Teoría Nº	La primera del 2008 ya era hora
Objetivo	Aprender a Eliminar una NAG basándonos en la pila.
Victima	Tune up Programa para mantener el PC brillante
Herramientas	1 Depurador y un poco de Cabeza no vendrá nada mal saber algo sobre ASM.
Dificultad	Hazlo sin leer el tutorial y opina! Si te doy la Solución ☺.
Compilador	Esta claro (Delphi).
Cracker	KmL ReVeRsEr ®

RENUNCIA

Este tutorial tiene una finalidad únicamente educativa, no asumo ninguna Responsabilidad por el mal uso que se le pueda dar a éste material.

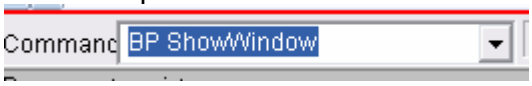
Bueno en este nuevo documento vamos a aprender como eliminar una nag con nada mas ver la pila y con un poco de cabeza caer encima del salto mágico.
-No es magia es Ciencia OJO hay que practicar bastante.

Comenzamos

1-Examinamos el Programa.

Ya tenemos la información necesaria así que a atacar se a dicho.

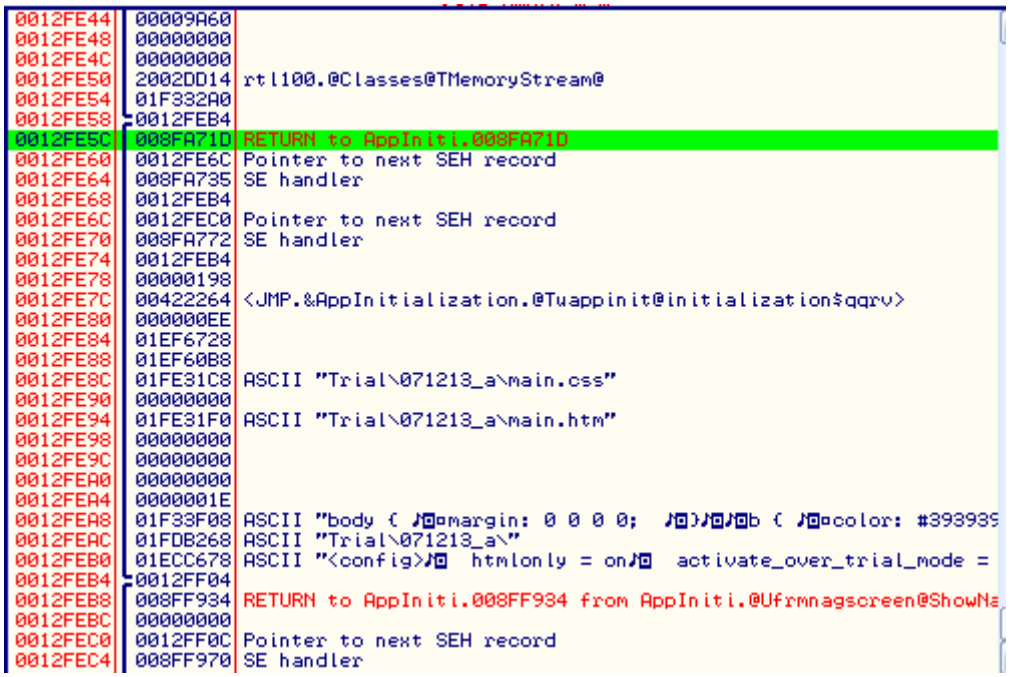
Empezamos el Ataque.

