[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

Software	I Hate This Key Deluxe v5.0.0.98(http:/www.bytegems.com)
Descarga	http://www.bytegems.com/files/IHateThisKeyDeluxeSetup.exe I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)
Protección	**Serial.**
Herramientas	Windows 10 Version 1803 x64 Bits (SO donde trabajamos) OllyDBG OllyICE v1.10 (for.Win_v8.1_x64 nad_x32) Visual Studio 2015 (VB.NET)
SOLUCIÓN	SERIAL VÁLIDO + KEYGEN
AUTOR	LUISFECAB
RELEASE	Julio 2018

INTRODUCCIÓN

Todo lo que escribí lo perdí, más de cinco días haciendo este tuto, eran má de 34 páginas. Me sentía muy contento, de lo que había hecho; había explicado paso a paso y dejaba unas explicaciones de todo, que hasta parecían redundantes, y todo aquello dirigido al lector novato como yo. Las imágenes con explicaciones y resaltaba lo importante. ¡Ah! Dios mío todo se me perdió y es que para mí en hacer un tuto me conlleva un esfuerzo gigante, el esfuerzo físico que hago no es cualquier cosa, solo imagínense que solo puedo usar un solo dedo para hacer todo y literalmente es tecla por tecla.

Había abordado cómo cazar nuestro serial ingresado con la API_GetWindowTexA, luego utilizábamos un par de APIS para trabajar con el registro de Windows como son la API_RegOpenKeyExA y API_RegCreateKeyExA.

Hacíamos mucho traceo para explicar cómo funcionaba y qué hacía el programa, y ponía énfasis en lo que hacíamos porque sabía que podría servir para aprender un poco más, para crackear aplicaciones semejantes, dejaba mis consejos por así decirlo.

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

También había explicado, cómo se podía crackear cambiando código, invirtiendo saltos y valores de los registros (que era solo uno), que aceptara cualquier serial de 31 caracteres; mostrando que puede haber diferentes formas de lograr el cometido.

Todo, todo aquello se perdió completamente. Sentía que era un buen tuto. Solo me quedó lo de sacar el serial válido que era mi objetivo final, pero lo perdido era igual de importante porque la idea es siempre compartir lo aprendido para que otros también aprendan.

Ya mi tuto nos para un novato novato porque solo voy a dejarles lo salvado y es el serial válido.

