# ESTUDIO DE PROTECCIONES BASICO PARA PRINCIPIANTES

(También llamado cracking)
Impartido por Ratón (Nivel principiante)

Nota
Cada capitulo ira acompañado de su crackme correspondiente. No facilitare páginas de donde bajarse herramientas ni enlaces a páginas de crackers, la intención es que busquéis en Internet todo lo necesario. Seguro que encontráis mas paginas de herramientas, tutoriales y utilidades relacionadas con este tema que las que yo pueda deciros.
Con esto solo quiero fomentar vuestro interés, además se que la búsqueda os proporcionara gratas sorpresas.
A todos un saludo.

## Capitulo 9

### Victima

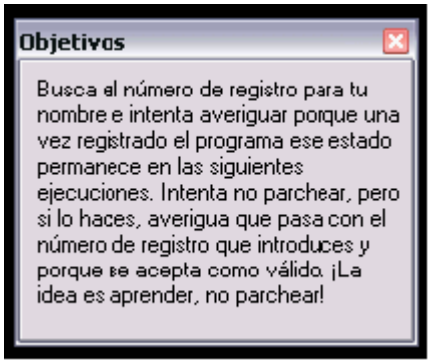
Crackme 6 de Joe Cracker

### Herramientas

Olly Debugger.
DeDe
Instinto

### Objetivo

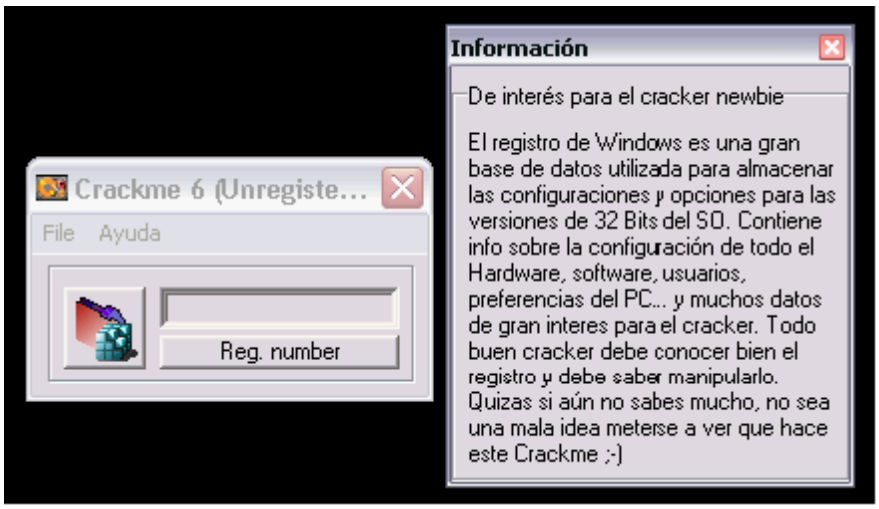
Lo deja claro Joe, sobran las palabras.




### Al ataque

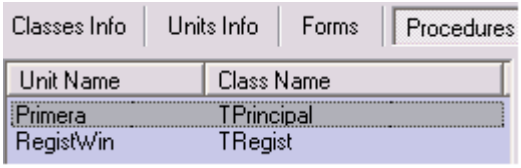
No es que tenga preferencia por Joe, pero de los muchos crackmes que he revisado creo que este también tiene su interés para el curso pues toca el tema del registro de Windows que era un tema que yo quería que se viera en el curso.

Vemos el crackme y el consejo de Joe



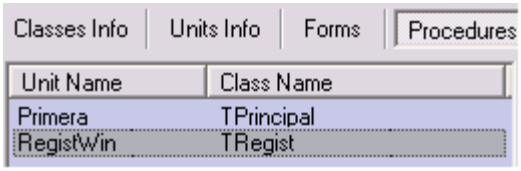

Pasemos a analizar el crackme
Hay un botón que dice reg number, lo pulso por curiosidad y me llama vago y me ordena que lo crackee


Analizo con Peid y me dice que esta en Delphi y sin comprimir/proteger
Lo cargo en DeDe
En procedures miro el TPrincipal

