di Raffaello De Masi

Febbre da virus

Una panoramica sui virus presenti nel mondo Mac

prima parte

Mia nonna, grande saggia come tutte le nonne del mondo, (ero in terza media e mi aveva visto «studiare» troppo spesso con la mia compagna di banco) mi disse un giorno: «Stai attento, nipote mio, che presto o tardi se non è già successo, ti becchi un malanno che non va via con le medicine che vendono i farmacisti!». Cosa che poi puntualmente successe, e che per la verità ha avuto una serie innumerevoli di ricadute, tanto che mia nonna, che ormai è nell'altro mondo da venticinque anni, si sarà più volte chiesta come questo suo nipote dalla mole e dalle spalle di peso massimo si ammali così facilmente di questo male antico, che, meno male, non ha mai fatto male a nessuno!

A parte questa malattia ricorrente da cui, per la verità, non ho mai, comunque, sentito il bisogno di chiedere al Padreterno di liberarmi, la salute di ferro che finora mi ha accompagnato mi ha permesso di scorrere metà della mia vita (almeno lo spero, che sia la metà) senza neppure il classico raffreddore. Mal di testa, sì, e parecchi, per cause organiche, finanziarie, di lavoro, e così via, ma, nient'altro, anche se sono fortunosamente scampato a manicaretti di alta cucina della mensa universitaria e di quella militare! Ed ecco che una mattina accendo il mio amato Mac (all'epoca era un SE con una ventola che pareva uno Spitfire in picchiata) e mi ritrovo con una macchina incontrollabile che si rifiutava di aprire applicazioni, sparava bombe meglio di Rambo, e a un certo momento si puntò e non volle saperne di concludere più alcunché.

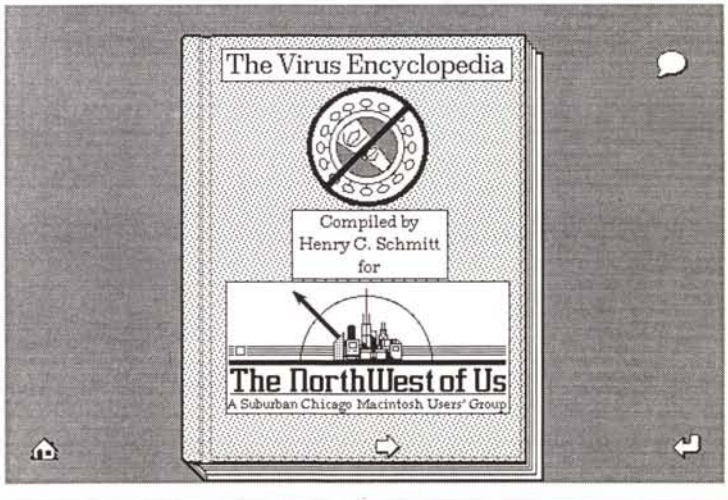
Era la fine dell'87 e, sebbene nel mondo PC avessi già sentito da qualche tempo parlare dei virus e dei problemi relativi, il mondo Mac, almeno il mio, ne era rimasto fino ad allora immune. Fortunatamente avevo a portata, da buona formica previdente, un antivirus, dal significativo nome di 'Assassin, fornitomi da un collega di lavoro, e, come si suol dire, per quella volta parai la botta; ma devo confessare che mi sono sentito in un certo qual senso defraudato come chi, non avendo mai posseduta un'automobile, si vede recapitare a casa una multa per divieto di sosta.

Fatte le debite ricerche nel mio archivio di dischetti scoprii che il focolaio d'infezione era in un dischetto di public domain, ricevuto da un collega universitario, e contenente alcune utility; costui avvisato cercò di risalire nella scala per capire la precedente provenienza, ma questa specie di catena di S. Antonio non portò ad alcuna conclusione.

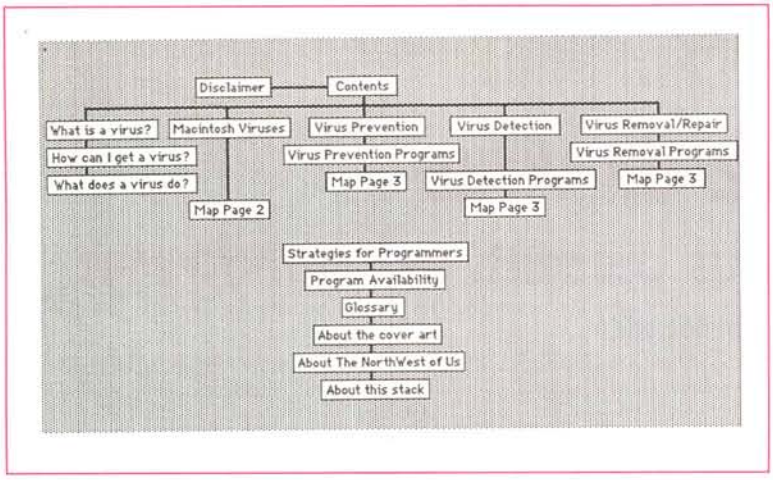
Il virus di cui risultai infetto era un nVir, lo ricordo con chiarezza; non era neanche tanto cattivo, visto che le applicazioni rifunzionavano di nuovo se appena uno era capace di giocherellare nelle risorse con il ResEdit; ma la cosa mi dispiacque soprattutto perché divenni senza colpa, l'untore dell'istituto, fama che ho faticato molto a scrollarmi di dosso. Ne ho approfittato per farmi una certa cultura nel campo delle infezioni tanto da essere divenuto, oggi, un po' il Pasteur dei miei amici. Ecco, in breve, quanto sono riuscito a mettere insieme in un periodo di tre anni!

