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

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

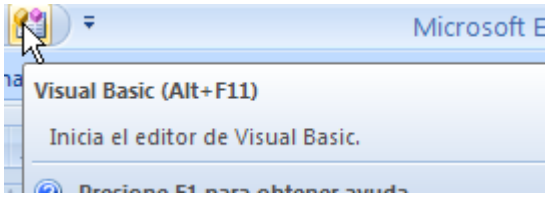
Las claves almacenadas en excel siempre suelen ser con tablas de crc o RC4

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

Asi que comenzamos

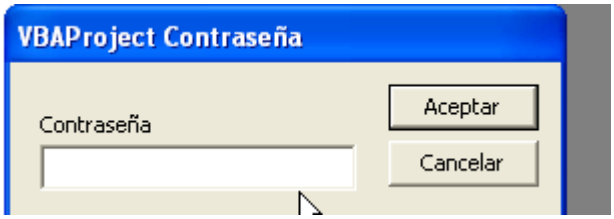
Lo primero es depurar el Excel en su carpeta por defecto.

Con el depurador corriendo ok, presiono presiono:

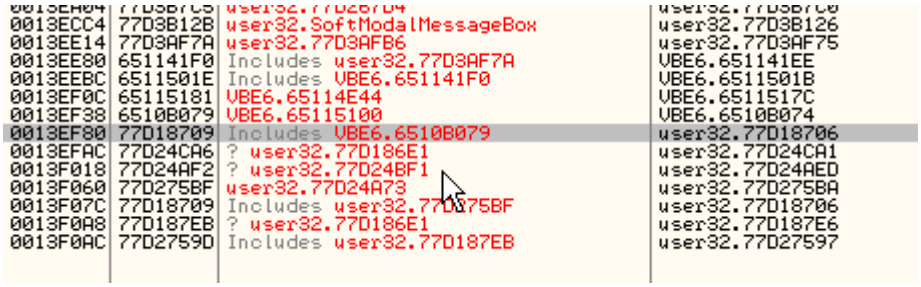


Y abro el documento de Excel

En el proyecto me muestra lo siguiente:

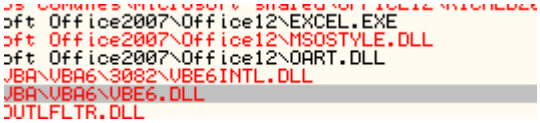


Coloco una contraseña que no es. Pause+ Alt+k y miro

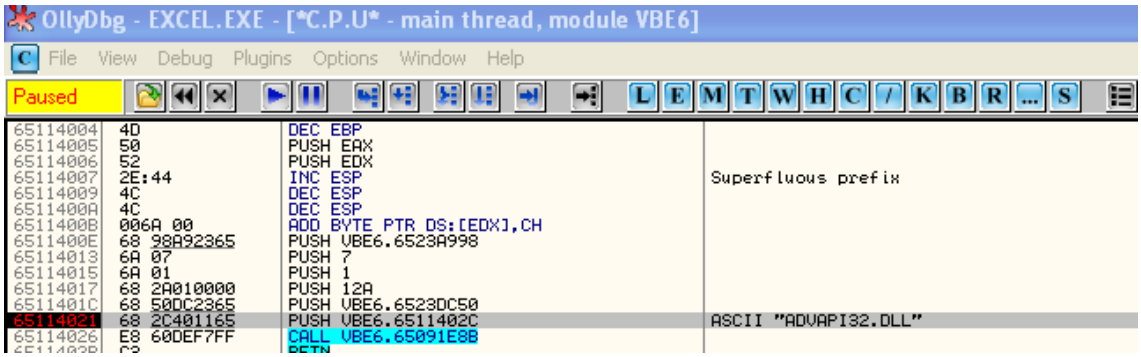


El modulo vbe6 ..de vb puede ser guia

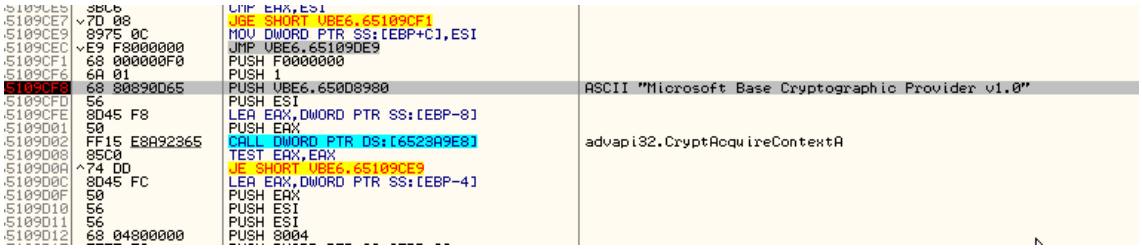
Pulto alt+e



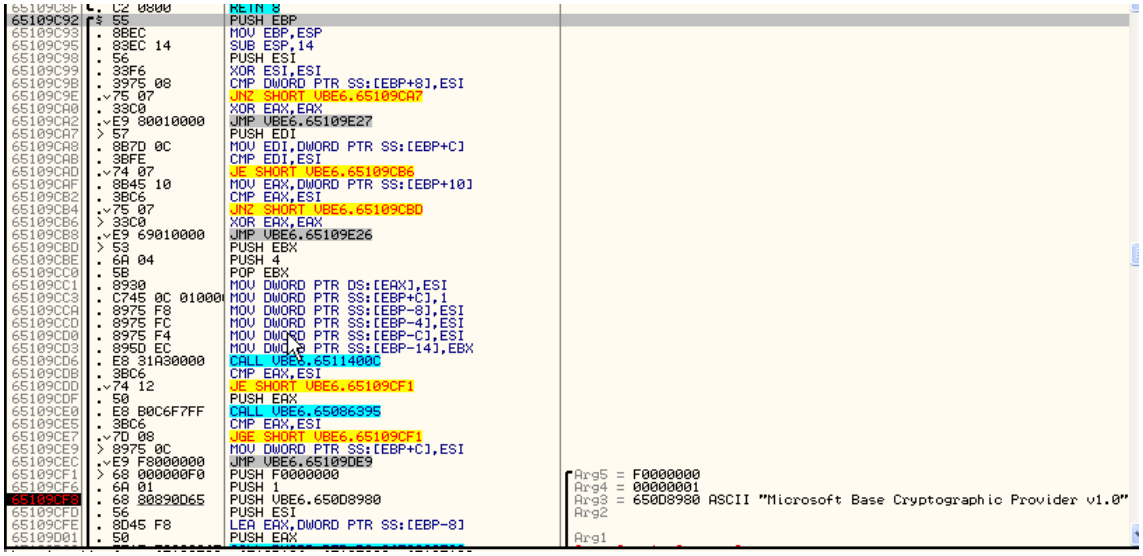
Luego entra a



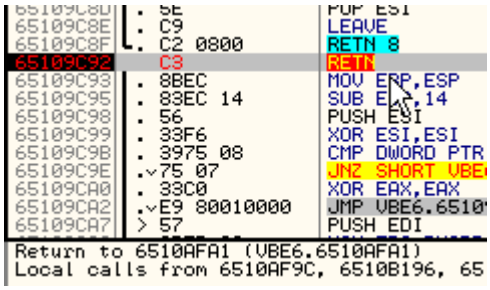
Luego pasa por



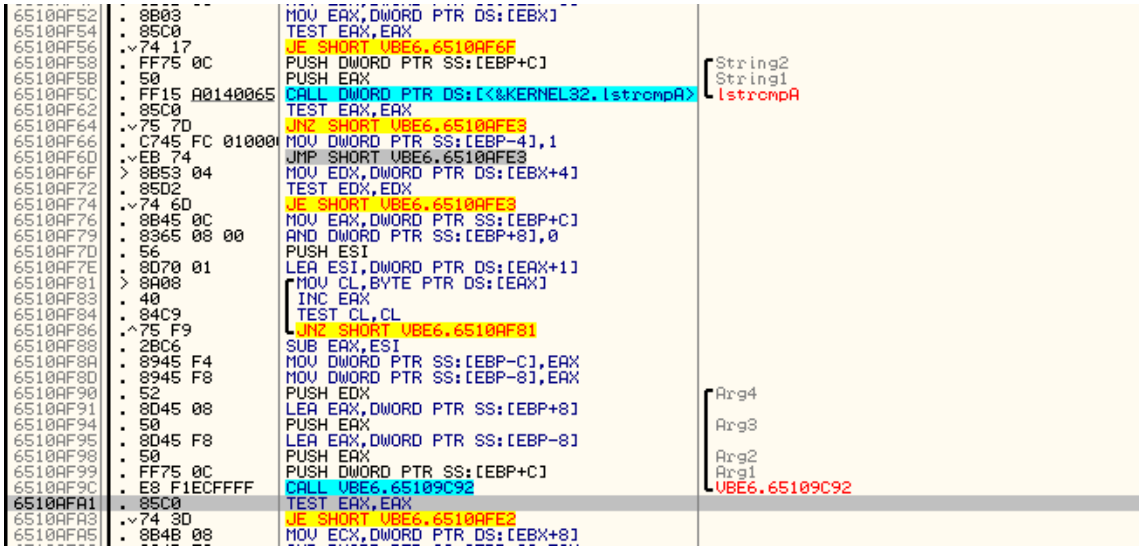
Analizo y tiene 4 llamadas



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



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



```
6510AF9C  . E8 F1ECFFFF    CALL VBE6.65109C92                    VBE6.65109C92
6510AFA1  . 85C0           TEST EAX,EAX
6510AFA3  .v74 3D          JE SHORT VBE6.6510AFE2
6510AFA5  . 8B4B 08        MOV ECX,DWORD PTR DS:[EBX+8]
6510AFA8  . 394D F8        CMP DWORD PTR SS:[EBP-8],ECX
6510AFAB  .v75 2C          JNZ SHORT VBE6.6510AFD9
6510AFAD  . 8B75 08        MOV ESI,DWORD PTR SS:[EBP+8]
6510AFB0  . 57             PUSH EDI
6510AFB1  . 8B7B 04        MOV EDI,DWORD PTR DS:[EBX+4]
6510AFB4  . 33C0           XOR EAX,EAX
