Crackare i files di CAMOUFLAGE

Testo realizzato da FauLeY

e-mail to: axel_fauley@yahoo.it
www.autistici.org/hackarena

Cos'è
Camouflafe è un programma di steganografia sostitutiva che permette in maniera gratuita di nascondere dati all'interno di testi, immagini, programmi, files video e altro ancora..
Steganografia tradotto dal graco significa "scrittura nascosta", e riscuote molto successo per la capacità di far passare dati sensibili per files comuni o comunque "insospettabili".
Il suo obiettivo dovrebbe essere insomma quello di non far sospettare la presenza di un documento da attenzionare..
L'obiettivo è stato perso in partenza da parte della Camouflage Software.. vediamo il perchè..

L'attacco
Per il crackaggio di un files stenografato con Camouflage è necessario un editor esadecimale, qualche minuto di tempo e un pò d'attenzione.
Per prima cosa apriremo il file con l'editor ed andremo ad analizzare la parte finale del testo esadecimale: se il file è stato precedentemente stenografato con Camouflage, in fondo alla sequenza di codice esadecimale si troverà la sigla

74 A4 ** 22 ** (*= numero variabile) ed t.T"

che ci permetterà di comprendere subito se il file è stato stenografato o meno.
Camouflage al momento della staganografizzazione del file richiede una password; l'attaccante potrà optare per eliminare la password o decrittarla.
Per eliminare la password dovrà cercare i caratteri della stessa poco sopra la sigla, individuandola con l'ausilio dell'editor (il numero di caratteri sarà uguale a quello della password) ed eliminare i caratteri cancellandoli; adesso dovrà accedere con camouflage al file e senza l'ausilio di alcuna password avrà accesso al file nascosto.
Se l'attaccante vorrà decrittare la password dopo essersi fornito una tabella con i valori dei corrispondenti caratteri esadecimali, sostituirà i valori e verra in possesso della password.
La vulnerabilità più evidente è la mancanza di una vera crittazione della password, i cui caratteri vengono solamente sostituiti senza modificare la lunghezza della password.

In conclusione
Usare Camouflage significa affidare la propria sicurezza ad un software davvero scadente che permette a CHIUNQUE di venire in possesso sia della password che del file nascosto.
Si consiglia in ogni caso nel caso di dati sensibili, di crittare i dati con software a chiave asimmetrica come pgp (in ambito windows - gratuito) o gpg (in ambito *nix like - sotto licensa GNU) ed infine steganografare i dati con software più sicuri.