2017

Revisando Internet Download Manager

By

Apuromafo

Apuromafo

CLS

8-7-2017

Índice

Contenido

Introducción

Programa	Internet Download Manager 6.28 Build 15.3
Descarga	http://filehippo.com/es/download_internet_download_manager/ http://www.internetdownloadmanager.com/
Dificultad	Depende de quien lo mire.
Información	www.internetdownloadmanager.com/data/update623.txt
Herramientas usadas	X64dbg ,PID
Fecha	08/07/2017
Cracker	Apuromafo

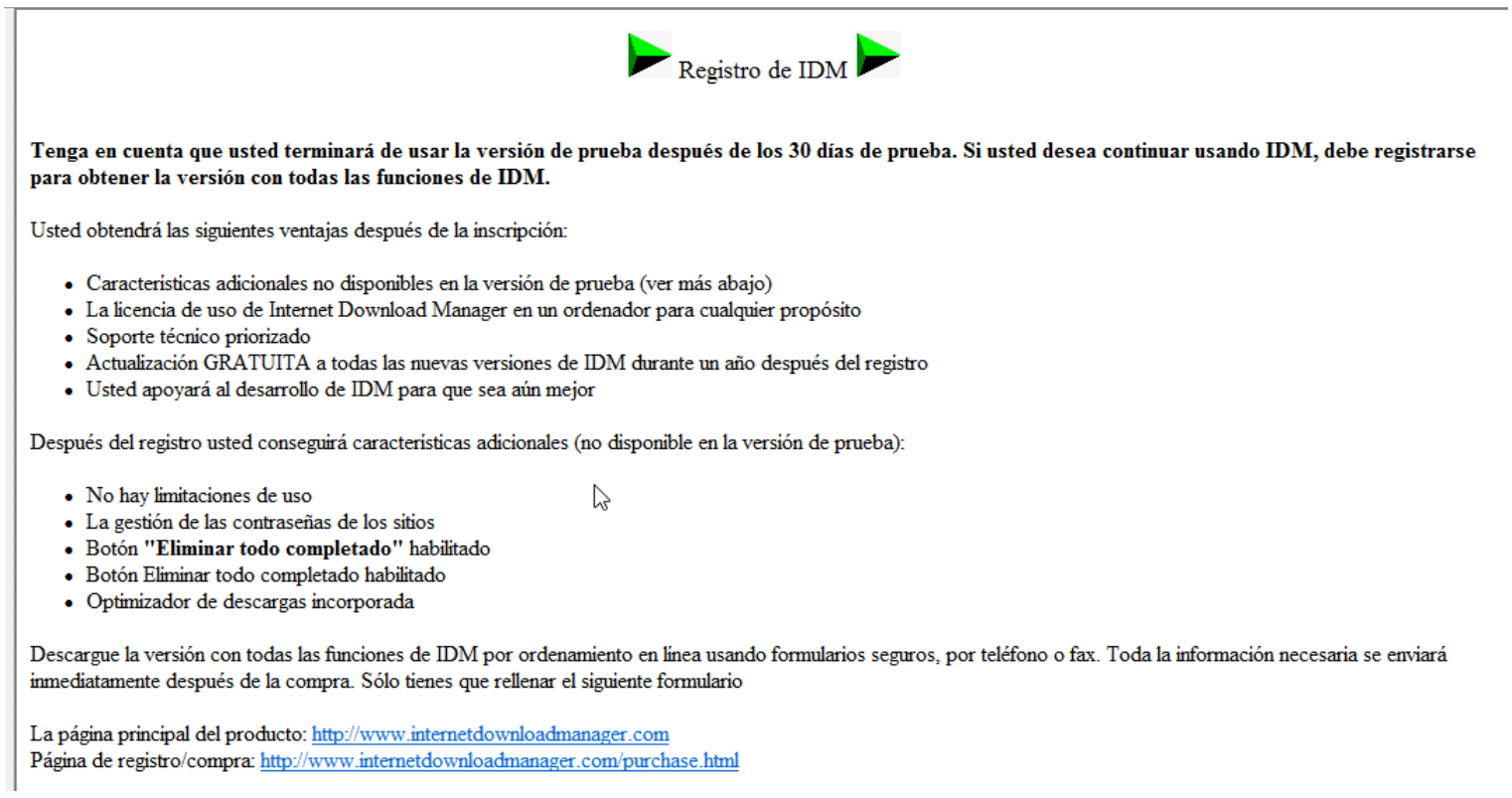
Herramientas usadas:

Herramienta	***Descarga***	***Utilidad***
Procesador de texto	***(está incluido con el suite de office)***	***Para redactar el tutorial***
Sharex	***https://getsharex.com/***	***Para capturar las imágenes***
Everything	***http://www.voidtools.com/***	***Para buscar los archivos en el pc***
X64dbg	***http://x64dbg.com/***	***Depurador***
PID	***https://web.archive.org/web/20170620171730/http://pid.gcwstorage.xyz/dl.php?f=ProtectionId.685.December.2016.rar***	***Analizador de Ejecutables***
****Puppy***	https://www.mzrst.com/	***Explorador de string para regedit y para webs para darse una idea antes de depurar. (apuntar direcciones)***
****ExeinfoPE***	http://exeinfo.atwebpages.com/	***Analizador de Programa, también permite escanear las webs (http) y menú de rip.***
****cffexplorer***	http://www.ntcore.com/exsuite.php	PE editor para editar a gusto.

**no mostrado en el tutorial, dado su uso intuitivo.*

Explorando el Programa

Bienvenidos a esta pequeña lectura e historia explorando un programa, este es una aplicación de pago , con duración de 30 días de prueba y si usamos mas de 1 año, estamos buscando soporte, respecto este programa, siempre se encuentran por la red muchos cracks y parches que desconozco que pueden hacerle al programa, así que por tranquilidad, todo lo que este en este tutorial queda en mi pc, si alguno quiere replicarlo, mínimo intente dar soporte al autor del programa .Lo que escribo es sin fines de lucro, sigamos.
A veces una imagen habla más que mil palabras, así que comienzo viendo el about



<img1: Info del programa desde help>

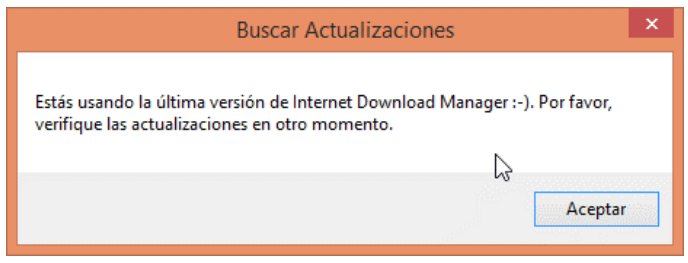
Refiere que “eliminar todo completado” y “gestión de contraseñas” es una opción de versión registrada.

Comencemos a ver el programa:

El setup se puede bajar de la web (dispone de la versión 15.1/15.2) en filehippo se dispone de mas versiones, en general entre mas nuevo mas soporte a los sitios de streams hasta donde veo, bueno bajo el setup de la web, actualizo y ve con Everything en mi caso se puede encontrar en esta ruta:

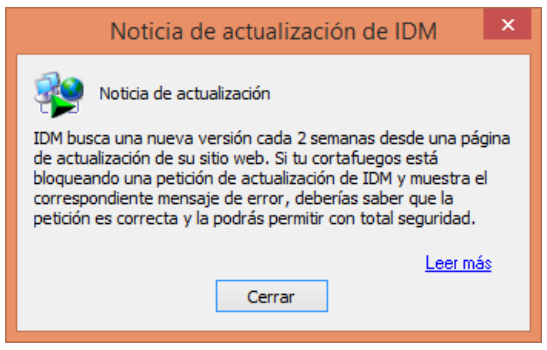
<img2: Ruta del Setup update del programa desde Everything searcher>

Una vez instalado y actualizado al pulsar el botón de buscar actualizaciones dice:



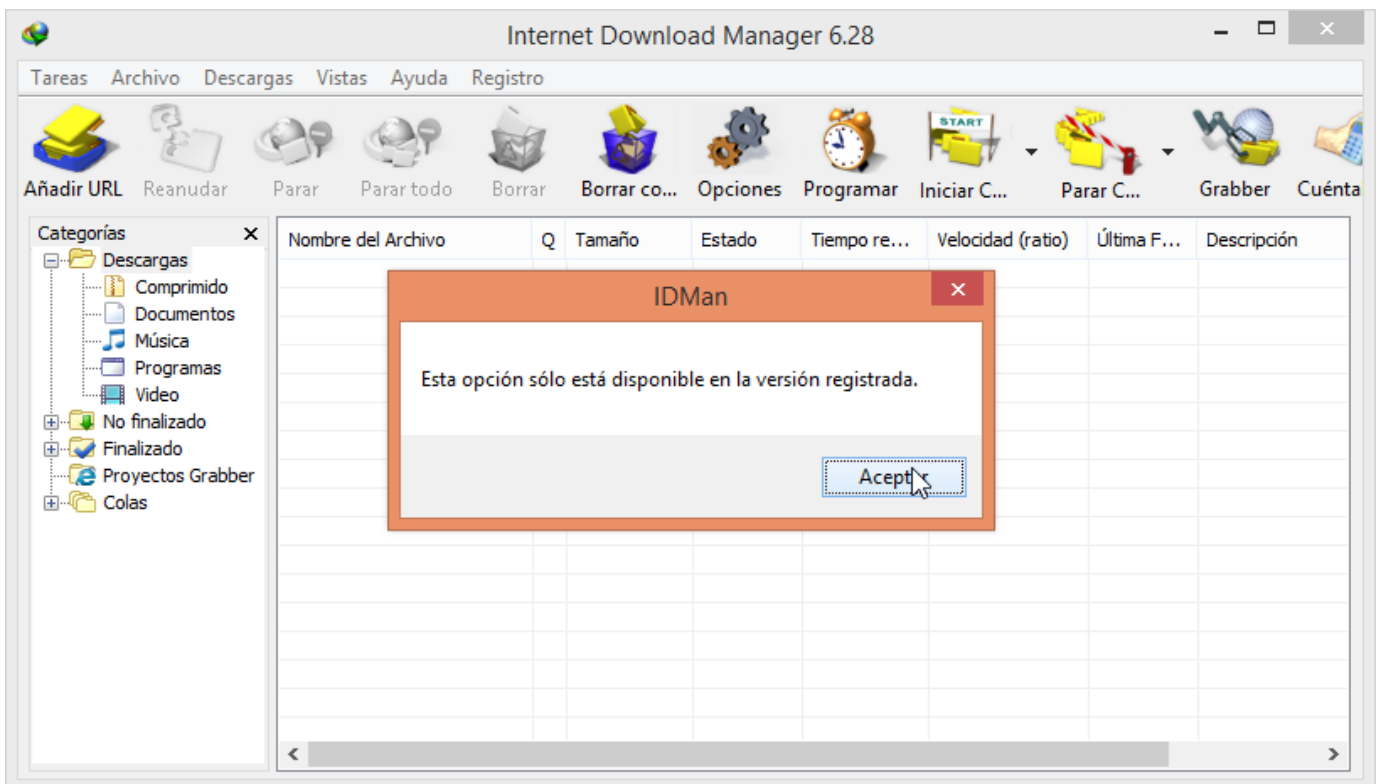
<img3: No hay más Actualizaciones a la fecha>

Luego de un tiempo aparecen mensajes avisando de cantidad de días para usar el programa (30) y además una noticia de actualización (cada 2 semanas hay una nueva versión) si verifico en http://filehippo.com/es/download_internet_download_manager/history/ confirmo que es cierto lo que refiere.



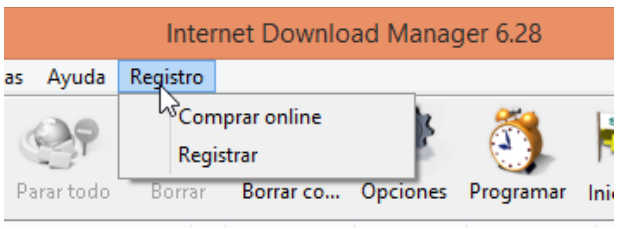
<img4: Actualizaciones cada 2 semanas del programa aproximadamente>

Así que debería ser valido el tutorial por algún pequeño tiempo. Si vemos el interfaz y pulsamos el botón demo:



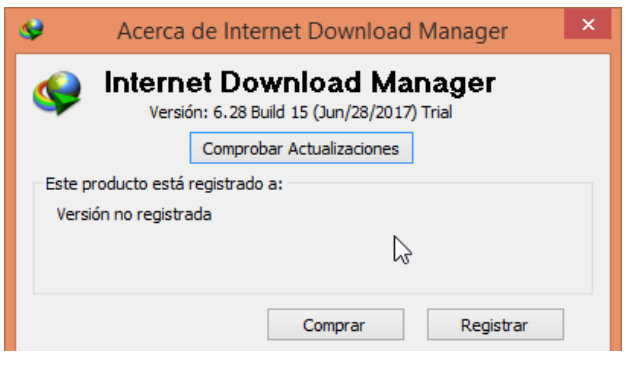
<img5: Limitación demo Borrar completados>

Explorando el menú se ven así: En el menú



<img6: Menú de registro con opciones de comprar y registrar>

El About Respecto del registro



<img7: desde el programa Al pulsar about "el producto a…versión no registrada… >

PID sobre el setup:

Comenzamos la hazaña, Iuego de descargar el instalador, actualizado el programa Analizo con PID y obtengo un setup tiene firma Digital (visto desde Puppy) y además no tiene ningún tipo de instalador conocido

```
 -=[ ProtectionID v0.6.8.5 DECEMBER]=-
(c) 2003-2017 CDKiLLER & TippeX
Build 24/12/16-13:09:21
Ready...
Scanning -> C: \idmupdt.exe
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 7191176 (06DBA88h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x54D1C77F -> Wed 04th Feb 2015 07:17:19 (GMT)
[TimeStamp] 0x54D1C77F -> Wed 04th Feb 2015 07:17:19 (GMT) | PE Header | - | Offset: 0x000000E8 | VA: 0x004000E8 | -
-> File Appears to be Digitally Signed @ Offset 06D8650h, size : 03438h / 013368 byte(s)
-> File has 7148112 (06D1250h) bytes of appended data starting at offset 07400h
[File Heuristics] -> Flag #1 : 00000000000101001100000000000110 (0x0014C006)
[Entrypoint Section Entropy] : 6.41 (section #0) ".text   " | Size : 0x3B80 (15232) byte(s)
[DllCharacteristics] -> Flag : (0x0000) -> NONE
[SectionCount] 3 (0x3) | ImageSize 0x9000 (36864) byte(s)
[VersionInfo] Company Name : Tonec Inc.
[VersionInfo] Product Name : Internet Download Manager installer
[VersionInfo] Product Version : 6. 22. 1. 1
[VersionInfo] File Description : Internet Download Manager installer
[VersionInfo] File Version : 6. 22. 1. 1
[VersionInfo] Original FileName : installer.exe
[VersionInfo] Internal Name : installer
[VersionInfo] Version Comments : Please visit http://www.internetdownloadmanager.com
[VersionInfo] Legal Trademarks : Internet Download Manager (IDM)
[VersionInfo] Legal Copyrights : © 1999-2015. Tonec. Inc. All rights reserved.
[ModuleReport] [IAT] Modules -> MSVCRT.dll | KERNEL32.dll | USER32.dll | ADVAPI32.dll | SHELL32.dll
[!] File appears to have no protection or is using an unknown protection
- Scan Took : 0.578 Second(s) [000000242h (578) tick(s)] [566 of 580 scan(s) done]
```

