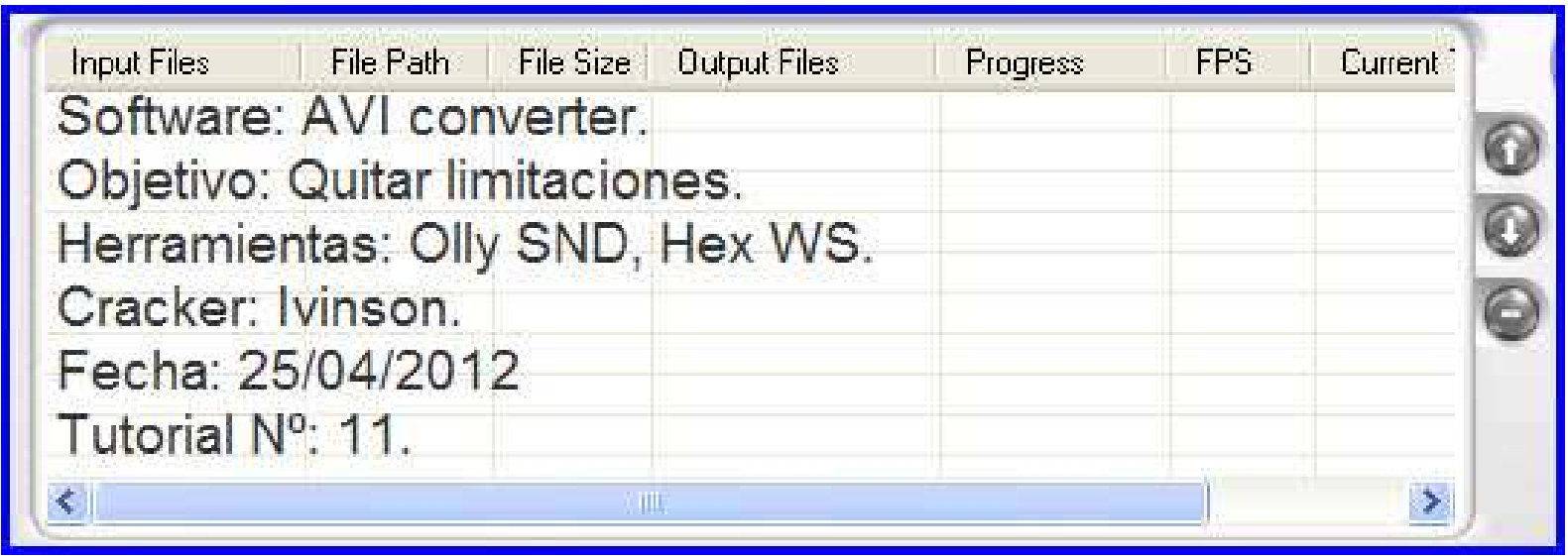
.-<Iv!n$on - Ing. R3v3rS!v0>-.

CLS T3aM-No CoMp3t3Nc3



Download:

http://www.mediafire.com/?xaflace0z7t4quc

Lo analizamos con RDG.

Me imagino que Alexei hizo este packer cuando era un newbie. ☺

Opciones para desempacarlo:

a) Técnica PUSHAD-POPAD
   Ver tuto:
   http://ricardonarvaja.info/WEB/CURSO%20NUEVO/TEORIAS%20NUMERADAS/1301-1400/1328-AudioCutter-%20Mi%20primer%20tuto%20para%20CLS-By%20Ivinson.pdf

b) Usando el siguiente Script hecho por SHaG te dejará en el OEP y con el plugin OllyDump dejando la casilla Rebuild Import queda listo.

```
// Script for OllyScript plugin by SHaG - http://ollyscript.apsvans.com
find eip, #68000000#
go $RESULT
sti
sti
cmt eip,"Estás en el OEP"
msgyn "¿Quieres analizar ahora?"
cmp $RESULT,0
je cancel
an eip
cancel:
ret

// [BACK]
```

