The Norton Antivirus

di Gabriele Romanzi

Peter Norton è uno dei nomi più famosi nel campo dei prodotti software per l'ambiente MS-DOS; chi di noi non ha mai fatto ricorso ad una delle celebri Norton Utilities per trarsi d'impaccio da qualche problema con l'hard disk o con un floppy un po'... strapazzato in borsa?

Il nome di questo geniale imprenditore statunitense è da sempre stato legato ad una serie di prodotti che hanno avuto un enorme successo tra gli utilizzatori di personal computer grazie alla loro estrema facilità di utilizzo unita ad una grossa potenza operativa.

Prodotti, quindi, utilizzabili da tutte le categorie di utenti (anche i meno smaliziati) che permettono di accostarsi in maniera guidata all'utilizzo delle risorse del proprio elaboratore per poterne trarre il meglio in termini di prestazioni ed affidabilità (famosa, a questo riguardo, è la manualistica delle Norton Utilities, una vera guida di riferimento per le memorie di massa in generale).

Per non parlare poi di prodotti quali il Norton Commander (forse il più famoso shell per MS-DOS) o il Norton Backup (per il salvataggio periodico del contenuto dell'hard disk); tutti prodotti, come si vede, nati con l'impronta del «facilitare il lavoro con il PC». In questo filone si inserisce il prodotto oggetto di questa prova, il Norton Antivirus, che si propone come sistema software per la prevenzione e l'eliminazione dei più noti virus esistenti in ambiente MS-DOS.

Il problema dei virus ha ormai raggiunto uno spessore tale da comportare delle considerazioni abbastanza serie in termini di possibili danni economici e va quindi tenuto nella giusta considerazione sia dai gestori di sistemi di PC in rete locale sia dai singoli utilizzatori per i quali il computer è lo strumento di lavoro principale.

Virus, vermi e Cavalli di Troia

Vediamo brevemente come vengono catalogati i vari virus attualmente cono-

sciuti e quali sono i loro «sintomi» più comuni; per una trattazione più dettagliata vi rimando al più esauriente articolo di Stefano Toria sul numero 100 di MC.

Un virus altri non è che un software il quale, una volta inseritosi in un sistema (PC), opera sulle sue risorse in maniera sconosciuta all'utente, replicandosi, installando una propria copia in altri programmi eventualmente presenti, sovrapponendo propri messaggi a quelli degli applicativi che vengono fatti girare sulla macchina o, nel peggiore dei casi, alterando alcune componenti del sistema (cancellazione di file, formattazione del disco rigido, ecc...).

Da tutto questo si comprende il perché sia stato associato il nome di «virus» a questi programmi (che nel loro modo di operare ricordano proprio i microorganismi presenti nel corpo umano) ed i motivi che li rendono particolarmente temuti dagli utenti di personal computer. La differenza tra virus, vermi («worms») e Cavalli di Troia è nel modo in cui essi agiscono per entrare nel sistema informatico e quindi propagarsi; in sintesi possiamo dire che:

— il **virus** è generalmente immerso in un programma che, in determinate circostanze (ad esempio quando viene mandato in esecuzione) si propaga ad altri programmi trovati nel sistema, attaccando una propria copia all'eseguibile da «infettare», rendendolo così un «portatore» in grado di attaccare a sua volta il virus ad altri programmi (come vedete la terminologia usata nel campo dei virus informatici ha mutuato molti termini dal campo medico);

— il **verme** è un programma concepito non tanto per diffondere il contagio ad altri programmi quanto per replicarsi un numero indefinito di volte, sia in RAM che su memoria di massa, in modo tale da provocare un progressivo intasamento delle risorse della macchina con conseguente pesante rallentamento delle prestazioni, fino (a volte) a provocare il blocco totale del sistema;

— un **Cavallo di Troia**, infine, opera con il principio del suo omonimo mitologico: immerso in un programma «ospite», dal comportamento apparentemente innocuo, viene attivato soltanto in determinate circostanze (una particolare data, una determinata operazione richiesta al programma ospite) provocando danni spesso gravi (come la formattazione del disco rigido). I Cavalli di Troia, in genere, non replicano se stessi in altri programmi.

