PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 665 di lunedì 18 novembre 2002

Diffusi software open source "infetti"

I codici sorgente di due noti software, distribuiti in rete, sono stati modificati da un intruso e sono...pericolosi.

Il Cert, centro per la sicurezza di Internet, ha segnalato che i codici sorgente dei due prodotti open source libpcap e tcpdumpdue, distribuiti da alcuni siti, sono stati modificati da un intruso e contengono un "trojan horse", cioè un codice dannoso inserito nell'applicazione.

Le versioni modificate sono le seguenti tcpdump-3.6.2.tar.gz, tcpdump-3.7.1.tar.gz e libpcap-0.7.1.tar.gz; i pacchetti sono stati distribuiti sul server HTTP di www.tcpdump.org tra l'11 ed il 13 novembre. Tuttavia altri siti che utilizzano o distribuiscono i codici sorgente potrebbero non aver ancora tolto dai loro server le versioni "infette".

La versione del trojan horse inserita nel codice sorgente di tcpdump contiene un codice malevolo che si attiva quando il software è compilato.

Il trojan tenta di connettersi ad un sito Web per scaricare uno script di shell, cioè un insieme di comandi, chiamato services. Se l'operazione va a buon fine e lo script viene eseguito, si avvia una procedura che porta alla creazione di una backdoor che potrebbe consentire al creatore del trojan horse di guadagnare l'accesso al sistema colpito.

L'avviso del Cert.
