PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 484 di martedì 29 gennaio 2002

Allarme virus!

E' stata segnalata la presenza di un nuovo pericoloso worm. Alcune indicazioni per individuarlo.

Nella giornata di ieri e' stata segnalata da Symbolic, azienda che distribuisce i prodotti F-Secure, la diffusione di un nuovo worm, denominato W32/Myparty.
I primi "contagi" sono stati ricevuti da Singapore, tuttavia alcuni elementi del virus fanno pernsare che sia di origine russa.
Al momento l'infezione si sta propagando in Asia, Europa e negli Stati Uniti.

L'e-mail alla quale e' allegato W32/Myparty si autoinvia a tutti gli indirizzi di posta elettronica contenuti nel data base Windows Address Book e nei file con estensione dbx (data base di Outlook).
Il messaggio proveniente da un mittente noto e un soggetto "attraente" possono cosi' trarre in inganno l'utente...

Il worm W32/Myparty si diffonde tramite una e-mail dalle seguenti caratteristiche:
Soggetto: new photos from my party!
Messaggio: Hello!
My party... It was absolutely amazing!
I have attached my web page with new photos!
If you can please make color prints of my photos. Thanks!
Allegato: www.myparty.yahoo.com
L'allegato ha l'apparenza di un link verso un sito web, ma si tratta di un file eseguibile che attiva il virus...

Quali danni puo' arrecare l'apertura di questo file?
Il worm effettua un controllo sul layout della tastiera: nel caso si tratti di una tastiera russa non sortisce alcun effetto.
In caso rilevi una tastiera occidentale, sui sistemi basati su NT (Windows NT, Windows 2000) il virus inserisce una backdoor, consentendo in questo modo il controllo da remoto del computer colpito.