.-<Iv!n$on - Ing. R3v3rS!v0>-.

CLS T3aM-No CoMp3t3Nc3

Download: http://www.mediafire.com/?we6bx2br38yz3sb

Introducción

Tenemos otro programa al cual desempacar con fines educativos porque somos una lista que busca e intenta constantemente que los integrantes puedan compartir sus conocimientos y ¿qué mejor manera que dejarlos por escritos para la posteridad? Cuando desempaques, crackees o consigas algo interesante en un software sería muy importante que lo publiques a través de un tutorial para que todos podamos seguir investigando y ampliando ese descubrimiento o novedad.

Reconozco que este arte no es tan fácil como parece, por lo menos cuando empezamos, pero poco a poco vamos desentrañando sus secretos. Esto será una lucha constante entre Programador-Cracker. ¿Quién ganará? Pienso que siempre habrá un equilibrio porque ni ellos dejarán de programar ni nosotros dejaremos de crackear.

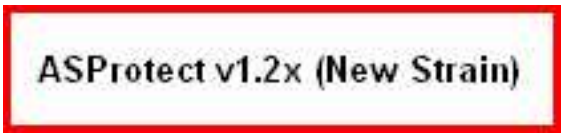
¿Quién dejaría de hacer algo que le guste y qué le ponga retos interesantes?

Quiero cerrar esta introducción con la frase: Más sabe el diablo por viejo que por diablo.

Buscando un packer

Nuestro amigo RDGMAX creó un detector de packer muy bueno.

¿Quién no ha utilizado RDG Packer Detector? Revisemos nuestro PE a ver con qué sorpresa nos saldrá.



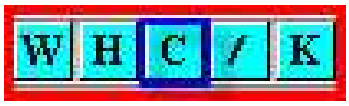
En este PE, RDG no nos dice con qué está compilado. Por ahora, carguémoslo en Olly y veamos su EIP.

Detenemos el análisis con la tecla Espacio. ☺

Podemos buscar en memoria "M" a ver si conseguimos algo que nos indique con qué está compilado.

Podemos observar la DLL de Visual Basic “msvbvm60”

Volvamos al desensamblado de Olly.



El OEP de un programa compilado en Visual Basic tiene esta apariencia:

1) Un PUSH a la dirección de la DLL “VB5!6&VB6FR.DLL”
2) Un CALL al salto indirecto de la DLL “msvbv60.ThunRTMain”

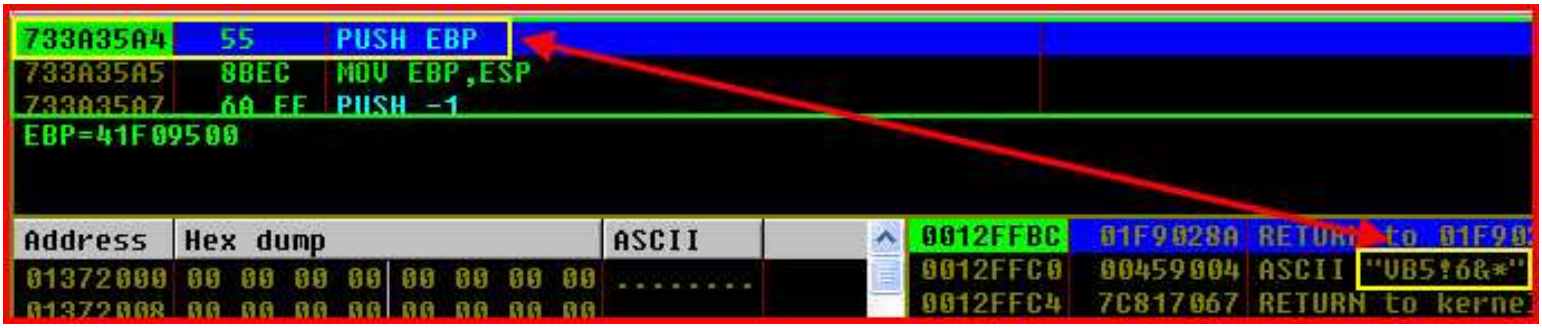
Para encontrar el OEP en nuestra víctima buscaremos la String “ThunRTMain” presionando CTRL+G.

Caemos aquí:

Anotemos esta dirección 733A35A4. Reiniciemos Olly con CTRL+F2.

Y vayamos a esa dirección con CTRL+G.

