|  |
| --- |
|  |

****

|  |
| --- |
| **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 |
|  |
| **Apuromafo** |
| **30/11/2015** |
|  |

Contenido

[*Introducción:* 2](#_Toc436780626)

[Protecciones en el Armadillo: 3](#_Toc436780627)

[Unpacking con Tool/herramientas: 5](#_Toc436780628)

[Unpacking con Ollydbg+Script: 6](#_Toc436780629)

[Herramientas Keygening: 10](#_Toc436780630)

[Resultados: 13](#_Toc436780631)

[Conclusión: 14](#_Toc436780632)

# *Introducción:*

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

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

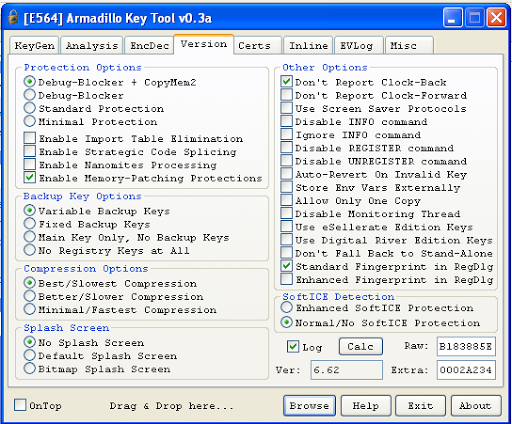
|  |  |
| --- | --- |
| Programa | Remo Recover for Android |
| Compañía | © Remo Recupere |
| Descarga | <http://www.remorecover.com/es/descargar.html>  -> <http://www.download-recovery.com/recover-android.exe> |
| Tamaño | Setup: 15.77 MB / Programa: 0.5 a 2 MB |
| Víctima | actkey32.exe |
| Versión del Programa | 2.0.0.9 |
| Herramientas | OllyDbg y las que se necesiten para armadillo. |
| Packer/protector | Armadillo 6.x |
| Utilidad | Remo Recuperar Android Se trata de una potente utilidad que realiza la recuperación eficiente de archivos como fotos, videos, música,Archivos APK, etc de un dispositivo ,Una aplicación fácil de usar que viene con fácil de navegar interfaz gráfica de usuario que permite a los usuarios alcanzar un libre de riesgo y el esfuerzo de recuperación de datos desde dispositivos Android. |
| Entorno | Windows 8.1 / Virtual Machine Windows XP sp3 |
| Compilador | Visual C/C++ |
| Objetivos | Registrar/Desempacar |
| Tutorial por | Apuromafo CLS |
| Fecha | 30-11-2015 |

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 por otro lado la última versión conocida de armadillo se baja de aqui:  
<http://web.archive.org/web/20140625052607/http://siliconrealms.com/armadillo.php>

El programa de hoy está empacado con armadillo, pero además tiene algo especial que permite que sea diferente a otros que he conocido

# 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) **En la opción “reléase” existen versiones ya compiladas del código en el cual podemos descargar , en el tab Version nos dice que las opciones**



Armadillo Informant de Ghandi, además me refiere

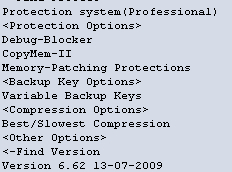
Call exe OEP: 0x004D380D //Call dll OEP: 0x004D1FB5

Offset to Security.dll: 0x0000000E //Security.dll size: 0x000F4000

Security.dll base: 0x10000000 //CopyMem-II decrypt: 0x1008DCD0

A primera vista,tenemos un armadillo 6.62 con Debug Blocker y Copymew2, además de un memory-Patching que hará complicaciones a las herramientas.