Luego en x64dbg observamos las strings apunta que irá a una carpeta con IDM1.tmp, dado la potencia de Everything para buscar, no me costará encontrarlo en el pc.

```
String
"KERNEL32"
"GetDiskFreeSpaceExW"
"SHELL32"
"SHGetDesktopFolder"
"SHGetPathFromIDListW"
"SHGetMalloc"
"Internet Download Manager"
"%s Setup"
"/delsetup"
"-delsetup"
" delsetup"
"/skipdlgs"
"-skipdlgs"
" skipdlgs"
"IDM_Setup_Mutex_st23nZ7a"
"Welcome"
"IDM Setup"
"The IDM Installation program requires a
L"Select Temp Directory "
"\r\n"
"Could not find temp path in unpacker"
L"IDM_Setup_Temp"
"\r\n"
"Could not create temp dir in unpacker"
L"setup_error.log"
L"%s%s"
L"IDM1.tmp"
L"%s%s"
L" -skdlgs"
L"\"%s%s\" -d \"%s\"%s -rmsetup \"%s\""
L" -skdlgs"
L"\"%s%s\" -d \"%s\"%s"
"\r\n"
"Could not create process in unpacker"
"IDM Setup"
"Install process has been stopped becaus
"Software\\Microsoft\\Windows NT\\Curren
L"WIN"
L"win"
L"WIN"
L"win"
"IsWow64Process"
"kernel32"
"%s. Error ID=%s"
```

<img8:X64dbg al buscar referencias refiere ruta de temporales>

Luego encuentro que está en temporales el setup de los archivos

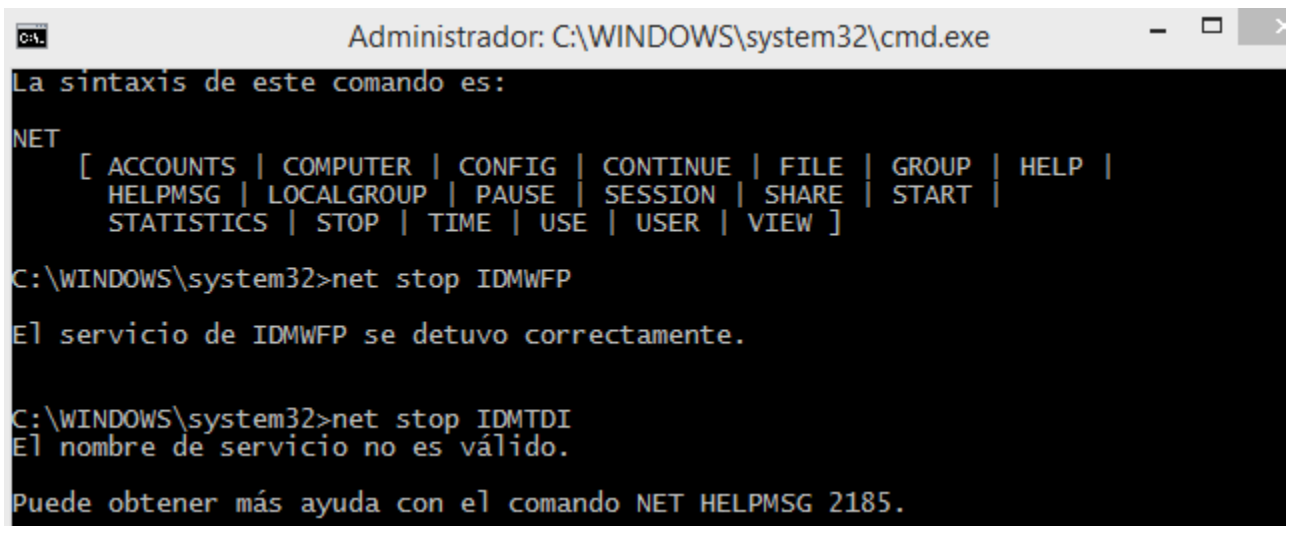
```
Scanning -> C:\Users\Pc\AppData\Local\Temp\IDM_Setup_Temp\IDM1.tmp
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 190008 (02E638h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x594CFB0A -> Fri 23rd Jun 2017 11:27:06 (GMT)
[TimeStamp] 0x594CFB0A -> Fri 23rd Jun 2017 11:27:06 (GMT) | PE Header | - | Offset: 0x000000F8 | VA: 0x004000F8 | -
-> File Appears to be Digitally Signed @ Offset 02B200h, size : 03438h / 013368 byte(s)
[File Heuristics] -> Flag #1 : 00000000000101001100010000000110 (0x0014C406)
[Entrypoint Section Entropy] : 6.14 (section #0) ".text   " | Size : 0xE37E (58238) byte(s)
[DllCharacteristics] -> Flag : (0x0000) -> NONE
[SectionCount] 4 (0x4) | ImageSize 0x30000 (196608) byte(s)
[VersionInfo] Company Name : Tonec Inc.
[VersionInfo] Product Name : Internet Download Manager installer
[VersionInfo] Product Version : 6. 28. 14. 1
[VersionInfo] File Description : Internet Download Manager installer
[VersionInfo] File Version : 6. 28. 14. 1
[VersionInfo] Original FileName : Uninstall.exe
[VersionInfo] Internal Name : Uninstall
[VersionInfo] Version Comments : Please visit http://www.internetdownloadmanager.com
[VersionInfo] Legal Trademarks : Internet Download Manager (IDM)
[VersionInfo] Legal Copyrights : © 1999-2017. Tonec. Inc. All rights reserved.
[ModuleReport] [IAT] Modules -> COMCTL32.dll | SHLWAPI.dll | KERNEL32.dll | USER32.dll | ADVAPI32.dll | SHELL32.dll | ole32.dll | OLEAUT32.dll |
MSVCRT.dll
[!] File appears to have no protection or is using an unknown protection
- Scan Took : 0.516 Second(s) [000000204h (516) tick(s)] [506 of 580 scan(s) done]
```

Dado que tenemos el archivo pareciera tener apariencia de .exe así que lo cargo en x64dbg (una vez renombrado a .exe) y intentare darme una idea global (en x64dbg), podemos darnos cuenta que con esto podremos saber al instalar donde mas menos esta funcionando el programa.

Destacando a lo más el acceso a regedit, antivirus, registros de dll ejemplo:

004013C1 push idm1.tmp.412724	L"Software\\DownloadManager\\IDMBI" //rama de registro
00401848 push idm1.tmp.412B30	L"Software\\Microsoft\\Windows\\CurrentVersion\\Run" //rama de registro que indica que al iniciar el equipo se estará ejecutando
00401862 push idm1.tmp.412B24	L"IDMan" //clave de registro
0040186C push idm1.tmp.412B1C	L"IDM"//clave de registro
Hacia 2 servicios de driver	
04030DA push idm1.tmp.412A18	L"SOFTWARE\\Internet Download Manager" //nombre rama regedit
004030FC push idm1.tmp.4129C4	L"AdvIntDriverEnabled2" //nombre de driver
0040311C mov ecx,idm1.tmp.41348C	L"SYSTEM\\CurrentControlSet\\Services\\IDMWFP" //nombre servicio driver “IDMWFP”
0040312D mov ecx,idm1.tmp.413438	L"SYSTEM\\CurrentControlSet\\Services\\IDMTDI"//nombre servicio driver “IDMTDI”
00403165 push idm1.tmp.41342C	L"Start" //comandos cmd
00403190 mov ecx,idm1.tmp.41341C	L"IDMWFP"
00403197 mov ecx,idm1.tmp.41340C	L"IDMTDI"
0040319F mov eax,idm1.tmp.413400	L"start" //comandos cmd
004031A6 mov eax,idm1.tmp.4133F4	L"stop" //comandos cmd

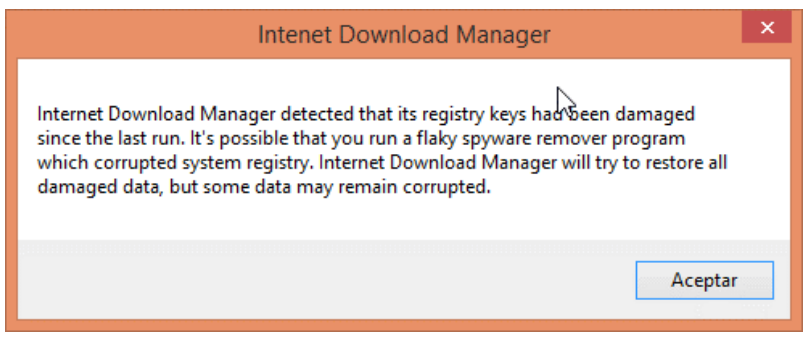
Así que antes que comencemos a depurar, necesito verificar como funciona con los errores (sin driver) que el driver no esté en este minuto: (verifico como funciona el comando net), refiere:



<img9:consola cmd con permisos de admin usando comando net stop>

Veo que funciona bien el comando,y aun así funciona bien el soft, ya conocido más menos los programas comienzo a leer los tutoriales al respecto para saber a que vamos a encontrar (a primera impresión de los escritos es que hay nags, validacion de serial online, condiciones para registrarse entre otros.) veamos como funciona con los errores mas harcoded (que no tenga su rama de regedit registrada)

Comencemos entonces a explorar Si elimino las ramas de regedit no pasa lo mismo jeje



<img10: programa con error si se ejecuta sin valores en regedit>

Así que si eliminan regedit realmente el programa no estará operativo. (Hay valores importantes desde regedit) este programa no puede simplemente copiarse sin existir en sus datos de regedit.sigamos viendo así que a comenzar de 0

Conclusión 1:

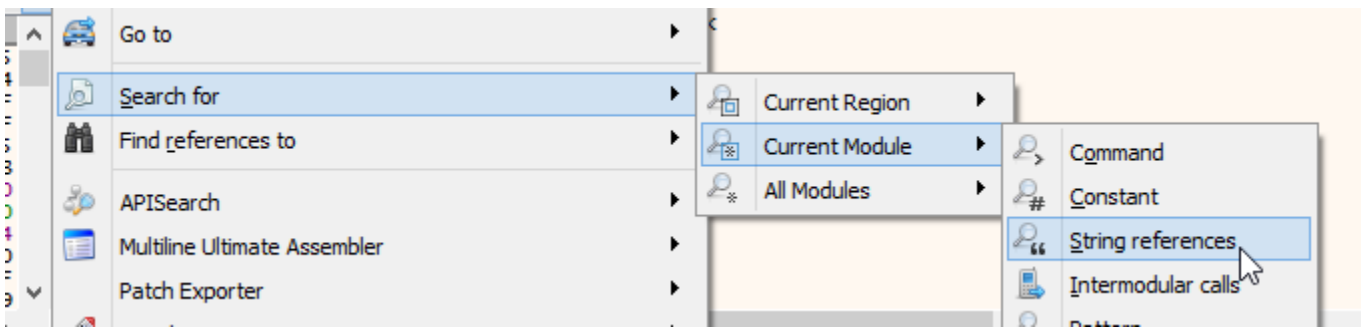
Cuando yo instalo un setup.exe y quiero actualizar a una nueva versión, si quiero tener una ruta mas menos limpia, puedo borrar la rama de regedit antes mencionada y será como si hubieras instalado el update por primera vez, o mas bien, si tengo que alguien quiere usar el IDM sin ramas de regedit es algo falso, requiere de instalación previa antes de usarse. En principio básico si alguien quiere guardar una versión full tendria que guardar el setup, el update, el cracked.exe y un firewall para evitar nuevas actualizaciones (así sin mirar aun el programa)

Al ver IDMan.exe , es el que tiene string mas relevantes, comencemos por aquí:

```
EDI  005DFDBF   55              push ebp                                EntryPoint
     005DFDC0   8B EC           mov ebp, esp
     005DFDC2   6A FF           push 0xFFFFFFFF
     005DFDC4   68 38 0B 68 00  push idman.680B38
     005DFDC9   68 80 CC 5D 00  push idman.5DCC80
     005DFDCE   64 A1 00 00 00 00 mov eax, dword ptr fs:[0]
     005DFDD4   50              push eax
     005DFDD5   64 89 25 00 00 00 mov dword ptr fs:[0], esp
     005DFDDC   83 EC 58        sub esp, 0x58
     005DFDDF   53              push ebx
     005DFDE0   56              push esi
     005DFDE1   57              push edi
     005DFDE2   89 65 E8        mov dword ptr ss:[ebp - 0x18], es
     005DFDE5   FF 15 D0 83 62 00 call dword ptr ds:[<&GetVersion>]
     005DFDEB   33 D2           xor edx, edx
```

<img11:entrypoint del Idman.exe desde x64dbg>

Si busco referencias en x64dbg (coloco search for, current module, string references)



<img12: Idman.exe desde x64dbg, buscando referencias>

Tenemos de por hecho validaciones de su web , logro apreciar un secure. (obviamente lo que sigue debería ser decodificado en runtime con la web ya me advierte que esto tiene validacion online)

```
0040203C  mov edx,idman.6BA088          "%s"
00402074  push idman.6BA088             "%s"
00402156  push idman.6BA07C             "%s&lng=%s"
00402182  push idman.6BA070             "http://www."
00402187  push idman.6BA060             "https://secure."
004021AA  push idman.6BA08C             ".internetdownloadmanager.com/"
00402248  mov edx,dword ptr ds:[6E5B5C] "p[n"
```

<img13: x64dbg muestra string que refieree secure posiblemente valide sus keys o serial online>

