PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 431 di lunedì 29 ottobre 2001

Nuovo worm in circolazione: Kletz

I messaggi infetti hanno soggetti diversi. Due le modalità di diffusione.

Symbolic ha individuato un nuovo virus denominato KLETZ.
Questo worm invia messaggi con testo e allegato casuali.

In base a quanto rilevato Kletz, probabilmente creato in Asia, rilascia nei sistemi infetti un virus chiamato Elkern.
Al momento il virus è ancora allo studio degli analisti, per ora è stato verificato che ha due diverse modalità di diffusione.

In un caso sfoglia i drive di rete e lascia in essi delle copie di se stesso, creando file con nomi casuali e con doppia estensione (ad esempio .TXT.EXE).

In base alla seconda modalità, invece, il virus localizza file EXE sui drive locali e di rete, e li infetta attraverso copie polimorfiche di se stesso.

---

www.puntosicuro.it