



FOREX TESTER 3

Activando a un asprotect by Apuromafo y de paso parchando si es necesario



19 DE SEPTIEMBRE DE 2018

CLS

Release:19/09/2018

INDICE

Contenido

INDICE	1
Introducción	2
Frase.	2
Herramientas usadas en el Escrito:	3
Analizando al protector:	4
Limitaciones del programa:	7
Manos a la Obra: Validación Online->offline	8
Errores tras activar:	10
Venciendo las últimas Limitaciones del programa:	13
Palabras Finales:	15

Introducción

Programa	Forex Tester 3
Descarga	http://forextester.com/
Dificultad	Asprotect 2.4 build 11.20 Release Depende de quien lo mire.
Objetivo	Dejarlo mas funcional que el demo
Información	Es un software que simula el tradeo en el mercado de inversiones "Forex market"
Herramientas usadas	X64dbg ,ollydbg +codedoctor, Loader, y muchas más, observación
Fecha	19/09/2018
Fecha Liberación Tutorial	19/09/2018
Autor	Apuromafo + Erisoftdevelop

Frase.

No necesitas ser un científico para ser rico. No necesitas una educación universitaria, un empleo bien pagado o dinero alguno para comenzar. Todo lo que tienes que hacer es saber qué quieres, tener un plan y seguirlo. Robert Kiyosaki



<img1.Splash inicial>

Herramientas usadas en el Escrito:

Herramienta	Descarga	Utilidad
Procesador de texto	<i>(está incluido con el suite de office)</i>	<i>Para redactar el tutorial</i>
Sharex	https://getsharex.com/	<i>Para capturar las imágenes</i>
Everything	http://www.voidtools.com/	<i>Para buscar los archivos en el pc</i>
X64dbg	http://x64dbg.com/	<i>Depurador</i>
7zip	http://www.7-zip.org/download.html	<i>Descomprimir archivos</i>
Resource Hacker	http://www.angusj.com/resourcehacker/	<i>Editor de Recursos</i>
Notepad ++	https://notepad-plus-plus.org/	<i>Editar archivos (no hexadecimal)</i>
Loader	https://www.crackinggsm.co.in/2017/11/gautams-loader-generator-beta.html	<i>Loader para comparar original y cracked y hacerle un loader</i>
Protection ID*	https://pid.gamecopyworld.com/	<i>Analizar cómo están hechos los exe</i>
IDR*	https://web.archive.org/web/20170501145746/http://kpnc.org/idr32/en/ https://github.com/crypto2011/IDR	<i>Analizador de Delphi (interactive 3elphi ...)</i>
Pexplorer*	http://www.heaventools.com/download-pe-explorer.htm	<i>Editor de Recursos de pago.</i>
Ollydbg*	http://www.ollydbg.de	<i>Depurador</i>
Codedoctor*	https://tuts4you.com/e107_plugins/download/download.php?view.2834	<i>Plugin para desempacar asprotect</i>
Stealth64 1.3*	https://tuts4you.com/e107_plugins/download/download.php?view.2425	<i>Plugin para ocultar el depurador y evitar alguno que otro crash.</i>
Aspr_idc.dll*	https://reverseengineeringtips.blogspot.com/2015/10/customizable-aspridedll-with-source-code.html	<i>Una dll customizable para asprotect por si está desempacado</i>
DecomAs	https://www.pediy.com/kssd/pediy12/135658.html	<i>Unpacker para asprotect solo para analizar Password: dNjo5RfUsaecwYPqMO8gzWn0QhV9mIA</i>
Embarcadero Delphi*	https://www.embarcadero.com/es/products/delphi/starter/free-download	<i>Compilar un programita en Delphi/pascal, obviamente en una máquina virtual ☺, sugiero Windows 8.1</i>
Windows 8.1 *	https://www.microsoft.com/es-mx/software-download/windows8ISO	<i>Iso de Windows 8.1</i>
VMWARE*	https://www.vmware.com/go/getworkstation-win	<i>Máquina virtual</i>
SwissArmyKnife	https://github.com/Nukem9/SwissArmyKnife	<i>Plugin para x64dbg que permite importar .map y otros.</i>
Windows Hack 3.0*	http://www.woodmann.com/collaborative/tools/index.php/Window_Hack	<i>Permite encontrar nombres de algún form en alguna ventana activa y más (hacerlo visible/no visible, etc)</i>
Buscador*	http://www.google.cl	<i>buscador</i>

