PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 872 di martedì 28 ottobre 2003

Worm spiritoso

Si diffonde con un messaggio di posta elettronica (in italiano) ed invita a scaricare uno screen saver.

I creatori di worm sfruttano argomenti al centro dell'attenzione dell'opinione pubblica, prodotti o eventi di successo per fare leva sulla curiosità dei destinatari dei messaggi ed indurli a cliccare su file o su link contenenti "codici malevoli", capaci di modificare le impostazioni del PC o di distruggerne i file.

Sull'onda del successo della trasmissione televisiva "Zelig", l'autore del worm Voltan (detto anche W32/Voltan.A@mm, I-Worm.Voltan, Marque) ha diffuso nei giorni scorsi in rete uno spiritoso messaggio che invita l'utente a visitare un sito per scaricare un salva schermo.

Secondo quanto appreso da Symbolic, il worm viene trasmesso mediante una mail in italiano così composta:
Da: Utente@computer.infetto
A: Contatto@utente.infetto
Soggetto: Il momento e' catartico
Testo: Ricevo e cortesemente inoltro,.... un premio per la genialita
hanno reso mitico un salva schermo scaricalo, "poesie catartiche",
che non sai cosa ti perdi
ciao

Il messaggio contiene un link ad una pagina web che presenta il testo:
"Il momento è catartico... per parafrasare un noto comico di ZELIG !!!"
Poi offre all'utente il download di un file chiamato zelig.scr, che contiene il codice del worm.

Quando si esegue il file, viene visualizzato il seguente messaggio
"Congratulazioni !
Il "CATARTICO" screen saver è stato installato con successo ."

Dopo l'esecuzione, Voltan modifica le impostazioni di Windows in modo che il salvaschermo predefinito venga impostato sul testo scorrevole, con la frase.
"A volte ti sento così vicina...A volte ti sento così lontana
...Certo che hai proprio un cellulare di m****!"

Per diffondersi, Voltan raccoglie gli indirizzi nel Windows Addreess Book e spedisce la mail "infetta" usando il proprio motore SMTP.

Secondo quanto riportato da Symbolic, "se il worm non riesce a rilevare l'indirizzo dell'utente sul computer infetto, ne utilizza uno pre-impostato."
Il worm non sarebbe in grado di infettare i sistemi Windows 95/98/ME e NT 4.0.

Altre fonti hanno riportato che collegandosi al sito indicato nell'e-mail, ora non più attivo, il worm modificasse la connessione di internet collegando l'utente ad un numero a tariffazione maggiorata.
