PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 409 di giovedì 27 settembre 2001

Allarme virus!

E' stata segnalata la diffusione di un nuovo worm capace di mettere a repentaglio la privacy degli utenti.

Una e-mail, che circola in Rete proponendo un argomento di sicuro interesse ed attualita',ha, invece, per allegato un file contenente il virus W32.Vote.
Le aziende produttrici di antivirus hanno messo in guardia gli utenti da questo worm capace di creare danni e disagi e che, in alcuni casi, potrebbe costituire un pericolo per la riservatezza dei dati contenuti nel computer colpito.

Il virus e' scritto in Visual basic ed e' contenuto nel file WTC.exe, allegato ad un messaggio di posta elettronica con le seguenti caratteristiche.
DA: nome utente
A: nome casuale preso dall'address book
SOGGETTO: Fwd: Peace BeTween AmeriCa and IsLaM !
TESTO DEL MESSAGGIO: Hi
iS iT waR Against AmeriCa Or IsLaM !?
Let's Vite To Live in Peace!

Nel caso l'utente incauto apra il file WTC.exe, per esprimere il suo "voto", il virus si installa sul computer e si attiva al successivo riavvio della macchina.
Dopo l'attivazione appare il messaggio: " I promiss We WiLL Rule The World Again... By The Way, You Are Captured By Zacker!!".

In questo caso il virus si autoinvia a tutti gli indirizzi contenuti nell'address book e tenta di cancellare alcune porzioni di programmi antivirus.

Nelle intenzioni del realizzatore di W32.Vote vi era probabilmente quella di attivare una procedura di formattazione della macchina colpita; una operazione che, fortunatamente, non gli e' riuscita.
Il pericolo maggiore, secondo gli esperti dell'azienda di antivirus Symantec, e' costituito dalla possibilita' che vada a buon fine l'installazione da parte del virus di un particolare programma, detto trojan, creato allo scopo di prendere il controllo del computer colpito.
Tra i rischi Symantec segnala la possibilita' che l'autore del trojan possa sottrarre o modificare le password o i file che le contengono, installare software per connessione da remoto, leggere o modificare file o impedirne l'accesso all'utente, inviare file dall'account email dell'utente colpito.

Le indicazioni per la rimozione del virus sono indicate nel sito di Trend Micro, azienda produttrice di antivirus.