PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 943 di giovedì 19 febbraio 2004

Worm...rinnovati

Segnalata la diffusione di una nuova variante del worm Bagle. Le caratteristiche dell'infezione.

L'infezione del worm Mydoom sembra ora contenuta, ma si affaccia ora una nuova minaccia per la sicurezza di computer e reti informatiche. In realtà si tratta di una "vecchia conoscenza", il worm Bagle, ripresentatosi sotto una nuova veste.

Bagle.B, così è stata denominata la variante, può mettere a rischio sicurezza e la riservatezza dei dati contenuti nel PC colpito. Infatti, secondo quanto riportato da Symbolic, il worm "contiene una backdoor che ascolta sulla porta 8866. Questa backdoor può essere sfruttata per avere accesso al computer sul quale in worm è in esecuzione permettendo di scaricare ed eseguire file inviati alla backdoor in un certo formato."

Il worm si diffonde via e-mail. Il messaggio contenente l'allegato infetto ha le seguente caratteristiche, in parte variabili:
Oggetto:
ID [caratteri casuali]...thanks
Testo:
Yours ID [caratteri casuali]
--
Thank
Allegato:
[caratteri casuali].exe
L'allegato ha una icona che rappresenta un file audio.

Il worm raccoglie indirizzi mail ai quali inviarsi da file con le seguenti estensioni: .html, .html, .wab, .txt.
