PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 922 di mercoledì 21 gennaio 2004

Worm in circolazione

Medio il livello di gravità dell'infezione. La caratteristiche dell'e-mail "contagiosa".

Gli esperti di Symbolic hanno segnalato, nei giorni scorsi, la diffusione di un nuovo worm che si diffonde tramite e-mail. "Bagle", così è stato denominato il worm, si cela nel file, con nome casuale ed estensione ".exe", di una e-mail riconoscibile dal soggetto: Hi.
Il messaggio infetto si presenta nel modo seguente:
Da: [indirizzo casuale]
Soggetto: Hi
Testo:
Test =)
[sequenza casuale di caratteri]
--
Test, yep.

Se il file viene aperto, Bagle si copia nella directory di sistema di Windows e modifica le configurazioni in modo tale da attivarsi ad ogni riavvio della macchina.
Quando il worm si avvia la prima volta, apre la calcolatrice di Windows (calc.exe) per nascondere la sua presenza.
Una volta installatosi, Bagle ricerca indirizzi e-mail, a quali inviarsi, nei files WAB (Windows Address Book), file di testo ed HTML.
Secondo quanto riferito dagli esperti di Symbolic, Bagel contiene una backdoor che permette di accedere da remoto su una macchina infetta e che può essere sfruttata per scaricare ed eseguire programmi da Internet. In particolare tale funzionalità verrebbe usata per raccogliere gli indirizzi delle macchine infette.
Il worm Bagle tenta inoltre di scaricare sulla macchina infetta un altro il "cavallo di troia" dal web.

La diffusione di Bagle dovrebbe presto esaurirsi, infatti è programmato per disattivarsi il 28 gennaio 2004...salvo la comparsa di varianti.
Ricordiamo infatti che nel maggio scorso, il virus Sobig, programmato per essere inoffensivo a partire dal 31 maggio 2003, aveva imperversato in rete a lungo tempo, riproponendo numerose varianti nelle quali la "scadenza" era posticipata. (Si vedano a tale proposito i numeri di PuntoSicuro del 20 maggio 2003 e del 5 giugno 2003).
