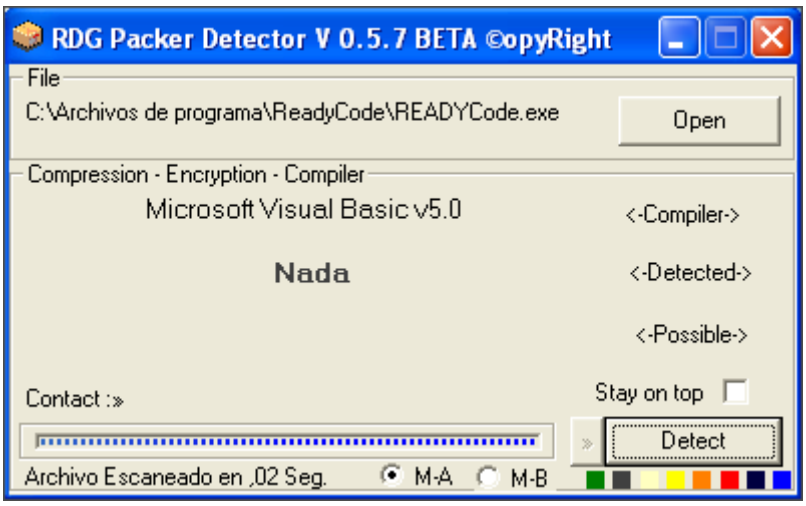
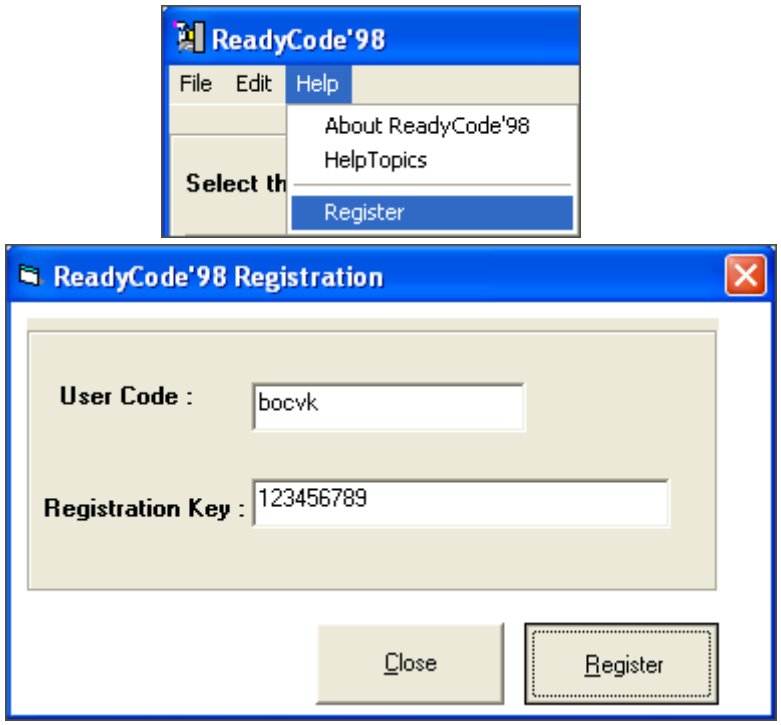
Ready Code'98

Instalamos el programa , luego tomamos a nuestra victima y la analizamos con el RDG. Para esto haremos click en Open y buscamos nuestro programa, luego haremos click en Abrir, y despu?s en Detect:



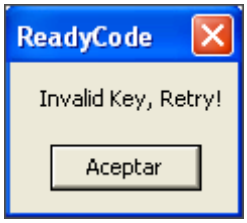
Como vemos el programa fu? programado en Visual Basic y no est? empacado, cosa que nos facilita el trabajo.
Para el VB se utiliza la herramienta VB Reformer para encontrar informacion que nos facilite las cosas en el Olly pero en este caso no la usaremos ya que nos vota error al tratar de abrirlo.

