CRACKING

WOW Sinastry

Escrito por: tHOBAS

DESCARGO LEGAL

DOCUMENTO ESCRiTO PARA FiNES DE EDUCACiON/iNVESTiGACION

[Proyección]

Aprender un poco mas de la generación de seriales

[E/l a realizar]

Encontrar el numero de serie para registrarnos

[WOW Sinastry]

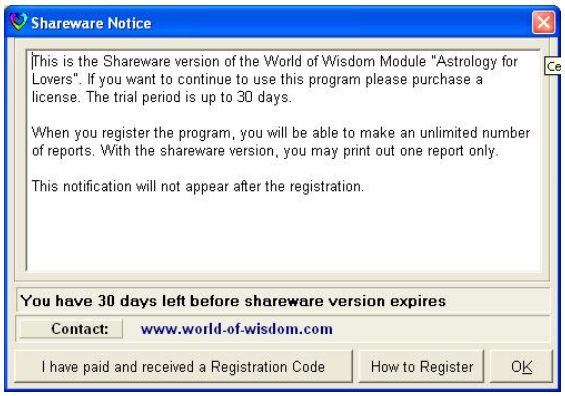
The WOW synastry program lets you see how a relationship functions, the energy between the two people involved, the areas which may be problematic and the areas where each partner is able to help and support the other.

[Url de Descarga]

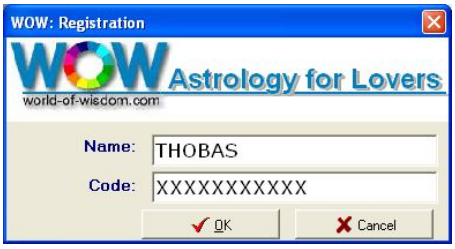
http://world-of-wisdom.com

[Manos a la Obra]

Cuando ejecutamos el programa nos muestra una ventana que nos pide registrarnos

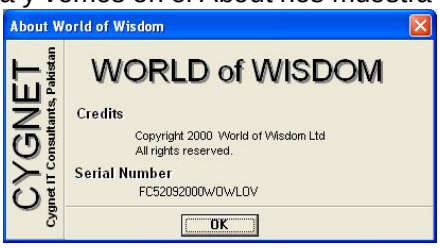


Intentaremos registrarnos dándole Click en el Boton : I have paid and received a Registration code. Se nos muestra una ventana donde nos pide que ingresemos nuestros datos

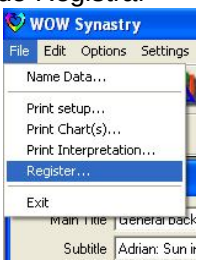


Al darle en el botón OK se nos muestra una mensaje de que los datos son incorrectos

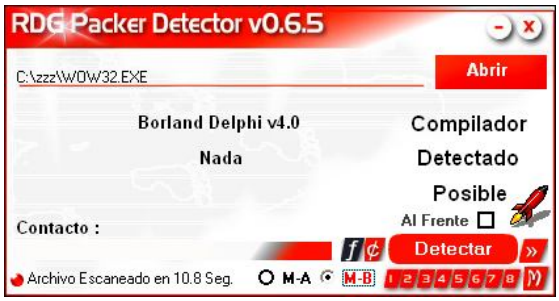
Si ingresamos al programa y vemos en el About nos muestra que:



Y en el menú archivo esta el botón de Registrar



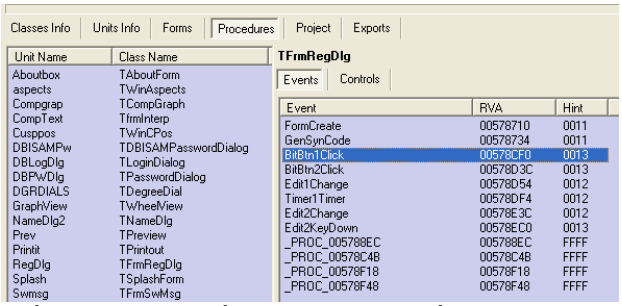
Solo nos faltaría saber si el programa esta empaquetado o no y saber en que lenguaje fue hecho para empezar. Para eso lo analizaremos con el RDG. El cual nos muestra la siguiente información