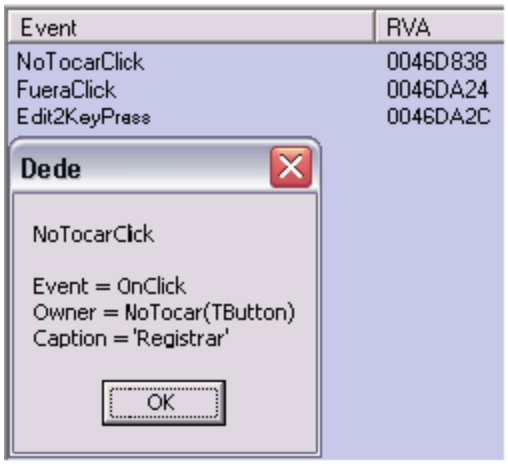



Me apunto esas dos direcciones que me interesan para lo que quiero mostraros en este capitulo

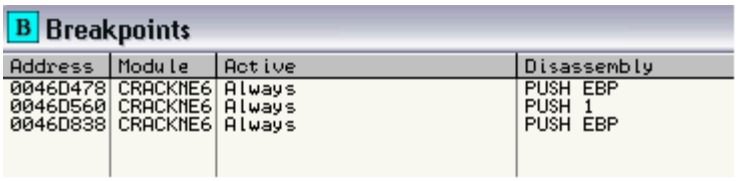

Miro después el TRegist



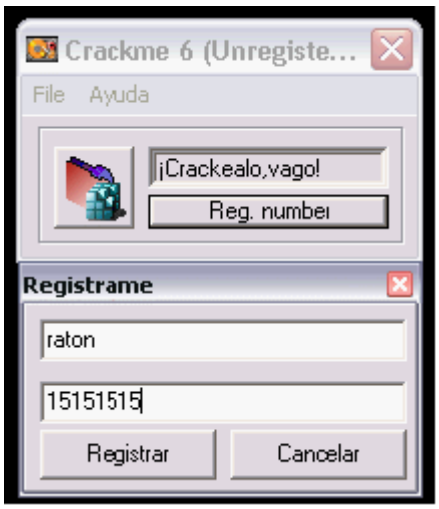

Apunto esa dirección (46D838) después de mirar que corresponde al botón con el Caption registrar




Voy a Olly y pongo BPs en las tres direcciones que apunte, las cuales corresponden a tres botones




Vamos a cazar el serial
En Olly F9 introduzco mi nombre y numero habituales




Al pulsar el botón para en uno de los BP, el que corresponde al botón con el Caption registrar

```
0046D837|   00          |DB 00
0046D838|. 55          |PUSH EBP                 | Boton registrar
0046D839|. 8BEC        |MOV EBP,ESP
```

Voy bajando poco a poco con F8, al llegar a 46D873 veo que aparece mi nombre en la ventana registers

```
0046D870|. 8B45 F4     |MOV EAX,DWORD PTR SS:[EBP-C]
0046D873|. E8 9468F9FF |CALL CRACKME6.0040410C   | En registers vemos "raton"
0046D878|. 8BD8        |MOV EBX,EAX
```

Sigo bajando (F8) y poco después veo mi numero en la ventana registers

```
0046D8DB|. 8B45 EC     |MOV EAX,DWORD PTR SS:[EBP-14]
0046D8DE|. E8 EDA5F9FF |CALL CRACKME6.00407ED0   | En registers vemos 15151515
0046D8E3|. 3BD8        |CMP EBX,EAX
```

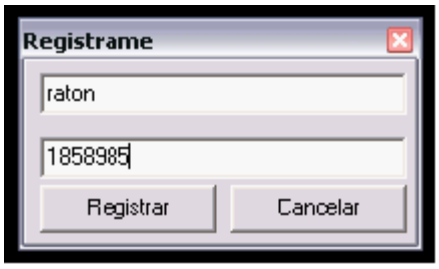
Justo debajo un CMP y un salto condicional, miro en el CMP y compara ebx con eax

```
0046D8DB|. 8B45 EC     |MOV EAX,DWORD PTR SS:[EBP-14]
0046D8DE|. E8 EDA5F9FF |CALL CRACKME6.00407ED0   | En registers vemos 15151515
0046D8E3|. 3BD8        |CMP EBX,EAX
0046D8E5|.v0F85 B5000000|JNZ CRACKME6.0046D9A0
0046D8EB|. B2 01       |MOV DL,1
EAX=00E7319B
EBX=001C5DA9
```

Voy a Olly a la command bar (plugin command bar) y escribo: ? valor de eax y pulso Enter
A la derecha me aparece los valores hex. dec y ascii, veo que el valor decimal corresponde a mi numero 15151515


Hago lo mismo con el valor de ebx y apunto el valor decimal que apareció 1858985


Pruebo a registrarme pues ya tengo un poco de experiencia y esto lo veo claro




Me pide reiniciar el crackme tened esto en cuenta a la hora de practicar con programas comerciales (si es que lo hacéis)
Al reiniciar pulso en reg number y aparece el serial que encontré y vemos arriba que el Caption del form (ventana) cambio de unregistered a registered