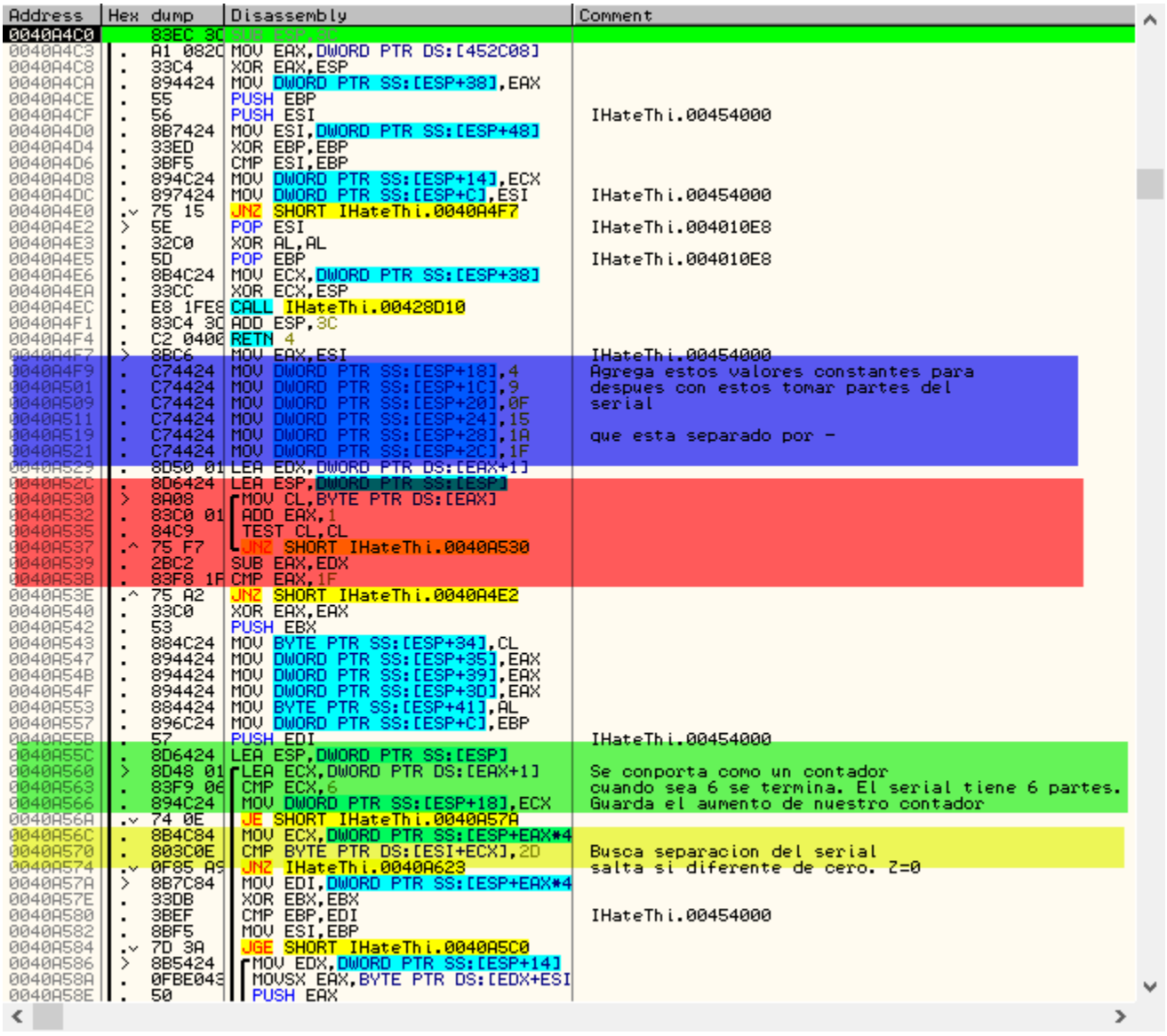
Bueno, con escribir de nuevo la esta introducción muy diferente a la anterior, me desahogado un poco. Como siempre un saludo a Ricardo Narvaja y al resto de los miembros de CRACKSLATINOS y también a los chicos de PERUCRACKERS, que al final somos todos uno solo, aficionados al cracking que nos gusta compartir esta experiencia.

Para terminar, esto lo hice tuto a partir de una consulta en la lista.

AL ATAQUE

Como todo se perdió, entonces lo primero que deben hacer es llegar a la NAG e ingresar nuestro serial de 31 caracteres "S1E2R3I4A4LDEBETENERTREINTAYUNO", el cual es tomado como correcto y reiniciar la aplicación. Luego van a la dirección **0040A4C0** y le ponen un **BREAKPOINT (BP)**.

Esto será resumido, lo prometo y lo explicaré en contexto general, seguro ustedes lo entenderán, si pude yo solito, com mis observaciones no tardarán tanto como yo.



Recuerden estamos trabajando sobre el archivo original y hemos agregado nuestro serial de 31 caracteres, "S1E2R3I4A4LDEBETENERTREINTAYUNO". Ustedes deben analizarlo y llegar a entender el funcionamiento y pueden descubrir que algo que yo diga no es correcto y que lo he interpretado mal.

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

Empecemos por lo resaltado en rojo, ese **LOOP** es solo para comparar la longitud de nuestro serial que deber ser **0x1F**, y como esa es la longitud, pues no hay lio.

Esos valores constantes que se guardan en **[ESP+XX]** (resaltado azul) se utilizan con el serial en la zona amarilla. Con esto podemos hallar el formato de nuestro serial.

[ESP+18],04 es para comparar el quinto carácter de nuestro serial con **0x2D** (ASCII: **-**). En los archivos del tuto les adjunto la tabla que tiene los valores ASCII. Nuestro quinto carácter resaltado en rojo, "S1E2**R**3I4A4LDEBETENERTREINTAYUNO".

Como ven, debería ser **-** (**0x2D**). entonces sigamos esa lógica con los otros valores de **[ESP+XX]**.

