PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 758 di giovedì 10 aprile 2003

Worm a caccia di indirizzi

Symantec ha rilevato un "curioso" worm. Le caratteristiche dell'infezione.

Colpisce i sistemi Windows (95, 98, NT, 2000, XP, Me) il nuovo worm, denominato W32.HLLW.Cult.C@mm, segnalato da Symantec.

I veicoli di diffusione sono quelle tradizionali, W32.HLLW.Cult.C@mm si cela nell'allegato di un messaggio di posta elettronica, composto nel modo seguente:

Soggetto: Hi, I sent you an eCard from BlueMountain.com
Messaggio: Hi , I sent you an eCard from Blue-Mountain.com To view your eCard, open the attachment
If you have any comments or questions, please visit http:/ /www.bluemountain.com/customer/index.pd
Thanks for using BlueMountain.com.
Attachment: BlueMountaineCard.pif

Particolare è invece la modalità con la quale il worm cerca gli indirizzi di posta elettronica ai quali inviarsi. Diversamente da quanto in genere accade, il worm non "ruba" gli indirizzi dalla rubrica del programma di posta elettronica installato sul pc infettato.
W32.HLLW.Cult.C@mm "crea" migliaia di indirizzi ai quali inviarsi, creando un traffico eccessivo del server di posta elettronica, nel modo seguente:
[cognome casuale preso da una determinata lista][numero casuale]@[dominio scelto tra: email.com, earthlink.net, roadrunner.com, yahoo.com, msn.com, hotmail.com].

Nel caso l'invio vada a buon fine e l'incauto utente clicchi l'allegato al messaggio, il worm modifica alcuni parametri di sistema in modo tale da essere attivato ad ogni riavvio del sistema e crea una backdoor, tramite la quale possono essere inviati e modificati dati all'insaputa dell'utente.

Ulteriori informazioni possono essere reperite sul sito di Symantec.