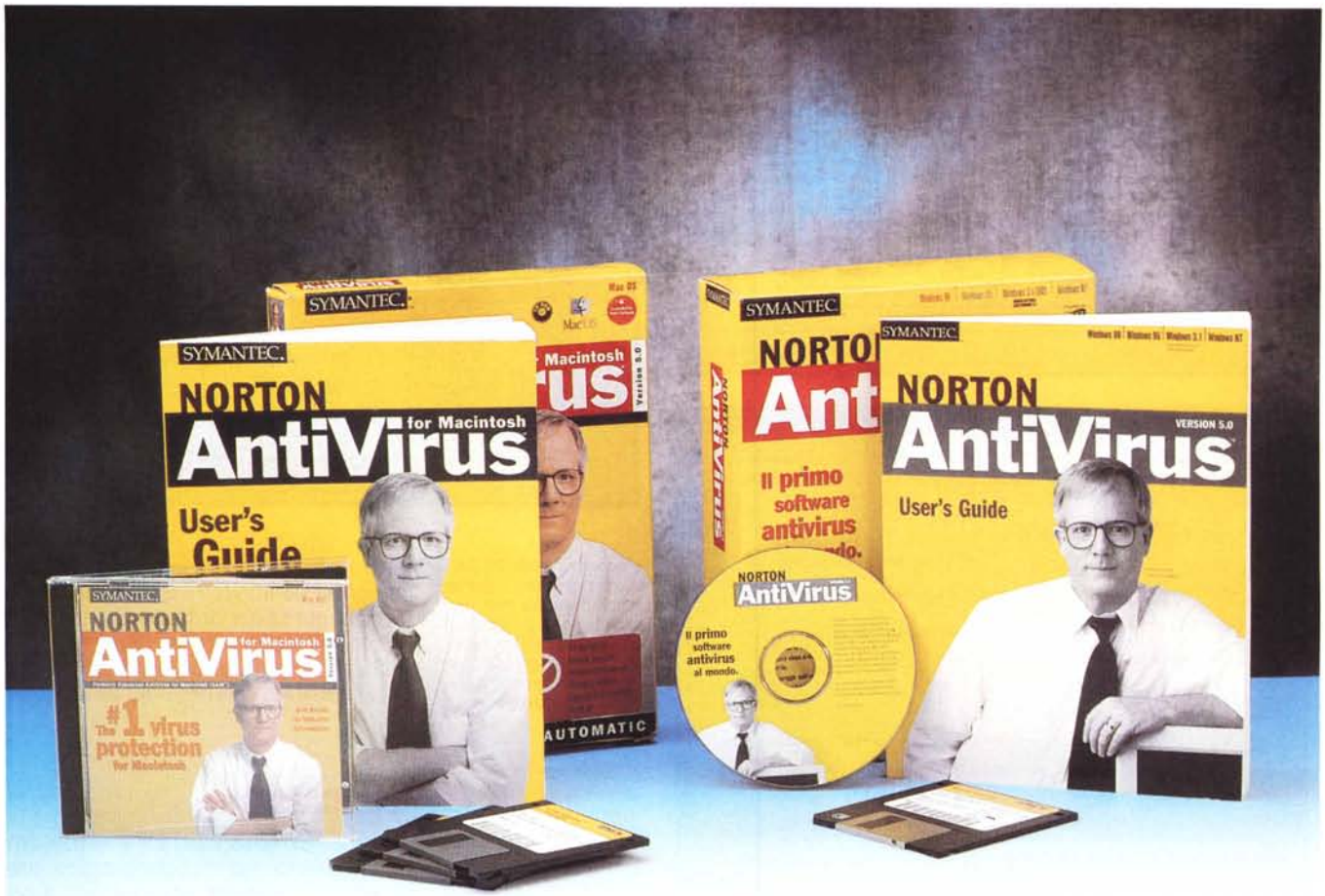
di Raffaello De Masi



Norton Antivirus 5.0

per Windows 95/98 e Macintosh

Che fare quando la salute se ne sta andando? Gli sciamani applicano un unguento protetto da un loro copyright, i medici prescrivono un buon antibiotico, la mia vecchia mamma mi preparava le pezzuole di flanella, il mattone sotto il fuoco e il miracoloso decotto di malva e miele, e io, per non essere da meno, ho la mia ricetta miracolosa: pasta e fagioli con le cotiche e salsicce con patate al forno. Difficile stabilire quale funzioni meglio, ma io sono sempre del parere che mammà non sbagliava mai e che la mia medicina, come tutte quelle alternative, almeno ha il pregio d'essere naturale e di non portare danni, tranne alle coronarie.

