PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 501 di giovedì 21 febbraio 2002

Allarme worm!

Arriva via e-mail e "parla tedesco". Ancora limitata la diffusione, ma...

Non e' ancora molto diffuso, ma potrebbe avere un effetto devastante sui computer colpiti, il nuovo worm, denominato "Yarner", scoperto in Germania nei giorni scorsi.
La sua attivazione potrebbe infatti causare la cancellazione dei dati presenti sul disco fisso.

Yarner si diffonde tramite un messaggio di posta elettronica, in lingua tedesca, al quale e' allegato il file eseguibile di dimensione 437 Kb (il file "yawsetup.exe").
Il soggetto dell'email e' composto dalla frase "Trojaner-Info Newsletter" e dalla data dell'invio, mentre come mittente indica "webmaster@trojaner-info.de".
L'autore del virus, per rendere credibile il messaggio e indurre l'utente a cliccare sul file, ha scelto appunto di utilizzare una falsa newsletter sulla sicurezza informatica, utilizzando con l'imbroglio il nome di un famoso portale tedesco di antivirus.

Nel caso l'utente apra il file yawsetup.exe", il worm si installa nel sistema; crea una sua copia con un nome casuale nella cartella di Windows e crea una chiave di avvio nel Registro per accertarsi di venire attivato all'avvio del sistema:
[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRunOnce]
Il nome della chiave e' casuale e il suo valore contiene il percorso al file del worm nella directory di Windows. Nello stesso percorso viene poi creata una copia del file col nome NOTEPAD.EXE, mentre l'applicazione originale del Blocco Note viene rinominata in NOTEDPAD.EXE.

Il worm ricerca gli indirizzi e-mail contenuti in file con determinate estensioni e nell'Address Book di Outlook. A questo punto Yarner si autoinvia a tutti gli indirizzi trovati.
