|  |
| --- |
|  |

|  |
| --- |
| **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 |
|  |
| **Apuromafo** |
| **08/07/2015** |
|  |

Contenido

*[Introducción:](#_Toc424919775)* [2](#_Toc424919775)

*[Análisis (que opciones tiene el packed de Armadillo)](#_Toc424919776)* [3](#_Toc424919776)

[Estrategias para analizar este Armadillo 9: 4](#_Toc424919777)

# *Introducción:*

Hola hace no mucho he estado volviendo de a poco depurar programas que había dejado de lado en el pasado, hoy les dejaré una pequeño escrito dado que me sorprendió

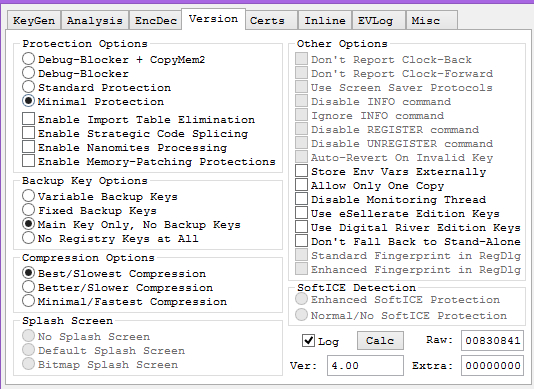
|  |  |
| --- | --- |
| Programa | Swdoctor.exe |
| Compañía | PC Tools |
| Descarga | Original: www.pctools.com/spyware-doctor/ dado que ya no existe: https://tuts4you.com/download.php?view.146 |
| Tamaño | Setup: 4.23 MB / Programa: 1.43 MB |
| Versión del Programa | 3.2.1 |
| Herramientas | Atk tool |
| Packer/protector | Armadillo 3-4 |
| Utilidad | En aquel tiempo era un buen antispyware, descontinuó en 2013 |
| Entorno | Windows 8.1 |
| Objetivos | Registrar |
| Tutorial por | Apuromafo CLS |
| Fecha | 17 -07-2015 |

Hoy, vamos a comentar hoy sobre un packed con “Armadillo”, un packer y protector bastante bueno y bastante configurable , Su web es <http://siliconrealms.com/> Actualmente refiere que ya no existe más soporte desde el primero de Julio de 2014

# *Análisis (que opciones tiene el packed de Armadillo)*

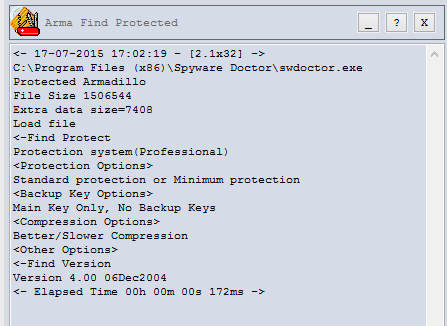
Las 2 herramientas que son de interés son de Mr.exodia (atk) y vel (arma fp 2.1)

1. **<https://github.com/mrexodia/akt> En la opción “reléase” existen versiones ya compiladas del código en el cual podemos descargar si no tenemos CODEBlocks para compilar, si alguno le interesa el codeblock se baja el** codeblocks-13.12mingw-setup.exe de <http://www.codeblocks.org/downloads/26> para inline es necesario tener codeblock para que en el caso particular de las dll puedan hacer uso.



1. **Arma Find Protected 2.1**

|  |
| --- |
| **<http://forum.exetools.com/showthread.php?t=14131>**  **->**<http://rghost.ru/36912724> |
| **<http://www.manhunter.ru/underground/94_programmi_dlya_analiza_ispolnyaemih_faylov.html>**  **->http://www.manhunter.ru/download/9329/Armadillo.Find.Protected.2.1.zip** |



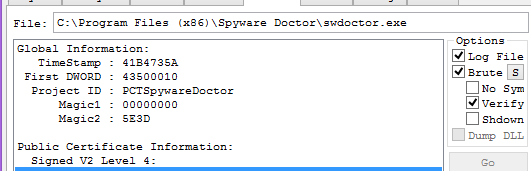
# Estrategias para analizar este Armadillo 4:

Como pueden ver el tutorial en el archivo donde hemos descargado “files” está la víctima, pero hay un tutorial donde permiten Desempacar o registrar o parchar, por mi lado intentaré registrarme.

