PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1057 di giovedì 29 luglio 2004

Worm in agguato

Elevato il livello di allarme per Mydoom@mm che si diffonde via e-mail. Come riconoscerlo.

Pubblicità

Un nuovo worm che si diffonde via e-mail minaccia e intasa le caselle di posta elettronica; si tratta di Mydoom@MM, un worm che Symantec pone al livello di gravità 4 (su una scala di 5).
Molti utenti potrebbero essere tratti in inganno ed aprire il file infetto allegato al messaggio spedito da Mydoom, in quanto il worm riesce a mascherare il nome del mittente, utilizzando anche indirizzi trovati sui computer infettati.

Il worm utilizza un proprio motore SMTP per inviarsi a tutti gli indirizzi di posta che trova su un sistema infetto. L'e-mail presenta un allegato con estensione file .bat, .com, .cmd, .exe, .pif, .scr, o .zip; l'allegato può avere una seconda estensione, solitamente .doc, .txt, .htm, o .html.
Il nome dell'allegato può contenere un dominio scelto a caso, trovato sul sistema del mittente.
Il soggetto dell'e-mail è scelto tra i seguenti: "say helo to my litl friend", "click me baby, one more time", "hello", "error", "status", "test", "report", "delivery failed", "Message could not be delivered", "Mail System Error - Returned Mail", "Delivery reports about your e-mail", "Returned mail: see transcript for details".
Il contenuto del corpo del messaggio può variare, scelto tra una serie di frasi.

Sono vulnerabili al worm i sistemi operativi: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP.
Una volta installatosi, Mydoom@MM scarica ed esegue una backdoor, rilevata come Backdoor.Zincite.A, sulla porta TCP 1034. Connettendosi a tale porta un assalitore potrebbero assumere il controllo del computer infettato.