VIRIT.EXE: L'antivirus made in Italy e per l'Italia

di Gianfranco Tonella

I virus nascono pure nel Bel paese

Come ancora non tutti sanno data da molto tempo la proliferazione di virus informatici "italiani", ovverosia creati e diffusi sul nostro patrio suolo. Stando (ahimè) così le cose, diversi esperti, per conto di aziende importanti e preoccupate del dilagare di questo spiacevole fenomeno, si sono messi alla caccia di questi agenti... patologici.

Fra questi, il sottoscritto ricercatore anti-virus Gianfranco Tonello, che ha escogitato e messo a punto il programma di scansione e rimozione dei virus informatici chiamato **VirIT**. Si tratta, per l'esattezza della versione 0.94e. rilasciata il 19/06/1994 (quindi ben aggiornata: per fortuna non si presentano troppi nuovi virus a distanza di pochi mesi...).
Il VirIT vuole essere un programma di rilevazione & rimozione dai virus informatici MS-DOS, con particolare attenzione verso quelli circolanti nella penisola italiana. VirIT ha una doppia modalità intercettativa, FIRME ed EURISTICA. Tali modalità sono disgiunte: in modalità firme il software è in grado di intercettare con precisione e, nella maggior parte dei casi, rimuovere i virus italiani ad esso già noti. Invece nella modalità euristica cerca di individuare i codici virali di nuova produzione.

Un circolo virtuoso

Purtroppo è ovvio che, essendo tali codici virali nuovi (e fino a quel momento, sconosciuti), non ne è possibile la disinfezione immediata, a meno di non avere un esperto sottomano. Niente paura: per il bene di tutti, dovranno essere inviati all'autore del software per l'estrazione della stringa di univoca identificazione. Grazie a questo circolo virtuoso che si stabilisce - pronuba anche la rivista PC Floppy - ogni qual volta la cosa sia possibile verrà aggiornata anche la rimozione dello sgradito nuovo intruso.
La modalità firme risulta essere strutturata in modo da poter individuare nuove varianti dei codici virali già inseriti. Eventuali nuove varianti identificate verranno segnalate con apposito messaggio.
IMPORTANTE: Si prega, ogni qual volta il software identifichi un codice virale di segnalarlo telefonicamente al ricercatore antivirus indicato in fondo all'articolo. Questo al solo scopo di monitorare la proliferazione dei codici virali in Italia, e quindi permettere l'aggiornamento del software verso i virus realmente circolanti.
Essendo questa versione del software distribuita come freeware (gratuita), la telefonata di segnalazione di infezioni in atto non è in alcun modo vincolante. Segnalare la proliferazione di un certo codice virale significa dare modo di aggiornare il software verso i reali bisogni dell'utenza, e quindi dare un serio contributo alla lotta anti-virale.

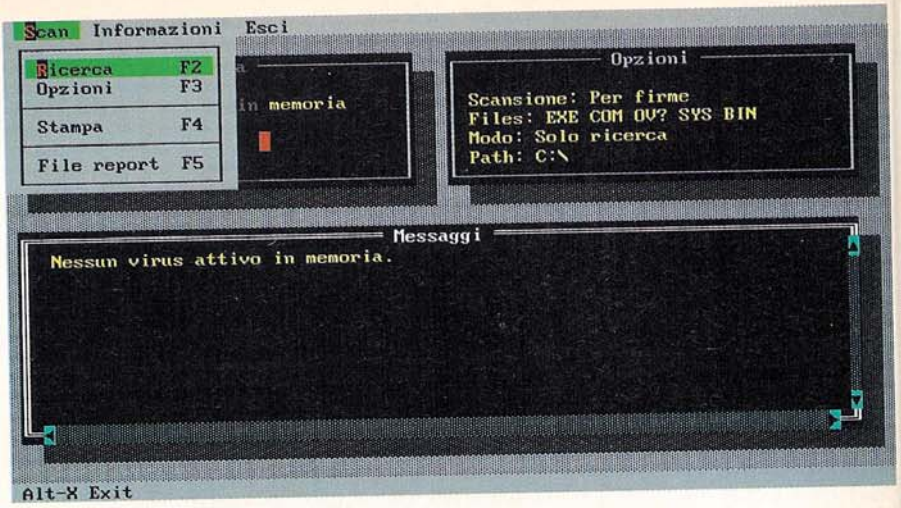

Figura 1:La scrivania di VirIT.