6510AFB6  . F3:A6          REPE CMPS BYTE PTR ES:[EDI],BYTE PTR DS
6510AFB8  . 5F             POP EDI
6510AFB9  .v75 1E          JNZ SHORT VBE6.6510AFD9
6510AFBB  . 8B45 F4        MOV EAX,DWORD PTR SS:[EBP-C]
6510AFBE  . 40             INC EAX
6510AFBF  . 50             PUSH EAX
6510AFC0  . E8 5D7CEFFF    CALL VBE6.65002C22
6510AFC5  . 59             POP ECX
6510AFC6  . FF75 0C        PUSH DWORD PTR SS:[EBP+C]             String2
6510AFC9  . 8903           MOV DWORD PTR DS:[EBX],EAX
6510AFCB  . 50             PUSH EAX                              String1
6510AFCC  . FF15 84140065  CALL DWORD PTR DS:[<&KERNEL32.lstrcpyA>] lstrcpyA
6510AFD2  . C745 FC 01000  MOV DWORD PTR SS:[EBP-4],1
6510AFD9  > FF75 08        PUSH DWORD PTR SS:[EBP+8]
6510AFDC  . E8 30A7EFFF    CALL VBE6.65005711
6510AFE1  . 59             POP ECX
6510AFE2  > 5E             POP ESI
6510AFE3  > 8B45 FC        MOV EAX,DWORD PTR SS:[EBP-4]
6510AFE6  . 5B             POP EBX
6510AFE7  . C9             LEAVE
6510AFE8  L. C2 0800       RETN 8
```

