

Programa: macro de vb en excel,->VBA project

Por ende: Reservados todos los derechos. y el fin de este escrito es educativo

Herramientas: Ollydbg 1 + plugins

Compilador: vb /macros

Objetivos: bypasear la key del proyecto , para luego cambiarla a la que uno quiera o leer el codigo original.

Cracker: Apuromafo /c_c / Astronado

Introducción,

Tenia un xls, con una clave, la cual se me olvido , llego el momento de probar en olly si era posible encontrarla o bien bypasearla, y si , es posible

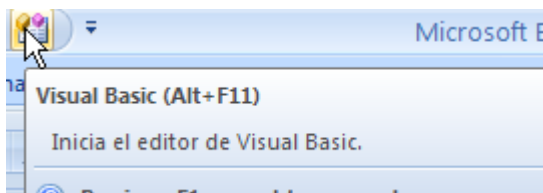
Las claves almacenadas en excel siempre suelen ser con tablas de crc o RC4

Pero este es solo una hazaña que vi en la la version xp y version 2007

Asi que comenzamos

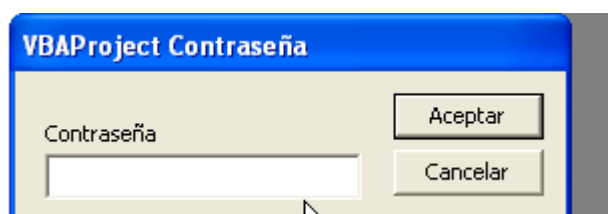
Lo primero es depurar el Excel en su carpeta por defecto.

Con el depurador corriendo ok, presiono presiono:



Y abro el documento de Excel

En el proyecto me muestra lo siguiente:



0013E004	77D3B7C5	user32.77D3B7C5	user32.77D3B7C5
0013ECC4	77D3812B	user32.77D3812B	user32.77D3812B
0013EE14	77D3AF7A	user32.77D3AF7A	user32.77D3AF7A
0013EE80	651141F0	Includes user32.77D3AF7A	user32.77D3AF75
0013EEBC	6511501E	Includes UBE6.651141F0	UBE6.651141EE
0013EF0C	65115181	UBE6.65114E44	UBE6.6511501B
0013EF38	6510B074	UBE6.65115100	UBE6.6511517C
0013EF80	77D18709	Includes UBE6.6510B074	UBE6.6510B074
0013EFAC	77D24C6E	? user32.77D18709	user32.77D18706
0013F018	77D24AF2	? user32.77D24C6E	user32.77D24CA1
0013F060	77D275BF	user32.77D24AF2	user32.77D24AED
0013F07C	77D18709	Includes user32.77D275BF	user32.77D275BA
0013F0A8	77D187EB	? user32.77D18709	user32.77D18706
0013F0AC	77D2759D	Includes user32.77D187EB	user32.77D187E6
			user32.77D27597

```

jvs COMMITTEEMEMBERSHIP - STATED NOT TO BE A MICROB...
>ft Office2007\Office12\EXCEL.EXE
>ft Office2007\Office12\MSOSTYLE.DLL
>ft Office2007\Office12\OART.DLL
JBA\UBA6\3082\UBE6INTL.DLL
JBA\UBA6\UBE6.DLL
OUTFLTR.DLL

```

OllyDbg - EXCEL.EXE - [*C.P.U* - main thread, module VBE6]

File View Debug Plugins Options Window Help

Paused

DEC EBP
 PUSH EAX
 PUSH EDX
 INC ESP
 DEC ESP
 DEC ESP
 ADD BYTE PTR DS:[EDX], CH
 PUSH UBE6.6523A998
 PUSH 7
 PUSH 01
 PUSH 12A
 PUSH UBE6.6523DC50
 PUSH UBE6.6511402C
 CALL UBE6.65091E88
 PUSH 0
 PUSH 0

Superfluous prefix

ASCII "ADVAPI32.DLL"

.5109CEB	8B B6	LMP EBX,ESI	
.5109CE7	>7D 08	JGE SHORT UBE6.65109CF1	
.5109CE9	8975 0C	MOV DWORD PTR SS:[EBP+C],ESI	
.5109CEC	>E9 F8000000	JMP UBE6.65109DE9	
.5109CF1	68 000000F0	PUSH F0000000	
.5109CF6	6A 01	PUSH 1	
.5109CF8	68 80809D65	PUSH UBE6.650D8980	ASCII "Microsoft Base Cryptographic Provider v1.0"
.5109CFD	5E	PUSH ESI	
.5109CFE	8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	
.5109D01	50	PUSH EAX	
.5109D02	FF15 E8A92365	CALL DWORD PTR DS:[652BA9E8]	advapi32.CryptAcquireContextA
.5109D08	85C0	TEST EAX,EAX	
.5109D0A	>74 D0	JE SHORT UBE6.65109CE9	
.5109D0C	8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
.5109D0F	50	PUSH EAX	
.5109D10	56	PUSH ESI	
.5109D11	56	PUSH ESI	
.5109D12	68 04800000	PUSH 8004	

