PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 692 di mercoledì 08 gennaio 2003

Reti aziendali a rischio

Segnalato un nuovo worm che si diffonde nelle reti di pc e può provocare un "Denial of Service".

Symantec ha recentemente segnalato la diffusione, per ora limitata, di una nuova minaccia per le reti di pc basate su Windows NT.
Si tratta di un worm che cerca di copiarsi nella rete e di infettare i pc, non tramite la posta elettronica, bensì mediante le risorse condivise.

I sistemi vulnerabili sono Windows 2000 e Windows XP.

Quando il worm, denominato Lioten (W32.HLLW.Lioten), viene attivato, ricerca in internet pc vulnerabili generando casualmente una serie di indirizzi IP. L'indirizzo IP generato casualmente è uno dei seguenti: [0-255].[0-127].[0-255].[0-127]; cioè con il primo blocco di numeri compreso tra 0 e 255, il secondo tra 0 e 127 ecc. (Ad esempio la macchina con indirizzo 172.155.25.66 è immune in quanto il secondo blocco di numeri non è inferiore a 127).

Il worm cerca di determinare se un indirizzo IP è valido interrogando l'indirizzo IP sulla porta 445 e cerca di utilizzare gli indirizzi IP validi per accedere alle risorse condivise del network ed installarsi su altri computer del network come "iraq_oil.exe".

Nel caso il worm si installi in molti computer del network, si puo' verificare un Denial Of Service.

---

www.puntosicuro.it