Busco la palabra anterior “registrer” vemos adicionalmente que hay validaciones que le dicen, se ha encontrado un serial falso o que existe bloqueo, se cerrará. Lo que me advierte que además tendre que tener cuidado donde se puede cerrar el programa.

```
Address   Disassembly          String
00412D68  push idman.6BB700    "http://www.internetdownloadmanager.com/register/new_faq/enableBFE.html"
004390D4  push idman.6BDDC0    "http://www.internetdownloadmanager.com/register/new_faq/chrome_extension2.html"
00448697  push idman.6BEF38    "DllRegisterServer"
004486D1  push idman.6BEF38    "DllRegisterServer"
004486F7  push idman.6BEF38    "DllRegisterServer"
0044871D  push idman.6BEF38    "DllRegisterServer"
004494CD  push idman.6BEF38    "DllRegisterServer"
004D5173  push idman.6D35D4    "This feature is available in registered version only."
004D5E30  push idman.6D0484    "You have %d days left to use Internet Download Manager. Do you want to register your copy of IDM now?"
004D62EF  push idman.6CF990    "Internet Download Manager has been registered with a counterfeit Serial Number. IDM is exiting..."
004D62FE  push idman.6CF908    "Internet Download Manager has been registered with a counterfeit Serial Number or the Serial Number has been blocked. IDM is exiting..."
004D630D  push idman.6CF89C    "Internet Download Manager has not been registered for 30 days. Trial period is over and IDM is exiting..."
004D631C  push idman.6CF848    "Internet Download Manager has not been registered for 15 days. IDM is exiting..."
004D698E  push idman.6CEAAC    "Please register IDM before updating.\r\n Pick \"Registration->Registration\" menu item and enter your registration information. Then pick \"Help->Quick Up
004D7A98  push idman.6C8DC8    "You'll need to provide administrator permissions to register IDM for all users on this computer"
004D8254  push idman.6C49AC    "You registered IDM with the serial number below\r\n%s\r\n\r\nThis serial number is blocked on IDM servers. IDM is exiting..."
0050442C  push idman.6BB700    "http://www.internetdownloadmanager.com/register/new_faq/enableBFE.html"
00509748  push idman.6D47A4    "register"
0056F47D  mov edi,idman.6DB4C  "register.cgi"
005A3E9B  push idman.6DD77C    "http://www.internetdownloadmanager.com/register/new_faq/How_to_configure_Firewalls_for_IDM.html"
006029E8  push idman.67EDDC    "Unregister"
007154FD  adc dword ptr ds:[6  &"Internet Download Manager has been registered with a counterfeit Serial Number or the Serial Number has been blocked. IDM is exiting..."
007C6971  imul ecx,eax,rpcrt4  "ncRegisterInfo"
```

<img14: x64dbg muestra al escribir register subraydo la palabra a buscar que se escribe en el command bar >

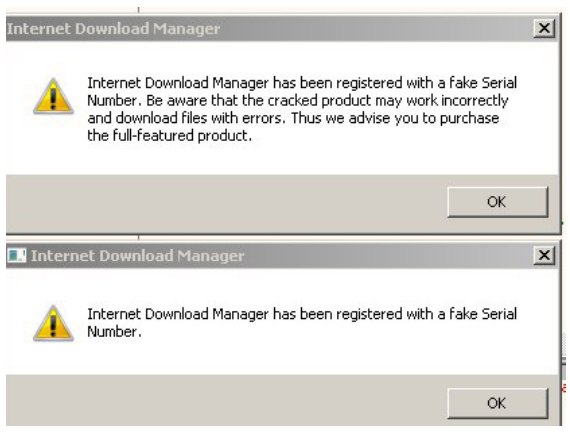
Comencemos con el mensaje que tenemos x dias para usarlo al buscar el you have, tambien refiere que cuando usas mas de 1 año, deberias comprar la licencia o subscribirte dado que esta en los acuerdos y muchas más, así que solo pensando al ojo ya hay mas de 2 lugares a parchr , aun sin nisiquiera depurarlo.(lo que refiere que tambien el programa puede validar serial en tiempos de expired.

Strings (idman.exe) | Constant: 006D35D4 (Region idman.exe) | Strings (idman.exe)

```
Address   Disassembly          String
004D5218  push idman.6D32      "You have changed the \"site/path field.\" The login information for this new site/path already exists in your password list.\nThe login information hasn't been change
004D5281  push idman.6D2F      "No connection could be made because the target machine actively refused it. \nProbably the service is inactive on the server or you have a firewall installed that blo
004D5E30  push idman.6D04      "You have %d days left to use Internet Download Manager. Do you want to register your copy of IDM now?"
004D62E0  push idman.6CF9      "You have entered incorrect Serial Number.\r\n\r\nPlease don't mix O(zero) and O(ou), I and 1 while typing your S/N! CUT and PASTE your S/N!"
004D6682  push idman.6CF2      "From %d:%02d to %d:%02d you downloaded %ld MB. All IDM downloads will be stopped because you have exceeded your download limits set in in IDM Scheduler (or 'Options->
004D699D  push idman.6CE9      "According to our license agreement that you have accepted, you are allowed to update Internet Download Manager freely during one year after the purchase. If you want
004D6ABA  push idman.6CD8      "You have turned off advanced browser integration. If you found a problem with advanced browser integration, we would like to fix the problem for you. In order to fix
004D6AD8  push idman.6CD7      "IDM is trying to download a test page to check your Internet connection. Please ensure that you are connected to the Internet. If you have a firewall, please ensure t
004D747B  push idman.6CAD      "Temporary directory is required for storing file parts during download.\nIf you have several physical drives on your computer, you should select different physical dr
```

<img15: x64dbg muestra strings de exstencia de un acuerdo>

Si sigo buscando por internet dice que algunos mensajes de error son por expiracion de licencia entre otros, pero aquí hay un detalle bueno, notese que las 2 ventanas son diferentes (esto en conclusion significa que uno es del programa y otro de un nuevo proceso creado)



<img16:mensajes de alerta QUE SI detecta si usas una licencia falsas>

Conociendo al is_registred:

Comienzo a depurar el programa, para trabajar con este programa es necesario tener un poco de práctica cuando se pelean con nags, esto es saber identificar timer, identificar mensajes y/o procesos nuevos que se van creando, comencemos viendo el primer mensaje de limitacion.El programa refiere que es solo disponible en versión registrada, aparece el mensaje con el entorno normal como messagebox y puede presionarse mas de una vez, coloco bp en messageboxA y en su retorno espero ver de donde quiere sorprenderme o bien, espero el mensaje, pauso, coloco call activo, ejecuto retorno y tenemos el mismo resultado.
(si pausas el programa, puedes esperar colocar retornar (con comandos ctrl+f9), luego ver al salir de messagebox el mensaje de donde proviene si no lo pausas, debes por lo menos tener un breakpoint en la api MessageBoxA así te pausará):

```
005F6047   85 F6              test esi, esi
005F6049   75 04              jne idman.5F604F
005F604B   33 C9              xor ecx, ecx
005F604D   EB 03              jmp idman.5F6052
005F604F   8B 4E 1C           mov ecx, dword ptr ds:[esi + 0x1C]
005F6052   FF 74 24 10        push dword ptr ss:[esp + 0x10]
005F6056   50                 push eax
005F6057   FF 74 24 10        push dword ptr ss:[esp + 0x10]
005F605B   51                 push ecx
005F605C   FF 15 FC 87 62 00  call dword ptr ds:[<&MessageBoxA>]
005F6062   5E                 pop esi
005F6063   C2 0C 00           ret 0xC
```

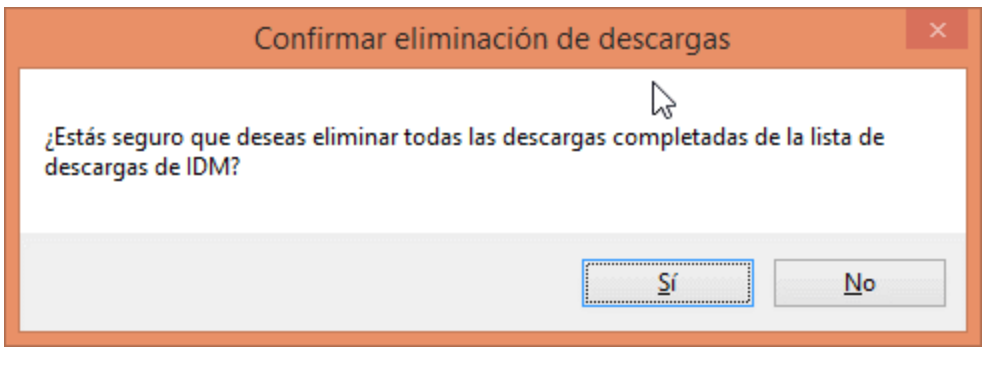
<img17 x64dbg: imagen donde esta lanzando el messagebox>

Parece algo generico, así que voy al retorno y vemos un salto a comparar

```
00463BA3   8B F1              mov esi, ecx
00463BA5   89 65 F0           mov dword ptr ss:[ebp - 0x10], esp
00463BA8   85 C0              test eax, eax
00463BAA   89 75 EC           mov dword ptr ss:[ebp - 0x14], esi
00463BAD   74 20              je idman.463BCF
00463BAF   A1 AC BA 6E 00     mov eax, dword ptr ds:[0x6EBAAC]
00463BB4   6A 00              push 0x0
00463BB6   6A 00              push 0x0
00463BB8   50                 push eax
00463BB9   E8 76 24 19 00     call idman.5F6034                 Mensaje solo registrado
00463BBE   8B 4D F4           mov ecx, dword ptr ss:[ebp - 0xC]
00463BC1   5F                 pop edi
00463BC2   5E                 pop esi
```

<img18 x64dbg: imagen del retorno del messagebox>

Si modifico que salte siempre (je a jmp) en la direccion de 463bad : tenemos la primera funcion desbloqueada



<img19 x64dbg: al cambiar el flujo del salto anterior, permite una opcion que supuestamente no se puede>

Con la imagen anterior ya tenemos claro que realidad tenemos, guardo el parche y no tengo ningún problema de uso,

Por lo que tenemos ya nuestra primera conclusión hay una comparacion con un dword que yo llamaré is_registred, luego si tiene un valor esperado salta o no salta, para esto debemos investigar si se usa mas ese dword Así que en principio basico debemos lograr que al cambiar los saltos sean funcionales a lo que se necesita, veamos referencia al dword anterior (6BE2F0)

```
004017FA  mov eax,dword ptr ds:[6BE2F0]
004021E3  cmp dword ptr ds:[6BE2F0],esi
0042BF41  cmp dword ptr ds:[6BE2F0],edi
0042CB45  mov eax,dword ptr ds:[6BE2F0]
00447AE2  mov eax,dword ptr ds:[6BE2F0]
0044977A  mov eax,dword ptr ds:[6BE2F0]
0044A521  mov dword ptr ds:[6BE2F0],0
0044A579  mov eax,dword ptr ds:[6BE2F0]
0044A8DC  mov eax,dword ptr ds:[6BE2F0]
0044AA09  mov eax,dword ptr ds:[6BE2F0]
0044B6FE  mov eax,dword ptr ds:[6BE2F0]
0044BBF9  mov eax,dword ptr ds:[6BE2F0]
0044C0C9  mov eax,dword ptr ds:[6BE2F0]
0044C430  mov eax,dword ptr ds:[6BE2F0]
0044C53D  cmp dword ptr ds:[6BE2F0],ebx
004537FF  mov eax,dword ptr ds:[6BE2F0]
00454D5E  mov eax,dword ptr ds:[6BE2F0]
004551CE  mov eax,dword ptr ds:[6BE2F0]
004555AA  mov eax,dword ptr ds:[6BE2F0]
00455A13  mov eax,dword ptr ds:[6BE2F0]
0045DE31  mov eax,dword ptr ds:[6BE2F0]
0046268A  cmp dword ptr ds:[6BE2F0],ebx
00463B9B  mov eax,dword ptr ds:[6BE2F0]
00464FEF  mov eax,dword ptr ds:[6BE2F0]
004666AE  mov eax,dword ptr ds:[6BE2F0]
0046791D  mov eax,dword ptr ds:[6BE2F0]
0046795E  mov eax,dword ptr ds:[6BE2F0]
00467A96  mov eax,dword ptr ds:[6BE2F0]
00467E34  mov eax,dword ptr ds:[6BE2F0]
00467F64  mov eax,dword ptr ds:[6BE2F0]
00473F2B  mov eax,dword ptr ds:[6BE2F0]
0050B372  mov eax,dword ptr ds:[6BE2F0]
0050B968  mov dword ptr ds:[6BE2F0],0
0050C596  cmp dword ptr ds:[6BE2F0],esi
005137C0  mov eax,dword ptr ds:[6BE2F0]
005148AD  mov eax,dword ptr ds:[6BE2F0]
00514AF3  mov eax,dword ptr ds:[6BE2F0]
00515596  mov eax,dword ptr ds:[6BE2F0]
005592ED  mov ecx,dword ptr ds:[6BE2F0]
0056F41F  mov ecx,dword ptr ds:[6BE2F0]
```

<img20 x64dbg: conociendo las comparaciones con is_registred?>

Cabe destacar que puede apreciarse en 2 lugares moviendo un valor de 0 , manejando principalmente el registro en ebx, edi y esi, por lo cual esos son los registros mas importantes para ver.

Honestamente, no creo ser adivino pero si forzamos todos los saltos a los valores necesarios, ya tendriamos el primer cracked.exe en el cual si valida cualquier cosa como registrado no tendra ningún problema, pero sin saber que buscamos puede que nunca rompa y no sepamos que pasará.(así que dejo un bp en todos los dwords que es mi is_registred)

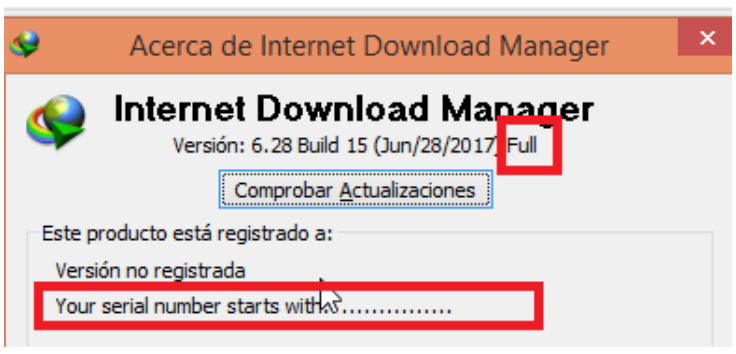
Tenemos por lo cual si fuera a buscar cualquier valor de registro solo basta invertir bandera(flag para verificar) y con el tiempo algún parche mas definitivo, dependerá del tiempo que se quiera utilizar el soft, en mi caso solo es para revisarlo y dejarlo funcional un tiempo.