Luego, le ponemos un HBP en Execution. Presionamos F9 y caemos en:

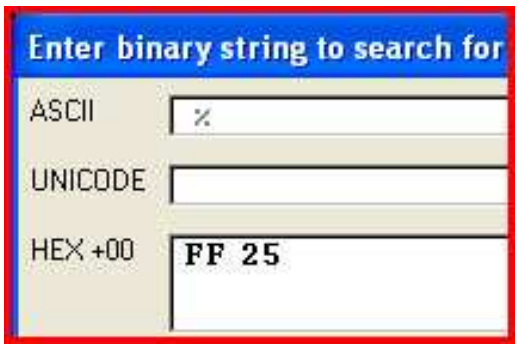


En el Stack vemos algo interesante: “VB5¡6&*” el cual está incompleto.

Debería ser así: “VB5!6&VB6FR.DLL”. Por los momentos, solo anotemos la dirección interesante que vemos en el Stack 459004.

Buscando el OEP

Reiniciamos con CTRL+F2. Damos run con F9 y presionemos CTRL+B . Busquemos FF25 que son saltos indirectos.



Caemos en:

```
0045845F    00FF    ADD BH,BH
00458461    25 BC1  AND EAX,4011BC
00458466  - FF25 9  JMP DWORD PTR DS:[401294]   msvbvm60.__vbaExceptHandler
0045846C  - FF25 E  JMP DWORD PTR DS:[4012E4]   msvbvm60.__vbaFPException
```

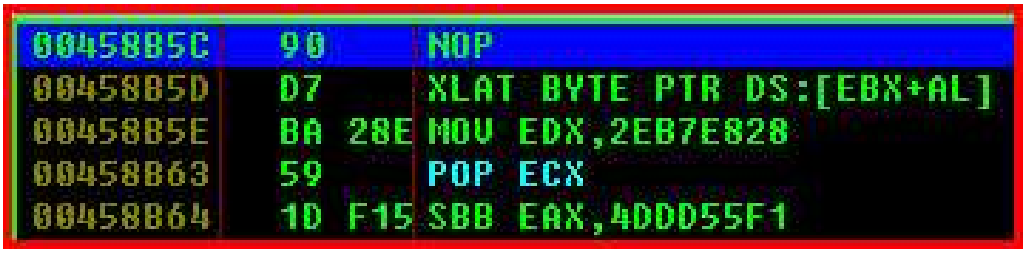
Vayamos al final de esos JMP con CTRL+L o como ustedes quieran.

Y nos encontramos el OEP:

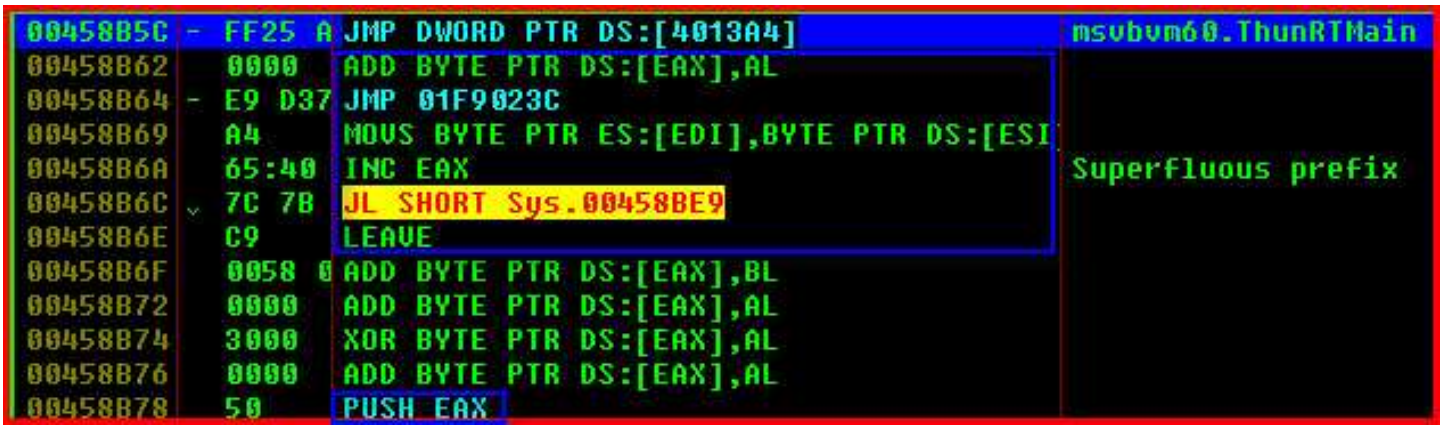
```
00458B5C  - FF25 A  JMP DWORD PTR DS:[4013A4]   msvbvm60.ThunRTMain
00458B62    0000    ADD BYTE PTR DS:[EAX],AL
00458B64  - E9 D37  JMP 01F9023C
00458B69    A4      MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
00458B6A    65:40   INC EAX                     Superfluous prefix
00458B6C  v 7C 7B   JL SHORT Sys.00458BE9
00458B6E    C9      LEAVE
00458B6F    0058 0  ADD BYTE PTR DS:[EAX],BL
00458B72    0000    ADD BYTE PTR DS:[EAX],AL
00458B74    3000    XOR BYTE PTR DS:[EAX],AL
00458B76    0000    ADD BYTE PTR DS:[EAX],AL
00458B78    50      PUSH EAX
```