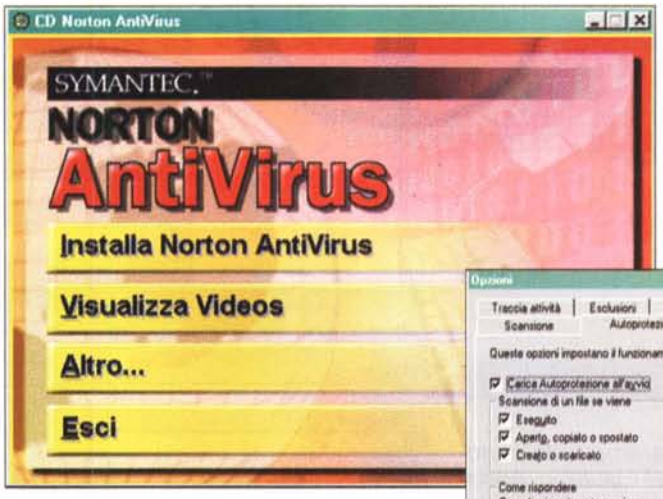
Una sera, comunque, ci rendiamo conto che qualcosa, nel nostro computer, non va! E' tutta la giornata che lo abbiamo visto distratto, insonnolito, risponde ai comandi con svogliatezza, talvolta si addormenta senza motivo. Gli mettiamo la mano in fronte, sia esso un Pc o un Mac, e ci rendiamo conto che scotta. Passerà, diciamo, e dopo poco rinunciamo a pensare; ma la notte un dubbio atroce ci assale, e torniamo dal nostro amato "capoccione"; la febbre non è passata per nulla, anzi le condizioni di malessere sono più evidenti; il nostro amato parla a vanvera di cose sconclusionate, con Yahoo! che, colto da un improvviso assatanamento, è saltato addosso ad Altavista (tanto caruccia e perbene, poverina) con intenzioni a dir poco

Norton Antivirus 5.0

Produttore :
Symantec Corp.
10201 Torre Avenue
Cupertino, CA 95014
http://www.symantec.it

Distributore:
Symantec Italia
Via Abadesse 40
20124 Milano - Tel. 02/695521

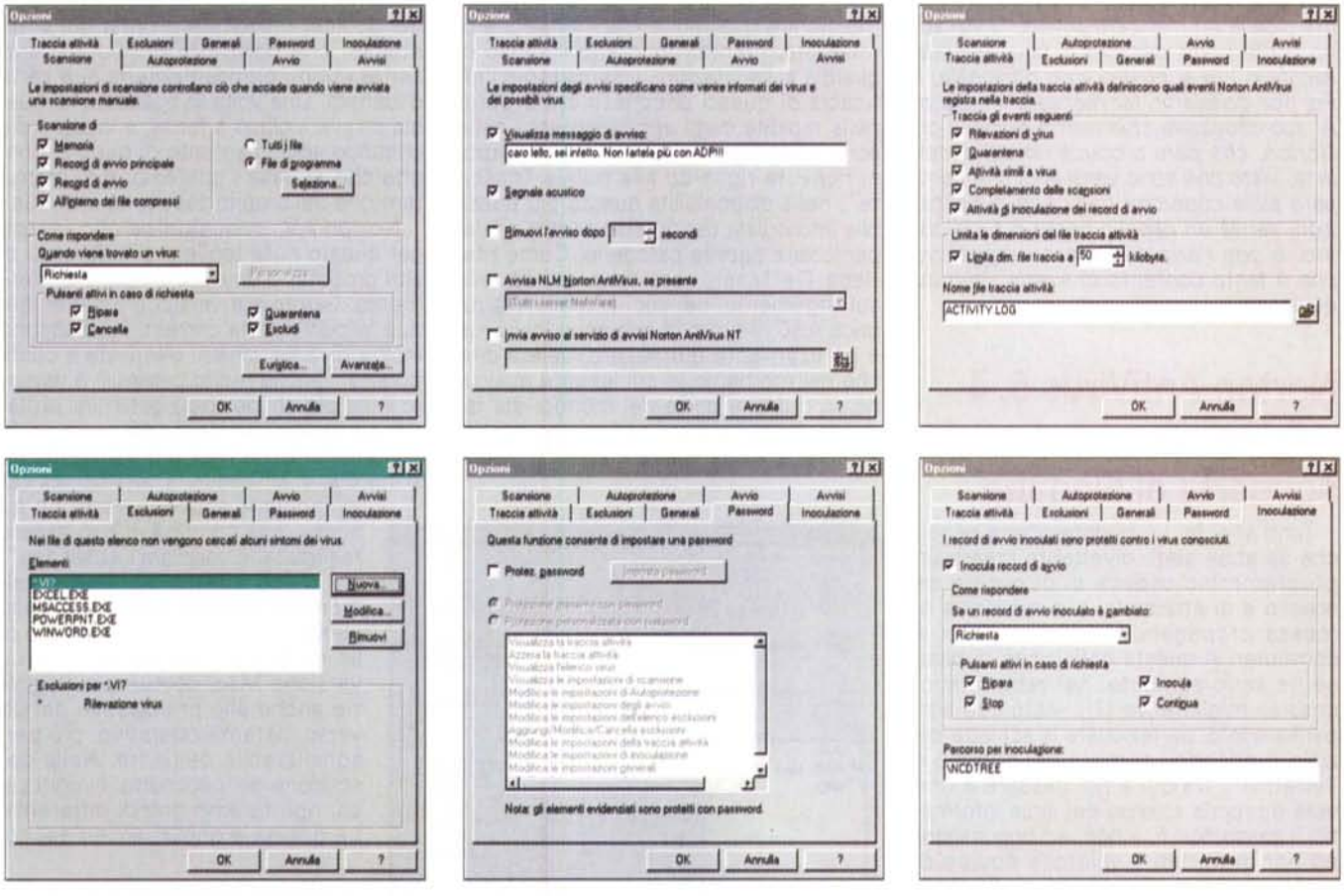
Prezzi al pubblico (IVA esclusa):
Retail Edition W95/W98/W3.1/WNT
L. 119.000
Professional Edition Win & Mac
L. 162.000



