a cura di Enrico Tonello

Il virus Form

Un virus pressoché innocuo ma pur sempre fastidioso

Il virus Form è stato isolato per la prima volta nell'anno 1990, il codice virale è di origine svizzera ma ha una diffusione mondiale ed è particolarmente attivo in Italia. E' residente in memoria (TSR), infetta il boot sector dei floppy disk e quello della partizione attiva del disco fisso.

Quando il Form si attiva dal boot dei floppy disk si alloca in memoria e la memoria libera del sistema diminuisce di 2 Kbyte. Viene caricata in memoria la seconda parte del codice virale, e infettato il disco fisso. In questa fase viene copiata alla fine del disco fisso la seconda parte del codice virale e il boot sector originale della partizione attiva (figura 1). A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) e il 18 di ogni mese anche l'interrupt 09H (Keyboard).

Ogni floppy disk non protetto in scrittura verrà quindi infettato dal codice virale. Il virus Form

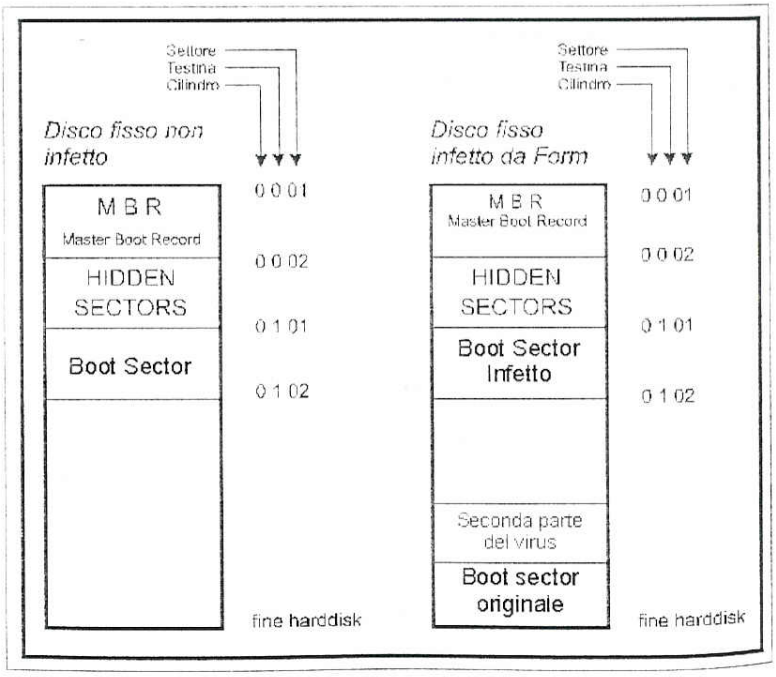

Figura 1: La metodologia di infezione del disco fisso.

I virus al microscopio

Nome:	Form
Alias:	Nessuno
Variante:	Nessuna
Stato:	Endemico
Isolato:	Noto dall'anno 1990
Sintomi:	Diminuzione della memoria libera del sistema, "click" dallo speaker del PC
Origine:	Svizzera
Dimensione:	2 settori (512 byte)
Tipo:	Residente in memoria, infetta boot sector dei floppy disk e del disco fisso

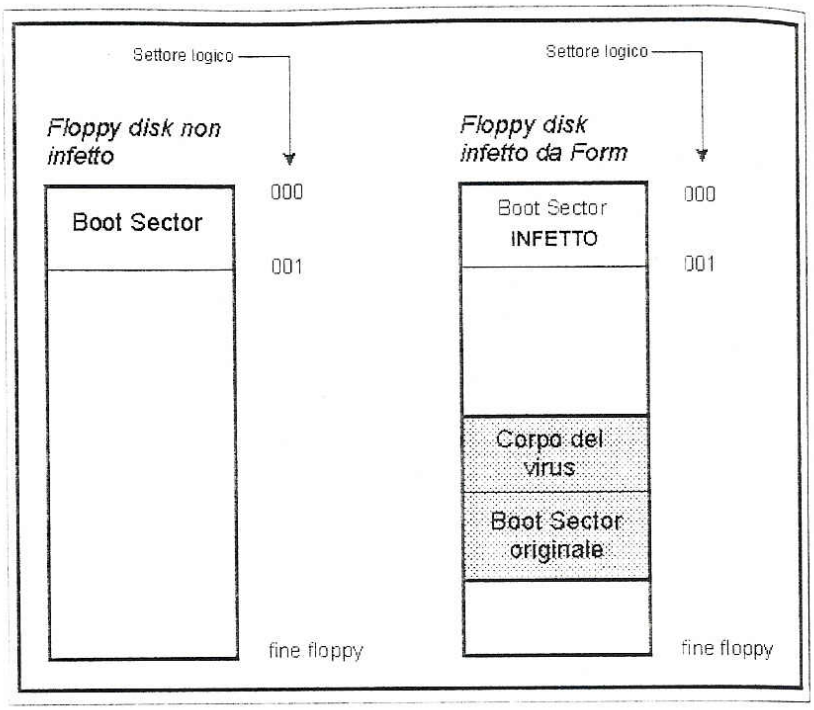

Figura 2: **Ecco come è strutturata invece l'infezione dei floppy.**

modifica poi la FAT (File Allocation Table) del floppy, in modo da alterare due settori marcandoli come bad cluster. In questi due settori verrano registrati la seconda parte del codice virale e il boot sector originale del floppy (figura 2). I settori in scuro indicano che sono marcati come bad cluster, in questo modo il codice virale evita di venire sovrascritto casualmente. La posizione dei settori marcati bad è variabile da floppy a floppy, dipende dalla quantità di dati registrata al suo interno.

Il codice virale Form si attiva il 18 di ogni mese, intercettando l'interrupt 09H per la gestione della tastiera, l'intento dell'autore era quello di emettere un "click" dallo speaker del calcolatore ogni qual volta si premeva un tasto. Questo effetto sembra non funzionare correttamente in alcune configurazioni di sistema.

Il virus Form contiene inoltre il seguente testo: "The FORM-Virus sends greetings to every one who's reading this text. Form doesn't destroy data! Don't panic! (...)", che però non viene mai visualizzato a video.

PC MAGAZINE

Modulo di segnalazione di attacco da Computer Virus

Dati completi del mittente: ----------

Data dell'attacco: ----------
Nome del virus: ----------
Numero di computer infettati: ----------
Prodotto anti-virus utilizzato: ----------
Presunta fonte dell'infezione: ----------