(LECCION SESENTA Y UNO)

Introducción de Ricardo Narvaja: Mr. Gandalf está hecho una máquina de hacer tutes de calidad, otra muestra de ello es este tute, que es nuestra lección 61, una vez más. Le deseamos suerte en lo que está esperando, el sabe.

GRACIAS GANDALF

Programa: Kitchendraw 4.0

Download: www.scitechsoft.com

Protección: Trial de tiempo. Carga de horas a través de un código.

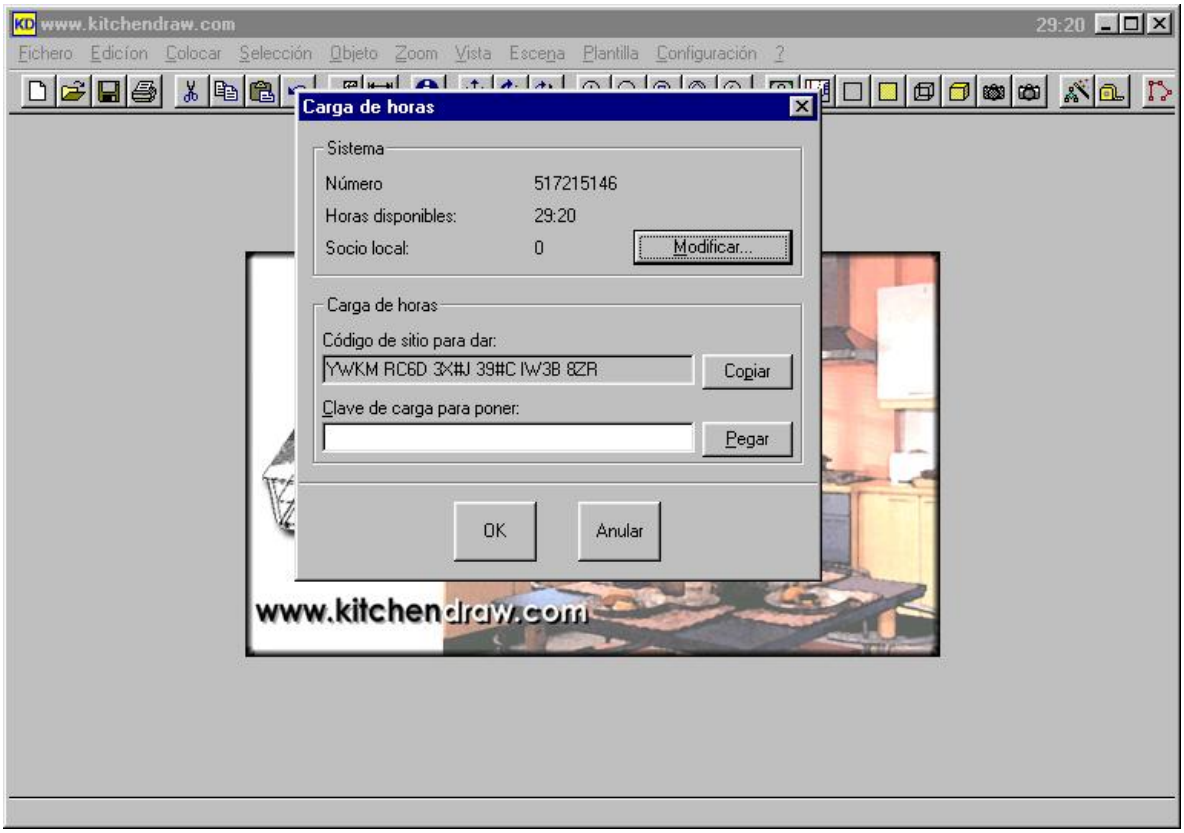
Dificultad: Fácil.

Herramientas: SoftICE 4.0. W32Dasm 8.93. TechFacts 98. Advanced Registry Tracer 1.43. Hiew 6.76.

Cracker: mR gANDALF.

Fecha: 8/02/2002

Introducción: Mientras espero una llamada importante solo tengo dos opciones: Volver a fumar o seguir "desguazando" bytes. Nada calma mis dendritas como cepillarme una protección. Como no me llame hoy el Cifuentes me va a dar un “jamacuco”.
En fin, que como anduvieron pidiendo el crack del kitchendraw este lo he instalado y la verdad que es facilón. El programa en sí se trata de un CAD de cocinas, no lo he probado mucho, todo sea dicho, pero skrapie sí y le gusta bastante. Cuando lo instalamos y lo ejecutamos por 1º vez nos aparece un contador de tiempo en la esquina sup-dcha que índica 29:55.
Son 30 las horas que este trial nos dejará usarlo y cada vez que lo usemos nos restará al menos 5 minutos. Tenemos una ventana que nos permite introducir un código para la recarga de tiempo que previamente habremos comprado por teléfono o por internet, algo parecido a las tarjetas de teléfono móvil.



Desguaze: El objetivo de este tutorial es averiguar como realiza el programa el conteo del tiempo y detenerlo. Este es el listado del TechFacts cuando el programa cuenta que nos quedan 29 horas y 20 minutos:

TechFacts 98 System Watch Report
02/08/02 04:17:00 pm

The following files were modified:(5)
c:\KD\Catalogs\catalogs.lst
c:\KD\Scenes\Key0202.log
c:\KD\Scenes\scenes.lst
c:\WINDOWS\APPLOG\APPLOG.ind
f:\kd\Space.ini

No changes made to INI file: C:\WINDOWS\WIN.INI

No changes made to INI file: C:\WINDOWS\SYSTEM.INI

Registry key values changed: (4)
HKEY_CLASSES_ROOT\G41512715
Value "517215146": binary data changed
HKEY_LOCAL_MACHINE\Software\CLASSES\G41512715
Value "517215146": binary data changed

Registry key values deleted: (1)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\TechFacts 98="F:\ARCHIVOS DE PROGRAMA\CRACK\HERRAMIENTAS\MONITORS - UTILIDADES ESPIA\TEKFCT98\TEKFCT98.EXE"

Pues bien, siguiendo el "método cartesiano" de las lecciones 58 y 59, es decir, haciendo uso intensivo de las aplicaciones ART (cuidado que cuelga el ordenador cuando corremos también el Sice, aunque usemos el FPLoader - aquí yo recomiendo la opción ASPAck/ASProtect más que la opción ART que incorpora el programa-) y TechFacts, llegamos a la conclusión de que es la clave HKEY_LOCAL_MACHINE\Software\CLASSES\G41512715 y el archivo catalogs.lst los que guardan el tiempo que nos queda. El archivo Key0202.log también debe ser importante, pues si lo borramos pasamos automáticamente a tiempo 0. Si guardamos una copia de la clave G41512715 y del archivo catalogs.lst al contar el programa 29:30, los podremos utilizar para volver a esta cifra siempre que queramos. En si podemos considerar ya la protección vencida, pues nos basta un cargador *.bat para vencer la limitación, pero nos sentimos curiosos y queremos llegar mas lejos.

... el método es el método (Perogrullo S. XXI dc) ...

Un listado del APYSpy muestra desde donde se lee esta clave:

```
 ============  Created by APIS32  v. 2.5  ============
70BE2CF8:RegOpenKeyExA()
70BE2CFE:RegOpenKeyExA = 2 (SHLWAPI.DLL)
70BE3003:RegOpenKeyExA()
70BE3009:RegOpenKeyExA = 2 (SHLWAPI.DLL)
7FCB1972:RegOpenKeyExA()
7FCB1978:RegOpenKeyExA = 0 (SHELL32.DLL)
7FCBD590:RegCreateKeyA(HANDLE:80000001,LPSTR:7FCBD618:"Software\Microsoft\Windows\CurrentVersion\Explorer",LPDATA:7FD381B4)
7FCBD592:RegCreateKeyA = 0 (SHELL32.DLL)
7FCBD59D:RegCreateKeyA(HANDLE:80000002,LPSTR:7FCBD618:"Software\Microsoft\Windows\CurrentVersion\Explorer",LPDATA:7FD381B0)
7FCBD59F:RegCreateKeyA = 0 (SHELL32.DLL)
7FE1F662:RegQueryValueExA()
7FE1F664:RegQueryValueExA = 2 (COMDLG32.DLL)
7FE1F67D:RegQueryValueExA()
7FE1F67F:RegQueryValueExA = 2 (COMDLG32.DLL)
7FE1F68C:RegCloseKey()
7FE1F692:RegCloseKey = 0 (COMDLG32.DLL)
00487210:RegCreateKeyA(HANDLE:80000002,LPSTR:0043DC6F:"Software\Laudrin\In Situ",LPDATA:0085FB4C)
00487215:RegCreateKeyA = 0 (DV.DLL)
004871B5:RegSetValueExA(HANDLE:C49FC390,LPSTR:0043DC87:"Busy",DWORD:0
```

