PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 590 di mercoledì 03 luglio 2002

Allarme worm!

"Kowbot" si diffonde tramite le reti KaZaa. Come riconoscerlo?

Nel numero 560 di PuntoSicuro abbiamo dato notizia della diffusione del worm Benjamin sulle reti KaZaa peer-to-peer, reti di comunicazione che permettono lo scambio diretto di dati, programmi e documenti tra computer.

Ora la rete KaZaa è veicolo di diffusione di un nuovo worm, denominato Kowbot.
Si tratta di un "cavallo di Troia", cioè di un programma dannoso mascherato da applicazione "innocente".

Nel caso sia eseguito un file infetto, il worm si copia numerose volte nella cartella utilizzata per la condivisione dei file.
I nomi utilizzati, scelti a caso in una lista di 157 titoli, riguardano per lo piu' materiale pornografico, software per l'hacking, giochi e film.
Il worm si puo' celare, ad esempio, in questi file: Star Wars Episode 2 - Attack of the Clones VCD CD2.exe, WinRAR with crack.exe, Windows 2000 win2k password stealer.exe, Playstation 2 PS2 Emulator.exe, Credit Card number generator VERIFIER (cc cc#).exe.
A mettere all'erta l'utente del possibile pericolo sono le esigue dimensioni del file: 19,584 bytes (19 K).

Una volta eseguito, il worm permette di svolgere azioni quali l'invio al suo autore di informazioni sulla macchina colpita (ad esempio sistema operativo utilizzato e software installati), o l'aggiornamento del virus con una nuova versione.

Inoltre Kowbot puo' essere utilizzato da remoto per attaccare i server Internet Relay Chat.