Analizo y tiene 4 llamadas

65109C92	55	RETN 8	
65109C93	8BEC	PUSH EBP	
65109C95	83EC 14	MOV EBP,ESP	
65109C98	56	SUB ESP,14	
65109C99	33F6	PUSH ESI	
65109C9B	3975 08	XOR ESI,ESI	
65109C9E	75 07	CMP DWORD PTR SS:[EBP+8],ESI	
65109CA0	33C0	JNZ SHORT UBE6.65109CA7	
65109CA2	E9 80010000	XOR EAX,EAX	
65109CA7	57	JMP UBE6.65109E27	
65109CA8	8B7D 0C	PUSH EDI	
65109CAB	3BFE	MOV EDI,DWORD PTR SS:[EBP+C]	
65109CAD	74 07	CMP EDI,ESI	
65109CAF	8B45 10	JGE SHORT UBE6.65109CB8	
65109CB2	3BC6	MOV EAX,DWORD PTR SS:[EBP+10]	
65109CB4	75 07	CMP EAX,ESI	
65109CB6	33C0	JNZ SHORT UBE6.65109CB0	
65109CB8	E9 69010000	XOR EAX,EAX	
65109CB0	53	JMP UBE6.65109E26	
65109CBE	6A 04	PUSH EBX	
65109CC0	5B	POP EBX	
65109CC1	8930	MOV DWORD PTR DS:[EAX],ESI	
65109CC3	C745 0C 010000	MOV DWORD PTR SS:[EBP+C],1	
65109CCA	8975 F8	MOV DWORD PTR SS:[EBP-8],ESI	
65109CCD	8975 FC	MOV DWORD PTR SS:[EBP-4],ESI	
65109CD0	8975 F4	MOV DWORD PTR SS:[EBP-C],ESI	
65109CD3	895D EC	MOV DWORD PTR SS:[EBP-14],EBX	
65109CD6	E9 31A30000	CALL UBE6.65114000	
65109CDB	3BC6	CMP EAX,ESI	
65109CDD	74 12	JGE SHORT UBE6.65109CF1	
65109CDF	50	PUSH EAX	
65109CE0	8B0C6F7FF	CALL UBE6.65086395	
65109CE5	3BC6	CMP EAX,ESI	
65109CE7	7D 08	JGE SHORT UBE6.65109CF1	
65109CE9	8975 0C	MOV DWORD PTR SS:[EBP+C],ESI	
65109CEC	E9 F8000000	JMP UBE6.65109DE9	
65109CF1	68 000000F0	PUSH F0000000	
65109CF6	6A 01	PUSH 1	
65109CF9	68 80890065	PUSH UBE6.65008980	
65109CFD	56	PUSH ESI	
65109CFE	8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	
65109D01	50	PUSH EAX	

Arg5 = F0000000
Arg4 = 00000001
Arg3 = 65008980 ASCII "Microsoft Base Cryptographic Provider v1.0"
Arg2 =
Arg1 =

Luego coloco una contraseña que obviamente no es y al comienzo de la rutina investigo

65109C8D	5E	POP ESI	
65109C8E	C9	LEAVE	
65109C8F	C2 0800	RETN 8	
65109C92	C3	RETN	
65109C93	8BEC	MOV EBP,ESP	
65109C95	83EC 14	SUB EBP,14	
65109C98	56	PUSH ESI	
65109C99	33F6	XOR ESI,ESI	
65109C9B	3975 08	CMP DWORD PTR SS:[EBP+8],ESI	
65109C9E	75 07	JNZ SHORT UBE6.65109CA7	
65109CA0	33C0	XOR EAX,EAX	
65109CA2	E9 80010000	JMP UBE6.65109E27	
65109CA7	57	PUSH EDI	

Return to 6510AFA1 (UBE6.6510AFA1)
Local calls from 6510AF9C, 6510B196, 65

Con retn , pues me muestra que retorna a aquel lugar, un follow y tengo una rutina