Comenzamos directamente con el depurador así que abrimos nuestro depurador y seleccionamos el Archivo Integrator.exe
Aparecen unas alertas que pasamos de ellas olímpicamente.
Bueno vamos colocando un punto de corte en Show Window así que en nuestra barra de Comandos pones 

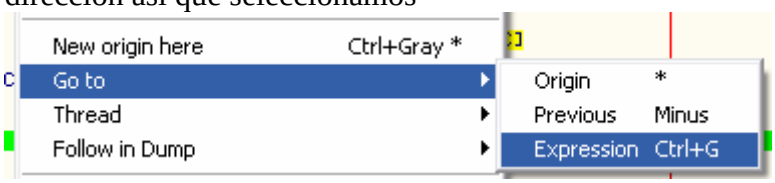
y ejecutamos el programa con F9 o el botón play.

Bueno vamos a aprovechar la Pila la que nos relevara mucha información de lo que se ha hecho ya veréis la importancia de esta ☺

Echamos una mirada a la pila y vemos estoy algo muy sospechoso ☺ pero demasiado.

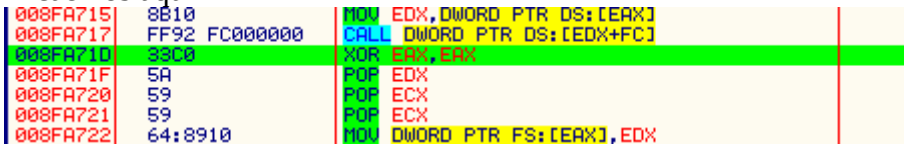


Nos interesan los punteros
0012FE5C |008FA71D RETURN to AppIniti.008FA71D
0012FEB8 |008FF934 RETURN to AppIniti.008FF934 from ....Etcetera...
Bueno ya tenemos las direcciones mágicas que son
008FA71D
008FF934 (en mi caso) Pueden cambiar en vuestro PC
La mas importante es la primera así que vamos a ver que hacemos bueno vamos a esta dirección así que seleccionamos

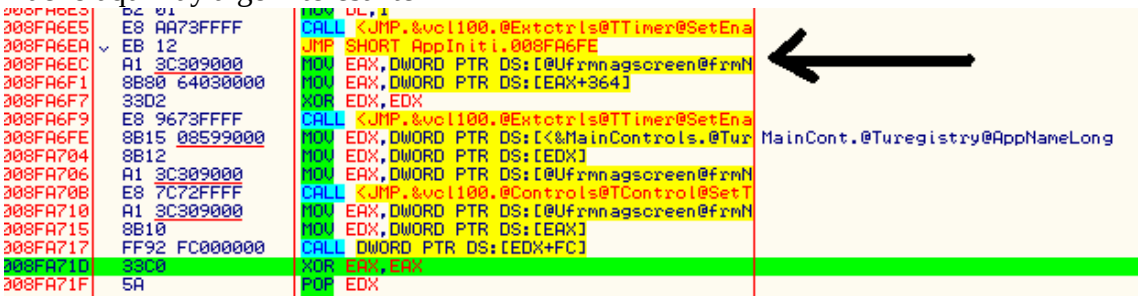


Y pegamos nuestra dirección en mi caso. 008FA71D

Y caemos aquí



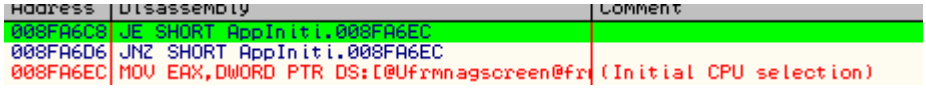
Bueno aquí hay algo interesante



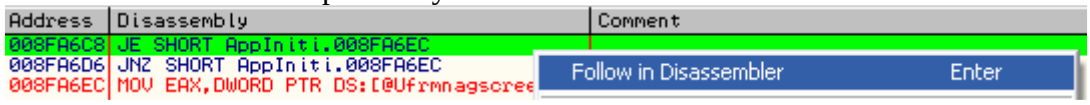
Justamente donde indica la flecha hay un salto que evita la nag por lo cual tiene que haber otro que evite el salto así que nos colocamos justo debajo del salto