Veamos colooco bp en el dword, y vemos si al pulsar about cambiaria algo si alteramos el resultado de nuestro is_registred. (salto del salto que proviene luego del dword anterior encontrado que llamare “is_registred” , si es is_registred true entonces me llevara a chico bueno o chico malo) aquí apreciamos si pulsamos about , valida nuestro is_registred y además me indica que rama de regedit está guardando la informacion.

```
004017EF   8B 50 1C        mov edx, dword ptr ds:[eax + 0x1C]
004017F2   6A 01           push 0x1
004017F4   56              push esi
004017F5   6A 30           push 0x30
004017F7   52              push edx
004017F8   FF D3           call ebx
004017FA   A1 F0 E2 68 00  mov eax, dword ptr ds:[0x68E2F0]   #2 about, es una version  registrada ?
004017FF   85 C0           test eax, eax
00401801   0F 85 07 02 00 00 jne idman.401A0E
00401807   A1 5C 5B 6E 00  mov eax, dword ptr ds:[0x6E5B5C]   6E5B5C:"p[n"
0040180C   89 45 E8        mov dword ptr ss:[ebp - 0x18], eax
0040180F   8D 4D E0        lea ecx, dword ptr ss:[ebp - 0x20]
00401812   C6 45 FC 01     mov byte ptr ss:[ebp - 0x4], 0x1
00401816   51              push ecx
00401817   6A 01           push 0x1
00401819   6A 00           push 0x0
0040181B   68 8C 9F 68 00  push idman.689F8C                  689F8C:"SOFTWARE\\Internet Download Manager"
00401820   68 02 00 00 80  push 0x80000002
00401825   FF 15 08 80 62 00 call dword ptr ds:[<&RegOpenKeyExA>]
0040182B   85 C0           test eax, eax
0040182D   89 45 DC        mov dword ptr ss:[ebp - 0x24], eax
```

<img21 x64dbg: viendo el acceso de is_registred>

Altero el flag de salto del jne en los registros…tengo claramente que no dice “Trial”, refiere “Full”, no dice solo versión no registrada, refiere your serial number start with…(eso no estaba en la versión anterior)



<img22: About registrado?>

Reinicio, intento ver ahora te quedan x dias misma tecnica pause return ejecuto el (opcion no del mensaje de te quedan x dias) o el messagebox y tengo: el lugar generico donde valida la cantidad de dias

```
005F6044   8B 40 10        mov eax, dword ptr ds:[eax + 0x10]
005F6047   85 F6           test esi, esi
005F6049   75 04           jne idman.5F604F
005F604B   33 C9           xor ecx, ecx
005F604D   EB 03           jmp idman.5F6052
005F604F   8B 4E 1C        mov ecx, dword ptr ds:[esi + 0x1C]
005F6052   FF 74 24 10     push dword ptr ss:[esp + 0x10]
005F6056   50              push eax
005F6057   FF 74 24 10     push dword ptr ss:[esp + 0x10]
005F605B   51              push ecx
005F605C   FF 15 FC 87 62 00 call dword ptr ds:[<&MessageBoxA>]
005F6062   5E              pop esi
005F6063   C2 0C 00        ret 0xC
005F6066   55              push ebp
```

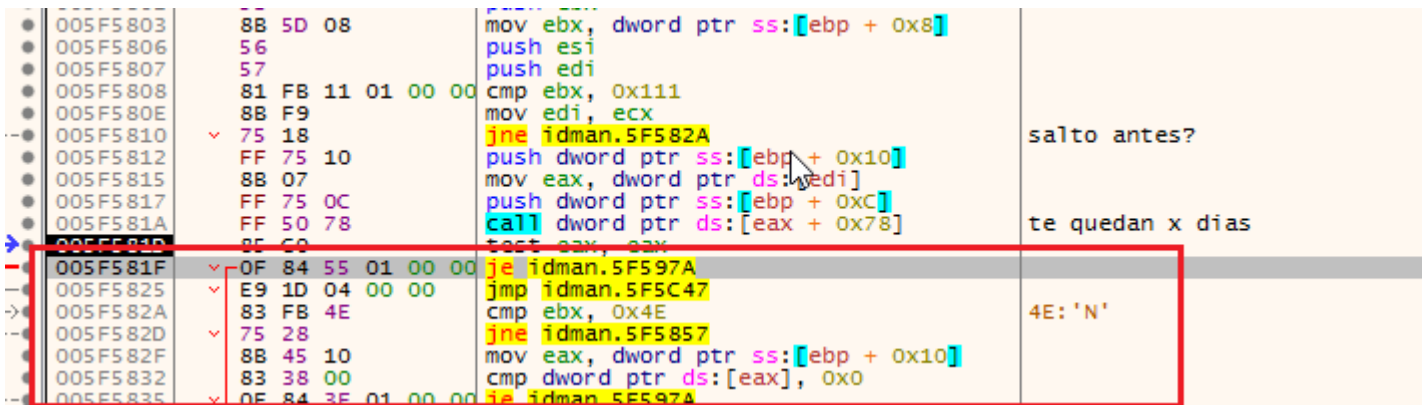
<img23 x64dbg: viendo el retorno del mensaje>

Encuentro al retorno muchas llamadas

```
Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References
004577A1   83 C4 0C        add esp, 0xC
004577A4   FF 15 F8 87 62 00 call dword ptr ds:[<&GetDesktopWindow>
004577AA   50              push eax
004577AB   E8 90 D1 19 00  call idman.5F4940
004577B0   8B 55 EC        mov edx, dword ptr ss:[ebp - 0x14]
004577B3   68 04 00 01 00  push 0x10004
004577B8   68 40 EB 6B 00  push idman.6BEB40                  6BEB40:"Internet Download Manager 6.28"
004577BD   52              push edx
004577BE   8B C8           mov ecx, eax
004577C0   E8 6F E8 19 00  call idman.5F6034                  te quedan x dias
004577C5   83 F8 06        cmp eax, 0x6                      aqui retorno luego del nag
004577C8   75 07           jne idman.4577D1
004577CA   8B CB           mov ecx, ebx
004577CC   E8 8F C1 00 00  call idman.463960
004577D1   8D 4D EC        lea ecx, dword ptr ss:[ebp - 0x14]
004577D4   C6 45 FC 00     mov byte ptr ss:[ebp - 0x4], 0x0
004577D8   E8 FC 07 1A 00  call idman.5F7FD9
004577DD   B8 01 00 00 00  mov eax, 0x1
004577E2   8B 4D F4        mov ecx, dword ptr ss:[ebp - 0xC]
004577E5   64 89 0D 00 00 00 00 mov dword ptr fs:[0], ecx
004577EC   5F              pop edi
004577ED   5E              pop esi
004577EE   5B              pop ebx
```

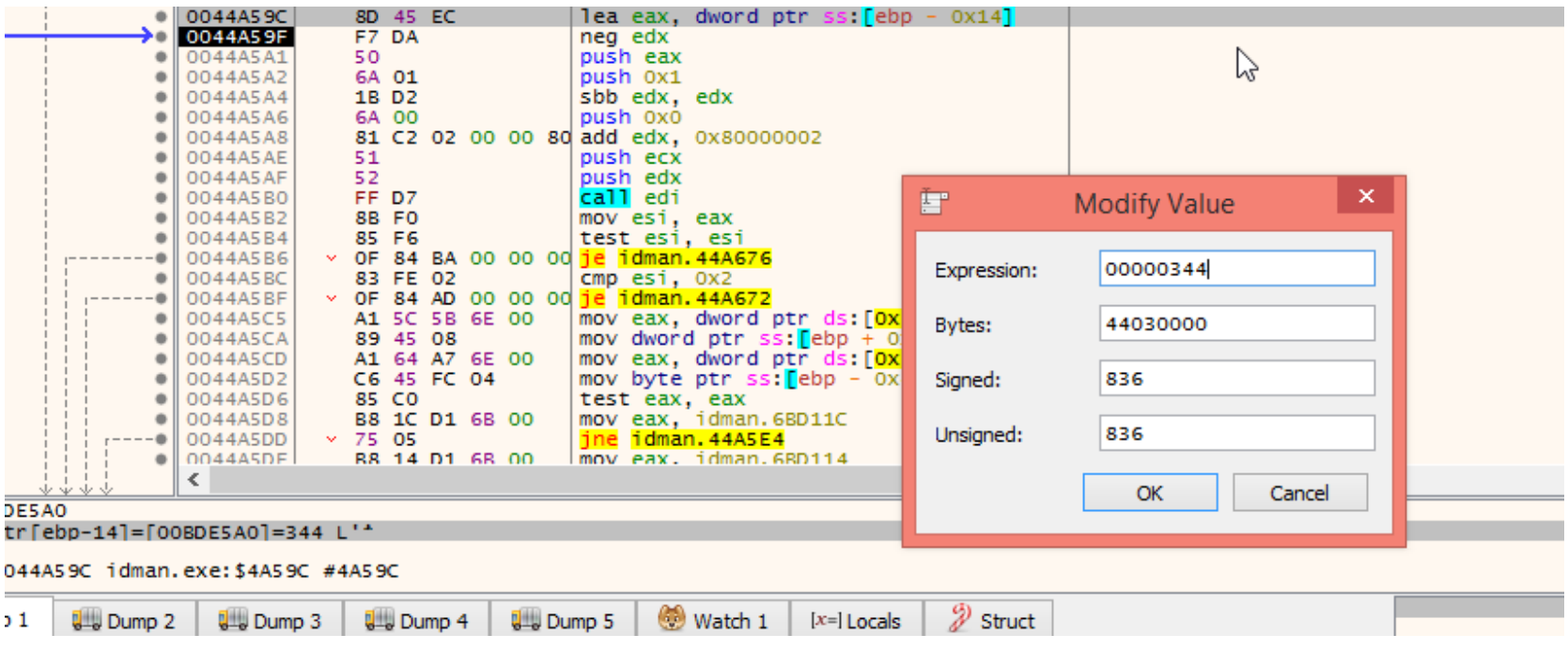
<img24 x64dbg: validando los dias>

Y luego sacamos conclusiones, denuevo un salto que valida la cantidad de dias o quien sabe que mas, su flujo es basico, compara con una cantidad de dias no se 20, luego otro valor y de ahí otro, haciendo true/false, es para perderse un poco si no se tiene costumbre.



<img25 depurando: comparaciones en multiple hacia la cantidad de días transcurridos>

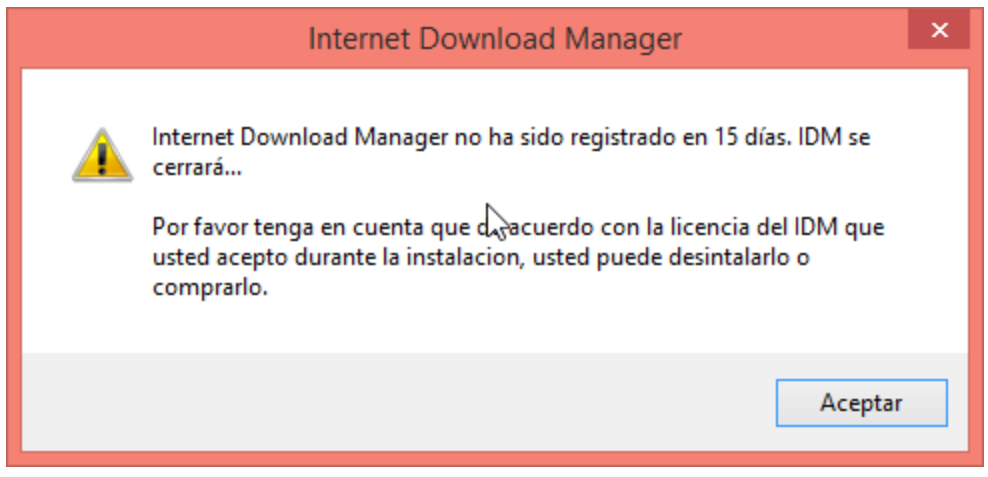
Reinicio y verifico un pequeño salto (recordemos el principio, si esta registrado no salta, si lo esta salta, y así al inverso, hago que no fuerce el salto para verificar el contenido de ebp -0x14), en este caso encuentro 344 (si recordamos que un año tiene 365 dias menos 344 es 21 bingo, aquí esta la cantidad de dias que he usado este soft (wow) , no esperaba que lo manejara desde un valor de regedit.