Vemos que hay Stolen Bytes e instrucciones raras que no se parecen en nada a un OEP de un Visual Basic normal.

Entonces, nuestro OEP temporal será: 458B5C. Reinicimos Olly con CTRL+F2. Luego, CTRL+G y vamos a 458B5C.



¡Que feo! ¿Verdad? Pongámosle un HBP en Execution y damos F9.



Ahora, sí. ☺ Arreglemos los Stolen Bytes de la siguiente manera:

PUSH 459004 ;Dirección de "VB5!6&VB6FR.DLL".
CALL 458B5C ;Dirección del salto indirecto a "ThunRTMain".

Al arreglar esas instrucciones, debemos poner a cero las 2 siguientes porque están muy raras.

Está quedando mejor. Hasta recuperamos un POP EAX:

Arreglemos "VB5¡6&*" por esto "VB5!6&VB6FR.DLL"

En el Dump, lo editamos así:

Arreglando la IAT

La IAT de los Visual Basic comienzan en 401000. Por lo tanto, vayamos al Dump a esa dirección y elijamos la vista Long Address.

Vayamos al final:

Datos recopilados:

OEP: 458B62

Inicio de IAT: 401000

Fin de IAT: 4014AC

Datos para ImpRec:

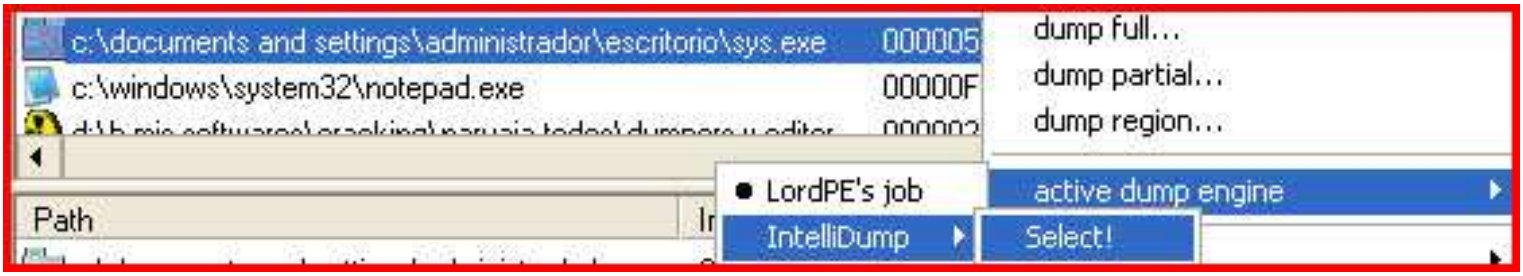
OEP: 58B62 (458B62-400000==58B62)

RVA: 1000 (401000-400000==1000)

Size: 4AC (Fin – Inicio==Size. 4014AC-401000==4AC)

Dumpeando

Abramos LordPE y seleccionemos el proceso Sys.exe.

