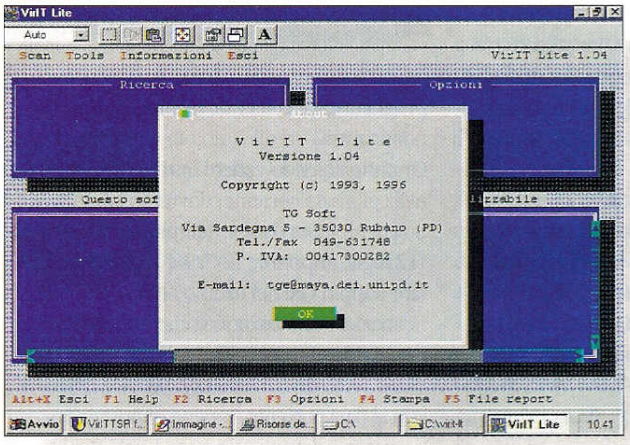
VirIT Lite ver. 1.04

L'ANTIVIRUS ITALIANO ON DEMAND

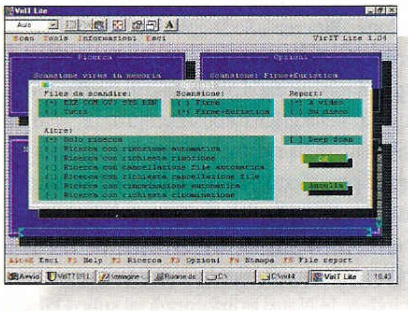
Gianfranco Tonello (*)

Prima o poi, purtroppo, a molti capita di incappare in qualche virus informatico; il fenomeno, generalmente, è dovuto alla smodata voglia di provare nuovi software segnalati da amici o conoscenti.
E' proprio durante la prova indiscriminata di nuovi software dalle provenienze più disparate che si può incappare nello sgradito incontro di qualche agente patogeno. Nei casi più fortunati l'utente è in grado di riconoscere la situazione anomala, in altri casi, nonostante l'utilizzo di software atti allo scopo, l'intercettazione dei virus di nuova generazione non dà i risultati sperati.



VirIT Lite ver. 1.04

Si tratta di un software antivirus, di immediato utilizzo, che cerca di intercettare i virus presenti sui floppy disk e sui programmi prima che questi vengano utilizzati e sia propagata l'infezione. La sua distribuzione è di tipo Freeware, quindi gratuita a tutti gli effetti, per incoraggiare l'utilizzo sistematico, nella piena legalità, di questo software sviluppato interamente in Italia. VirIT Lite è un pacchetto di identificazione e cancellazione dei file infetti dai virus noti, vale a dire quelli inviati dall'utenza presso i laboratori della TG Soft. L'intercettazione avviene attraverso il classico metodo delle Firme - dette anche impronte virali - che permette, a partire da queste, anche l'identificazione di eventuali varianti dei virus già catalogati. Per quanto riguarda i codici virali non inviati presso i laboratori TG Soft (perché non hanno mai fatto la loro comparsa in Italia, o per pigrizia dell'utente che, pur individuandoli, ha evitato di inviarli al centro di ricerca) sono stati implementati vari Automi di Ricerca Euristica, che cercano di intercettare eventuali virus dei quali non è nota la Firma virale. Con queste due modalità di identificazione, il software è in grado di intercettare virus informatici che, per sfuggire all'identificazione, sono stati eventualmente crittografati. Per far fronte alle patologie virali più complesse, come i codici virali extratraccia e i virus polimorfici (cioè crittografati in modo multivariato) generati



con "motori" - quali MtE (citiamo per tutti MtE.Pogue e MtE.Dedicated, "firmati" dal bulgaro Dark Avenger - e TPE (tra i quali citiamo l'italiano TPE.Lamer_ Exterminator) sono stati implementati due automi finiti per l'intercettazione degli algoritmi crittografici mutanti generati dai suddetti motori. Restando nel campo dei virus maggiormente complessi, che implementano le tecniche più raffinate della crittografia poliforme, gli sviluppatori TG Soft hanno implementato un complesso automa finito proprietario. Questo, denominato Deep Scan, permette l'identificazione dei virus non più attraverso il riconoscimento del metodo di crittografazione (seppur multivariata), ma attraverso la decrittografazione del codice virale e l'identificazione del virus vero e proprio. Con un automa del genere sono identificabili virus altamente polimorfici a infezione rapida a frammentazione del file come One_Half.3544, noto anche come Slovakia_Bomber. Queste le peculiarità principali di VirIT Lite, che sebbene sia un applicativo nativo Dos, è utilizzabile con Windows compatibile anche col nuovo sistema operativo Microsoft Windows 95.