Gli attrezzi dell'untore

Come si manifesta generalmente, su Mac, una infezione da virus? «Tot capita, tot sententiae», come dicevano i latini. Generalmente l'applicazione, nel bel mezzo del suo funzionamento, si «congela», si blocca, e per riutilizzare la macchina occorre resettare e ricominciare daccapo. Solo che questo difetto, per nostra fortuna (o sfortuna) non dipende solo da infezioni; spesso abbiamo sovraccaricato il sistema di font, FKey e DA, magari abbiamo giocherellato con il Multifinder, dimenticando che



La testata dello Stack «The Virus Encyclopaedia», un volume Hypercard, scritto da Henry Schmitt per un User Group di Chicago, che raccoglie, in maniera esauriente e ordinata tutte le notizie attualmente disponibili sul fenomeno virus. È uno stack «shareware», che, pur nella sua stringatezza, risulta esauriente e costruito con ordine e criteri informativi ben chiari. Il simbolo che compare sul libro è quello internazionale adottato nella lotta contro l'AIDS.



Un «albero» di analisi del fenomeno Virus, ricavato dalla stessa pubblicazione.

non è il pozzo di S. Patrizio, oppure abbiamo caricato più INIT dei missili del comandante Samarov in assetto di guerra su «Ottobre Rosso».

Un altro sintomo è la continua sbandata in bomba, con ID sempre diversi. Qui la diagnosi riesce ad essere più precisa e il probema più circoscrivibile se si considera che, generalmente, errori di malfunzionamento di una applicazione danno sempre lo stesso ID number, mentre una infezione da virus, per i motivi che diremo in questo stesso articolo e in quello del mese prossimo, possono dare, volta per volta, messaggi d'errore diversi.

Un terzo guaio è quasi sempre sintomatico di infezione; durante il lancio di una applicazione, il sistema si blocca e non dà più segni di vita o reazione; questo avviene anche con il System e ancora di più col Finder; nel primo caso compare il ben noto «Sad Mac» che, nelle ultime macchine, è accompagnato da un accordo in mi minore niente male! Una variazione sul tema è la difficoltà di stampa, soprattutto da parte di programmi di grafica e di spreadsheet; un'altra, più curiosa, è il ritorno al Finder quando si lancia una applicazione!

Ma qualunque sia il sintomo, una infezione da virus, specie se si dispone di un HD di discreta potenza, è cosa per lo meno seccante. Questo non tanto per il pericolo insito nella infezione stessa (come vedremo, nella maggior parte dei casi, non ci sono grossi problemi a liberarsi di questi ospiti sgraditi), quanto per il talora tedioso lavoro di esame e spulciatura di tutto il contenuto dell'HD; infatti, come prevedibile, occorre eliminare tutti, ma proprio tutti i residui virali dalla macchina per essere sicuri che, presto o tardi, il problema non si ripresenterà. Alcuni considerano i virus con occhio benevolo, come simpatici avversari con cui combattere e sui quali vincere; d'altro canto, poiché nella stragrande parte dei casi, i virus attaccano le applicazioni e non i file dati, sarebbe sufficiente rimpiazzare tutte le applicazioni infette per risolvere il problema! Ma si tratta di un lavoro seccante, a dir poco, e resta sempre il dubbio che l'operazione di pulizia non sia proprio stata fatta a dovere. Non sempre, poi, la cosa è fattibile; parlo della stupida protezione che certi programmi hanno, che consente un numero limitato di installazioni (spesso solo una) su HD. Così, quando, ad esempio, Excel o Word si ammala, siamo nei guai!

Macintosh e il suo software possono essere attaccati da tre categorie principali di agenti infettivi, che, pittorescamente (e anche con un occhio alle loro modalità di funzionamento) prendono il nome di cavalli di Troia, vermi e virus veri e propri. La differenza sta nelle modalità di attacco e di «funzionamento».

Molti utenti Macintosh ricorderanno, forse anche amaramente, uno stack HyperCard che ebbe una gran fortuna, anche in funzione del soggetto che trattava, Sexy Ladies (che, sicuramente in buona fede, fu distribuito per un certo periodo gratuitamente anche da un paio di organizzazioni di freesoftware). Mentre l'ignaro utente navigava tra immagini più o meno piccanti, una parte del codice provvedeva a cancellare settori su settori dell'HD. Questo è un esempio di cavallo di Troia.

Per definizione, quindi, un cavallo di Troia è un programma vero e proprio, caricato intenzionalmente dall'utente, ma che ha alcune funzionalità che restano nascoste all'utente fino a che se ne accorge a sue spese. Esso può fare di tutto; lanciare messaggi, mandare in bomba programmi, o cancellare informazioni. Ciononostante, almeno nella loro eccezione iniziale, non si propagano e, una volta localizzati e cancellati, l'azione di danno si blocca e scompare.