Crackme crackeado


Aunque lo tenemos crackeado haremos caso a Joe y lo analizaremos un poco mas
Carguémoslo en Olly de nuevo
Habíamos puesto al principio 3 BPs y solo utilizamos uno, el necesario para cazar el serial correcto, ahora veremos que hacen los otros dos

Pulsamos el botón reg number y Olly para en el BP que pusimos en este botón

```
0046D474  . C3          RETN
0046D475    8D40 00     LEA EAX,DWORD PTR DS:[EAX]
0046D478  . 55          PUSH EBP                        Boton Reg number
0046D479  . 8BEC        MOV EBP,ESP
0046D47B  . 33C9        XOR ECX,ECX
```

Bajamos con F8 y llegamos a este call 46D4C5 y entremos en el con F7

```
0046D4C0  . 33C9        XOR ECX,ECX
0046D4C2  . 8B45 FC     MOV EAX,DWORD PTR SS:[EBP-4]
0046D4C5  . E8 1EF5FBFF CALL CRACKME6.0042C9E8
0046D4CA  . 84C0        TEST AL,AL
0046D4CC    74 33       JE SHORT CRACKME6.0046D501
```

Dentro del call seguimos con F8 hasta llegar a 42CA61 donde vemos una llamada a la API RegOpenKeyExA

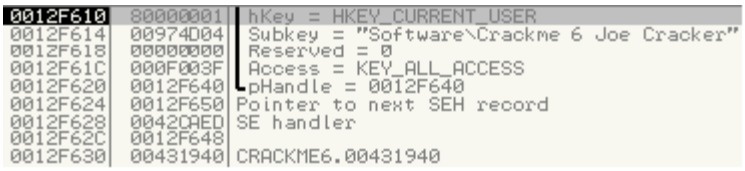
```
0042CA5A  . 8BC6        MOV EAX,ESI
0042CA5C  . E8 79FFFFFF CALL CRACKME6.0042C9D4
0042CA61  . 50          PUSH EAX                        hKey = HKEY_CURRENT_USER
0042CA62  . E8 D193FDFF CALL <JMP.&advapi32.RegOpenKeyExA>  RegOpenKeyExA
0042CA67  . 85C0        TEST EAX,EAX
0042CA69  . 0F9445 FE   SETE BYTE PTR SS:[EBP-2]
```

Miramos la ventana del Stack y vemos un par de frases que si alguna vez accedimos al registro de Windows nos deberían ser familiares

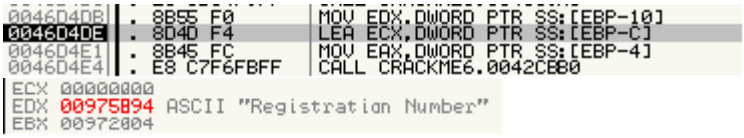
HKEY_CURRENT_USER

Y debajo

Software\Crackme 6 Joe Cracker

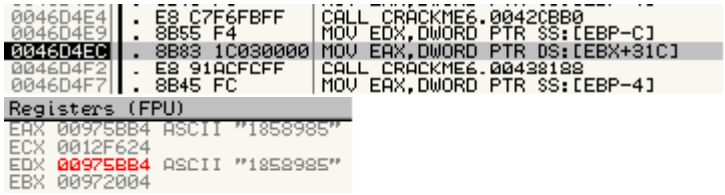



Continuamos con F8 y observando la ventana registers y el Stack (esto sobraría decirlo a esta alturas, pero bueno)
Vemos la frase Registration number