* Herramienta opcional

Historia :

Hola Erisoftdevelop me invitó a ver esta aplicación , así que le mando un abrazo a la distancia, lo primero a comentar es que en temas económicos algunos viven como quieren, **yo en mi caso vivo como puedo**, así que si algún inversionista o proyecto de inversionista que sepa reversing, *este tutorial le dejará una idea que si es posible hacer algo para que pueda estudiar de inversiones con este programa...*



<img2.Tipos de personas que estudian inversiones viven como quieren>

Analizando al protector:

Luego de tener el instalador a mano lo primero es ver si está protegido, luego de instalar analizo en PID:

```
=[ ProtectionID v0.6.9.0 DECEMBER]-  
(c) 2003-2017 CDKILLER & TippeX  
Build 24/12/17-21:05:42  
Ready...  
Scanning -> C:\ForexTester3\ForexTester3.exe  
File Compression State : 0 (Not Compressed)  
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 15658100 (0EEEC74h) Byte(s) | Machine: 0x14C (I386)  
Compilation TimeStamp : 0x5AEC9317 -> Fri 04th May 2018 17:06:31 (GMT)  
[TimeStamp] 0x5AEC9317 -> Fri 04th May 2018 17:06:31 (GMT) | PE Header | - | Offset: 0x00000108 | VA: 0x00400108 | -  
-> File has 628 (0274h) bytes of appended data starting at offset 0EEEEA00h  
[File Heuristics] -> Flag #1 : 00000000000001001100000100100110 (0x0004C126)  
[Entrypoint Section Entropy] : 8.00 (section #0) " " | Size : 0x297200 (2716160) byte(s)  
[DllCharacteristics] -> Flag : (0x0000) -> NONE  
[SectionCount] 13 (0xD) | ImageSize 0x15AE000 (22732800) byte(s)  
[Export] 100% of function(s) (1 of 1) are in file | 0 are forwarded | 1 code | 0 data | 0 uninit data | 0 unknown |  
[VersionInfo] Company Name : Forex Tester Software Inc  
[VersionInfo] Product Version : 3.0  
[VersionInfo] File Version : 3.3.0.59  
[VersionInfo] Internal Name : Forex Tester 3  
[ModuleReport] [IAT] Modules -> kernel32.dll | oleaut32.dll | advapi32.dll | user32.dll | user32.dll | gdi32.dll | version.dll |  
advapi32.dll | oleaut32.dll | oleaut32.dll | ole32.dll | comctl32.dll | shell32.dll | wininet.dll | comdlg32.dll | wsock32.dll | shell32.dll |  
user32.dll | msvcrt.dll | winspool.drv | winspool.drv | winmm.dll | oledlg.dll | advapi32.dll | oleaut32.dll | kernel32.dll  
[!] ASProtect SKE v2.72 or higher detected !  
[CompilerDetect] -> Borland Delphi (unknown version) - 80% probability  
- Scan Took : 0.797 Second(s) [00000031Dh (797) tick(s)] [501 of 580 scan(s) done]
```

Lo primero que se aprecia es que tiene **asprotect**, desempacamos con ollydbg +stealth +codedoctor
Luego colocamos nuestra dll customizada al lado (está en la sección de herramientas)

el resultado no es bueno, ejecuta un splash , pero no continua porque tiene muchas excepciones ,
ahora a leer la información de los logs de Codedoctor y DecomAs

De codedoctor, tenemos la información de registro y el packer usado en su versión exacta 2.4

Version Info:

[Forex Tester], [3], [2.4 build 11.20 Release], [Natalia Makeeva].

Ya tenemos la versión de asprotect, y quien registró ese asprotect, podemos usarlo para registrarnos a su nombre, al usar Google encontramos un mail cualquiera Natalya.Makeeva@moex.com , sigamos

Leyendo la información se resume que este asprotect tiene de protecciones:

Overlay (extra data)

Victim: C:\ForexTester3\ForexTester3.exe

Start...

Extra data found at RAW: 00EEEEA00, Size: 00000274

===== Overlay =====

Size: 274h

Offset Original: EEEA00h

Offset New: 1473000h

Aspr DLL -> ImageBase: 032D0000, SizeOfImage: 0005A000

=====

(Asprotect sdk)AsProtect envelope functions:

(note: these are used only if aspr_ide.dll is imported)

Processing "aspr_ide.dll"...

