PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 336 di martedì 15 maggio 2001

Allarme virus!

Attacca i server Sun Solaris e Miscrosoft IIS. Si stima siano oltre 8000 i server web colpiti nel mondo...

Nei primi giorni di maggio e' stata diffusa dal CERT la segnalazione di un virus che attacca i server Sun Solaris e Miscrosoft IIS (Internet Information Server).
Secondo alcune stime, forse azzardate, nel mondo sarebbero 8000 i server colpiti.

Ad essere in pericolo sono i server non aggiornati; il virus, chiamato "sadmind/IIS Worm" o "PoizonBox", sfrutta infatti vulnerabilita' gia' note da mesi su Solaris e Windows NT, due tra i sistemi operativi piu' diffusi su Internet.

Secondo quanto riportato da un comunicato di Symbolic, azienda produttrice di antivirus, il worm "utilizza un bug noto del servizio Sadmin disponibile sulle macchine Sun Solaris per compromettere l'integrità dei server IIS " e sostituisce alla homepage di default una pagina contenente un messaggio anti-americano.

"In pratica, la piattaforma Solaris viene compromessa e utilizzata come punto di partenza su cui eseguire il worm; questo programma cercherà a sua volta altre macchine Solaris da attaccare e server IIS su cui inserire la homepage modificata."

Questa intrusione, benche' non causi alcuni tipo di problema a chi consulta la pagina web modificata, crea sicuramente danno al gestore del sito a causa dell'interruzione del servizio.

Nella nota diffusa da Symbolic e' inoltre indicato che sui siti di Sun Solaris e Microsoft IIS e' possibile reperire le patch applicabili per evitare che i server siano vulnerabili a tali attacchi (Per Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS00-078.asp
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp)