Ventana registers ->

Vemos el número de registro bueno



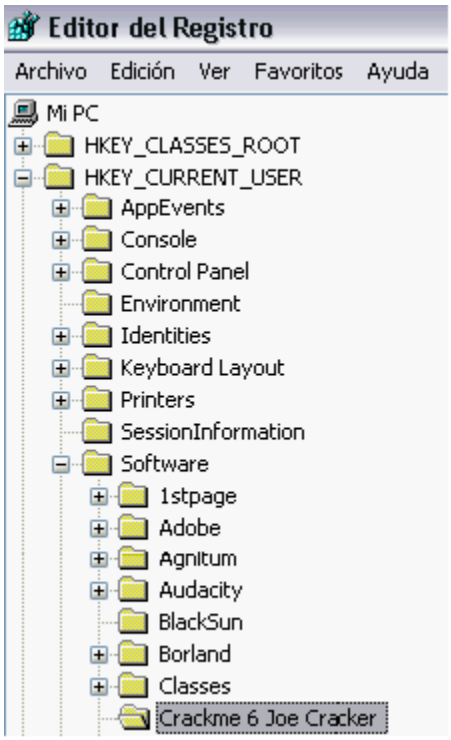

Ventana registers ->

En el Stack vemos también como van apareciendo poco a poco

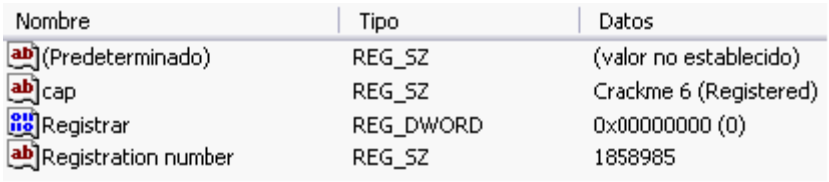

Bueno a estas alturas si llevamos un tiempo con el PC y somos curiosos (si sigues este curso una de dos: o eres curioso - que es para los que va destinado este curso - o eres un guarreras que lo único que te interesa es aprender esto para tener programas comerciales registrados por el morro y enseñarle a tus amiguetes lo que sabes hacer sin importarte un pimiento lo que pasa dentro de esa caja gris que compraste un día que hace ruiditos y tiene lucecitas ) ya habremos investigado y trasteado con el PC lo suficiente como para darnos cuenta que este programa interactúa de alguna manera con el registro de Windows.

Abramos el registro
Para los nuevos que no saben (y para los guarreras también, que yo no discrimino a nadie) en el escritorio pulsamos Inicio – Ejecutar y escribís regedit y aceptáis

Aparece el registro de Windows buscamos lo que habíamos visto en Olly
HKEY_CURRENT_USER\Software\Crackme 6 Joe Cracker




Pulsamos sobre el y vemos en la ventana de la derecha los valores de esa clave del registro

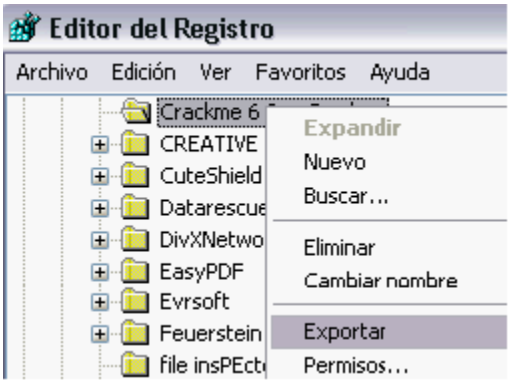


| Nombre | Tipo | Datos |
|---|---|---|
| (Predeterminado) | REG_SZ | (valor no establecido) |
| cap | REG_SZ | Crackme 6 (Registered) |
| Registrar | REG_DWORD | 0x00000000 (0) |
| Registration number | REG_SZ | 1858985 |

y observamos que las strings que vimos en Olly están aquí también, partiendo de lo cual deducimos que al introducir el numero de registro correcto el crackme escribió estos valores en el registro con el objeto de acudir a el cada vez que el crackme se ejecuta para tomar la información y ver si estamos registrados o no

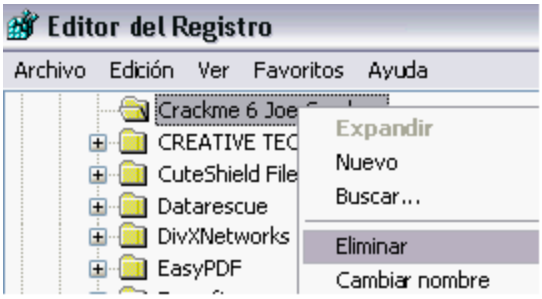

Cuidadin con lo que haremos a continuación
Tocar el registro de Windows puede ser perjudicial para la salud del PC si no sabemos lo que estamos haciendo

Primero guardaremos una copia de la información del crackme, lo haremos colocándonos sobre la carpeta y con botón derecho – Exportar
Le damos un nombre y lo guardamos




Lo que vamos a hacer ahora es lo que puede trastocar el PC si no tenemos cuidado o no sabemos lo que hacemos: vamos a eliminar esa clave y todos sus valores
Si seguís estos pasos que yo os doy no tendréis problemas, pero aseguraros bien de que lo hacéis bien antes de eliminar nada

Nos ponemos encima de la carpeta que nos interesa eliminar - de la cual hicimos antes una copia exportándola – picamos y vemos que este sombreada – aseguraros bien que solo se sombrea lo que queremos eliminar -
Con click derecho – Eliminar o pulsamos la tecla Supr o Del y aceptamos.

