

Anexo a lección 45 de Ricardo INTRODUCCION AL CRACKING CON OLLYDBG



Lisa && Alquimista

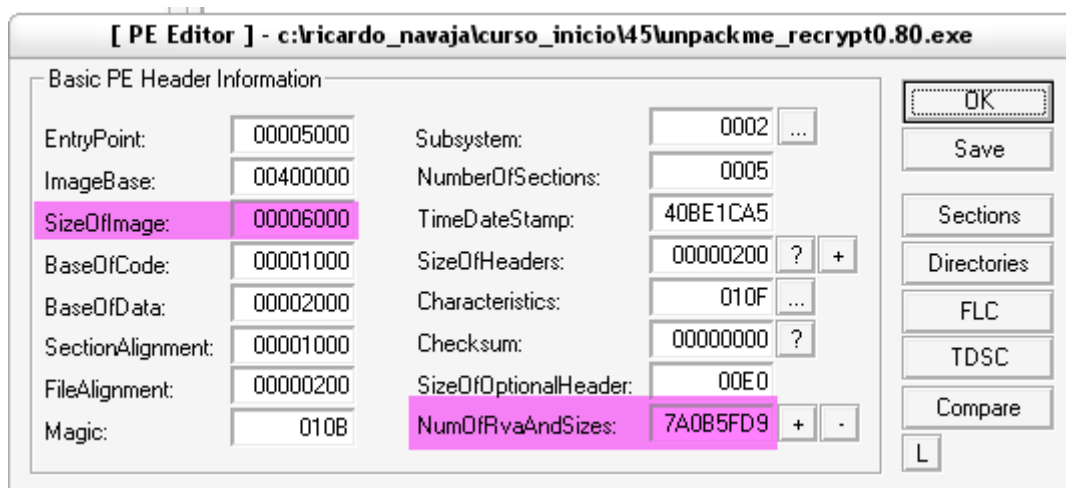
El siguiente ensayo mostrara otra forma de enfrentarnos al paker de dicha lección solo a golpes de ratón sin hacer nada de nada.

Nota: El Ollydbg usado será un olly normal solo modificado con Ollyghost y el plugins Ollydump para dumpear el proceso.

- También se usara un editor PE, lord PE y dos herramientas de la lista, Estricina y Pokemon Anti_Attach.

*** Recopilando información ***

Primero de todo como vamos lo atacaremos en memoria veamos unos datos del archivo, para lo cual abrimos el programa con Lord PE.



Esos datos serán importantes, pues el paker puede cambiarlos en tiempo de descompresión y no podremos hacer nada, como vemos el dato de NumberOfRvaAndSizes esta cambiado pues sabemos que tenia 10 Hex, eso lo cambiaremos, para lo cual necesitamos su Offset si abrimos con un editor P vemos que el Offset esta en **B4**



Otro dato que necesitaremos es su OEP que nos lo da el plugin de PEID.