[ESP+1C],9 "S1E2**R**3I4A**4**LDEBETENERTREINTAYUNO"

[ESP+20],0F "S1E2**R**3I4A**4**LDEBE**T**ENERTREINTAYUNO" : **0x0F** = 15

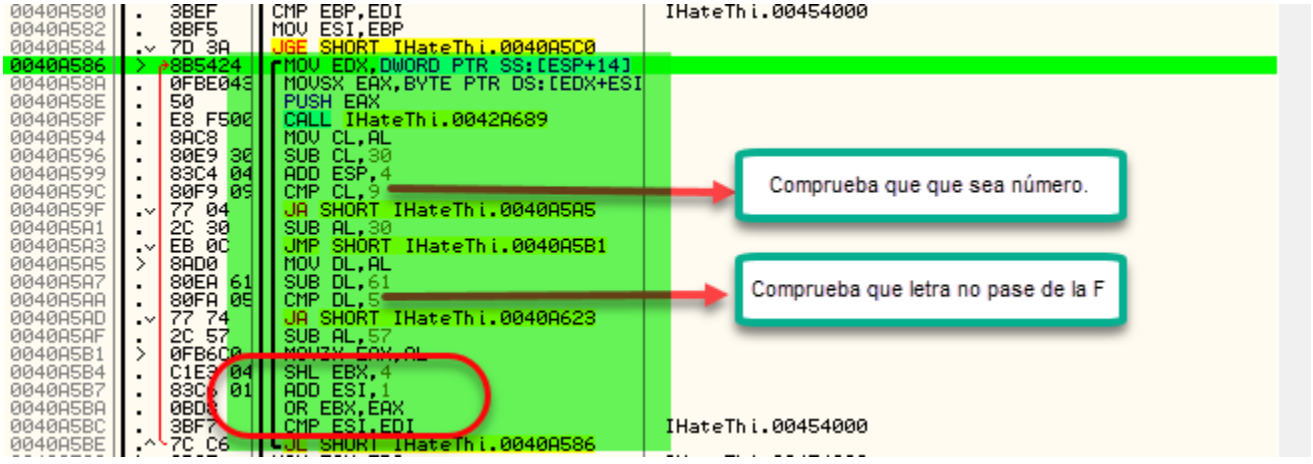
[ESP+24],15 "S1E2**R**3I4A**4**LDEBE**T**ENERT**R**EINTAYUNO" : **0x15** = 21

[ESP+28],1A "S1E2**R**3I4A**4**LDEBE**T**ENERT**R**EINT**A**YUNO" : **0x1A** = 26

Listo, debemos reemplazar nuestros caracteres resaltado en rojo por **-**, quedando nuestro serial "S1E2-3I4A-LDEBE-ENERT-EINT-YUNO".

Como podemos ver, el serial se compone de 6 partes y ahí entra en juego la zona resaltada en verde que es un **LOOP** que se repite por cada parte del serial.

Lleguemos a la NAG y metamos nuestro nuevo serial. Reiniciamos para ver qué pasa con nuestro nuevo serial en la "**ZONA CALIENTE**".



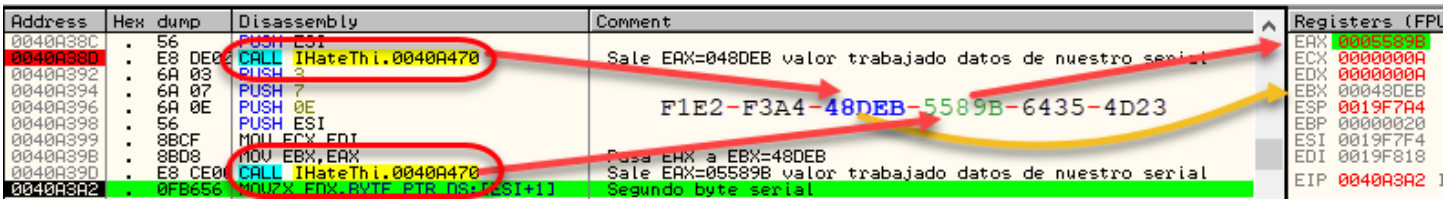
Lleguemos hasta **0040A586**. Ese **LOOP** resaltado en verde nos comprueba los caracteres permitidos en el serial. El serial solo puede tener números y hasta la letra F, y si miramos nuestro serial "S1E2-3I4A-LDEBE-ENERT-EINT-YUNO", nos podemos dar cuenta que tenemos letras que pasan de la F. Bueno cambiemos esos caracteres por unos que cumplan la condición de ese **LOOP**. Bueno, ahí lo cambié "F1E2-F3A4-48DEB-5589B-6435-4D23". En ese recuadro en rojo hay un procedimiento que se realiza con los valores que saca con cada carácter, ahí el valor importante va quedando en **EBX**. Cuando hagan este procedimiento con este serial ya

corregido notaran que en **EBX** queda la parte del serial que se está trabajando. Por ejemplo, la primera parte es "F1E2" entonces **EBX=0000F1E2**.

