PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 2 - numero 74 di martedì 21 marzo 2000

Virus in agguato

Ritorna un pericoloso virus in grado di portare al crash del sistema infettato. Come agisce e quali precauzioni prendere.

Il suo nome e' da tempo conosciuto, ma negli ultimi giorni ne e' stata segnalata la diffusione in alcune importanti aziende statunitensi: e' il virus Melting.worm, che si installa nel sistema della vittima e puo' portare anche al crash del sistema.

Il virus Melting.worm arriva in un messaggio di posta elettronica che ha per subject la frase "Fantastic Screensaver" e in allegato il file "MeltingScreen.exe".
Il file MeltingScreen.exe non deve essere assolutamente aperto; in quanto in caso di apertura il virus cerca immediatamente i file eseguibili (".exe") che si trovano nella directory di Windows, rinomia il primo ".exe" trovato in ".bin" e si copia al posto del file eseguibile originale.

Il virus e' attivato dall'utente quando apre l'applicazione infettata, a questo punto il virus contagia un altro file ".exe" della directory di Windows.
Tentando di aprire piu' applicazioni infette si puo' arrivare al malfunzionamento di Windows fino al crash di sistema.

Melting.worm si copia in C:/WINDOWS/MeltingScreen.exe e cerca nel registro la HKEY_CURRENT_USERMeltingScreenString.
Se questa chiave non esiste allora la crea e configura il suo valore a "MeltingScreen".
Il virus, a questo punto, si serve di Outlook per inviare una copia del messaggio "Fantastic Screensaver" ad ogni indirizzo e-mail contenuto nella rubrica del sistema infetto.