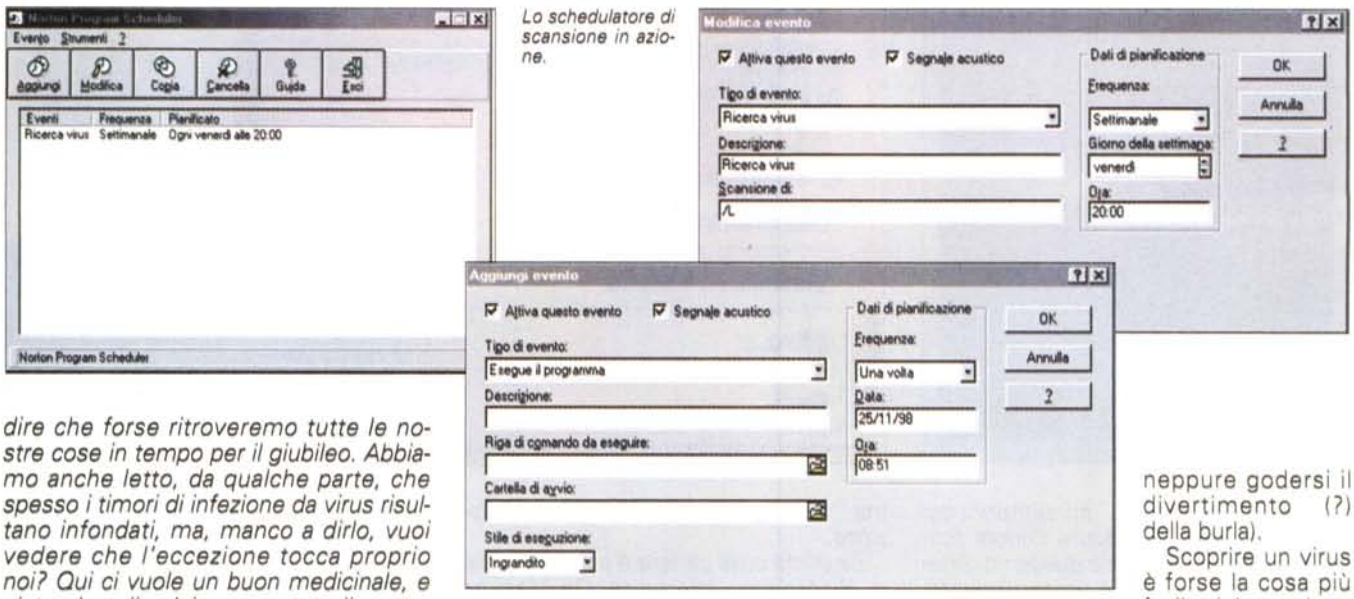
La fase di installazione del pacchetto.

irriferibili (valli a capì, 'sti signorini col punto esclamativo); oppure Eudora scrive, per conto suo, di fila duecento lettere d'amore a Naomi. A un certo punto, ad onta delle pezzuole fredde, l'amato bene cade in collasso, con perdita, per le vie basse, di bit maleodoranti. Insomma, 'sto disgraziato si è beccata un'infezione.

La prima cosa da fare è correre ai ripari. Ricordiamo che un tal De Masi ha scritto qualcosa sull'argomento sulle pagine di MC, ma la signora moglie ci ha messo la scrivania a posto e questo vuol



Alcune delle finestre di opzione disponibili; si noti come sia possibile disattivare l'autoprotezione, selezionare le aree di quarantena, escludere certi file dalla scansione, impostare password di protezione dei setup, eseguire operazioni di ricerca di inoculazione.



