PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 628 di mercoledì 25 settembre 2002

Infezioni "mutevoli"

Segnalate varianti di "Slapper", worm che si diffonde su computer che utilizzano il sistema operativo Linux.

Continua la diffusione di Slapper, un worm della rete che si diffonde su computer che utilizzano il sistema operativo Linux (Si veda PuntoSicuro n.622.)
Il worm, che per diffondersi utilizza un bug nella libreria OpenSSL, attacca computer che eseguono il sistema operativo Linux e che utilizzano il server Web Apache con il protocollo SSL attivato.

Oltre alla versione tradizionale del worm, è stata segnalata da Symbolic la diffusione di sue nuove varianti, denominate "Cinik" e "Unlock", che come Slapper contengono un codice sfruttato per creare una rete di computer utilizzabili da remoto per lanciare attacchi di tipo denial of service (distributed denial of service).

Mentre Slapper contiene una backdoor (cioè una porta che permette di accedere alla macchina dall'esterno) che "ascolta" sulla porta 2002 e puo' essere controllata da remoto; Unlock, rilevato il 22 Settembre 2002, si presenta con un file dal nome "unlock.c" ed utilizza la porta 4156.

La variante conosciuta come "Cinik", rilevata il 23 Settembre 2002, utilizza invece la porta 1978 invece della porta 2002 e il worm si presenta con un file dal nome "cinik.c".
Il worm inoltre ha delle funzioni di backup: quando viene rimosso dall'host preleva una nuova copia di se stesso da un sito web in Romania, anche se in realta' ora la pagina del sito contenente il virus e' stata rimossa.
