a cura di Massimo Negrisoli

VirIT 1.00d

Un completo servizio anti-virus, mirato all'identificazione e alla rimozione dei virus circolanti in Italia; Il Virus B1

Il prodotto anti-virus in questione dovrebbe già essere noto ai lettori più assidui della rivista PC Floppy + PC Magazine poiché alcune versioni Lite sono già state ospitate sui dischetti allegati. La versione Lite è infatti distribuita in modalità freeware, in modo che chiunque possa usarla e distribuirla liberamente, senza che nulla sia dovuto agli autori del programma. E' limitata fondamentalmente alla scansione e al rilevamento virus, quindi non possiede il modulo di rimozione che viene rilasciato solo con la versione completa. Come avviene sempre più frequentemente parlando di prodotti anti-virus la registrazione non solo consente di ricevere il programma completo del modulo di rimozione, ma anche di usufruire del completo servizio di assistenza e aggiornamento fornito dalla TG Soft di Padova (Tel. 049/631748, E-mail: tge@maya.dei.unipd.it).

La registrazione prevede la possibilità di acquistare solo una versione del programma, alla quale viene abbinato il servizio di assistenza con validità di quattro mesi a partire dalla data di registrazione. Alternativamente, è possibile sottoscrivere un abbonamento annuale, costituito da sei aggiornamenti di VirIT (uno ogni due mesi). Il servizio di assistenza consiste nella possibilità da parte degli utilizzatori registrati di inviare alla TG Soft eventuali file sospetti, che verranno esaminati gratuitamente e se all'interno dei file inviati fosse effettivamente presente un virus, la TG Soft provvede a fornire, approssimativamente entro le 24 ore dalla ricezione del materiale, un VirIT Personal Version, in grado di rimuovere la nuova forma virale individuata.

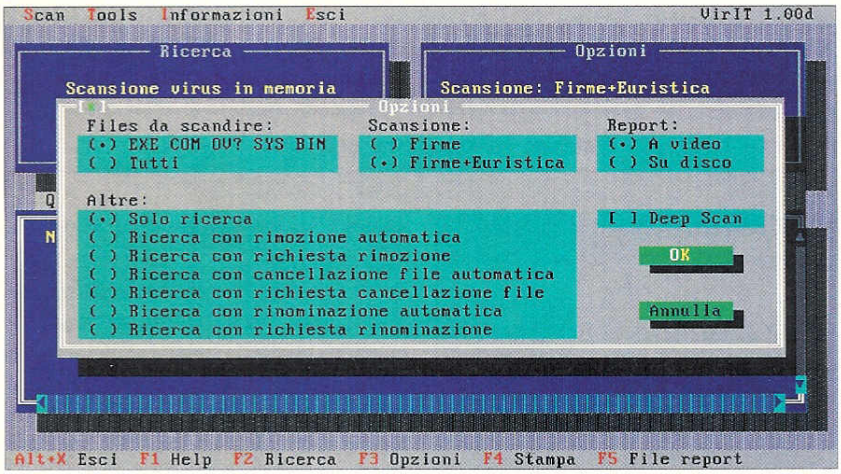


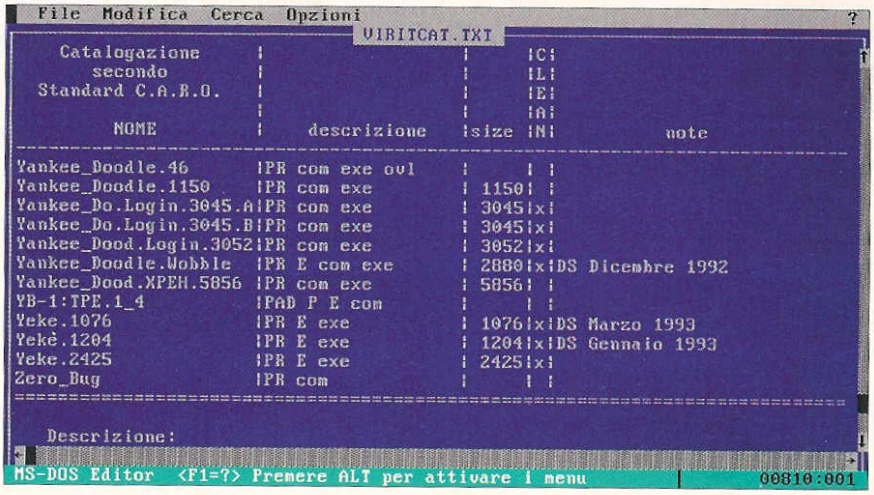
Figura 1: La finestra d'impostazione dove è possibile definire il comportamento del programma durante la fase di scansione.