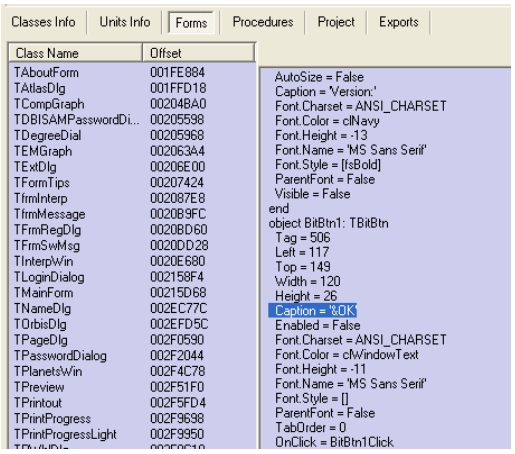
Bueno el programa esta hecho en Delphi y para suerte nuestra no esta empaquetado.

Como no me va bien aun con Delphi, haremos uso del DeDe para averiguar la dirección exacta del botón de OK.

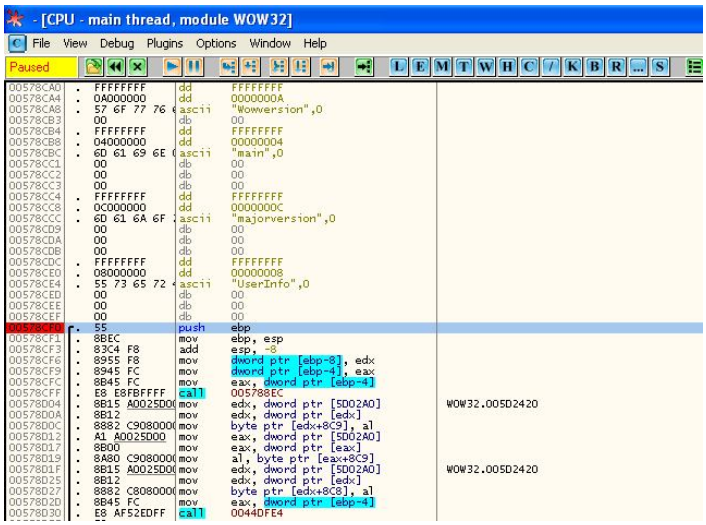
El DeDe nos da la siguiente información.



Ahí esta la dirección de nuestro botón OK, en la dirección 00578CF0. Ahora bien como sabemos que es el botón de Ok?
Bueno el DeDe nos lo aclara bien

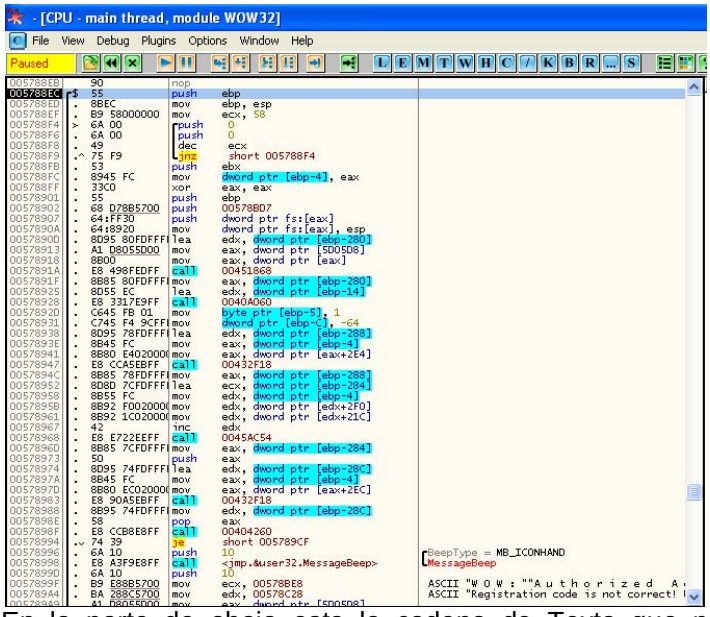


Bueno despejada nuestras dudas. Abrimos nuestro OllyDbg, cargamos el ejecutable y CTRLG+G y colocamos la dirección 00578cf0 y llegamos hasta aquí