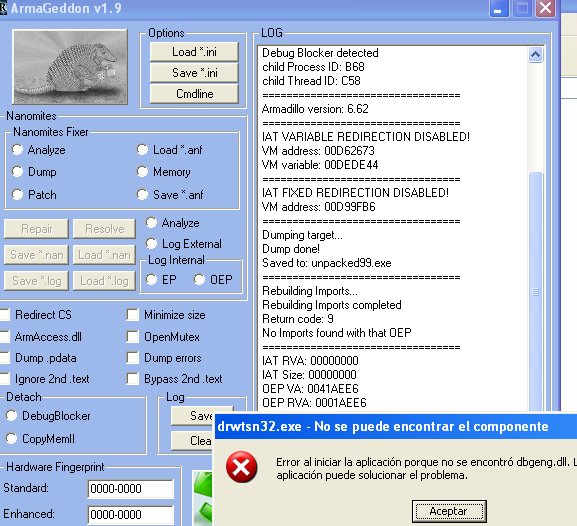
**Arma Find Protected 2.1**



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

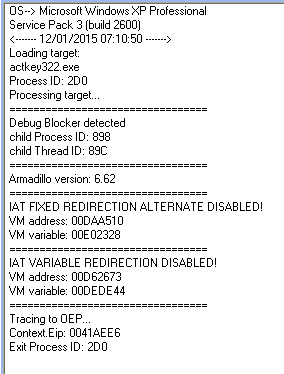
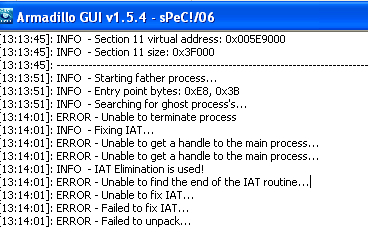
# Unpacking con Tool/herramientas:

Probando armageddon:

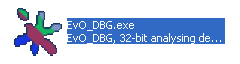


encuentra el OEP, pero me dice que no es capaz de reparar la iat por falta de permisos.

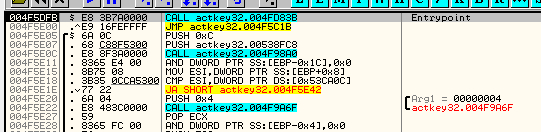
La versión 2

# Unpacking con Ollydbg+Script:

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

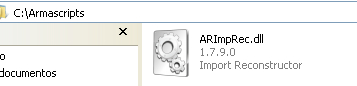
AL abrir estoy en entrypoint



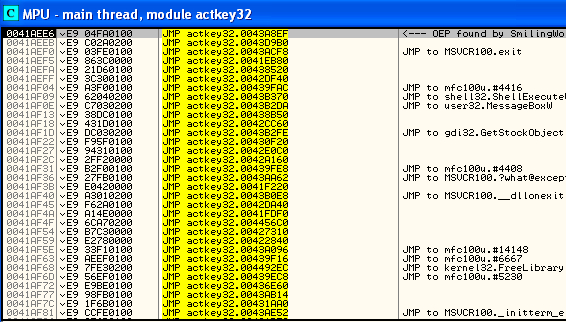
Al ejecutar script genérico para armadillo en <https://forum.tuts4you.com/topic/36970-armadillo-factotum-universal-10/>

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

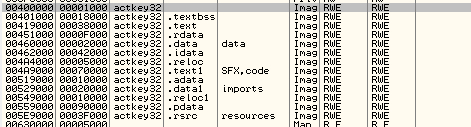
1. Da indicaciones configurar la ruta de un dll de nacho\_dj