N- 00899D20: GetHardwareID

N- 00899D24: CheckKey

N- 00899D28: CheckKeyAndDecrypt

Number of functions: Eh

ID 1h, Address: 42C49Ch, Name: GetRegistrationKeys

ID 2h, Address: 42C4B8h, Name: GetRegistrationInformation

ID 3h, Address: 42C508h, Name: RemoveKey

ID 4h, Address: 42C5F4h, Name: CheckKeyAndDecrypt

ID 5h, Address: 42C550h, Name: CheckKey

ID 6h, Address: 42C72Ch, Name: GetKeyDate

ID 7h, Address: 42C794h, Name: GetKeyExpirationDate

ID 8h, Address: 42C7FCh, Name: GetTrialDays

ID 9h, Address: 42C858h, Name: GetTrialExecs

ID Ah, Address: 42C8B4h, Name: GetExpirationDate

ID Bh, Address: 42C91Ch, Name: GetModelInformation

ID Ch, Address: 42C96Ch, Name: GetHardwareIDEx

ID Dh, Address: 42CA28h, Name: GetHardwareID

ID Eh, Address: 42CA9Ch, Name: SetUserKey

===== API information =====

Code stolen +morph

===== Virtualized dll functions =====

Stolen functions - RVA in exe and Offset in Poly:

PUSHes - Offset and Destination in Poly:

A partir de idr.exe tenemos 2 desempacados distintos (uno de decompas y otro de codedoctor), podemos afirmar que es un delphi-XE4 y las direcciones que veamos en ambas, serán validas entonces para parchar en memoria , comencemos entonces:

Desde el depurador ocultando lo básico (pulsar en barra de comandos HIDE) y hacer los mismos pasos cuando desempacamos un asprotect, lo primero es saber bien el oep :encontramos el salto al oep y el oep como tal.

```
04450126 03DF      ADD EBX,EDI
04450128 5B          POP EBX
04450129 334424 08     XOR EAX,DWORD PTR SS:[ESP+8]
0445012D C1D8 C5      RCR EAX,0C5                ; Shift constant out of range 1..31
04450130 58          POP EAX
04450131 8D8408 341539C5 LEA EAX,DWORD PTR DS:[EAX+ECX+C5391534]
04450138 2BC1        SUB EAX,ECX
0445013A 03C3        ADD EAX,EBX
0445013C 5C          POP ESP
0445013D FFE0      JMP EAX
```

ese jmp salta al oep **00C6E3C8**

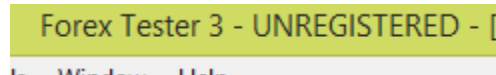
este dato nos ayudará a futuro a cargar los maps, o bien si el unpacked necesita ser corregido, saber desde donde comenzar a tracear osea si tengo el packed , puedo usar un hw bp y detenerme directamente en el oep, y así comenzar a ver la aplicación según la necesidad,

yo en este tiempo luego de usar un tiempo prudente, ya conozco las limitaciones del programa, asi que de ahí continuamos probando que tanto llegamos...

Limitaciones del programa:

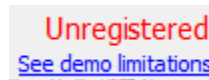
Lo primero a conocer es la parte trial

- 1) El título refiere unregistered



<img3.Limitación 1:estético>

- 2) Al costado refiere unregistered



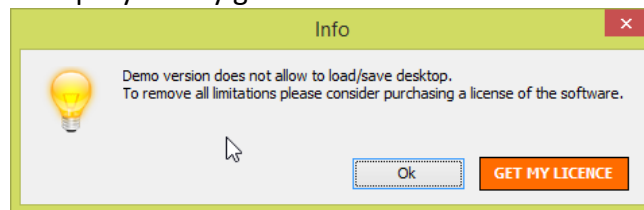
<img4.Limitación 2:estético>

- 3) En about refiere not activated , además con validación online

Status: NOT REGISTERED

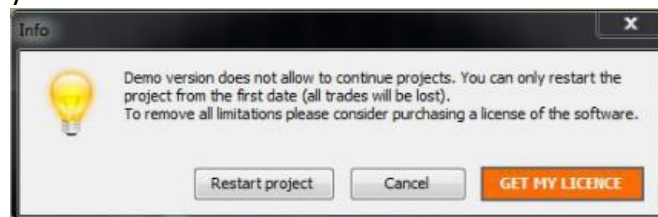
<img5.Limitación 3:estético>

- 4) Funcionalidades de guardar proyectos y guardar el escritorio no funcionan



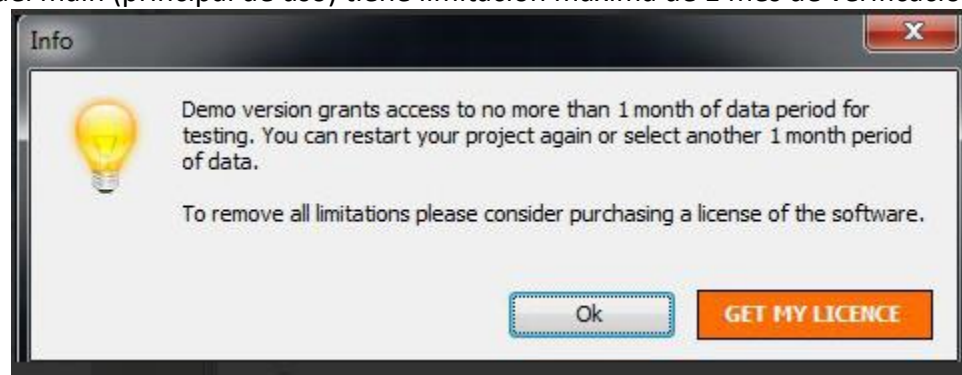
<img6.Limitación 4:nag>

- 5) En el uso del main (principal de uso) te manda a reiniciar lo hecho , además de opciones de guardar la vista actual y otras.



<img7.Limitación 5:nag>

- 6) En el uso del main (principal de uso) tiene limitación máxima de 1 mes de verificación



<img8.Limitación 5:nag con timer>

Manos a la Obra: Validación Online->offline

Cuando se lleva tiempo pensando como vencer una validación online, pues a todos se nos ocurre hacer algo offline, pero que requerirá programar algo, yo usaré embarcadero Delphi en una máquina virtual con windows 8.1 y de paso una versión trial activada con un mail temporal, pero es válido usar otras alternativas mas livianas como el Lazarus.

Exploramos primeramente la validación online, pasé horas intentando ver si podía encontrar algún dato importante, y si lo hay Existe una validación online desde nuestros datos

<http://www.forextester.com/partners/AffSystem/activate.php?type=FT3&name=Natalia%20Makeeva&email=Natalya.Makeeva@moex.com&id=0&mkey=1234-1234-1234-1234-1234>

el resultado es 'ERR,3,Key not found'

hasta aquí en el depurador tenemos una información importante, que luego de validar el serial tiene una respuesta del servidor y la almacena en su ruta de instalación+TEMP+reply

probaré con una respuesta diferente (reply.txt) almacena este mensaje, al cambiarlo por 0,4,Key found , me da un activated, asi que me propongo hacer algo para codear:

y además En el archivo host de Windows %windir%\System32\drivers\etc\ colocamos la entrada 127.0.0.1 www.forextester.com

Round 1: activación online-offline en Delphi,

```
unit Unit1;

interface

uses
  Winapi.Windows, Winapi.Messages, System.SysUtils, System.Variants,
  System.Classes, Vcl.Graphics,
  Vcl.Controls, Vcl.Forms, Vcl.Dialogs, IdBaseComponent, IdComponent,
  IdTCPServer, IdHTTPServer, StdCtrls,
  ExtCtrls, HTTPApp, IdContext, IdCustomHTTPServer, IdCustomTCPServer,
  IdTCPConnection, IdTCPClient, IdHTTP;

type
  TForm1 = class(TForm)
    Memo1: TMemo;
    IdHTTPServer1: TIdHTTPServer;
    procedure HTTPServerCommandGet(AContext: TIdContext;
      ARequestInfo: TIdHTTPRequestInfo; AResponseInfo: TIdHTTPResponseInfo);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
implementation
{$R *.dfm}

procedure TForm1.HTTPServerCommandGet(AContext: TIdContext;
  ARequestInfo: TIdHTTPRequestInfo; AResponseInfo: TIdHTTPResponseInfo);
begin
  if (ARequestInfo.Document = '/partners/AffSystem/activate.php') then
  begin
    AResponseInfo.ContentText := '0,4,License Found';
  end;
end;
end.
```