I vermi agiscono proprio come gli animaletti di cui portano il nome; si tratta di «pieces» di programma che scavano una strada nelle memorie; in pratica il programma cancella parti del disco rigido come un lombrico che scava nel terreno. Essi non abbisognano di un ospite (un programma su cui attaccarsi) per sopravvivere. Si tratta di una infezione poco nota su Mac; la più grave infezione, da parte di un verme (il tristemento noto Fall 1988) avvenne un paio di anni fa, quando una serie di macchine UNIX governative, legate in rete, furono infettate e parzialmente disabilitate nel giro di un solo giorno.

I virus sono la categoria più «cattiva» del gruppo. Essi sono generalmente costruiti con due finalità; quella di propagarsi e quella di fare qualcosa.

Il nome non è stato dato a caso. Quando un dischetto infetto viene lanciato, l'applicazione che contiene il virus passa nella memoria centrale e di qui si attacca, riproducendosi, ai file di sistema. Da questa posizione privilegiata domina la scena, incollandosi alle applicazioni che successivamente vengono lanciate, inserendo un codice «virulento» nel «resource fork» dell'applicazione stessa.

Fin qui, ancora nulla di pericoloso, anche se non può far certo piacere che, con le dovute differenze, un parassita, ancorché innocuo, ci si moltiplichi addosso. Ma qui subentra la seconda funzione, stabilita dal programmatore.

Il 2 marzo 1988, mercoledì, primo anniversario della nascita della serie II del Mac, molti utenti saranno rimasti stupiti, accendendo la loro macchina, di trovare un messaggio del tipo «Peace in the World». Il messaggio ricompariva ogni volta al reboot della macchina. Si trattava di un virus commissionato da Richard Brandow, l'editore canadese della rivista MacMag, ad un noto programmatore dell'Arizona, Drew Davidson, che si autocancellava dopo questa data senza dare più problemi. Ambedue gli autori dello scherzo (che poi di scherzo, peraltro di buon gusto, si trattava) non negarono mai, sotto alcuna forma, la paternità del virus (tanto è vero che Davidson lasciò il suo nome nel codice oggetto del programma). Addirittura Brandon (che aveva inserito il suo programma in una rete e lo distribuiva gratuitamente «agganciato» a una sua applicazione tramite una organizzazione di

«public domain»), sostenne, e non a torto che scopo del suo virus era quello di attrarre l'attenzione della comunità internazionale sui problemi dei virus stessi, visto che già in quel periodo il problema non pareva niente affatto trascurabile. Egli mostrò in diverse occasioni che il suo virus era del tutto innocuo e una volta, in una conferenza, sostenne anche che la paura da virus poteva essere senz'altro considerata un ottimo deterrente contro la pirateria.

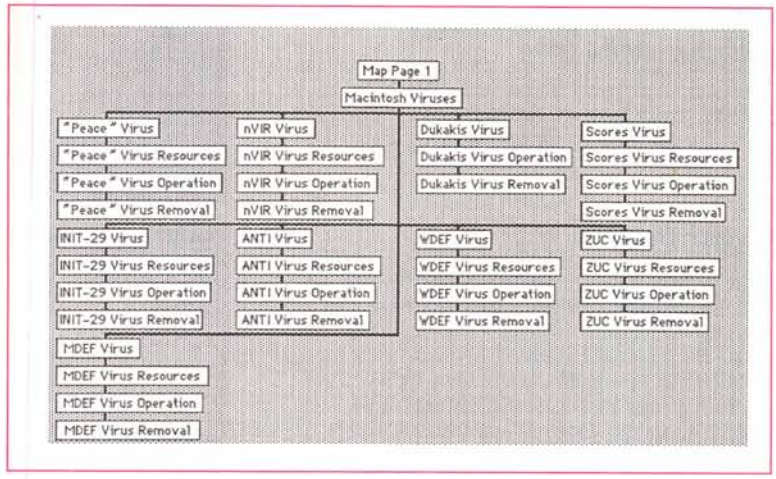
Addirittura una serie di copie di Aldus PageMaker furono distribuite infette da questo virus, ma la cosa non fu di soverchia preoccupazione; addirittura il problema, nonostante questa clamorosa dimostrazione di virulenza, fu inizialmente sottovalutato (come riferisce Mac World, in un articolo di Suzanne Stefanac, un redattore specializzato del Washington Post, T.R. Reid, scrisse, nella rubrica «Personal Computing» che «i virus non attaccano i personal computer»).

Visto che stiamo parlando di un fatto per così dire storico, vediamo come agiva; esso si insinuava nel sistema attraverso una applicazione infetta; entrava nel System e si installava come un INIT; bastava lanciare una applicazione su un dischetto perché l'INIT del sistema lo installasse su questa applicazione stessa e la trasformasse in veicolo per l'infezione (essa era, oltre tutto, poco evidente, visto che pesava solo 1.5K). La sua presenza comunque fu notata prima del fatidico 2 marzo, e i commenti della comunità Mac furono, sebbene il virus fosse del tutto innocuo, molto amari. Si parlò, allora, di alcune decine di migliaia di infezioni riconosciute; ma il numero è senz'altro molto inferiore alla realtà, visto che il virus diede vita al messaggio sugli schermi solo quel fatidico giorno, e si autocancellava anche non attivato già il giorno dopo.