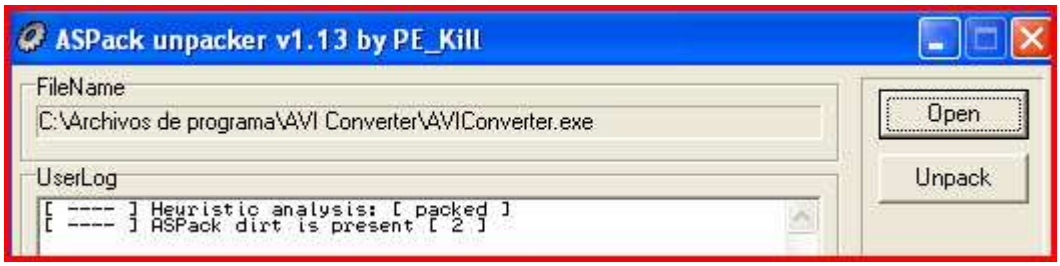
c) Usando FUU. 

http://code.google.com/p/fuu/downloads/detail?name=FUUv0.1.1b.exe&can=2&q

Y luego le damos al botón:

d) Y por último, ASPack unpacker por PE_Kill.

http://www.mediafire.com/?s0u1ub7d3rwg76v



Cree que tienen suficientes formas de desempacar Aspack 2.12.

Que comience la fiesta

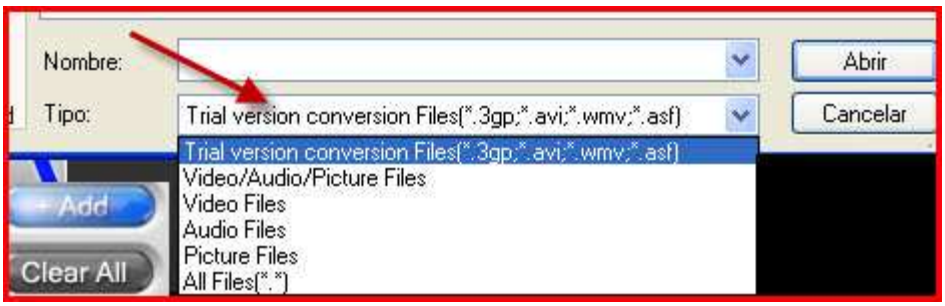
Abramos el software fuera de Olly para ver por donde atacar.

UnRegistered. Primera pavada.

Y luego nos muestra una nag recordándonos que nos quedan 6 días.

También vemos los límites de formatos para la versión Trial. Denle al botón +ADD/Agregar.

Dice **Trial version conversion Files.** Esta String nos servirá a futuro.



Seleccionenos All Files(*.*) y carguemos una imagen .jpg, por ejemplo.

Dice que si no compramos la versión full, solo podrá trabajar con los formatos 3gp, AVI, WMV y ASF.

Lo compraré con mi tarjeta de crédito **Olly**. ☺

Entonces, ya tenemos otra String importante.

"**Trial versión can only convert"Try Converter Files…**"

Ordenemos las Strings para trabajar más cómodos.

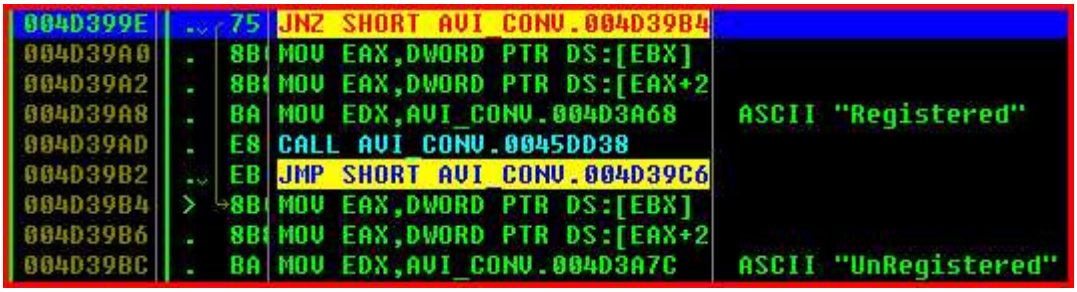
1) **Unregistered.**
2) **Trial version conversion Files.**
3) **Trial version can only convert**

Olly in Action

Ahora, sí. Lo abrimos en Olly y buscaremos la primera String haciendo click derecho **Search for all referenced text strings**.

```
004D39A8 | MOV EDX,AVI_CONV.004D3A68 | ASCII "Registered"
004D39BC | MOV EDX,AVI_CONV.004D3A7C | ASCII "UnRegistered"
```

Damos doble clic en **4D39BC**. Más fácil que pelar una mandarina.