Come usare VirIT

L'utilizzo del programma viene di seguito esposto, raccomandiamo agli utilizzatori esperti e non di seguire attentamente il contenuto di queste note. Nessuna responsabilità è imputabile all'autore del programma nel caso di danni diretti o indiretti causati dal suo utilizzo. (Tutti i diritti sono riservati).
I file componenti sono stati compressi entro l'archivio autoestraente **VIRITSFX.EXE**. Li si scompatta con note modalità, le stesse illustrate nel primo articolo. Si tratta degli archivi seguenti: **VIRIT.EXE**, **VIRIT.INI**, **NEWVIRIT.94E**, **ANALISI.TXT** e **VIRITCAT.TXT**.
Dopo di che si compiano i passi seguenti.

- Fare una copia su apposito dischetto dei suddetti file e proteggere il dischetto dalla scrittura;
- lanciare il programma digitando:

VIRIT [INVIO]

Subito appare una schermata con la denominazione del programma nonché il nome dell'autore. Dopo la conferma con [OK] si accede al programma vero e proprio, la cui "scrivania" è costituita da tre finestre, mentre nella parte alta dello schermo figura una barra di menu (figura 1).
In tale barra menu, orizzontalmente, si possono notare tre voci:

Scan
Informazioni
Esci

Facendo clic con il mouse sulla voce **Scan** oppure premendo contemporaneamente i tasti [Alt] [S] si accede a un menu a tendina con le seguenti opzioni (accanto i tasti funzione equivalenti):

Ricerca F2
Opzioni F3
Stampa F4
File report F5

Esaminiamo sinteticamente le caratteristiche di ciascuna.

Ricerca

Dà inizio alle operazioni di scansione e/o rimozione. Prima di ciò viene però visualizzata la finestra attraverso la quale viene definita la directory o il drive da analizzare. Esempi: C: = Analisi dell'intero disco C; C:\MIADIR = Analisi dell'intera directory MIADIR.
Dopo aver inserito il percorso, ed aver confermato hanno inizio le operazioni di ricerca, con le modalità predefinite (o di default) nel menu Opzioni.

Opzioni

Visualizza la finestra delle opzioni (figura 2), dalla quale possono essere fissati: a) File da scandire; b) Scansione: ( ) EXE COM OV? SYS BIN ( ) Per firme ( ) Tutti ( ) Euristica; c) Altre: ( ) Solo ricerca ( ) Ricerca con rimozione automatica ( ) Ricerca con richiesta rimozione ( ) Ricerca con cancellazione files automatica ( ) Ricerca con richiesta cancellazione files ( ) Ricerca con rinominazione automatica ( ) Ricerca con richiesta rinominazione. Per passare da una finestra all'altra premere il tasto **Tab**.

Stampa

Permette di stampare il report della scansione avvenuta.

File report

Crea un file di report **VIRIT001.REP**, contenente il risultato della scansione.
Tornando alla barra menu, un clic del mouse

sulla voce **Informazioni** o la pressione contemporanea dei tasti **Alt+I** dà accesso a un sottomenu con le voci:

Rilasciato a...
Distributore
Programma
Autore

La prima rivela il nominativo dell'azienda a cui il software è stato rilasciato. La seconda voce dà informazioni relative al distributore ufficiale del software. Analogamente con le altre due voci.
Infine attivando con il mouse l'opzione **Esci** della barra menu o premendo assieme Alt+E si accede a un menu con le voci:

Salva opzioni
Esci Alt-X

La prima crea il file VIRIT.INI con la configurazione corrente del programma, mentre con Esci, ovviamente, si esce dal programma.