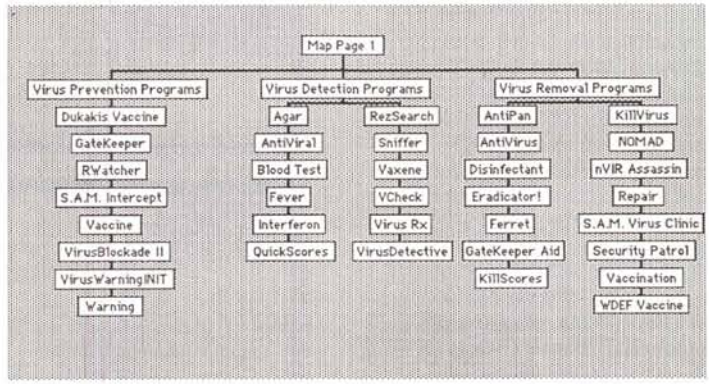
Ma questo è stato solo l'inizio. È la notizia (restiamo sempre nell'ambito Mac) che nel settembre 1988 membri del «Hamburg's Computer Club Chaos» infiltrarono in un network della NASA un virus; sebbene il club abbia sempre rifiutato qualunque addebito, l'arresto dell'esperto di virus del club lascia molte ombre sulla innocenza del gruppo. È un fatto, anche che immediatamente dopo la stessa Università di Amburgo fondò un centro di Analisi Virale, per combattere il fenomeno che cominciava a presentarsi in tutta la sua gravità.

Da qui il panico; ogni scoppio di bomba (che nel mondo Mac, per la verità, non sono mai mancate) faceva gridare all'infezione; questo, è la notevole ignoranza sull'argomento, seminò un'atmosfera da caccia all'untore che raggiunse limiti di paranoia (non era raro chi pensava che addirittura un virus potesse distruggere microprocessori e RAM). La cosa peggiorò quando si scoprì che esistevano diversi ceppi di virus, che agivano in maniera diversa e non erano riconducibili a uno stesso antidoto. Fortunatamente la comunità non era stata con le mani in mano e cominciarono a vedersi in giro prodotti efficaci, che non solo localizzavano, ma distruggevano l'agente infettante e spesso, recuperavano l'applicazione infetta.

Il virus della Pace nel mondo era un nVir, molto più difficili da localizzare e ben più cattivi si dimostrano i successivi Scores Virus (così chiamati per un file invisibile che il virus crea nel System Folder). Esso creò gravi problemi alla rete dei computer NASA (ben 120 macchine) che mostrarono i primi sintomi di infezione incontrando difficoltà nel lanciare e far funzionare MacDraw, nello stampare documenti così redatti e nell'utilizzare il pannello di sistema. La persona che per prima si accorse del problema, Dave Lovery, contattò immediatamente la Apple che dopo due giorni di lavoro isolò e classificò il problema stesso. Lovery, dopo la disinfezione della rete, scrisse un articolato resoconto del fatto (i tecnici Apple avevano stabilito che l'infezione era arrivata attraverso software importato da un bullettin board) e lo spedì alle più estese reti nazionali. Impose, inoltre, che tutto il software inserito nella rete NASA fosse tenuto in «quarantena» per un certo periodo. Howard Hupcurch (autore, tra l'altro di alcuni splendidi caratteri per laser) e la Apple Corps di Dallas ripresero l'articolo di Lovery, ampliandolo e aggiornandolo, tanto che oggi è considerato una specie di bibbia sul problema.



La mappa dei virus Mac attualmente presenti nella comunità.



Una mappa delle tre famiglie di antivirus disponibili attualmente, suddivise nelle tre tipologie di intervento che esse coprono.

I tipi di virus presenti oggi nella comunità Mac

Esistono almeno undici famiglie principali di virus tuttora circolanti sul mercato; vediamo le caratteristiche di alcune di esse.

Il virus Scores

Gli Scores virus; li abbiamo già nominati. È stata dimostrata la provenienza del ceppo da una sotware house piuttosto nota. Infatti esso attacca immediatamente due applicazioni che, nel periodo compreso nella prima metà dell'88 erano in fase di avanzata realizzazione (le applicazioni, poi, non sono mai state messe in vendita). Le prime testimonianze della sua comparsa sono da riferire alla primavera dell'88; variazioni sul tema sono i virus «Eric», «Vult», «NASA», e «San Josè Flu».

Nonostante l'alta virulenza gli Scores virus hanno un tallone d'Achille molto esposto. Una infezione da Score è individuabile facilmente aprendo la cartella sistema e esaminando i file Appunti e Archivio Appunti. Normalmente essi sono rappresentati da icone di piccoli Mac; se invece essi presentano la generica icona a foglio bianco con l'angolo ripiegato (in inglese, molto pittorescamente, «blunted ear dog»), ci sono problemi! Il software è probabilmente infetto! Occorre un accertamento più da vicino. Per fare ciò bisogna disporre di un editor di file nascosti (come ResEdit, Resource Editor, Mac Tools, Mac Copy II o altri). Scores virus crea infatti due nuovi file, invisibili, «DeskTop» e «Scores», da cui il nome. Si noti che il primo non ha nulla a che vedere con l'omonimo file di sistema; tanto per chiarire la differenza DeskTop (buono) è un file che risiede nalla root del disco, l'altro (che si riconosce per avere un carattere di spazio, invisibile, alla fine del nome) vive attaccato al System. Scores non infetta mai documenti, solo il software di sistema e le applicazioni (e nemmeno tutte: alcune restano del tutto immuni, altre, come MacDraw e Excel, sono le vittime preferite).