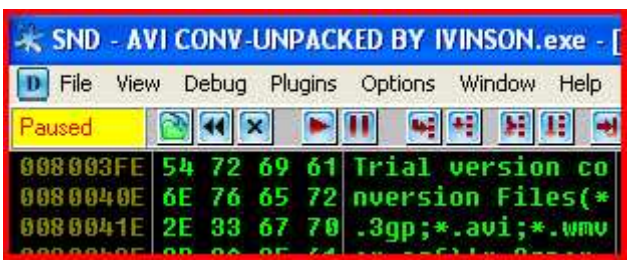
Si el salto JNZ se ejecuta, nos mostrará "Unregistered" en la primera Splash Screen al iniciar el programa. NOPearemos ese salto y ya resolveríamos un problema. Vayan guardando los cambios.

Busquemos la String 2.

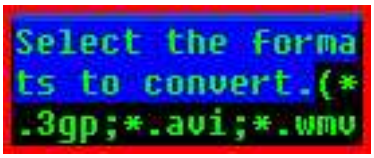
Vamos a "M" en Olly.

CTRL+B y escribimos:

Caeremos aquí:

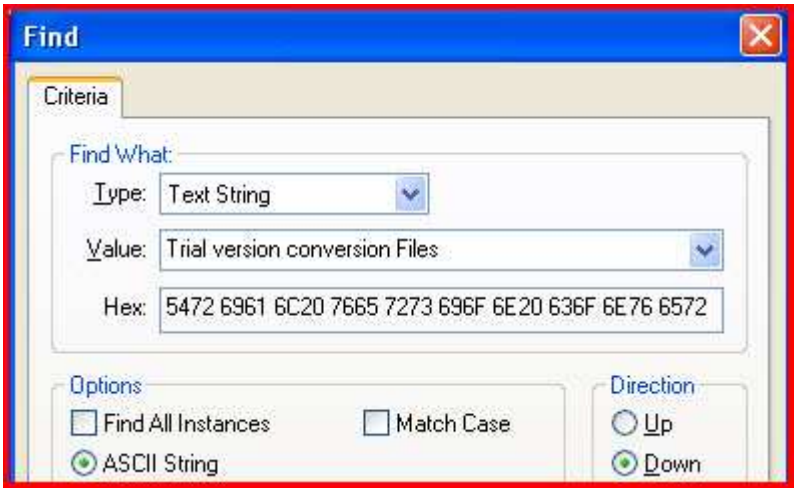


Solo motivos de estética seleccionamos esos bytes, damos Enter y le pondremos algo así:

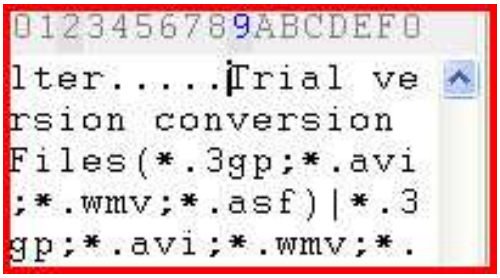


No se guardarán los cambios porque esa String está en otra sección del ejecutable **00800000**.

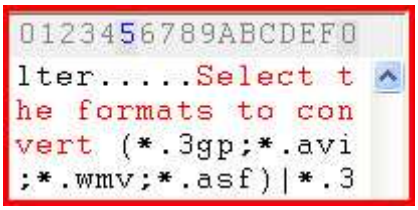
Hagámoslo con un editor hexadecimal como Hex WorkShop.



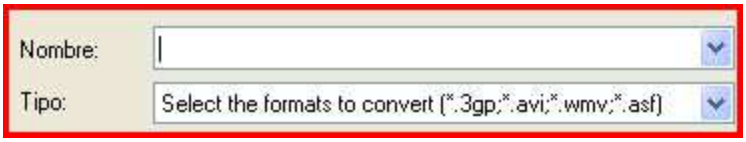
Al aceptar, caemos aquí:



Y lo editamos así:



Guardemos a ver y cerremos Hex WS. Ejecutemos AVI converter y démosle al botón ADD.