0000000,DWORD:00000004,LPDATA:0085FB70,DWORD:00000004)
004871BA:RegSetValueExA = 0 (DV.DLL)
00487234:RegCloseKey()
00487239:RegCloseKey = 0 (DV.DLL)
004871CF:RegOpenKeyA(HANDLE:80000000,LPSTR:0085F37C:"G41512715",LPDATA:0085F32C)
004871D4:RegOpenKeyA = 0 (DV.DLL)
00487198:RegQueryValueExA()
0048719D:RegQueryValueExA = 0 (DV.DLL)
004871F5:RegCloseKey()
004871FA:RegCloseKey = 0 (DV.DLL)
004871CF:RegOpenKeyA(HANDLE:80000000,LPSTR:0085FA94:"G41512715",LPDATA:0085FA44)
004871D4:RegOpenKeyA = 0 (DV.DLL)
00487198:RegQueryValueExA()
0048719D:RegQueryValueExA = 0 (DV.DLL)
004871F5:RegCloseKey()
004871FA:RegCloseKey = 0 (DV.DLL)
004871CF:RegOpenKeyA(HANDLE:80000000,LPSTR:0085FA94:"G41512715",LPDATA:0085FA44)
004871D4:RegOpenKeyA = 0 (DV.DLL)
00487198:RegQueryValueExA()
0048719D:RegQueryValueExA = 0 (DV.DLL)
004871F5:RegCloseKey()
004871FA:RegCloseKey = 0 (DV.DLL)
00487210:RegCreateKeyA(HANDLE:80000000,LPSTR:0085FABC:"G41512715",LPDATA:0085FA4C)
00487215:RegCreateKeyA = 0 (DV.DLL)
004871B5:RegSetValueExA(HANDLE:C49FC390,LPSTR:0085FA94:"517215146",DWORD:00000000,DWORD:00000003,LPDATA:0085FA74,DWORD:00000020)
004871BA:RegSetValueExA = 0 (DV.DLL)
00487234:RegCloseKey()
00487239:RegCloseKey = 0 (DV.DLL)
004871CF:RegOpenKeyA(HANDLE:80000000,LPSTR:0085F998:"G41512715",LPDATA:0085F948)
004871D4:RegOpenKeyA = 0 (DV.DLL)
00487198:RegQueryValueExA()
0048719D:RegQueryValueExA = 0 (DV.DLL)
004871F5:RegCloseKey()
004871FA:RegCloseKey = 0 (DV.DLL)
004871CF:RegOpenKeyA(HANDLE:80000000,LPSTR:0085F820:"G41512715",LPDATA:0085F7D0)
004871D4:RegOpenKeyA = 0 (DV.DLL)
00487198:RegQueryValueExA()
0048719D:RegQueryValueExA = 0 (DV.DLL)
004871F5:RegCloseKey()
004871FA:RegCloseKey = 0 (DV.DLL)

Parece que es en 004871CF donde se abre la clave y en **0048719D** donde se lee. Sí ponemos un Bpx en 0048719D y traceamos un poquito (tratad bien a F10 que tiene que durarnos para otros tutes) llegamos a este trocito de código perteneciente a DV.dll:

```
004E820D E8E4970000          call 004F19F6
:004E8212 83C408             add esp, 00000008
:004E8215 8B45E4             mov eax, dword ptr [ebp-1C]
:004E8218 8B55EC             mov edx, dword ptr [ebp-14]
:004E821B 03C2               add eax, edx
:004E821D 8B4DE8             mov ecx, dword ptr [ebp-18]
:004E8220 8B55F0             mov edx, dword ptr [ebp-10]
:004E8223 03CA               add ecx, edx <- ecx=Nº de usos gastados
:004E8225 2BC1               sub eax, ecx <- eax=Nº usos restantes.
:004E8227 8BE5               mov esp, ebp
:004E8229 5D                 pop ebp
:004E822A C3                 ret
```

Imagínense las posibilidades que se nos ofrecen... por cierto, entren en DV.dll poniendo un bpx en hmencpy antes de pulsar ok en la ventana de introducción de códigos de recarga y tengan en cuenta que en el Sice la dirección es 558225 en vez de 004E8225.

El remate final lo dejo a su gusto, crackers.

mR gANDALF

(LECCION SESENTA Y DOS)

Programa: Kitchendraw 4.0

Download: http://www.KITCHENDRAW.COM/ESP

Objetivo: Habilitar la "producción de imágenes fotorealistas".

Dificultad: Si yo lo he hecho, facilísimo.

Herramientas: TRW2K (o Softice). W32Dasm 8.93. Editor Hexa (p.ej.: Ultraedit). R!SC's Process Patcher v1.5.1.

Cracker: Scrapie.

Fecha: 15/02/2002

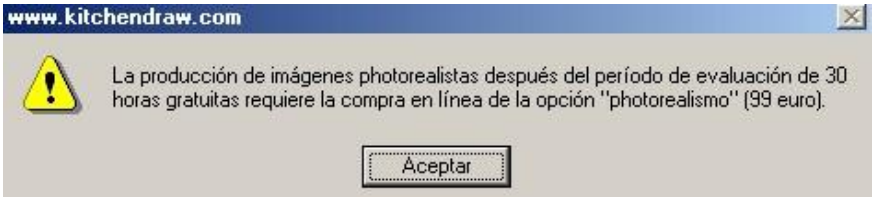
Introducción:

Después de la Lección 61, hice el crack (gracias a mR gANDALF) para acabar con la limitación de tiempo de este programa, y como no lo uso para nada, creí que ya estaba totalmente crackeado. Pero, debido al aburrimiento, un día me puse a enredar con él y descubrí que la opción de "producción de imágenes fotorealistas" no estaba habilitada, y sirve para poder ver el diseño de la cocina en una especie de realidad virtual aunque un poco más triste (yo con mi tarjeta de video de 8Mb casi ni lo veo).

Pero ¿Cómo pueden cobrarte 3 Euros por hora y además exigir 99 Euros más?. ¡¡Increíble!! ¡¡¡Tenemos que reventarlo totalmente, se lo merece!!! (Aunque exclusivamente con fines educativos, evidentemente)

Re-Desguace:

¡Al ataqueee! Ejecutamos el programa y abrimos el proyecto de ejemplo que adjunta. Pulsamos sobre un icono que es como una cámara fotográfica y nos aparece este mensaje:



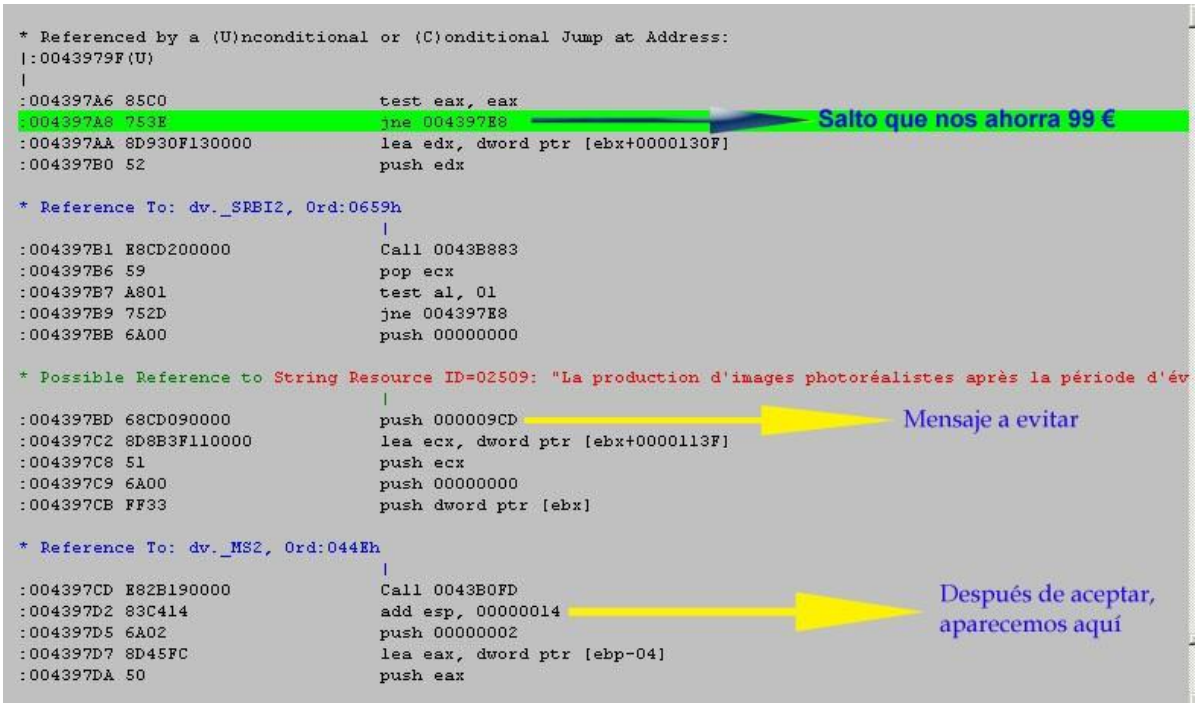
Desensamblamos con el W32Dasm, y en String Referentes no veo nada que se le parezca (aquí hablo en 1ª persona a propósito, por motivos que veremos más abajo). Es hora de recurrir al TRW2K…

Antes de darle, otra vez, a  probamos con bpx messagebox y messageboxexa, pero en ninguno de los dos salta el "debugger" al aparecer la ventana, como casi nunca falla lo intentaremos esta vez con bpx hmemcpy y … nada tampoco funciona. Pensemos un poco… el programa tiene que comprobar si hemos comprado el producto o no, y o accede al registro (vimos en la gran primera parte de esta lección, que se cambian algunas "cosas") o lo comprueba de algún archivo escondido en las entrañas de nuestro PC.

Lo intentaremos con el registro, poniendo bpx RegQueryValue (nunca lo había usado) y procedemos…

(***Técnica de La Marcha Atrás***)

¡Si! Esta vez ha saltado el TRW, aparece en el Kernell, quitamos el bp (bc *).Pulsamos F12 hasta que aparece el "molesto cartelito". Aceptamos y vuelve a saltar el TRW, esta vez aparece en User, clavamos el dedo en F10 (cuidado los que usen Softice) hasta que volvamos al código del programa (KD). Miramos donde hemos ido a parar y estamos en 004397D2. Usando *la técnica de mirar lo que hay encima*, nos pueden parecer interesantes algunas Calls y algunos saltos cercanos, pero como la zona "conflictiva" ya la hemos localizado, para verlo todo más cómodos volvemos al W32Dasm, buscamos 004397D2:



Ohh!! El mismo mensaje de “chico malo” (pero en francés) está ahí y en String Referentes antes no había visto nada, lo compruebo y está de las primeras. ¡Dolorrrrrrrr! Pero como aquí lo que intentamos es aprender no importa, porque gracias a no verlo he usado un bpx que hasta ahora no había empleado, y puede sernos útil para crackear programas donde no nos lo ponen tan fácil. Seguimos.
La imagen lo aclara todo, los saltos que evitan el mensaje señalan hacia la misma dirección o sea que parcheando cualquiera de ellos funcionará igual (esto lo sé porque lo he comprobado con el debugger, jeje).

