infetto.

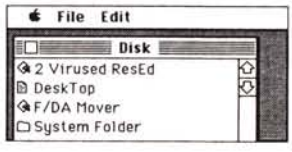

Figura 2

Figura 3

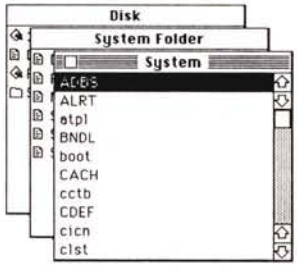

Figura 4

Figura 1

Lanciare Resource Editor o ResEdit: stessa trafila per quanto attiene alla possibilità di infezione.

Se tutto funziona ci troveremo al livello principale di radice dei file presenti sul disco (fig. 2); tra gli altri avremmo un File, il DeskTop, non visibile normalmente, che non ha niente a che vedere con virus et alia (è il file che viene ricostruito quando, nel lanciare il sistema, si tengono premuti contemporaneamente i tasti Option e Command).

Scrollare con le barre laterali fino a trovare la Cartella Sistema, ed aprirla col doppio click. Avremo qualcosa di simile alla figura 3, selezionare Desktop File e scegliere «Clear» (o Cut) dal menu Edit; fare la stessa cosa con l'archivio appunti ed il blocco note (se, come abbiamo visto nelle puntate precedenti, presentano un aspetto sospetto).

Localizzare il System ed aprirlo; avremo una figura simile alla 4. Selezionare «atpl» e aprirlo; qui selezionare «aptl id 128» ed eseguire l'operazione di Clear o Cut, come dinnanzi.

Chiudere «aptl» ed aprire «DATA»; cancellare «DATA ID-4001». Chiudere di nuovo ed aprire «INIT»; cancellare ID 10, ID 17 e ID 6. Chiudere tutto e salvare così come è, quando ci verrà richiesto.

Attenzione; un System pulito non contiene alcuna risorsa del tipo «aptl» o «DATA»; ciononostante abbiamo elencato quelle che bisogna cancellare; infatti alcune applicazioni, come Laser Speed, Autoinit, o Superfast Finder, e molti giochi, tanto per fare qualche esempio, manipolano il System introducendo delle loro risorse in queste aree; perciò, cancellare solo quello che abbiamo elencato.

Questo discorso ci ha portato ad un problema, per così dire, di procedura. Poiché l'installazione di «Vaccine» o di «Antibiox» blocca qualunque attività appena si accorge che qualcosa sta modificando qualche applicazione, ci si ritroverà a lanciare, probabilmente, giochi o applicazioni, come quelle nominate che, per il motivo appena detto, stavolta andranno in bomba immancabilmente al lancio.

Ricordarsi, quindi, di quanto abbiamo appena detto, prima di iniziare, in questo caso, una caccia all'untore tanto inutile quanto vana.

Il System è, adesso, pulito. Ma siamo solo al primo passo, verso la distruzione della peste.

Ma, ancora una volta, lo spazio stringe; a risentirci tra un mese.