Reverseando NOD32 antivirus (PARTE I) (parte I)

Alejandro torres (torrescrack)

Alejandro Torres

Torrescrack.blogspot.com

torrescrack

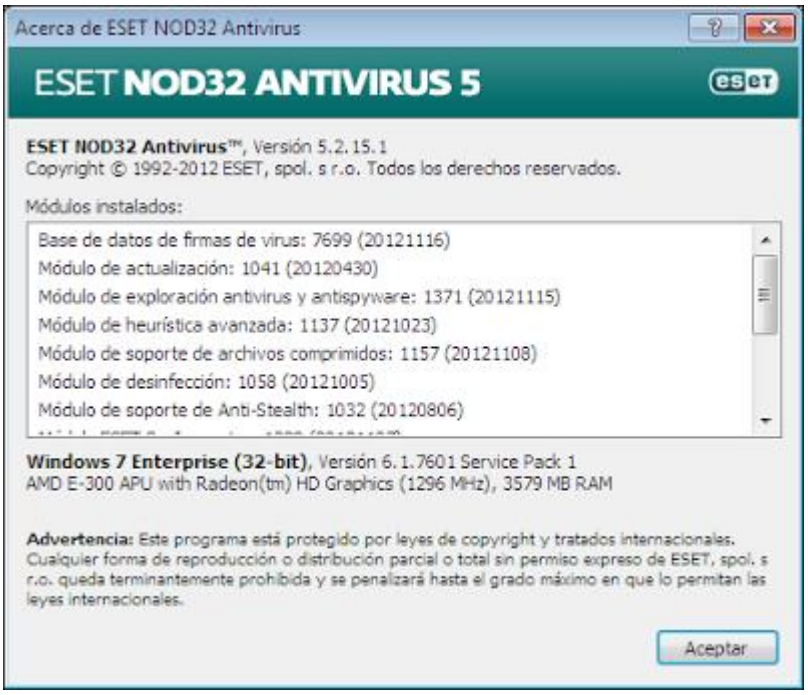
Reverseando NOD32 antivirus (PARTE I)

http://www.facebook.com/yo.torrescrack

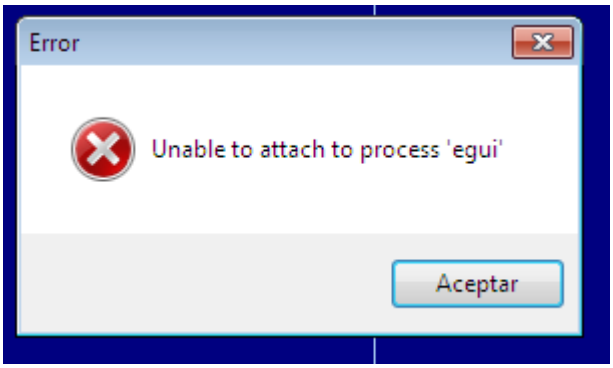
https://twitter.com/TorresCrack248

www.torrescrack.blogspot.com

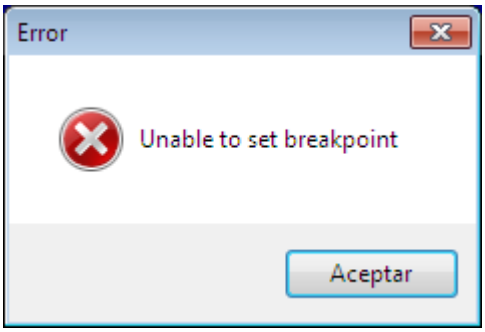
Reverseando NOD32 antivirus (PARTE I)

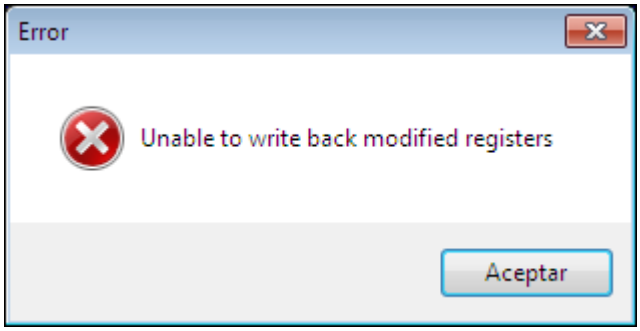


Bien en esta ocasion se me ocurrio darle una mirada al pionero antivirus ESET 32 , lo cual me puse a intentar ver un poco por dentro al bicho haber de que estaba hecho , y si en verdad era tan dificil lograr burlar la seguridad del mismo , existen algunos activadores en la red , algunos funcionan , otros no y otros creo que no se pueden ni actualizar , en mi caso no uso nada de eso ya que a mi me gusta ver como funcionan y como poder burlar la proteccion , por el momento le damos una mirada muy de fuera al antivirus , para ello solo utilizaremos un debugger (olly en este caso) , pero me encuentro con el problema de que no puedo attachear el proceso ya que como sabemos el antivirus siempre esta ejecutandose en el ordenador por lo tanto si abrimos otro proceso es obvio se cerrara entonces intentamos attachear pero este me dice simplemente que no se deja ..