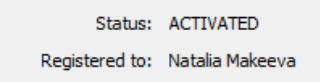
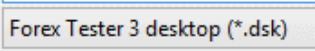
Probamos ejecutarlo (componente indi+memo+ cruzar los dedos), si :



Bien, ahora probamos en el programa con el link:

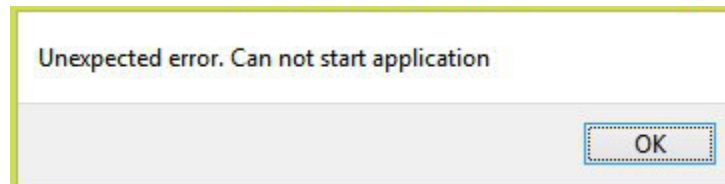


podemos activarlo de forma offline, el programa queda activado ya sea el mensaje que sea en el 3er parámetro, el primero no debe ser ni 2 ni 3 ,ni decir err

Limitación	Vencida con la activación online
1) El título refiere unregistered	Si se reinicia el escritorio, si se va
2) Al costado refiere unregistered	No, queda en el menú lateral
3) En about refiere not activated , además con validación online	about, si es activado “activated”  <img10.Mensaje de activado>
4) Funcionalidades de guardar proyectos y guardar el escritorio no funcionan	Si funcionan, no salen nags, además puedes guardar sin problema  <img11.activado las opciones de guardar>
5) En el uso del main (principal de uso) te manda a reiniciar lo hecho , además de opciones de guardar la vista actual y otras.	Si , es vencido, No reinicia el proyecto, no salen nags
6) En el uso del main (principal de uso) tiene limitación máxima de 1 mes de verificación	En forma parcial, sale una nag al ser mayor del mes.

Errores tras activar:

Reiniciamos:



<img12.crash al reiniciar>



<img13.impresión con tanto crash, una imagen de Chan Kong-sang a.k.a Jackie Chan>

Bueno, luego de verificar tenemos un antes y un después de activar, si activamos tenemos la oportunidad de tener las opciones que antes no, solo debemos editar bien el “options.dat” pues ahora se le insertaron algunos valores con algo inválido

La solución 1, es borrarlo en la ruta

(solución 2 editarlo)

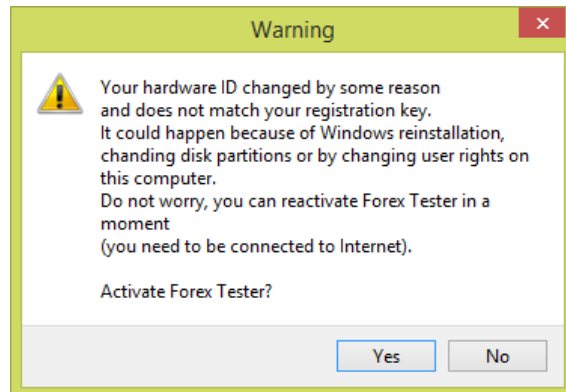
```
MasterKey=  
RegistrationKey=  
HardwareID=  
UserName=  
UserEmail=  
ProjectName=
```

Son insertados estos datos, y al ser erróneos son detectados, no es tanto los datos sino el Project name, el original era Sample, corregimos y tenemos, ahora con los datos nuestros.

funcionan con registration key no vacío ni proyect vacío. (solución 3)

```
MasterKey=1234-1234-1234-1234-1234  
RegistrationKey=999  
HardwareID=0  
UserName=Natalia Makeeva  
UserEmail=Natalya.Makeeva@moex.com  
ProjectName=Sample Project
```

Al reiniciarlo ahora:



<img14.detección del id -> sdk de asprotect >

Bueno, que mas esperaban, el id es detectado xD , aquí vemos que al reiniciar estamos con nuestros datos, y al ver todo este panorama, tenemos solo que continuar.



<img15.About luego de estos datos ingresados >

Vemos que los datos han sido validados, pero no activados, así que ahora tocará analizar con idr un poco más, activamos offline cuantas veces queramos, no hay problema de ahora en adelante, no hay que ingresar datos diferentes , y guardar el options.dat con 7z porsiacaso. El sabe project y other features funciona, solo faltan los detalles estéticos y 1 nag.