Lo schedulatore di scansione in azione.

dire che forse ritroveremo tutte le nostre cose in tempo per il giubileo. Abbiamo anche letto, da qualche parte, che spesso i timori di infezione da virus risultano infondati, ma, manco a dirlo, vuoi vedere che l'eccezione tocca proprio noi? Qui ci vuole un buon medicinale, e visto che, di salsicce e patate il nostro PC ne ha voluto un solo boccone, che ha immediatamente risputato, ci vuole un rimedio chemioterapico, anzi per meglio dire bitoterapico. Ovviamente, come diceva un mio caro amico, "i vizi sono come i figli, per loro si fa qualunque sacrificio"; e al nostro vizio principale, il Pc, non possiamo far mancare il meglio. Al suo capezzale chiamiamo quindi il dr. Norton, che pare produca rimedi eccellenti, visto che sono venti anni che compare sulle copertine delle sue pubblicazioni senza un capello perso o fuori posto, e con l'aria dell'eterno ragazzino che è tanto contento di averci venduto qualcosa.

Norton AntiVirus 5, il miglior rimedio dopo la scoperta di Fleming

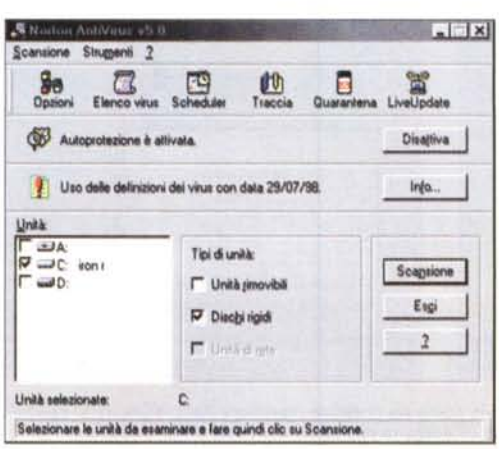
Tanti anni fa, un buontempone pensò che sarebbe stato divertente creare un programmino capace di duplicare se stesso e di attaccarsi alle memorie di massa propagandosi da computer a computer. A questa definizione di base se ne sono aggiunte, nel tempo, successive migliorative (?!), visto che altri pensarono di perfezionare la schiatta iniziale rendendoli sempre più subdoli e "infettivi". Da qui a poi passare a una vera e propria scienza dei virus informatici il passo non fu lungo, ed oggi esistono fior di trattati e valorose équipe di professionisti impegnati a combattere strenuamente i sempre nuovi rampolli, che ennesimi buontemponi continuano a sfornare a piene mani.

Frutto di questo sforzo è la disponibilità di prodotti d'elevato livello qualitativo che, grazie ad uno sforzo costante nel monitorare qualunque manifestazione di morbilità, mantengono alto il livello di guardia sulle infezioni. Il successo e l'efficacia di questi pacchetti sta proprio nella rapidità degli aggiornamenti, nella completezza giornaliera delle informazioni ricevute riguardo alle nuove "nascite", nella disponibilità quanto più possibile immediata del rimedio adatto a quel particolare agente patogeno. Come riferisce De Masi, vero faro del sapere sull'argomento, nei suoi articoli nella rubrica ABC, il ritmo di comparsa dei virus è praticamente giornaliero, vale a dire che nel momento in cui leggete qualcuno, in qualche parte del mondo, sta facendo il debug di un codice che servirà a danneggiare la vostra macchina (senza neppure godersi il divertimento (?) della burla).

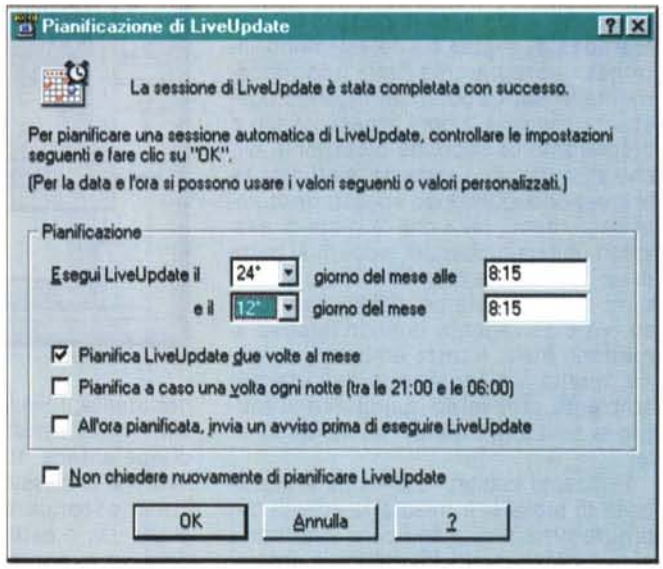
Scoprire un virus è forse la cosa più facile del mondo, a patto di conoscerlo e saperlo individuare. Per questa seconda bisogna ecco che occorre individuare una stringa identificativa, vale a dire una sequenza ASCII del codice, univoca e propria del virus stesso, che permetta di riconoscerlo senza dubbi, praticamente la sua carta d'identità. Una volta in possesso di questa chiave il gioco è facile; e infatti è sul continuo aggiornamento di queste stringhe che si basa l'operazione di manutenzione del proprio pacchetto antivirus.