Con un editor hexadecimal cambiamos p. ej. el primer salto por 74 o EB (para que siempre salte), y ejecutamos el programa… Oh!!! Me estoy empezando a enfadar con los programadores de este “engendro”. El programa no funciona y da error, debe tener algún tipo de protección contra modificaciones en su código, pero siendo tan fácil de crackear se molestan poniendo esto?…

Tengo que borrarlo e instalarlo otra vez porque aunque hice una copia del original, esta también ha dejado de funcionar.
La solución sería parchearlo en memoria: crearemos un loader con el R!SC's Process Patcher. Este es el script:

```
; KitchenDraw 4 (Produccion de imagen fotorealista)99 Euros menos ;-)
; Loader para Poder usar la Produccion de imagen fotorealista
; Esta opción sirve para poder ver el diseño en 3D con movimiento

F=kd.EXE:                       ; VICTIMA
O=Loader_KitchenDraw.exe:               ; ASESINO
P=4397a8/75/74:                 ; Salta siempre, por favor
$ ;end of script                        ; Fin
```

Lo probamos y funciona. ¡Lo hemos reventado, y además se lo merece! (Doble alegría) ☺

Scrapie

Saludos a todos los miembros de la lista.

PD: Gracias a Ricardo y mR gANDALf por sus fabulosas lecciones, perdón a mR gANDALf por copiar (también) la plantilla que usa para hacer sus magníficos tutes.

PD2: Este es mi primer tute, y no hace mucho que me incorporé a la lista por lo que pido perdón si hay algún error, ya que me doy cuenta cuando leo las lecciones de Ricardo y los demás, de lo poco que sé y de lo mucho que me queda por aprender.

(LECCION SESENTA Y DOS)

Programa: EasyPDF 1.6.1

Download: www.visagesoft.com

Protección: VisualProtect 1.1. Trial de 20 días. La versión demo imprime un texto y un logotipo sobre el documento creado.

Dificultad: Mediana.

Herramientas: SoftICE 4.0. Dede 2.51. W32Dasm 8.93. Hiew 6.76. Princess Sandy Patcher 1.0.

Cracker: mR gANDALF.

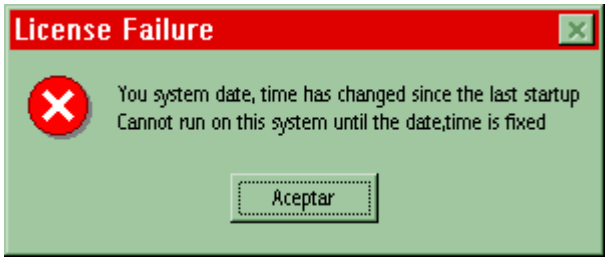
Fecha: 16/02/2002

Introducción: El Cifuentes no trajo buenas noticias. Pero bueno, que se le va hacer. En este, mi octavo tutorial, quiero atraer su atención sobre un bonito programa llamado EasyPDF. Este programa sirve para convertir nuestros textos al formato PDF, pesa mucho menos que el Adobe Acrobat 4.0 y es muy sencillo de manejar. Tiene una interesante protección que consta de dos elementos. Por un lado el Visual Protect, compresor de la misma casa que el EasyPDF y que ya fue diseccionado en un mas que interesante tutorial de Kuato Thor que les recomiendo encarecidamente que lean http://karpoff.topcities.com/tutoriales/archivos/visualp_k.htm. Fue Skrapie quien me llamo la atención sobre este tutorial. Por otra parte, la versión demo realiza una especie de sobreimpresión del logotipo de visagesoft sobre nuestro documento y además añade en la cabecera unas palabritas en estruendoso color rojo animándonos a registrarnos. Todo un detallito para los que buscaban como animar sus textos. Para registrarnos debemos ponernos en contacto con la compañía que suponemos nos remite un key file con el que se solucionan estos inconvenientes. Pero nosotros vamos a ver una ruta alternativa a este key file que resulta mucho mas ... "interesante".

Desguaze: Si echamos un vistazo con FileINspector veremos que es Visual Protect 1.1. ¿Y que demonio es esto?. Pues es un sistema de protección que consiste en una nag inicial que nos informa de que estamos en versión demo, nos dice los días que nos faltan y nos muestra un botón Buy para registrarnos a través de Internet, un botón OK para continuar y un botón QUIT para salir. Además esta protección incluye la compresión del ejecutable y dll`s. Todo este meollo se realiza desde vp.dll que tiene un call que llama a la nag y vuelve con un numero en EAX que representa el botón pulsado. Si cambiamos este call por un mov eax,1 el programa no llama a la nag, se comporta siempre como si hubiésemos pulsado Ok, y además tiene el efecto de que no reconoce el vencimiento del trial. Este cambio puede realizarse con el Princess Sandy Loader de Eminence (protools).

... algunos restos del Visual Protect ...

Hasta aquí un breve resumen del tute de Kuato Thor. Pero si prueban a retrasar el reloj un mes, p.ej, verán que el programa reconoce que le han toqueteado el reloj, ya que seguramente guarde la fecha de instalación en el registro, y nos muestra un molesto cartelito.



Este cartelito nos aparece aunque hallamos cargado el programa con un loader evitando el call anterior. De hecho aparece antes de ese Call y es un messageboxexa. Traceando un poquito y cambiando alternativamente la fecha del sistema, vemos que:

```
:017C6581 8B151CB97C01          mov edx, dword ptr [017CB91C] <- Flag
:017C6587 3B02                cmp eax, dword ptr [edx]   <- EAX=Flag?
:017C6589 0F849C090000          je 017C6F2B          <- salta a cartel
:017C658F A164BC7C01            mov eax, dword ptr [017CBC64]
:017C6594 8B00                mov eax, dword ptr [eax]
:017C6596 8B1568BB7C01          mov edx, dword ptr [017CBB68]
:017C659C 3B02                cmp eax, dword ptr [edx]
:017C659E 0F84D8080000          je 017C6E7C
:017C65A4 A164BC7C01            mov eax, dword ptr [017CBC64]
:017C65A9 8B00                mov eax, dword ptr [eax]
:017C65AB 8B1504BC7C01          mov edx, dword ptr [017CBC04]
:017C65B1 3B02                cmp eax, dword ptr [edx]
:017C65B3 0F84CB090000          je 017C6F84
:017C65B9 A164BC7C01            mov eax, dword ptr [017CBC64]
:017C65BE 8B00                mov eax, dword ptr [eax]
:017C65C0 8B15BCBA7C01          mov edx, dword ptr [017CBABC] <- Flag
:017C65C6 3B02                cmp eax, dword ptr [edx] <- EAX=Flag?
:017C65C8 7432                je 017C65FC          <- evita cartel
:017C65CA A164BC7C01            mov eax, dword ptr [017CBC64]
:017C65CF 8B00                mov eax, dword ptr [eax]
:017C65D1 8B151CBB7C01          mov edx, dword ptr [017CBB1C]
:017C65D7 3B02                cmp eax, dword ptr [edx]
```

Similares saltos presenta en 17C66A6 y 17C6793. “Corrigiéndolos” evitamos que si tenemos que mover el reloj para atrás por alguna razón nos salga el cartelito.

... la segunda parte: ese molesto logotipo en nuestros PDF`s ...

Fíjense que feo cartel nos parece utilizando la versión demo.

Fíjense además que en la cabecera aparece una frase de 3 líneas sobre las ventajas de registrarse (eliminación de cartelito incluida, claro esta). Indudablemente, durante el proceso de creación de nuestro PDF se ha sobreimpreso “esto”.
Antes de apretar Ctrl-D como posesos pensemos un poco. Efectivamente se trata de Delphi y en estos casos olvídense de hacer nada sin el Dede. Tracear a lo bruto solo nos lleva a desgastar F10 y volvernos locos. Pero como Dede no admite empacados lo mejor es dumpear con ProcDump seleccionando de la ventana de procesos activos easypdf.exe (clic derecho y seleccionen dump full).

El dumpeado original lo editan con PE Editor, hacen dumpfix (lección 34) arreglan la tabla de secciones para que permita usar el Wdasm (E0000020) y lo cargan en el Dede. Aquí vallan a Procedures y elijan Main. Échenle un vistazo, sin duda se trata del procedimiento que crea la pagina principal, la que contiene el botoncito que al apretarlo nos crea nuestro PDF. Verán que hay uno que se llama DoPDFExecute, lo cual resulta mas que sugerente. Si ponemos un Bpx al comienzo del procedure, ósea en 68b144, veremos que nada mas tocar el botón caemos en el Sice.

