TUTORIAL #3Reverseando software VB con Ollydbg +VBdecompiler

BY NECROX!4 REV3RSER

Programa:	**LuloWin NG v. 11**
Protección:	**Límite de Tiempo – Opciones Ocultas y otros**
Lenguaje:	**Visual Basic 6**
Dificultad:	**Principiante**
Objetivos:	**Parchear + eliminar restricción de tiempo**

INTRODUCCION

Saludos a todos los integrantes de la lista CracksLatinos aunque no soy muy autodidacta, este es mi tutorial Nro. 3 de la lista y a la vez el primero referente al Crackeo de una aplicación de “Visual Basic 6.0” utilizando herramientas actuales,el motivo de este estudio a la aplicación era ver la forma de protección que utiliza este programa comercial y como atacarla.

PRESENTACION

Lulowin NG:

Sistema para controlar efectivamente los costos en el área construcción.

Este sistema esta orientado principalmente a las compañías e instituciones dedicadas a las actividades de construcción y campos afines, ya que soporta los procesos técnicos y administrativos relacionados con la administración de contratos.

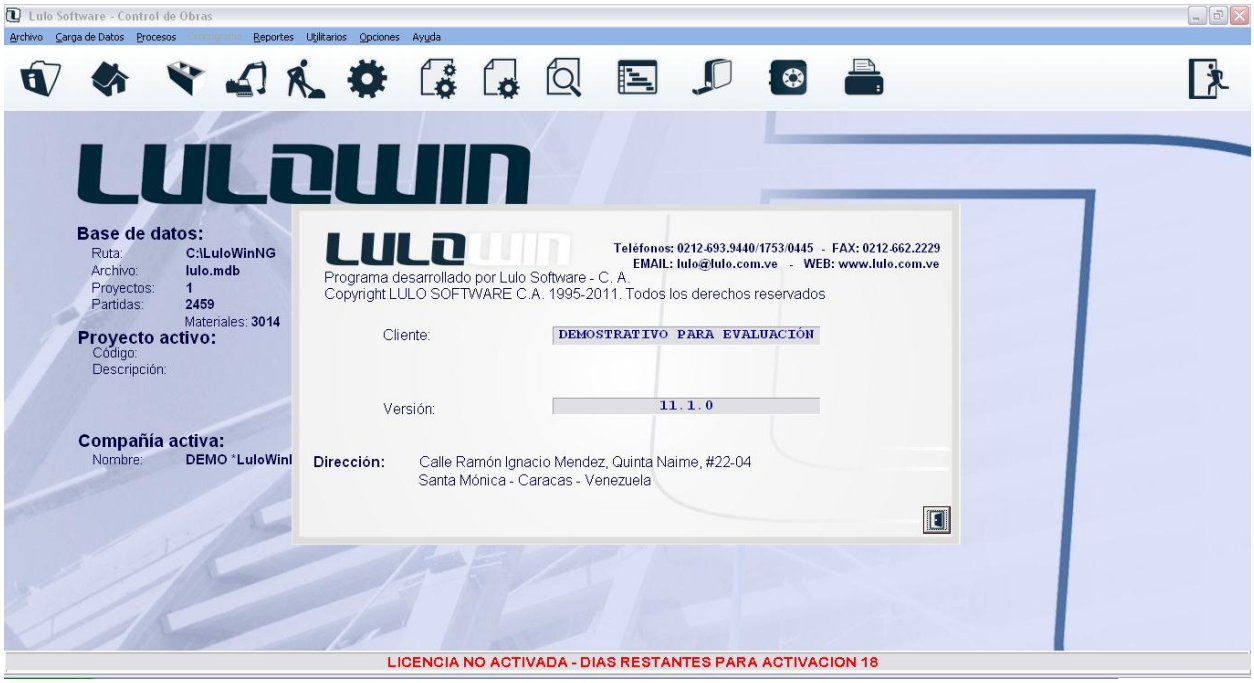
FASE I: ANALISIS DE LA APLICACION.

