PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 683 di giovedì 12 dicembre 2002

Curiosita'...pericolosa

Segnalata la diffusione di un nuovo worm. Conosciamone le caratteristiche.

Symantec, nota azienda produttrice di antivirus, ha segnalato la diffusione, per ora ancora limitata, di un nuovo worm, denominato W32.Heovin@mm.
Si tratta di un mass-mailing worm che utilizza Microsoft Outlook per inviarsi a tutti i contatti presenti nella Windows Address Book. W32.Heovin@mm cerca di inviare una copia di se stesso agli altri utenti di mIRC (software utilizzato per le chat).
Il pericolo maggiore è costituito tuttavia dal fatto che il worm crea una backdoor che può consentire ad un hacker il controllo da remoto del computer infettato.

Il messaggio infetto ha le seguenti caratteristiche:
Soggetto: Flash funny pic
oppure
Soggetto: Check This update
Testo del messaggio: Check dis out!
Allegato: Funnyflush.pif
La dimensione dell'allegato è di 118,784 bytes.

Se l'allegato alla mail infetta viene aperto, il worm modifica alcune chiavi di registro e crea il file ~dP00Z1.tmp nella cartella C:%Temp% folder.
Questo file è utilizzato per memorizzarvi il numero della porta TCP che il worm utilizza per connettersi all'hacker .
W32.Heovin@mm invia questo file, con ulteriori informazioni sul computer infettato, all'indirizzo e-mail dell'hacker e attende comandi dal client remoto.

L'assalitore potrebbe, ad esempio, cambiare la porta TCP che il worm utilizza per connettersi, farsi inviare informazioni di rete e di sistema del pc infettato, cancellare o eseguire file, assumere il completo controllo del sistema.