Aquí el procedimiento lógico es ponerse a mirar saltos condicionales y probar a cambiarlos, a ver que pasa, igual que en el Winomega y en tantos otros. Ya destaca desde el principio la escasez de estos saltos, pero cuando nos ponemos a cambiarlos vemos que efectivamente así no vamos a ningún lado. Probemos a buscar algún elemento de la cadena que sobreimprime, por ejemplo evaluation, con el comando S 0 l FFFFFFFF ´evaluatión´. Ya el primer hallazgo es significativo y no hay que seguir buscando más, caemos en plena cadena. Ponemos un bpmd en un punto de la misma, ya que con los bpr se cuelga la maquina (creo que forma parte de la protección), y le damos a F5. Pulsamos F12 para volver a vp-dll y terminamos cayendo en un sitio como este:

```
:0068D04D E8EAD2FAFF          call 0063A33C <- Escribe el texto de evaluación.
:0068D052 6800000040          push 40000000
:0068D057 6834D26800          push 0068D234
:0068D05C 8B45F4              mov eax, dword ptr [ebp-0C]
:0068D05F 50                  push eax
:0068D060 E863D2FAFF          call 0063A2C8 <- Pone rojo el Logo
:0068D065 6800004842          push 42480000
:0068D06A 8B45F0              mov eax, dword ptr [ebp-10]
:0068D06D 50                  push eax
:0068D06E 8B45F4              mov eax, dword ptr [ebp-0C]
:0068D071 50                  push eax
:0068D072 E8B5D2FAFF          call 0063A32C <- da tamaño grande al logo
:0068D077 6A00                push 00000000
:0068D079 6A00                push 00000000
:0068D07B 6A00                push 00000000
:0068D07D 680000803F          push 3F800000
:0068D082 6830D16800          push 0068D130
:0068D087 6844D26800          push 0068D244
:0068D08C 8B45F4              mov eax, dword ptr [ebp-0C]
:0068D08F 50                  push eax
:0068D090 E8EFD2FAFF          call 0063A384 <- etc…
:0068D095 6A00                push 00000000
:0068D097 68C9C8483F          push 3F48C8C9
:0068D09C 68C9C8483F          push 3F48C8C9
:0068D0A1 68C9C8483F          push 3F48C8C9
:0068D0A6 6830D16800          push 0068D130
:0068D0AB 6834D16800          push 0068D134
:0068D0B0 8B45F4              mov eax, dword ptr [ebp-0C]
:0068D0B3 50                  push eax
:0068D0B4 E8CBD2FAFF          call 0063A384
:0068D0B9 683CD16800          push 0068D13C
:0068D0BE 6840D16800          push 0068D140
:0068D0C3 DD45E8              fld qword ptr [ebp-18]
:0068D0C6 D8354CD26800        fdiv dword ptr [0068D24C]
:0068D0CC 83C4FC              add esp, FFFFFFFC
:0068D0CF D91C24              fstp dword ptr [esp]
:0068D0D2 9B                  wait
```

```
:0068D0D3 DD45E0              fld qword ptr [ebp-20]
:0068D0D6 83C4FC              add esp, FFFFFFFC
:0068D0D9 D91C24              fstp dword ptr [esp]
:0068D0DC 9B                  wait
:0068D0DD DD45E8              fld qword ptr [ebp-18]
:0068D0E0 D83550D26800        fdiv dword ptr [0068D250]
:0068D0E6 83C4FC              add esp, FFFFFFFC
:0068D0E9 D91C24              fstp dword ptr [esp]
:0068D0EC 9B                  wait
:0068D0ED 6A00                push 00000000
:0068D0EF 6854D26800          push 0068D254
:0068D0F4 8B45F4              mov eax, dword ptr [ebp-0C]
:0068D0F7 50                  push eax
:0068D0F8 E83FD2FAFF          call 0063A33C
:0068D0FD 6A00                push 00000000
:0068D0FF 6834D26800          push 0068D234
:0068D104 8B45F4              mov eax, dword ptr [ebp-0C]
:0068D107 50                  push eax
:0068D108 E8BBD1FAFF          call 0063A2C8
:0068D10D 8B45F4              mov eax, dword ptr [ebp-0C]
:0068D110 E87FD1FAFF          call 0063A294

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0068CF56(C) <- Aqui viene el salto que evita el "marcado" del texto.
|
:0068D115 8BE5                mov esp, ebp
:0068D117 5D                  pop ebp
:0068D118 C21000              ret 0010
```

Con esto queda limpia la protección. Puede hacerse un bonito loader con el Princess Sandy patcher.

Hasta la proxima... o nó, quien sabe?

PD: Agradecimientos en especial para Ricardo, a quién estimo más cada día.

mR gANDALF

(LECCION SESENTA Y TRES)

Introducción de Ricardo Narvaja: A pesar de que estamos de lleno metidos con el nuevo curso, nos siguen llegando colaboraciones de amigos, esta es de un amigo (JIKI) de 15 años, que hizo su primer tute y se lo agradecemos mucho, lo colocamos como LECCION 63 del curso viejo.

GRANDE AMIGO JIKI.

Programa: Bustout! Versión 2.0

Tipo: Juego

Protección: Solo te deja jugar 3 pistas

Herramientas: TRW; w32dasm; hex workshop; language 2000; ProcDump.

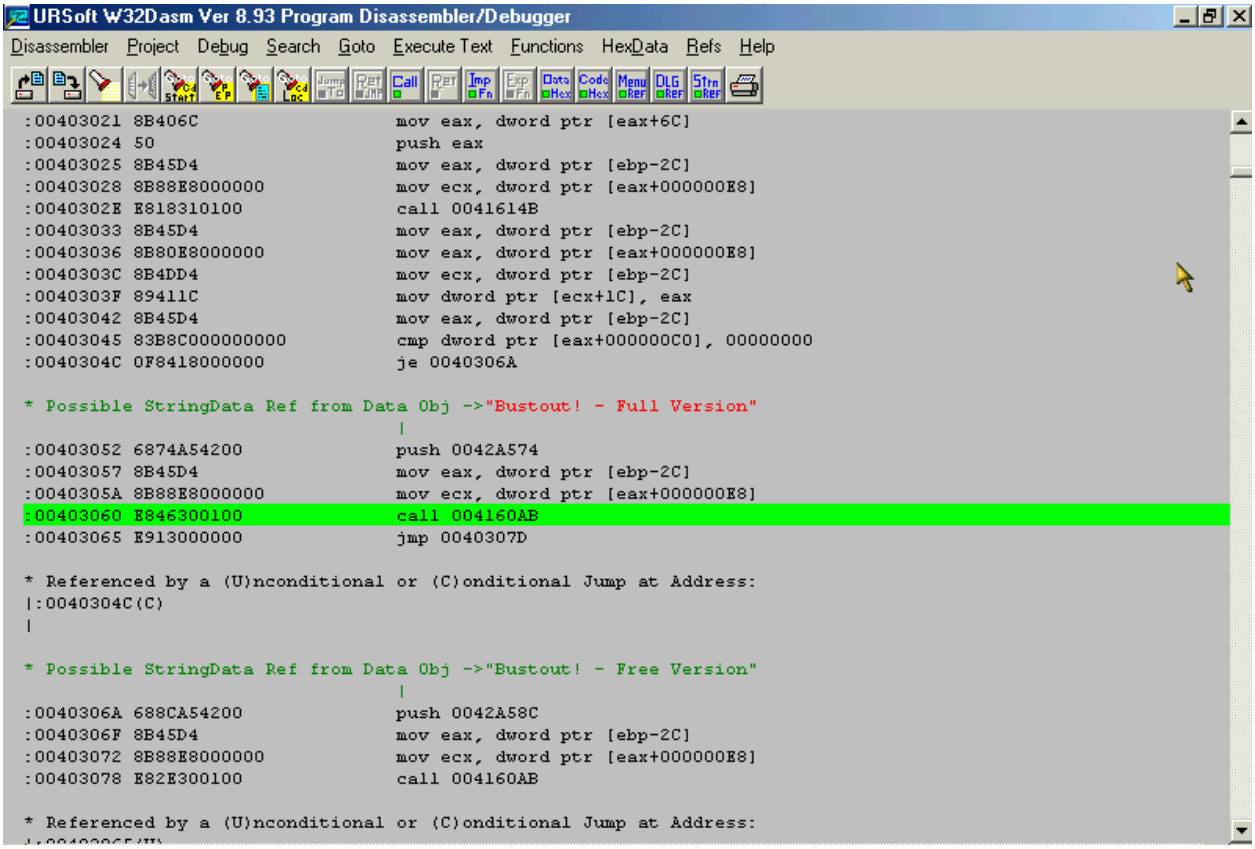
Cracker (si se me puede llamar así): JIKI

Introducción...

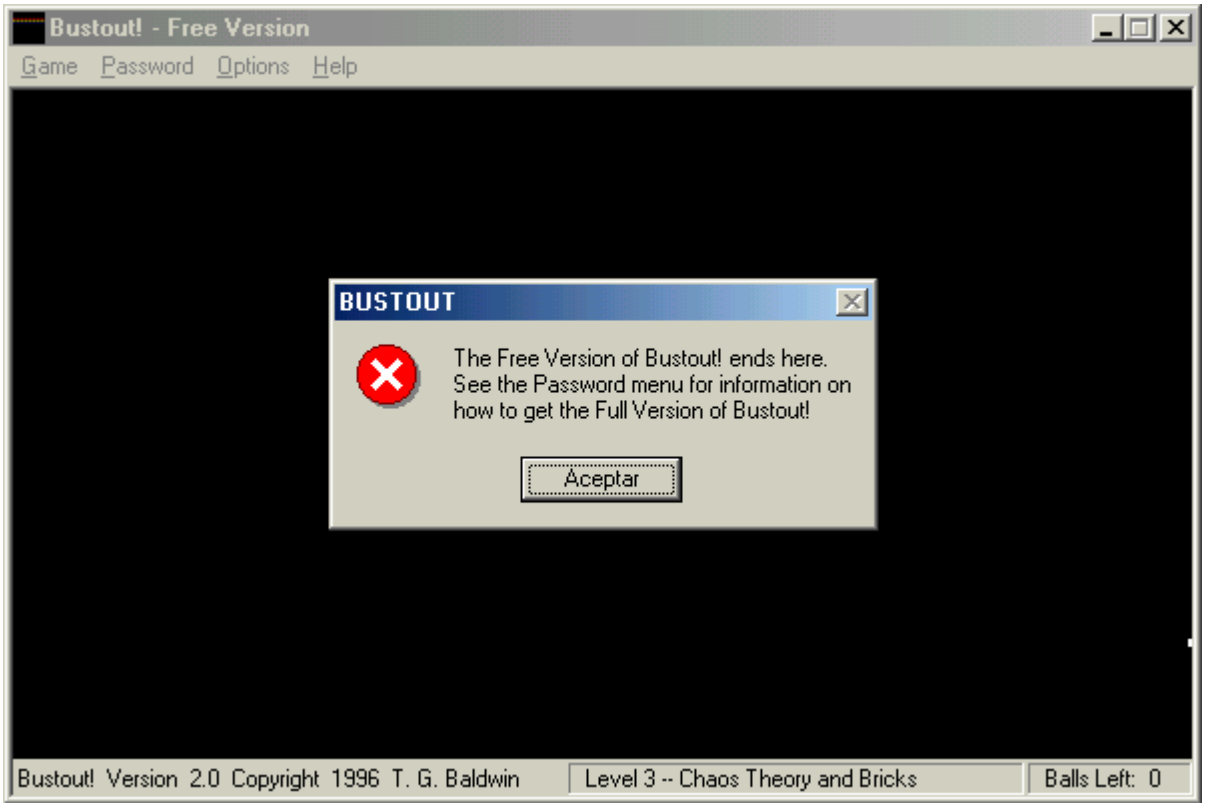
Ya que todos están escribiendo algún tute es hora de que yo haga uno. Este juego es bastante viejo, pero a mí me encanta y seguro que a muchos de ustedes también les va a gustar. Es un juego que te ofrece la posibilidad de registrarte metiendo un serial, pero ese trabajo se lo dejaremos a un cracker con más experiencia.

