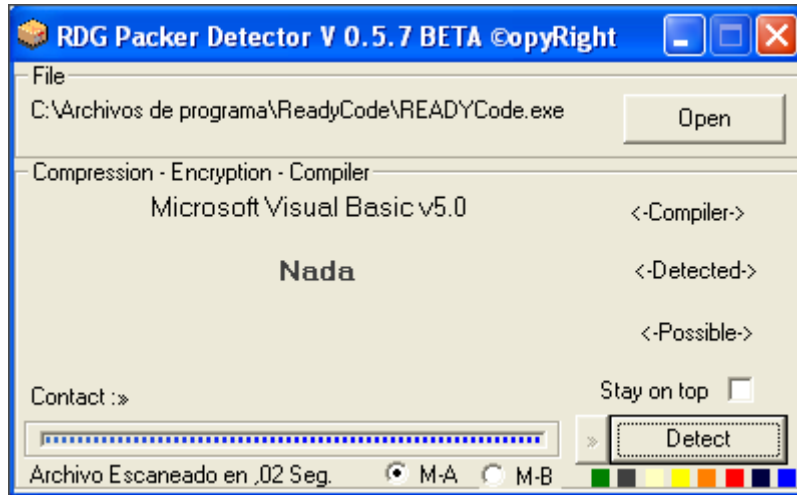


Ready Code'98

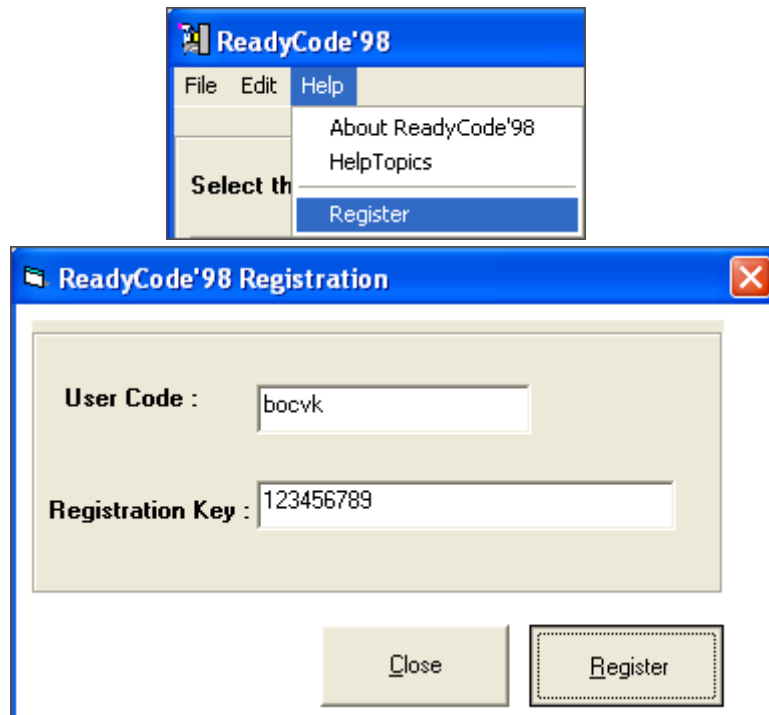
Instalamos el programa , luego tomamos a nuestra victima y la analizamos con el RDG. Para esto haremos click en Open y buscamos nuestro programa, luego haremos click en Abrir, y despu?s en Detect:



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

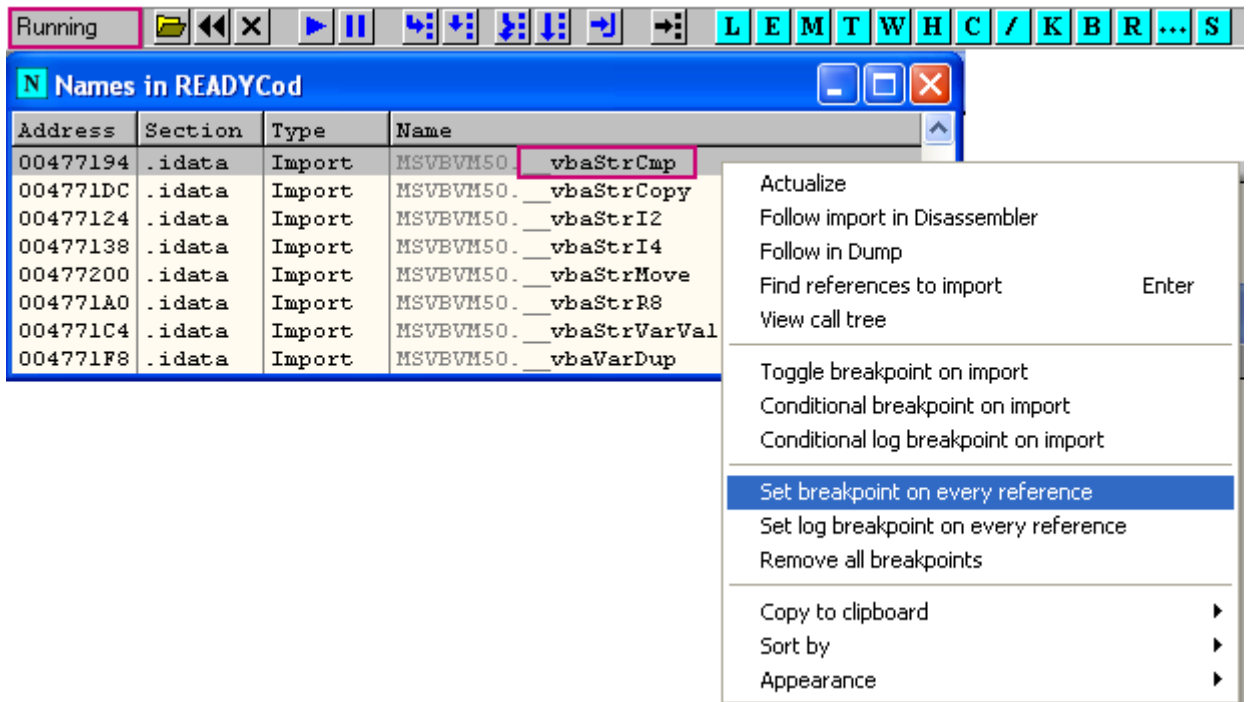
ingresado es incorrecta, en el caso de VB es poco usual trabajar con las strings debido a que se encuentran lejos de la parte del código donde se utiliza así que no nos servirá de nada copiarla pero por si acaso hay que tenerla de referencia :



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 manipulación de strings o texto, y las más conocidas en caso de que trabajemos con VB son todas las comienzan con "str" , aquí nosotros elegiremos una que compare (comparación 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 botón Register), y luego le ponemos un BreakPoint a la API que encontramos haciendo clic en dicha API y luego presionando clic 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 :

0043001F	. FFD7	call edi	
00430021	. 50	push eax	
00430022	. FF15 9471470	call dword ptr [&MSUBUM50.__vbaStrC	MSUBUM50.__vbaStrCmp
00430028	. 8BF0	mov esi, eax	
0043002A	. 8D45 D0	lea eax, dword ptr [ebp-30]	

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

0042FFEE	. BB 01000000	mov ebx, 1	
0042FFF3	> B8 09000000	mov eax, 9	Rutina donde comienza a generarse el serial
0042FFF8	. 66:3BD8	cmp bx, ax	
0042FFFB	. 7F 65	je short 00430062	
0042FFFD	. 8B4D D8	mov ecx, dword ptr [ebp-28]	
00430000	. 8B55 E0	mov edx, dword ptr [ebp-20]	
00430003	. 51	push ecx	
00430004	. 52	push edx	
00430005	. 53	push ebx	
00430006	. FF15 2471470	call dword ptr [&MSUBUM50.__vbaStrI	MSUBUM50.__vbaStrI2
0043000C	. 8B00	mov edx, eax	
0043000E	. 8D4D D4	lea ecx, dword ptr [ebp-2C]	
00430011	. FFD7	call edi	
00430013	. 50	push eax	
00430014	. FF15 5C71470	call dword ptr [&MSUBUM50.__vbaStrC	MSUBUM50.__vbaStrCat
0043001A	. 8B00	mov edx, eax	
0043001C	. 8D4D D0	lea ecx, dword ptr [ebp-30]	
0043001F	. FFD7	call edi	
00430021	. 50	push eax	Estamos aquí
00430022	. FF15 9471470	call dword ptr [&MSUBUM50.__vbaStrC	MSUBUM50.__vbaStrCmp
00430028	. 8BF0	mov esi, eax	
0043002A	. 8D45 D0	lea eax, dword ptr [ebp-30]	
0043002D	. F7DE	neg esi	
0043002F	. 1BF6	sbb esi, esi	
00430031	. 8D4D D4	lea ecx, dword ptr [ebp-2C]	
00430034	. 50	push eax	
00430035	. 46	inc esi	
00430036	. 51	push ecx	
00430037	. 6A 02	push 2	
00430039	. F7DE	neg esi	
0043003B	. FF15 E071470	call dword ptr [&MSUBUM50.__vbaFree	MSUBUM50.__vbaFreeStr
00430041	. 83C4 0C	add esp, 0C	
00430044	. 66:85F6	test si, si	
00430047	. 75 10	jnz short 00430059	
00430049	. B8 01000000	mov eax, 1	
0043004E	. 66:03C3	add ax, bx	
00430051	. 70 6C	jo short 004300BF	
00430053	. 8B08	mov ebx, eax	
00430055	. 33F6	xor esi, esi	
00430057	. EB 9A	jmp short 0042FFF3	Traceamos hasta aquí
00430059	> C745 DC FFFF	mov dword ptr [ebp-24], -1	