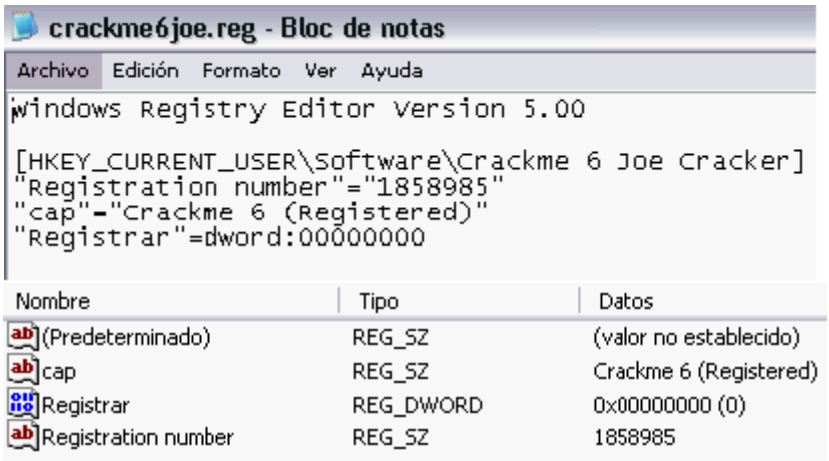



Eliminada la clave cerramos el registro y ejecutamos el crackme, si pulsamos reg number nos llama otra vez vagos ya que borramos la información del registro y al buscarla el crackme al ejecutarse no la encontró y volvió al estado de no registrado.


También observamos que si intentamos registrarnos con un serial cualquiera al pulsar el botón registrar no aparece la ventana pidiéndonos que reiniciemos el crackme, por tanto:

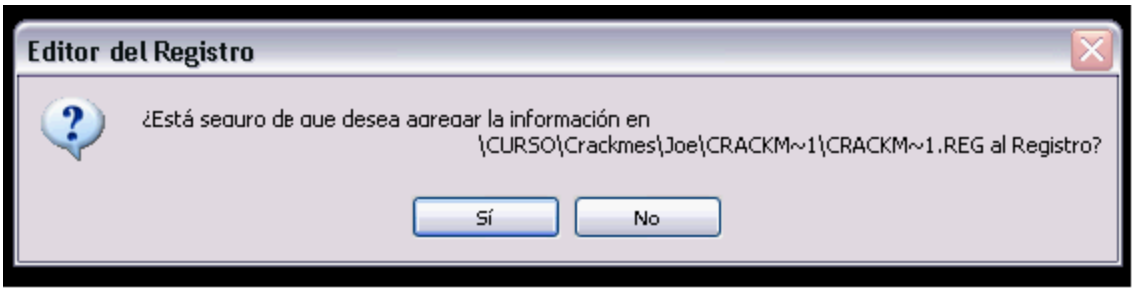
Si introducimos numero correcto – salta ventana de reinicio – escribe los valores en el registro
Si introducimos numero incorrecto – no salta ventana de reinicio – no escribe los valores en el registro

Prosigamos con el análisis
Abramos el archivo que exportamos del registro con la información del crackme en mi caso lo llame crackme6joe.reg, lo podéis ver en la imagen superior
Lo abrimos con botón derecho editar




Comparad

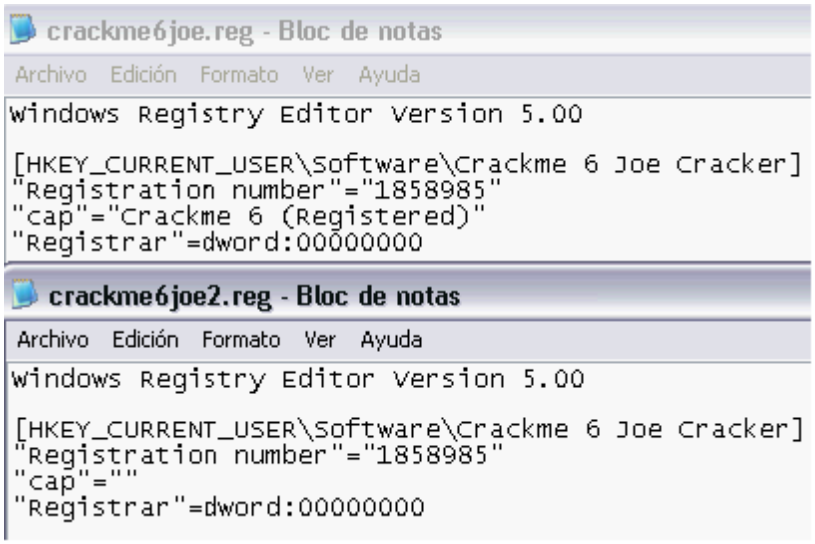
Ahora lo cerramos hacemos click izquierdo sobre el archivo y nos aparece esta ventana




