PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 561 di giovedì 23 maggio 2002

Un worm all'attacco dei MS SQL Server

Giunte alcune segnalazioni di infezione. Attenzione alle password...

Alcuni laboratori anti-virus hanno segnalato la diffusione di un worm che ha come obiettivo i server MS SQL. Il worm è conosciuto con i seguenti nomi: Digispid.B.Worm, JS_SQLSpida.B, Hacktool.IPStealer, JS.Spida.B, JS/SQLSpida.b.worm, SQLSnake, SQLSpida, MS SQL Worm.

Nei giorni scorsi era stato notato un incremento di tentativi di attacco alla porta TCP 1433, comunemente utilizzata dal database Microsoft SQL Server; un aumento anomalo non attribuibile ad attacchi "manuali" di aspiranti assalitori.

Il bersaglio del worm sono i server MS SQL nei quali l'account "sa" (login di default dell'amministratore del sistema) non e' protetto da password.
Il worm copia alcuni file sul computer infetto (tra i quali System32DriversServices.exe, System32Sqlexec.js, System32Clemail.exe, System32Sqlprocess.js, System32Pwdump2.exe, System32Samdump.dll) e cambia la password dell'amministratore in una stringa di caratteri casuali.

Una volta infettato il computer, il worm invia la configurazione ad un host remoto utilizzando la macchina appena attaccata allo scopo di propagarsi ulteriormente.

Per prevenire l'infezione, nel caso non lo si abbia ancora fatto, è bene utilizzare una password sicura per l'account dell'ammistrazione del sistema ed aggiornare l'antivirus.
Nel caso un computer sia stato infettato, è necessario fare una scansione del computer con l'antivirus e modificare le password del sistema operativo e di SQL Server.

---

www.puntosicuro.it