Se ve más serio. ¿Verdad?

Ahora, la String 3.

Trial version can only convert

Volvámoslo a cargar en Olly. Clic derecho **Search for all referenced text strings**.

Y caemos en un sitio interesante.

```
004D0D2F  MOV EDX,AVI_CONV.004D0F50  ASCII "Your 7-DAY Trial Period Has Expired! Register full version now?"
004D0D55  PUSH AVI_CONV.004D0F90     ASCII "http://www.avi-converter.com-video-converter.com"
004D0DD1  MOV EDX,AVI_CONV.004D0F38  ASCII "AVI Converter"
004D0DE8  MOV EDX,AVI_CONV.004D0FCC  ASCII "Trial version can only convert "Try Converter Files(3GP,AVI,WMV,A
```

Vaya, vaya. En la primera línea vemos la String más importante. La de expiración.

Aseguremos las dos direcciones colocándoles un BP con F2.

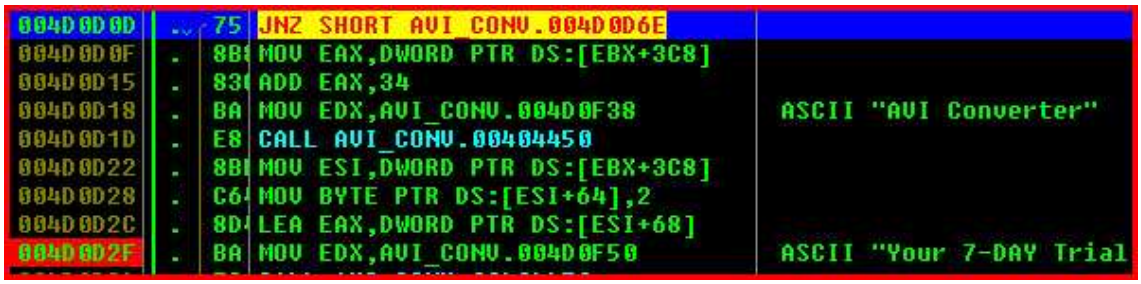
Vamos despacio. Démosle doble clic a la segunda.

Trial version can only convert que es la que estábamos buscando, ¿no? Después nos encargamos de la primera.

Cambiemos es JE por JMP y tendremos otra restricción eliminada.

Ahora, sin perder más tiempo iremos a revisar la parte de expiración.

Solo subimos un poco.



Igual que la anterior. JNZ por JMP y no vencerá nunca.

Guardemos todos los cambios. Copy to executable/All modifications/Copy all/Save file.

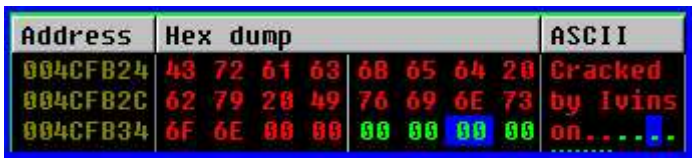
Analicemos esta parte:

Busquemos esa String. Clic derecho **Search for all referenced text strings**.

UnRegistered (

Le ponemos un BP con F2 y damos doble clic.

Demos clic derecho Follow in Dump immediate constant y modifiquémosla.



Seleccionamos los bytes modificados. Clic derecho Copy top executable file/Save file.

Le estamos haciendo latonería y pintura a este software.

Eliminando la nag

Buscaremos donde se crea la siguiente nag. La pondré completa.

Reiniciemos y demos F9. Cuando pare en el BP 4CFA9C que fue donde puse Cracked by Ivinson. Empecemos a trazar con F8 hasta que lleguemos a una CALL ejecuta el programa.

Ésta es 4D39EB. Le ponemos un BP y reiniciamos Olly. F9 hasta que lleguemos de nuevo a esa CALL para trazar con F7. Caemos aquí:

Entramos con F7 en esa CALL y luego seguimos con F8 hasta llegar a la CALL causante de la nag.

¿Cómo llegue a la conclusión de que esa era la CALL?

Si entramos con F7 vemos que es una pequeña rutina. Y si la trazamos con F8, comienza a formarse.