Pulsamos Si para agregar esta información al registro
Ejecutamos el crackme y registrados otra vez

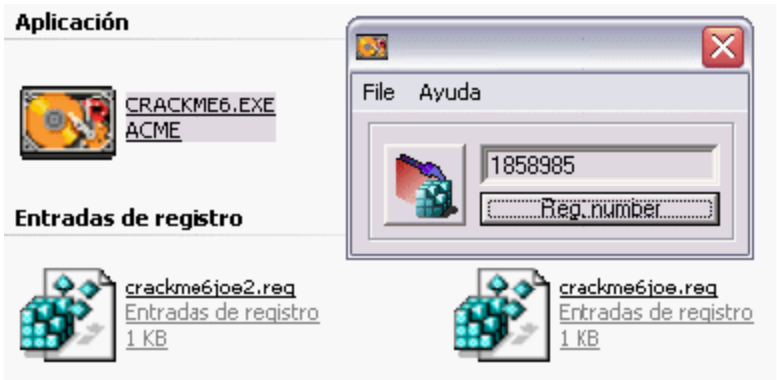
Vuelvo a repetir: tened mucho cuidado al manipular claves del registro


Ahora crearemos otro archivo de registro con los mismos valores pero dejaremos el campo cap vacío
Como podéis ver en la imagen se crean con el bloc de notas y al guardar se les da la extensión *.reg




Aquí podéis ver mis archivos: el que tiene los valores buenos (crackme6joe.reg) y el que he creado dejando el campo cap vacío (crackme6joe2.reg)

Si ejecuto crackme6joe2.reg y añado al registro la información de este archivo que he creado al ejecutar el crackme veo que falta el Caption de la ventana, falta registered
Por lo demás el crackme sigue registrado, solo lo hice como ejemplo para que vierais el resultado de manipular un valor en el registro.



El tercer botón

El tercero de los BPs que pusimos fue para que Olly parara al pulsar el botón 
Por tanto corremos el crackme con F9 y pulsamos ese botón
Olly para aquí y podemos ver que en esta parte del código se llama a ejecutar por medio de la orden ShellExecuteA al archivo regedit.exe
Si abrís la carpeta que esta en vuestro disco duro C llamada Windows entre los ejecutables podéis ver uno llamado regedit.exe
Cuando se pulsa este botón hace lo mismo que hicimos manualmente cuando fuimos a escritorio Inicio – Ejecutar y escribimos regedit y aceptamos

```
0046D560  . 6A 01         PUSH 1                          Llamada para abrir el registro de Windows
0046D562  . 6A 00         PUSH 0
0046D564  . 6A 00         PUSH 0
0046D566  . 68 80D54600   PUSH CRACKME6.0046D580           ASCII "C:\Windows\regedit.exe"
0046D56B  . 6A 00         PUSH 0
0046D56D  . A1 140C4700   MOV EAX,DWORD PTR DS:[470C14]
0046D572  . E8 BD13FDFF   CALL CRACKME6.0043E934
0046D577  . 50            PUSH EAX                        hWnd
0046D578  . E8 6F90FBFF   CALL <JMP.&shell32.ShellExecuteA>  ShellExecuteA
0046D57D  . C3            RETN
```

Joe lo incluyo por si alguno de nosotros novatos no teníamos idea de cómo acceder al registro.