Listo, ya tenemos un nuevo serial que nos lleva más al fondo del camino correcto y no nos vota. Hagamos todo de nuevo, llegar a la NAG y meter este nuevo serial. Reinicias y llega de nuevo a la "**ZONA CALIENTE**".

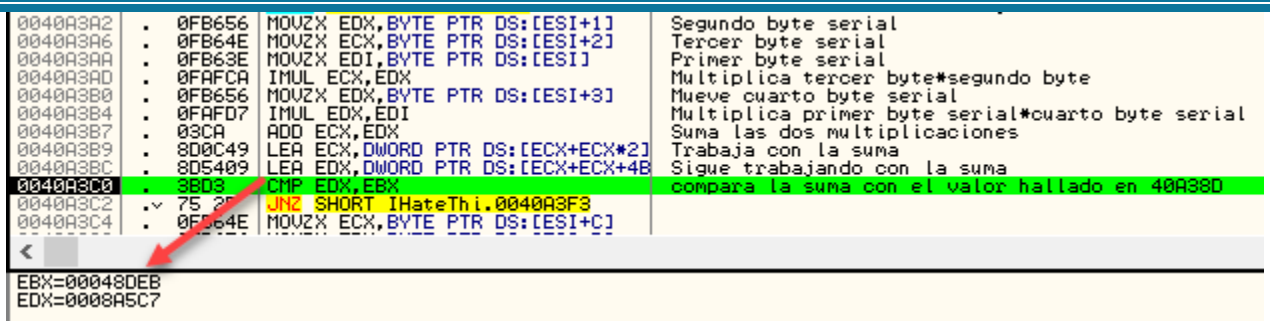
Recorre los **LOOP** hasta llegar a la dirección **0040A601**, fíjate lo que sucede ahí, hazlo hasta terminar todo. Esa imagen lo explica muy bien. Todo ese rollo de los dos **LOOP** es para legar a esto. En el **DUMP** se guarda nuestro serial en la dirección **0019F7F4** en parejas originando valores hexadecimales y ese es el motivo de poder ingresar letras hasta la F. Esto se hace seis veces y ya saben el motivo, porque el serial se compone de seis partes.

Bueno, después de que salgan de esos procedimientos sigan traceando con <**F7**> hasta llegar a **0040A38D**.

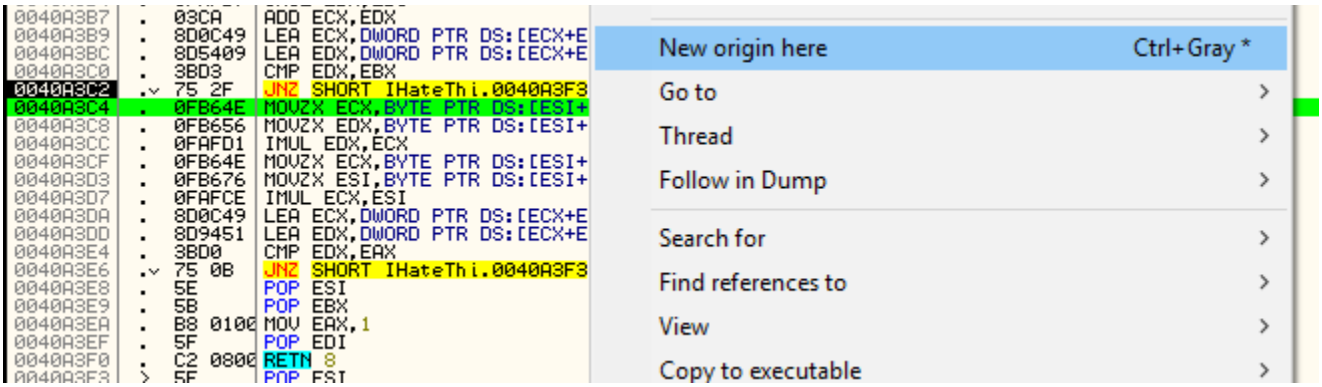


Y tenemos dos **CALL** y que hacen prácticamente lo mismo. El primer **CALL** pone la tercera parte del serial que inicialmente queda en **EAX**, pero termina finalmente en **EBX=00048DEB** cuando se llega al segundo **CALL**, y precisamente el segundo **CALL** pone la cuarta parte del serial en **EAX=0005589B**. Ahora en las siguientes imágenes se trabajará con la parte 1 y 2 del serial para hallar un valor y ser comparado con **EBX**; y también con la parte 5 y 6 para luego ser comparado con **EAX**.

