|  |
| --- |
|  |

****

|  |
| --- |
| **Armadillo 9.x** |
| Usando las herramientas en los momentos indicados |
|  |
| Este pequeño tutorial expondrá herramientas de otros usuarios para enfrentarnos a un armadillo 9.x un poco especial |
|  |
| **Apuromafo** |
| **02/12/2015** |
|  |

Contenido

[*Introducción:* 2](#_Toc436818796)

[Protecciones en el Armadillo: 3](#_Toc436818797)

[Unpacking con Ollydbg+Script: 4](#_Toc436818798)

[Conclusión: 5](#_Toc436818799)

# *Introducción:*

Hola siempre que abro mi carpeta de verificar encuentro uno que otro armadillo, comparto otra mini historia

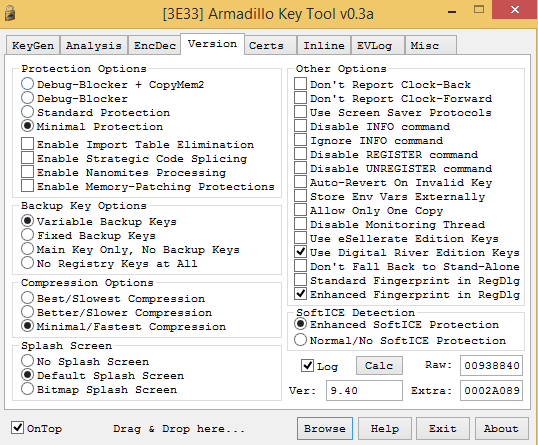
*Si quieres triunfar, no te quedes mirando la escalera. Empieza a subir, escalón por escalón, hasta que llegues arriba.*

|  |  |
| --- | --- |
| Programa | DJ.Java.Decompiler |
| Compañía | Developer : Atanas Neshkov |
| Descarga | Web-site : http://www.neshkov.com/ |
| Tamaño | Setup: 10 MB / Programa: 5.84 MB |
| Víctima | DJ.exe |
| Versión del Programa | 3.12.12.100: |
| Herramientas | OllyDbg y las que se necesiten para armadillo. |
| Packer/protector | Armadillo 9.x |
| Utilidad | JAVA decompiler |
| Entorno | Windows 8.1 / Virtual Machine Windows XP sp3 |
| Compilador | Borland Delphi |
| Objetivos | Desempacar |
| Tutorial por | Apuromafo CLS |
| Fecha | 30-11-2015 |



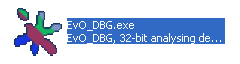
El programa es full funcional, pero tiene limitación de usos, esto significa que si desempacamos, ya no habrá mas limitación.

# Protecciones en el Armadillo:

1. Analizando el Packer : Tool de Mr.exodia Armadillo Keytool (atk) [**https://github.com/mrexodia/akt**](https://github.com/mrexodia/akt)

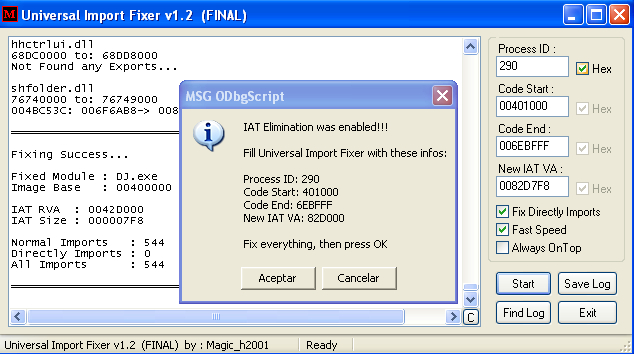
Datos actuales: Checksum: AD75689C salt: 3B6E957D Level Short V3 Lv 10

# Unpacking con Ollydbg+Script:

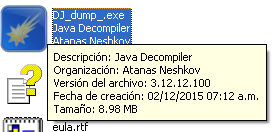
Windows xp sp3 en un entorno virtual Me propongo encontrar información relevante en un Evo Dbg

Hago uso de <https://forum.tuts4you.com/topic/36970-armadillo-factotum-universal-10/>

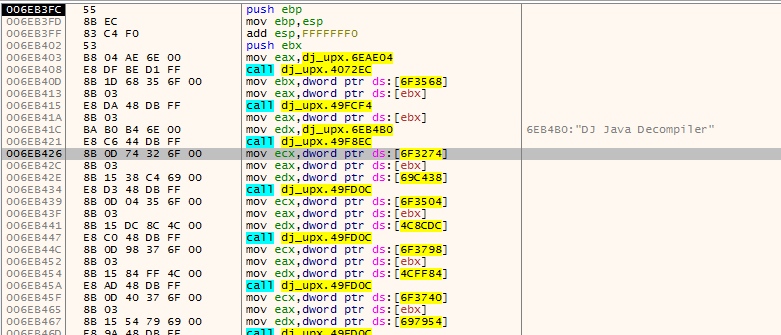
En el entrypoint, ejecuto script, Muestra un error en una comparación en una línea 9xx , luego de eso muestra el nag trial, al colocar continuar muestra el mensaje de reparación de iat. Una vez reparado con UIF 1.2 pulso ok (aceptar)



y en la ruta lo tenemos desempacado.



Verifico si corre en Windows 8.1 y tenemos el programa sin limitación:



Al googlear, se puede encontrar <http://forum.exetools.com/showthread.php?t=15715> que ya está desempacado, pero no hay como tener su programa sin dudas de existencia de malware.

# Conclusión:

Si fuera por resumir el escrito, tenemos un empacado con armadillo con Digital Signature, además no sirven las herramientas automáticas, solo script, tiene muy buenas opciones de protección, a primera vista no veo secured section, pero basta con desempacar y está funcional, ya está desempacado de otros lados, pero igual nunca es tarde para verificar herramientas.

Pd: Armadillo es un buen protector, el tema es cuando se quita la protección ya no es lo mismo de bueno, en este caso es mejor desempacar que registrar.

Saludos a toda la Lista de Crackslatinos. Apuromafo CLS

