PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 952 di mercoledì 03 marzo 2004

Risposte fallaci

Segnalata la diffusione di un nuovo worm. Si propaga attraverso una e-mail il cui oggetto inizia con "Re:...".

Botta e...risposta fra i virus che affollano la rete. Nella giornata di ieri è stata segnalata la rapida diffusione di una variante del worm Netsky.
Secondo quanto riportato da Symbolic, Netsky.D si diffonde solamente mediante l'allegato infetto di un messaggio e-mail. Rispetto alle varianti precedenti, Netsky.D non mostra una finestra di errore quando viene eseguito per la prima volta. Come nelle varianti precedenti, NetSky.D si installa nel sistema operativo e modifica alcune chiavi di registro.

L'e-mail con l'allegato infetto ha caratteristiche per lo più variabili; unico "segno di riconoscimento" è l'inizio dell'oggetto dell'e-mail "Re: ", oppure "Re: Re:".
Ad esempio possiamo trovare e-mail che indicano nell'oggetto una delle seguenti frasi: Re: Document, Re: Re: Document, Re: Re: Thanks!, Re: Hi, Re: Hello, Re: Here, Re: Your music, Re: Excel file, Re: Word file.
Il corpo del messaggio infetto può essere uno dei seguenti:
Your document is attached.
Here is the file.
See the attached file for details.
Please have a look at the attached file.
Please read the attached file.
Your file is attached.
L'allegato infetto ha un nome casuale generato in una lista; tra i quali compare: your_document.pif, your_picture.pif, mp3music.pif, my_details.pif.
Il worm cerca nei computer infetti file, con determinate estensioni, per reperire gli indirizzi e-mail ai quali inviarsi.

---

www.puntosicuro.it