Come funziona

Anche questa nuova versione è stata aggiornata con le impronte, o forme virali, dei virus circolanti in Italia al momento del rilascio. La nuova versione inoltre è stata ulteriormente migliorata per quanto riguarda gli algoritmi euristici. Si è infatti cercato di implementare degli algoritmi che evitino la segnalazione di falsi positivi, operando la scansione dei soli file che generalmente possono venire infettati dai virus. Il programma VirIT consente quindi l'identificazione delle forme virali attraverso la doppia modalità: firme ed euristica. La prima esamina i file alla ricerca di quella che viene definita l'impronta (o firma, appunto) lasciata dal virus per evitare di ripetere l'infezione di archivi già corrotti. La modalità euristica invece comprende diversi e complessi algoritmi che analizzano i file alla ricerca di comportamenti sospetti. La versione registrata del programma contiene anche alcuni tool particolarmente utili, come per esempio l'utility che consente la ricostruzione dell'MBR (Master Boot Record dell'hard disk) o quella per la scrittura di un boot sector generico su floppy disk.

Come quasi sempre avviene parlando di prodotti anti-virus, giunge la fatidica domanda: "ma quanti virus è in grado di riconoscere?". Il discorso è molto più complesso di quanto si possa immaginare, soprattutto oggi dove la lotta anti-virus ha assunto una fisionomia ben precisa. E' passata ormai

l'epoca in cui i virus circolanti erano dell'ordine delle centinaia e quindi era relativamente semplice creare anti-virus universali. Oggi esistono decine di varianti di uno stesso virus, e inoltre la schiera di coloro che nulla hanno da fare nella vita se non procurare danni e fastidi al prossimo sembra aumentare in modo esponenziale. Se si volesse produrre un anti-virus sempre aggiornato, lo sfortunato creatore del prodotto dovrebbe passare le sue giornate ad analizzare e decifrare tutte le impronte virali delle nuove varianti. Ecco perché iniziano a svilupparsi nuove tendenze e strategie, come quella di creare prodotti dedicati solo ai virus circolanti su un determinato territorio, il raffinamento degli algoritmi di ricerca euristica, la cattura delle forme virali individuate e un attento servizio di assistenza. I nuovi programmi cercano di sviluppare particolari tecniche di controllo delle impronte virali, per fare in modo che una sola firma principale possa essere utilizzata per individuare più varianti di uno stesso virus. Inoltre, è meglio garantire l'individuazione e la rimozione dei virus effettivamente circolanti sul territorio in cui ci si trova ad operare, anziché occuparsi anche di virus circolanti in altre nazioni. Infatti un programma anti-virus in grado di riconoscere ben sette milioni di diversi virus circolanti sul territorio statunitense, avrà sicuramente un valore notevole negli U.S.A., ma potrebbe avere scarsa efficacia se usato nel nostro paese. E' anche vero che il crescente interesse nei confronti di Internet aumenta il rischio d'importare virus provenienti da qualsiasi parte del globo, comunque ci si potrà sempre occupare di un nuovo virus straniero quando farà la sua comparsa in Italia.



● **Figura 2: Particolare del file contenente l'elenco dei virus attualmente riconosciuti da VirIT.**

Alla luce di quanto detto fino ad ora è quindi impensabile, nel momento in cui si vuole valutare la bontà di un programma anti-virus, concentrare l'attenzione solamente sul numero di virus che al momento è o sarebbe in grado di riconoscere (parlando di ricerca euristica dei virus il condizionale è d'obbligo). Ritengo che gli aspetti fondamentali da valutare in un prodotto anti-virus siano: il tipo di servizio offerto, la possibilità di ricevere versioni del prodotto aggiornate o di poter inviare file sospetti ricevendone una versione personalizzata per la rimozione del nuovo virus. Per gli amanti delle cifre riporto comunque nel box relativo la carta d'identità della nuova versione di VirIT.

Tutti i numeri di VirIT 1.00d

Il numero di virus intercettati da VirIT non è quantificabile poiché, grazie agli algoritmi euristici, il software è in grado di identificare codici virali di nuova generazione. Grazie agli accorgimenti adottati nell'implementare le firme virali, il software è in grado di intercettare anche molte varianti dei codici virali catalogati.

Annessi e connessi

Il programma VirIT (prezzo orientativo L. 125.000) funziona in ambiente DOS, e prevede una configurazione veramente minima. Tra i file in formato testo (.txt) contenuti nel dischetto fornito, sono presenti il manuale dettagliato che spiega come usare il programma direttamente dalla riga di comando, e un'enciclopedia nella quale sono riportati tutti i virus riconosciuti dall'attuale versione, incluse sintetiche note sul modo d'agire del virus, la posizione occupata al momento dell'infezione, il tipo di file colpiti e i danni procurati. La versione completa di VirIT comprende anche il monitor residente VirITTsr, un programma residente in memoria che permette di bloccare i virus conosciuti e/o le loro varianti prima che producano l'infezione. Abbiamo pro-

vato la versione registrata di VirIT su consistenti gruppi di virus polimorfici quali: MtE.Pogue, MtE.Dedicated, Dream_Man, MTZ.Pink_Panther.4510, Yeke e Stoned.Angelina. Il programma in tutti i casi ha dimostrato la sua efficacia, infatti tutte le mutazioni funzionanti (ovvero ancora in grado di replicarsi) sono state correttamente identificate. In particolare, ha costituito una gradita sorpresa il riconoscimento e la corretta rimozione del virus Stoned.Angelina. L'autore di VirIT ci ha confermato che si tratta di un virus giunto solo recentemente sul nostro territorio. La provenienza potrebbe essere la Germania, ma per ora si tratta solo di un'ipotesi.