a cura di Enrico Tonello

Il virus B1

Il virus B1 è stato isolato per la prima volta in Italia nel mese di Ottobre 1994, e molto probabilmente la sua origine potrebbe anche non essere italiana, visto che è conosciuto negli Stati Uniti con il nome NYB.
Colgo l'occasione per sottolineare come sia necessario che i produttori di antivirus si uniformino a un unico standard, per riuscire a capire quali e quanti siano i virus realmente circolanti. A tale proposito gli sviluppatori di anti-virus europei sono per la maggior parte uniformati allo standard C.A.R.O. (Computer Antivirus Research Organization). Gli sviluppatori d'oltre oceano snobbano questo standard e si affidano alla classificazione del N.C.S.A. (National Computer Security Association).
Per tornare a B1, il codice virale risulta essere residente in memoria (TSR), stealth, infetta il boot sector dei floppy disk e l'MBR (Master Boot Record) del disco fisso. Quando il B1 si attiva dal boot dei floppy disk, si colloca in memoria nel modo consueto occupando 1 Kbyte, e la memoria libera del sistema diminuisce di conseguenza. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) all'indirizzo CS:0044H e infettata la tavola delle partizioni (Master Boot Record, MBR) dell'hard disk. L'infezione dell'MBR è similare a quella addottata da molti codici virali equivalenti, e l'originale viene salvato nella posizione: cilindro 0, testina 0, settore 17.
Una caratteristica del codice virale è quella di essere invisibile (stealth) quando è residente in memoria. Andando a leggere il boot sector di un floppy disk o l'MBR di un disco fisso infetto, il virus B1 mostrerà rispettivamente i settori originali, quelli non infetti. Ad ogni accesso all'interrupt 13H con la funzione (AH=02 Read Disk/Diskette Sectors), il codice virale B1 legge il secondo e il terzo byte del Timer Ticks Counts (0040:006C) ed esegue l'operazione AND con il valore 178FH. Se questa operazione risultasse nulla, allora viene attivata la routine di payload del codice virale. Il payload del virus B1, consisterebbe nella lettura in modo alternativo del settore di coordinate cilindro=0 testina=0 settore=1 e del settore di coordinate cilindro=255 testina=0 settore=1 (in caso di floppy disk) o del settore di coordinate cilindro=1023 testina=0 settore=1 (in caso di hard disk).
Nel caso di floppy disk, la lettura del cilindro 255 non è fisicamente possibile con i correnti disk drive in commercio. I valori limiti per i drive da 1.44 Mbyte e 2.88 Mbyte nei vari formati è di 80 cilindri per testina. Quindi il tentativo di accesso al cilindro 255 produrrebbe lo sbattimento della testina del drive contro il fine corsa. Il payload del codice virale B1 potrebbe in alcuni casi danneggiare la testina del disk drive. Fino ad ora però non è ancora stata segnalata da alcuno questa situazione, e abbiamo evitato di riprodurre l'evento in laboratorio.

Occhio a...

...B1 (Boot) e Stoned.Angelina. Il primo virus causa una serie di segnali d'errore ogni volta che si tenta di formattare un floppy, impedendo l'uso dei dischetti. I segnali d'errore generati sono particolarmente credibili e inducono a pensare che il dischetto usato possieda qualche difetto. Un sistema colpito da B1 non sarà più in grado di formattare i dischetti, mentre riuscirà ad effettuare copie su e da dischetti già formattati e contenenti dati, questo per permettere il diffondersi del "contagio". Il virus Stoned.Angelina invece sembra sia apparso sul nostro territorio solo recentemente, probabilmente proveniente dalla Germania, ed è attualmente in fase di studio. Nelle prossime puntate della rubrica spero di potervi fornire notizie più dettagliate su entrambi i virus. Nel frattempo occhio...al drive, e prima di gettare dischetti che vengono segnalati inutilizzabili durante un processo di formattazione, procuratevi un anti-virus in grado di rilevare la presenza del virus B.