Norton AV, in questo campo, senza per questo nulla togliere all'efficienza di altri prodotti, è davvero il punto di riferimento. Giunto alla versione 5 per ambedue le piattaforme correnti (ne esistono inoltre diverse varianti destinate a configurazioni anche molto dissimili) è davvero il top per chi desidera garantirsi protezione e rapidità di intervento.

Come funziona NAV è presto detto; lo si installa, in ambedue le versioni, da CD (disponibile anche la versione su floppy, che comunque può essere realizzata in maniera "casalinga") e il gioco è fatto. Fondamentalmente le versioni funzionano nello stesso modo, in quanto godono di un motore pressoché identico. La versione Mac, comunque, è, grazie anche alle prerogative del diverso sistema operativo, più personalizzabile dell'altra. Nella descrizione del pacchetto, in ogni caso, non faremo grandi differenze tra questa e quella, anche se, co-



La finestra di gestione delle attività di NAV; si noti il pulsante per mettere in quarantena file sospetti.



Live Update al lavoro; l'operazione va eseguita il più frequentemente possibile, prima che sia troppo tardi.

me si vedrà, certe implementazioni Mac meriteranno, talvolta, un maggiore approfondimento.

Le funzionalità fondamentali di NAV, partendo dal principio che esso è capace di eseguire operazione di prevenzione e di cura, si basano su due ambienti fondamentali: verifica continua e monitoraggio discreto ma costante dell'ambiente d'uso, alla ricerca di anomalie dovute a probabili virus, e prevenzione dall'infezione, verificando tutto ciò che, con un termine specifico dell'infanzia, il computer "mette in bocca".

In base a questo assunto, NAV esegue una serie di operazioni concorrenti, che assicurano, se opportunamente settate e costantemente aggiornate nei dati, tranquillità d'uso; esse possono essere così riassunte:

1) eliminazione di virus, se già presenti, e riparazione, ove possibile, dei file

2) protezione del computer da virus che agiscono all'avvio

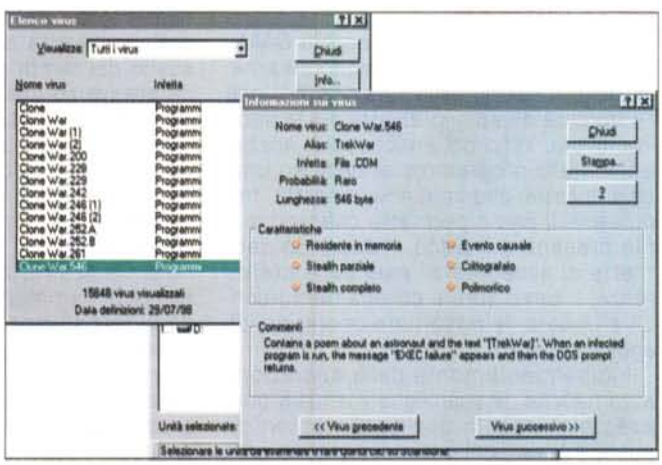
3) controllo di presenza dei virus ad ogni lancio di un programma o ad ogni apertura di un file, dovunque siano questi presenti

4) controllo di attività insolite coinvolgenti periferiche e memorie di massa

5) scansione pianificata e costante delle memorie di massa a disposizione del computer. Questa scansione viene eseguita, in base ai setup del programma, una volta la settimana.

6) Protezione del sistema da virus provenienti da fonti esterne diverse dalle memorie di massa. E' il caso di virus trasportati da Internet, e in questo NAV è ben organizzato, visto che esegue automaticamente la scansione dei file di programma e dei documenti appena termina il download o appena viene eseguita la consueta operazione di decompressione.

Ovviamente occorrerà avere a disposizione il database più aggiornato possibile delle "carte d'identità" dei virus, che, ormai quotidianamente, sono immessi, per così dire, sul mercato. Per questo, Norton, attraverso la sua ben nota tecnologia LiveUpdate, permette di scaricare continuamente le "chiavi" di riconoscimento dei virus, attraverso una procedura pressoché completamente automatizzata. Ovviamente nessun medicinale funziona senza la collaborazione del paziente, per cui occorrerà usare un minimo di attenzione nel maneggiare dischi e file, partendo dal principio che, finché non è dimostrato che sono "puliti", possono essere infetti. Non è certo paranoia, si tratta solo di regole di vita pratica che, una volta acquisite ad abitudine, diverranno parte integrante della nostra vita quotidiana.