Il meccanismo di azione di Scores è ben noto; esso risiede inattivo nel system per due giorni dopo l'infezione (potremmo dire che resta in incubazione), poi, allo scadere esatto del secondo giorno, si risveglia e, a intervalli di tre minuti circa, parte alla ricerca di una applicazione sterile (è questo il motivo dell'interferenza con processi di stampa). Al ritrovamento esso installa una risorsa di tipo Code di 7026 byte nel secondo slot libero delle risorse.

Immediatamente dopo il virus inserisce un codice adatto nella tabella dei salti contenuti nel Resource Code ID 0, all'undicesimo posto (che abitualmente contiene l'indirizzo del secondo segmento di codice). Qui il virus, con il nuovo codice, provvede a deviare il flusso del programma allo slot di risorsa precedentemente realizzato; dopo di ciò il gioco è fatto è il virus, senza che l'utente se ne sia accorto, restituisce il controllo al programma.

Quattro giorni dopo l'infezione iniziale il virus si riattiva, andando a cercare file e programmi con sigla di identificazione Eric e Vult. Esso non si attacca al programma, ma lo lascia funzionare per 25 minuti, poi lo manda in bomba (è questo il motivo per cui sembra che la stessa applicazione a volte funzioni, a volte no). Al settimo giorno il virus accorcia i tempi e, dopo aver atteso per 15 soli minuti, manda in bomba il programma appena si tenta di scrivere su disco.

Sebbene il virus non tenti di attaccarsi ad applicazioni diverse da quelle con gli identificatori appena nominati, esiste un altro danno indiretto che, possiamo dire, determina involontariamente; il fatto che si moltiplica incollandosi addosso alle applicazioni determina inevitabilmente delle sovrascritture su file attigui. Ancora, esiste una profonda incompatibilità tra Scores e i sistemi operativi pari o superiori al 6.0.4, nei quali Apple ha iniziato ad utilizzare risorse di tipo simile a quelle adottate da Scores. Quando il virus infetta il file di sistema, alcune versioni delle risorse proprie dell'Apple sono sostituite da quelle specifiche dell'infezione. In questo caso, sovente, il sistema stesso si rifiuta di partire.

◀ *Una serie di pagine dello stack nominato; ogni scheda è dedicata a un virus e al modo con cui liberarsene. Sebbene non si entri nelle specifiche tecniche delle singole infezioni, i consigli forniti sono facilmente attuabili disponendo semplicemente di un Resource Editor come quello distribuito dalla Apple o quelli disponibili, quasi sempre, come freeware presso le organizzazioni di «public domain».*

Il virus nVir

Il primo virus di questa specie fu isolato in Europa nel 1987 e negli Stati Uniti nel 1988. Di questo ceppo se ne conoscono due rami principali, nVir A e nVir B. Pare che addirittura ne esistesse una terza versione, la più vecchia, che però non è stata mai esaminata a fondo e di cui si sono perse addirittura le tracce.

nVir è più semplice e, potremmo dire, più rozzo di Scores. Ciononostante è molto più difficile da localizzare. Sia il file appunti che l'archivio non sono attaccati o modificati, né viene creato alcun file invisibile. Non esistono tempi di incubazione; appena trasmesso nVir comincia ad attaccarsi e ad infettare le applicazioni appena queste vengono lanciate; anche qui alcune applicazioni appaiono praticamente immuni dal contagio mentre altre, come Excel e Filemaker divengono inutilizzabili già al secondo lancio. Il Finder e DA Handler sono quelli più esposti. Anche qui i documenti non sono attaccati né modificati.

Esiste comunque un meccanismo di ritardo che permette al virus di propagarsi in gran copia prima di mostrare la sua presenza; esso è articolato in maniera semplice, ma efficace. Appena entrati in un sistema gli nVir infettano tutto quello con cui vengono a contatto, senza dare alcun segno della loro presenza.

Quando il file di Sistema viene raggiunto (generalmente è uno dei primi) un contatore viene settato a 1000; il contatore è decrementato di 1 ogni volta che viene lanciato il System e decrementato di 2 ogni volta che una applicazione infetta viene lanciata.

Quando il contatore giunge a zero, compare sullo schermo una scritta del tipo «Dont't Panic» se AppleTalk è settata; nel caso contrario si ha solo un beep. Questo avviene anche allo startup con una probabilità di 1:16. Dopo di ciò lo stesso avviene anche lanciando una applicazione infetta, con una probabilità di 15/128; infine, giusto per non essere complicati, la scritta appare due volte di seguito con una probabilità di 1/256. Questo avviene generalmente con nVir A; il tipo B esegue più o meno le stesse cose, ma non chiama in causa AppleTalk.