Así que, NOPeémosla y guardemos los cambios.

```
004D1216    90    NOP                          ;nag
004D1217    90    NOP
004D1218    90    NOP
004D1219    90    NOP
004D121A    90    NOP
004D121B  .  33(  XOR EAX,EAX
```

Aún queda el botón de comprar.

Borremos todos los BP.

Si le damos clic al botón Buy Now, abre la página:

http://www.avi-converter.com-video-converter.com

Busquemos esa String en Olly, y aparece varias veces.
Pongámosle BP en las siguientes direcciones:

004CE39D
004CE4B1
004D0D55
004D0E0E
004D1B31
004D1BF1
004D32FD

Al dar F9, caemos en el sitio caliente.

```
004D1BE5  .  C3  RETN
004D1BE6     8B  MOV EAX,EAX
004D1BE8  .  53  PUSH EBX
004D1BE9  .  8B  MOV EBX,EAX
004D1BEB  .  6A  PUSH 1
004D1BED  .  6A  PUSH 0
004D1BEF  .  6A  PUSH 0
004D1BF1  .  68  PUSH AVI_CONV.004D1C10      ASCII "http://
004D1BF6  .  68  PUSH AVI_CONV.004D1C44      ASCII "open"
004D1BFB  .  8B  MOV EAX,EBX
004D1BFD  .  E8  CALL AVI_CONV.00474BCC
004D1C02  .  E8  CALL AVI_CONV.004644F0
004D1C07  .  50  PUSH EAX                    hWnd
004D1C08  .  E8  CALL <JMP.&shell32.ShellExecuteA>  ShellExecuteA
004D1C0D  .  5B  POP EBX
004D1C0E  .  C3  RETN
```

Se me ocurre NOPear toda la rutina que está en el rectángulo azul para ponerle un MessageBox que diga Registrado o algo así.

NOPeemoslo y guardemos los cambios. Cerremos con ALT+F2 y cambiémosle el nombre al software por si acaso Olly crashea.

Al dar clic al botón Buy Now no hace nada. Perfecto.

El siguiente paso CTRL+N para ver si la API MessageBoxA está en el ejecutable, si no, la agregamos con LordPE.

Si está. ¡Que bueno!

Veamos en WinAPI32 para saber que parámetros necesitamos.

MessageBox

1. HWND hWnd, // handle de la ventana
2. LPCTSTR lpText, // Dirección del texto del MB.
3. LPCTSTR lpCaption, // Dirección del título del MB.
4. UINT uType // Estilo del MB.

Abramos el Crackme1 de CrueHead para verlo más claro.

Al momento de ensamblar en Olly, se hará de abajo hacia arriba.

Por ejemplo:

PUSH <4. UINT uType> // Estilo del MB.
PUSH <3. LPCTSTR lpCaption> // Dirección del título del MB.
PUSH <2. LPCTSTR lpText> // Dirección del texto del MB.
PUSH <1. HWND hWnd> // Handle de la ventana

Nos faltaría obtener el handle. Eso lo haremos con la API FindWindow.

Veamos los parámetros en WinAPI.

FindWindow

1. LPCTSTR lpClassName, // Puntero al nombre de la clase.
2. LPCTSTR lpWindowName // Puntero al nombre de la ventana.

También, la tiene el ejecutable. ☺

En Olly ensamblaríamos así:

PUSH <XXXXXXXX> ; // Puntero al nombre de la ventana.
PUSH 0 ; Cero porque no buscaremos la clase.

Para buscar el título de la ventana, pondremos un BP en CreateWindowExA y entre los nombres más llamativos es Welcome…

Veamos el botón de ventanas “W” y clic derecho Actualize.

Podemos probar con ese o si no, con AVI Converter. (Este fue el que funcionó)

Creemos un nueva sección con Topo.

A mi me la creó en 0B6600. Lo cargamos en Olly y vamos a hacer las pruebas. Busquemos la parte que nopeamos. La rutina del botón Buy Now y ensamblemos un JMP al injerto en 4D1BEF. Ponle un BP.

Vamos a la dirección del injerto dándole Enter arriba de ese JMP. Ensamblen esto así como lo hice yo.