Utilizare RGD Packer Detector para anilizar este ejecutable, se puede apreciar la victima es un Visual Basic 6.0 , no contiene ningún tipo de packer asi que nos facilita un poco la tarea.

:

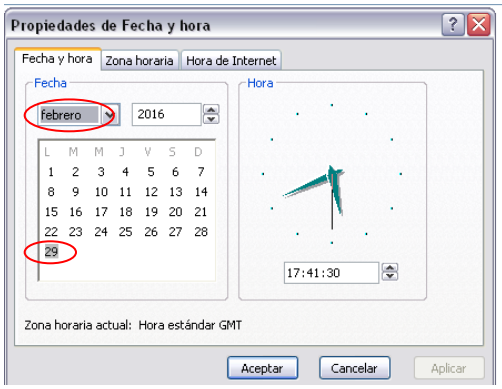
FASE II: ELIMINAR RESTRICCIÓN DE TIEMPO DE EJECUCIÓN.

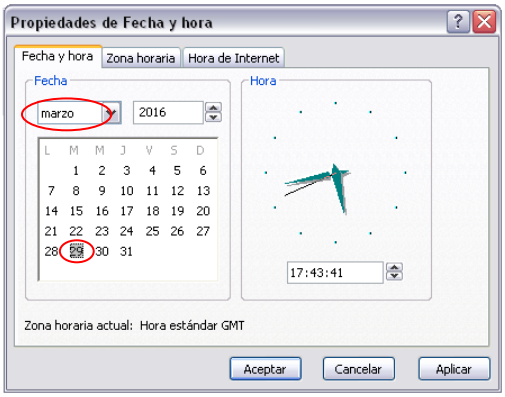
Para empezar en esta imagen se puede apreciar el lulowin ng con una string que dice licencia no activada a ósea tenemos que “Comprar el programa”, jajajaja



Pero como yo soy escaso de recursos económicos y lo que me interesa es aprender pues vamos a probar unos truquitos aprendidos de uno de los integrantes de la lista el amigo neutrino de aca de mi país.

Empecemos lo primero que hay que hacer es que caduque el programa para poder reversarlo ,que muestre la típica "**Nag**" de expiración a continuación, para esto necesitamos adelantar la fecha Windows para eso vamos a la barra de tareas y nos dirijimos hacia donde marca la hora..