Esempio di utilizzo

Esempio di scansione. Premere la voce RICERCA o il tasto **F2**, digitare il path da scandire (es. "C:" per scandire l'intero disco C). La ricerca verrà eseguita sul percorso definito con le modalità di default del menu opzioni: a) File da scandire; b) Scansione: (*) EXE COM OV? SYS BIN (*); Per firme; Tutti; Euristica; c) Altre: (*) Solo ricerca; Ricerca con rimozione automatica; Ricerca con richiesta rimozione; Ricerca con cancellazione files automatica; Ricerca con richiesta cancellazione files; Ricerca con rinominazione automatica; Ricerca con richiesta rinominazione.
Conclusa la scansione con le modalità di default, si acceda al menu OPZIONI per modificare le modalità di ricerca ad esempio per passare dalla semplice ricerca alla ricerca con richiesta rimozione, o qualunque altra combinazione possibile.
Scegliere a questo punto la voce Ricerca o premere il tasto F2 per dare inizio alla scansione. Nella finestra in alto a sinistra apparirà il nome del file analizzato nell'istante considerato, nella finestra in alto a destra la corrente cofigurazione di VirIT e nella finestra in basso il report della scansione.

Esempio di rimozione. Prima di eseguire la rimozione su HARD DISK o dischetti, si procederà alla verifica della funzionalità del programma. Creando una directory con un nome piacere (es. VIRUS) copiare alcuni files .COM e .EXE infetti nella direcory appena creata (si scelgano file dalla funzionalità evidente, es. test mouse, giochini ecc.).

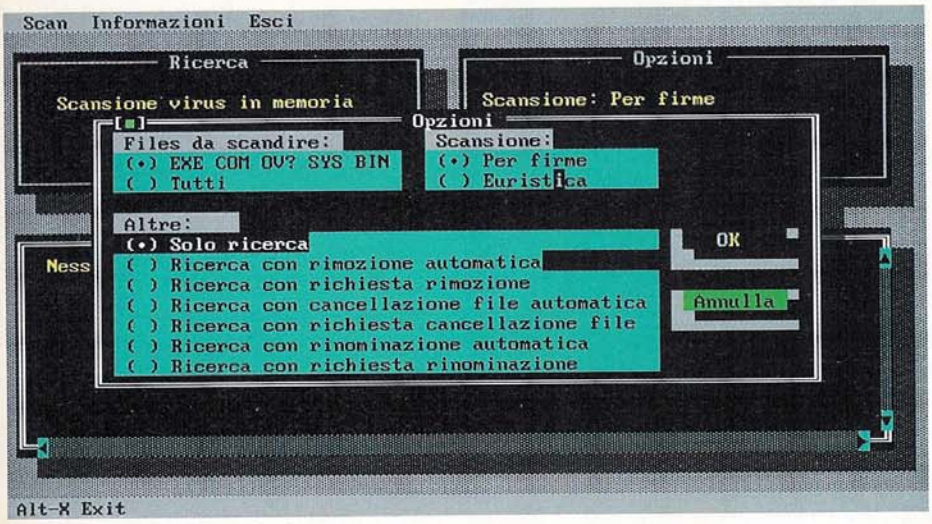

Figura 2:La finestra delle opzioni.

Eseguire VirIT con le seguenti operazioni: premere la voce RICERCA o il tasto F2; digitare il path da scandire (es. C:\VIRUS per scandire la directory VIRUS); scegliere la voce Opzioni o il tasto F3, selezionare Ricerca con richiesta Rimozione; scegliere Ricerca o il tasto F2 per dare inizio alla scansione. Nella finestra in alto a sinistra apparirà il nome del file da analizzare, nella finestra in alto a destra la corrente cofigurazione di VirIT e nella finestra in basso il report della scansione.
Esempio: C:\VIRUS\MIOFILE.COM Infetto da Jerusalem.1588 virus ** VIRUS RIMOSSO.
Concluse queste operazioni, premere Alt+X per uscire, e verificare la funzionalità dei file appena ripuliti dal codice virale. Se l'operazione ha buon esito procedere alla rimozione sulla totalità dei supporti magnetici, altrimenti inviare alcuni files infetti al ricercatore antivirus Gianfranco Tonello, il quale provvederà ad aggiornare il software VirIT.

Per informazioni:
Gianfranco Tonello
Via Sardegna, 5
35030 - Sarmeola di RUBANO (PD)
Tel. 049/631748
FidoNet: Gianfranco Tonello 2:333/316.4
E-mail: tge@maya.dei.unipd.it