PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 927 di mercoledì 28 gennaio 2004

Allarme worm!

Si diffonde tramite le reti Peer-to-Peer e via e-mail. Contagio rapido.

Sta imperversando nelle caselle di posta elettronica in tutta Italia il worm Mydoom, denominato anche Shimgapi o Novarg, che Symantec ha posto ai massimi livelli di pericolosità (livello 4 su un massimo di 5).

Secondo quanto appreso da Symbolic, Mydoom si diffonde attraverso e-mail e le reti peer to peer Kazaa. Quando eseguito apre il blocco note di Windows visualizzando caratteri a caso. Nelle e-mail utilizza un oggetto, corpo ed allegato variabile.
Il worm installa sul computer infetto una backdoor in grado di ricevere un file eseguibile e di eseguirlo sulle macchine già infette.
Il worm raccoglie indirizzi email a cui inviarsi dal Windows' Address Book e da file con varie estensioni, tra le quali dbx, php, htm, txt.
Il worm inoltre sarebbe stato programmato per sferrare, il 1 febbraio 2004, un attacco del tipo DDoS al sito SCO.COM.
Secondo quanto riportato da Symbolic, nel caso un computer sia infettato, "quando la macchina viene avviata dal primo Febbraio, il worm richiede la pagina iniziale del sito SCO.COM ogni secondo per ogni macchina infetta nel mondo. La richiesta è una semplice "GET / HTTP/1.1", creata appositamente per sovraccaricare il loro webserver"

I messaggi e-mail tramite i quali il worm si diffonde hanno le seguenti caratteristiche. Il mittente è preso tra gli indirizzi individuati nella macchina infetta. L'oggetto del messaggio è scelto tra i seguenti: test, hi, hello, Mail Delivery System, Mail Transaction Failed, Server Report, Status, Error.
Il testo dell'e-mail è del tipo " test", oppure "The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.", "The message contains Unicode characters and has been sent as a binary attachment", oppure "Mail transaction failed. Partial message is available."
Gli allegati sono composti combinando i nomi: document, readme, doc, text, file, data, test, message, body. L'estensioni del file è una delle seguenti: pif, scr, exe, cmd, bat.

Per quanto riguarda la diffusione attraverso P2P, il worm scandisce il registro di Windows cercando il valore contenente la directory condivisa di Kazaa, si copia al suo interno con il un nome scelto in una lista (winamp5, icq2004-final, activation_crack, strip-girl-2.0bdcom_patches, rootkitXP, office_crack, nuke2004), con una delle seguenti estensioni: pif, scr, exe, bat.