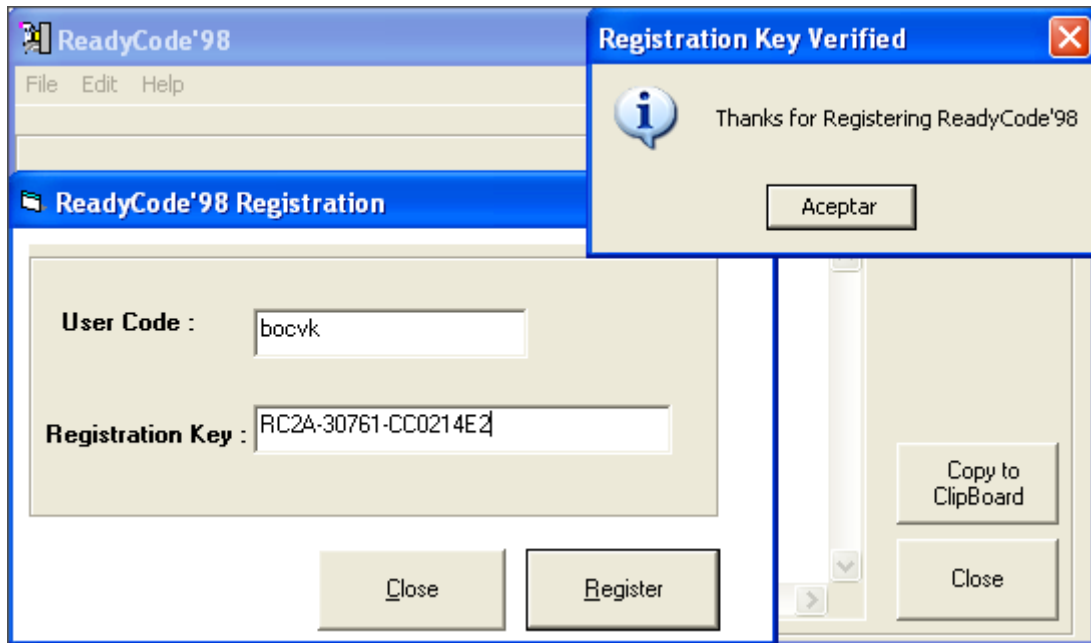
Una vez que llegamos hasta donde indique anteriormente presionan F8 , y los llevara a la rutina donde comienza a generarse el serial (Esto es un bucle si repiten esta rutina 9 veces les generar? 9 serials xD) , ahora comenzamos a tracear denuovo con F8 hasta donde indico :

0042FFEE	. BB 01000000	mov ebx, 1	
0042FFF3	> B8 09000000	mov eax, 9	
0042FFF8	. 66:3BD8	cmp bx, ax	
0042FFFB	. 7F 65	je short 00430062	
0042FFFD	. 8B4D D8	mov ecx, dword ptr [ebp-28]	
00430000	. 8B55 E0	mov edx, dword ptr [ebp-20]	Aquí Algo sospechoso pero no es la serial xD
00430003	. 51	push ecx	
00430004	. 52	push edx	
00430005	. 53	push ebx	
00430006	. FF15 2471470	call dword ptr [&MSUBUM50.__vbaStrI	MSUBUM50.__vbaStrI2
0043000C	. 8B00	mov edx, eax	
0043000E	. 8D4D D4	lea ecx, dword ptr [ebp-2C]	
00430011	. FFD7	call edi	
00430013	. 50	push eax	
00430014	. FF15 5C71470	call dword ptr [&MSUBUM50.__vbaStrC	MSUBUM50.__vbaStrCat
0043001A	. 8B00	mov edx, eax	
0043001C	. 8D4D D0	lea ecx, dword ptr [ebp-30]	
0043001F	. FFD7	call edi	
00430021	. 50	push eax	Traceamos hasta aquí
00430022	. FF15 9471470	call dword ptr [&MSUBUM50.__vbaStrC	MSUBUM50.__vbaStrCmp
00430028	. 8BF0	mov esi, eax	

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

0043001F	. FFD7	call edi	
00430021	. 50	push eax	
00430022	. FF15 94714701	call dword ptr [MSUBUM50.__vbaStrC	MSUBUM50.__vbaStrCmp
eax=0014EF5C, (UNICODE "RC2A-30761-CC0214E2") Texto sospechoso (serial)			

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