La cosa più curiosa, in tutto questo, è che i due ceppi, A e B, possono coesistere nello stesso sistema e dare origini a varianti che recuperano parte del codice dall'uno e dall'altro virus, con caratteristiche imprevedibili. Purtroppo, come dicevamo, non è semplice individuare una infezione latente o parzialmente in atto, in quanto, a differenza di Scores, non esistono segni esteriori del male che si sta diffondendo (come le icone guaste di Scores). Occorre, per un utente esperto, lavorare un poco con ResEdit e cercare nel sistema una risorsa del tipo nVir (da cui il nome).

Si conoscono almeno 6 cloni del ceppo nVir. Essi sono tutti simili all'nVir B, con eccezione di alcune piccole differenze.

Il virus INIT 29

Esso prende il nome da una risorsa di tipo INIT che crea nel sistema, e da una ID resource number n° 29.

Si tratta di uno dei virus più vecchi, visto che è comparso all'inizio dell'88. Non se ne conoscono le origini. Si tratta di uno degli agenti più feroci e virulenti, visto che si attacca alle applicazioni in maniera velocissima; a questo si aggiunge il fatto che, al contrario di quelli precedenti, non è necessario lanciare una applicazione perché questa sia infetta. Inoltre INIT 29 può infettare qualunque file, non solo di sistema o applicazioni, ma anche documenti; in quest'ultimo caso però, non sono contagiosi.

Esiste un metodo molto efficace per localizzare la presenza di questo agente. Tentando di inserire un dischetto protetto in scrittura in una macchina con System infetto si ottiene la ben nota finestra di «alert»:

Il disco "AAAAA" ha bisogno di riparazioni minori; desideri procedere?

decisamente in contrasto con la presenza del floppy protetto; ci sono, decisamente, ottime possibilità di avere un sistema infettato da INIT 29.

Come nel caso precedente, INIT 29 non procura intenzionalmente danno, tranne quello di moltiplicarsi a spese dello spazio libero su disco. I risultati possono comunque essere disastrosi; generalmente i danni si manifestano con bombe di sistema, difficoltà di utilizzo del Multifinder (uno dei mezzi diagnostici più efficaci) e incompatibilità con programmi e documenti di startup.

Il virus ANTI

L'autore di questo virus ha incluso, come se fosse una firma, la stringa ANTI nel sorgente, da cui il nome di questo agente infettivo.

Si conoscono due ceppi diversi di virus di questo tipo, ambedue scoperti in Francia; quello di tipo A diede segno di sé inizialmente nel febbraio dell'89, il secondo, il "B" è recentissimo, essendo stato segnalato inizialmente nel settembre del '90.

Al contrario della gran parte dei virus presenti, esso non infetta il System file, ma solo applicazioni o file che funzionano da applicazioni (come il DeskTop e il Finder). Non colpisce, come la maggior parte dei suoi simili, i documenti. È meno virulento del precedente, ma la sua pericolosità non gli è da meno, avendo la capacità, finora ignota, di attaccarsi anche ad applicazioni senza che queste siano state lanciate. A causa di una particolare sua struttura interna, ANTI perde qualsiasi potere se la macchina funziona in Multifinder.

ANTI è ancora pericoloso in quanto determina vere e proprie modifiche nell'applicazione attaccata; questo vuol dire che, anche se riparata con i più efficienti disinfettanti in commercio, l'applicazione non sarà identica a quella precedente e potrebbe, in certi casi particolari, creare problemi (difficoltà di stampa e bomba quando si tenta di salvare il documento). Questo ultimo difetto impone di cancellare del tutto l'applicazione, quando scoperta «ammalata» e di sostituirla con una nuova.

Per essere precisi, occorre rilevare che il danno determinato da ANTI è rappresentato dalla distruzione degli attributi numerici contenuti nelle risorse CODE 1. I disinfettanti in commercio, ovviamente, non possono conoscere i valori originari per tutte le applicazioni presenti sul mercato; i difetti che si verificano, comunque, sono rari, e rappresentati quasi sempre da una non corretta gestione della memoria; essi sono più frequenti con le macchine dotate di ROM da 64 e 128K.

Ancora, un particolare curioso; il virus B neutralizza il virus A, quando ambedue sono presenti sullo stesso HD.

Il virus MacMag (detto anche Peace Virus)

La storia di questo virus è già nota; si tratta di uno dei più vecchi, avendo origine già nel 1987. Esso è anche conosciuto come «Drew», «Brandow», Aldus (per aver infettato numerose applicazioni originali di PageMaker) e «Peace».

Esso, lo abbiamo accennato, infettava solo il System, per una sola volta, quando veniva lanciato uno stack Hypercard, prodotto dalla redazione di Montreal di MacMag Magazine. Questo stack conteneva solo alcune immagini digitalizzate, di scadente fattura dell'allora non ancora presente sul mercato scanner della Apple.

Quando lo stack veniva lanciato il virus si attaccava al System e di lì si incollava a tutti i dischetti contenenti un System che successivamente venivano utilizzati su quella macchina.

Incollandosi solo sul System e solo per una volta, MacMag si diffondeva piuttosto lentamente, anche perché è ben difficile che chi scambia dischetti inserisca in essi anche il sistema operativo. Il fatto che il virus sia stato progettato per fini non distruttivi è dimostrato dal fatto che esso non si propaga nemmeno attaccandosi ad altri stack Hypercard.