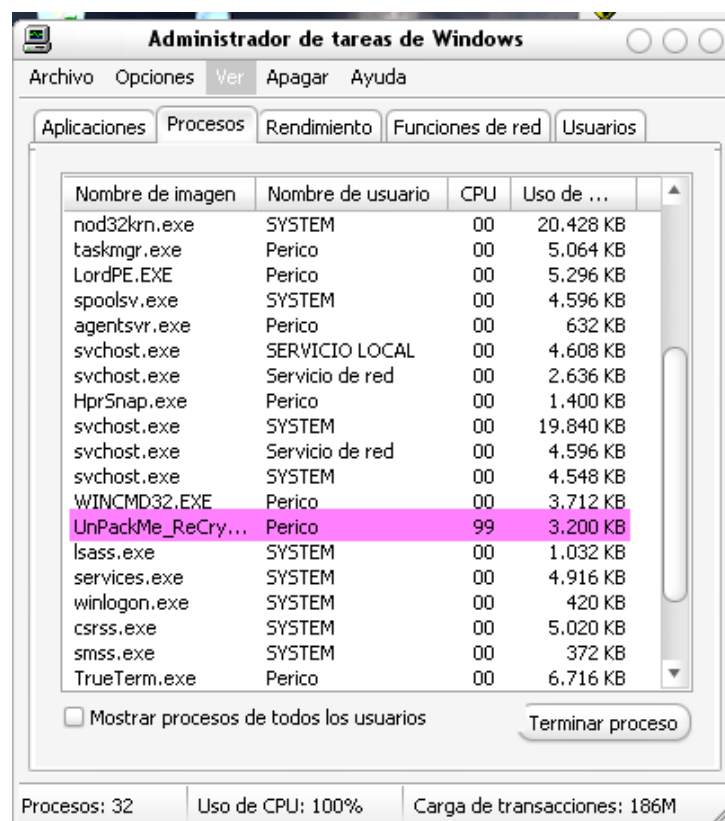
Bueno ya tenemos todos los datos necesarios para atacarle... así pues al ataque.

Los datos obtenidos son :

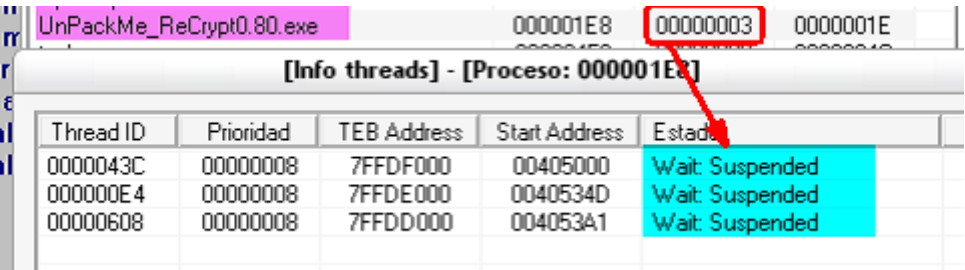
- 1. OEP → 00401000
- 2. SizeOfImage → 00006000
- 3. NumberOfRvaAndSizes → Esta en el offset b4 y será cambiado a 10

*** Atacando ***

Ejecutamos el paker fuera de Olly y este funciona, pero vemos que nos come todos los recursos.



Para trabajar un poco mas a gusto, usaremos una herramienta de Marciano, Estricina, con la cual paramos los tres thread que contiene el paker. (Este paso no es necesario pero se trabaja mucho mas cómodo con el ordenador, liberado de un proceso que lo relentiza enormemente) .



[Info threads] - [Proceso: 000001E8]				
Thread ID	Prioridad	TEB Address	Start Address	Estado
0000043C	00000008	7FFDF000	00405000	Wait: Suspended
000000E4	00000008	7FFDE000	0040534D	Wait: Suspended
00000608	00000008	7FFDD000	004053A1	Wait: Suspended

Si nos fijamos suspendiendo los thread el consumo de la CPU es cero, antes era 99.

Nombre de imagen	Nombre de usuario	CPU	Uso de ...
SMTPServer.exe	Perico	00	5.600 KB
taskmgr.exe	Perico	01	2.504 KB
UnPackMe_ReCry...	Perico	00	3.332 KB
OllyGhost.exe	Perico	00	1.008 KB
HprSnap.exe	Perico	00	3.124 KB
fl.exe	Perico	00	6.428 KB
alg.exe	SERVICIO LOCAL	00	3.936 KB
nod32kui.exe	Perico	00	2.504 KB
ALCXMNTR.EXE	Perico	00	3.412 KB
jusched.exe	Perico	00	1.864 KB
THUNDE~1.EXE	Perico	00	1.832 KB
svchost.exe	SYSTEM	00	3.832 KB
nvsvc32.exe	SYSTEM	00	1.872 KB
nod32krn.exe	SYSTEM	00	20.152 KB
explorer.exe	Perico	02	26.900 KB
WINWORD.EXE	Perico	00	3.092 KB
WINCMD32.EXE	Perico	01	8.884 KB
spoolsv.exe	SYSTEM	00	4.600 KB
svchost.exe	SERVICIO LOCAL	00	4.692 KB

Con esto ya podemos usar tranquilamente nuestra maquina.