<img26 x64dbg: detectando la cantidad de dias actuales que tiene>

Está mas que decir que ya pille como dejar trial denuevo de 30 dias al soft, podria pasarme mucho tiempo buscando, así que me enfocare en buscar mas referencias

En este caso con este valor me quedarian entre 8 y 9 dias (21 de 30) seamos honestos, si hay unas 30 llamadas de regedit, es practicamente aburrido buscar 1 a 1 que rama puede ser la que guarda la fecha (pero ya sabemos que es un classid), en general si el programa dura mas de 30 dias, permite el botón, debería ser casi igual al registrado.
Bueno sigamos entonces por el camino del expired, adelantamos el tiempo 07/11/2017 hoy estamos a 08/07/17



<img27 programa: en tiempo expirado, anunciando que se cerrará>

Recordando el mismo dword, que hablamos al comienzo esta el salto a hacer posible seguir, diciendo que debemos alterar algunos saltos…

```
0044977A   A1 F0 E2 6B 00    mov eax, dword ptr ds:[0x6BE2F0]
0044977F   85 C0             test eax, eax
00449781   74 4D             je idman.4497D0
00449783   A1 5C 5B 6E 00    mov eax, dword ptr ds:[0x6E5B5C]      6E5B5C:"p[n"
00449788   89 45 EC          mov dword ptr ss:[ebp - 0x14], eax
0044978B   8B 0D 2C AE 6E 00 mov ecx, dword ptr ds:[0x6EAE2C]      6EAE2C:&"Por favor tenga en cuenta que de acuerdo con la li
00449791   8B 15 F8 B5 6E 00 mov edx, dword ptr ds:[0x6EB5F8]
00449797   51                push ecx
00449798   52                push edx
00449799   8D 45 EC          lea eax, dword ptr ss:[ebp - 0x14]
0044979C   68 88 B8 6B 00    push idman.6BB888                     6BB888:"%s\r\n\r\n%s"
004497A1   50                push eax
004497A2   C6 45 FC 23       mov byte ptr ss:[ebp - 0x4], 0x23     23:'#'
004497A6   E8 60 76 1A 00    call idman.5F0E0B
004497AB   8B 4D EC          mov ecx, dword ptr ss:[ebp - 0x14]
004497AE   83 C4 10          add esp, 0x10
004497B1   68 30 00 05 00    push 0x50030
004497B6   68 10 A0 6B 00    push idman.6BA010                     6BA010:"Internet Download Manager"
004497BB   51                push ecx
004497BC   6A 00             push 0x0
004497BE   FF 15 FC 87 62 00 call dword ptr ds:[<&MessageBoxA>]
004497C4   C6 45 FC 1D       mov byte ptr ss:[ebp - 0x4], 0x1D
004497C8   8D 4D EC          lea ecx, dword ptr ss:[ebp - 0x14]
004497CB   E8 09 E8 1A 00    call idman.5F7FD9
004497D0   85 F6             test esi, esi
004497D2   0F 84 D2 01 00 00 je idman.4499AA                       taken
004497D8   8B 7D C0          mov edi, dword ptr ss:[ebp - 0x40]
004497DB   6A 00             push 0x0
004497DD   8D 8D DC FC FF FF lea ecx, dword ptr ss:[ebp - 0x324]
```

<img26 x64dbg: luego de is_registred aparece el salto de la nag actual>

Mientras sigo explorando puedo ver que hay validaciones de regedit:

```
Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Thread

0044A579   A1 F0 E2 6B 00    mov eax, dword ptr ds:[0x6BE2F0]      primera validacion...posiblemente x dias
0044A57E   C6 45 FC 03       mov byte ptr ss:[ebp - 0x4], 0x3
0044A582   85 C0             test eax, eax
0044A584   0F 85 F3 01 00 00 jne idman.44A77D
0044A58A   8B 15 64 A7 6E 00 mov edx, dword ptr ds:[0x6EA764]
0044A590   8B 0D 58 B2 6E 00 mov ecx, dword ptr ds:[0x6EB258]      6EB258:&"Software\\Classes\\CLSID\\{6DDF00DB-1234-46EC-8
0044A596   8B 3D 08 80 62 00 mov edi, dword ptr ds:[<&RegOpenKeyEx
0044A59C   8D 45 EC          lea eax, dword ptr ss:[ebp - 0x14]    cantidad de dias colocar un numero no se 360 como dia 0
0044A59F   F7 DA             neg edx
0044A5A1   50                push eax
0044A5A2   6A 01             push 0x1
0044A5A4   1B D2             sbb edx, edx
0044A5A6   6A 00             push 0x0
```

<img27 x64dbg: validaciones cerca de la cantidad de dias>

Ya despues de hacer unas pruebas pequeñas, la manipulacion de dias en este caso cuando se valida es comparada en el valor de la clase, llamada a traves de ebpx -0x14 , por otro lado es algo así posible de modificar y eureka, se pueden forzar algún salto de forma indirecta (dado que le quedan x dias entonces ir por este lado..

```
977A   A1 F0 E2 6B 00    mov eax, dword ptr ds:[0x6BE2F0]
977F   85 C0             test eax, eax
9781   74 4D             je idman.4497D0                       deberia saltar
9783   A1 5C 5B 6E 00    mov eax, dword ptr ds:[0x6E5B5C]      6E5B5C:"p[n"
9788   89 45 EC          mov dword ptr ss:[ebp - 0x14], eax
978B   8B 0D 2C AE 6E 00 mov ecx, dword ptr ds:[0x6EAE2C]      6EAE2C:&"Por favor tenga en cuenta que de acuerdo con
9791   8B 15 F8 B5 6E 00 mov edx, dword ptr ds:[0x6EB5F8]
9797   51                push ecx
9798   52                push edx
9799   8D 45 EC          lea eax, dword ptr ss:[ebp - 0x14]
979C   68 88 B8 6B 00    push idman.6BB888                     6BB888:"%s\r\n\r\n%s"
97A1   50                push eax
97A2   C6 45 FC 23       mov byte ptr ss:[ebp - 0x4], 0x23     23:'#'
97A6   E8 60 76 1A 00    call idman.5F0E0B
97AB   8B 4D EC          mov ecx, dword ptr ss:[ebp - 0x14]
97AE   83 C4 10          add esp, 0x10
97B1   68 30 00 05 00    push 0x50030
97B6   68 10 A0 6B 00    push idman.6BA010                     6BA010:"Internet Download Manager"
97BB   51                push ecx
97BC   6A 00             push 0x0
97BE   FF 15 FC 87 62 00 call dword ptr ds:[<&MessageBoxA>]
97C4   C6 45 FC 1D       mov byte ptr ss:[ebp - 0x4], 0x1D
97C8   8D 4D EC          lea ecx, dword ptr ss:[ebp - 0x14]
97CB   E8 09 E8 1A 00    call idman.5F7FD9
97D0   31 F6             xor esi, esi                          deberia ser 0
97D2   0F 84 D2 01 00 00 je idman.4499AA                       taken
97D8   8B 7D C0          mov edi, dword ptr ss:[ebp - 0x40]
97DB   6A 00             push 0x0
```

<img28 x64dbg: asumo 2 valores que deberian ser para que funcione luego de expired>

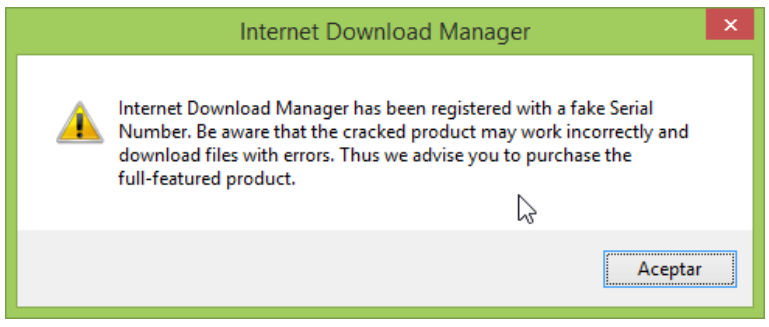
Aquí la idea seria que esi condiciona el tipo de saltos a tomar, cuando es 0 es como el mas interesante. Y con eso tenemos el programa que corre mas de los x dias establecidos… 449785

```
977A   A1 F0 E2 6B 00    mov eax, dword ptr ds:[0x6BE2F0]
977F   85 C0             test eax, eax
9781   74 4D             je idman.4497D0                       deberia saltar
9783   31 F6             xor esi, esi
9785   EB 49             jmp idman.4497D0
9787   90                nop
9788   89 45 EC          mov dword ptr ss:[ebp - 0x14], eax
978B   8B 0D 2C AE 6E 00 mov ecx, dword ptr ds:[0x6EAE2C]      6EAE2C:&"Por favor tenga
9791   8B 15 F8 B5 6E 00 mov edx, dword ptr ds:[0x6EB5F8]
9797   51                push ecx
9798   52                push edx

0|00449783:A1->31
0|00449784:5C->F6
0|00449785:5B->EB
0|00449786:6E->49
0|00449787:00->90
```

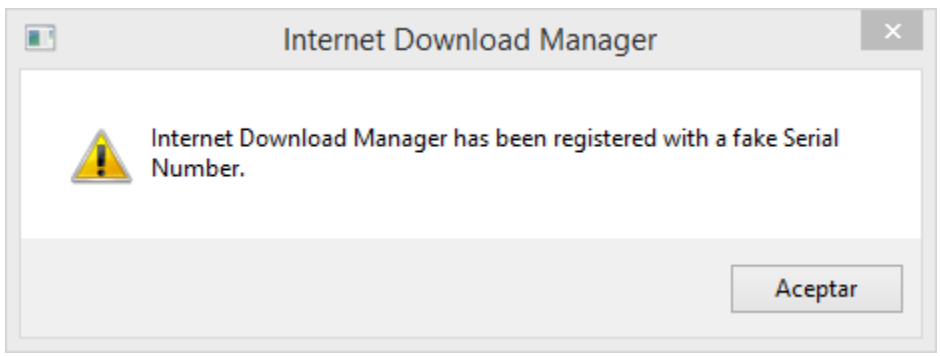
<img29-30: x64dbg parchando is_registred otra vez>

Como hemos forzado 1 valor de is_registred el programa piensa que estamos registrados, así que ahora nos validó y nos avisa con una primera nag;



<img29 programa: nag otra vez>

Y luego veo que se ejecuta otro proceso (no hereda el mismo tipo de dialogo que el primero (tiene icono arriba jeje)



<img30 programa (invocado): nag otra vez>

¿Fake serial?:

Si lo pensamos de una forma critica si hay un serial que permite registrar el programa porque ha pasado todo el algoritmo del programa, es imposible que sea un serial falso, es un serial que realmente si ha pasado la validacion del programa, lo que no es comprado, que es otra cosa, el serial que posee no está autorizado por el autor, por otro lado refiere lo siguiente:

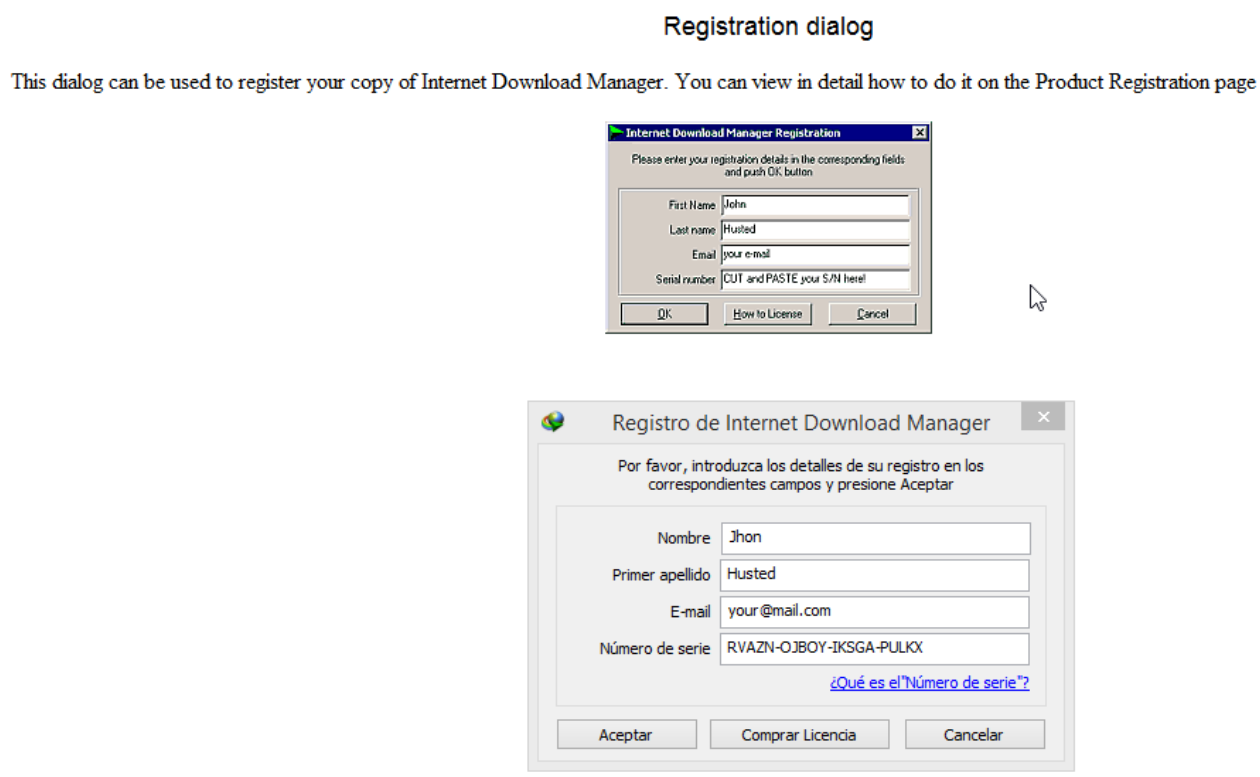
Veamos que dice el navegador que abre:

http://www.internetdownloadmanager.com/fserial.html

Internet Download Manager has been registered with a fake Serial Number.
Be aware that the cracked product may work incorrectly and download files with errors. Besides all key generators, patches and cracks will infect your computer with viruses or create a security breach which can be used to compromise your computer and all information on it including access to your banking accounts and credit cards. Also your computer can be used to conduct an illegal activity. Please NEVER use a cracked/patched versión of IDM and NEVER run cracks/patches to crack IDM!
If you would like to use IDM, you must purchase it instead of using cracks.

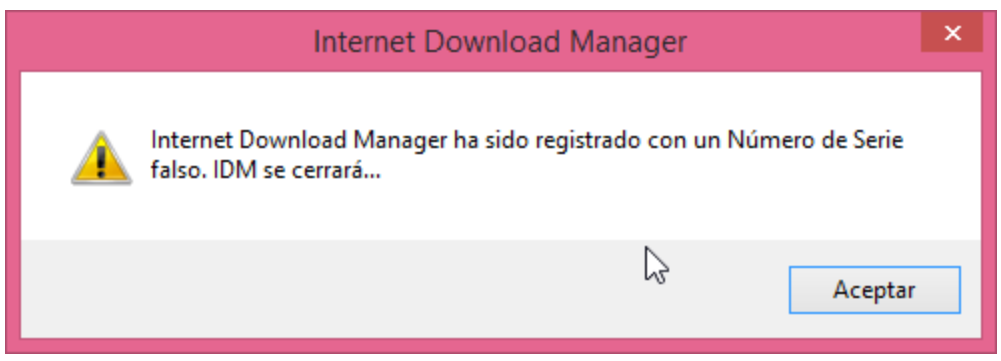
Pues aquí para quien necesite tiene un tutorial que no atenta a robar ninguna tarjet de crédito y tener el programa operativo y solo requiere conocimientos en ingenieria inversa.