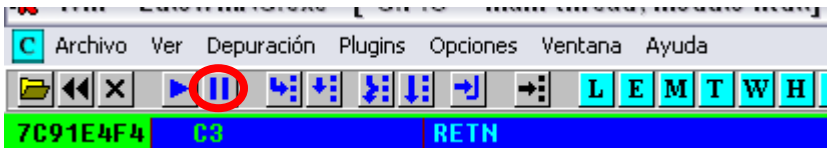




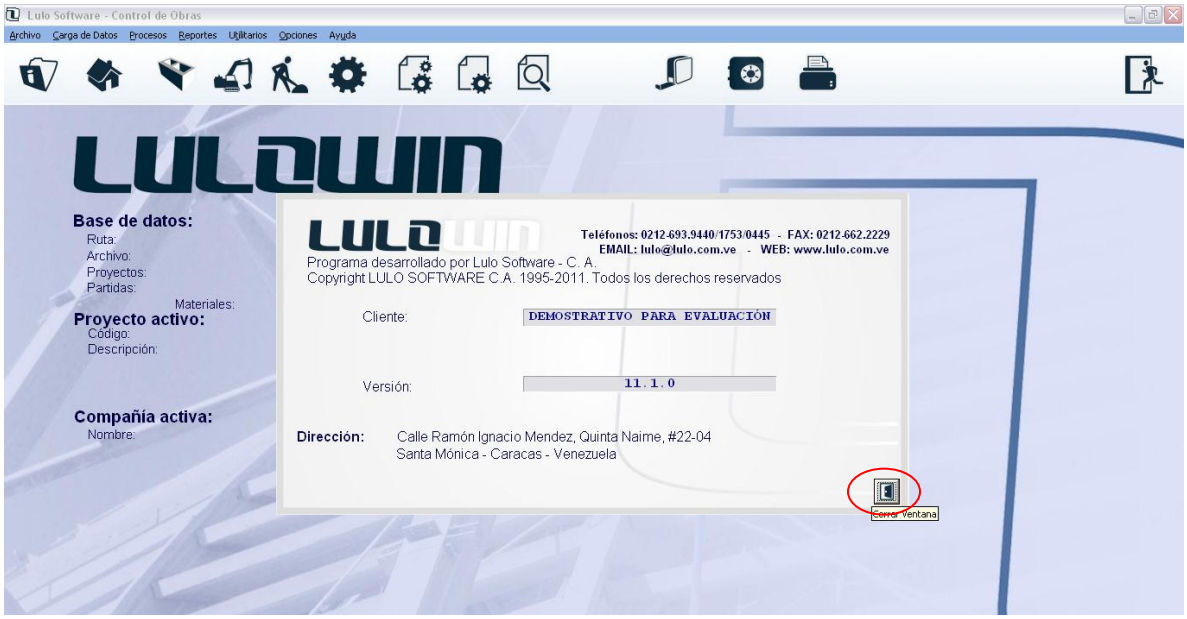
Una vez adelantada la fecha saldrá la NAG de Tiempo Expirado.

Asi que aquí empiezo con unas técnicas de romper en procedimientos en VB 6 aprendida por el amigo neutrino.

1) Lo primero que hacemos cuando sale esta tipica nag es pausar la ejecución de programa con F12 o con el botón pause.



2) Luego ejecutamos el retn hasta el código de usuario lo podemos hacer desde el menú o precionamos Alt + F9 y volveremos a al programa una ves demos click en la boton puerta.



Vamos a romper aquí:

Vamos arriba hasta donde este el Push EBP colocamos un break point

Del mismo modo procedemos a reiniciar el Ollydbg Ctrl + F2 Y presionamos F9 para ejecutar el programa y una vez echo esto realizaremos lo siguiente.

Una vez que paro en el break point ,,vamos al stack a ver donde va a retornar asi que damos enter y automáticamente caemos en **03C0D08C**

Caemos Aquí

Vamos para arriba del código para ver el salto sospechoso que quita la expiracion.

Ahora vamos hacia la dirección donde esta el salto **03C0D081** y lo cambiamos por un (JMP SHORT 03C0D0A8) con esto qitamos la típica nag.

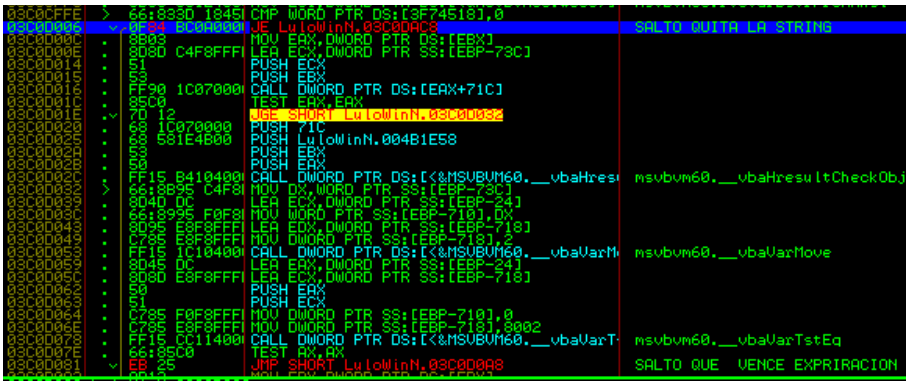
Habiendo echo esto guardamos los cambios hechos en el ejecutable ,abrimos el ejecutable que guardamos y veremos si es verdad.

Uff Expiración Vencida….

