EssentialPIM

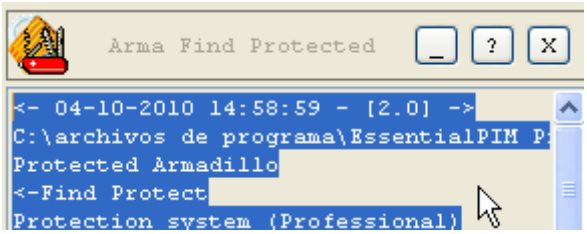
by

Apuromafo

Programa: http://www.essentialpim.com/es/index.php?r=download

Version :EssentialPIM Pro 3.73 15/09/2010 8.39 MB
Lenguaje: Delphi:
Proteccion:Armadillo:

Presentando la tool que hace poco bajamos

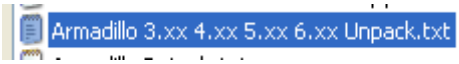


Vemos que tiene

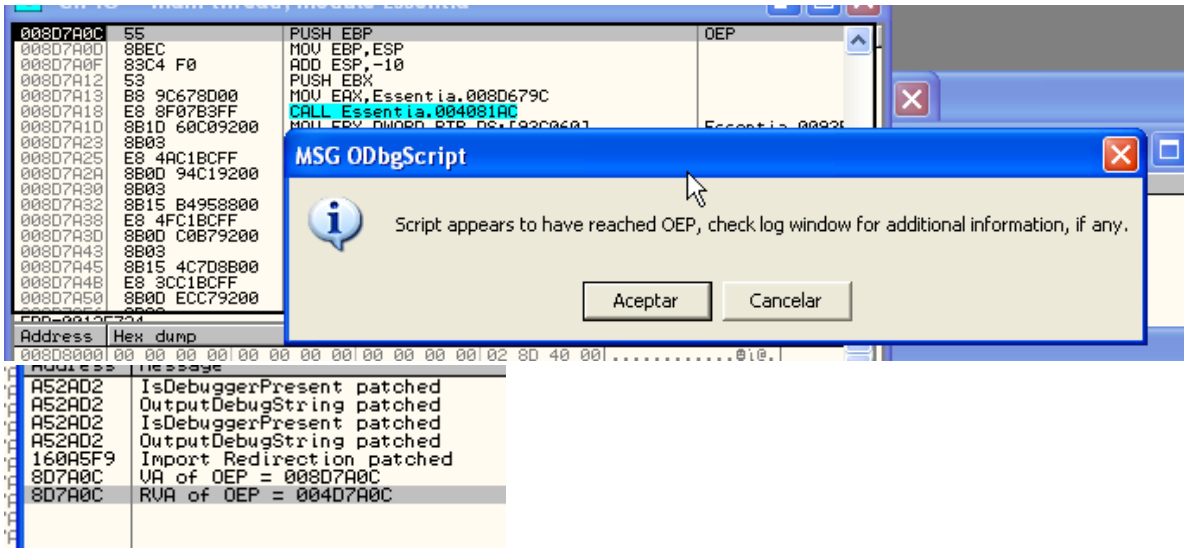
<- 04-10-2010 14:58:59 - [2.0] ->
C:\archivos de programa\EssentialPIM Pro\EssentialPIM.exe
Protected Armadillo
<-Find Protect
Protection system (Professional)
<Protection Options>
Debug-Blocker
Strategic Code Splicing
<Backup Key Options>
Fixed Backup Keys
<Compression Options>
Best/Slowest Compression
<Other Options>
<-Find Version
Version 5.42 20-02-2008
<- Elapsed Time 00h 00m 08s 984ms ->

Como bien dice el debug bloquer existen 3 rutas, si lo detecta automaticamente o debo hacerlo mediante script, o a mano, si no resultan los script lo hago a mano, pero funcionan, asi que vamos:

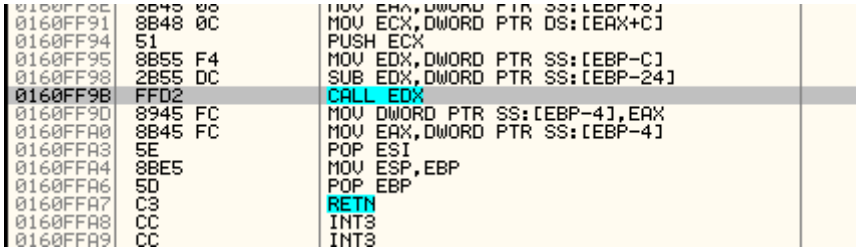
Comenzamos con la del script



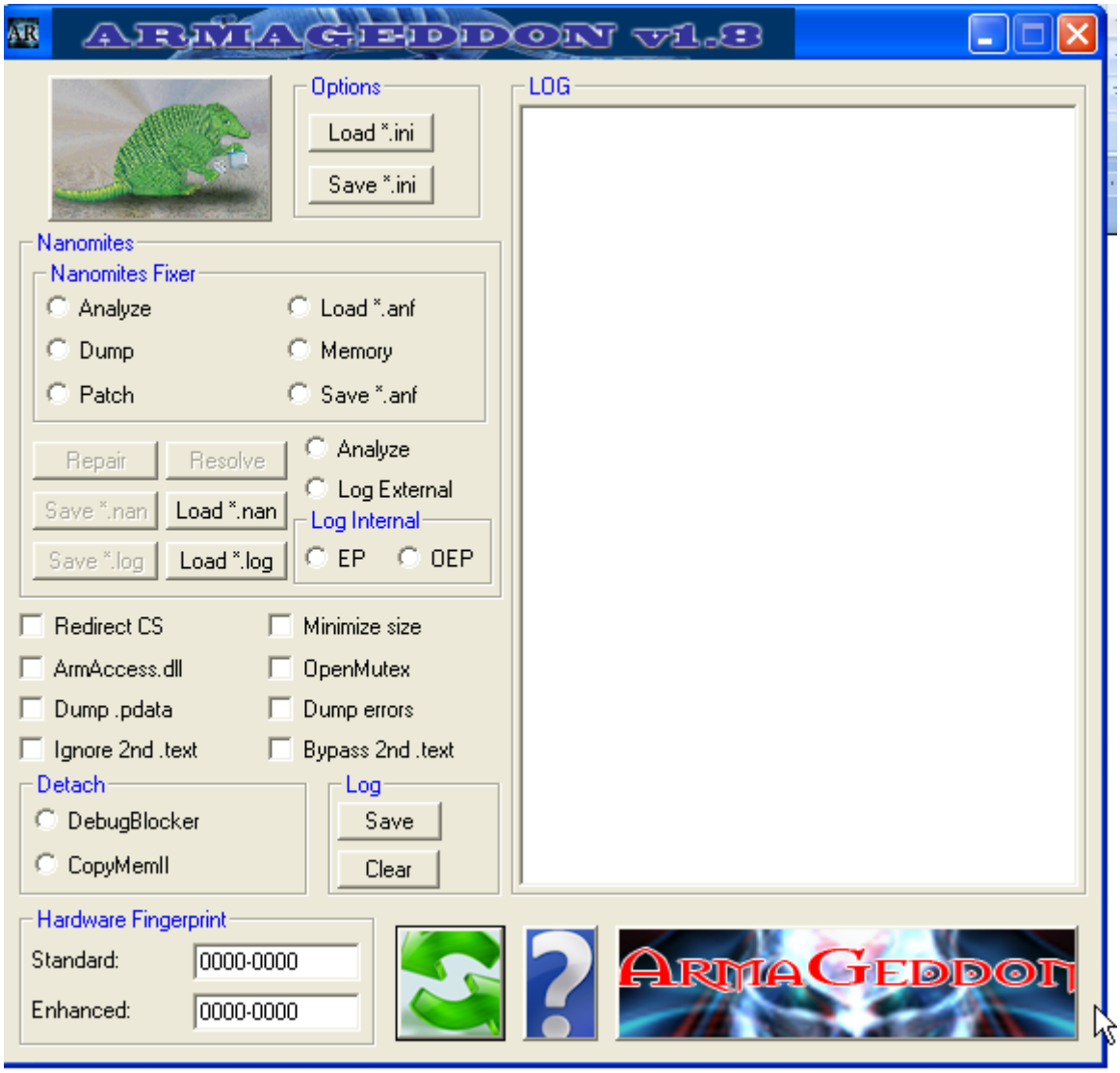
Le coloco que es version 5 y que tiene debug blocker
Luego del ok, vemos esto:



Si coloco menos vemos que el salto lo hizo call edx



Como hay tiempo, ahora vamos con armaggedon,
http://www.accessroot.com/arteam/site/download.php?list.9
Este es la apariencia

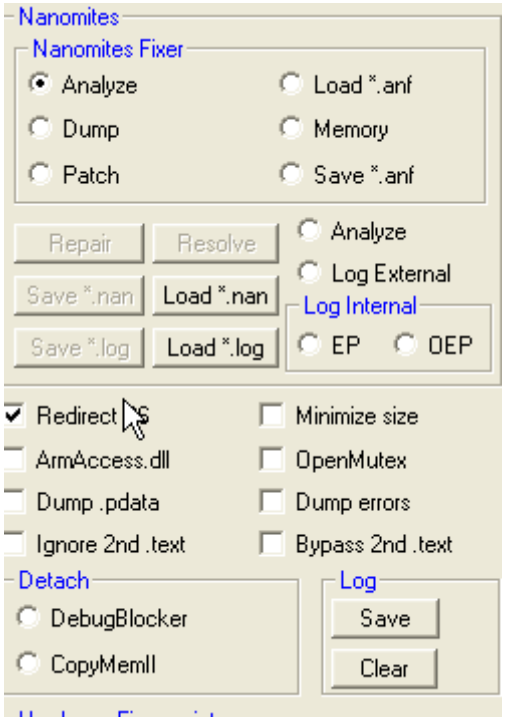


Pulso el armadillo

Como observacion, para resetear todo a cero, como si nada hubiera pasado se puede usar

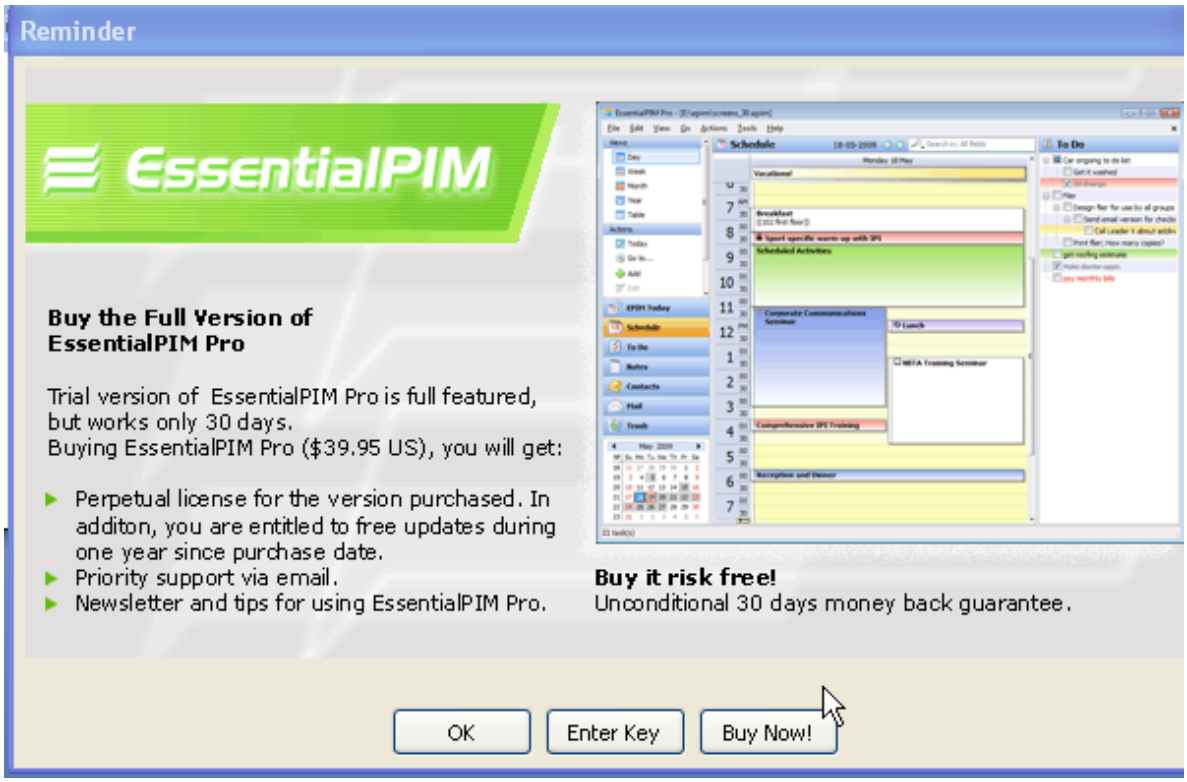
Pero no es necesario, solo el boton de armadillo cuando ya tildamos lo necesario