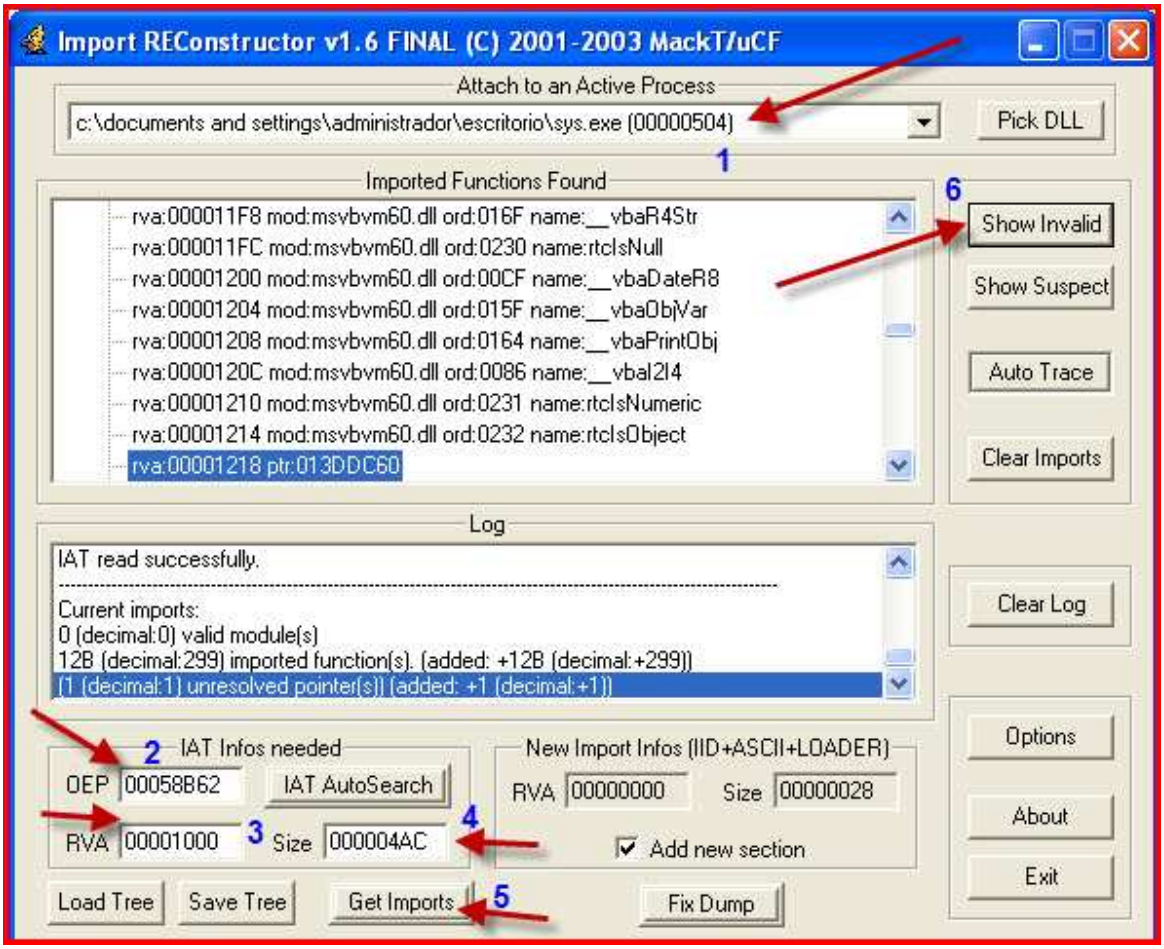


Y luego:

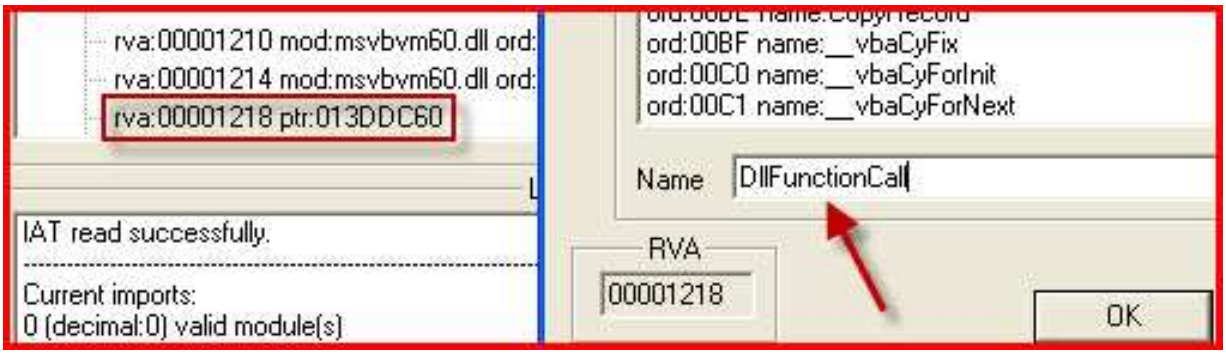
Guardamos el Dumpeado.

Arreglando el Dumpeado

Cargamos el original en ImpRec y colocamos los datos recopilados.



Vemos que solo tenemos una entrada mala. La de siempre. Le damos doble click y la escribimos a mano.



Ahora, le damos a Fix Dump y buscamos el Dumpeado.

Lo ejecutamos y:

Gracias por leer.

Contacto: ipadilla63@hotmail.com