6510AF52	8B03	MOV EAX,DWORD PTR DS:[EBX]	
6510AF54	85C0	TEST EAX,EAX	
6510AF56	74 17	JGE SHORT UBE6.6510AF6F	
6510AF58	FF75 0C	PUSH DWORD PTR SS:[EBP+C]	
6510AF5B	50	PUSH EAX	
6510AF5C	FF15 A0140065	CALL DWORD PTR DS:[&KERNEL32.lstrcmpA]	String2 String1 lstrcmpA
6510AF62	85C0	TEST EAX,EAX	
6510AF64	75 7D	JNZ SHORT UBE6.6510AFE3	
6510AF66	C745 FC 010000	MOV DWORD PTR SS:[EBP-4],1	
6510AF6D	EB 74	JMP SHORT UBE6.6510AFE3	
6510AF6F	8B53 04	MOV EDX,DWORD PTR DS:[EBX+4]	
6510AF72	85D2	TEST EDX,EDX	
6510AF74	74 6D	JGE SHORT UBE6.6510AFE3	
6510AF76	8B45 0C	MOV EAX,DWORD PTR SS:[EBP+C]	
6510AF79	8365 08 00	AND DWORD PTR SS:[EBP+8],0	
6510AF7D	56	PUSH ESI	
6510AF7E	8D70 01	LEA ESI,DWORD PTR DS:[EAX+1]	
6510AF81	8A08	MOV CL,BYTE PTR DS:[EAX]	
6510AF83	40	INC EAX	
6510AF84	84C9	TEST CL,CL	
6510AF86	75 F9	JNZ SHORT UBE6.6510AF81	
6510AF88	2BC6	SUB EAX,ESI	
6510AF8A	8945 F4	MOV DWORD PTR SS:[EBP-C],EAX	
6510AF8D	8945 F8	MOV DWORD PTR SS:[EBP-8],EAX	
6510AF90	52	PUSH EDX	
6510AF91	8D45 08	LEA EAX,DWORD PTR SS:[EBP+8]	Arg4
6510AF94	50	PUSH EAX	Arg3
6510AF95	8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	Arg2
6510AF98	50	PUSH EAX	Arg1
6510AF99	FF75 0C	PUSH DWORD PTR SS:[EBP+C]	
6510AF9C	E8 F1ECFFFF	CALL UBE6.65109C92	UBE6.65109C92
6510AF9E	85C0	TEST EAX,EAX	
6510AF9F	74 8D	JGE SHORT UBE6.6510AFE2	
6510AFA0	8B4B 08	MOV ECX,DWORD PTR DS:[EBX+8]	

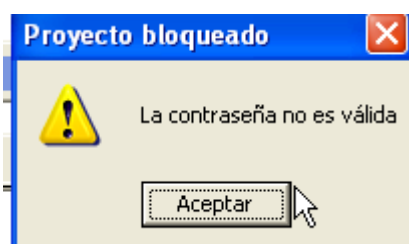
6510AF9C	. E8 F1ECFFFF	CALL UBE6.65109C92	UBE6.65109C92
6510AF9D	. 85C0	TEST EAX,EAX	
6510AF9E	. 74 3D	JE SHORT UBE6.6510AFE2	
6510AF9F	. 8B4B 08	MOV ECX,DWORD PTR DS:[EBX+8]	
6510AFA0	. 394D F8	CMP DWORD PTR SS:[EBP-8],ECX	
6510AFA1	. 75 2C	JNZ SHORT UBE6.6510AFD9	
6510AFA2	. 8B75 08	MOV ESI,DWORD PTR SS:[EBP+8]	
6510AFA3	. 57	PUSH EDI	
6510AFA4	. 8B7B 04	MOV EDI,DWORD PTR DS:[EBX+4]	
6510AFA5	. 33C0	XOR EAX,EAX	
6510AFA6	. F3:A6	REPE CMPS BYTE PTR ES:[EDI],BYTE PTR DS	
6510AFA7	. 5F	POP EDI	
6510AFA8	. 75 1E	JNZ SHORT UBE6.6510AFD9	
6510AFA9	. 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
6510AFAB	. 40	INC EAX	
6510AFAC	. 50	PUSH EAX	
6510AFAD	. E8 5D7CEFFF	CALL UBE6.65002C22	
6510AFAE	. 59	POP ECX	
6510AFAF	. FF75 0C	PUSH DWORD PTR SS:[EBP+C]	
6510AFB0	. 8903	MOV DWORD PTR DS:[EBX],EAX	String2
6510AFB1	. 50	PUSH EAX	String1
6510AFB2	. FF15 84140065	CALL DWORD PTR DS:[<<KERNEL32.istrncpyA>	istrncpyA
6510AFB3	. C745 FC 010000	MOV DWORD PTR SS:[EBP-4],1	
6510AFB4	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	
6510AFB5	. E8 30A7EFFF	CALL UBE6.65005711	
6510AFB6	. 59	POP ECX	
6510AFB7	. 5E	POP ESI	
6510AFB8	. 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
6510AFB9	. 5B	POP EBX	
6510AFBA	. C9	LEAVE	
6510AFBB	. C2 0800	RET 8	

