PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 658 di giovedì 07 novembre 2002

Worm in circolazione

"Brid.A" si diffonde via e-mail. Conosciamone le caratteristiche.

E' stata segnalata la recente diffusione di Brid.A (detto anche Braid.A), un nuovo worm che si diffonde via e-mail e contiene una variante del worm FunLove.
Brid.A può colpire le seguenti versioni di Windows: 95, 98, NT, 2000, XP, Me.

Aprendo il file README.EXE allegato all'e-mail infetta, il worm cerca di connettersi ad hotmail.com.
In un secondo tempo cerca di inserire numerosi file nel sistema (tra i quali explorer.exe e help.hml sul Desktop), modifica chiavi di registro, attiva una variante del virus Funlove.

Nel caso l'utente abbia una versione di Internet Explorer non aggiornata con le patch rilasciate da Microsoft, il worm cerca di sfruttare una vulnerabilità per eseguirsi in modo automatico.

Il worm una volta attivato cerca di autoinviarsi, utilizzando un proprio motore SMTP, agli indirizzi reperiti nei file HTM e .DBX.
Queste le caratteristiche della e-mail infetta:

Da: [Proprietario del computer infetto]
Soggetto: [Nome dell'azienda]
Testo: Hello,
Product Name: [Versione del sistema oprativo Windows]
Product Id: [id del prodotto Windows]
Product Key: [chiave di registrazione]
Process List: [Processi in corso al momento dell'infezione]
Thank you.
Allegato:"README.EXE"

Il worm vuole indurre l'utente a ritenere che il messaggio provenga da un programma antivirus; in alcuni casi appare infatti il messaggio "Anti Virus World System" da "Trend Microsoft Inc."
