PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 560 di mercoledì 22 maggio 2002

Attenzione: nuovo worm in rete!

L'''infezione'' utilizza le reti KaZaa peer-to-peer per diffondersi. Privacy a rischio?

Dalle aziende produttrici di antivirus giunge la segnalazione di un nuovo worm che per diffondersi utilizza le reti KaZaa peer-to-peer, reti di comunicazione che permettono lo scambio diretto di dati, programmi e documenti tra computer.

Esposti all'infezione del worm Benjamin, capace di celarsi in file apparentemente innocui, sono solo i computer che hanno il software per le reti KaZaa installato.
Quando un file nel quale e' contenuto il worm viene eseguito mostra il seguente messaggio di errore fasullo:
"Error
Access error #03A:94574: Invalid pointer operation
File possibly corrupted."

Il worm modifica la configurazione del sistema in modo tale da essere eseguito ad ogni successivo riavvio del sistema. Benjamin legge le impostazioni del software per le reti KaZaa, crea una directory chiamata Sys32 nella directory temporanea di Windows e la rende visibile a tutti gli altri sistemi connessi alla rete P2P.

Il worm riempie questa directory con copie di se stesso; per non essere individuato si duplica utilizzando svariati nomi, in particolare titoli di famosi software, film, giochi e canzoni. Ad esempio "AbeautifulMin, ACDSeePowerPackRetail-installer, Adobe Photoshop 6.0 -full-downloader, Adobe Pagemaker -full-downloader, American Pie 2 -divx-full-downloader."
Un utente di KaZaa, cercando un file, potrebbe quindi imbattersi nel worm...

---

www.puntosicuro.it