Como ven en la imagen anterior. Ensamblé un PUSHAD para guardar los registros, luego PUSH 0B66371. Yo elegí esa dirección del injerto ustedes elijan la que quieran y la buscan en el Dump en donde guardarán la String AVI Converter. Esa String debe terminar en 0. Luego PUSH 0 y por último CALL 00406F2C.

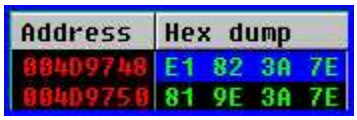
O sea:

PUSHAD
PUSH 0B66371 ;Dirección del nombre de la ventana.
PUSH 0
CALL 0406F2C

La CALL 0406F2C es porque allí está el salto indirecto a la API FindWindow.

Para llegar allí, CTRL+N y le damos doble clic al nombre de la API FindWindow.

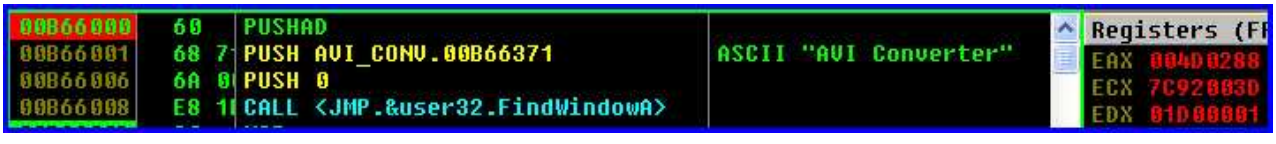
Caemos en el Dump en esa dirección.



Seleccionamos sus bytes y le damos CTRL+R.

Ahí está. Así buscaremos la dirección de MessageBoxA. ☺
Habíamos quedado aquí.

Tenemos un BP en 4D1BEF JMP 0B66000. Demos F9 y luego, tracemos con F8 o F7 y al pasar la CALL de FindWindow, veremos el handle de la ventana en EAX== 04D0288.



Lo comparamos con el que está en “W”.

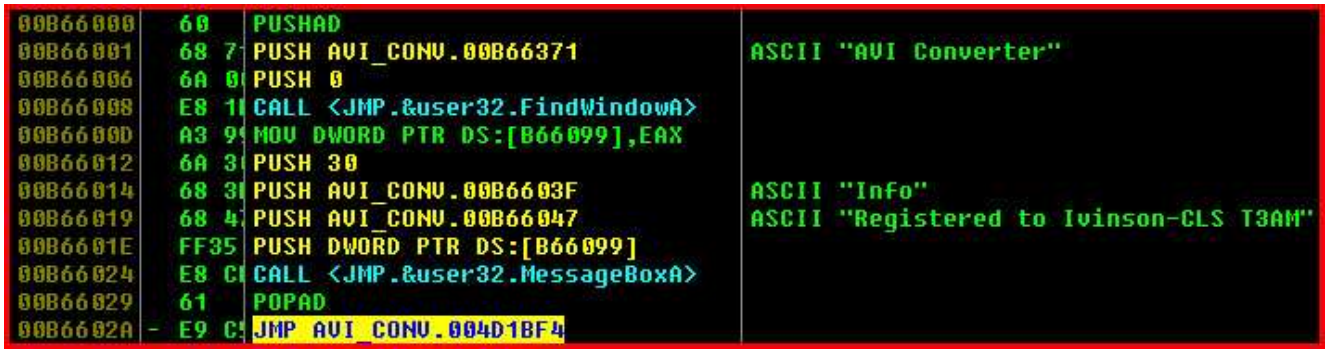
Es el mismo. Vamos bien. ☺

Sigamos ensamblando. Ya que, tenemos el Handle en EAX, es el momento perfecto para guardarlo donde queramos. Siempre y cuando sea dentro del injerto. Yo elegí esta dirección 00B66099.

Por lo que, la siguiente instrucción sería:

MOV [0B66099], EAX

Vean la imagen del injerto final.



Si le damos al botón “Buy Now” veremos nuestra MessageBox.

Lo que si no supe hacer fue cambiarle el nombre al botón “Buy Now” por About. Si alguien sabe, por favor, notificármelo. ☺

Gracias por leer.
Contacto ipadilla63@gmail.com