*** Atacando en memoria para no ser detectados ***

Después usamos el Pokemos, para evitar posibles anti Attach y de paso también recomponemos el dato de NumberOfRvaSizes, que si recordamos estaba en el offset B4. (NO es necesario restaurar el dato de NumberOfRvaAndSizes, pero así le facilitaremos la tarea o Olyydbg)

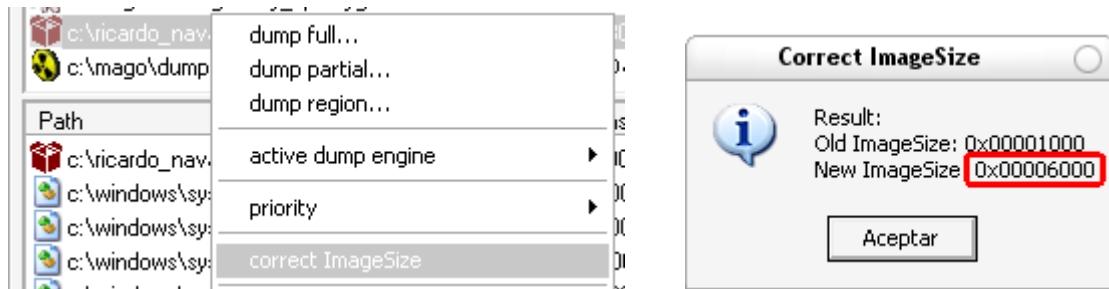


Bueno si tenia protección Anti_Attach, esta ha desaparecido, seguiremos atacando al paker en memoria, abriremos lordPE y lo buscaremos en la lista de procesos.

Path	PID	ImageBase	ImageSize
c:\archivos de programa\email security\smtps...	00000C94	00400000	00140000
c:\utils_win\fast launcher\fl.exe	000008E8	00400000	00110000
c:\mago\utils_varios\dibujo\hypersnap\hprs...	00000910	00400000	00144000
c:\mago\debugger\olly_xp\ollyghost.exe	00000BA8	00400000	00193000
c:\ricardo_navaja\curso_inicio\45\unpackm...	00000BB4	00400000	00001000

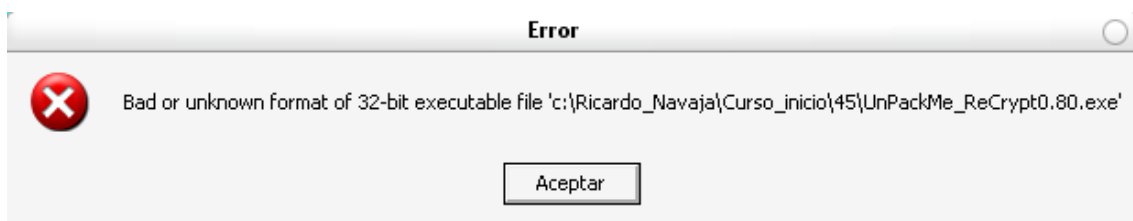
Como vemos tiene el **imagenSize a 0001000** y nosotros sabemos que tiene que estar en 0006000, eso confundirá a Olly y a cualquier dumper con lo cual no obtendremos un ejecutable en buen estado, además impedirá que usemos el programa Import para restaurar las tabla de importación.

Conclusión: Hay que repararlo, eso esta claro, el mismo lordPE lo realiza botón derecho y corregir ImageSize.



Y como vemos en la captura de la derecha la ha quedado en **00060000** que es la que tenia que tener, como sabemos desde el principio.