Colocamos un BP (F2)en esa Direccion y ejecutamos el programa(F9); ingresamos nuestros datos y el OllyDbg parara en el BP que pusimos traceamos un poco (F8)hasta llegar al primer CALL[dirección 00578CFF], ya que si Apretamos una vez mas F8, nos muestra el mensaje de que nuestros datos son incorrectos. Quiere decir que en esa CALL[00578cff] esta el meollo de donde se genera el serial y compara el serial Correcto con el Falso.

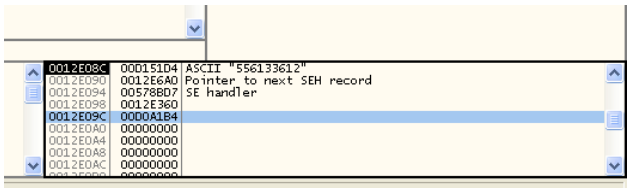
Reiniciamos todos (Ctrl+f2) realizamos de nuevo todo el procedimiento hasta llegar a la dirección 00578CFF y esta vez en vez de Apretar F8 lo haremos con el F7 y vemos algo que nos indica de que vamos por buen camino:

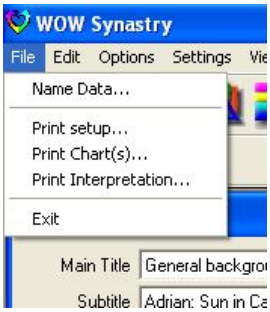


En la parte de abajo esta la cadena de Texto que nos dice que el código para registrarnos no es correcto. Traceamos otra vez con F8 pero si nos fijamos en esta parte :

```
005788EC  /$  55                    push    ebp
005788ED  |.  8BEC                  mov     ebp, esp
005788EF  |.  B9 58000000    mov     ecx, 58
005788F4  |>  6A 00                 /push    0
005788F6  |.  6A 00                 |push    0
005788F8  |.  49                    |dec     ecx
005788F9  |.^ 75 F9                 \jnz     short 005788F4
005788FB  |.  53                    push    ebx
```

Existe un bucle que se va a repetir 58h veces (88 veces en decimal) hasta que ecx sea 0. Como no nos pasaremos un buen rato traceando hasta que ECX valga 0. Entonces colocare un BP en la dirección 005788FB y apretamos F9 para que se detenga en el BP. Traceamos hasta el CALL de la dirección 00578983 y vemos en la ventana del Stack nuestro numero de serie correcto





Para los que quieren ver como se genera el serial, esta se realiza en el CALL de la dirección 00578968. Lo que realiza el programa es que juega con nuestro nombre ingresado hasta lograr un resultado de 8 digitos, por ejemplo en mi caso seria : 87307322 de ahí coge el resultado y realiza operación cogiendo el ultimo digito primero y terminando con el primer digito del resultado, hasta lograr nuestro numero de serie correcto que en este caso seria : 55613612

Y como para tener un poco mas de ayuda el serial correcto siempre será de 9 digitos, sea cual fuese el nombre ingresado

[Aclaracion]

Perdonen, se que lo hice extenso pero es la forma como lo hice yo

[pF del autor]

Saludos a todo rVLCN; CracksLatinoS, Arc; y a ti por tomarte tu tiempo para leer este tutorial

[El autor puede ser contactado]

eMail: tHOBAS@gmail.com

www: http://RVLCN.com
http://RVLCNsecurity.com
http://rvlcn.iespana.es
http://beam.to/RVLCN - Lista
http://RVLCNsecurity.com/foro - Foro

Noviembre-2008

-------/ REVOLUCiON /-------