Ahora procederemos a eliminar la string de “LICENCIA NO ACTIVADA”

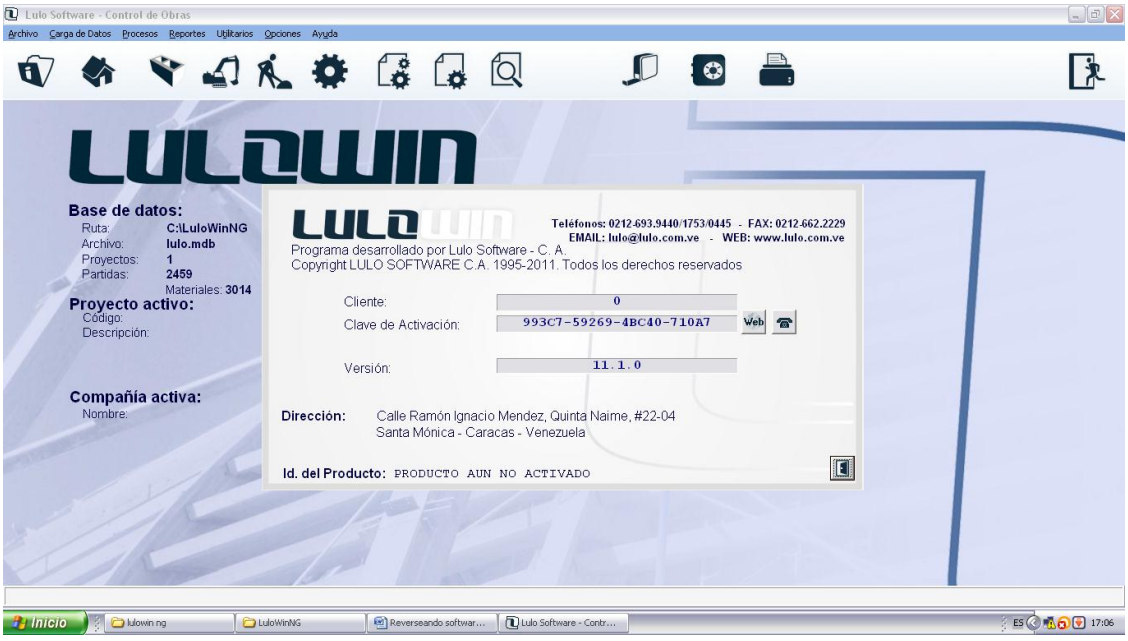
Mi intuición de cracker me dice que para eliminar la string tengo que ir arriba del anterior salto asi que subo hasta que encuentro este salto JNE 03C0D006 y lo revierto con JE 03C0D006 guardamos cambios echos al ejecutable y probamos.

Salto Revertido:



Demos RUN o F9 y pummm… desapareció la String de Licencia No Valida…


Lulo Software - Control de Obras
Archivo Carga de Datos Procesos Cronograma Reportes Utilitarios Opciones Ayuda
LULOWIN
NG EDICIÓN PROFESIONAL Versión: 11.1.0
Base de datos:
Ruta: C:\LuloWinNG
Archivo: lulo.mdb
Proyectos: 1
Partidas: 2459
Materiales: 3014 Equipos: 521 Mano de Obra: 311
Proyecto activo:
Código:
Descripción:
Compañía activa:
Nombre: DEMO *LuloWinNg - Control de Obras*
ES 11:14 p.m.