Ya hemos reparado parte del programa en memoria ahora lo attacharemos con Olly y vemos que nos informa que la cabecera esta errónea.



Damos a aceptar y el programa queda Atacado, y parado en la API

Attached process paused at ntdll.DbgBreakPoint

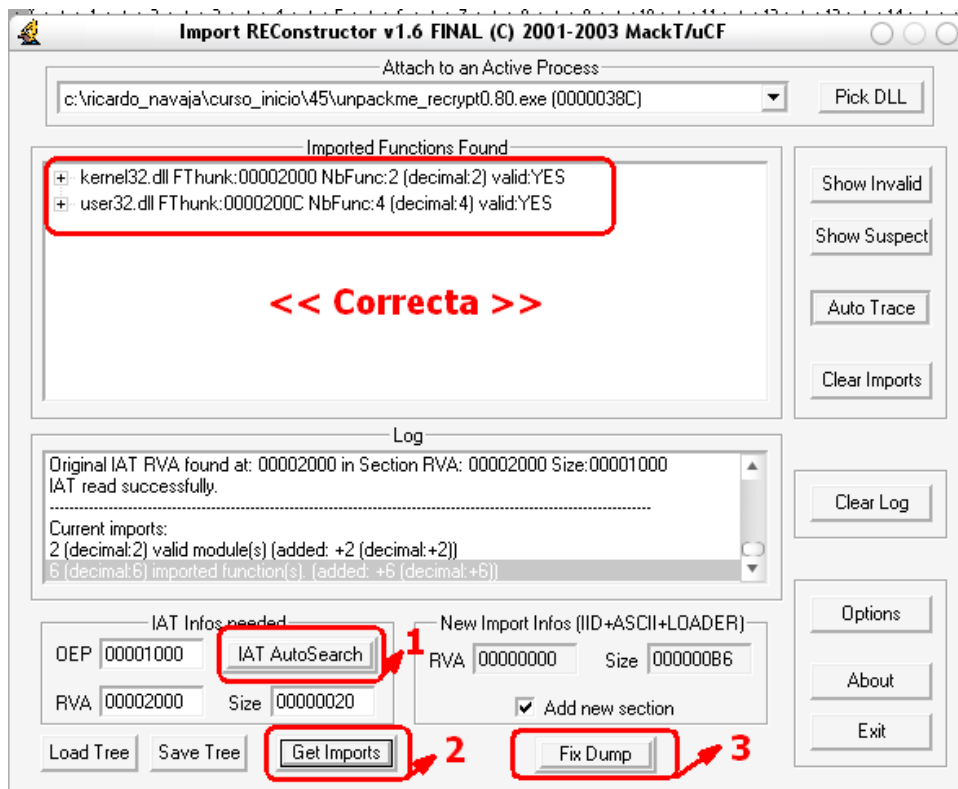
ahora como conocemos su OEP en la ventana de código le damos a ir en 00401000 y estaremos en el OEP del programa.

00401000	6A 00	PUSH 0	
00401002	E8 D9000000	CALL UnPackMe.004010E0	JMP to kernel32.G
00401007	A3 40304000	MOV DWORD PTR DS:[403040],EAX	
0040100C	6A 00	PUSH 0	
0040100E	68 2B104000	PUSH UnPackMe.0040102B	
00401013	6A 00	PUSH 0	
00401015	68 00304000	PUSH UnPackMe.00403000	ASCII "Genesis"
0040101A	FF35 40304000	PUSH DWORD PTR DS:[403040]	UnPackMe.00400000
00401020	E8 A3000000	CALL UnPackMe.004010C8	JMP to user32.Dia