Continuemos haciéndole los honores al crackme de Joe

Las APIs

Si miramos las Cracker notes podemos ver esto (entre otras muchas cosas)

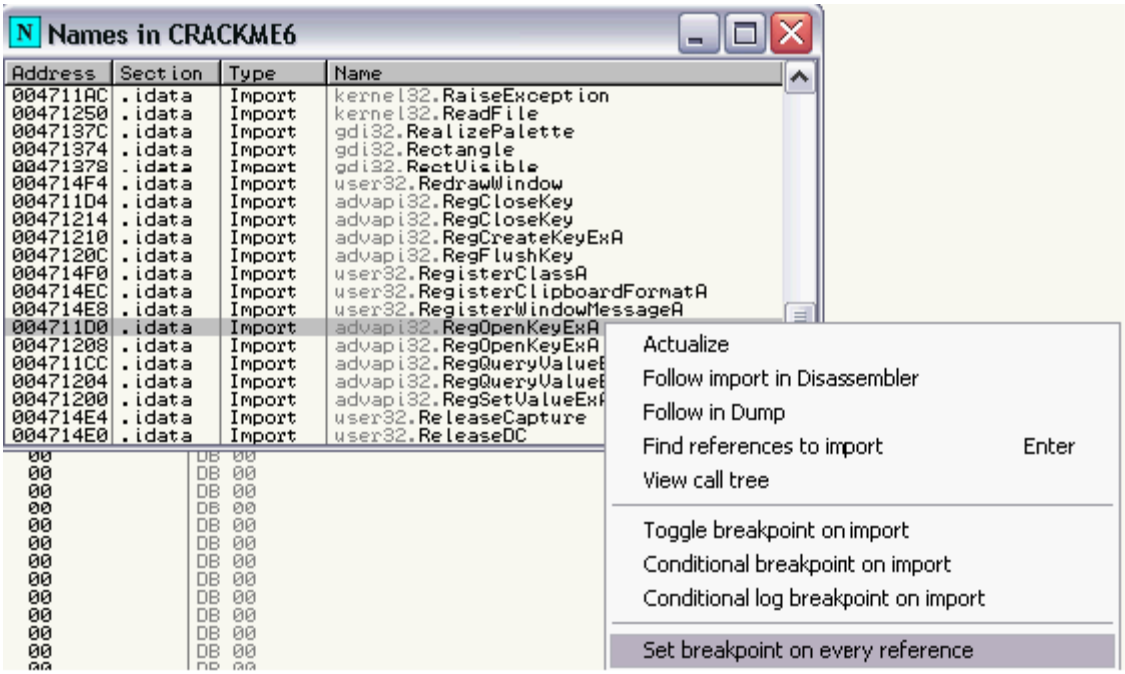
RegOpenKeyA / RegOpenKeyW

La función RegOpenKey abre la clave especificada

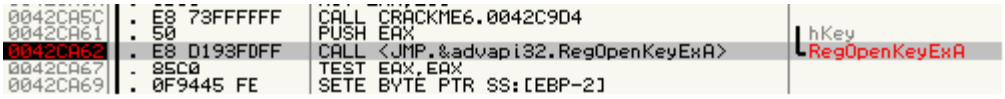
RegCreateKeyExA / RegCreateKeyExW

La función RegCreateKeyEx crea la clave especificada

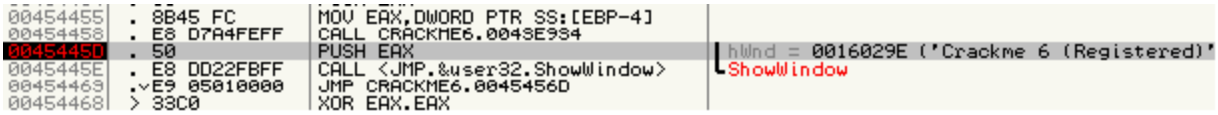
Abriremos el crackme registrado en el Olly y le quitaremos todos los BP que teníamos y pondremos BP en la llamada a la API RegOpenKeyA, la mas parecida es RegOpenKeyExA Control + N para hacer aparecer esta ventana y luego BP on every reference




F9 y después de parar y comprobar algunas claves del registro de Borland Delphi para aquí, si recordáis ya pasamos antes por esta zona cuando vimos que el crackme escribía en el registro

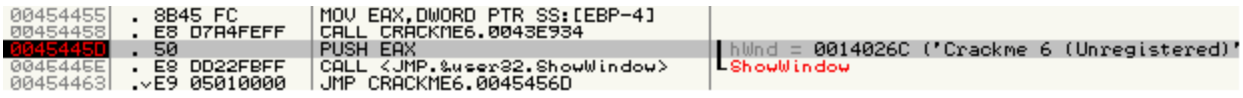



Seguimos con F8 y después de un rato llegamos aquí, vemos que ha terminado de comprobar y va a mostrar una ventana (ShowWindow) que es la principal del crackme como veis sombreado el caption es Crackme 6 registered




Comprobó nada mas arrancar el registro vio que existía la clave y nos saca la ventana principal con el cartelito registered.