Sigamos, en el caso puntual hay un Dword is registred = valido, entonces muestra full o si no trial…todo es así… al minuto parece triste que solo al minuto no hay nada nuevo,solo cambios de saltos pero sigamos explorando , así que para no hacerlo tan directo, prefiero seguir la orientacion de tutoriales del pasado, veamos, teoria 1563 haber que encuentro de nuevo, casi al finalizar el analisis del algoritmo comparte un keygen, en general solo usando un serial verifico con los datos como refiere el help:



<img31 programa:ingresando un serial valido>

Bam (pasa de largo todas las validaciones de serial , porque son correctas, pero luego pareciera conectar con internet y avisar al programa en cuestion) muestra una alerta:



<img32 programa: otra nag>

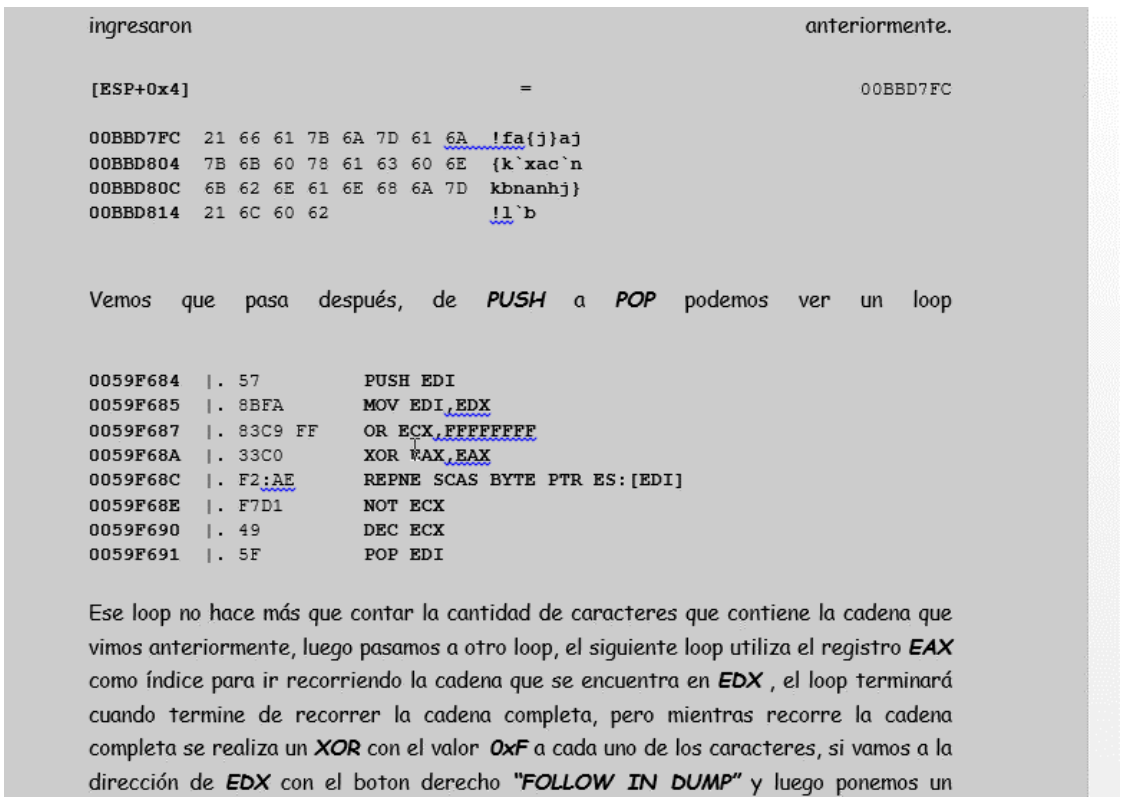
Pero si veo about si ha guardado el serial, si existe el serial valido.

<img33 programa: el supuesto serial invalido si valida de forma full al programa, solo no deja usarlo por los nags /timer y más.>

Bueno, el tema de registrarlo se puede quedar en regedit, pero ahora tenemos un registrado irresponsable, a hacernos cargo de eliminar las limitaciones adicionales, ya el programa esta registrado, ahora viene lo importante, las **validaciones online**

Validacion Online:

Guiandome del escrito parte 2 (teoria 1565) refiere la validacion online desencripta las cadenas ,y luego conecta a las webs en concreto:



ingresaron anteriormente.

```
[ESP+0x4]                          =                    00BBD7FC

00BBD7FC  21 66 61 7B 6A 7D 61 6A  !fa{j}aj
00BBD804  7B 6B 60 78 61 63 60 6E  {k`xac`n
00BBD80C  6B 62 6E 61 6E 68 6A 7D  kbnanhj}
00BBD814  21 6C 60 62              !l`b
```

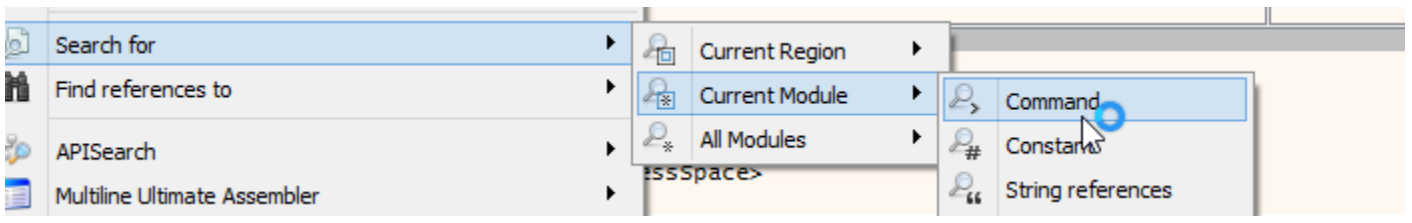
Vemos que pasa después, de ***PUSH*** a ***POP*** podemos ver un loop

```
0059F684  |. 57          PUSH EDI
0059F685  |. 8BFA        MOV EDI,EDX
0059F687  |. 83C9 FF     OR ECX,FFFFFFFF
0059F68A  |. 33C0        XOR EAX,EAX
0059F68C  |. F2:AE       REPNE SCAS BYTE PTR ES:[EDI]
0059F68E  |. F7D1        NOT ECX
0059F690  |. 49          DEC ECX
0059F691  |. 5F          POP EDI
```

Ese loop no hace más que contar la cantidad de caracteres que contiene la cadena que vimos anteriormente, luego pasamos a otro loop, el siguiente loop utiliza el registro ***EAX*** como índice para ir recorriendo la cadena que se encuentra en ***EDX*** , el loop terminará cuando termine de recorrer la cadena completa, pero mientras recorre la cadena completa se realiza un ***XOR*** con el valor ***0xF*** a cada uno de los caracteres, si vamos a la dirección de ***EDX*** con el boton derecho ***"FOLLOW IN DUMP"*** y luego ponemos un

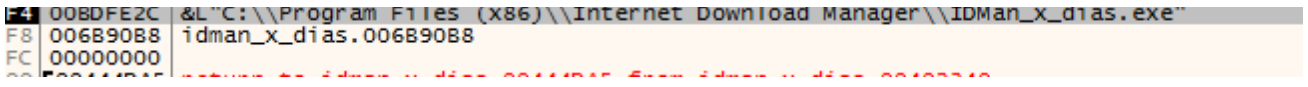
<img33 tutorial:parte 2 idm>

De aquí buscare entonces un patrón "REPNE SCAS BYTE PTR ES:[EDI]" o bien "REPNE SCAS BYTE PTR ES:[r32]"



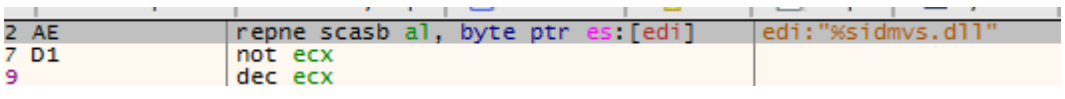
<img34 x64dbg:buscar por comandos>

Iniciando de cero en este cracked, tengo el primero apunta al exe



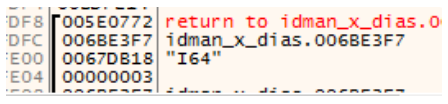
<img35 x64dbg:viendo el stack con los repne scas>

El segundo a una dll (cual podria ser la funcion?)



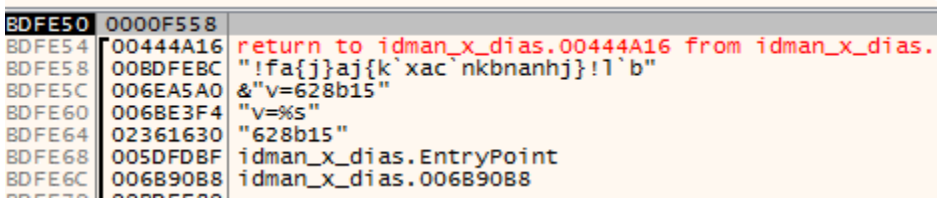
<img36 x64dbg:una dll sospechosa>

El tercero



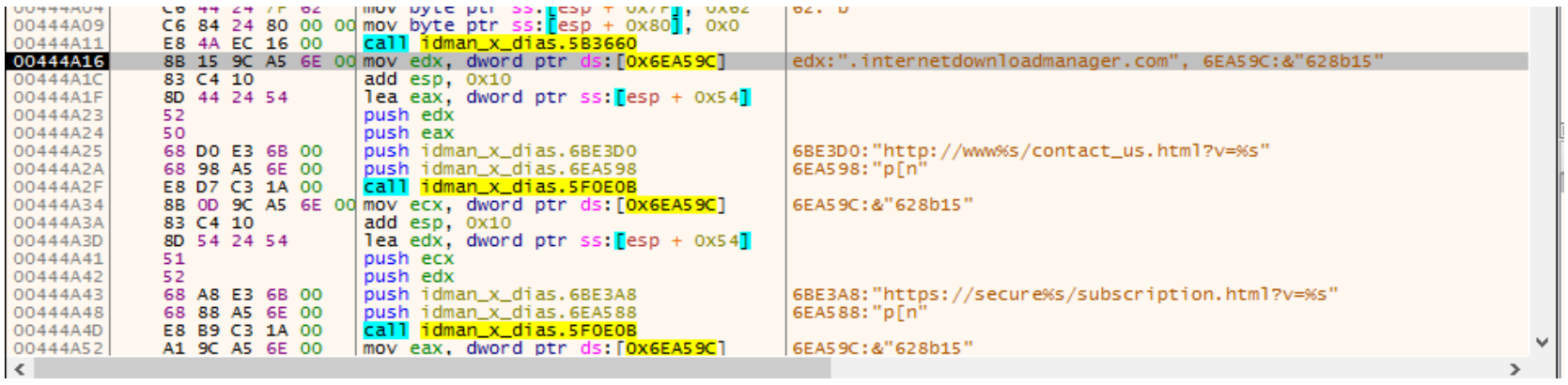
<img37 x64dbg:viendo el stack con los repne scas>

El cuarto “bingo”



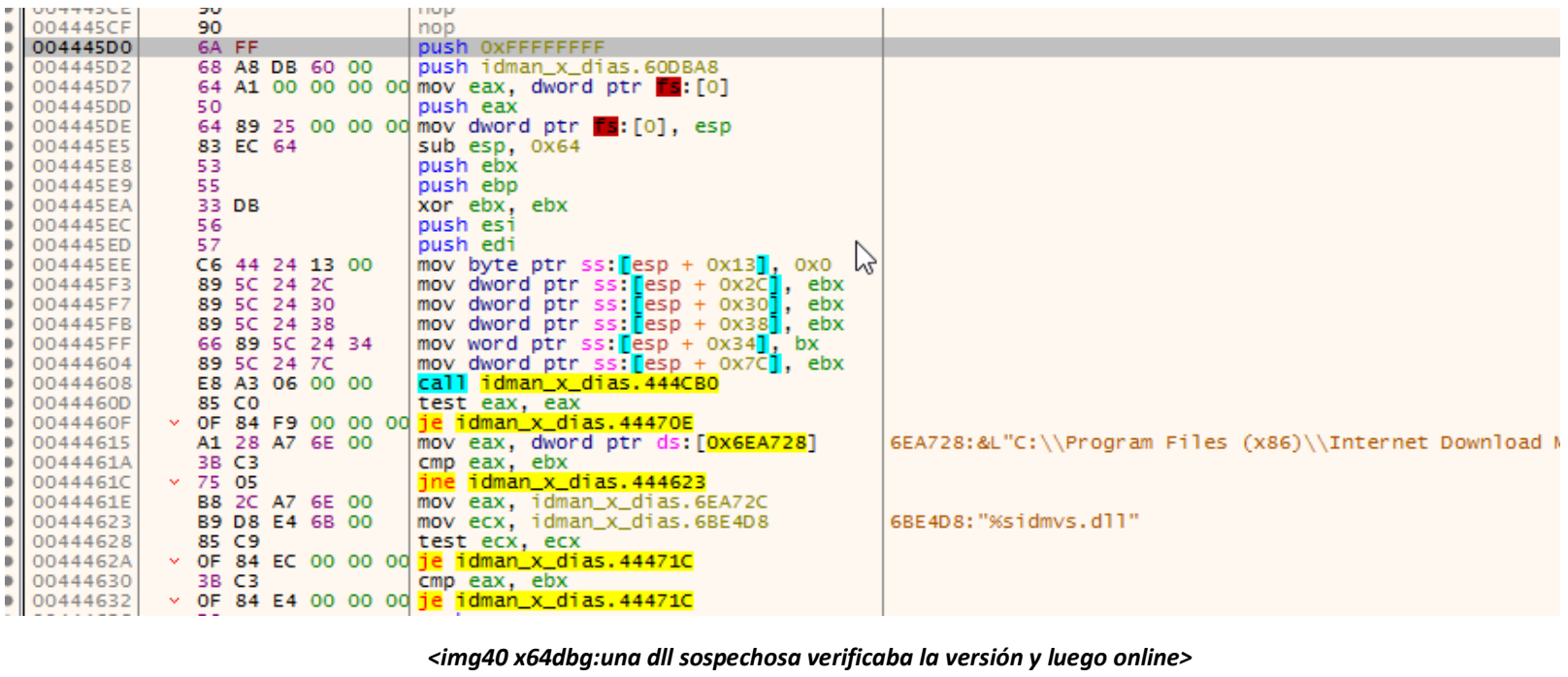
<img38 x64dbg:viendo el stack con los repne scas hemos pillado el encripted>