Here you can see the difference between a free demo and a paid version of Forex Tester

Benefits	Demo version (free) ?	Full version (paid)
Amount of <i>data</i> for back testing	No more than <u>1 month</u> of historical data	Unlimited. You can test strategies on 17 years of our free data service + Import any amount of data for any symbol from external sources
Amount of <i>time</i> for back testing	No more than <u>1 hour</u> of uninterrupted testing	Unlimited. Test your strategies, save projects, resume testing anytime you need – <i>lifetime license</i>
Save projects ?	✗	Save and open any number of projects
Other features	✓	✓
Support ?	✓	✓
		• 10 simple manual strategies to start

<img16.Limitaciones que refiere de la web >

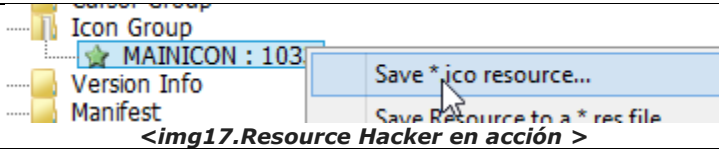
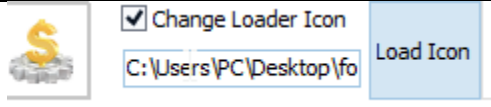
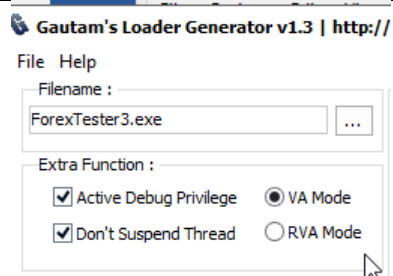
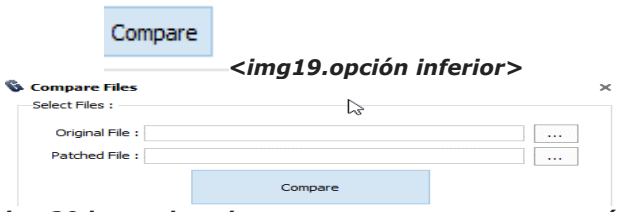
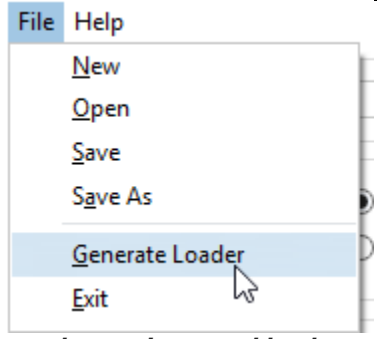
Tarea de Parchar Asprotect 2.xx:Loader

¿Cómo se parcha en asprotect 2.4?

Leímos a partir de algunos escritos y casi todo sugiere hacer mejor un loader o programa que parche al ejecutar el programa su crc , aquí usaremos un loader:

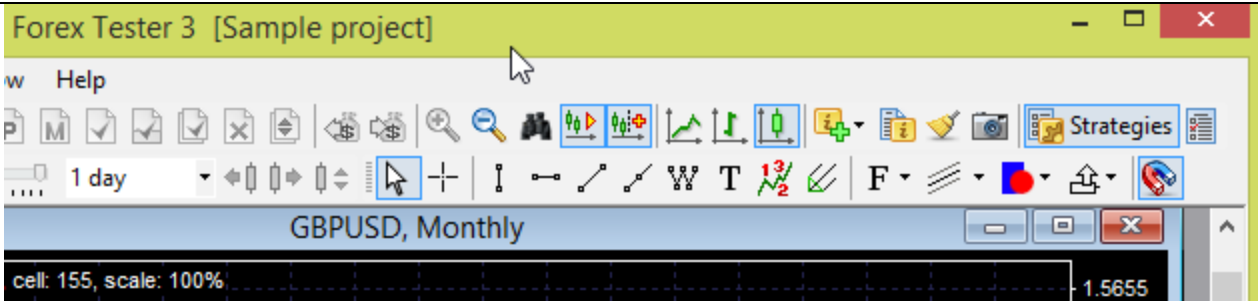
Dup 2->detectado (error)

Gautam loader 1.3->no detectado , Así que seguimos con este loader :