Esso non ha mai avuto una grande diffusione, sia per i motivi predetti, sia perché programmato per autodistruggersi il 2 marzo del 1988. Oggi ha solo valore e significato storico, visto che è ben raro che esista un disco che da date precedenti a quella indicata non sia stato utilizzato. L'effetto era di mostrare un messaggio di pace, lampeggiante, sullo schermo, per qualche secondo.

Il virus Dukakis

Visto che ci troviamo a parlare di stack e di Hypercard, accenniamo ad un virus poco diffuso passato come una meteora nel mondo Mac. Scritto interamente in linguaggio HyperTalk, attacca solo stack Hypercard, ma non applicazioni né il System. Si tratta di un virus più seccante che dannoso; quando uno stack infetto viene lanciato, l'handler «OpenStack» mostra sullo schermo un messaggio del tipo «Dukakis for President». Lo script corrispondente è presente a livello dello stack «Home» da cui si propaga agli altri stack.

Si tratta di un virus che non procura alcun danno alle applicazioni e ai documenti, e inoltre è molto semplice da eliminare. Occorre agire a livello 5 di Hypercard (Scripting) leggere nello stack infetto lo script specifico del virus, che inizia con il comando «on OpenStack» e cancellare tutto il codice del virus (che, ad onor del vero, è ben commentato e individuabile). Occorre fare questa operazione per tutti gli stack presenti sul disco; è tutto.

In Italia, a quanto ci risulta, non è stato mai segnalato.

Il virus WDEF

Questo virus è stato isolato per la prima volta nel dicembre 1989 in Belgio. Si tratta di un virus piuttosto rozzo e semplice nel suo meccanismo d'azione, ma dalla eccezionale virulenza. Esso attacca solo il «DeskTop File», invisibile, presente sulla scrivania. È molto interessante in quanto non si propaga attraverso lo scambio di applicazioni, ma solo attraverso quello dei dischetti; così anche il semplice passaggio, da una macchina all'altra, di un disco già inizializzato (e quindi già contenente il DiskTop File) può essere fatale. Esso, quindi non si propaga attraverso l'uso di reti.

Se ne conoscono due varianti principali; WDEF A e B; la sola differenza è rappresentata dal fatto che nel primo caso il sistema lancia un beep quando il DeskTop File viene infettato (potrebbe essere un mezzo diagnostico, ma chi ci fa caso?), nel secondo ciò non avviene, sebbene non sia intenzionalmente distruttivo, WDEF provoca diversi danni e problemi; sulle macchine IIci e IIfx e sul portatile si ha un crash di sistema appena si tenta di lanciare un disco infetto (ivi compreso quello di boot). Ma anche sulle altre macchine il fenomeno è abbastanza frequente e nei casi più gravi può portare alla parziale o totale illegibilità della memoria stessa (il recupero è abbastanza facile, comunque, con mezzi adatti, come Norton Utilities o Disk 1st Aid). Altro problema frequente è la scarsa leggibilità dei caratteri sullo schermo (specie sul portatile) e problemi di stampa con macchine PostScript. Ma diversi altri problemi sono stati riferiti, come scambio di lettere sulla tastie-

ra, o forma strana assunta dal cursore, cosa che prelude ad un quasi immediato crash di sistema.

Usare un disinfettante è abbastanza utile, ma esiste un metodo diretto e semplice che mette al sicuro dall'infezione da questo virus; esso consiste nella periodica ricostruzione del DeskTopFile, cosa che come tutti sanno si esegue tenendo, al boot, premuti contemporaneamente i tasti di Option e Command e seguendo le successive istruzioni. WDEF non si propaga attraverso AppleShare, in quanto gli utenti di questa rete non utilizzano nelle ordinarie operazioni il loro DeskTop File, ma quello del gestore della rete; ciononostante se questo ha permesso l'opzione «make changes» alla directory radice del server, ogni utente infetto del server può a sua volta infettare il DeskTop file del server stesso.

È questo il motivo per cui i gestori di rete AppleShare impediscono agli utenti del network di utilizzare il privilegio di operare cambi alla root. È invece appurato che il virus non si può attaccare da un server di rete ad altri Mac collegati sul network.

Se la rete è gestita attraverso l'uso di Tops, l'infezione può avvenire attraverso lo scambio del DeskTop pubblico, ma solo dal cliente al server; non sono stati segnalati casi di infezioni in senso inverso.

Infine, su questo virus poco pericoloso, una curiosità; utilizzando il ResEdit per scandagliare le intime viscere dei programmi non è raro il caso di trovare risorse del tipo WDEF in file diversi dal DeskTop; si tratta di un tipo di risorsa quindi prevista anche in altre applicazioni; quando la loro presenza non è nel file di scrivania, non deve allarmare (anzi, azioni sterilizzanti a carico di queste risorse possono portare alla inabilitazione del programma stesso).

