PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 940 di lunedì 16 febbraio 2004

Vulnerabilita' e nuovi worm

Una grave falla nei sistemi Windows e worm con nuove modalità di diffusione potrebbero mettere a rischio la sicurezza informatica di milioni di utenti.

Settimana negativa quella appena trascorsa per la sicurezza informatica di milioni di utenti, dalle aziende ai privati cittadini.
Un grave baco di sicurezza riguardante il sistema operativo Windows è stato reso noto da Microsoft, che ha sollecitato tutti gli utenti all'applicazione immediata della patch disponibile nel bollettino MS04-007.
La vulnerabilità è del tipo Buffer Overrun (sovraccarico del buffer); se viene sfruttata consente ad un assalitore di effettuare qualsiasi operazione sul sistema interessato, incluse installazione di programmi, visualizzazione, modifica o eliminazione di dati e creazione di nuovi account con pieni privilegi.

Fonte di preoccupazione è anche la diffusione di nuovi tipi di worm, capaci di diffondersi anche senza utilizzare il tradizionale espediente dell'e-mail ingannevole.
E' il caso di Doomjuice, un worm che "va a caccia" di computer colpiti dal precedente worm MyDoomA; nel caso la ricerca abbia esito favorevole Doomjuice si installa senza che l'utente se ne accorga, mediante una porta "aperta" da MyDoomA.
Doomjuice, come il suo predecessore, effettua un attacco di tipo Distributed Denial of Service contro microsoft.com, al fine di sovraccaricare il server di richieste.
In dettaglio, secondo quanto riportato da Symbolic, "per localizzare i computer vulnerabili, il worm scandisce un numero di indirizzi casuali, cercando di collegarsi alla porta TCP 3127. Se la porta è aperta, Doomjuice si spedisce all'host in un package creato in modo da essere eseguito immediatamente, causando perciò una seconda infezione."
Dopo essersi installato, Doomjuice si copia nella cartella di sistema di Windows e modifica le impostazioni del sistema.

---

www.puntosicuro.it