|  |
| --- |
|  |

****

|  |
| --- |
| **Armadillo 6.x** |
| Usando las herramientas en los momentos indicados |
|  |
| Este pequeño tutorial expondrá herramientas de otros usuarios para enfrentarnos a un armadillo 6.x un poco especial con sdk |
|  |
| **Apuromafo** |
| **02/12/2015** |
|  |

Contenido

[*Introducción:* 2](#_Toc436834835)

[Protecciones en el Armadillo: 3](#_Toc436834836)

[Conclusión: 8](#_Toc436834837)

# *Introducción:*

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

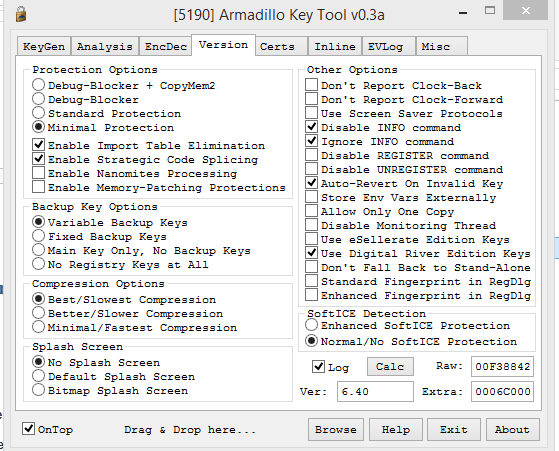
*Si quieres triunfar, no te quedes mirando la escalera. Empieza a subir, escalón por escalón, hasta que llegues arriba.*

|  |  |
| --- | --- |
| Programa | TagTuner |
| Compañía | Copyright © 2009 tagtuner.com. All rights reserved. |
| Descarga | http://www.tagtuner.com/ |
| Tamaño | Setup: 4.0.1 / Programa:4.05 mb |
| Víctima | TagTuner.exe |
| Versión del Programa | 2.0.0.1921 |
| Herramientas | ATK tool. |
| Packer/protector | Armadillo 6.4 |
| Utilidad | Música |
| Entorno | Windows 8.1 / Virtual Machine Windows XP sp3 |
| Compilador | Borland Delphi |
| Objetivos | verificar si se puede registrar |
| Tutorial por | Apuromafo CLS |
| Fecha | 02-12-2015 |

El programa es full funcional, solo algunas limitaciones de tiempo y cosas de armadillo.

# Protecciones en el Armadillo:

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



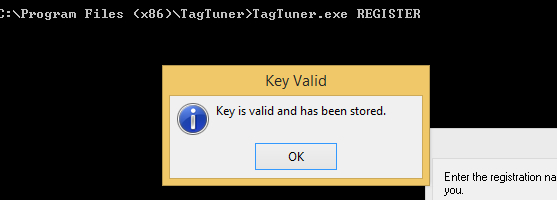
Lo que destaca de esto es que no está desactivado el comando register



Luego en un bat puedes colocar el comando y registrar

Tengo de apunte del pasado una versión anterior

el objetivo de hoy es probar si sirve, **y de paso generar una clave con diferente nombre a la provista solo de un tipo de licencia que me han dado…**



Al minuto sirven,

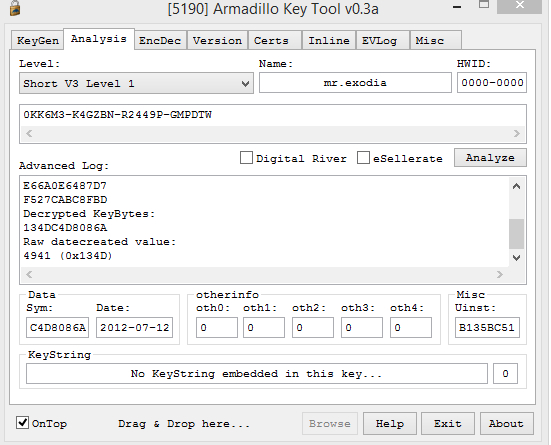
|  |
| --- |
| 1. Install TagTuner v2.0.1892 2. Copy REGISTER.bat to install DIR and open      1. Use any of the provided serials to register if you like, buy it ☺     Serials (various license types):  Name : mr.exodia  License --30 Days Trial Code : 0KK6MV-7NH8P2-ZHRZRK-5ZGXK7  License --90 Days Trial Code : 0KK6NM-HTCXGR-M58825-T89DTU  License --Single User License 1 Code : 0KK6NH-T9AZUV-FRMG5E-5KEJQM  License --Single User License 2 Code : 0KK6M9-XE5Z7E-7AY6EK-Q9QP9E  License --2 User License Code : 0KK6MN-BP5RPB-0VJQ8Q-C3VB9X  License --3 User License Code : 0KK6MF-D0N6U8-5GF4MT-BFM33Z  License --4 User License Code : 0KK6MM-3HFGY3-H0RKPV-MBV40T  License --5 User License Code : 0KK6NY-NAH1AQ-ZU9JGQ-HGC03T  License --5 User Family Pack Code : 0KK6M6-MC4WZD-WT7P9E-0EDD9C  License --Enterprise 5 User License: Code : 0KK6M3-K4GZBN-R2449P-GMPDTW |