Il virus ZUC

Gli italiani, popolo di santi poeti e navigatori, non poteva non distinguersi anche in questo campo; questo tipo di virus fu per la prima volta scoperto in Italia da un prete, Don Ernesto Zucchini (da cui il nome). Fu scoperto nel marzo del 1990, infetta applicazioni ma non Sistema o documenti. Esso è regolato per entrare in funzione dopo il 2 marzo, o dopo due settimane da quando l'infezione è avvenuta. Prima che ciò avvenga, il virus si attacca da applicazione ad applicazione (non è necessario lanciare un programma perché si infetti). Dopo tale periodo di incubazione, circa 90 secondi dopo il lancio dell'applicazione infetta, il cursore assume una forma diversa quando il bottone del mouse è schiacciato. Inoltre si muove diagonalmente sullo schermo cambiando continuamente direzione e rimbalzando contro i bordi come una palla da biliardo. L'effetto sparisce quando il tasto del mouse viene rilasciato, ma diviene fisso se si clicca 3 volte di fila.

L'effetto del virus è simile a quello di un vecchio DA, «Bouncing Mac» che aveva il compito di prevenire bruciature dello schermo. Inoltre cambia in maniera strana e imprevedibile lo sfondo della scrivania, e i tempi di accesso stranamente lunghi e una prolungata attività della memoria di massa quando si lancia una applicazione. Inoltre può attaccarsi da un utente al server di rete e da questo agli altri utenti collegati. Nonostante questa notevole attività, gli unici effetti rilevati sono quelli descritti, ed è ben raro che si rovinino applicazioni o file in maniera irreparabile. Onore al merito del realizzatore, ZUC non cambia la data dell'ultima modifica al programma (visibile nella finestra informazioni) per cui è ben difficile rintracciare la fonte e il momento della infezione stessa.

Il virus MDEF

Virus dalle conseguenze leggere, ha tre varianti principali; le prime due furono scoperte alla Cornell University di New York e denominate forma A e B (la fantasia non è il forte del mondo Mac). La prima diede segno di sé nel maggio '90 e la seconda nel successivo agosto; sono anche note nel mondo Mac come «Garfield Virus» e «TopCat». La terza, MDEF C fu scoperta all'High Scool di Ithaca nell'ottobre del '90.

Una efficiente azione della «Computer Security» della sezione di polizia dello stato di New York portò alla identificazione dell'autore del virus, un ragazzo di quattordici anni, che dopo un processo rapidissimo fu condannato (secondo una di quelle condanne curiose ed esemplari tanto frequenti nella giustizia americana) a non possedere calcolatori e a non toccare una tastiera per tre anni, sotto la diretta responsabilità dei genitori. Successivamente si scoprì che egli era anche autore del virus CDEF (di cui discutiamo in seguito).

MDEF infetta applicazioni e System file, e, con minore frequenza, documenti e file di scrivania. L'infezione avviene solo se l'applicazione viene lanciata o il documento aperto. Anche qui il System è infettato per primo.

Come dicevamo precedentemente, MDEF non produce grandi disastri, visto che, intenzionalmente non produce altro danno che quello di attaccarsi alle applicazioni. Ciononostante è molto ben progettato visto che riesce a bypassare numerosi INIT di protezione contro le infezioni. Un esempio è Vaccine, un ottimo programma antivirus, che riesce a bloccare l'azione di MDEF impedendo l'attacco alle applicazioni, ma MDEF e Vaccine interagiscono conflittualmente tra di loro, disastrando il System; questo «perde» completamente i menu, cosa che può essere un efficace strumento diagnostico.

Il nome di questo virus proviene da risorse che esso crea nelle applicazioni infette; anche qui c'è da notare che usando ResEdit si possono trovare risorse di questo tipo che non hanno niente a che fare con infezioni o altro. A vantaggio dell'«utente» è il fatto che MDEF Virus è uno dei più semplici da eliminare con disinfettanti presenti sul mercato.

Il virus Frankie

Si tratta di un agente di piccolo cabotaggio, presente da diversi anni e pochissimo diffuso; esso funziona solo su alcuni emulatori Mac, come quelli disponibili per Amiga e Atari. Non colpisce né infetta macchine Macintosh.

L'effetto prodotto è per lo meno curioso; dopo che l'infezione è avvenuta, il sistema va in bomba e compare una finestra di messaggio con la fase: — Frankie says: «no more piracy» — sempre sugli emulatori. Franckie si attacca sia alle applicazioni che sul System; infetta altresì il file DeskTop; funziona solo sotto Finder.

Il virus CDEF

Scoperto nell'agosto del 1990 è stato scritto dalla stessa persona responsabile del virus MDEF, e ad esso è molto simile negli effetti (colpisce il DeskTop). Ciononostante il suo progetto è del tutto originale, e i suoi effetti sono anche meno disastrosi di quelli, ben modesti, di MDEF, non essendo stato disegnato per produrre altro danno che quello di attaccarsi alle applicazioni. Il suo nome è dovuto al tipo di risorse che crea nel System, anche se queste sono proprie del sistema operativo originale del Mac. Perciò, anche in questo caso, attenzione a togliere indiscriminatamente questo tipo di risorsa.

Termina così la prima parte di questo articolo dedicato al gran contagio che ha colpito il mondo del silicio e anche il mondo Mac. La prossima volta vedremo quali sono i mezzi che la moderna medicina, pardon informatica, mette a disposizione per riportare in buona salute il «melone»; a risentirci.

MS