Y seleccionamos

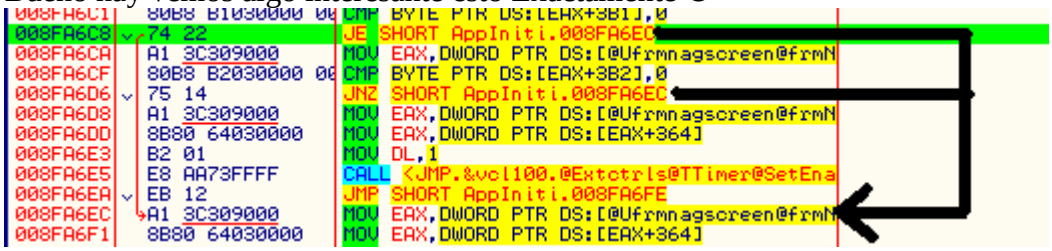
Y encontramos estos



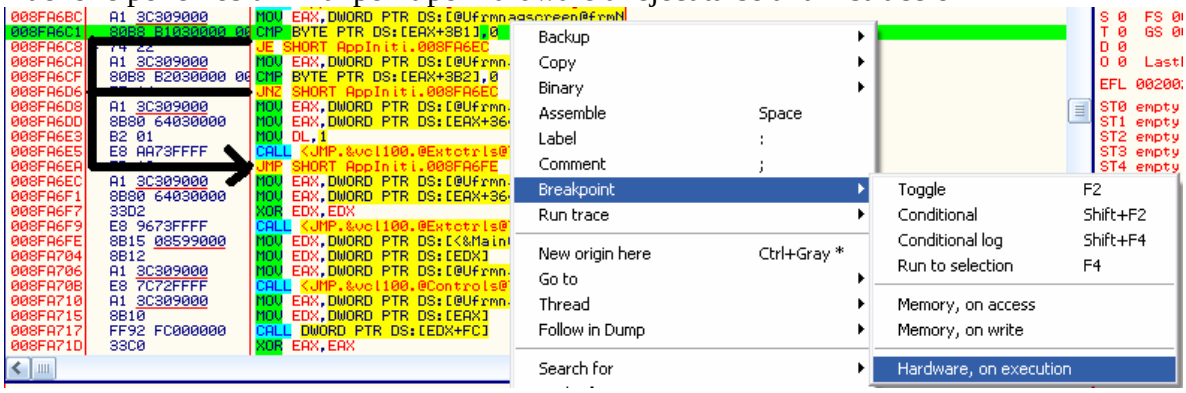
Bueno seleccionamos el primero y le damos a