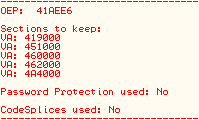


Luego ejecutar el script



Las secciones están bien con los permisos, estas en el oep y la iat está listo



en la ventana de información me muestra las secciones que se deben mantener

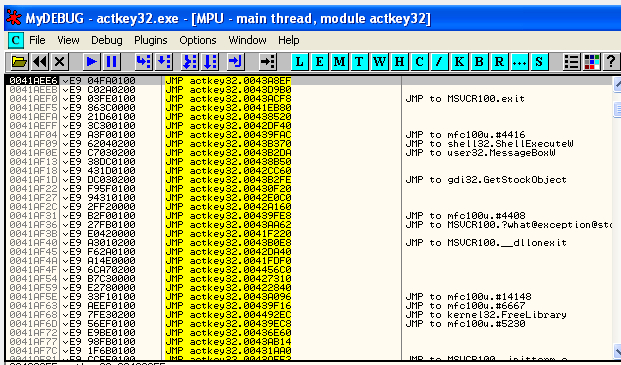
Y el dumped corre sin problemas dependiente a la dll de armadillo



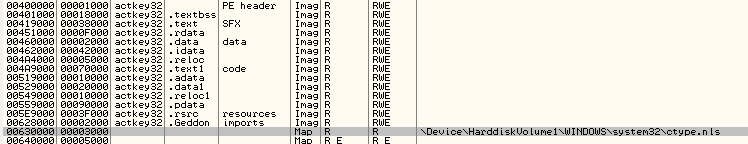
Ahora el verdadero tema a mostrar y que me llamó la atención

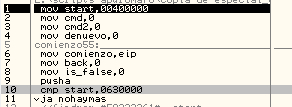
OEP, no tiene pinta real de un oep y tiene la misma ofuscación que en aquel concurso 8 Neutron Crackme **http://ricardonarvaja.info/WEB/CONCURSOS 2011/CONCURSO 8**

41AEE6 es el oep, en el comienzo de la ofuscación al igual que el Neuron crackme, tiene la misma estructura de ofuscación. Con la misma separación de int al comienzo y al igual que el anterior es un visual C/c++

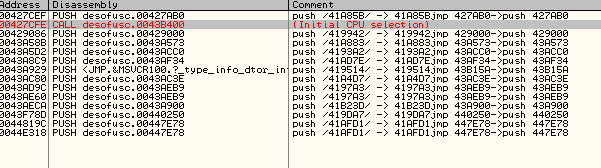


Con ayuda de mi script personal reparé JMP1>jmp 2 ->JMP 2 y CALL1 JMP2 Call 2 (los cuales dejé en concurso 8 lo único a cambiar es cmp start,(FINDEL CODIGO)

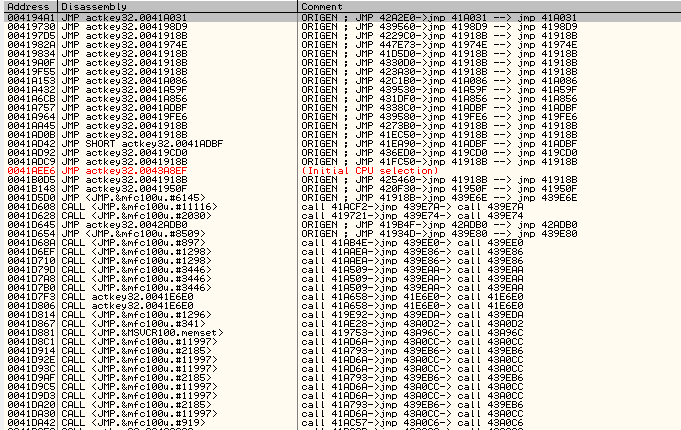




La realidad de cambiar Push, Jump-jump, call call

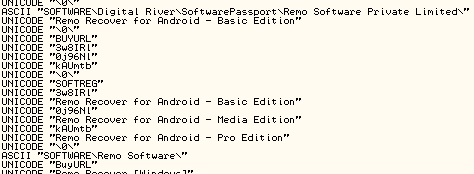


Entre todo código que permite



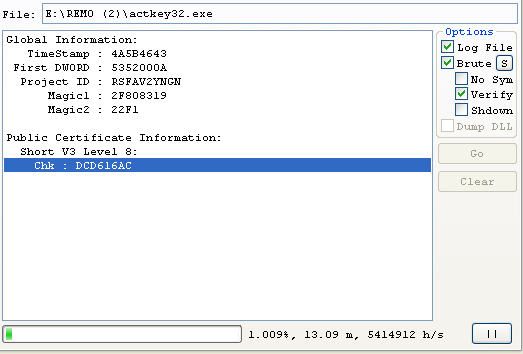
Fin de los saltos 0041B256 . E9 65EE0000 JMP actkey32.0042A0C0

