PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 706 di martedì 28 gennaio 2003

Patch trascurate

Il recente attacco informatico, che ha provocato blocchi della rete in molti Paesi, ha potuto diffondersi grazie a server Windows non aggiornati...

Nella notte tra sabato e domenica, in molti Paesi (in particolare dell'Asia, dell'Europa e del nord America,) si è assistito a blocchi della rete e rallentamenti provocati da attacchi del tipo Denial-of-Service causati dalla diffusione del worm denominato SQL Slammer.

Il worm non si è diffuso tramite posta elettronica, ma ha attaccato i computer con installato Microsoft SQL Server 2000 o Microsoft Desktop Engine (MSDE) 2000 e nei quali non erano state installate le patch rilasciate da Microsoft.

Il worm ha sfruttato la vulnerabilità di questi computer (alcune decine di migliaia di server), facendoli divenire di fatto una "base" dalla quale inviare incessantemente pacchetti di dati in grado di intasare la rete.
La massiccia diffusione del worm ha potuto avvenire, quindi, anche grazie all'imprudenza di amministratori di sistema che hanno trascurato l'aspetto sicurezza, non applicando gli aggiornamenti necessari.

Come riferito da Symbolic, "il codice del worm e' lungo 376 byte ed e' stato probabilmente scritto e ottimizzato utilizzando il linguaggio Assembly.". Slammer "non memorizza copie di se stesso sul disco, ma esiste solo sotto forma di pacchetti di rete e processi eseguiti nella memoria dei computer infetti."

Il worm "sfrutta una buffer overflow vulnerability in Microsoft SQL Server 2000 (MS02-039). Quando il server riceve la richiesta tramite rete, il suo buffer permette al codice del worm di essere eseguito. Dopo che il worm si e' installato nel sistema, inizia la propria routine di scansione su Internet alla ricerca di altre macchine vulnerabili." [...] "SQL Slammer cerca di collegarsi alla porta UDP 1434 sulla macchina remota, in modo da contattare il server SQL, se presente."

Gli esperti temono che il worm , che per ora non ha effetti distruttivi, possa essere nuovamente diffuso con varianti più pericolose, ad esempio in grado di modificare i dati contenuti nei computer colpiti.