Si volvemos a borrar la clave del registro parara en RegOpenKeyExA y al seguir con F8 llegaremos al mismo sitio pero con una ligera variación: Crackme 6 Unregistered




Pongamos un BP ahora en RegCreateKeyExA corramos el crackme y nos registramos con el numero

bueno al pulsar el botón parara en el BP pues al detectar el numero bueno procede a escribirlo en el registro

```
0042CA90  . E8 3FFFFFFF   CALL CRACKME6.0042C9D4
0042CA95  . 50            PUSH EAX                          hKey
0042CA96  . E8 8D93FDFF   CALL <JMP.&advapi32.RegCreateKeyExA>  RegCreateKeyExA
0042CA9B  . 85C0          TEST EAX,EAX
0042CA9D  . 0F9445 FE     SETE BYTE PTR SS:[EBP-2]
```

Stack

```
0012F248  0042CA9B  CALL to RegCreateKeyExA from CRACKME6.0042CA96
0012F24C  80000001  hKey = HKEY_CURRENT_USER
0012F250  00971FE0  Subkey = "Software\Crackme 6 Joe Cracker"
0012F254  00000000  Reserved = 0
0012F258  00000000  Class = NULL
0012F25C  00000000  Options = REG_OPTION_NON_VOLATILE
0012F260  000F003F  Access = KEY_ALL_ACCESS
0012F264  00000000  pSecurity = NULL
0012F268  0012F2BC  pHandle = 0012F28C
0012F26C  0012F2B4  pDisposition = 0012F284
0012F270  0012F29C  Pointer to next SEH record
0012F274  0042CAED  SE handler
```

Si miramos el Stack vemos la llamada a la creación de la clave del registro y el programa nos pedirá que reiniciemos volviendo a hacer lo mismo, pasara por RegOpenKeyExA y ahora al ver que estamos registrados evitara pasar por RegCreateKeyExA y nos mostrara de nuevo como registrados

```
00454455  . 8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
00454458  . E8 D7A4FEFF   CALL CRACKME6.0043E934
0045445D  . 50            PUSH EAX                          hWnd = 0016029E ('Crackme 6 (Registered)'
0045445E  . E8 DD22FBFF   CALL <JMP.&user32.ShowWindow>     ShowWindow
00454463  .v E9 05010000  JMP CRACKME6.0045456D
00454468  > 33C0          XOR EAX,EAX
```

Bien aunque parezca un poco lioso no lo es tanto es un ciclo que se repite y depende de si encuentra o no la clave en el registro de Windows  te da el resultado registrado / no registrado.

Que pasaría si cambiamos el valor del salto donde compara el numero de registro nuestro con el bueno ¿?
Cambiémoslo como en la imagen e introduzcamos nuestro número malo

```
0046D8DB  . 8B45 EC       MOV EAX,DWORD PTR SS:[EBP-14]     En registers vemos 15151515
0046D8DE  . E8 EDA5F9FF   CALL CRACKME6.00407ED0
0046D8E3  . 3BD8          CMP EBX,EAX
0046D8E5  .v 0F84 B5000000 JE CRACKME6.0046D9A0
0046D8EB  . B2 01         MOV DL,1
0046D8ED  . A1 E4C74200   MOV EAX,DWORD PTR DS:[42C7E4]
```

Hemos conseguido registrarnos con nuestro número con solo cambiar el valor del salto.

Fin del capitulo

Podéis tener algún problema con este crackme o haceros un lio al crear y eliminar las claves del registro, aseguraros de lo que hacéis, mirad bien si la parte del capitulo donde estáis leyendo requiere que el programa este registrado o no lo este y os evitareis liaros.
Lo mejor si te lías es dejarlo un rato y retomarlo cuando estemos frescos y desde el principio.

Gracias
A todas las personas que colaboran desde el foro de HackxCrack para llevar adelante el curso, tanto los que colaboran aportando sus conocimientos como complemento al curso como a los que postean sus dudas para que aprendamos todos y por supuesto a los moderadores del mismo
A todos los crackers y programadores de los cuales he aprendido y sigo aprendiendo.
A los creadores de crackmes
En especial y sin menospreciar a nadie a Ricardo Narvaja por su aportación y su trabajo sobre el estudio de las protecciones y sus tutoriales en castellano y a Makkakko por sus tutoriales con Olly Debugger (Recomendados 100%) y por supuesto a Shoulck por la ayuda desinteresada que me esta prestando a costa de algo tan preciado como su tiempo.
A ti que me estas leyendo.

Ratón Febrero 2004