ISPEZIONE DEL FILE COMPARSO SUL SERVER THETA

Ci è stata segnalata la comparsa di un misterioso file su uno dei server dell'azienda Theta, e ci è stato richiesto dalla stessa di analizzarlo.

Ovviamente, questo ha comportato un piccolo incremento della nostra parcella, per ovvi motivi di tempo e risorse impiegate in questo compito aggiuntivo.

Segnalo per correttezza che ci siamo appoggiati alla collaborazione con altri team per quanto riguarda questa parte della commessa.

Abbiamo inizialmente scansionato il file con una lunga serie di antivirus di varia natura e con diversi tipi di funzionamento per scongiurare la presenza di malware che avrebbero potuto compromettere le nostre macchine di lavoro. Le scansioni sono andate a buon fine, e abbiamo quindi proceduto con le operazioni di analisi.

Il file conteneva dei file di configurazione, un file html e una serie di immagini.

Abbiamo analizzato i vari script, notando alcune "stranezze" nelle annotazioni del codice, che si sono rivelati indizi per poter esaminare le immagini.

Abbiamo quindi effettuato delle verifiche sulle immagini, attraverso i comuni metodi di steganografia (principalmente StegHide su Kali Linux), scoprendo una serie di messaggi cifrati, uno collegato all'altro, che abbiamo dovuto decodificare con metodi come la codifica/decodifica Base64, e la "traduzione" di linguaggi esoterici come il BrainFuck e il Moo.

Abbiamo anche tentato un attacco "brute force" alle passphrase che venivano fuori con StegHide, tramite il comando StegSeek e una libreria creata ad-hoc in base ai vari indizi raccolti, purtroppo senza successo.

Nonostante la preoccupazione iniziale, tolto un messaggio vagamente intimidatorio, contenuto nell'ultima immagine, legato ai conti dell'azienda Theta (che però siamo sicuri non abbia avuto seguito, in quanto sappiamo che l'azienda è ancora in piedi e completamente sana. E comunque ci teniamo a precisare, essendoci stato segnalato il problema solo a file trovato, eventuali perdite dell'azienda,visto che sicuramente è anche tutelata da un punto di vista assicurativo, non rientrano nella nostre responsabilità), abbiamo appurato che si trattasse solo di un innocente scherzo.

In conclusione, possiamo dire di non aver avuto riscontri di alcun pericolo, ma solo l'operazione di un hacker della vecchia scuola che ancora si diverte (e giustamente) in questo tipo di operazioni.

P.S.: In caso ci venga chiesto, abbiamo sì un'idea di chi sia il responsabile della comparsa del file, ma essendo persona cara e fidata, oltre alla totale bonarietà dell'operazione, non abbiamo intenzione di rivelare l'identità del nostro sospetto, prendendoci la responsabilità di questa nostra scelta.Anzi, lo ringraziamo per averci fatto in fondo divertire e, come sua consuetudine, di aver sfidato le nostre menti, la nostra logica e la nostra fantasia.