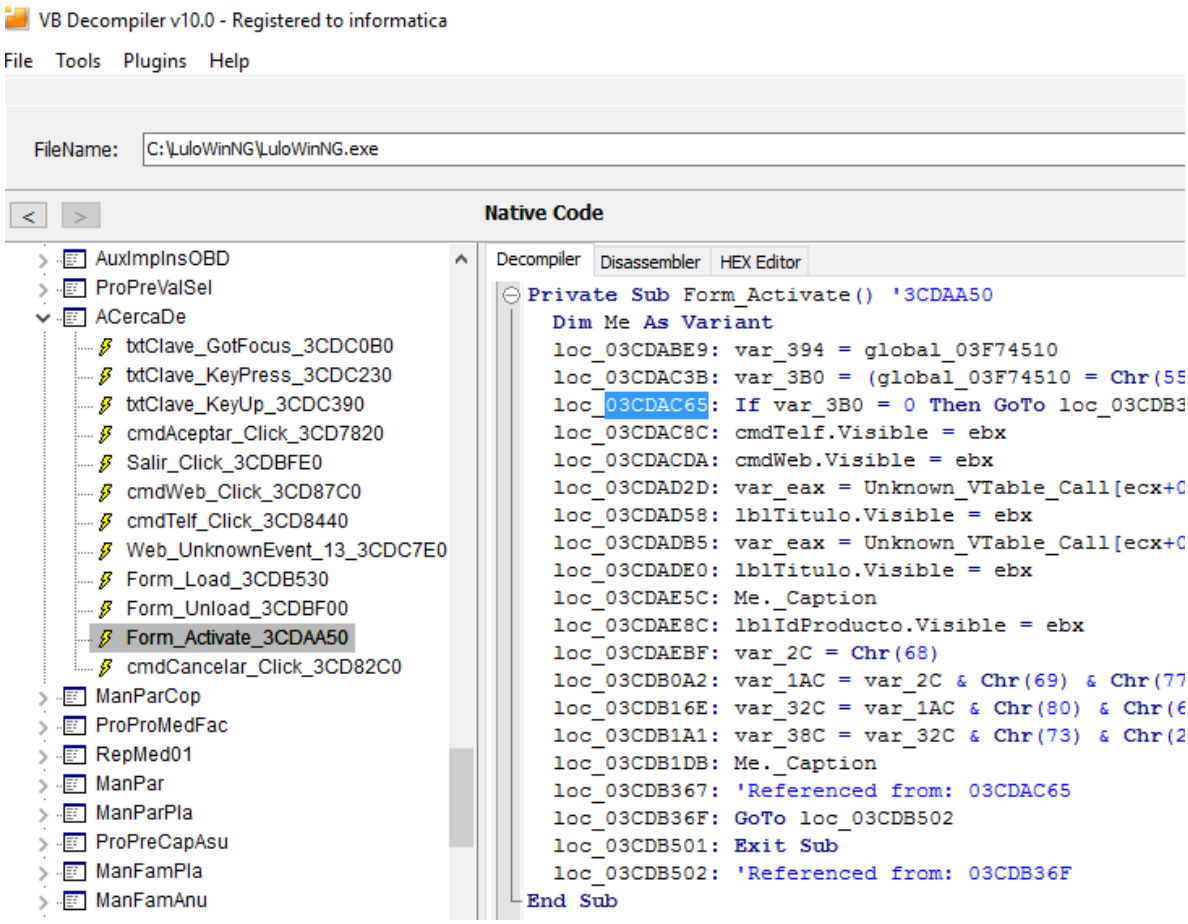

Lulo Software - Control de Obras
Archivo Carga de Datos Procesos Reportes Utilitarios Opciones Ayuda
LULOWIN
Base de datos:
Ruta: C:\LuloWinNG
Archivo: lulo.mdb
Proyectos: 1
Partidas: 2459
Materiales: 3014
Proyecto activo:
Código:
Descripción:
Compañía activa:
Nombre:
LULOWIN
Teléfonos: 0212-693.9440/1753/0445 - FAX: 0212-662.2229
EMAIL: lulo@lulo.com.ve - WEB: www.lulo.com.ve
Programa desarrollado por Lulo Software - C. A.
Copyright LULO SOFTWARE C.A. 1995-2011. Todos los derechos reservados
Cliente: 0
Clave de Activación: 993C7-59269-4BC40-710A7
Web
Versión: 11.1.0
Dirección: Calle Ramón Ignacio Mendez, Quinta Naime, #22-04
Santa Mónica - Caracas - Venezuela
Id. del Producto: PRODUCTO AUN NO ACTIVADO
Inicio
lulowin ng
LuloWinNG
Reverseando softwar...
Lulo Software - Contr...
ES 17:06

Manera Simple…..

