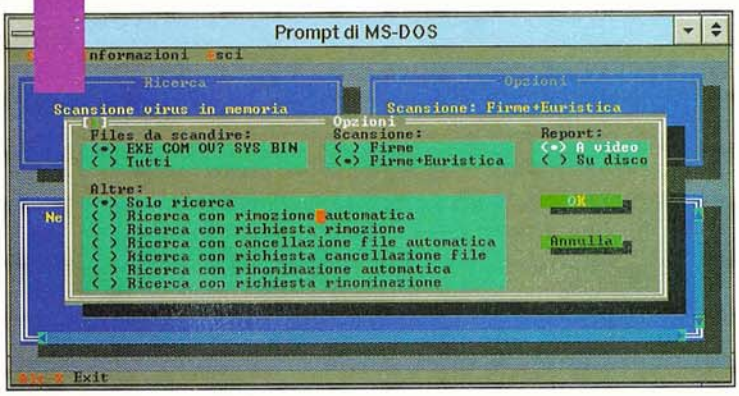
di Luca Alberto Stucchi

Un prodotto e un servizio anti-virus per combattere i virus di casa nostra.

VIRIT



Già dagli albori del fenomeno computer virus, a fianco dei ricercatori anti-virus "ufficiali" ingaggiati dalle grosse società di software si è man mano sviluppata una sorta di underground informatico costituito da ricercatori "in proprio" che hanno nel tempo sviluppato (spesso da soli, altre volte in gruppi di due, tre elementi) vari prodotti anti-virus.

Questo anti-virus si dichiara in grado di riconoscere e rimuovere i virus realmente presenti nel territorio

Nella maggior parte dei casi, questi prodotti hanno avuto una circolazione molto limitata. Infatti, un po' a causa di una certa cultura da sottobosco, un po' a causa della prepotente forza di marketing delle grosse società, questi programmi non sono quasi mai riusciti a diventare dei veri e propri prodotti commerciali.

Eppure, molti di questi prodotti hanno i numeri giusti per affermarsi; specificatamente rivolta al mercato italiano, questa categoria di anti-virus non afferma pomposamente di riconoscere oltre 6.000 virus, ma più modestamente si dichiara in grado di riconoscere e rimuovere i virus realmente presenti nel territorio.

In pochi hanno infatti la necessità di possedere, e utilizzare, un prodotto anti-virus in grado di rimuovere anche i virus in circolazione nella sola Cina.

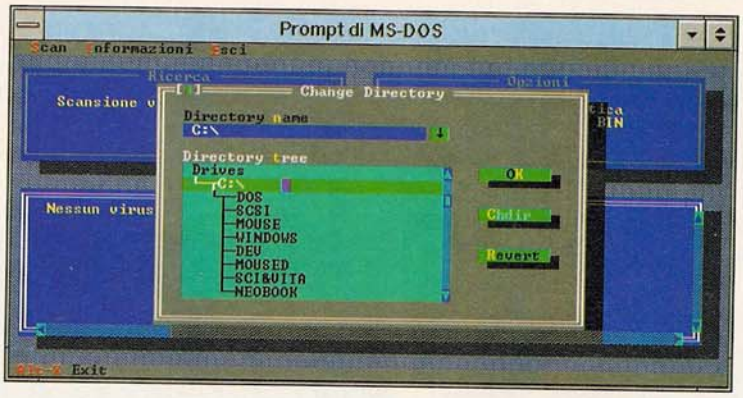
VirIT

Fra i prodotti anti-virus "artigianali" che non solo non sembrano destinati al dimenticatoio, ma sembrano essere destinati ad affermarsi sul mercato, c'è VirIT, un programma realizzato dalla Tg Soft, una piccolissima software house della provincia di Padova.

Il nucleo di VirIT, costituito dal consueto scanner, consente l'individuazione dei codici virali attraverso una doppia modalità di intercettazione: Firme ed Euristica.

La modalità Firme permette l'univoca identificazione dei virus noti (e presenti in Italia) fino al momento del rilascio della versione del software.

La modalità Euristica è invece caratterizzata da complessi algoritmi che analizzano i file e ne individuano i comportamenti sospetti, segnalandoli opportunamente.



VirIT è dotato di un'interfaccia utente semplice ma gradevole, che consente la visualizzazione dell'albero delle directory del disco corrente, permettendo, con un doppio click del mouse, la selezione della directory e/o del volume da scandire. Al fine di includere la scansione di uno o più dischi fra le procedure avviate durante la fase di boot, VirIT è utilizzabile anche dalla linea di comando.

Per esempio, il comando:

```
VIRIT C:\DOS /a /nomem
```

Esegue la scansione della directory C:\DOS di tutti i file (/a), ma non la scansione della memoria (/nomem).

Protezione residente

Il monitor residente VirITTsr, fornito a corredo dello scanner, consente di individuare e bloccare i virus riconosciuti e le loro varianti prima che producano l'infezione.

L'occupazione di memoria di VirITTsr è limitata, e si aggira intorno ai 30 kbyte.

Il servizio

Agli acquirenti di VirIT viene fornito compreso nel prezzo, oltre al consueto servizio di aggiornamento delle signature, un servizio di assistenza caratterizzato dall'analisi gratuita di eventuali file sospetti.

Nel caso l'analisi desse esito positivo (ovvero i file inviati alla Tg Soft risultassero infetti da parte di un nuovo virus), viene fornito, di norma entro le 24 ore successive all'arrivo del materiale sospetto, una copia aggiornata di VirIT in grado di identificare e rimuovere lo sgradito ospite. Un servizio non da poco, se si considera l'offerta media del mercato.

Prestazioni

Per testare opportunamente VirIT, abbiamo dovuto variare i criteri di test che normalmente impieghiamo nella valutazione di un prodotto anti-virus.

Sarebbe infatti stato concettualmente errato provare VirIT in modalità Firme utilizzando anche file infetti da parte di virus che non hanno mai realmente circolato in Italia. Il nostro database di virus (che contiene oltre 1.800 virus e varianti) è quindi stato opportunamente purgato dai virus non effettivamente presenti nella nostra penisola.

Con questa premessa i risultati ottenuti sono stati più che soddisfacenti: VirIT è stato in grado di riconoscere (e ove possibile rimuovere) oltre l'89% dei file infetti.

Ovviamente, per provare la funzionalità del riconoscimento in modalità Euristica abbiamo utilizzato l'intero database, ottenendo anche in questo caso prestazioni decisamente positive.

Conclusioni

I test effettuati su VirIT hanno fornito esiti decisamente positivi. Certo, ci piacerebbe vedere incluse nel prodotto (attualmente disponibile per il solo ambiente Dos) caratteristiche attualmente non disponibili, quali la possibilità di effettuare la scansione all'interno di file compressi e la presenza di un database dei virus.

Da notare che, oltre alla mera produzione di VirIT, la Tg Soft si occupa anche di monitorare il fenomeno computer virus, sia da un punto di vista quantitativo che dal punto di vista della diffusione territoriale.

VirIT
Prezzi: L. 83.200 + Iva (per utenti privati)
L. 124.000 + Iva (per aziende)

Tg Soft
via Sardegna, 5
35030 Sarmeola di Rubano (Pd)
tel. 049/631748

Luca Stucchi è un consulente free-lance e scrittore in Milano. Laureato in Scienze dell'Informazione, fornisce dal 1987 consulenze di programmazione avanzata per gli ambienti Windows, Unix e OS/2. E' autore di vari programmi per la protezione dei dati e dai virus. E' possibile contattare Luca scrivendo alla redazione di BIT.