1. En la carpeta creo un archivo .bat llamado “registrar.bat” que permita registrar vía comando que diga lo siguiente

|  |
| --- |
| @echo off  Swdoctor.exe register  @exit |

1. En armadillo keygen tool en el tab de certificados cargaré el archivo y pondremos estas opciones “verify” y “log”, el cual estará en la ruta de origen.



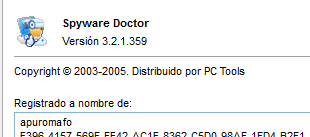
Voy a la ruta del programa y veo esto

|  |
| --- |
| Global Information:  TimeStamp : 41B4735A  First DWORD : 43500010  Project ID : PCTSpywareDoctor  Magic1 : 00000000  Magic2 : 5E3D  Public Certificate Information:  Signed V2 Level 4:  Chk : B5D5C062  Sym : A7499A04  Y : 1309A390970C4C  Pvt : 6A0D3A4114E685  Short V3 Level 5:  Chk : DEF72BB6  Sym : CACE4287  E740FBD5  Y : EE4DDD6E90CF041A  Pvt : 1E8BAE74C08B05DE  Signed V3 Level 4:  Chk : B5D5C062  Sym : A7499A04  Y : 8A01CDEE8BF9A2  Pvt : 21063317B4A04D  Intercepted Libraries:  -\*  Elapsed Time: aqui va el tiempo que tardé en procesar el brutefoce |

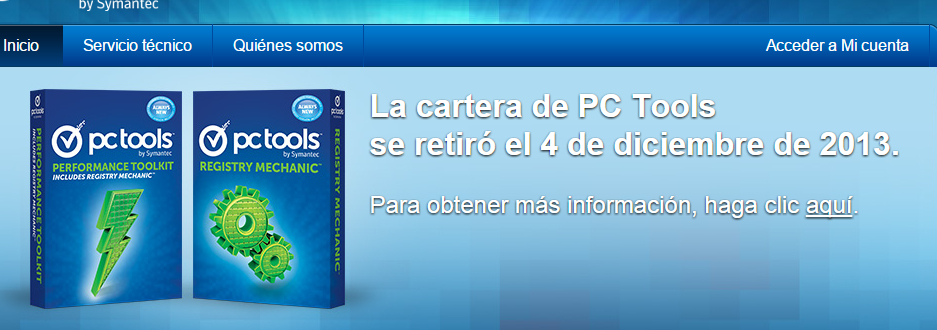
Ahora voy al tab de keygening de armadillo keygen tool, y me guio en los datos del certificado “nivel”, “sym”, “Y”,”pvt” generar y pruebo con el registrar.bat

|  |  |
| --- | --- |
| Signed V2 Level 4:  Chk : B5D5C062  Sym : A7499A04 VÁLIDO  Y : 1309A390970C4C  Pvt : 6A0D3A4114E685 |  |
| Short V3 Level 5:  Chk : DEF72BB6  Sym : ~~CACE4287 INVÁLIDO~~  E740FBD5 VÁLIDO  Y : EE4DDD6E90CF041A  Pvt : 1E8BAE74C08B05DE |  |
| Signed V3 Level 4:  Chk : B5D5C062  Sym : A7499A04  Y : 8A01CDEE8BF9A2  Pvt : 21063317B4A04D |  |

En todos los casos muestra registrado el programa y a la vez detectamos un sym inválido en el segundo certificado, al ejecutar el programa muestra como registrado sin problema.



EL programa actualmente está fuera del mercado así que nuevas actualizaciones ya no tendrá:



Un saludo cordial a la lista y personas que me son conocidas, saludos cordiales

Si fuera por resumir el escrito, simplemente les comento que tenía una carpeta con armadillos por resolver, un día sabiendo keygenear registre casi todos, entonces la espera era solamente que hicieran la herramienta pública, bueno eso es todo por hoy

Saludos Cordiales a toda la lista

Apuromafo