Ejecutamos el programa , y buscamos una pesta?a o boton para registrarnos , hacemos click y nos aparece otra ventana para poner algunos datos, llenemoslos :



Le damos al boton Register , y nos aparece el Chico Malo diciendonos que el key

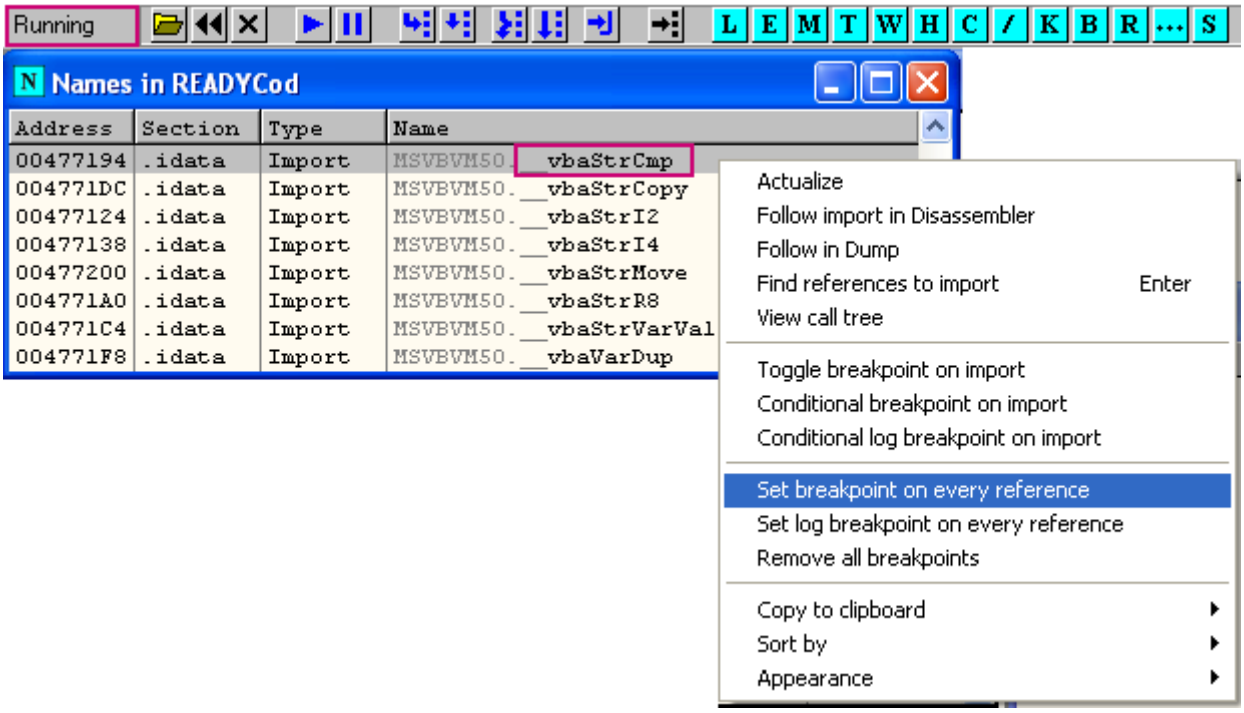
ingresado es incorrecta, en el caso de VB es poco usual trabajar con las strings debido a que se encuentran lejos de la parte del codigo donde se utiliza asi que no nos servira de nada copiarla pero por si acaso hay que tenerla de referencia :



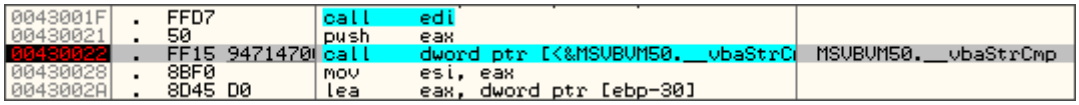
Abrimos el OllyDbg, y cargamos nuestro programa; en seguida presionamos CTRL+N para buscar en las APIs del programa, alguna que haga referencia a la manipulaci?n de strings o texto, y las mas concocidas en caso de que trabajemos con VB son todas las comienzan con "str" , aqui nosotros elegiremos una que compare (comparacion abreviado cmp) entonces buscamos la API "strcmp" o alguna parecida:

0047715C	.idata	Import	MSVBVM50.__vbaStrCat
00477194	.idata	Import	MSVBVM50.__vbaStrCmp
004771DC	.idata	Import	MSVBVM50.__vbaStrCopy
00477124	.idata	Import	MSVBVM50.__vbaStrI2
00477138	.idata	Import	MSVBVM50.__vbaStrI4
00477200	.idata	Import	MSVBVM50.__vbaStrMove
004771A0	.idata	Import	MSVBVM50.__vbaStrR8
004771C4	.idata	Import	MSVBVM50.__vbaStrVarVal

