|  |
| --- |
|  |

****

|  |
| --- |
| **Armadillo 3.3d** |
| Usando las herramientas en los momentos indicados |
|  |
| Este pequeño tutorial expondrá herramientas de otros usuarios para enfrentarnos a un armadillo 3.x un poco especial |
|  |
| **Apuromafo** |
| **01/12/2015** |
|  |

Contenido

[*Introducción:* 2](#_Toc436764316)

[Protecciones en el Armadillo: 3](#_Toc436764317)

[Unpacking con Tool/herramientas: 5](#_Toc436764318)

[Unpacking con Ollydbg+Script: 6](#_Toc436764319)

[Herramientas Keygening: 10](#_Toc436764320)

[Resultados: 13](#_Toc436764321)

[Conclusión: 14](#_Toc436764322)

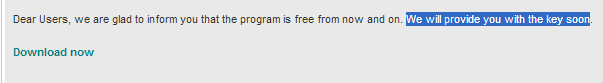
# *Introducción:*

Hola hace mucho un buen amigo, pidió ayuda a desempacar, pero dado que normalmente no me detengo cuando de armadillo se trata, aquí otro pequeño tutorial.

*Hay una manera de contribuir a la protección de la humanidad, y es no resignarse. Ernesto Sábato (1911); escritor argentino*

|  |  |
| --- | --- |
| Programa | UnJpeg |
| Compañía | Copyright Aggressive Imaging, Inc. 2003-2005 |
| Descarga | [http://www.unjpeg.com/unjpeginst.exe](http://www.google.com/url?q=http%3A%2F%2Fwww.unjpeg.com%2Funjpeginst.exe&sa=D&sntz=1&usg=AFQjCNEkiGg92xFTBOnnxk20hVvbMvJrcA) |
| Tamaño | Setup: 3.7 MB / Programa: 2.05 MB |
| Víctima | UnJpeg.exe |
| Versión del Programa | 1.5.0.11 |
| Herramientas | OllyDbg y las que se necesiten para armadillo. |
| Packer/protector | Armadillo 3.3d |
| Utilidad | Advanced techniques in our product make it possible for you to return JPEG images to their original look, removing the JPEG artifacts and cleaning up the blotchy look. This program is able to recover up to 98% of the original image data of high-quality JPEGs. Even non-restorable heavily compressed images will improve as well - they will not look "scary" anymore and will be suitable for publishing/printing. |
| Entorno | Windows 8.1 / Virtual Machine Windows XP sp3 |
| Compilador | Visual C/C++ |
| Objetivos | Desempacar/ver limitaciones |
| Tutorial por | Apuromafo CLS con la Colaboración de Ivinson |
| Fecha | 30-11-2015 |

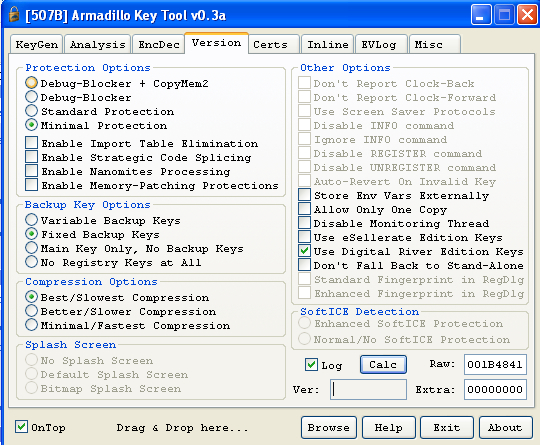
Hoy, vamos a comentar hoy sobre un packed con “Armadillo”, la historia de hoy es del pasado , prometieron dar una llave gratuita hace años 2005 , luego de 10 años online creo que es tiempo de hacerle escrito,para revivir un poco una hazaña: <http://foro.elhacker.net/ingenieria_inversa/ayuda_con_armadillo_peleon-t395518.0.html>



Esa llave pronto, realmente lleva años el mensaje.

# Protecciones en el Armadillo:

Usando Atk de Mr.exodia [**https://github.com/mrexodia/akt**](https://github.com/mrexodia/akt):



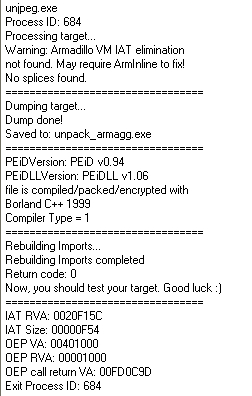
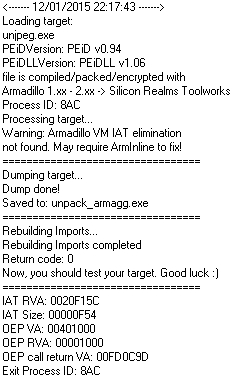
Armadillo Informant de Ghandi, además me refiere

|  |
| --- |
| Call exe OEP: 0x006D86FF //Call dll OEP: 0x006D709F  Offset to Security.dll: 0x0000000E //Security.dll size: 0x0003B000  Security.dll base: 0x10000000 //CopyMem-II decrypt: 0x1001FB11 |

