PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1048 di venerdì 16 luglio 2004

Worm difficile da scovare

Segnalata la diffusione del nuovo worm Atak. Come riconoscerlo.

Si nasconde ai tentativi degli antivirus di rilevare la sua presenza. Questa è la caratteristica che rende degno di attenzione il worm Atak.A, segnalato da "Panda Software" nei giorni scorsi.
Il nuovo worm non è particolarmente dannoso, ha l'obiettivo di diffondersi quanto più possibile via e-mail, ma ha la particolarità di disattivarsi quando rileva un'azione di debugger sul computer infettato.

Atak si diffonde tramite un messaggio con caratteristiche variabili; cela l'indirizzo di posta del destinatario utilizzando alcuni nomi, tra i quali kevin, mike, andrew.
Il soggetto può essere vuoto o uno dei seguenti: Read the Result!; Important Data!
Il messaggio è vuoto oppure contiene la frase "Authorized Researcher Only".

L'attachment può avere doppia estensione. L'estensione può essere JPG o GIF, seguita da un numero casuale di spazi bianchi e dall'estensione finale .exe.
Il worm cerca, in file con determinate estensioni, gli indirizzi ai quali inviarsi e modifica alcuni file in modo da essere attivato ad ogni avvio di Windows.