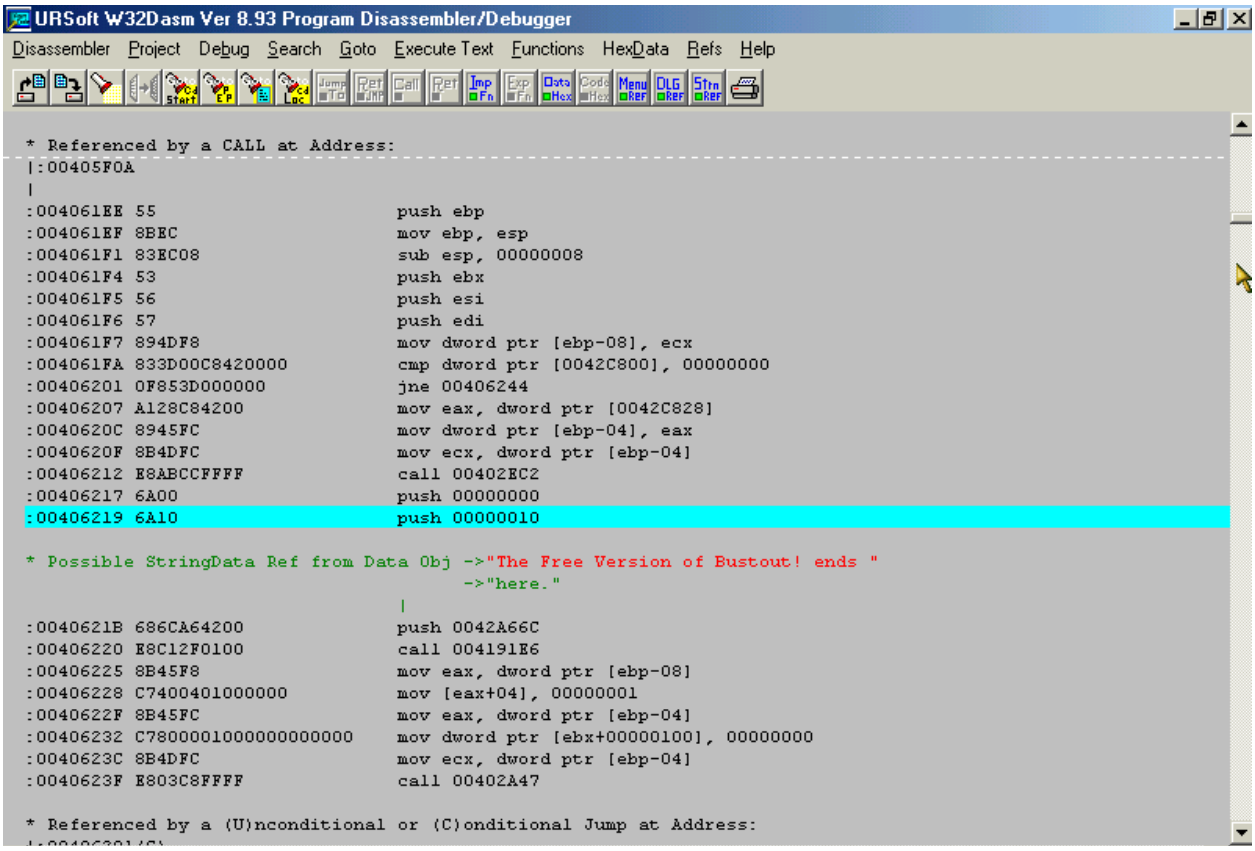
Pos parto...
Abrimos el juego con el Language 2000 y vemos que no está comprimido y está hecho en Visual C++. Paso siguiente abrimos el ProcDump, vamos a PE EDITOR, seleccionamos el nombre del juego y hacemos clic en abrir. Ni bien apretamos abrir nos saldrá una ventana en la cual hacemos un clic donde dice SECTIONS. Luego procedemos a hacer clic derecho en .data y ponemos edit section y en donde dice sections characteristics cambiamos de C0000040 a E0000020. Hacemos lo mismo con el .idata.

Al ataque...
Abrimos el W32Dasm y desensamblamos el juego. Una vez abierto vamos a String Data Referentes y buscamos Free versión. Miren la sorpresa que debajo de Free versión está Full versión. Bueno ahí vamos (a full versión). Hacemos 2 clicks y vemos que para llegar ahí nos manda desde un salto condicional. Anotamos esa dirección en un papel. Volvemos a String data referentes y hacemos de nuevo 2 clicks en Full versión. Ahora vemos que es desde otra dirección de donde salta; la anotamos. Volvemos a hacer lo mismo solo que esta vez vemos otra cosa:



Ahí podemos ver que en 40304c hay un salto condicional que si nos registramos nos manda a Full versión, y si no a free versión. Anotamos eso en un papel y listo. Ahora vamos al TRW y ponemos bpx en todos los saltos que teníamos (40174f, 4018c5 y 40304c) cargamos y vemos en cuál para. Paró en el tercero (40304c). O sea que vamos al Hex Workshop y cambiamos ese 0f8418000000 por 909090909090.
Entramos en el Bustout! Y bingo!!! Full Versión. Bueno, jugamos un rato, y justo nuestra madre nos llama para comer ponemos pausa (click derecho) y vemos que ese Full Versión pasó a Free Versión (paused) ¿qué pasa acá?, bueno, que no cunda el pánico. Cuando terminamos de comer volvemos y echamos un vistazo en las String Data Referentes a ver qué pasa con Free Versión (Paused). Vemos que es llamada desde 40176e. Anotamos esa dirección vamos al Hex Workshop y cambiamos ese 0f8412000000 por 909090909090. Abrimos el juego ponemos pausa y... NO PASA NADA!!! SIGUE EN FULL VERSION!!!, sacamos la pausa para seguir jugando y... #$%"& SE CAMBIO A FREE VERSION!!!. Bueno, como yo soy muy haragán decidí buscarle otra salida. Empecé a jugar el juego y al pasar la tercera pista apareció un cartel que decía algo parecido a: "The Free versión of Bustout! Ends here" y algunas cosas más. Bueno, vamos al W32Dasm a buscar eso. Miramos un poco y casi al final lo encontramos. Hacemos 2 clicks y caemos aquí:


Bustout! - Free Version
Game Password Options Help
BUSTOUT
The Free Version of Bustout! ends here.
See the Password menu for information on
how to get the Full Version of Bustout!
Aceptar
Bustout! Version 2.0 Copyright 1996 T. G. Baldwin
Level 3 -- Chaos Theory and Bricks
Balls Left: 0

