PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 2 - numero 85 di mercoledì 05 aprile 2000

Allarme virus!

In circolazione un nuovo virus che e' in grado di formattare l'hard disk. Come si diffonde e come agisce.

La notizia giunge dagli USA dove l'FBI sta indagando riguardo alla diffusione del virus conosciuto come "911 Share Virus".
Il nome e' dovuto al fatto che il virus, quando infetta un computer, decide in base ad un criterio casuale o di formattare i dischi rigidi o di chiamare via modem il 911, il numero americano per le emergenze.
Il virus e' conosciuto anche come: "Bat/911" e "Foreskin", " Bat/Chode.worm", ma il suo "vero" nome e' "W95/Firkin.worm".

Il virus non si diffonde mediante la posta elettronica, bensi' su reti di condivisione dei file; dalle indagini sembra emergere che il virus si sia propagato attraverso grossi provider Internet e che abbia raggiunto alcune reti aziendali.
La presenza del virus e' stata segnalata sui network di AmericaOnline, MCI WorldCom, AT&T, NetZero.

Come agisce "911 Share Virus"?
Copia i file ashield.pif e mstum.pif nel percorso "windowsstartm~1programsstartup". Questi file si attivano quando il computer viene riavviato. Ashield.pif avvia hide.bat, un file che utilizza ashield.exe, mentre "mstum.pif" attiva mstum.bat.

Questo file genera una serie di altri file (da a.bat, b.bat, c.bat...fino a j.bat), che contengono i codici necessari a scansionare le sottoreti cui è collegata la macchina infetta, e modifica altri file tra i quali final.bat.
mstum.bat individua i dischi condivisi nella rete e li rende condivisibili anche da internet.
I file del worm vengono copiati in "c:progra~1foreskin" e in "j:progra~1foreskin".

Quando la macchina viene riavviata, tentera' di chiamare il 911 oppure, secondo uno schema casuale, di formattare tutti i dischi rigidi ai quali accede lasciando un messaggio: "You have been sLamMeD By fOREsKIN mOThERfUCKER".
