PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 523 di lunedì 25 marzo 2002

Attenzione ai file scaricati attraverso le chat di IRC o i servizi di istantant messaging

Secondo il CERT cresce il pericolo dei "Social Engineering Attacks".

I sistemi informatici in molti casi sono resi vulnerabili da comportamenti incauti da parte degli utenti.
A quanto afferma il CERT, organismo USA per la sicurezza informatica, un pericolo emergente è costituito dai "Social Engineering Attacks"; sulle chat o i network di IM, gli hacker per raggiungere i loro scopi sfruttano la mancanza di cultura nel campo della sicurezza informatica di molti utenti.

I messaggi utilizzati dagli hacker solitamente induco gli utenti a scaricare gratuitamente software (protezioni antivirus, file musicali, file pornografici...).
In realta', una volta eseguiti, questi software (malicious software) permettono agli hacker di sfruttare il sistema per lanciare attacchi del tipo Distributed Denial of Service (DDoS).

Un esempio di "messaggio ingannevole" e' il seguente:
You are infected with a virus that lets hackers get into your machine and read ur files, etc. I suggest you to download [link al programma maligno] and clean ur infected machine. Otherwise you will be banned from [canale IRC].
(Sei stato infettato da un virus che consente agli hacker di entrare nel tuo computer e di legger i file. Ti suggerisco di scaricare questo programma [link al programma maligno] di ripulire il tuo computer infetto. In caso contrario sarai bandito da [canale IRC].)

Si tratta di e' un "social engineering attack" poichè la decisione dell'utente di scaricare ed eseguire il software è il fattore decisivo per il successo dell'attacco.

Un rapporto ricevuto dal CERT indica che decine di migliaia di sistemi sarebbero stati recentemente compromessi in questo modo.

Sfruttando i computer "infettati", gli hacker possono lanciare attacchi del tipo DDoS e sono in grado di esercitare un controllo remoto sui sistemi, modificare file, accedere a dati riservati, installare ulteriori "malicious software".

Gli esperti del CERT raccomandano di tenere sempre aggiornato il programma antivirus, di non scaricare file dei quali non si conosce la provenienza, ma soprattutto di essere informati, aggiornandosi costantemente sulle questioni inerenti la sicurezza informatica.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.