Da questa breve descrizione dei vari tipi di virus e delle conseguenze che essi possono provocare qualora riescano ad installarsi in un PC, si può comprendere come il problema della protezione dei propri dati o programmi abbia ormai assunto un posto di primo piano, soprattutto in sistemi collegati in rete tra di loro.

La migliore protezione contro questi virus, nati inizialmente come «scherzi tra informatici» ma poi diventati un vero e proprio flagello, è senza dubbio il back-up periodico dei dati; ciò non esclude comunque che occorra prendere delle opportune contromisure per evitare il contagio (o per eliminare il virus quando possibile) ed a questo scopo è destinato proprio il Norton Antivirus, che ora andiamo ad analizzare nel dettaglio.

The Norton Antivirus

Produttore:
Symantec.

Distributore:
MicroBusiness Italiana S.r.l.
Via Aurelio Saffi, 16 - 20123 Milano
Tel. 02/4390421

Prezzi *(IVA esclusa):*

The Norton Antivirus inglese	*L.*	*280.000*
Versione in italiano disponibile fine aprile 91	*L.*	*295.000*

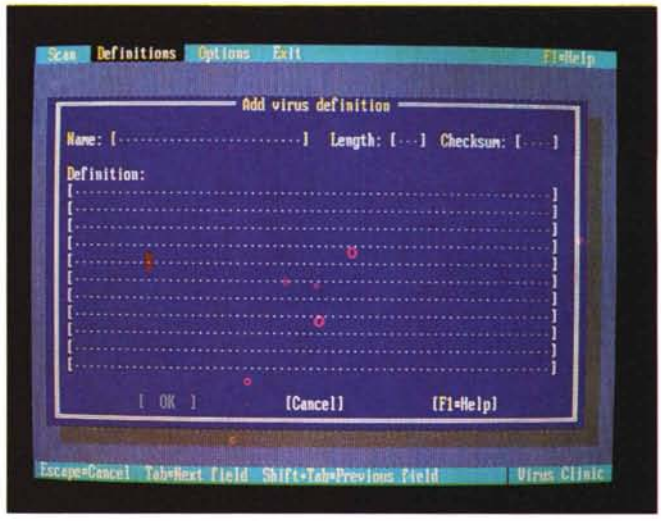
Il pacchetto, l'installazione ed il funzionamento

Aperta la confezione troviamo un manuale di circa 80 pagine ed una busta contenente i floppy (in entrambi i formati) con il programma, unitamente ad una serie di brochure pubblicitarie.

La prima cosa che salta all'occhio è il logo SYMANTEC presente su tutte le componenti del pacchetto; è stato in-

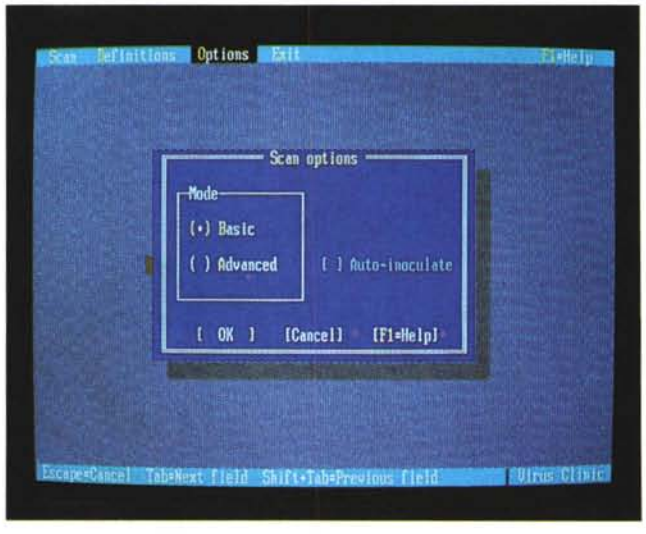
Il report generato da NAV.EXE alla fine della scansione del drive prescelto; sulla sinistra sono visibili le opzioni disponibili.

Una scheda in bianco in cui inserire i parametri di definizione di un nuovo virus scoperto.



Particolare dell'elenco dei virus conosciuti dal Norton Antivirus.

Il menu di configurazione di Norton Antivirus.



