PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1067 di venerdì 27 agosto 2004

Pericolo "variante"

Si diffonde via e-mail una nuova versione del worm Mydoom. Le caratteristiche dell'infezione.

E' stata classificata da Symantec al livello 3 di pericolosità (su una scala di 5) la nuova variante del worm Mydoom (Mydoom.S@MM), individuata nel mese di agosto.

Come le varianti precedenti, il worm è contenuto in un file allegato ad un messaggio e-mail. Prima della propagazione il worm raccoglie gli indirizzi e-mail dal computer infetto. Il worm, per non essere facilmente individuato, non si trasmette agli indirizzi e-mail che contengono determinate parole, tra le quali "syma", "msn", "hotmail", "abuse", "spam", "secur".

Secondo quanto riportato dall'azienda di sicurezza Symbolic, le e-mail che il worm usa per diffondersi hanno la seguente forma:
Oggetto:
photos
Testo:
LOL!;))))
Attachment:
photos_arc.exe
L' indirizzo e-mail del mittente è falsificato. Il worm usa nomi comuni, tra i quali: anna, alex, alice, bob, claudia, michael, mike, maria, mary, robert. Attenzione, quindi, ad aprire gli allegati dei messaggi, anche se vi sembrano provenire da indirizzi conosciuti.

Il worm, al quale sono vulnerabili i sistemi Windows, modifica alcune impostazioni del computer infetto per impedire all'utente e alle applicazioni locali di raggiungere i siti web dei fornitori dei prodotti Anti-Virus.

---

www.puntosicuro.it