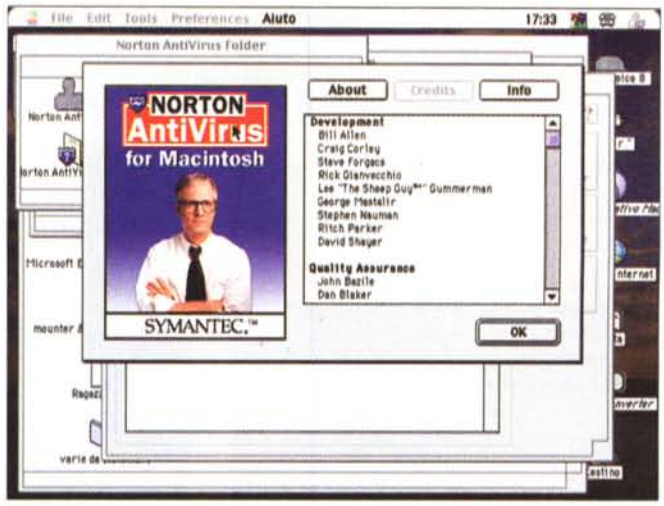
Eccoli, i "cattivi" all'opera; interessanti le descrizioni dei virus e del loro effetto. La libreria presente è enorme se si pensa che, i primi di dicembre del '98, erano classificati circa ventimila esemplari di virus diversi.

Mac e PC, piattaforme e ambienti d'uso diversi, per uno stesso risultato

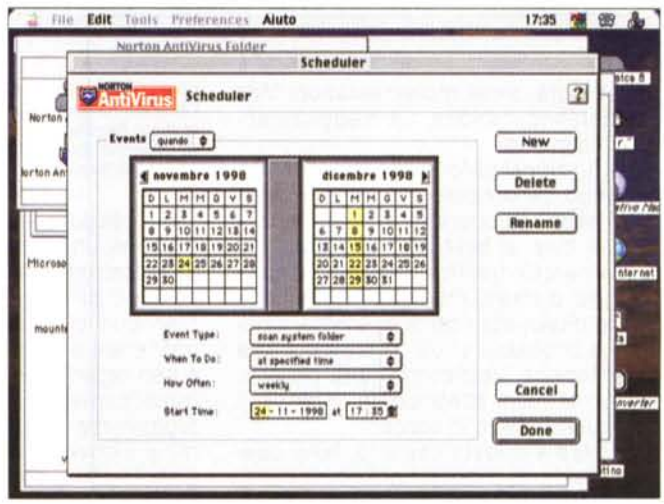
Sebbene si tratti, a conti fatti, dello stesso programma, la differenza delle due piattaforme ha determinato, alla resa dei fatti, due ambienti d'uso molto diversi tra loro, con quello Mac più riccamente personalizzabile e quello PC più, per così dire, "automatico". Ovviamente, poiché è il risultato che conta, nell'economia dell'articolo il fatto inciderà solo dove davvero le differenze comportano, alla conclusione, risultati effettivamente separabili.

La protezione offerta da NAV si esercita, essenzialmente, attraverso tre operazioni distinte; autoprotezione automatica, utilizzo dei dischi di soccorso, altre operazioni definibili dall'utente.

La prima è di gran lunga la più importante; l'autoprotezione è il metal detector del nostro computer, capace di fermare tutto quel che di sospetto dovesse arrivare alle vie d'accesso alla nostra



Lo splashscreen di NortonAV per Macintosh.



La fase di schedulatura delle attività; il monitoraggio può avvenire a intervalli regolari, o a date prefissate.

macchina, siano esse le porte di I/O alle memorie di massa o i collegamenti Internet. Il programma "gira" continuamente in background, verificando ogni attività anomala e ogni accesso a file e programmi. La seconda protezione, più che altro una cura estrema, è affidata alla creazione (purtroppo spesso trascurata dagli utenti; pare che la metà di essi ignori questa procedura, eppure si tratta di un'operazione che richiede, una tantum, pochi minuti) dei dischi di soccorso, vero salvagente quando le cose si mettono male. Il terzo ambiente è, infine, quello a disposizione dell'utente, ambiente attraverso cui gestire al meglio la nostra guardia del corpo personale.

In questo habitat l'utente ha la possibilità di tagliarsi a misura le attività del programma e di pianificare secondo i suoi desideri le attività della sua sessione di lavoro. Il tutto è legato all'apertura di una finestra che contiene una serie di comandi-pulsanti, ognuno dei quali raggiunge attività diverse.

