Nicole M. Ramirez Mulero

801-19-3940

Prof. Arce

CCOM 4702

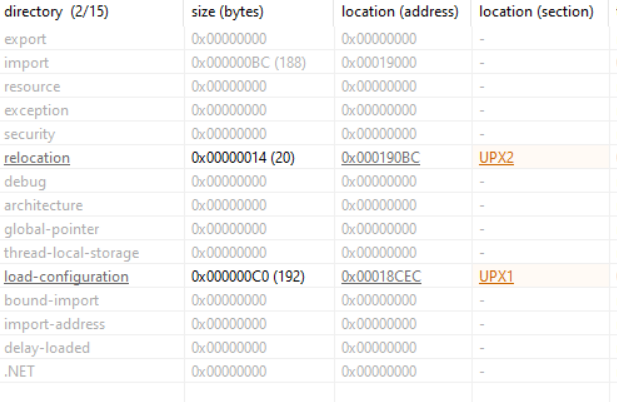
Lab 7

**I. Identificando las caracteristicas de los binarios empacados (hwin-packed.ex y hwin.exe)**

a. signature



b. secciones adicionales no comunes:



c. Entry point fuera de sección .text:



d. Entropia alta (sobre 7):



e. Muy pocas funciones del API siendo importadas (no decta ningún import ni librería):

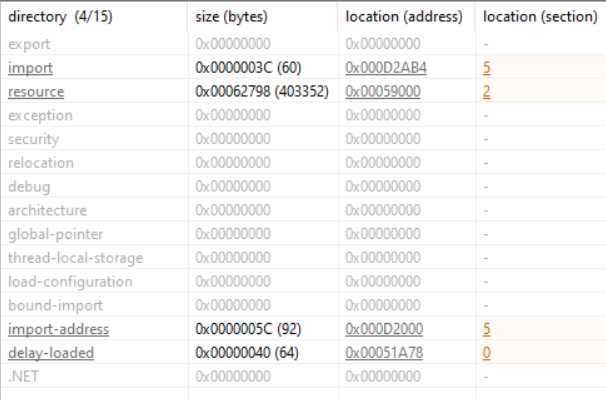


**II. Analizar usando PE Studio y Detect It Easy (lab07-guess01-03.exe)**

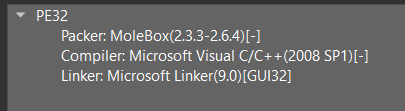
a. lab07-guess01 esta empaquetado. Esto lo podemos saber primeramente por la antropología alta que tiene



También tiene secciones con nombres fuera de lo común



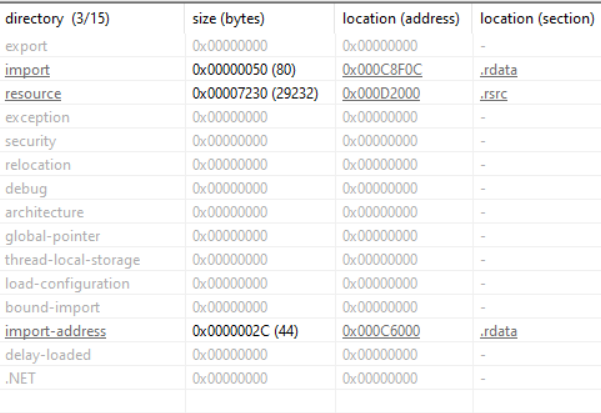
Y usando Detect It Easy, nos muestra cual fue el packer utilizado:



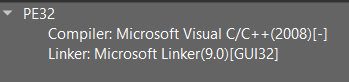
b. lab07-guess02 no esta empaquetado. Esto lo podemos saber primeramente porque la antropología esta bajo de 7:



Tambien tiene secciones con cnombres comunes:



Y si usamos Detect it Easy no nos detecta que se allá usando algún packer. Si vemos el signature, parece que tampoco hay ninguno registrado

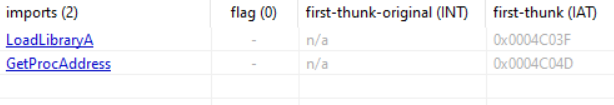




c. lab07-guess03 esta empaquetado. Esto lo se primero por que la entropía esta sobre 7



Tambien se nota que hay muy pocas funciones siendo importadas



**III. Desempacando el binario usando una aplicación (misteriousUnpackMe.exe)**