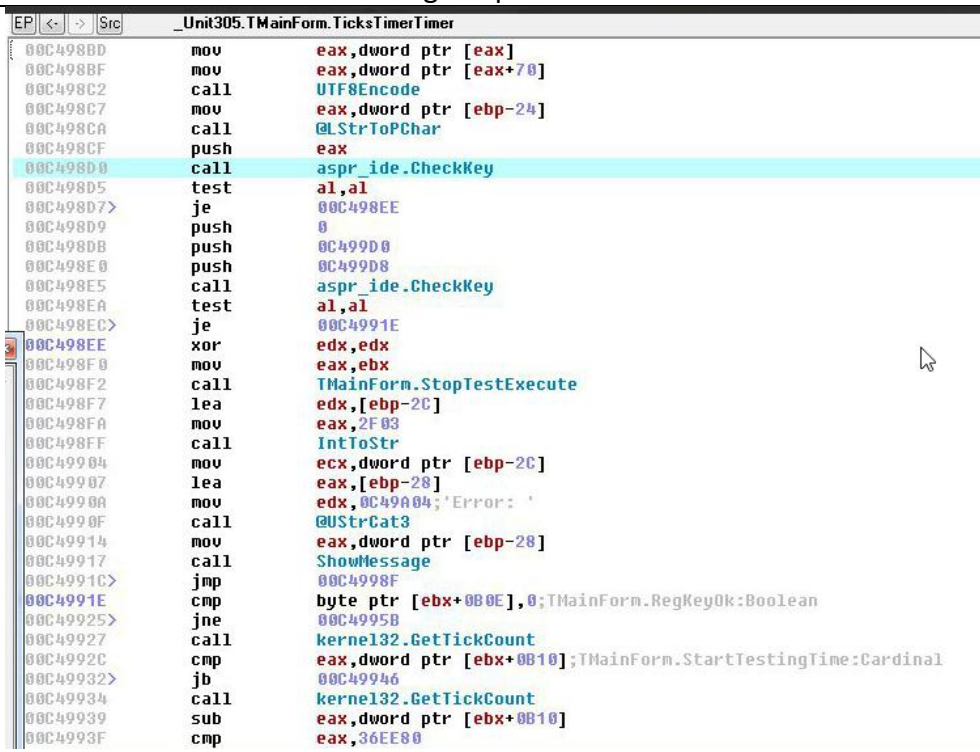
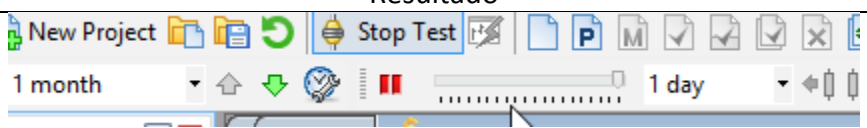
Imagen	Descripción
 <p><img17.Resource Hacker en acción ></p>	Para sacar el icono del forextester3.exe, abrimos el resource hacker y en el main icon, lo guardamos así en .ico
 <p><img17.loader con icono ></p>	Luego cargamos el icono a partir del .ico
 <p><img18.loader con opciones ></p>	Ahora hay que ver las direcciones, yo lo trabajaré con VA, y funciona con las opciones posibles
 <p><img19.opción inferior></p> <p><img20.luego de pulsar compara aparece este menú ></p>	Original.exe y parchado.exe *Usaremos el programa unpacked (si el que usaba el api_dll) *Usaremos el programa unpacked en x64dbg y guardaremos el cambio que queremos como parchado.exe
 <p><img21.luego de terminar en el loader, se guarda></p>	Para cuando ya tenemos todas las direcciones, generamos el loader

Con estas opciones son más que suficiente para seguir, en resumen teniendo claro las limitaciones, debemos buscar ahora en el depurador los lugares claves y cambiarlos, aquí nos apoyaremos de IDR, porque necesitamos la información más importante, y en esto se pueden pasar días...

Venciendo las últimas Limitaciones del programa:

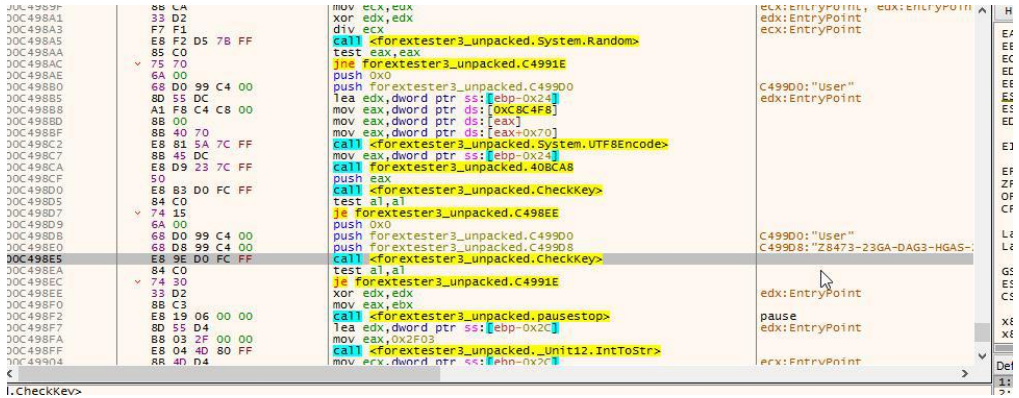
Lugar a parchar	¿Cómo parchar?
<p>Unit305.TMainForm.Registered</p> <pre> 00C543B4 mov eax,[0C8C4F8];^guar_00C95F28:TOptions 00C543B9 mov eax,dword ptr [eax] 00C543BB cmp dword ptr [eax+6C],0 00C543BF> jbe 00C543CE 00C543C1 mov eax,[0C8C4F8];^guar_00C95F28:TOptions 00C543C6 mov eax,dword ptr [eax] 00C543C8 cmp dword ptr [eax+70],0 00C543CC> jne 00C543D1 >00C543CE xor eax,eax 00C543D0 ret >00C543D1 mov al,1 00C543D3 ret </pre> <p><img22.Mainform_Registered IDR.exe></p>	<p>Este lugar valida si está o no registrado (0/1) TOptions > que tenga un valor en el puntero +6c /+70 en valores que no sean cero luego no necesitar activar pero dará errores random por ser muchas llamadas a los dword</p> <p>> cambiar el retorno de 0 a 1 antes del return Para que el programa inicie sin los 3 problemas estéticos Analizando el lugar hay 3 call a este lugar >otra forma seria parchar los saltos asociados a estos 3 lugares para lograr el mismo resultado.</p>
Resultado:	
 <p><img22.Mainform_Registered cuando es 1, no hay limitación estética></p>	

Viene la última funcionalidad a vencer y con esto damos fin a este tutorial.

Lugar a parchar	¿Cómo parchar?
	<p>Parchar la sdk- >retornará 1 o con nombre+serial si así lo quieren.</p> <p>Parchar los saltos >que no vaya a stop test execute</p> <p>Parchar regkeyok boolean >de 0 a 1</p> <p>sea como sea es solucionable de forma tradicional de evitar caer en el chico malo (stoptestexecute)</p>
<img23.Mainform_ TicksTimerTimer cuando es 1, no hay limitación estética>	
Resultado	
	
<img24.sin limitación de la nag >	

Nota: Es posible usar los maps de IDR.exe del unpacked.exe y exportar el .map ; luego x64dbg con SwissArmyKnife podrás importarlos y con ello mejorará la vista de todos los símbolos para usarlos ya sea en el

unpacked o en el packed (detenido en el oep)  <img25. .maps >



<img26.viendo con los simbolos cargados desde el map cambia la apariencia de donde depuramos >

Palabras Finales:

Tenemos un programa que ha sido revisado tiene asprotect, así que engañarlo no es fácil. No se ha mostrado todos los parches del programa ni los intentos iniciales cuando quería activarlo, pero para dejar una idea amena que es posible solo explorando con IDR (herramienta indispensable del tute), y el unpacked en el cual cada uno verá que quiere hacer, los parches quedan a la imaginación de cada uno, y la finalidad principal no es liberar un crackeado, sino demostrar que se pueden vencer las limitaciones en ciertos programas aunque tengan asprotect en este caso tiene hasta sdk y muy bien implementados, en este programa revisé por la red y existe un keygen para la versión 1.0 por el team Revenge pero nada para la versión que acabo de ver.

Tiempo en ser verificado	Tiempo en hacer el tutorial
Lapsos pequeños de a 5 -10 minutos, a lo más en 2 horas ha caído, en 1 día.	En lapsos pequeños de redacción, 2 horas a lo más No me pidan corregir ortografía, es muy poco el tiempo que dispongo, recuerden que yo vivo como puedo.

Saludos A la Lista de Crackslatinos, PeruCrackers 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 y si me quieres regalar algo **puede ser la respuesta correcta del servidor si es que lo compras y lo depuras en el repy.txt**.

Saludos Cordiales