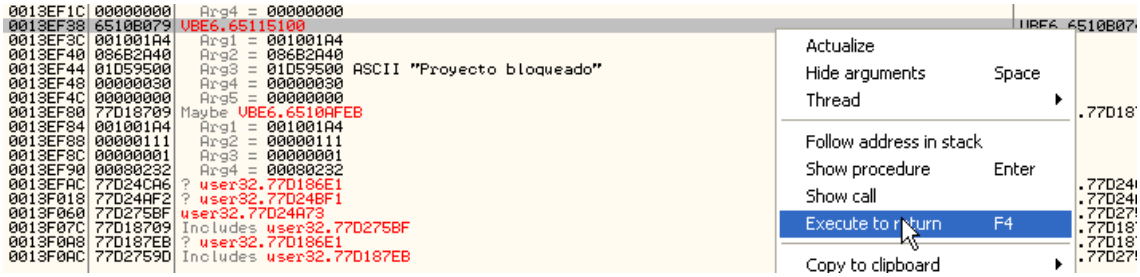
Y al retorno de este llega a la comparación decisiva

```
6510B035  . 50             PUSH EAX                              Buffer
6510B036  . BF 5E150000    MOV EDI,155E
6510B03B  . 57             PUSH EDI                              ControlID => 155E (5470.)
6510B03C  . 56             PUSH ESI                              hWnd
6510B03D  . FF15 B4170065  CALL DWORD PTR DS:[<&USER32.GetDlgItemT GetDlgItemTextA
6510B043  . 8D45 DC        LEA EAX,DWORD PTR SS:[EBP-24]
6510B046  . 50             PUSH EAX                              Arg2
6510B047  . 6A EB          PUSH -15                              Index = GWL_USERDATA
6510B049  . 56             PUSH ESI                              hWnd
6510B04A  . FF15 98180065  CALL DWORD PTR DS:[<&USER32.GetWindowLo GetWindowLongA
6510B050  . 50             PUSH EAX                              Arg1
6510B051  . E8 EEFEFFFF    CALL VBE6.6510AF44                    VBE6.6510AF44
6510B056  . 85C0           TEST EAX,EAX
6510B058  .v75 40          JNZ SHORT VBE6.6510B09A
6510B05A  . 50             PUSH EAX
6510B05B  . 6A 30          PUSH 30
6510B05D  . 68 9F000000    PUSH 9F
6510B062  . E8 D07EF3FF    CALL VBE6.65042F37
6510B067  . 50             PUSH EAX
6510B068  . 68 9E000000    PUSH 9E
6510B06D  . E8 C57EF3FF    CALL VBE6.65042F37
6510B072  . 50             PUSH EAX                              Arg2
6510B073  . 56             PUSH ESI                              Arg1
6510B074  . E8 87A00000    CALL VBE6.65115100                    VBE6.65115100
6510B079  . 68 CC890D65    PUSH VBE6.650D89CC                    Text = ""
6510B07E  . 57             PUSH EDI                              ControlID
6510B07F  . 56             PUSH ESI                              hWnd
6510B080  . FF15 60180065  CALL DWORD PTR DS:[<&USER32.SetDlgItemT SetDlgItemTextA
6510B086  . 57             PUSH EDI                              ControlID
6510B087  . 56             PUSH ESI                              hWnd
6510B088  . FF15 3C180065  CALL DWORD PTR DS:[<&USER32.GetDlgItem> GetDlgItem
6510B08E  . 50             PUSH EAX                              hWnd
6510B08F  . FF15 14190065  CALL DWORD PTR DS:[<&USER32.SetFocus>] SetFocus
6510B095  > 33C0           XOR EAX,EAX
6510B097  . 40             INC EAX
6510B098  .vEB 3A          JMP SHORT VBE6.6510B0D4
6510B09A  > 6A 01          PUSH 1
6510B09C  > 56             PUSH ESI                              hWnd
6510B09D  . FF15 50180065  CALL DWORD PTR DS:[<&USER32.EndDialog>] EndDialog
6510B0A3  .^EB F0          JMP SHORT VBE6.6510B095
6510B0A5  > 57             PUSH EDI                              NewValue: Case 110 of switch 6510AFFE
6510B0A6  . 6A EB          PUSH -15                              Index = GWL_USERDATA
```

Siendo enddialog el indicado .

Vuelvo a iniciar la búsqueda pero esta vez esperare el mensaje

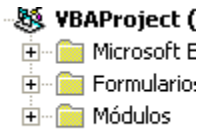
Pulso pause + alt+k



Pulso ok en el mensaje y cae aquí :

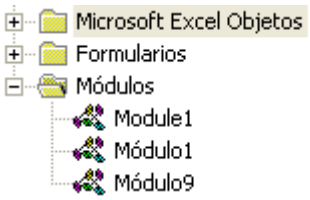
Coloco bp en la comparación y fuerzo el salto a que se ejecute, luego otra vez en el dialogo

Veo el efecto de un salto:



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

En 2003, es similar, la unica diferencia es que puedo guardarlo sin clave, en 2007, solo accedo a los modulos 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 .