PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 946 di martedì 24 febbraio 2004

Nuova minaccia in rete

Antivirus aggiornati e tanta attenzione per difendersi dall'infezione. A rischio i sistemi Windows.

I sistemi Windows (2000, 95, 98, Me, XPW) sono minacciati dalla diffusione di Netsky.B, un worm che si propaga via e-mail (tramite un proprio motore SMTP) o attraverso directory condivise di rete. Symantec ha indicato un elevato livello di allerta, classificandolo appena sotto il massimo indice di gravità (4 su 5). La principale caratteristica del worm è l'estrema...variabilità delle forme nelle quali si manifesta.
Riguardo alla sua diffusione via e-mail, il soggetto del messaggio, il testo, il nome dell'allegato sono scelti in tre liste. Il soggetto ad esempio può essere "hi", oppure "hello", "warning", "information", "read it immediately".
Il testo varia tra una serie di brevi frasi in lingua inglese, tra le quali "ok", "i'm waiting", "read the details", "here is the document", "read it immediately!", "my hero", "here", "is that true?".
Riguardo all'allegato infetto, il worm può utilizzare una o due estensioni; solitamente la seconda estensione è .zip o .exe.
Il worm pone come mittente del messaggio un indirizzo mail casuale trovato nel computer infettato; fate attenzione quindi ad aprire gli allegati delle e-mail che ricevete, anche se provengono da un soggetto conosciuto.

Quando il worm viene eseguito, per prima cosa mostra una falsa finestra di dialogo nella quale si afferma che l'allegato non può essere eseguito. Il worm modifica alcune impostazioni di sistema e inizia a raccogliere indirizzi e-mail in file con determinate estensioni posti nei dischi fissi del PC.
Se il worm trova una cartella con nome 'sharing' oppure 'share', si copia all'interno scegliendo uno dei nomi presenti in una lista, tra i quali: winxp_crack.exe, office_crack.exe, nero.7.exe, oppure nomi di soggetti musicali oppure a sfondo pornografico.

---

www.puntosicuro.it