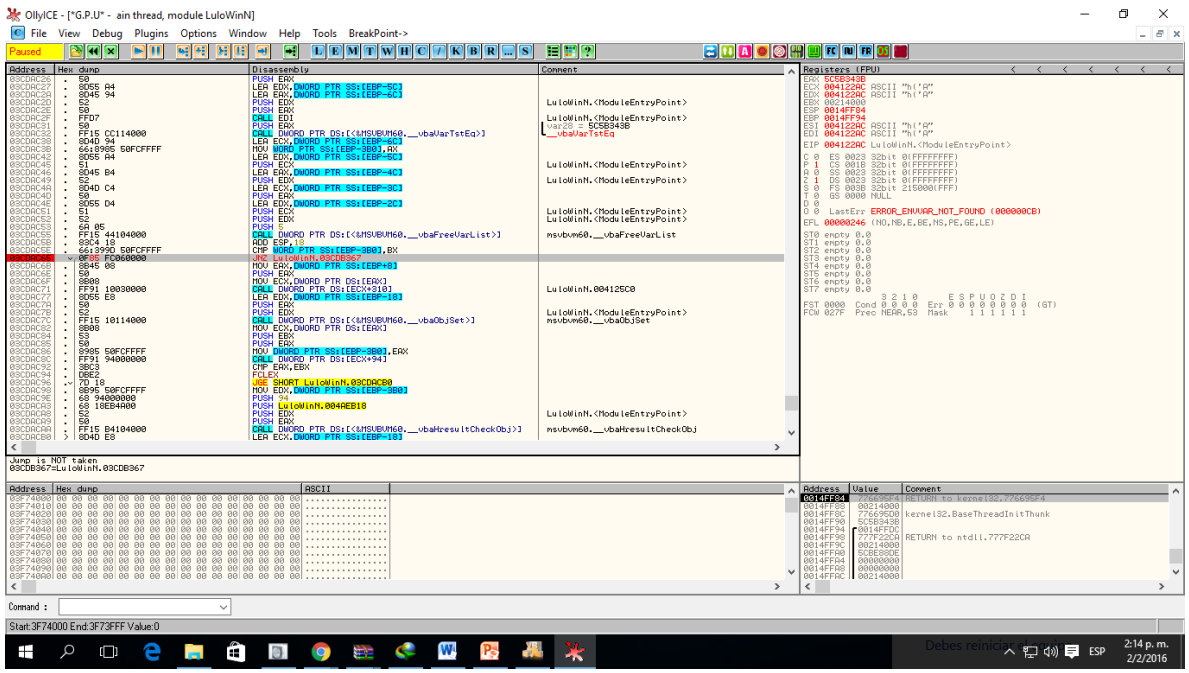
Aparecer las Opciones Ocultas de Activación (Ollydbg + Vb Decompiler 10)

Lo que hice para activar las opciones ocultas fue viendo los form con vbdecompiler v10

Me fui al menú -> Ayuda -> Acerca de.. por intuición y hay estaban las opciones en visible= false ,además de lo que ya me había el amigo neutrino en un hilo de CLS que había un modulo oculto me parecio que era asi lo cual tuve que descompilar el proyecto en una carpeta y revisar formulario por formulario hasta que di con el:



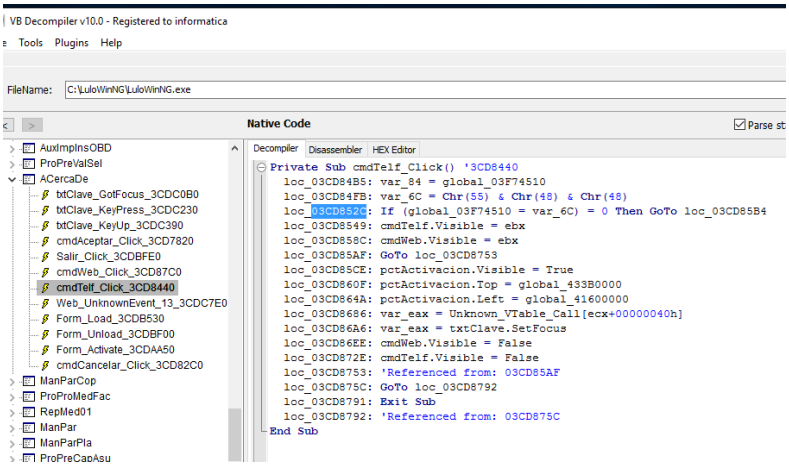
Me fui al offset 03CDAC65 cambie el je por jne y aparece los botones



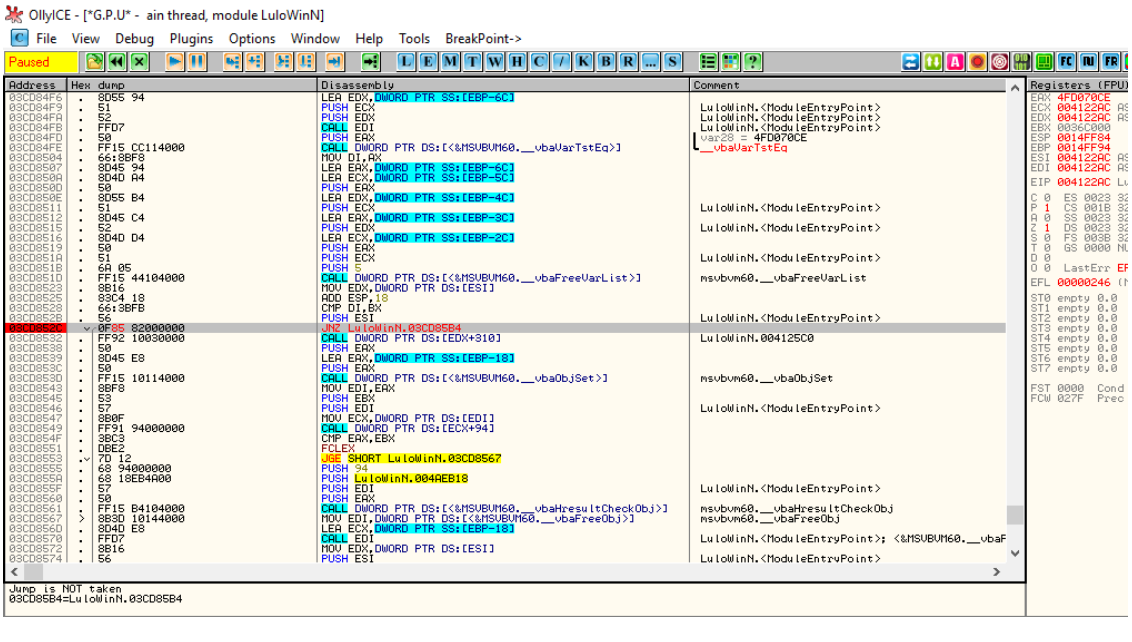
.

Pero al pulsarlo desaparecen

Algo me me dijo que eso estaba en el evento click de ambos



Me fui al offset 03CD852C cambie el je por jne y aparece los botones



Y asi mismo hice con la activación web en el offset 03CD8B90 cambie un je por un jne

Volaaaaa hay si la activo “PERO ES NECESARIO TENER INTERNET”

Les dejo como tarea como conseguir el serial valido para activar Lulowin NG

Gracias en especial al maestro Ricardo Narvaja por su biblia de introducción al cracking con Ollydbg ,a los amigos Neutrino, Ivinson, Apuromafo que siempre bombardeo con preguntas y ellos se toman la molestia de contestarlas sin ningún problema y sin menos preciar a nadie gracias a la familia CracksLatinoS