Ahora tildo redirect CS(code splicit), pues este lo posee



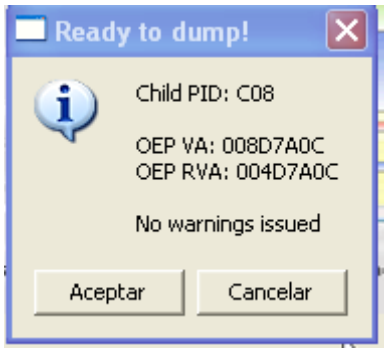
Pulsado el boton de armadillo 

Muestra



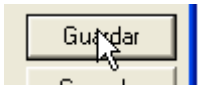
Al pulsar ok

Muestra el mensaje



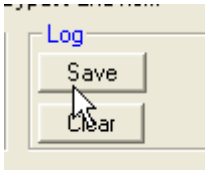
Coloco aceptar, y muestra un save y coloco

Y pulso guardar



Luego esta unpacked

Pero pulso



Para tener el log leemos todo lo que hizo

Loading target:

EssentialPIM.exe

PEiDVersion: PEiD v0.94

PEiDLLVersion: PEiDLL v1.06

file is compiled/packed/encrypted with

Armadillo V5.40 -> Silicon Realms Toolworks * Sign.By.fly * 20080214 [Overlay]

Process ID: E20

Processing target...

==========

Debug Blocker detected

child Process ID: BCC

child Thread ID: B94

==========

STRATEGIC CODE SPLICING DISABLED!

Code Splicing Section: .adata

Old VMaddress: 03F70000

Old VMsize: 0001FFC5

New VMaddress: 00A6A000

New VMsize: 00010000

Warning: Old VM size > New VM size

==========

IAT VARIABLE REDIRECTION DISABLED!

VM address: 0160B2BB

VM variable: 0163823C

==========

IAT FIXED REDIRECTION DISABLED!

VM address: 0160B753

==========

Tracing to OEP...

Context.Eip: 01610056

==========

Dumping target...

Dump done!

Saved to: unpacked.exe

==========

Rebuilding Imports...

Rebuilding Imports completed

Return code: 0

Now, you should test your target. Good luck :)

==========

IAT RVA: 005C72BC

IAT Size: 00000CAC

OEP VA: 008D7A0C

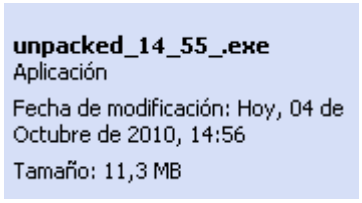
OEP RVA: 004D7A0C

OEP call return VA: 0160FF9D

Exit Process ID: E20

Saving logfile...

Done.



En cualquier caso armadillo en versiones menores a 7.x no es problema, sobre 7.x y 8.x , sera necesario crear mas script para los mutex, emulatexpired y otras cosas raras que ha incorporado para reconstruir la iat

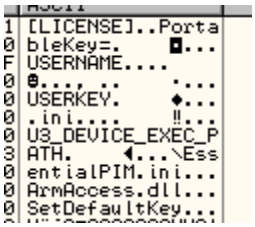
Ahora veo los entornos llamados con el uso de GetEnvironmentVariableA