Cuando terminamos de desofuscar, vemos las referencias sin problema y se entiende un poco mejor el código, a primera vista ha dejado todo el sistema de licencia en armadillo, por lo cual tenemos que conocer las versiones no mas:

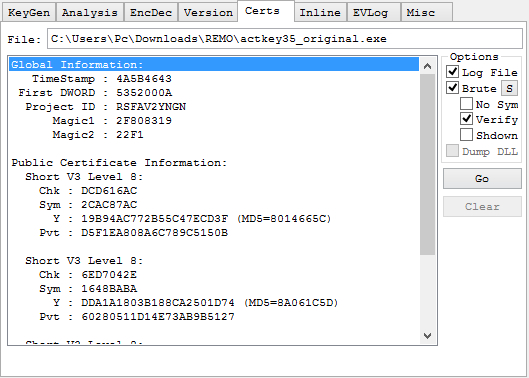


# Herramientas Keygening:

Abro denuevo atk tool en el tab de certificados



Al ver las licencias en la máquina virtual tarda unos 13minutos cada certificado, en mi pc normal, tarda segundos en terminar con todo el proceso.



Al terminar obtengo la siguiente información:

|  |
| --- |
| Global Information:     TimeStamp : 4A5B4643   First DWORD : 5352000A    Project ID : RSFAV2YNGN        Magic1 : 2F808319        Magic2 : 22F1  Public Certificate Information:    Short V3 Level 8:      Chk : DCD616AC      Sym : 2CAC87AC        Y : 19B94AC772B55C47ECD3F (MD5=8014665C)      Pvt : D5F1EA808A6C789C5150B    Short V3 Level 8:      Chk : 6ED7042E      Sym : 1648BABA        Y : DDA1A1803B188CA2501D74 (MD5=8A061C5D)      Pvt : 60280511D14E73AB9B5127    Short V3 Level 8:      Chk : 2E50E92D      Sym : 86477255        Y : F22EE596FAD360DB149DAD (MD5=CB40433F)      Pvt : EFB2BBD45A0BE37A32F75E  Intercepted Libraries:    -\*    Elapsed Time: 00h 00m 21s 969ms |

Para generar una clave válida en atk tool, colocamos en el TAB KEYGEN

Nivel Short V3 level 8, copiamos los otros datos, y como no lleva nombre no lo usaremos, el programa nos da una activación offline, nos da un HIW, luego ingresamos el HIW  que me da el activador

Solo es colocar los datos tal cual como refiere

Public Certificate Information:

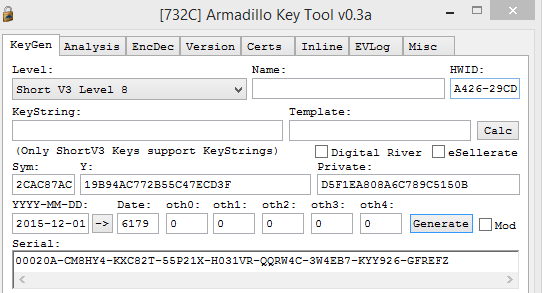
  Short V3 Level 8:

    Chk : DCD616AC

    Sym : 2CAC87AC

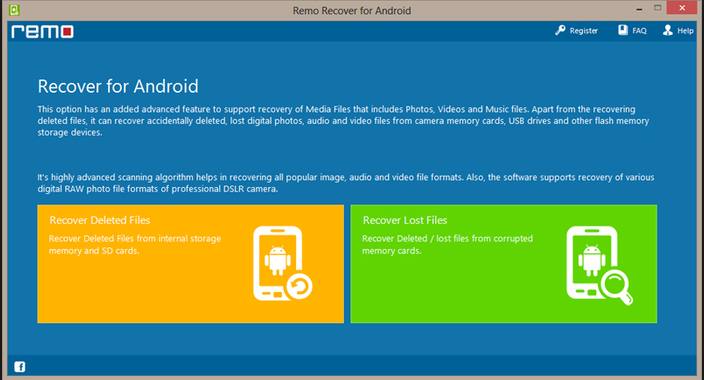
      Y : 19B94AC772B55C47ECD3F (MD5=8014665C)

    Pvt : D5F1EA808A6C789C5150B

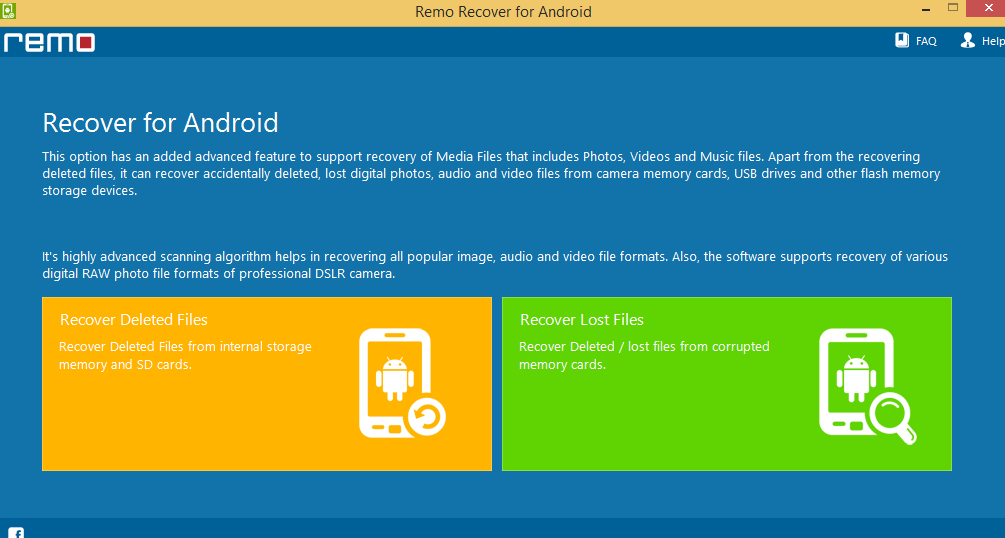
y generamos la llave, nos registra, y desde entonces el programa corre registrado

# Resultados:

Antes de la Clave:



Despues de colocar la clave:



**Desaparece el menú de register y el programa no demuestra ninguna limitación.**

# Conclusión:

Si fuera por resumir el escrito, tenemos un empacado con armadillo con Digital Signature, además no sirven las herramientas automáticas, solo script, cuando llego al oep, me encuentro mucha ofuscación de los saltos y call, luego de reparar puedo ver que posee EnvironmentVariables(EV) dependientes de la dll de armadillo, al colocarla en la ruta funciona sin problema, luego de visto por encima, todo lo importante es validado por las sdk de armadillo, por lo cual si se registra, queda operativo, al colocar los datos no requiere nombre, coloco el keygen los datos y terminé viendo el programa en full, actualmente siento que se usar estas herramientas, sino no las comentaría, bueno

Les mando un saludo es un escrito relativamente breve, solo se requiere tiempo para dar bruteforce a los certificados y segundos en colocar la clave ☺

El alcance de registrar los programas de la compañía REMO, es plena, al minuto revisé 3 y todos son con armadillo, como para registrar con un serial válido.

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 registrarlo que desempacarlo, este es un ejemplo.

Saludos a toda la Lista de Crackslatinos. Apuromafo CLS