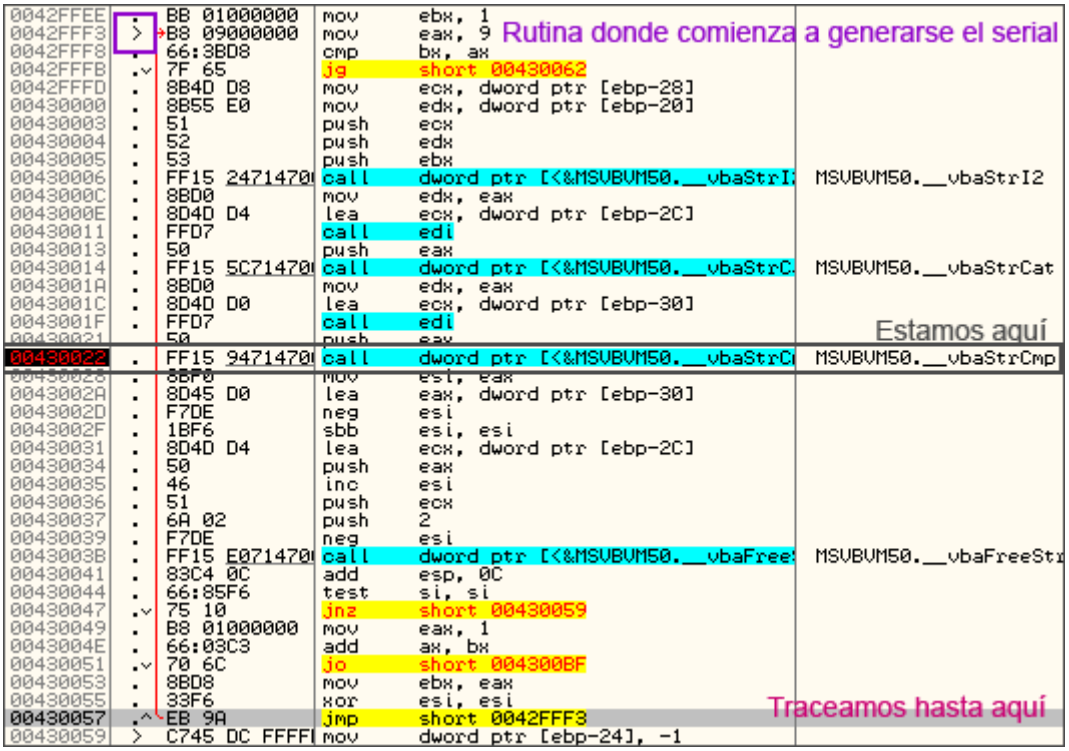
Ahora ejecutaremos el programa presionando la tecla F9 y llenamos los datos de la ventana de registro (sin presionar el boton Register), y luego le ponemos un BreakPoint a la API que encontramos haciendo anticlick en dicha Api y luego presionando click en "Set breakpoint on every reference" :



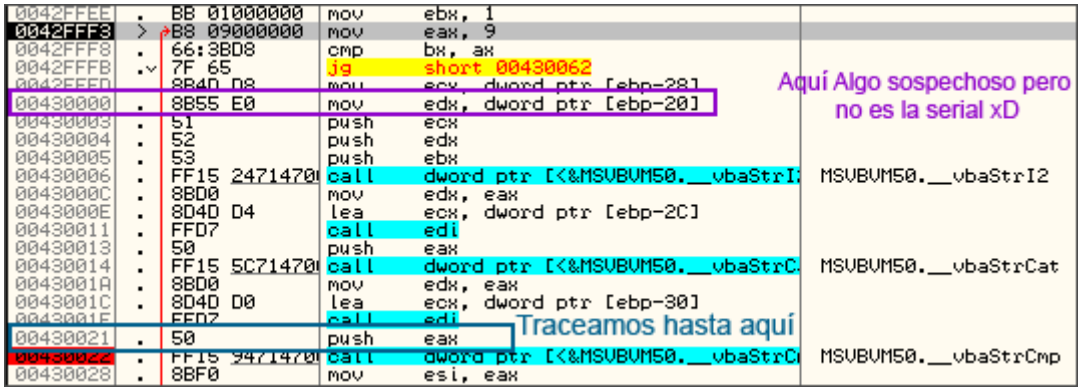
Ahora presionamos en el boton Register de la ventana de registro del programa y el OllyDbg rompe en la API :