Vemos al retorno la famosa validacion de internet desencriptada



<img39 x64dbg:decodificado la validacion online>

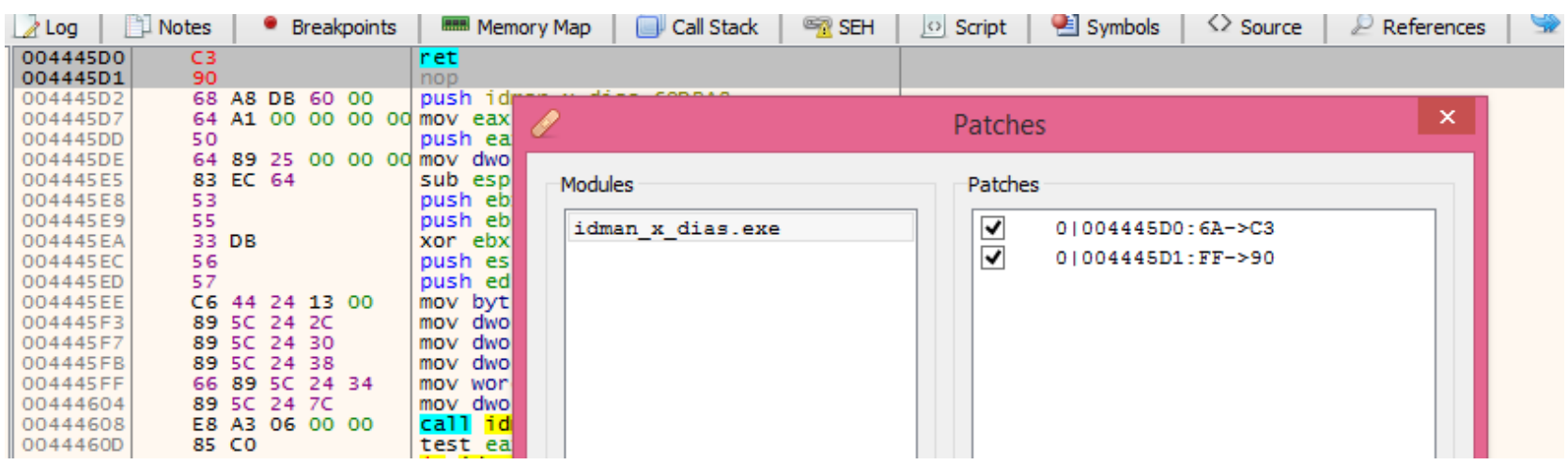
Si subo al comienzo de la rutina



<img40 x64dbg:una dll sospechosa verificaba la versión y luego online>

Fin Validacion Online:

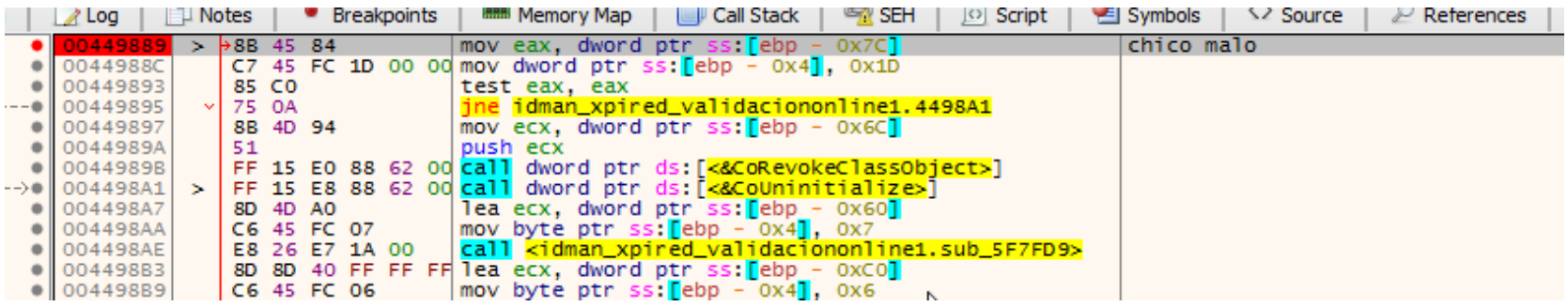
Respondemos, El dll se encargaba de verificar la versión actual ;) parchamos para que esta fncion online no exista (ret) 4445d0



<img40 x64dbg:patch , guardando los cambios del programa depurado>

Chico malo, cerrar el programa de forma silenciosa…:

Debemos pillar la zona que nos lleva a que se cierre la aplicación cuando la encontramos le llamamos chico malo guiandonos por saltos de is_registred cierra con esas 2 apis vemos que este es una salida del programa silenciosa.



<img41 x64dbg:chico malo que lleva a cerrar el programa silenciosamente>

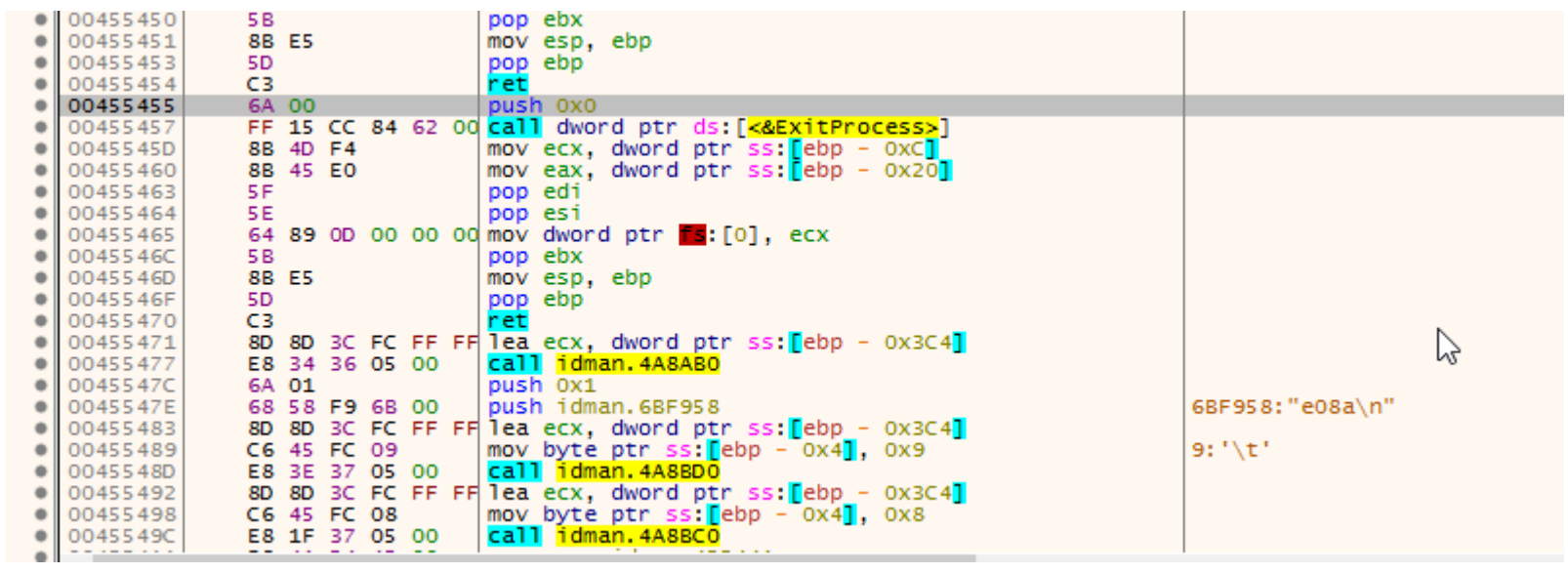
Luego se ven algunos mensajes como de timer..cuando se intenta evitar, por lo cual tambien hay timer xD

Decido entonces matar el timer que creo que es 4553ce cambiarlo un salto hacia una zona donde vaya destinado a que no se cierre

<img42 x64dbg: timer, chico malo que lleva a cerrar el programa silenciosamente>

Como se sabe que es este timer y no otro, es porque luego del set timer,

Llega a la zona de exitProcess ☺ así que lo que hago es forzar que no llegue al exitprocess



<img42 x64dbg :Lugar del timer que lleva a exitprocess osea cerrar el programa >

Bueno evitando que vaya a exit process, ya puedo estar tranqulo que no se cerrará por algún timer oculto

Si llegara a llamar otro exit process hay que rastrear de donde vienen Una vez matado las nags, ASI solo tendremos que evitar algún timer en concreto (evitando que vayan a exitprocess)

Resumen al minuto:

Hasta aquí tenemos

1) Programa que tiene un dword is_registred el salto condiciona como se ve el programa
2) Validaciones online que hace uso de decodificaciones antes de ir al sitio web (usar apis como conect, pero requere ver los export del programa)
3) Hay timer que ayuda que el programa se fuerce el cerrado en x tiempo.
4) Hay que colocar bp en exitprocess y chico malo para verificar que no llegue en ningún otro momento, hay que explorar los timers de algunos recursos para estar vigilando

Para no llegar a llegar con tantas pantallas ahora comentaré lo que viene, lo que encuentre mas relevante, pero no mostrare tanto (mensaje generico, stack, retorno, parche como lo parche etc, solo lo relevante pues en general puede que el programa no necesite aun usarlos, solo lo use en una instancia necesaria, pero no deja de ser llamativo)

Bueno luego sigo con el repe y pillo otra validacion online

```
004D3F2D    90              nop
004D3F2E    90              nop
004D3F2F    90              nop
004D3F30    55              push ebp
004D3F31    8B EC           mov ebp, esp
004D3F33    6A FF           push 0xFFFFFFFF
004D3F35    68 90 86 61 00  push idm3_xpired_validacion_timer.618690
004D3F3A    64 A1 00 00 00 00 mov eax, dword ptr fs:[0]
004D3F40    50              push eax
004D3F41    64 89 25 00 00 00 mov dword ptr fs:[0], esp
004D3F48    81 EC 84 00 00 00 sub esp, 0x84
004D3F4E    53              push ebx
004D3F4F    56              push esi
004D3F50    57              push edi
004D3F51    33 FF           xor edi, edi
004D3F53    89 65 F0        mov dword ptr ss:[ebp - 0x10], esp
004D3F56    89 7D FC        mov dword ptr ss:[ebp - 0x4], edi
004D3F59    89 7D D4        mov dword ptr ss:[ebp - 0x2C], edi
004D3F5C    89 7D DC        mov dword ptr ss:[ebp - 0x24], edi
004D3F5F    66 89 7D D8     mov word ptr ss:[ebp - 0x28], di
004D3F63    A1 A4 A5 6E 00  mov eax, dword ptr ds:[0x6EA5A4]      6EA5A4:"p[n"
004D3F68    C6 45 FC 01     mov byte ptr ss:[ebp - 0x4], 0x1
004D3F6C    50              push eax
004D3F6D    68 48 40 6C 00  push idm3_xpired_validacion_timer.6C4048  6C4048:"mailto:support@internetdownloadmanager.com?sub
004D3F72    68 7C B4 6E 00  push idm3_xpired_validacion_timer.6EB47C  6EB47C:&"mailto:support@internetdownloadmanager.com?su
004D3F77    E8 8F CE 11 00  call idm3_xpired_validacion_timer.5F0E0B
004D3F7C    B1 7B           mov cl, 0x7B                          7B:'{'
004D3F7E    83 C4 0C        add esp, 0xC
```

<img43 x64dbg:se ven mas validaciones pero que no lleva a cerrar el programa>

Pero lo importante es que no lleguen a abrir paginas ejemplo

```
00449657    75 46           jne <idman.sub_44969F>
00449659    8B 15 64 5B 6E 00 mov edx, dword ptr ds:[0x6E5B64]    6E5B64:"x[n"
0044965F    89 55 DC        mov dword ptr ss:[ebp - 0x24], edx
00449662    8B 45 A0        mov eax, dword ptr ss:[ebp - 0x60]
00449665    8D 4D DC        lea ecx, dword ptr ss:[ebp - 0x24]
00449668    50              push eax
00449669    68 04 EB 6B 00  push idman.6BEB04                     6BEB04:"https://secure.inte
0044966E    68 F8 EA 6B 00  push idman.6BEAF8                     6BEAF8:"%s?sn=%s"
00449673    51              push ecx
00449674    C6 45 FC 20     mov byte ptr ss:[ebp - 0x4], 0x20     20:' '
00449678    E8 AE 77 1A 00  call <idman.sub_5F0E2B>
0044967D    8B 55 DC        mov edx, dword ptr ss:[ebp - 0x24]
00449680    83 C4 10        add esp, 0x10
00449683    52              push edx
00449684    FF 15 F8 87 62 00 call dword ptr ds:[<&GetDesktopWindow>]
0044968A    50              push eax
0044968B    E8 50 10 05 00  call <idman.sub_49A6E0>
00449690    83 C4 08        add esp, 0x8
00449693    8D 4D DC        lea ecx, dword ptr ss:[ebp - 0x24]
00449696    C6 45 FC 1F     mov byte ptr ss:[ebp - 0x4], 0x1F
0044969A    E8 5A E9 1A 00  call <idman.sub_5F7FF9>
0044969F  > 8D 4D E8        lea ecx, dword ptr ss:[ebp - 0x18]    sub_44969F
004496A2  . C6 45 FC 1E     mov byte ptr ss:[ebp - 0x4], 0x1E
004496A6  . E8 4E E9 1A 00  call <idman.sub_5F7FF9>
004496AB  . C6 45 FC 1D     mov byte ptr ss:[ebp - 0x4], 0x1D
```

```
://secure.internetdownloadmanager.com/blocked_serial_info.html"
```

