PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 394 di giovedì 06 settembre 2001

Nuovo worm in Rete: Apost

Medio il livello di rischio per ora rilevato.

Apost alias Readme è il nuovo worm che si sta diffondendo in Europa dall'inizio della settimana.
Questo virus è contenuto in un file eseguibile formato PE di 24576 bytes e utilizza MS Outlook per diffondersi. Spedisce, infatti, a tutti gli indirizzi della Rubrica dell'utente colpito, un messaggio con il file infetto "Readme" in allegato.

Il messaggio "sospetto" si presenta con questa linea soggetto: "As per your request", mentre il corpo è "Please find attached file for your rewiew.
I look forward to hear from you again very soon. Thank you".

L'utente infetto non ha la possibilità di vedere le mail inviate in automatico, poiché vengono cancellate subito dopo l'invio, quindi la propagazione del virus procede rapidamente.

Symbolic, che ha annunciato la diffusione del virus, fornisce, nel proprio sito, le indicazioni per ripulire manualmente la macchina.
Basterà, infatti, cancellare il file README.EXE dalla directory di Windows e dalle directory radice di tutti i dischi.
Nel caso in cui il file fosse bloccato sarà necessario riavviare in modalità DOS e cancellare il file con il comando DEL.
Su piattaforme WinNT e Win2000 sarà, invece, utile rinominare il file con un'estensione non eseguibile, riavviare il computer e cancellare il file stesso.