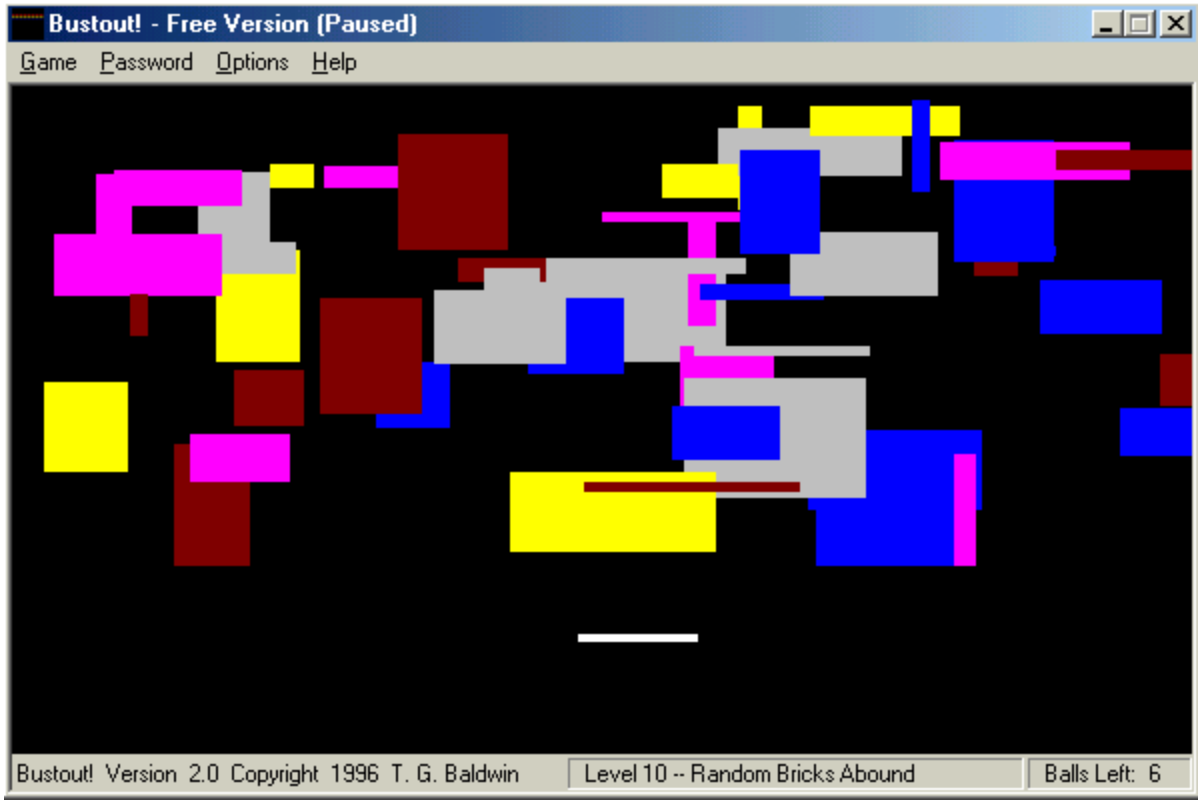

URSoft W32Dasm Ver 8.93 Program Disassembler/Debugger
Disassembler Project Debug Search Goto Execute Text Functions HexData Refs Help
* Referenced by a CALL at Address:
|:00405F0A
|
:004061EE 55 push ebp
:004061EF 8BEC mov ebp, esp
:004061F1 83EC08 sub esp, 00000008
:004061F4 53 push ebx
:004061F5 56 push esi
:004061F6 57 push edi
:004061F7 894DF8 mov dword ptr [ebp-08], ecx
:004061FA 833D00C8420000 cmp dword ptr [0042C800], 00000000
:00406201 0F853D000000 jne 00406244
:00406207 A128C84200 mov eax, dword ptr [0042C828]
:0040620C 8945FC mov dword ptr [ebp-04], eax
:0040620F 8B4DFC mov ecx, dword ptr [ebp-04]
:00406212 E8ABCCFFFF call 00402EC2
:00406217 6A00 push 00000000
:00406219 6A10 push 00000010
* Possible StringData Ref from Data Obj ->"The Free Version of Bustout! ends "
->"here."
|
:0040621B 686CA64200 push 0042A66C
:00406220 E8C12F0100 call 004191E6
:00406225 8B45F8 mov eax, dword ptr [ebp-08]
:00406228 C7400401000000 mov [eax+04], 00000001
:0040622F 8B45FC mov eax, dword ptr [ebp-04]
:00406232 C780000100000000000 mov dword ptr [ebx+00000100], 00000000
:0040623C 8B4DFC mov ecx, dword ptr [ebp-04]
:0040623F E803C8FFFF call 00402A47
* Referenced by a (U)nconditional or (C)onditional Jump at Address:

Vemos que ese cartel es llamado desde una Call en la dirección 405f0a, vamos a Goto/Goto code location y tipiamos la dirección. Así que lo que tendríamos que hacer sería anular esa Call. Tenemos que cambiar:

E8df020000 por 9090909090

Y listo, ya podemos jugarle a todas las pistas sin siquiera estar en "Full Versión" ¿Vieron que siempre hay otra salida?

(Esta es una foto del último level)



PD: Un enorme abrazo a Ricardo por confiar en mí aunque en un principio le hice muchas preguntas (¿Y QUE QUIEREN? SOLO TENGO 15 AÑOS).

(LECCION SESENTA Y CUATRO)

Introducción de Ricardo Narvaja: Sigue uno de nuestros jóvenes crackers con otro tute, despachándose a gusto con él y colaborando nuevamente.

Gracias JIKI

Programa:	Calendar 200X 4.3
Tipo:	Aplicación
Protección:	Ni se le puede llamar protección
Herramientas:	W32dasm; hex workshop; language 2000; ProcDump; Caspr
Cracker (si se me puede llamar así):	JIKI

Introducción...

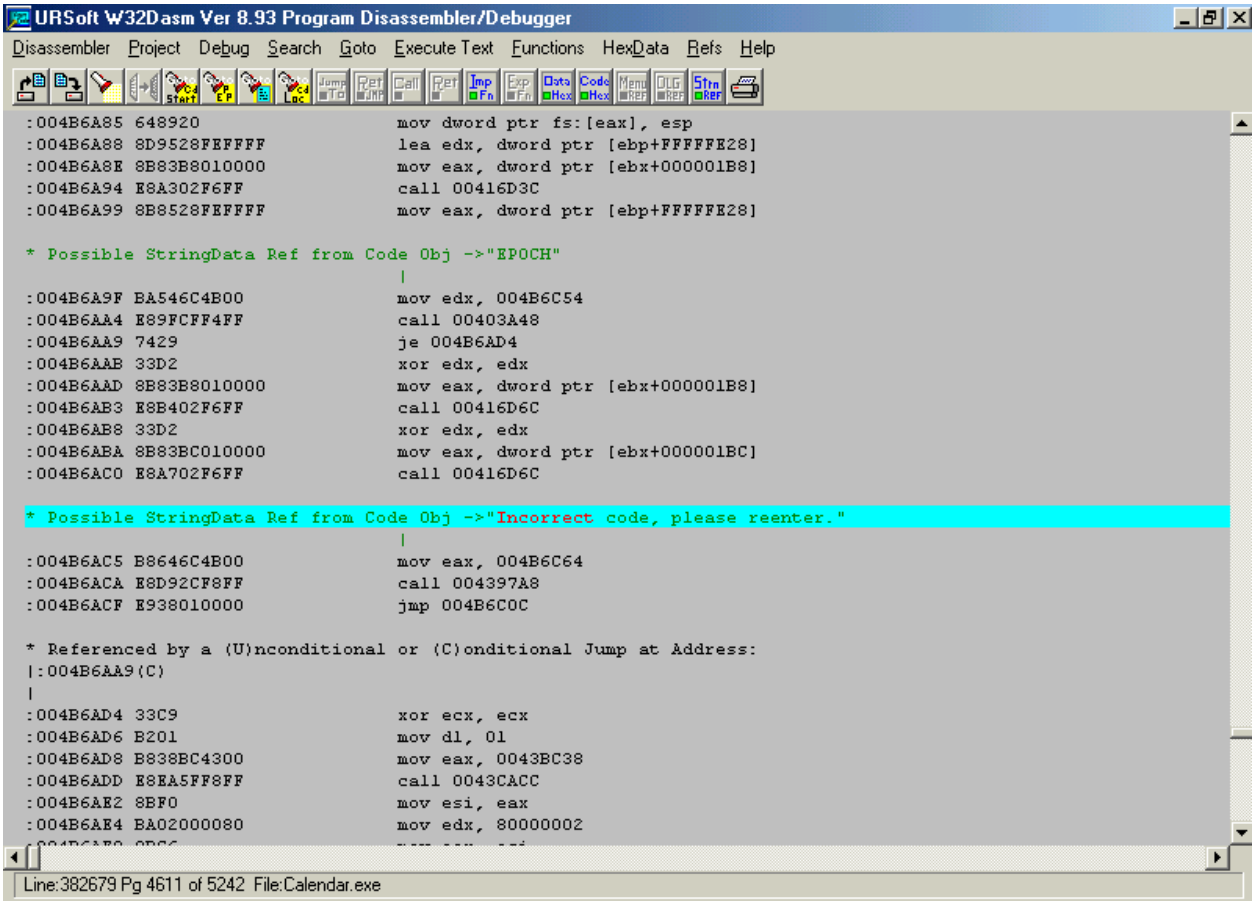
Este es mi segundo tute (espero que les haya gustado el primero) y les digo que estos tutes son para Newbies (de un Newbie para otro) ya que no son unas protecciones muy buenas y la verdad es que a veces la suerte ayuda. A este programa yo lo quería crackear "a lo bruto" (sin buscar el serial), pero por esas casualidades de la vida caímos justo con el serial.

PD: Quiero tratar de hacer otro tute antes de que me emiezen a matar de deberes en la escuela.

Pos parto...