Y al retorno de este llega a la comparación decisiva

6510B035	. 50	PUSH EAX	Buffer
6510B036	. BF 5E150000	MOV EDI,155E	ControlID => 155E (5470.)
6510B037	. 57	PUSH EDI	hWnd
6510B038	. 56	PUSH ESI	GetDlgItemTextA
6510B039	. FF15 84170065	CALL DWORD PTR DS:[<<USER32.GetDlgItemTextA>	Arg2
6510B03A	. 8D45 DC	LEA EAX,DWORD PTR SS:[EBP-24]	Index = GWL_USERDATA
6510B03B	. 50	PUSH EAX	GetWindowLongA
6510B03C	. 6A EB	PUSH -15	Arg1
6510B03D	. 56	PUSH ESI	UBE6.6510AF44
6510B03E	. FF15 28180065	CALL DWORD PTR DS:[<<USER32.GetWindowLongA>	
6510B03F	. 50	PUSH EAX	
6510B040	. E8 EEF0FFFF	CALL UBE6.6510AF44	
6510B041	. 85C0	TEST EAX,EAX	
6510B042	. 75 40	JNZ SHORT UBE6.6510B09A	
6510B043	. 50	PUSH EAX	
6510B044	. 6A 30	PUSH 30	
6510B045	. 68 9F000000	PUSH 9F	
6510B046	. E8 D07EF3FF	CALL UBE6.65042F37	
6510B047	. 50	PUSH EAX	
6510B048	. 68 9E000000	PUSH 9E	
6510B049	. E8 C57EF3FF	CALL UBE6.65042F37	
6510B04A	. 50	PUSH EAX	
6510B04B	. 56	PUSH ESI	
6510B04C	. E8 87A00000	CALL UBE6.65115100	Arg2
6510B04D	. 68 CC290065	PUSH UBE6.650089CC	Arg1
6510B04E	. 57	PUSH EDI	Text = ""
6510B04F	. 56	PUSH ESI	ControlID
6510B050	. FF15 60180065	CALL DWORD PTR DS:[<<USER32.SetDlgItemTextA>	hWnd
6510B051	. 57	PUSH EDI	SetDlgItemTextA
6510B052	. 56	PUSH ESI	ControlID
6510B053	. FF15 3C180065	CALL DWORD PTR DS:[<<USER32.GetDlgItemTextA>	hWnd
6510B054	. 50	PUSH EAX	GetDlgItem
6510B055	. FF15 14190065	CALL DWORD PTR DS:[<<USER32.SetFocus>	hWnd
6510B056	. 33C0	XOR EAX,EAX	SetFocus
6510B057	. 40	INC EAX	
6510B058	. EB 3A	JMP SHORT UBE6.6510B0D4	
6510B059	. 5A 01	PUSH 1	
6510B05A	. 56	PUSH ESI	hWnd
6510B05B	. FF15 50180065	CALL DWORD PTR DS:[<<USER32.EndDialog>	EndDialog
6510B05C	. EB F0	JMP SHORT UBE6.6510B095	
6510B05D	. 57	PUSH EDI	
6510B05E	. 6A EB	PUSH -15	NewValue; Case 110 of switch 6510AFFE
6510B05F	. 56	PUSH ESI	Index = GWL_USERDATA

Siendo enddialog el indicado .

Vuelvo a iniciar la búsqueda pero esta vez esperaré el mensaje



Pulso pause + alt+k

0013EF1C	00000000	Arg4 = 00000000	
0013EF38	6510B079	UB6.65115100	UB6.6510B079
0013EF3C	001001A4	Arg1 = 001001A4	
0013EF40	086B2A40	Arg2 = 086B2A40	
0013EF44	01059500	Arg3 = 01059500	ASCII "Proyecto bloqueado"
0013EF48	00000030	Arg4 = 00000030	
0013EF4C	00000000	Arg5 = 00000000	
0013EF80	77D18709	Maybe UB6.6510AFEB	
0013EF84	001001A4	Arg1 = 001001A4	
0013EF88	00000111	Arg2 = 00000111	
0013EF8C	00000001	Arg3 = 00000001	
0013EF90	00000232	Arg4 = 00000232	
0013EFAC	77D24C96	? user32.77D186E1	
0013F018	77D24AF2	? user32.77D24BF1	
0013F060	77D275BF	user32.77D24AF3	
0013F07C	77D18709	Includes user32.77D275BF	
0013F0A8	77D187EB	? user32.77D186E1	
0013F0AC	77D2759D	Includes user32.77D187EB	