Bueno hay vemos algo interesante esto Exactamente ☺

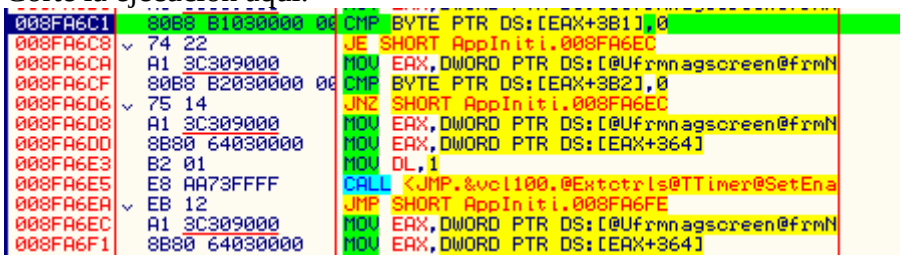


Bueno le ponemos un Brakpoint por hardware al ejecutarse a la instrucción



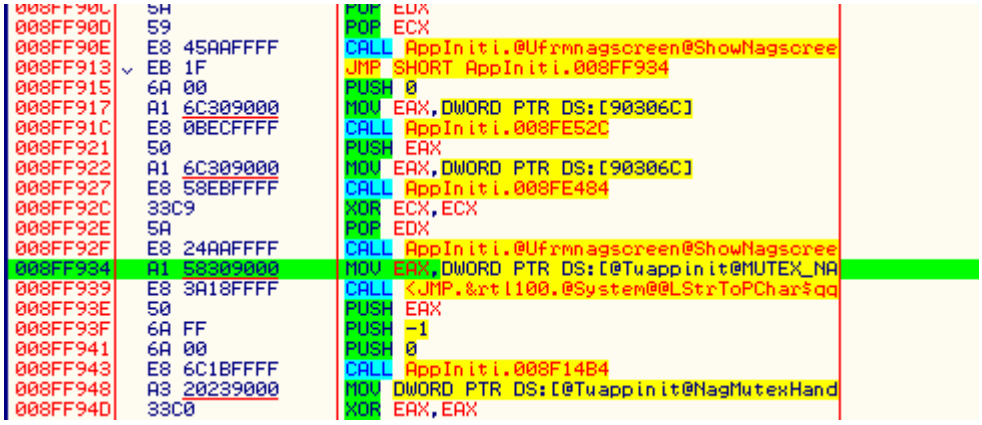
Bueno lo del BP por hardware es porque para mi es mas eficaz y cómodo (Todo esto relativo) en este caso nos
Da mejores ventajas este.

Después de ponerlo reiniciamos el Depurador. iniciamos la ejecución normal de la victima hasta que el depurador
Corte la ejecución aquí.



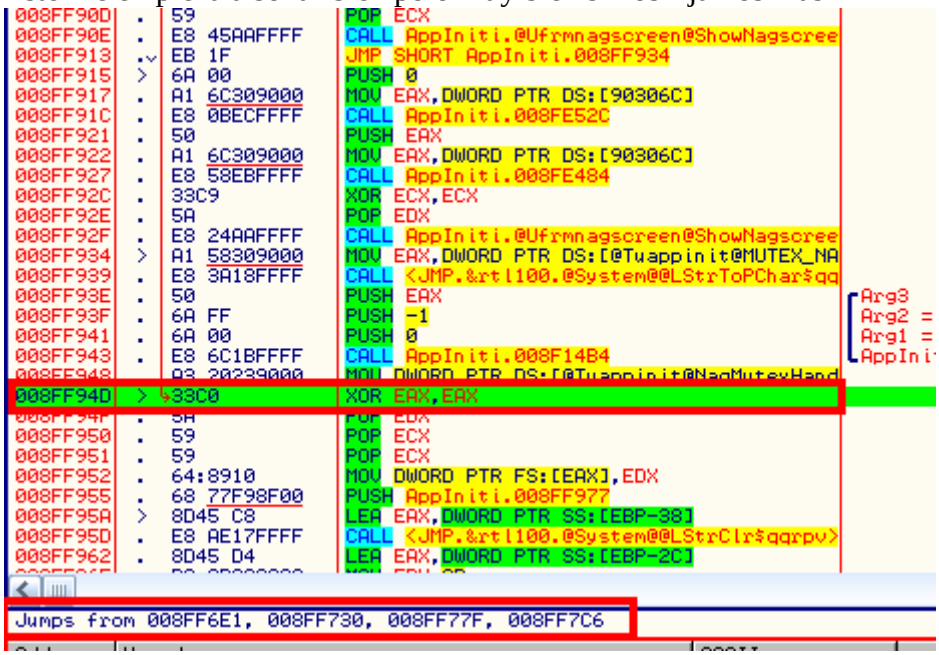
Bueno esto lo he echo para ordenarnos así bueno tenemos menos suciedad en la pila. ☺
Lo cual nos facilitara dar con la protección ☺
Si miramos la pila vemos esto

Buscamos de donde ha sido llamada
0012FEB8 |008FF934 RETURN to AppIniti.008FF934 from AppIniti.@Ufrmnagscreen@ShowNagscreen$qqriioo
Bueno hay la tenemos la dirección 008FF934
Bueno vamos hay a ver que es lo que pasa ☺



