CRACKING

Digy Tarot v8.1.7

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

[Digy Tarot]

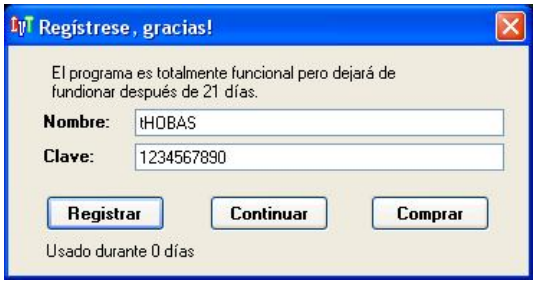
Para los que no tienen suficientes cargas positivas, amuletos de la suerte o datos cargados con significación mágica o astrológica, ya pueden estar tranquilos, ya que con DigyTarot podremos dar significado a cualquier número.

[Url de Descarga]

http://josejoa.net/digytarot_sample/

[Manos a la Obra]

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



Al darle en el boton Registrar nos muestra un mensaje de que hemos errado al ingresar los datos

Una aclaración si ingresamos un nombre con una longitud menor a 6 caracteres nos muestra un mensaje que debemos ingresar por lo menos un nombre con 6 caracteres

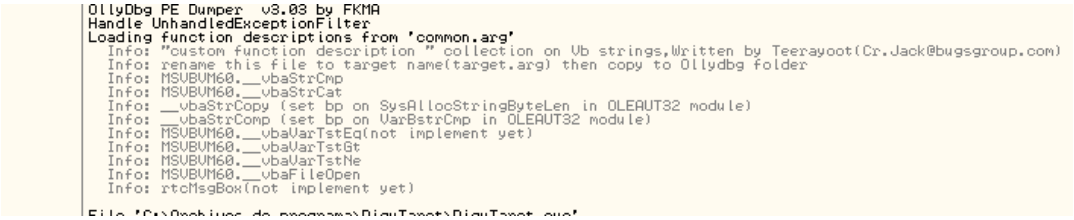
Bueno ya tenemos suficientes datos para saber por donde atacar a este programa.

Como siempre analizaremos el programa para saber en que lenguaje esta hecho y si es que esta empaquetado o no.

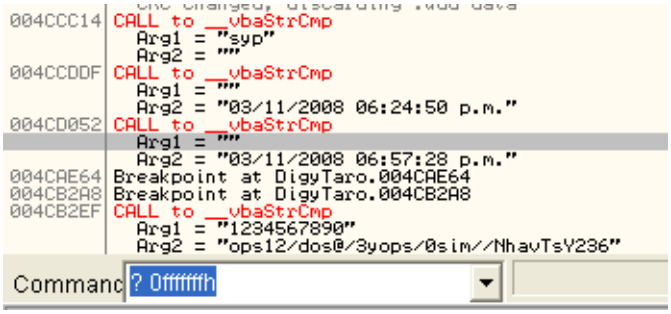
Como esta hecho en Visual Basic, lo resolveré de dos maneras diferentes,

[Primera Forma]

Haremos uso del archivo common.arg, esta en las teorías de Ricardo, Teoria 116. Ejecuto el OllyDbg y verificamos que el archivo Common.arg esta completamente cargado



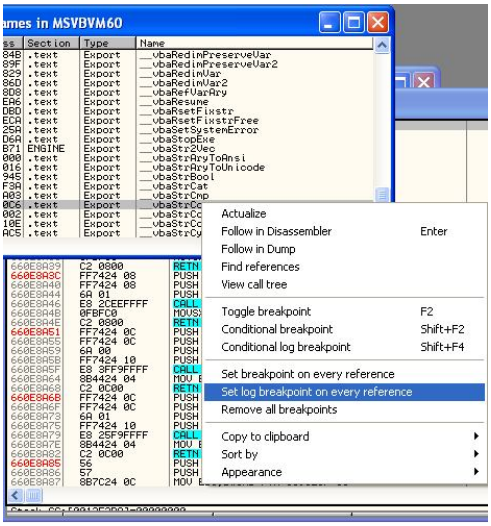
Realizamos los mismos pasos que Ricardo explico detallamente en la Teoria 116. Vemos nuestro numero de serie correcto en el Log de OllyDbg



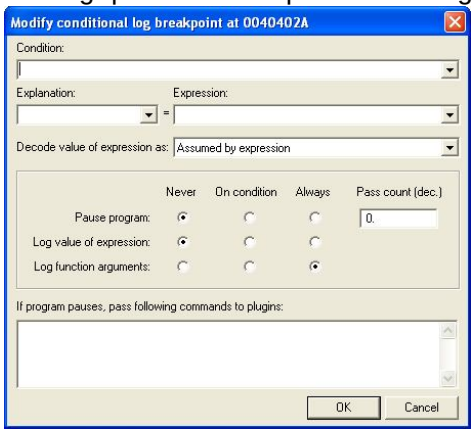
[Segunda Forma]

Haremos uso de las APIS que usa el VB en este caso pondremos un BP en _VbaStrCmp, como se darán cuenta Compara cadenas de texto [Str = String ; Cmp = Compare]

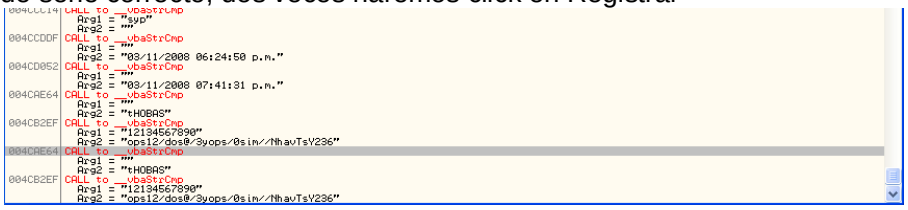
En el OllyDbg cargado con el ejecutable presionamos Ctrl +N y buscamos la API _VbaStrCmp, colocamos un Set Log Breakpoint on every reference



Modificamos los valores del Log que nos debe quedar de la siguiente forma



Ejecutamos el Programa F9 ingresamos los datos y vemos en el Log nuestro numero de serie correcto, dos veces haremos click en Registrar



Porque dos veces, simple por que en la primera interrupción hace la comparación de nuestro nombre y calcula nuestro numero de serie correcto y en la segunda interrupción compara nuestro numero de serie correcto con el erróneo que ingresamos.

Si alguien quiere ver como se realiza el calculo de nuestro numero de serie, lo que hace es convertir nuestro nombre ingresado a minúsculas de ahí realiza operaciones y los concatena con la una cadena fija que en este caso es :

ops12/dos@/3yops/0sim//NhavTsY

Lo unico que varia son los 3 ultimos digitos que salen de las operaciones de nuestro nombre ingresado

[Aclaracion]
Perdonen, se que lo hice extenso pero quería mostrarles como lo hice yo.

[pF del autor]

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

[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 /-------