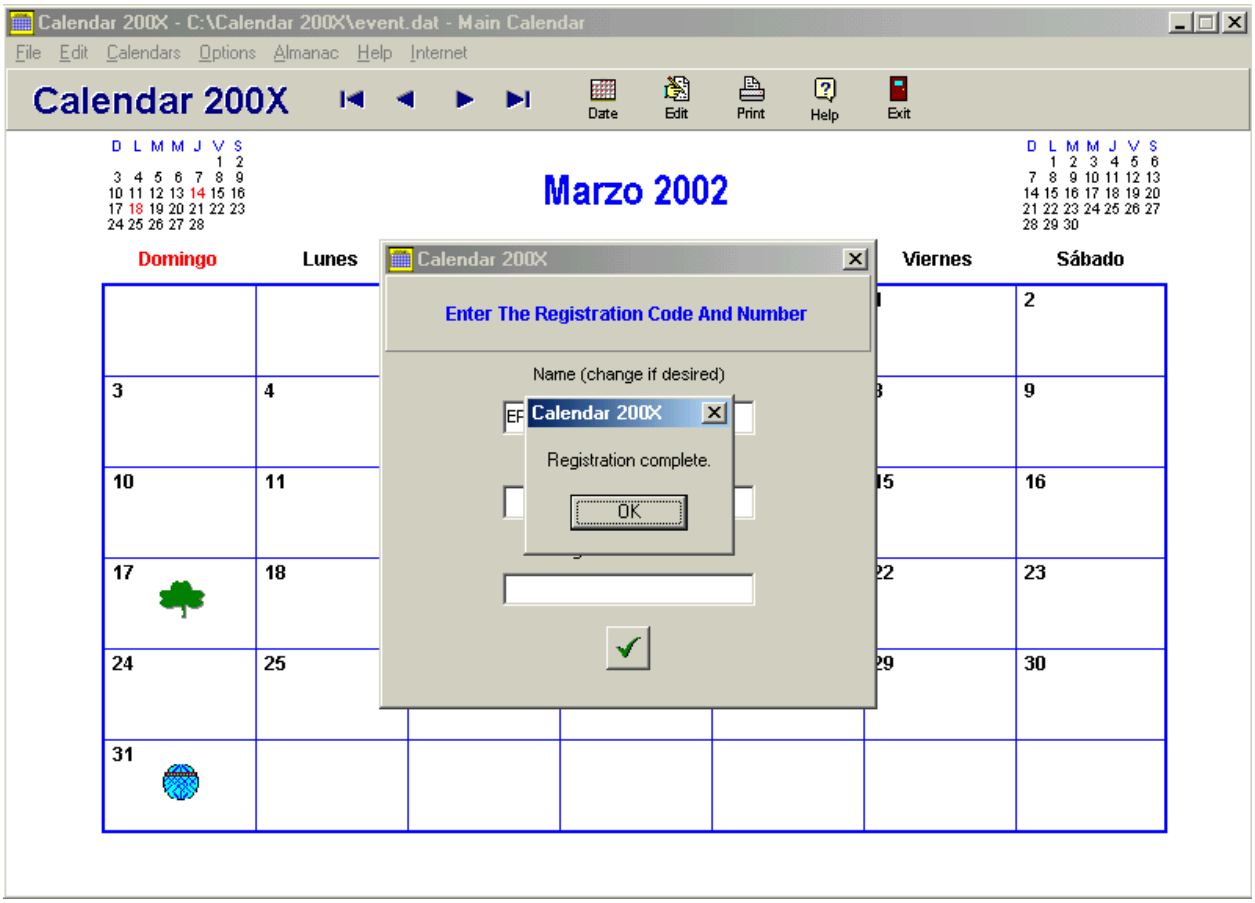
Abrimos el juego con el Language 2000 y vemos que está comprimido con Aspack y está hecho en Visual C++. Bueno, el Aspack no es problema, ya que con el Caspr queda limpito como un tomate. Paso siguiente abrimos el ProcDump, vamos a PE EDITOR, seleccionamos el nombre del juego y hacemos clic en abrir. Ni bien apretamos abrir nos saldrá una ventana en la cual hacemos un clic donde dice SECTIONS. Luego procedemos a hacer clic derecho en CODE, ponemos edit section y en donde dice sections characteristics cambiamos de C0000040 a E0000020. Hacemos lo mismo con todas las otras secciones (DATA; BSS; idata, etc.).

Al ataque...
Bueno, abrimos el Calendar 200X, vamos a File/Register Shareware y completamos con cualquier dato para ver qué pasa y... PIIIII "Incorrect code, plese reenter".
Abrimos el W32Dasm y desensamblamos la aplicación. Una vez abierto vamos a Search/Find Text y buscamos "Incorrect". Caemos en:



Ahí vemos que no hay ningún salto condicional anteriormente, el único salto que hay es uno que está en la palabra “EPOCH” (004B6AA9 7429 je 004b6ad4). Miren que raro que es desde esa palabra que se evita el comando “Incorrect code, please reenter”, bueno, yo ni me preocupé.

La joda es que lo crackeé a “lo bruto” (tenía un par de protecciones más) (External Exception %x y Access violation at adress %x y algo más que no va al punto). Bueno, el chiste es que una vez que lo crackeé me quedó una duda con la palabra EPOCH, así que instalé de nuevo el Calendar 200X, fui a File/Register Shareware, completé todos los datos con la palabra EPOCH y...



Bueno, después me dí cuenta que en el único lugar en donde tiene que estar la palabra EPOCH es en REGISTRATION CODE, en donde dice Name y Registration Number pueden poner lo que quieran.

PD: Bueno, un abrazo grande a Ricardo y aprovecho para saludarlo ya que hace mucho que no le escribo.

PD: DISCULPEN!!! En el tute anterior seguramente no habrán podido cambiar ningún valor en el Hex Workshop y es porque el atributo del juego estaba en "Solo Lectura" para cambiarlo hagan clic derecho en BUSTOUT, van a propiedades, le sacan el tilde a "Solo Lectura" y se lo ponen a "Archivo".

PD: Traten de crackear el programa Calendar 200X con el TRW ¡¡¡ES MÁS FÁCIL QUE CON EL W32DASM!!!

(LECCION SESENTA Y CINCO)

Programa: Teleport Pro 1.29.1590

Tipo: Para bajar Webs completas al disco rígido

Protección: Un dolor de huesos (si sos Newbie como yo)

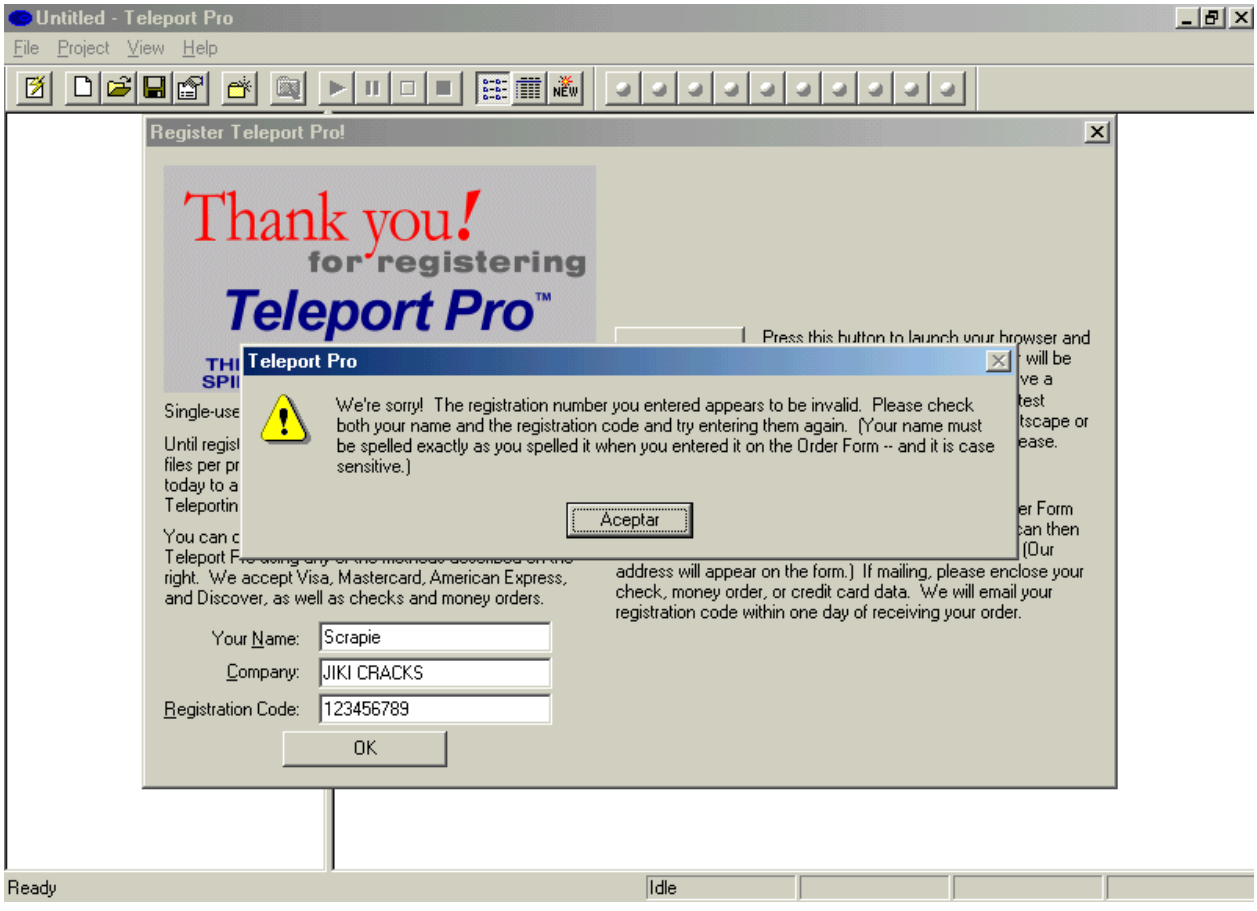
Herramientas: TRW; w32dasm; language 2000.