L'interfaccia

Diamo ora una rapida carrellata sull'utilizzo dell'interfaccia utente, realizzata in modalità Turbo Vision a finestre e menu a tendina. All'attivazione del software compare la classica schermata di About, ove sono riportati il nome del programma, la versione e l'indirizzo completo della software house che l'ha sviluppato. Per procedere oltre si deve premere Invio oppure cliccare con il mouse su tasto Ok. In seguito il software controlla la presenza in memoria di virus noti fino a quel momento e, conclusa tale operazione, inizia l'utilizzo del programma mediante accesso ai menu a tendina tipici della struttura Desk Top. I menu sono quattro: Scan, Tools, Informazioni ed Esci. L'accesso ai menu è ottenibile attraverso l'utilizzo del mouse (oramai compagno fedele di ogni utente di computer) o premendo il tasto Alt e quello indicato nei singoli menu.

Il menu Scan

E' costituito da 4 voci:
Ricerca: permette di accedere alla finestra per definire l'unità sulla quale indirizzare la ricerca dei virus. L'unità, directory sottodirectory etc. sono digitabili da tastiera, oppure possono essere "puntate" con il mouse direttamente sull'albero visualizzato. *Opzioni:* permette di accedere alla maschera delle opzioni di scansione divise in vari gruppi.

> La distribuzione è di tipo Freeware, quindi gratuita a tutti gli effetti, per incoraggiare l'utilizzo sistematico, nella piena legalità, di questo software sviluppato interamente in Italia.

L'impostazione si attua attraverso il mouse, utilizzando il tasto Tab e le freccette.
File Report: il risultato della scansione viene visualizzato sulla finestra dei messaggi della schermata principale, ma può essere anche registrata su file esterno Ascii, con numerazione progressiva Virit001.Rep, per la consultazione dopo l'uscita dal programma.
Stampa: permette la stampa del file report su stampante collegata alle varie porte (Lpt1, Lpt2 etc.).

Menu Tools

E' costituito da quattro voci:
Backup area di sistema: permette il salvataggio su file esterno del contenuto del Master Boot Sector del disco fisso 1 e il boot sector della partizione attiva.
Restore area di sistema: permette di ripristinare il Master Boot Sector e boot sector precedentemente salvato nel caso questo sia stato danneggiato (generalmente da qualche virus). *Floppy disk Boot fix:* scrive un settore di boot generico sui floppy disk, permettendo la bonifica dei floppy anche da virus sconosciuti che avessero colpito il dischetto.
Master Boot Sector fix: permette di scrivere il Master Boot Sector del disco fisso così da debellare infezioni di questa parte vitale del calcolatore anche da virus sconosciuti.
Il menu Tools è abilitato nella versione Professional e il suo utilizzo è consigliabile che sia sempre assistito telefonicamente dal servizio di assistenza TG Soft.

Menu Informazioni

Rilasciato a: sono contenute brevi informazioni sull'utilizzo nella piena legalità sia della versione Lite che Professional del software. *C.R.A.V. BBS:* informazioni sulla Bbs di supporto dei software sviluppati da TG Soft.

Menu Esci

E' costituito da due voci:
Salva opzioni: clickando su questa voce è possibile mantenere le opzioni correnti, evitando di impostarle nuovamente tutte le volte che si attiva il programma.
Esci: permette di uscire da VirIT Lite, analogamente alla pressione contemporanea dei tasti Alt + X.

Installazione

Su sistema operativo Dos.
Creare la directory VIRIT-LT nell'unità desiderata (per esempio per l'unità C: operare come segue: C:\ Md VIRIT-LT)
Trasferire i file dal Cd-Rom all'interno della directory creata.
Accedere alla directory VIRIT-LT e digitare Virit, premendo successivamente Invio e seguendo le indicazioni a video.

Su sistema operativo Windows 3.0, 3.1 e 3.11.
Creare, come nel caso del Dos, la directory VIRIT-LT nell'unità desiderata e trasferire i file dal Cd-Rom al suo interno.
Attivare Windows dalla finestra Program Manager e accedere al menu a tendina "File" clickando su "Nuovo...", si accederà così a una finestra dove si creerà un gruppo di programmi.
Scegliere la voce "Gruppo di Programmi" e, alla richiesta della loro descrizione, digitare VirIT Lite;
Cliccare su "File del gruppo" e digitaee VIRIT-LT.GRP.
Al gruppo di programmi Windows creato associare le icone desiderate per eseguire i programmi.
Cliccare sul menu a tendina File e al suo interno su "Nuovo...", selezionare "Programma" e confermare.
Alle successive richieste rispondere come segue:
Descrizione del programma: digitare VirIT Lite.
Riga di comando: digitare C:\VIRIT-LT\VIRIT.EXE
Cliccare su Cambia Icona e associare l'icona Virit.Ico che si trova all'interno della directory C:\VIRIT-LT

Ora avete creato il gruppo VIRIT-LT e associato allo scansore Virit.Exe l'icona Virit.Ico per la sua attivazione. Cliccando due volte velocemente con il mouse sull'icona potrete attivare Virit.Exe.

