PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 539 di giovedì 18 aprile 2002

Persiste la diffusione del worm Klez.E

Anche se individuato da tempo continua a "ingannare" gli utenti come allegato di mail provenienti dai piu' svariati indirizzi.

Il worm Klez.E, individuato tempo fa, continua a diffondersi in rete, anche se riconosciuto ed eliminato dai principali antivirus attualmente disponibili.
L'estensione dell'infezione, come avevamo sottolineato nel numero 521 del nostro quotidiano, avviene via e-mail, attraverso l'esecuzione automatica, in fase di anteprima, di un allegato infetto.

Sfruttando una vulnerabilità di Microsoft Outlook e Outlook Express, si autoinviano messaggi di posta elettronica decisamente insidiosi e non riconoscibili, perché il soggetto, il nome dell'allegato e l'estensione del file dell'allegato variano continuamente (.exe, .bat, .pif, .scr).

L'utente viene facilmente confuso anche perché le mail sembrano essere state inviate da un certo indirizzo, mentre provengono da un altro, dal momento che Klez inserisce nel campo del mittente un nome qualsiasi estratto casualmente dall'elenco presente nel Pc infetto.

Il 6 di ogni mese dispari (gennaio, marzo, maggio..) Kletz sostituisce il contenuto dei file del Pc con degli zeri ed è in grado di installare il virus W32.ElKern.3326.

Fortunatamente i principali antivirus sono in grado di riconoscere Klez in fase di preview di una email e di bloccarne l'attivazione.
Nel caso il worm si sia attivato prima dell'aggiornamento dell'antivirus, quest'ultimo potrebbe non funzionare; sarà, quindi, necessario rimuovere Klez manualmente.
