PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 550 di mercoledì 08 maggio 2002

Klez sempre piu' minaccioso : ora si diffonde in rete come "patch di se stesso"

La nuova variante del worm si spaccia come file antivirus e conserva le "capacita' di trasformismo" delle precedenti versioni.

Il worm Klez si impone ancora all'attenzione degli utenti con una nuova versione in rapida diffusione.

L'ultima variante si sta diffondendo attraverso una falsa email che sostiene di fornire la patch antivirus in grado di proteggere il computer da Klez stesso.

Come è stato sottolineato da un quotidiano esperto in sicurezza informatica, anche il messaggio che accompagna il file "ingannevole" è falso, sia perché spaccia una patch che non c'è, sia perché sostiene che i normali software di protezione non sono in grado di rilevare Klez; ecco il testo:

"Klez.E is the most common world-wide spreading worm.It's very dangerous by corrupting your files.
Because of its very smart stealth and anti-anti-virus technic,most common AV software can't detect or clean it.
We developed this free immunity tool to defeat the malicious virus.
You only need to run this tool once,and then Klez will never come into your PC.
NOTE: Because this tool acts as a fake Klez to fool the real worm,some AV monitor maybe cry when you run it.
If so,Ignore the warning,and select 'continuè.
If you have any question,please mail to me."

Il falso anti-Klez, come le altre versioni già in circolazione, inclusa quella che porta con sè il virus CIH (cfr. il numero 549 del quotidiano) ha notevoli capacità trasformistiche: l'indirizzo e-mail indicato nel messaggio "per saperne di più" è, infatti, scelto a caso nell'elenco degli indirizzi di posta elettronica presenti sul computer infettato.

Per creare confusione e ingannare chi riceve il messaggio, anche l'indirizzo di posta elettronica del mittente viene continuamente modificato utilizzando una email trovata nel PC infetto.
In questo modo sembra che all'origine del messaggio vi sia un certo utente, che in realtà non è stato infettato, ma il suo indirizzo è presente su un computer colpito da Klez.
