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:

RDG Packer Detector V 0.5.7 BETA ©opyRig	ht 💶 🖂
File C:\Archivos de programa\ReadyCode\READYCode.exe	Open
Compression - Encryption - Compiler	
Microsoft Visual Basic ∨5.0	<-Compiler->
Nada	<-Detected->
	<-Possible->
Contact :»	Stay on top 🔲
»	Detect
Archivo Escaneado en ,02 Seg. 📀 M-A 🔿 M-B	

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 :

	🔋 ReadyCode'98						
	File	Edit	Help				
	Sel	ect th	Ab He	out ReadyCode IpTopics	e'98		
			Re	gister			
🛱 ReadyCo	de'98	Regi	strati	ion			×
User Cod Registratic	le : In Kej	bo , : 12	cvk 345678	39			
				<u>C</u> lose		<u>R</u> egister	

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" :

Running	🖻 📢 🗙		- 4 + 4		LEMTWHC/KBR····S		
Names	Names in READYCod						
Address	Section	Туре	Name				
00477194	.idata	Import	MSVBVM50.	vbaStrCmp			
004771DC	.idata	Import	MSVBVM50.	vbaStrCopy	Actualize		
00477124	.idata	Import	MSVBVM50.	vbaStrI2	Follow import in Disassembler		
00477138	.idata	Import	MSVBVM50.	vbaStrI4	Follow in Dump		
00477200	.idata	Import	MSVBVM50.	vbaStrMove	Find references to import Enter		
004771A0	.idata	Import	MSVBVM50.	vbaStrR8	View call tree		
004771C4	.idata	Import	MSVBVM50.	vbaStrVarVa			
004771F8	.idata	Import	MSVBVM50.	vbaVarDup	Toggle breakpoint on import		
					Conditional breaknoint on import		
					Conditional log broakpoint on import		
					Condicional log breakpoint on import		
					Set breakpoint on every reference		
					Set log breakpoint on every reference		
					Remove all breakpoints		
					Copy to clipboard		
					Sort by		
					Appearance		

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

00	043001F	•	FFD7		call	edi
00	430021		50		push	eax
00	3430022		FF15	9471470	call	dword ptr [<&MSVBUM50vbaStrCi MSVBUM50vbaStrCmp
00	0430028	•	8BF0		MOV	esi, eax
00)43002A	•	8D45	DØ	lea	eax, dword ptr [ebp-30]

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

0042FFEE		MOV	ebx, 1	a second second second
0042FFF3	> > > B8 0900000	MOV	eax, 9 Rutina donde comienza	a generarse el serial
0042FFF8	66:3BD8		bx, ax	-
0042FFFB	.~ 7F_65	J9	short 00430062	
0042FFFD	. 884D D8	mov	ecx, dword ptr [ebp-28]	
00430000	. <u>8855</u> E0	mov_	edx, dword ptr [ebp-20]	
00430003	. 51	push	ecx	
00430004	. 52	push	edx	
00430005	. 53	push	ebx	
00430006	. FF15 <u>2471470</u>	call	dword ptr 14&MSVBVM50vbaStr1	MSVBVM50VbaStr12
00430000	. 8800 .	mov	edx, eax	
0043000E	. 8040 04	lea	ecx, dword ptr Lebp-20J	
00430011	• <u>FF</u> U7	cati	edi	
00430013	. 50	push	eax	
00430014	. FF15 <u>5071470</u>	call	dword ptr 14&MSVBVM50vbaStrC	MSVBVM50vbaStrCat
0043001H	. 8800	mov	edx, eax	
00430010	. 8040 00	lea	ecx, dword ptr Lebp-301	
0043001F	• FFU7	call	edi	Estamos aquí
00420021	EE1E 0471470		duand sty F/AMCUDUMER	MCUDUMEQ ub a Ctra Core
	. FF15 <u>24/14/0</u>	Cart	UWUTU ptr ttanovovnouvuastru	TISOBOTISEODAStromp
00430020	- 00F0 9D45 D0		est, ean esy duard str [ebs=20]	
00430020	. 0043 00	lea -	ean, dword por teop oos	
0043002E	18F6	lebb	est eci eci	
00430031		100	ecy dword ptr [ebp-20]	
00430034	50	nush	eax	
00430035	46	line	esi	
00430036	51	nush	ecx	
00430037	. 6 <u>0</u> 02	Dush	2	
00430039		nea	esi	
0043003B	EF15 F071470	loal	dword ptr [K&MSUBUM50, ubaFree]	MSUBUM50. UbaEreeStr
00430041	. 83C4 AC	add	esp. AC	
00430044	. 66:85F6	test	si. si	
00430047	75 10	inz	short 00430059	
00430049	. B8 01000000	mov	eax. 1	
0043004E	. 66:03C3	add	ax, bx	
00430051	.V 70 6C	lio	short 004300BF	
00430053	. 88D8	MOV	ebx. eax	
00430055	. 33F6	XOT	esi. esi Tr	acoamos basta aquí
00430057	-^ EB 9A	JMD	short 0042FFF3	accantos nasta aqui
00430059	> C745 DC FFFF	Imov	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 denuevo con F8 hasta donde indico :

D			PP 01000000	mou	obu 1	
0	042FFEE		PP 01000000	MOV	eux, 1	
Ы	042FFF3	>	•R8 03000000	MOV	eax, 9	
0	042FFF8	•	66:3BD8	CMP	bx, ax	
0	042FFFB	.~	7F 65	jg	short 00430062	· · · ·
Ø	042EEED		SB4D DS	mou	ecy dword atr [eba-28] AC	ul Algo sospechoso pero
0	0430000		8B55 E0	MOV	edx, dword ptr [ebp-20]	no es la serial xD
И	04300031	•	51	push	ecx	no cona cona Ab
0	0430004		52	bush	edx	
ā	0430005	-	63	Dush	ahu	
ă	0400000	•	EE1E 2471470		duord stry FZ9MCHDHMEQ	MCHDHMER UBSCHWT2
0	0430000	•	PF15 <u>24(14(6</u>	carr	uworu per reanovovnoovoasern	11505011500D450112
10	0430000	•	8800	INOV	edx, eax	
0	043000E	•	8D4D D4	lea	ecx, dword ptr [ebp-2C]	
0	0430011		FFD7	call	edi	
0	0430013		50	push	eax	
0	0430014		FF15 <u>5C71470</u>	call	dword ptr [<&MSUBUM50vbaStrC	MSVBVM50vbaStrCat
0	043001A		88D0	mov	edx. eax	
Ā	043001C	-	8040 DA	lea	ecy, dword ptr [ebp-30]	
ă	040001E	•	EED7	and I	odi Tasasana basha ami	
	0400004		50		l raceamos nasta adul	
0	0430021	•	50	pusn	eax	
0	04300ZZ	•	FF15 <u>9471470</u>	call	_ dword _ptr_EK&MSVBVM50vbaStrC	MSVBVM50vbaStrCmp
0	0430028	•	8BFØ	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 <u>9471470</u>	call	dword ptr [<&MSUBUM50vbaStrC	MSVBVM50vbaStrCmp
eax=00148	EF5C	, (UNICODE "R	C2A-3076	I-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 :

🕅 ReadyCode'98	Registration Key Verified 🛛 🛛 🛛
File Edit Help	Thanks for Registering ReadyCode'98
ReadyCode'98 Registration	Aceptar
User Code : bocvk Registration Key : RC2A-30761-CC0214E2	Copy to ClipBoard
Close	Register Close

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