PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 652 di martedì 29 ottobre 2002

Quando il worm...cambia

Segnalata la diffusione di una variante del worm OpaSoft.

E' stata recentemente segnalata da Symbolic, azienda nel campo della sicurezza informatica, la diffusione di una variante del worm OpaSoft del quale abbiamo parlato nel n.635del nostro quotidiano.

Si tratta di Opasoft.A (denominato anche Worm.Win32.Opasoft.a, Brasil).
Come Opasoft, Opasoft.A si diffonde attraverso sui network di condivisione dei file; nel caso un computer ne sia infettato crea una backdoor e cerca di connettersi ad un sito internet per scaricare aggiornamenti.

Opasoft.A si installa nella directory Windows come "brasil.exe" oppure "brasil.pif" e si registra nel registro di configurazione del sistema.
Ogni volta che infetta una macchina remota il virus copia se stesso come "brasil.exe" oppure "brasil.pif" nel sistema infettato e aggiunge una corrispondente riga nel file WIN.INI.

La componente backdoor di questa variante prova a connettersi al sito www.n3t.com.br (Opasoft si connetteva invece a www.opasoft.com) per prelevare ed eseguire sia nuove versioni (quando presenti) sia script presenti nel web server.