El notepad queda asi:

```
0012FA2C   004154BA  /CALL to GetEnvironmentVariableA from unpacked.004154B5
0012FA30   008851A4  |VarName = "PORTABLE"
0012FA34   0012FA3C  |Buffer = 0012FA3C
0012FA38   00000400  \BufSize = 400 (1024.)
0012FA3C   7FFEFFFF

0012FA2C   004154BA  /CALL to GetEnvironmentVariableA from unpacked.004154B5
0012FA30   008851B8  |VarName = "TRIAL"
0012FA34   0012FA3C  |Buffer = 0012FA3C
0012FA38   00000400  \BufSize = 400 (1024.)
0012FA3C   7FFEFFFF

0012FA2C   004154BA  /CALL to GetEnvironmentVariableA from unpacked.004154B5
0012FA30   008851C8  |VarName = "EXTRAINFO"
0012FA34   0012FA3C  |Buffer = 0012FA3C
0012FA38   00000400  \BufSize = 400 (1024.)
0012FA3C   7FFEFFFF

0012FA00   004154BA  /CALL to GetEnvironmentVariableA from unpacked.004154B5
0012FA04   0088320C  |VarName = "OUTLSYNC"
0012FA08   0012FA10  |Buffer = 0012FA10
0012FA0C   00000400  \BufSize = 400 (1024.)|

0012FA2C   004154BA  /CALL to GetEnvironmentVariableA from unpacked.004154B5
0012FA30   00885298  |VarName = "USERKEY"
0012FA34   0012FA3C  |Buffer = 0012FA3C
0012FA38   00000400  \BufSize = 400 (1024.)

0012F9B0   004154BA  /CALL to GetEnvironmentVariableA from unpacked.004154B5
0012F9B4   008B93DC  |VarName = "USERNAME"
0012F9B8   0012F9C0  |Buffer = 0012F9C0
0012F9BC   00000400  \BufSize = 400 (1024.)

0012FA54   004154BA  /CALL to GetEnvironmentVariableA from unpacked.004154B5
0012FA58   008888A0  |VarName = "KEYCREATED"
0012FA5C   0012FA64  |Buffer = 0012FA64
0012FA60   00000400  \BufSize = 400 (1024.)
```

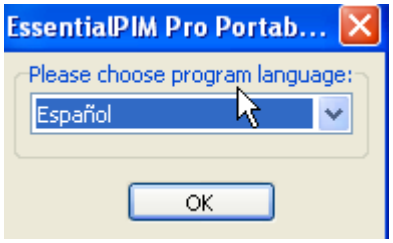
0012FA30 008851C8 |VarName = "EXTRAINFO"
0012FA04 0088320C |VarName = "OUTLSYNC"
0012FA30 00885298 |VarName = "USERKEY"
0012F9B4 008B93DC |VarName = "USERNAME"
0012FA58 008888A0 |VarName = "KEYCREATED"

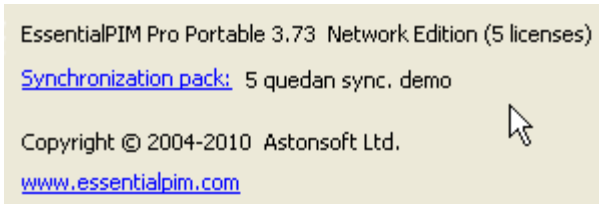
Si esta habilitado el portable y se crean las carpetas,debe tener los datos o similares a esto:



Pero no suelo crear licencias portables. Por lo que busco la variable y anulo el salto

Aparece:



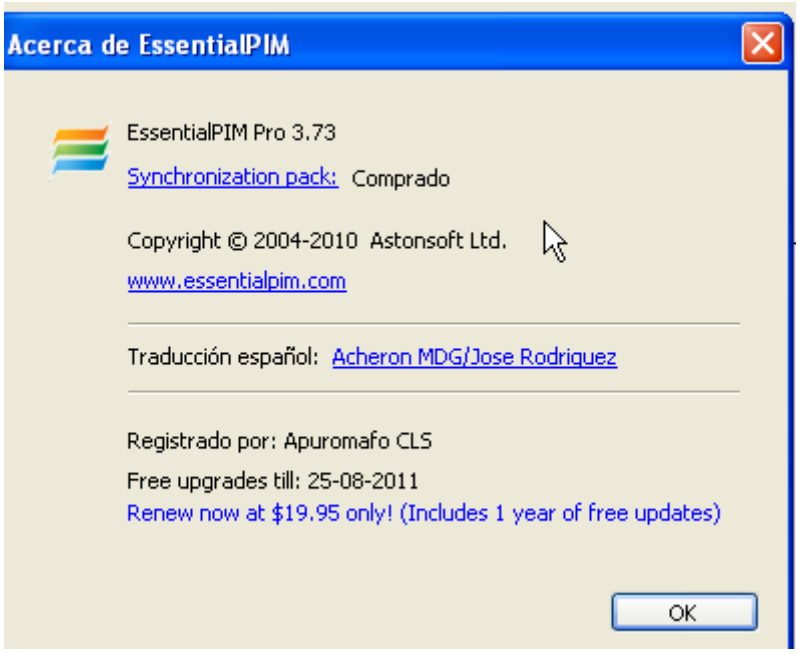


Como la version que tengo es demo para 5 pruebas

Si compraramos podriamos tener mas,

Asi que felicito a la aplicacion, tiene varias opciones

Aqui se agregaron todas las variables necesarios



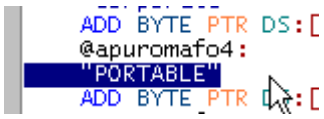
Si quieren 1 año de update aqui esta el enlace:

https://secure.bmtmicro.com/servlets/Orders.ShoppingCart?CID=4584&PRODUCTID=45840010

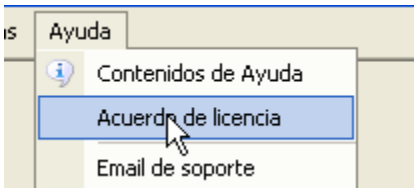
Ahora colocando algo en portable

```
008D7AB1  9C              PUSHFD
008D7AB2  BB C034837C     MOV EBX,kernel32.SetEnvironmentVariableA
008D7AB7  68 2C7B8D00     PUSH <unpacked.apuromafo>                ASCII "key"
008D7ABC  68 317B8D00     PUSH <unpacked.apuromafo2>               ASCII "USERKEY"
008D7AC1  FFD3            CALL EBX
008D7AC3  68 3A7B8D00     PUSH <unpacked.apuromafo3>               ASCII "Corporate"
008D7AC8  68 457B8D00     PUSH <unpacked.apuromafo4>               ASCII "PORTABLE"
008D7ACD  FFD3            CALL EBX
008D7ACF  68 4F7B8D00     PUSH <unpacked.apuromafo5>               ASCII "500"
008D7AD4  68 567B8D00     PUSH <unpacked.apuromafo6>               ASCII "OUTLSYNC"
008D7AD9  FFD3            CALL EBX
008D7ADB  68 607B8D00     PUSH <unpacked.apuromafo7>               ASCII "2010.10.28"
008D7AE0  68 6C7B8D00     PUSH <unpacked.apuromafo8>               ASCII "KEYCREATED"
008D7AE5  FFD3            CALL EBX
008D7AE7  90              NOP
008D7AE8  90              NOP
008D7AE9  90              NOP
008D7AEA  90              NOP
008D7AEB  90              NOP
008D7AEC  90              NOP
008D7AED  90              NOP
008D7AEE  90              NOP
008D7AEF  90              NOP
008D7AF0  90              NOP
008D7AF1  90              NOP
008D7AF2  90              NOP
008D7AF3  68 827B8D00     PUSH <unpacked.apuromafo11>              ASCII "01"
008D7AF8  68 867B8D00     PUSH <unpacked.apuromafo12>              ASCII "EXTRAINFO"
008D7AFD  FFD3            CALL EBX
008D7AFF  68 917B8D00     PUSH <unpacked.apuromafo13>              ASCII "Apuromafo CLS"
008D7B04  68 A07B8D00     PUSH <unpacked.apuromafo14>              ASCII "USERNAME"
008D7B09  FFD3            CALL EBX
```

SI coloco la opcion portable



Aparece lo mismo pero portable

Y lo ultimo, para que los links Sirvan 

, debemos renombrarlo por el nombre original.

Saludos Cordiales a la lista en General Apuromafo