Actualize
 Hide arguments Space
 Thread
 Follow address in stack
 Show procedure Enter
 Show call
 Execute to return F4
 Copy to clipboard

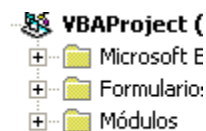
Pulso ok en el mensaje y cae aquí :

6510B047	6510B049	6510B04A	6510B050	6510B051	6510B055	6510B058	6510B05A	6510B05D	6510B05E	6510B062	6510B067	6510B069	6510B06D	6510B072	6510B073	6510B074	6510B075	6510B07F	6510B080	6510B086	6510B087	6510B088	6510B089	6510B08F	6510B095	6510B097	6510B099	6510B09C	6510B09D	6510B0A3	6510B0A5	6510B0A6	6510B0A9	6510B0AF	
• 6H EB	• 56	FF15 98180065	E8 EEF0FFFF	95C0	• 75 40	• 50	• 6A 30	• 68 9F000000	E8 D07EF3FF	• 50	• 6A 30	• 68 9E000000	E8 C57EF3FF	• 50	E8 87A00000	• 57 CC890065	• 56	FF15 60180065	• 57	FF15 3C180065	FF15 14190065	• 50	• 50	• 50	• 50	• 50	• 50	• 50	• 50	• 50	• 50	• 50	• 50	• 50	• 50
PUSH -1b	PUSH ESI	CALL DWORD PTR DS:[&USER32.SetWindowLongA]	CALL UB6.6510AF44	TEST EAX, EAX	JNZ SHORT UB6.6510B09A	PUSH EAX	PUSH 30	PUSH 9F	CALL UB6.65042F37	PUSH EAX	PUSH 30	PUSH 9E	CALL UB6.65042F37	PUSH EAX	PUSH ESI	PUSH UB6.650089CC	PUSH EDI	CALL DWORD PTR DS:[&USER32.SetDlgItemTextA]	PUSH EDI	CALL DWORD PTR DS:[&USER32.SetDlgItemTextA]	CALL DWORD PTR DS:[&USER32.SetFocus]	XOR EAX, EAX	INC EAX	JMP SHORT UB6.6510B0D4	PUSH 1	PUSH ESI	CALL DWORD PTR DS:[&USER32.EndDialog]	JMP SHORT UB6.6510B095	PUSH EDI	PUSH -15	PUSH ESI	CALL DWORD PTR DS:[&USER32.SetWindowLongA]	PUSH DWORD PTR DS:[EDI+C]		

[Index = GWL_USERDATA]
 hWnd
 SetWindowLongA
 Arg1
 UB6.6510AF44
 Arg2
 Arg3
 UB6.65115100
 Arg4
 ControlID
 hWnd
 SetDlgItemTextA
 ControlID
 hWnd
 SetDlgItemTextA
 hWnd
 SetFocus
 hWnd
 EndDialog
 NewValue: Case 110 of switch 6510AFFE
 Index = GWL_USERDATA
 hWnd
 SetWindowLongA
 Text

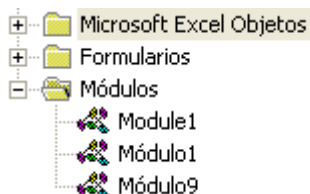
Coloco bp en la comparación y fuerzo el salto a que se ejecute, luego otra vez en el dialogo

Veo el efecto de un salto:



Y permitiéndome el acceso a los módulos y sin clave, exportar todos los módulos.

En 2003, es similar, la unica diferencia es que puedo guardarlo sin clave, en 2007, solo accedo a los módulos y puedo ver todo el codigo de fuente.



Saludos Apuromafo

Este documento va dedicado a todos mis compañeros de CrackSlatinoS(CLS),RVLCN, ARTeam , TeamICU, Seek n Destroy, RCE Forums, The Reverse Code Engineering Community, Exetools, BiW, Peidy, UnPackcN, BRD , RES, At4re , REA, CIM ,BlackStorm y otros amigos.Un saludo especial a a ti, que te has decidido a leer este documento, y que sin tu apoyo y colaboración no valdría la pena el tiempo dedicado a esta tarea. Y a mi Dios .