PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 401 di lunedì 17 settembre 2001

Circa mezzo milione di server a rischio sicurezza

Vulnerabilita' conseguenti agli attacchi dei virus Sadmind/IIS e Code Red II

In base all'indagine condotta dall'osservatorio Netcraft circa il 13% dei siti dotati di Internet Information Server (IIS) sono vulnerabili agli attacchi di cracker in grado di prendere il pieno controllo del sistema.

I due noti worm Sadmind/IIS e Code Red II, diffusisi rispettivamente lo scorso maggio e lo scorso agosto, hanno, infatti, installato su circa mezzo milione di server una back door denominata root.exe, che consente a qualsiasi malintenzionato di eseguire programmi di sistema utilizzando un semplice browser Web.

L'aspetto più preoccupante di questo fatto è che l'analisi, grazie alla quale è stata rilevata questa vulnerabilità, è stata effettuata soltanto su server dotati del protocollo di sicurezza SSL, in genere installato sui siti di e-commerce.

Molti server commerciali che hanno eliminato i virus citati, ma non hanno provveduto a controllare che la back door non fosse già stata installata, potrebbero ancora subire furti di numeri di carte di credito e di altri dati sensibili legati alle transazioni via internet.

---

www.puntosicuro.it