La prima cosa da fare, qui giunti, è quella di pianificare le scansioni. Questa procedura permetterà di eseguire un check-up completo della nostra macchina in un momento prestabilito. Le attività, come altre che vedremo, sono settabili anche, una volta per tutte, durante l'installazione del pacchetto sull'HD, e, tra i diversi ambienti PC (98, 95, NT, Windows 3), esistono piccole differenze nella tecnica d'impostazione. A tal proposito va ricordato che i dischi di soccorso vanno aggiornati ogni volta che si installa un nuovo componente hardware, si eseguono modifiche al sistema operativo (come spesso accade anche a seguito d'installazione di nuovo software), si eseguono nuove partizioni o si aggiorna la protezione antivirus; l'aggiornamento è comunque pressoché automatico e richiede solo un modesto intervento da parte dell'utente.

Interessante è la possibilità di personalizzare in maniera più particolare l'ambiente di NAV. Spesso i settaggi inseriti di default sono più che adatti alla maggior parte delle esigenze, ma si può intervenire su di essi in maniera più particolare (ad esempio, per adattarlo alle esigenze di un amministratore di rete).

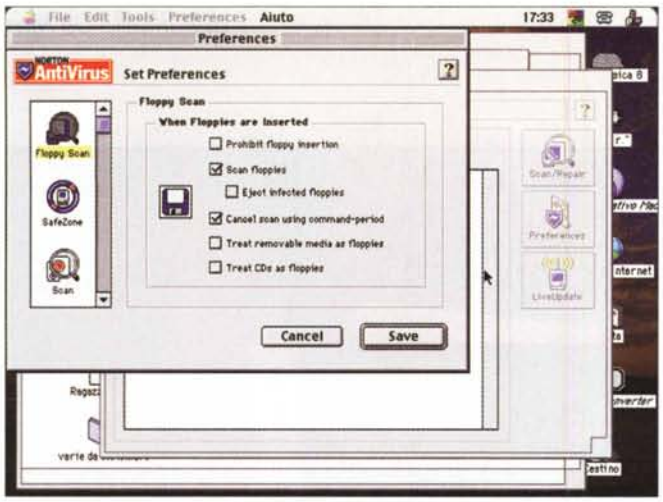
Ancora più pregevole è la possibilità di isolare file sospetti. Quando NAV rileva un'attività particolarmente inconsueta legata a un file, o crede di aver individuato un virus di nuovo tipo, provvede a isolare il documento o il programma sospetto, mettendolo in quarantena. La cosa può avvenire in maniera automatica, o in base a un preciso sospetto dell'utente; i file inseriti nella cartella di quarantena non avranno la possibilità di espandersi, duplicarsi, o estendere un eventuale contagio ad altri file, recando danni alla rimanente parte di HD. Nel frattempo il file potenzialmente infetto può essere inviato al SARC (Symantec Antivirus Research Center), che provvederà ad esaminarlo e ad avvertire l'utente di presenze indesiderate. E' necessario, per questo servizio, disporre di un collegamento Internet e di un indirizzo di posta elettronica per ricevere la risposta. Se viene rilevata la presenza di un nuovo virus, la relativa stringa di identificazione viene immediatamente comunicata al servizio Live Update.

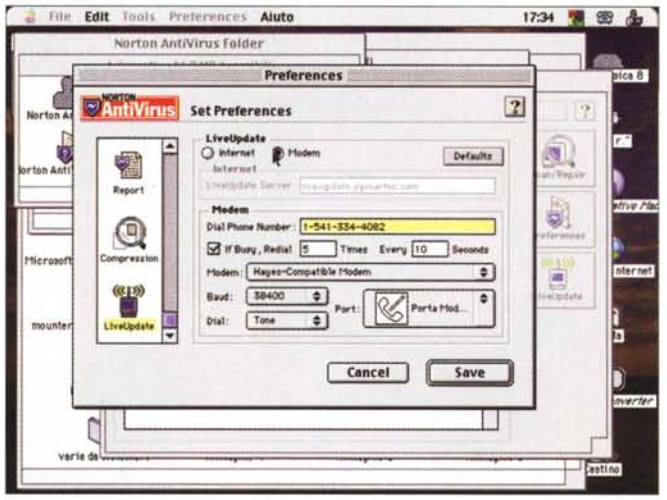
NAV e Mac

NAV per Macintosh (il vecchio SAM, di buona memoria) non è molto dissimile, nelle funzioni, dalla versione PC, ma l'ambiente d'uso si presenta più rapido, intuitivo e, in fondo, amichevole. Anche qui l'intero programma si basa su una sola finestra, che contiene, a destra, tre pulsanti. Il primo permette di scandire i file presenti sul disco, il secondo permette di accedere all'area delle preferenze, il terzo apre il collegamento con Live Update, le opportune operazioni di aggiornamento.

Indipendentemente dalle operazioni automatiche, la scansione manuale può essere avviata in qualsiasi momento, quando si verifichi qualche ipotetico problema. La scansione è rapida e non richiede alcun intervento da parte dell'operatore, se si è impostata l'opzione di autoriparazione. Dopo l'operazione, viene generato un report delle operazioni eseguite e degli interventi effettuati.

