PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1071 di giovedì 02 settembre 2004

Foto...con l'inganno

Ampia diffusione in Italia di varianti di Bagle; come riconoscere l'infezione.

Pandasoftware ha classificato a livello di gravità 3, su una scala di 4, due varianti del worm Bagle (Bagle.AV e Bagle.AW, BeagleAQ), che hanno fatto registrare una ampia diffusione in Italia nei giorni scorsi.

Il worm Bagle, "padre" delle numerose varianti è apparso per la prima volta nel mese di gennaio.

Anche le nuove varianti si diffondono via e-mail, tramite l'allegato di un messaggio; una volta aperto l'attach il worm esegue file scaricati da siti web e si autoivia a indirizzi reperiti sul computer infettato. Per mascherarsi, il worm cerca di bloccare i programmi di sicurezza.

Riconoscere l'e-mail dell'infezione è semplice, ma proprio per l'essenzialità del messaggio essa potrebbe trarre in inganno, soprattutto se giunge da una persona conosciuta. Questa caratteristica ne ha facilitato la diffusione.

Soggetto: foto
Testo del messaggio: foto
Allegato:FOTO.ZIP FOTO1.ZIP (oppure FOTOS.ZIP)

L'allegato contiene due file, uno con estensione .HTML, l'altro è un file nascosto con estensione .EXE.
