Matar al Padre rápido con ArmaDetach

Cracker: Ivinson
Victima: BlockWorks

Download Game:
http://hypervisual.com/blockworks/files/blw3setup.zip

Download PUPE:
http://www.mediafire.com/?33u450bnec6g069

Download ArmaDetach:
http://www.mediafire.com/?ghlm4moy66jiikb

Encontrar OEP en Armadillo con CopyMen II:

BP WaitForDebugEvent

F9. (Ver Stack)

12DAAC 004627F0 CALL to **WaitForDebugEvent** from 4627EA
12DAB0 0012EB60 **pDebugEvent** = 0012EB60

Clic derecho en **pDebugEvent,** Follow in Dump. (Para ver reporte)

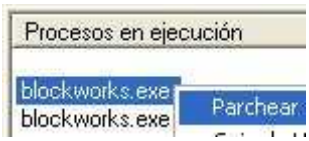
BC WaitForDebugEvent
BP WriteProcessMemory

F9 y Ctrl+F9. Ver OEP en el reporte.

0012EB78 **CB 11 40 00** 02 00 00 00
0012EB80 00 00 00 00 **CB 11 40 00**
0012EB88 **CB 11 40 00** 01 00 00 00

OEP= **4011CB (Anotarlo)**

Abrir PUPE, seleccionamos el proceso de arriba y ponemos el OEP. Marcar 2 bytes, luego presionar el botón Buscar y aparecerán los Bytes Originales. (Anotarlos)



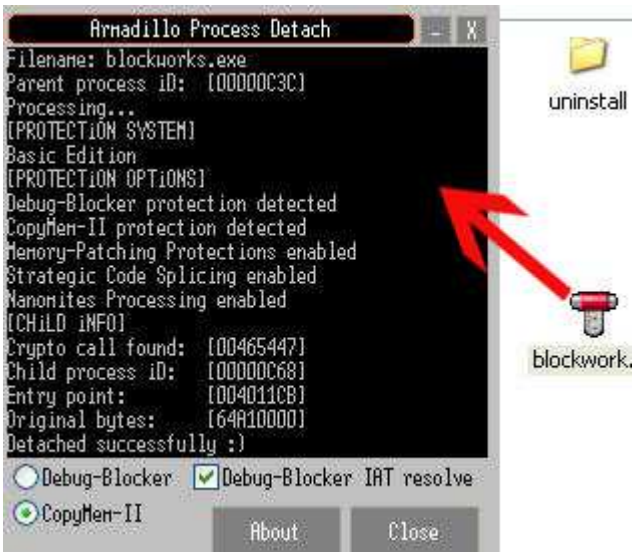
Bytes originales: 64A1

Reiniciar Olly.

++

Usando ArmaDetach

1) Ejecutar ArmaDetach y arrastrar el exe empacado dentro del ArmaDetach.
2) Seleccionar la Opción CopyMenII (Tambien trae para DBIR)



3) Atachear el proceso del empacado con Olly.

4) F9 y pausa.
5) Quitar el loop infinito (EBFE) poniendo los bytes originales que vimos en PUPE.

Antes:

Después:

Esos dos 9090 hay que cambiarlos por cero para que quede bien.

Presionamos la barra de espacio y lo editamos así:

++

Conseguir los Bytes originales sin PUPE.

BP WriteProcessMemory

F9 tres veces y ver el Stack, por ejemplo:

0012D94C 00466509 /CALL to WriteProcessMemory from 466503
0012D950 0000004C |hProcess = 0000004C (window)
0012D954 00401000 |Address = 401000
0012D958 003A2408 |Buffer = 003A2408
0012D95C 00001000 |BytesToWrite = 1000 (4096.)
0012D960 0012DA68 \pBytesWritten = 0012DA68

OEP – Address = Offset.
4011CB – 401000 = 1CB.

Buffer + Offset = DIR_OEP_HIJO.
3A2408 + 1CB = **3A25D3**.

Lo buscamos en el Dump.

003A25D3 64 A1 00 00

Esto es todo. Fue una nota rápida de los tutos que he leido.