Scelta della modalità di ricerca dei virus; nel caso di scelta della modalità <ADVANCED> è possibile inoculare i file trovati calcolandone il checksum.

fatti raggiunto di recente un accordo di fusione tra la Peter Norton Computing e questa società, già famosa negli Stati Uniti per pacchetti come Q&A.

La Peter Norton Computing rimane inalterata con il suo staff tecnico di sviluppo e supporto ai prodotti, la cui distribuzione è ora affidata alla SYMANTEC (la classica foto di Peter Norton in maniche di camicia continua sempre a campeggiare sulle confezioni dei prodotti come una sorta di «marchio di qualità»).

La manualistica è ben fatta e spiega nei dettagli le singole fasi dell'installazione e dei primi passi con questo programma, salvo tornare nell'ultimo capitolo («Reference») ad una descrizione dettagliata delle singole voci dei menu.

Prima di procedere all'installazione del programma e delle utility accessorie sul disco rigido viene giustamente consigliato di effettuare un boot da dischetto (protetto in scrittura) e quindi lanciare NAV.EXE (il modulo principale del Norton Antivirus) direttamente dal dischetto originale, in modo da verificare l'assenza di virus eventualmente già presenti sul disco fisso, che potrebbero infettare lo stesso programma NAV (che comunque ha una sua funzionalità di auto-controllo).

Già in questa fase possiamo vedere come lavora il Norton Antivirus; il disco e le sue eventuali partizioni vengono scanditi un file alla volta alla ricerca dei virus conosciuti.

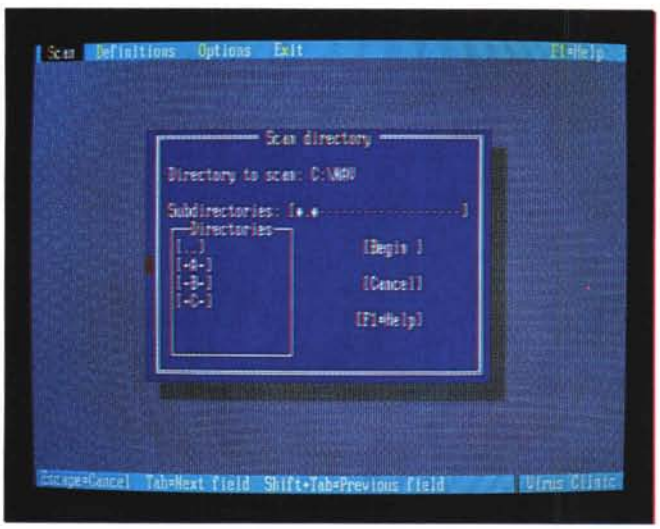
In una finestra sulla destra dello schermo viene visualizzato il procedere dell'analisi ed alla fine viene generato, sempre su schermo, un report dei virus eventualmente trovati con il relativo nome del file infetto.

La ricerca dei virus nei file viene effettuata basandosi sulle informazioni contenute in una serie di schede di definizione in cui sono riportati alcuni tra i dati più significativi di ognuno dei virus conosciuti, una sorta di «identikit» del virus; per permettere all'utente di avere un prodotto sempre aggiornato man mano che vengono individuati nuovi virus, è presente tra i menu una voce («Definitions») che, una volta selezionata, presenta una scheda di definizione in bianco da riempire con i dati identificativi dei nuovi virus prelevabili dalla BBS della Symantec.

Nella parte sinistra dello schermo sono presenti le voci delle principali operazioni che si possono effettuare al termine della fase di scansione; nel caso vengano rilevati dei virus è possibile sia cancellare il file incriminato che tentare di recuperarlo cancellando la parte infetta. Molto saggiamente nel manule viene ripetutamente consigliato di intraprendere preferibilmente la prima delle due strade, riservandosi la seconda soltanto in casi particolari (quando ad esempio non si ha a disposizione una nuova copia del file) ed in ogni caso di procedere al recupero dei file infetti uno alla volta, rilanciando sempre l'operazione di <scanning> per essere certi dell'avvenuta eliminazione del virus.

Una volta assicuratici che il disco fis-

Configurazione della password necessaria per poter accedere al menu di configurazione di Norton Antivirus.



