PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 736 di martedì 11 marzo 2003

Attenzione alle password "facili"

In circolazione un nuovo worm che può colpire i sistemi Windows.

Nei giorni scorsi è stata segnalata da Symbolic la propagazione in rete di un nuovo worm, denominato "Deloder".

Il worm può infettare i computer con sistema operativo Windows che hanno una password debole per l'utente "Administrator".
Il worm agisce per tentativi, contatta un indirizzo IP (identificativo numerico unico associato a ogni singolo computer connesso ad Internet) casuale alla ricerca di macchine Windows che hanno la porta 445 (Microsoft NetBIOS su TCP/IP) aperta.
Sulle reti aziendali protette da firewall, il traffico entrante diretto a questa porta è solitamente bloccato, il che porta a ritenere che le macchine inizialmente infettate da Deloder siano
stati PC connessi direttamente a Internet (ad es. computer di utenti privati, o telelavoratori oppure Road Warriors che si trovavano all'esterno della rete aziendale).

Molti computer che si connettano da casa sono vulnerabili a questo worm se hanno la password dell'utente "Administrator" debole.
Una volta che Deloder ha trovato un macchina attaccabile il worm cerca di fare un log on come "Administrator" e prova a turno 50 password differenti, come: "xxxxxxxxxx", "", administrator", "admin", "Admin", "password", "Password", "1", "12", "123", "pass", "passwd", "database", "oracle", "sybase", "123qwe2, "ihavenopass", "enable", "2002", "200, "123abc", "alpha", "patrick", "root", "a2, "win", "login", "pass", "love", "mypc", "mypass", "pw".

Se il login riesce, il worm si copia (sfruttando di solito il nome "INST.EXE") in diverse directory Startup e aggiunge una chiave al registro per eseguirsi automaticamente.
Quando la macchina viene fatta ripartire il worm ricomincia a cercare nuovi host da infettare.
Secondo quanto affermato da Symbolic, Deloder compromette la riservatezza dei dati contenuti nei computer infetti, installandovi una backdoor che permette ad un hacker di prenderne il controllo remoto.
