PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 995 di martedì 04 maggio 2004

Un worm poco pericoloso, ma evoluto

Sfrutta una recente falla di Windows. Preoccupazione per le modalità di diffusione.

Non preoccupano i danni arrecati ai computer infettati, la diffusione del worm Sasser impensierisce gli esperti di sicurezza per la modalità di propagazione e le vulnerabilità sfruttate.

Il worm sfrutta una falla segnalata da Microsoft nel mese di aprile (Bollettino MS04-011); sono vulnerabili pertanto tutti i sistemi che non siano stati aggiornati e che siano connessi a Internet senza la protezione di un firewall opportunamente configurato. [Si veda PuntoSicuro del 16.4.4].
Secondo quanto riportato da Symbolic, il worm cerca sistemi vulnerabili effettuando una scansione di indirizzi IP casuale. Per verificare se un sistema è vulnerabile viene controllata la porta 445.
Quando attacca un computer, Sasser determina l sistema operativo per usare i parametri giusti.
Se l'attacco ha successo, Sasser invia i comandi per effettuare il download del worm dal computer infetto utilizzando il protocollo FTP. Sasser per propagarsi non utilizza, quindi, la posta elettronica, non fa leva cioè sulla curiosità degli utenti, ma sulla loro poca attenzione alla sicurezza informatica, sul fatto che molti utenti trascurino di aggiornare i programmi.
Come riconoscere il computer infettato da Sasser? Possibili indicazioni sono la presenza del file 'C:\win.log' ed il verificarsi di frequenti crash di 'LSASS.EXE'. Sasser genera inoltre traffico sulle porte TCP 445, 5554 e 9996.

---

www.puntosicuro.it