**Arma Find Protected 2.1** [**http://forum.exetools.com/showthread.php?t=14131**](http://forum.exetools.com/showthread.php?t=14131)

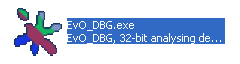
|  |
| --- |
| <- 01-12-2015 22:10:48 - [2.1x32] ->  C:\Archivos de programa\UnJPEG\unjpeg.exe  Protected Armadillo  File Size 2150400  Load file  <-Find Protect  Protection system(Digital River)  <Protection Options>  Standard protection or Minimum protection  <Backup Key Options>  Fixed Backup Keys  <Compression Options>  Better/Slower Compression  <Other Options>  Use Digital River Edition Keys  <-Find Version  Version 3.30d 12Oct2003 (limited release)  <- Elapsed Time 00h 00m 00s 561ms -> |

Al probar el unpacker Armageddon 1..9 /2.0



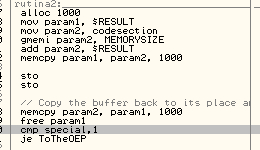
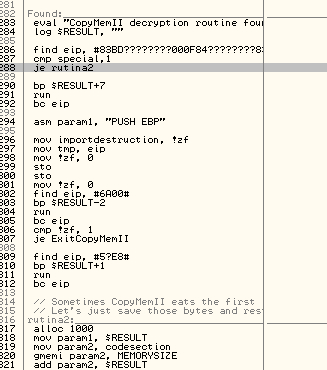
encuentra el OEP pero dado las largas distancias entre los saltos de la iat, este no encuentra el valor correcto..

# Unpacking con Ollydbg+Script:

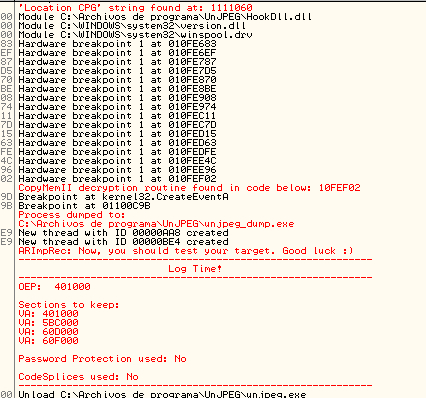
Windows xp sp3 en un entorno virtual Me propongo encontrar información relevante en un Evo Dbg

AL abrir estoy en entrypoint

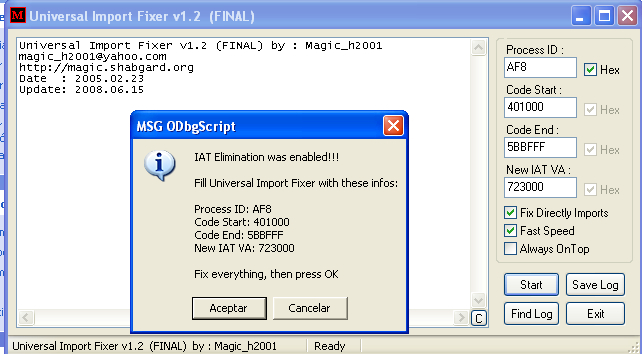
Al ejecutar script genérico para armadillo en <https://forum.tuts4you.com/topic/36970-armadillo-factotum-universal-10/> me refiere que soporta de la versión 3.7 a la última, este es un 3.3d, en este caso hay que modificar un poco porque tampoco sirve, la realidad es que la rutina de desencriptación de copymewII cuando no es usada, basta intentar llegar al oep y reparar la iat desde ahí.



Hace uso de la dll de Nacho\_dj que usa en ArmaGeddon, por otro lado es posible automatizar el proceso completo solo le falta opción para nanomites o bien casos particulares de versión 3.x



Con estas modificaciones puedo desempacar , luego pide reparar la iat con Universal Import fixer



Luego de seguir las instrucciones, reparar la importación, aceptar y tenemos unpacked:

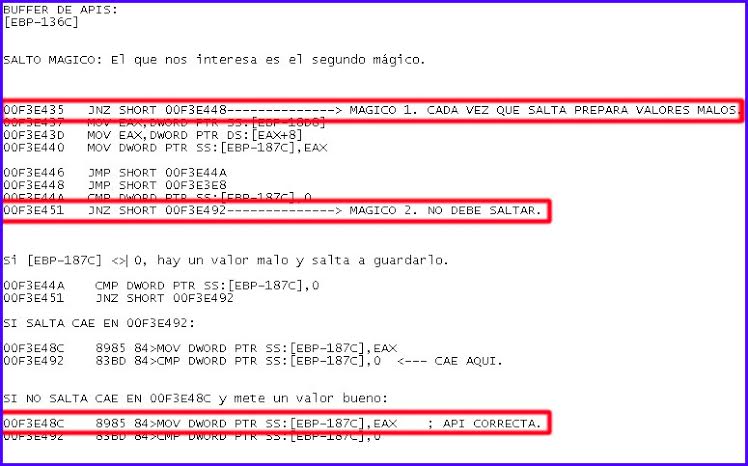
Al preguntar que opinaba ivinson, me refiere que no se anima a hacer escrito porque son similares a los escritos 1402 y 1436 .