Bueno pasa tres cuartos de lo mismo y esto a mi no me gusta así que vamos a ver si nos facilitamos las cosas

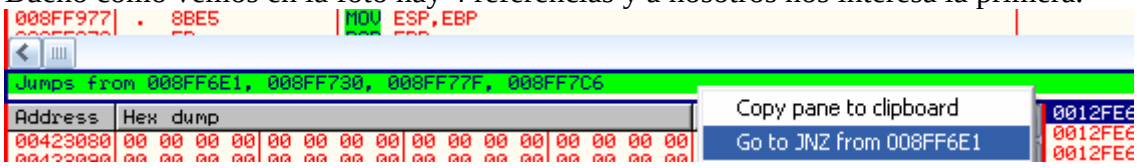
Esto me empieza a sonar bien pero muy bien si nos fijamos más



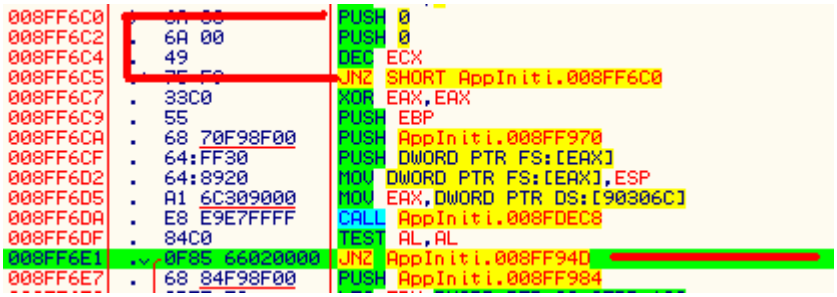
Y eso de donde salio, bueno si hubierais ido viendo las rutinas con el desamblador nos hubiéramos dado cuenta pero buen

También a plena vista se notaba debido a esas 4 instrucciones que me resultaron sospechosas a si sin más.

Bueno como vemos en la foto hay 4 referencias y a nosotros nos interesa la primera.

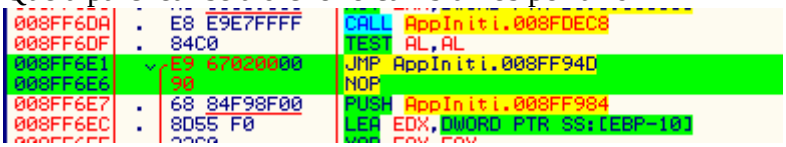


Y caemos aquí



Ya lo tenemos ese salto evita las nag y no hay nada que evite ese salto bueno si un Humano con un Depurador así

Que a parchear se a dicho lo cambiamos por un JMP



Y comprobamos que no removió la instrucción siguiente así que lo guardamos y lo probamos.

☺ Realmente Funciona.

Y con esto hemos eliminado la protección claro nos quedaría el info. Pero a mi personalmente me da igual he he ☺

Bueno espero que hoy hayas divertido y aprendido algo muy poco pero bastante para saber como eliminar un NAG nada más con la pila☺.

-RECORDAR: PRACTICAR Y REPRACTICAR Y ESCRIBIR

RECUERDA
SI CREES QUE UNA APLICAIÓN TE ES UTIL, ESTA BIEN PROGRAMADA Y ADEMAS TE GUSTA, NO SEAS GOLFO Y REGISTRATE, AYUDARÁS A SU PROGRAMADOR.

Agradecimientos: A toda la lista ☺ especialmente a la parte activa y a SOLID, RICARDO MEK Y C_C NCR Y Dapaf (hace mucho que no apareces) stxwei guan de dio y los que tengo en correo y en el MESENGER si tu eres uno de ellos Gracias.

Aparte me gustaría agradecer a una persona que me metió en esto y me hizo despertar y salir de un camino equivocado por el cual me llevaba a ningún destino. Un profesor que me ayuda, me enseña y me forma día a día para llegar a uno de mis sueños.

Gracias, a todos ☺