Su sistema operativo WindowS 95.
Dal tasto di "Avvio" accedere al Prompt di Ms-Dos;
Eseguire l'installazione seguendo la procedura evidenziata per il sistema operativo Dos precedentemente.
Posizionarsi sulla cartella VirIT Lite.
Eseguire l'icona "Ms-Dos" VirIT agganciata e seguire le indicazioni a video.

Attenzione:

poco prima di andare in stampa, ci è pervenuta l'ultima versione del programma (la 1.06) descritto in queste pagine e che comunque troverete nel nostro Cd Rom. La precedente versione qui recensita differisce di poco dalla nuova release.

TG Soft, un'azienda italiana

TG Soft studia da anni gli agenti patogeni, soprattutto quelli circolanti in Italia in ambito bancario e aziendale. Provvede inoltre a segnalare le stringhe di identificazione dei virus non ancora intercettati dagli antivirus stranieri più famosi, così da abbreviare i lunghi tempi di aggiornamento, almeno per quanto riguarda l'identificazione dei virus informatici non intercettati.
Dopo l'esperienza professionale, maturata in quest'opera di continuo aggiornamento personalizzato dei software stranieri, TG Soft realizzò nel 1993 la prima versione di VirIT (ver. 090) distribuita attraverso la rete amatoriale di Bbs FidoNet e nel circuito bancario. Con l'aumentare dei virus circolanti nel nostro Paese, e l'invio di pacchetti di virus da parte di appassionati di sicurezza informatica attenti alle problematiche relative, è iniziata la realizzazione continua di aggiornamenti del software, rilasciata generalmente con cadenza bimestrale. In concomitanza con il rilascio della versione 0.95 di VirIT, TG Soft è stata invitata a Smau '94 per presentare l'antivirus di sua produzione che ha rappresentato e rappresenta, nel panorama italiano, uno tra i pochi che limita l'importazione di software straniero nello specifico settore. Lo sviluppo del software è stato motivato non tanto dalla richiesta del mercato di questa tipologia di programmi, quanto dalle specifiche esigenze di sicurezza in ambito bancario e aziendale. Gli utenti di questi settori non possono certo attendere i lunghi tempi di aggiornamento in relazione alle patologie virali di nuova generazione e/o non intercettate dalla corrente versione del software. TG Soft ha rilasciato VirIT Lite mettendo contemporaneamente a disposizione i propri tecnici per l'analisi gratuita di materiale sospetto infetto, dando finalmente, anche in Italia, un punto di riferimento preciso per la soluzione di queste problematiche. VirIT Lite, ora giunto alla versione 1.04, è un software di identificazione e cancellazione dei file infetti, di libero (e quindi gratuito) utilizzo sia in ambito privato che aziendale. Si tratta quindi di un software antivirus Freeware a tutti gli effetti. E' doveroso sottolineare che VirIT Lite non riconosce solamente i virus "italiani" ma anche quelli "stranieri" (se così possiamo dire). La differenza consiste nel fatto che, operando TG Soft in Italia, la società mostra impegno prioritario nella soluzione delle problematiche virali inviate da utenti italiani. TG Soft, dal canto suo, mette a disposizione degli utenti più esigenti il pacchetto VirIT Professional, costituito dal programma di identificazione e rimozione VirITPro, e dall'intercettatore residente (TSR) VirITTSR per la preventiva identificazione dei virus prima dell'infezione della macchina. Tra i diversi servizi è da evidenziare, soprattutto, quello di assistenza telefonica e aggiornamento personalizzato per far fronte alle patologie virali sia di nuova che di vecchia generazione che dovessero fare la loro comparsa presso l'utenza.
L'utente di VirIT Professional, inviando materiale potenzialmente infetto presso i laboratori TG Soft, riceverà la versione personalizzata del software per l'identificazione e la rimozione dello sgradito "parassita", concertando con il servizio di assistenza le modalità di utilizzo dei software per debellare e/o circoscrivere l'infezione.