In ambito di automatismo di difesa, NAV, anche qui, permette di definire momenti prestabiliti per la scansione delle memorie disponibili e per il collegamento con Live Update per l'aggiornamento del database. In ossequio alla amichevolezza dell'ambiente Mac, la scelta dei tempi e degli intervalli avviene attraverso una pratica finestra-calendario, dove è possibile anche definire le tecniche da adottare, in default, in caso di problemi. Il programma può, inoltre, eseguire operazioni di controllo meno radicali, come controllo di attività cosiddette "virus-like" (ad esempio rilocazione di file sull'HD eseguite da un ottimizzatore di frammentazione). In questo caso l'utente viene avvisato della attività in corso e questi può intervenire, di volta in volta, permettendo, negando o liberalizzando l'attività riscontrata. Altra area "calda", ma non sempre pericolosa, appare essere l'attività di controllo di





La preziosa possibilità di creare un ambiente fortemente personalizzato. Interessante la facoltà di includere (o escludere) file compressi, in base al protocollo usato per lo "schiacciamento".

stato di file che hanno subito modifiche dalla loro ultima apertura; se è impostata l'opzione di protezione contro virus sconosciuti, e NAV riscontra che un file è stato oggetto di modifica o di un qualunque cambiamento nel periodo intercorso dall'ultima apertura, il sistema avvisa di questa anomalia, lasciando poi all'utente il controllo sulle successive operazioni da eseguire.

Fortunatamente, Mac non ha bisogno dei dischi di soccorso descritti in ambiente PC. Il computer può essere riavviato direttamente dal CD fornito nel pacchetto e le procedure di decontaminazione possono essere anche lanciate da qui; riguardo a queste ricorderemo che un file può essere soggetto a tentativo di riparazione e, in ultima analisi (ad esempio virus che sovrascrivono il codice), cancellati. L'area di customizzazione dell'ambiente è anch'essa molto piacevole da organizzare, visto che si basa su una striscia scorrevole laterale, che, ad ogni pulsante, apre una finestrina per la regolazione e la definizione di procedure personalizzate. Ad esempio è possibile definire quando, come e cosa fare in caso di floppy infetti, definire le caratteristiche della zona di quarantena (in essa è possibile definire e gestire cartelle personali, basate ad esempio sul tipo di virus di cui si sospetta la presenza). Ancora, è possibile indirizzare operazioni più frequenti di scansione su particolari cartelle (come quella definita dall'ambiente Internet Config di sistema operativo, che crea, a richiesta, una cartellina dove verrà riversato il materiale di downloading da Internet), definire particolari tipi di attività della macchina che vanno tenuti d'occhio. Ad esempio, è possibile gestire, una per una, una ventina d'attività particolari, come creazione di documenti di Startup nuovi, spostamento di risorse da una cartella all'altra, creazione d'applicazioni da parte d'altri programmi, aggiunta di file particolari a risorse di sistema (un esempio è l'aggiunta automatica di macroistruzioni a quelle già esistenti di programma, attività questa sempre sospetta), formattazioni non precedute da finestre di dialogo.

In ambedue le versioni, NAV può intervenire senza problemi su file compressi, e, in ambedue gli ambienti, pressoché tutti i protocolli sono riconosciuti e accettati. Ancora, e questo vale sia per l'ambiente Mac che per NT, molti dei settaggi di NAV possono essere protetti da password, in modo da impedire, da parte di un amministratore, accessi non autorizzati alle tecniche di difesa dell'ambiente. E infine, inutile raccomandarlo, conviene schedulare con sufficiente frequenza il collegamento a LiveUpdate; forse il problema virus in ambito Mac non è così grave come in PC, ma tenersi aggiornati non costa niente e ci permette di dormire sonni sereni.

Conclusioni

Norton AntiVirus 5 è il tool più potente oggi esistente in commercio per difendersi da attacchi di virus, macrovirus, cavalli di Troia e altre amenità del genere. Ma occorre precisare, a costo di diventare monotoni e fastidiosi, che la protezione è diretta conseguenza dell'aggiornamento della banca dati attraverso LiveUpdate. Occorre ricordare che mai come qui la potenza del programma non sta tanto nella più nuova o più vecchia versione, ma nella disponibilità di quelle benedette stringhe d'identificazione che poi ci permettono di riconoscere gli indesiderati ospiti che, a frequenza giornaliera, prolificano, si modificano, provocano danno e distruzione in maniera tanto subdola quanto insospettabile (pensate a quello che sono capaci di fare i CIH o a come sappiano ben mimetizzarsi i "polimorfi"). Norton mette a disposizione gratuitamente, per un anno, l'accessibilità agli utenti della libreria di LiveUpdate (dopo occorre pagare una piccola tassa d'iscrizione annua); è questa la vera chiave di volta della difesa, quindi non trascuriamola.

MS