1.F2 en .text 2.Arreglar la PE Header. 3.Darle Full Access a las secciones para dumpear.

Lo único es la puta IAT que un trozo está aquí y el otro a 100 metros. :) por eso es que hace fallar al

Armeggedon. Jeje.

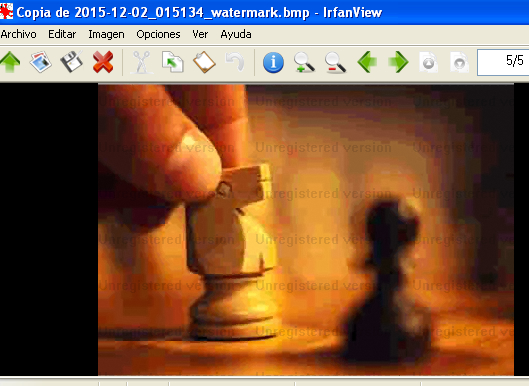
ImpRec:  
  
OEP: 1000 SIZE: F54 RVA: 20F15C Salto mágico1:00F3E435

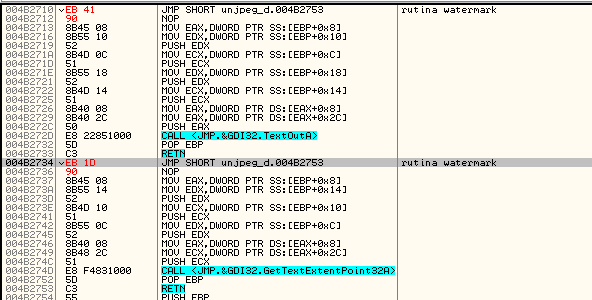


Y al ensamblar estos JMP, evito las APIS que crean el Watermark:

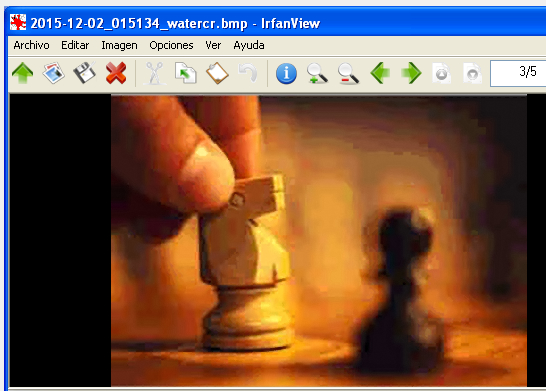
004B2710    JMP SHORT 004B2753  
gdi32.TextOutA  
  
004B2734    JMP SHORT 004B2753  
gdi32.GetTextExtentPoint32A

Antes





Después

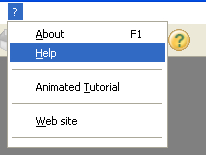


También puedes jugar con el archivo de lenguaje de Unjpeg: DefLang.ini

Si cambias: RegisterMenuItem\_Caption= por esto RegisterMenuItem\_Caption=- O sea, le pones un signo menos "-" el botón Register Now desaparece. Jeje.

Y en ProductName\_Caption=Unjpeg puedes poner:  
  
ProductName\_Caption=Registered to Ivinson

y te lo muestra en el About.



|  |
| --- |
| Pruebo el tema de licencia: con el primer certificado:  Certificate 1 :: Level 28d (1Ch) -> V3 Signed Short Level 9 (ElGamal-97)  -> pub/G/Base : 20174669929115443013078192424 d (4130188850F5911DD2579128 h)  -> P/Mod : 79228162514264337593543953223 d (1000000000000000000000B47 h)  -> Y/Power : 44207256277743581774112235690 d (8ED762A4CC32F08EE19E20AA h)  -> pvt/X/Exp : 48769062890053283180642877639 d (9D94D2C4C61E30813C20C0C7 h)  -> Checksum : 2113E6AE  Sym 5f228876, 2a12a7c3  Dado que es digital river, no me resuelve…seguir con otro certificado sería perdida de tiempo…en una versión 3.x existen muchos unsigned versión. |

# Conclusión:

Si fuera por resumir el escrito,Tenemos un empacado con armadillo con una versión limitada, cuando la iat no es común las herramientas fallan, pero cuando uno puede reparar algo hace la diferencia para integrar más cosas el programa es full,solo la limitación de watermark, se puede intentar keygening pero tiene muchos certificados falsos, en este caso revisé un certificado que parecía ser y no tomaba para otro día reviso con depurador que checksum es el que lee.

Les mando un saludo es un escrito relativamente brev Pd: Armadillo es un buen protector, el tema es cuando se quita la protección ya no es lo mismo de bueno, con este escrito puedo decir que en algunos casos es mejor desempacarlo que registrarlo con keygening, este es un ejemplo.

Saludos a toda la Lista de Crackslatinos. Apuromafo CLS