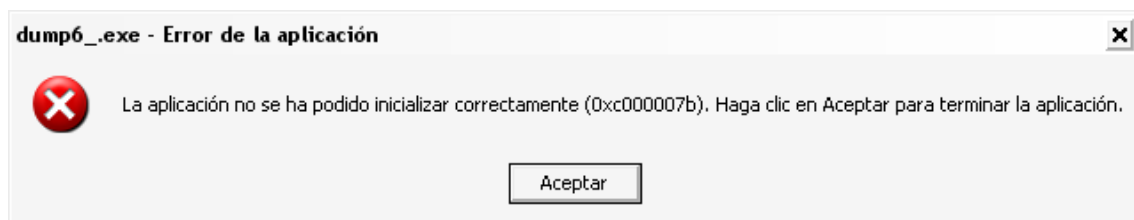
y vemos que esta perfecto.... botón derecho



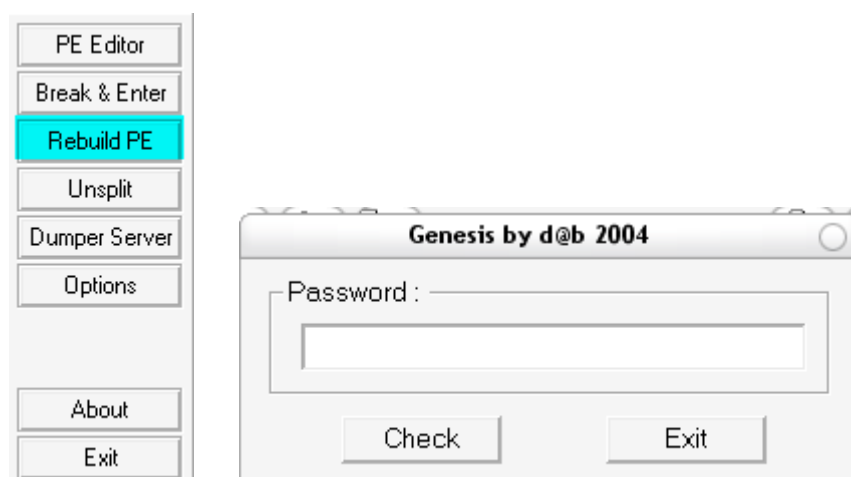
Y vemos en registro EIP que estamos parados en el OEP, así que ahora a dumper con el plugging.



solo queda añadirle la tabla cosa que aremos con el Import introducimos el OEP y apretamos a los tres botones en orden, elegimos el archivo anteriormente dumpado y no sale la pantalla de que la cabecera esta en mal estado, eso ya nos lo había informado antes Ollydbg,



Reconstruimos la cabecera con cualquier programa que tenga esa opción, en este caso Lord PE y el programa queda perfecto.



y si lo miramos con el administrador de tareas de windows, vemos que no consume recursos, el paker ha desaparecido.

Nombre de imagen	Nombre de usuario	CPU	Uso de ...
alg.exe	SERVICIO LOCAL	00	3.892 KB
jusched.exe	Perico	00	1.868 KB
WINWORD.EXE	Perico	00	2.012 KB
HprSnap.exe	Perico	00	1.292 KB
agentsvr.exe	Perico	00	1.128 KB
svchost.exe	SYSTEM	00	3.812 KB
nvsvc32.exe	SYSTEM	00	1.868 KB
nod32krn.exe	SYSTEM	00	18.440 KB
explorer.exe	Perico	00	20.412 KB
fl.exe	Perico	00	6.108 KB
WINCMD32.EXE	Perico	00	8.136 KB
spoolsv.exe	SYSTEM	00	4.592 KB
dump6_.exe	Perico	00	3.052 KB
wscntfy.exe	Perico	00	2.472 KB
svchost.exe	SERVICIO LOCAL	00	4.608 KB
svchost.exe	Servicio de red	00	2.632 KB
svchost.exe	SYSTEM	00	18.816 KB
svchost.exe	Servicio de red	00	4.564 KB
svchost.exe	SYSTEM	00	4.484 KB

Bueno pues basta de paker raros por hoy.