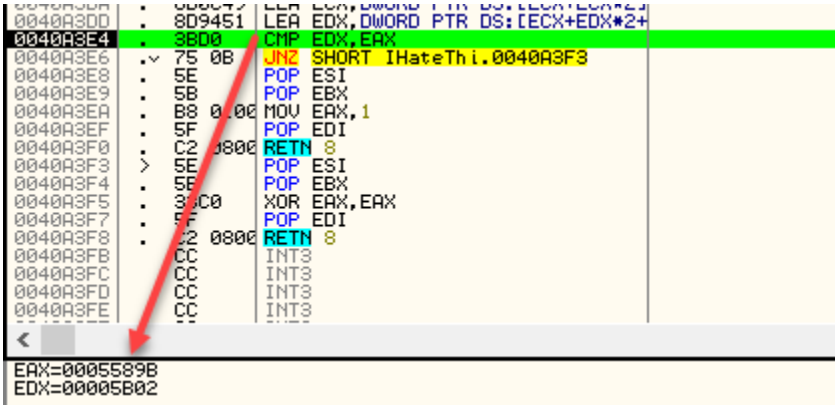
[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]



Aquí está la primera parte de la solución, todos estos cálculos se hacen con las partes 1 y 2 de nuestro serial y el resultado debería ser la tercera parte del serial, pero como vemos no son iguales. Nuestro resultado fue **EBX=00048DEB** y debería haber sido **EDX=0008A5C7**. Pues la solución es muy sencilla ya que la tercera parte del serial solo se utiliza para compararla con este resultado, pues ya sabemos que la tercera parte del serial debe ser **8A5C7**. El serial válido nos va quedando, "F1E2-F3A4-8A5C7-5589B-6435-4D23". Sigamos con el próximo cálculo que es lo mismo.



Primero, debemos pasar ese salto **JNZ** de **0040A3C2** porque como saben la comparación no nos dio, entonces nos bota fuera. Para eso nos posicionamos en la dirección **0040A3C4**, <**Clic derecho -> New origin here**>. Luego traceamos hasta la dirección próxim salto en **0040A3E4**.



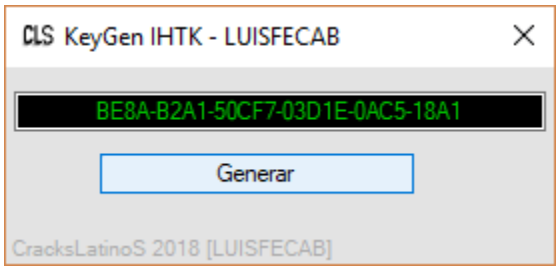
Lo mismo, pero el calculo se realiza con las partes 5 y 6 del serial y el resultado obtenido en **EDX=00005B02**, se compara con la cuarta parte de nuestro serial que está en **EAX=0005589B** y como vemos no son iguales ni por las curvas. Entonces para tener nuestro serial válido la cuarta parte de nuestro serial es el resultado de ese procedimiento que viene siendo **05B02**.

[I Hate This Key Deluxe v5.0.0.98 (Serial Válido + KeyGen)]

Con todo lo que hemos hecho nuestro serial válido sería, "F1E2-F3A4-8A5C7-05B02-6435-4D23".

Ahí está les presento mi primer serial válido. Les diría que muy contento, pero no, con la perdida prácticamente de todo el tuto, me queda un sabor agridulce.

Ya para ir terminando, me le medí a hacer el Keygen y lo pude hacer. Lo hice de la mejor forma posible, al inicio ni idea por dónde empezar a hacerlo porque mi única experiencia programando es en Visual Basic y ahora con el VB.net programando las formulas de perforación, producción o yacimientos cuando estudié mi carrera y no trabajaba con valores HEXADECIMALES; por ahí consulté información y le busqué "la comba a palo" para hacerlo.



Me despido, un abrazo inmenso para todos y espero sea de utilidad para la comunidad este pequeño tuto, hecho con mucho esfuerzo, pero hecho con más cariño, aún.