# Sommaire



## 1. Analyse de trames du fichier traffic.pcap

La machine Windows infectée est un pc de marque Dell

L'adresse IP du pc infecté est 172.16.4.193

L'adresse MAC du pc infecté est 5c:26:0a:02:a8:e4

Dans la partie du protocole NBNS nous pouvons trouver le nom du pc infecté :

- STEWIE-PC

Avec son groupe de travail :

- WORKGROUP

Nom du malware : Cerber Ransomware

Dans le protocole TCP nous pouvons trouver la date et heure de l'infection :

- 23h55

Dans les enregistrements DNS nous pouvons voir un enregistrement particulier :

- p27dokhpz2n7nvgr.1jw2lx.top (198.105.121.50)

Après quelques recherches sur l'enregistrement DNS particulier nous avons pu trouver des infos sur le kit d'exploitation utilisé :

- RIG exploit kit