Cracker (si se me puede llamar así): JIKI

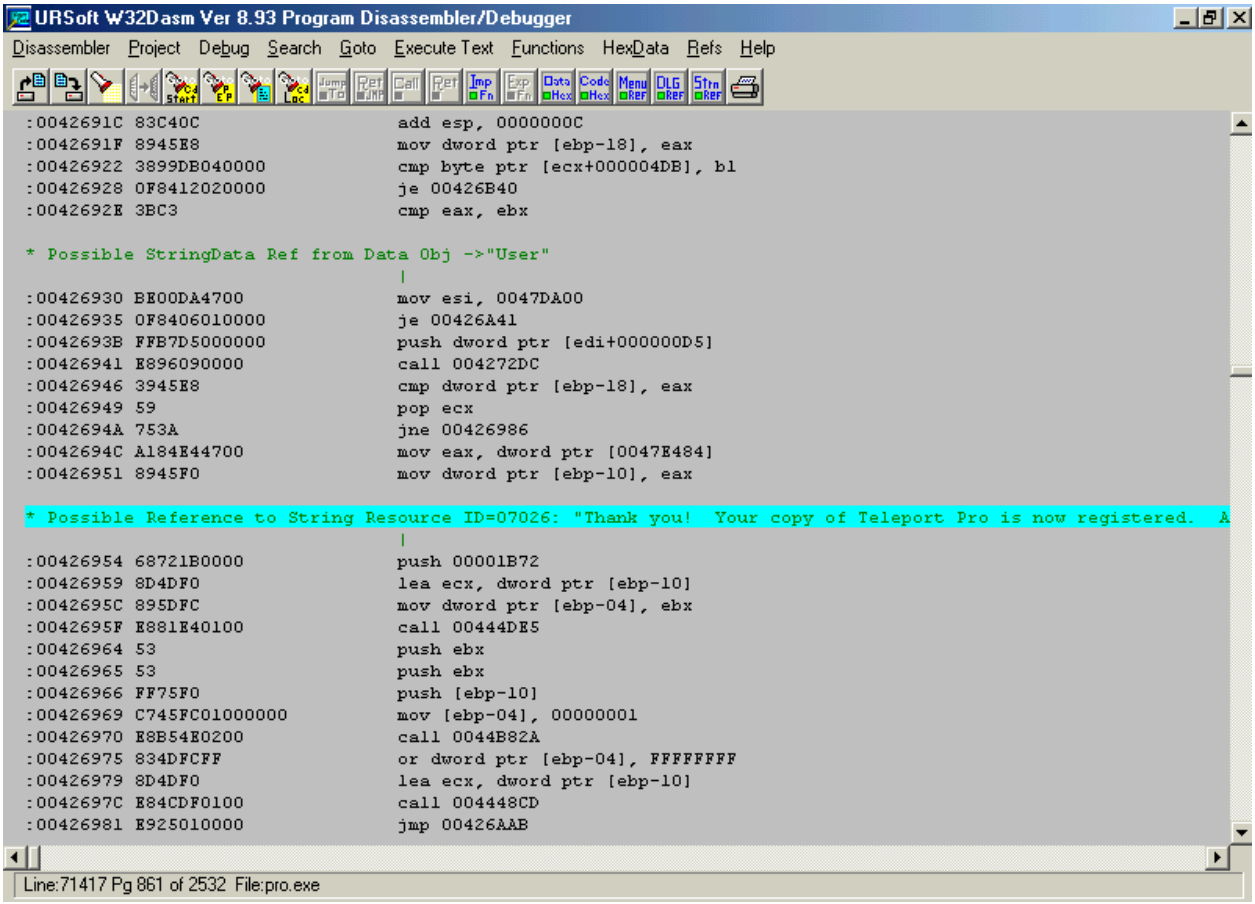
Introducción...
Y se va la tercera...Este es mi tercer tute y se lo voy a dedicar a Scrapie ya que casi tiene mi edad y espero que me escriba así tengo un amigo allá por España.
Este programa está bastante bueno, aunque no creo que sea muy útil para algunas personas pero estoy seguro de que otras lo van a necesitar algún día.

Pos parto...
Abrimos el juego con el Language 2000 y vemos que no está comprimido y está hecho en Visual C++. (Hasta ahora anda todo bien)

Al ataque...
Bueno, abrimos el Teleport Pro, vamos a Help/Register... Completamos con nuestros datos y vemos qué pasa...



Bueno, parece que no nos dejan registrarnos, bueno, no importa, vallamos al W32Dasm y busquemos ese cartel de error (We're sorry! Bla, bla, bla, bla, bla.).
Una vez que lo desensamblamos vamos a Search/Find Text, y ponemos We're sorry!, lo encuentra y por suerte es la única vez que aparece.
NOTA: Les cuento que lo traté de crackear a "a lo bruto", pero es más difícil que buscar el serial, después de media hora de estar intentando crackearlo a lo bruto sin resultados satisfactorios, me decidí a buscar el serial, estuve otra media hora pero apareció.Lo que en realidad tenemos que buscar ahora para encontrar el serial es:
Thank you! Your copy of teleport pro is now registered. Bueno, lo buscamos y caemos aquí:



Recuerden que estamos buscando el serial, así que no se emocionen y cambien ningún valor en el Hex Workshop, pero si se animan a hacerlo solos ¡NO HAY PROBLEMA VIEJO! Bueno, ya tenemos una idea de lo que está pasando:

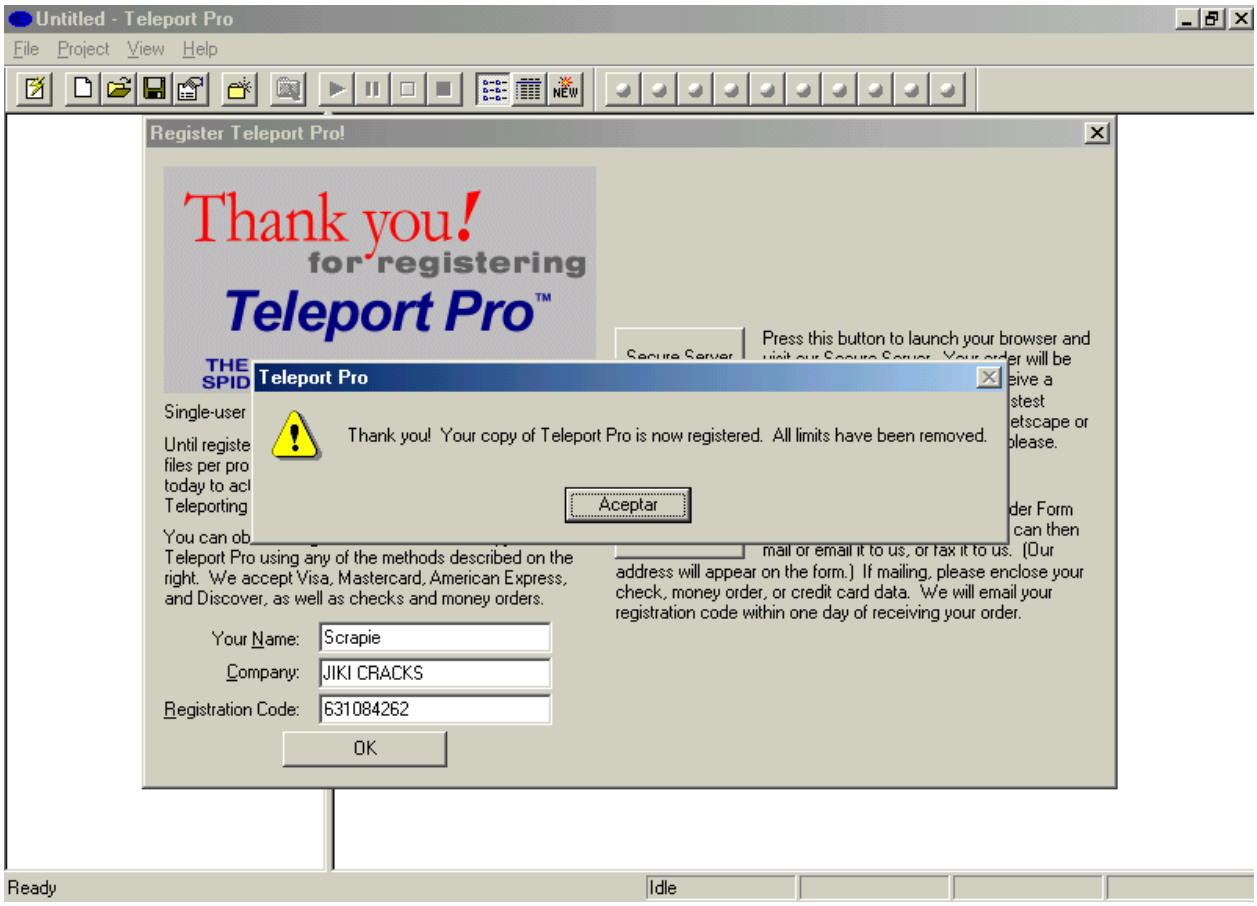
:00426941 E896090000 call 004272DC **----------;Se genera el serial**
:00426946 3945E8 cmp dword ptr [ebp-18], eax**------;Lo compara**
:00426949 59 pop ecx
:0042694A 753A jne 00426986**----------;Si está bien no salta**
:0042694C A184E44700 mov eax, dword ptr [0047E484]**;y continua a**
:00426951 8945F0 mov dword ptr [ebp-10], eax **;Thank you!...**

* Possible Referente to String Resource ID= 07026: " Thank you! Your copy of Teleport Pro is now regis te red . A

```
                                |
:00426954 68721B0000          push 00001B72
:00426959 8D4DF0              lea ecx, dword ptr [ebp-10]
:0042695C 895DFC              mov dword ptr [ebp-04], ebx
:0042695F E881E40100          call 00444DE5
:00426964 53                  push ebx
:00426965 53                  push ebx
```

Bueno, vamos al TRW, ponemos un bpx en 426946, vamos al Teleport Pro; Help/Register... Ponemos nuestros datos y...adentro mi alma (esa expresión me la copié de Ricardo, espero que no me demande, jaja.).
Bueno, donde caemos hacemos:
? ebp-18 y copiamos la cadena en DEC. (7402600)
? eax y copiamos la cadena en DEC. (631084262)

Bueno, vamos de nuevo a Help/Register... completamos nuestros datos solo que esta vez en Registration Code ponemos 7402600 y... We're sorry! Bla, bla, bla, bla.) Esperen!!!, no se desesperen, todavía nos queda probar con el otro número, vamos de nuevo a Help/Register... completamos nuestros datos solo que esta vez en Registration Code ponemos 631084262 y...



Ahora vamos a Help/About Teleport Pro y...

NOTA: Cuando hagan

? ebp-18

Y

? eax

Los resultados van a ser distintos según el nombre que hayan puesto.

PD: Un gran saludo para Ricardo y a todos los que me mandaron mails felicitándome!!!