PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 474 di martedì 15 gennaio 2002

Worm ad alto rischio in circolazione: Gigger

Si spaccia per un aggiornamento di Outlook e cerca di formattare il disco del drive C.

I principali produttori di antivirus hanno già aggiornato i propri software a causa della diffusione del worm Gigger, classificato ad alto rischio.

Questo worm, che si spaccia per un aggiornamento di Outlook , si diffonde attraverso un messaggio di posta elettronica che riporta come contenuto "This worm is donation from all Bulgarians" ed ha in allegato il file "mmsn_ofline.htm".

Diversamente dagli altri virus conosciuti, il codice di mmsn_ofline.htm, redatto in JavaScript e Visual Basic Script, non si limita ad inviare il file a tutti gli indirizzi presenti nel Windows Address Book del Pc infettato, ma modifica anche le impostazioni di Outllook in modo che una copia di mmsn_ofline.htm sia allegata in automatico ad ogni email HTML in uscita.

Inoltre Gigger è in grado di conservare un file log con tutti gli indirizzi e-mail dell'Address Book colpito, per poi inviarlo a uno specifico contatto creato dal virus stesso.
Per autoreplicarsi il virus attacca i file con estensione ".htm" o ".asp" , che rileva scansionando le unità disco locali e di rete dell'utente infettato.

La caratteristica più preoccupante di Gigger è, però, legata alla linea di codice "Echo y|format c:", contenuta nel file "autoexec.bat", che, al riavvio di Windows, tenta di formattare l'hard disk del drive C.