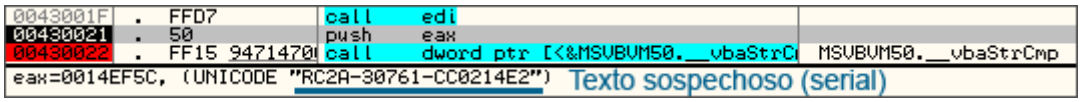
Ahora traceamos con F8 hasta donde se indica en la imagen sgte :



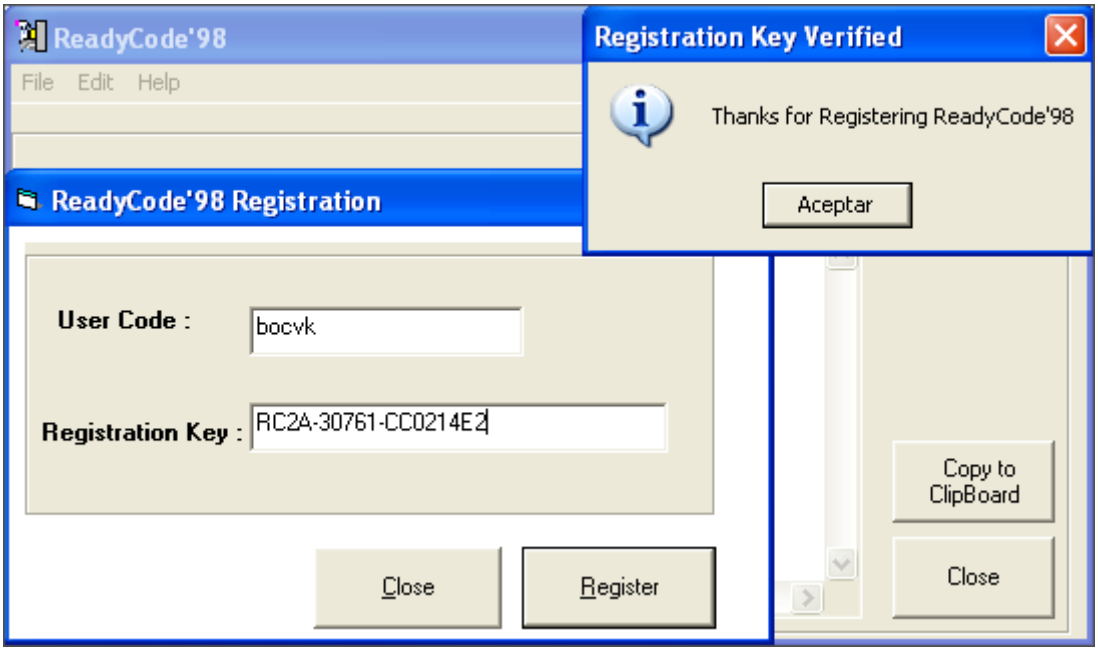
Una vez que llegamos hasta donde indique anteriormente presionan F8 , y los llevara a la rutina donde comienza a generarse el serial (Esto es un bucle si repiten esta rutina 9 veces les generar? 9 serials xD) , ahora comenzamos a tracear denuevo con F8 hasta donde indico :



Ahora vemos en la ventana de informaci?n adicional y encontramos algo demasiado sospechoso xD :



Copiamos lo que encontramos , cerramos el OllyDbg y nos vamos a ejecutar el programa , lo que encontramos lo ponemos como serial :



Ya estamos registrados !!! ...xD

Observaci?n :
* Si repetimos la rutina donde se genera el serial ,nos da 9 serials , que funcionan para

nuestro nombre , aqui las mias :

Código:
```
RC2A-30761-CC0214E1
RC2A-30761-CC0214E2
RC2A-30761-CC0214E3
RC2A-30761-CC0214E4
RC2A-30761-CC0214E5
RC2A-30761-CC0214E6
RC2A-30761-CC0214E7
RC2A-30761-CC0214E8
RC2A-30761-CC0214E9
```

*Pueden examinar la rutina donde se genera la serial (hay calls para entrar a ellos presionan F7 en vez de F8) y averiguar como es que se genero , y hacer un keygen ...

Espero que hayan aprendido algo... hasta la proxima
Salu2
Bocvk