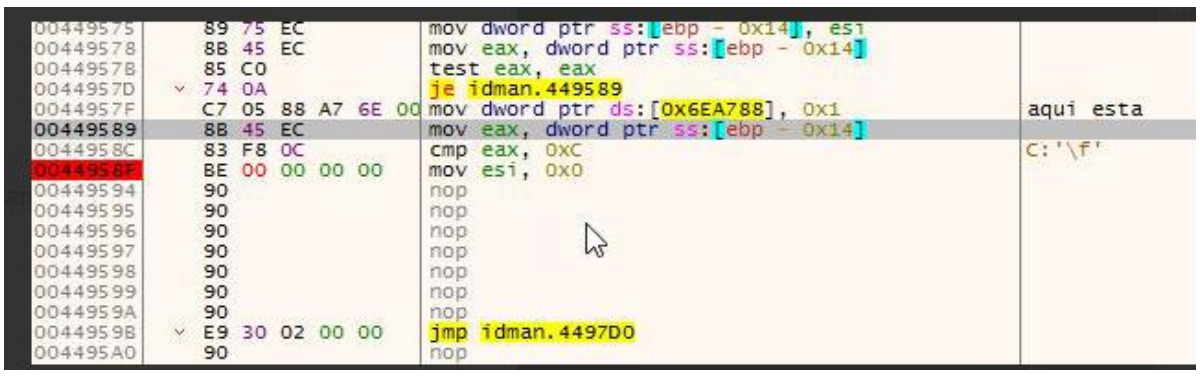
<img44 x64dbg:se ven mas validaciones, que lleva a leer una nueva web>

pero sigamos hay mas funciones que trabajan con el terminar procesos

```
005DD969    57              push edi
005DD96A    E8 9F 00 00 00  call idman.5DDA0E
005DD96F    6A 01           push 0x1
005DD971    5F              pop edi
005DD972    39 3D 5C DC 6E 00 cmp dword ptr ds:[0x6EDC5C], edi
005DD978    75 11           jne idman.5DD98B
005DD97A    FF 74 24 08     push dword ptr ss:[esp + 0x8]
005DD97E    FF 15 40 84 62 00 call dword ptr ds:[<&GetCurrentProcess>]
005DD984    50              push eax
005DD985    FF 15 A8 83 62 00 call dword ptr ds:[<&TerminateProcess>]
005DD98B    83 7C 24 0C 00  cmp dword ptr ss:[esp + 0xC], 0x0
005DD990    53              push ebx
005DD991    8B 5C 24 14     mov ebx, dword ptr ss:[esp + 0x14]
005DD995    89 3D 58 DC 6E 00 mov dword ptr ds:[0x6EDC58], edi
005DD99B    88 1D 54 DC 6E 00 mov byte ptr ds:[0x6EDC54], bl
005DD9A1    75 3C           jne idman.5DD9DF
005DD9A3    A1 98 F3 6E 00  mov eax, dword ptr ds:[0x6EF398]
005DD9A8    85 C0           test eax, eax
005DD9AA    74 22           je idman.5DD9CE
005DD9AC    8B 0D 94 F3 6E 00 mov ecx, dword ptr ds:[0x6EF394]
005DD9B2    56              push esi
005DD9B3    8D 71 FC        lea esi, dword ptr ds:[ecx - 0x4]
005DD9B6    3B F0           cmp esi, eax
005DD9B8    72 13           jb idman.5DD9CD
005DD9BA    8B 06           mov eax, dword ptr ds:[esi]
005DD9BC    85 C0           test eax, eax
```

<img45 x64dbg:se ven mas opciones que pueda cerrar cualquier proceso>

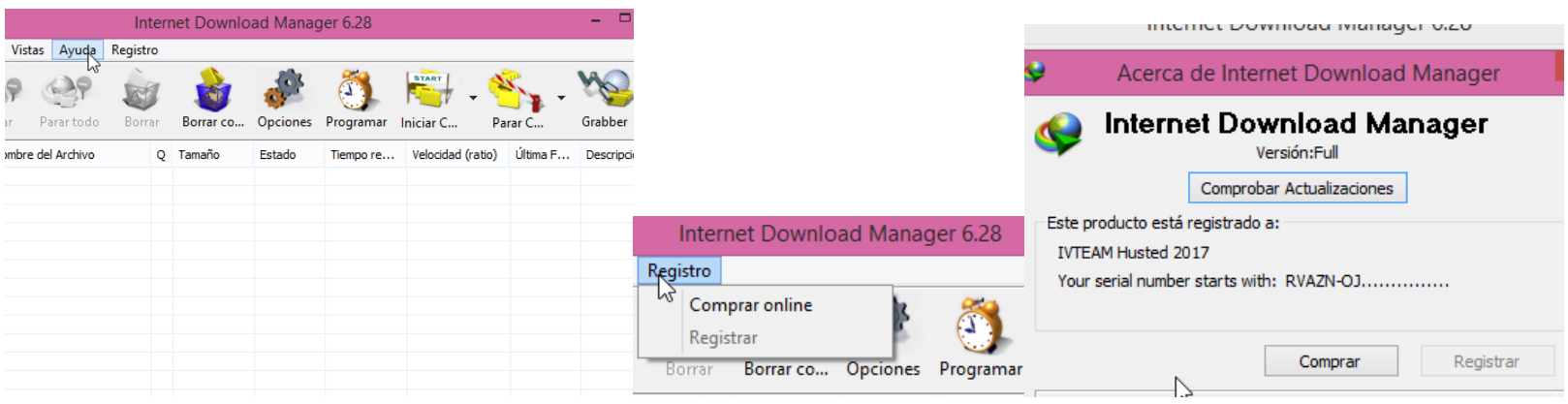
Y entre tanta condicion de salto se me ocurre parchar antes así que tenemos el salto que hace hacia el chico malo y seguir un chico bueno, todo se resume en que el valor de esi sea 0 y el valor de ebx -0x14 valida los dias. Aquí solo intentaré ver que vaya por buen camino (que evite llegar al chico malo.



<img46 x64dbg:se ven mas validaciones, este es el del chico bueno v/s malo, el mas importante del programa una vez que ha sido registrado>

Con eso ya deja de fastidiar que vuelve a registrarte, que vuelve a timer a checkear ☺, como ya hemos anulado la validacion de tiempo, el timer, el online, el valor is_registred que pillamos dando vuelta, ya esta vencido parcialmente.

¿Registred?:



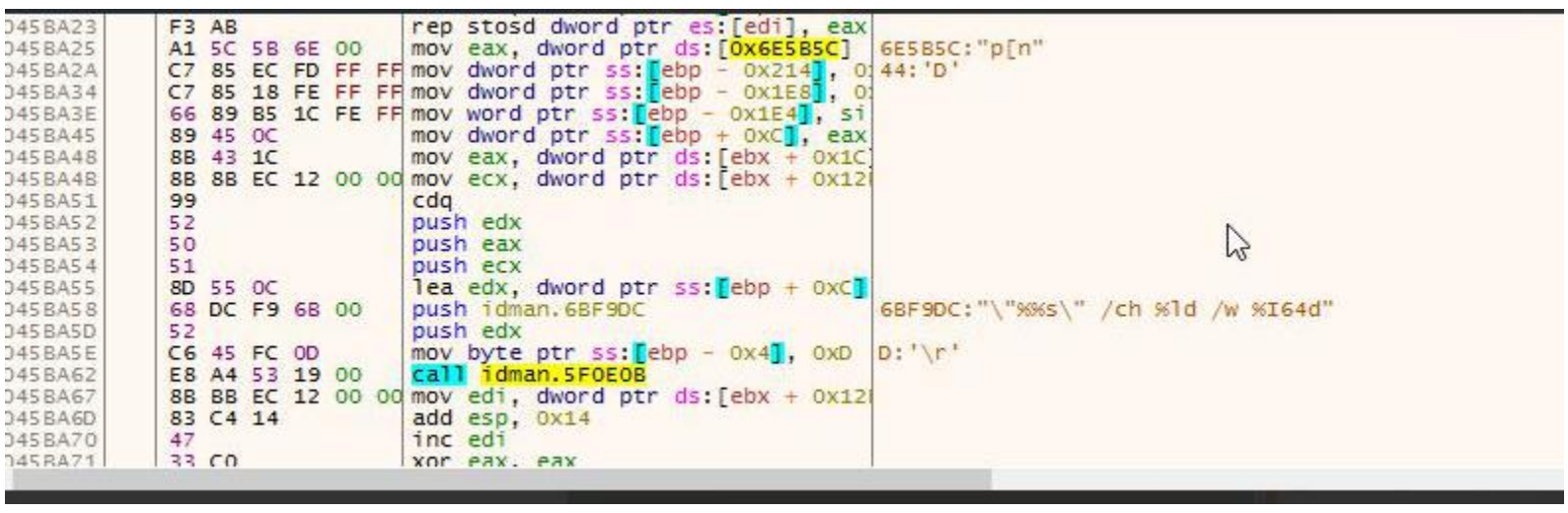
<img47,48,49 programa: ha sido registrado>

En about desaparece el registrar , desde regedit se cambia al nombre que se quiera

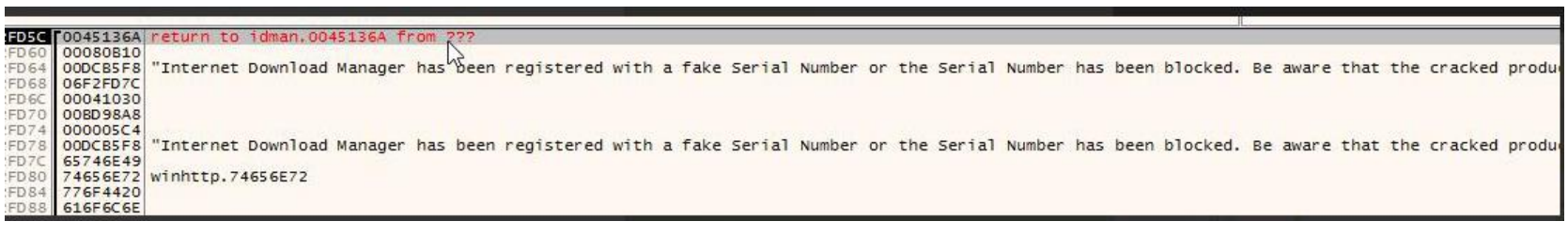
Hidden Check , los problemas luegos de un tiempo de uso:

Y luego aparece una nag desde IDMGrHlp al analizar las referencias parece invocarlo con varios parametros, reinicio y ahora en espera cuando realmente aparecera la nag (los primeros 3 no son)

Me pongo a esperar y a probar el programa si apareciera un nuevo mensaje , ahora los mensajes para cuando descargue un archivo, resultado que era otro proceso se llama aquí si comienza a prepararse para una buena nag

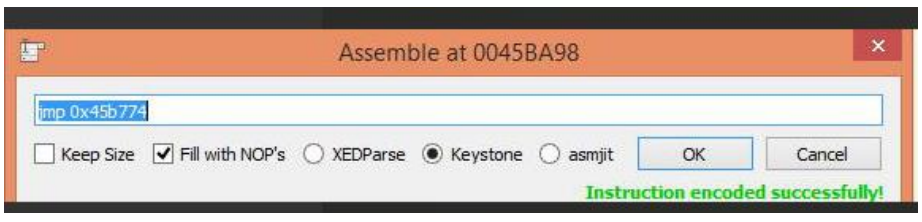


<img50 x64dbg:hidden check hacia createprocess usando IDMGrHLP>



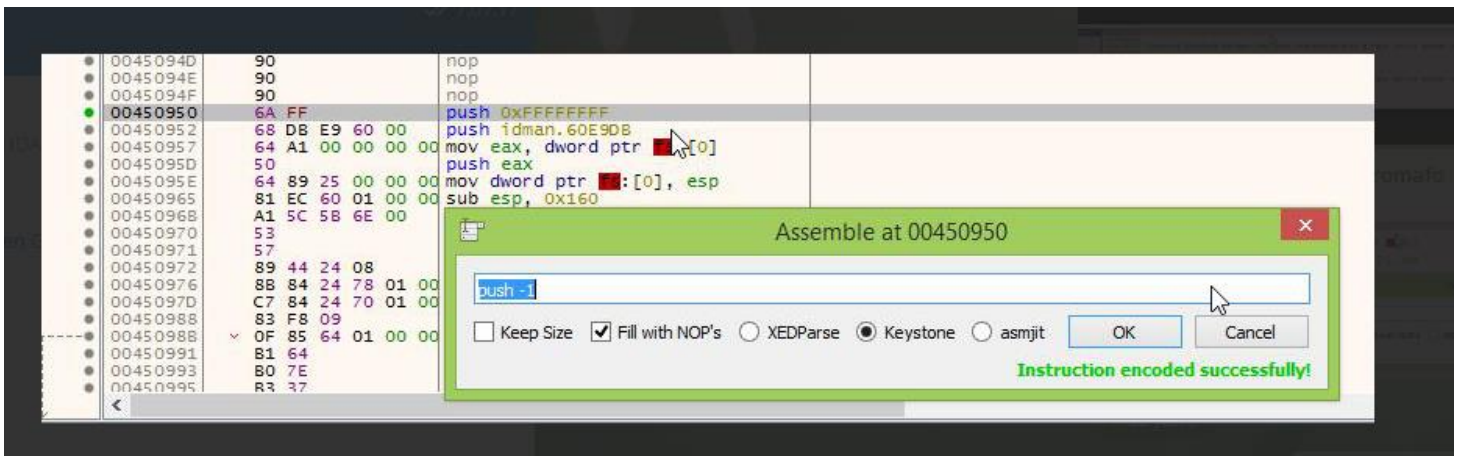
<img51 x64dbg:hidden check nueva nag>

Una vez retornado solo debemos forzar que no creee este nuevo proceso con este mensaje (que no pase a crearse el proceso)



<img52 x64dbg:hidden check nueva nag anulado>

Una vez que se evita que salte hacia el createprocessW con ese archivo, con parametros, no hay fake
Dejo pasar un tiempo mas para probarlo, luego de algunos minutos ,logro apreciar otro mensaje, retorno misma tecnica, busco el comienzo del mensaje y anulo de El comienzo es con push -1 y se cambia a ret



<img53 x64dbg:hidden check nueva nag , se rastrea y se anula la funcion colocando de push -1 a ret>

Con eso al minuto Internet download manager queda sin nuevos nags por el minuto y funcional.
adios validacion online y si te gusta el programa, compralo, solo que te advierto que si el programador piensa o sospecha de tu serial online, puede bloquearte el serial y decirte que lo estas usando en mas de una maquina y tendras que pensar bien que respuesta darle (si has comprado el soft), hasta aquí es entendible que si se pillara algo mas, solo basta anular la rutina, verificar si ha usado is_registred o bien simplemente verificar que no sea una nueva versión ☺ sino a repetir el proceso completo.

Palabras Finales:

Tengo un programa full que dura un breve tiempo (semanas), nisiquiera dependo de ingresar serial para que sea funcional, solo requiere que sea alterado a gusto, pero a conciencia, en general me ofrecí a realizar el tutorial de lo hecho pues el programa me habia quedado funcional y hay muchas cosas que en sentido critico no esta cercano a lo que ofrecen algunos teams de cracking, un uso de un buen programa, para quien obviamente lo necesite, ahora bien si alguien puede dar soporte es ideal que compren los que pueden realmente, aquí queda plasmada una experiencia,

Tiempo en ser verificado	Tiempo en hacer el tutorial
Lapsos pequeños de a 5 -10 minutos, a lo más en 1 hora ha caido	En lapsos pequeños de redacción, en lapsos de muchas imágenes y luego texto, en general referiría 1 día Solo el revisar los dias me ha llevado 1 día mas Y en terminar de leerlo de corrido para actualizar los índices 1 día mas. No me pidan corregir ortografía, es muy poco el tiempo que dispongo.

Saludos A la Lista de Crackslatinos y a TSRh.

Dedicado a los lectores que suelen practicar y/o aprender reversing o simplemente una lectura amena, está más que decir que si te ha gustado el software y si tienes la posibilidad de comprarlo no dejes de apoyar al soporte del programa.

Saludos Cordiales

Apuromafo TSRh