È possibile effettuare la ricerca anche limitatamente ad una directory.

so è immune da virus, possiamo procedere all'installazione su di esso del programma, dando prima un'occhiata al file READ.ME presente su floppy con gli ultimi aggiornamenti e correzioni della manualistica; durante la fase di installazione viene creata una directory in cui vengono copiati i file contenuti sul floppy e quindi viene aggiunta al Config.sys l'istruzione per il caricamento del device driver NAV_.SYS.

In questo modo, a partire dal successivo boot del sistema, verrà caricato in memoria un programma residente (denominato VIRUS INTERCEPT) che verifica, ad ogni operazione di lancio o copia di un programma, l'eventuale presenza di virus, attivando in caso affermativo la visualizzazione di una finestra di allarme sullo schermo oltre ad una segnalazione acustica tramite l'altoparlantino del PC.

Questo modulo di protezione occupa soltanto 15 Kbyte di memoria RAM e può quindi essere caricato senza eccessivi problemi, fornendo uno scudo protettivo in prima istanza contro eventuali attacchi da virus prima che questi possano manifestarsi con i loro pericolosi «sintomi»; qualora si voglia evitare il caricamento di questo programma basterà tenere premuti contemporaneamente i due tasti di shift durante il boot della macchina.

Tornando al programma NAV c'è da segnalare una sua interessante caratteristica; se si sceglie la modalità di funzionamento <ADVANCED> è possibile INOCULARE i file man mano che vengono verificati. Vediamo un po' più nel dettaglio cosa comporta questa operazione.

Quando un virus si attacca ad un programma ne modifica la lunghezza o la struttura di una sua parte; la procedura di inoculazione prevede il calcolo del checksum di ogni file analizzato e questo dato viene confrontato ogni volta che il file è soggetto ad una qualche operazione: in caso di variazione nel risultato ottenuto dal calcolo del checksum occorre quindi verificare l'integrità del file per controllare che non sia stato infettato.

I dati dei vari checksum calcolati vengono memorizzati in appositi file con attributo hidden (nascosto), quindi non facilmente individuabili; lo svantaggio di questa operazione è l'aumento dello spazio occupato sul supporto di massa e per permetterne una periodica pulizia viene fornita una apposita utility (UNINOCUL) che si occupa dell'eliminazione dei file con i valori di checksum presenti nella directory specificata (oltre che nelle sue sottodirectory).

Il Norton Antivirus è configurabile, tramite la voce <Configure> del menu Options, in modo da adattarlo alle specifiche esigenze di ogni utente; è possibile settare il tipo di monitor, la palette di colori più idonea, se memorizzare o meno l'attività del Virus Intercept in un file di testo oltre che abilitare o disabilitare alcune delle opzioni di intervento sui file infetti. Per un uso in rete locale è possibile far eseguire da una stazione la ricerca dei virus su tutti i drive di rete.

Le varie opzioni di configurazione sono soggette ad una password di controllo, che garantisce l'utente (o il gestore della LAN) contro manipolazioni esterne.

Conclusioni

Spesso non è facilmente quantificabile in termini monetari il danno provocato dalla perdita di dati o programmi; per questo motivo la spesa necessaria per l'acquisto di un programma come il Norton Antivirus la si potrebbe definire quasi irrisoria.

Per quanto si voglia essere attenti e scrupolosi, il rischio di trovarsi il computer infettato da uno dei tanti virus in circolazione non è poi così remoto; ritengo quindi che un programma che non solo funga da filtro di controllo ma che in caso di problemi possa essere di un qualche aiuto per la rimozione «dell'ospite indesiderato» sia senza dubbio consigliabile.

È facile da usare, è configurabile, assicura vari livelli di protezione ed inoltre permette di aggiornare la base dati dei virus conosciuti man mano che ne vengono scoperti di nuovi, salvaguardando quindi la spesa sostenuta per l'acquisto.

Il marchio di Peter Norton è inoltre garanzia di qualità ed affidabilità; da tutte queste considerazioni non posso quindi che consigliare caldamente questo prodotto a tutte quelle persone per le quali la sicurezza dei dati del proprio PC è un fattore di importanza primaria.

MC