Si realmente tengo mucho tiempo, aquí tengo todos los certificados, necesito primero los niveles de las licencias, como se puede apreciar todas son Short V3 Lv 1, esto es bueno, si fuera Short V3 lv 10 me sería necesario parchar ECDSA, si el serial que tenía en el apunte, no es valido, solo debo generarlo con lo que obtuve, si es válido solo debería confirmar de cual es cada cual.

|  |  |  |
| --- | --- | --- |
| Global Information:  TimeStamp : 4993DE88  First DWORD : 61540008  Project ID : TagTuner  Magic1 : DE368B9F  Magic2 : 26AD  Public Certificate Information:  Short V3 Level 1:  Chk : 0ECC1827  Sym : A6490591  Y : 67598ED3  Pvt : AD8C181  Short V3 Level 1:  Chk : 754E1105  Sym : 1885E8DC  Y : 58D4D65F  Pvt : 5F49BD76  Short V3 Level 1:  Chk : 6BA2E0AA  Sym : D030A883  Y : 50BDCC29  Pvt : 444C2EF  Short V3 Level 1:  Chk : 4D56B611  Sym : F71C2609  Y : B2A88145  Pvt : 5F47666B | Short V3 Level 1:  Chk : D9FEB0F3  Sym : 301607E8  Y : F417BD0C  Pvt : E68F306C  Short V3 Level 1:  Chk : FB9B2DA3  Sym : 9FCAA191  Y : 837BAC86  Pvt : ED6D6AD6  Short V3 Level 1:  Chk : 7EE30FCE  Sym : 9ACDF381  Y : E5088EB4  Pvt : 2C16EADD  Short V3 Level 1:  Chk : 10ECDAD0  Sym : 0D95D848  Y : B338859A  Pvt : 88B87CA9  Short V3 Level 1:  Chk : CD803DDA  Sym : ED12A073  Y : 45BA1404  Pvt : 9FBAD5C4  Short V3 Level 1:  Chk : 9FB96905  Sym : C4D8086A  Y : 38E6E9E3  Pvt : D3B91E13 | Intercepted Libraries:  +MSVBVM50.DLL  +MSVBVM60.DLL  +VFP5R.DLL  +VFP6R.DLL  +VFP7R.DLL  +VFP8R.DLL  +VFP9R.DLL  +PBVM70.DLL  +MSVCRT.DLL  +PROJ.DLL  +MSJAVA.DLL  +OLE32.DLL  +VDFVM8.DLL  +MFC71.DLL  +wxw  -\*  Elapsed Time: 00h 01m 56s 922ms |

La llave que analizaré es Name : mr.exodia Code : 0KK6M3-K4GZBN-R2449P-GMPDTW

Que corresponde a un License --Enterprise 5 User License , la relevancia de hacer esto, es para buscar solo cuál es el sym de la Enterprise 5 User licence, Voy al tab de análisis y coloco usuario y clave, analizarlo que debemos tener en cuenta es el SYM, además si hay Other info y si hay KeyString, eso es de relevancia, en este caso no hay nada adicional, asi que no hay nada en especial en este caso, aún sin el serial provisto podríamos generar una clave ☺



Por lo cual para generar una key válida debo buscar en mis certificados el SYM C4D8086A

**Short V3 Level 1:**

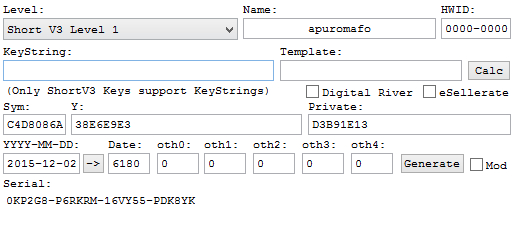
**Chk : 9FB96905**

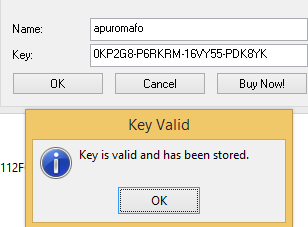
**Sym : C4D8086A**

**Y : 38E6E9E3**

**Pvt : D3B91E13**

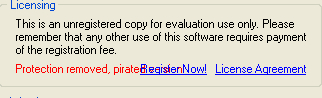
**Luego voy a keygen tool**





 **misión cumplida**

# Conclusión:

Si fuera por resumir el escrito, tenemos un empacado con armadillo con muchas opciones si desempaco tengo un mal mensaje  veo secured section, pero basta con registrar y está funcional y desencripta algo del código.

Si intento registrar, me permite mediante comando pero la idea de este escrito, es re-crear llaves , así es como algunos comparten una llave y luego la modifican por otra , o de esta forma evitan un largo bruteforce para encontrar el sym, este programa además tiene stolen key, por lo que también puede ser otro vector para atacar y encontrar un sym.

Pd: Armadillo es un buen protector pero no falta el que conoce alguna información relevante al packer.

Saludos a toda la Lista de Crackslatinos. Apuromafo CLS