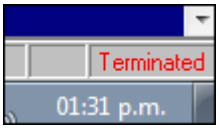


Uhmm.. vemos que no me deja , habría varias formas que se me estan ocurriendo en este momento para lograr hacerlo pero vamos por una mas sencilla , que es verlo con el debugger y aunque se cierre podemos analizar el codigo muerto , pues a mi solo me interesaria ver si esta empacado , ecriptado o si de plano no usa ninguna proteccion fuera de lo normal , asi que al ataque

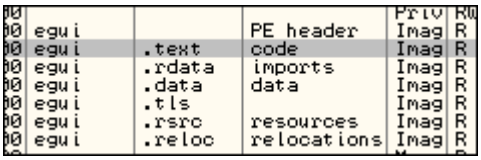




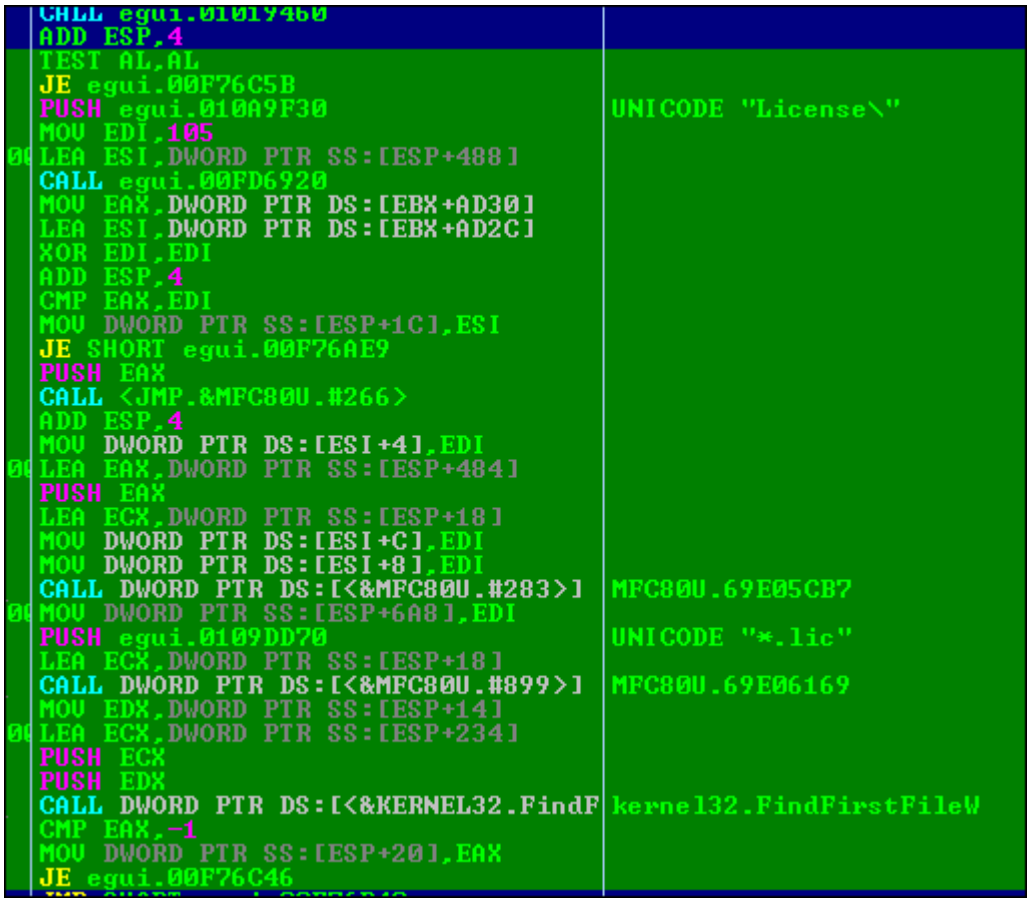
Tanto msgbox para nada....



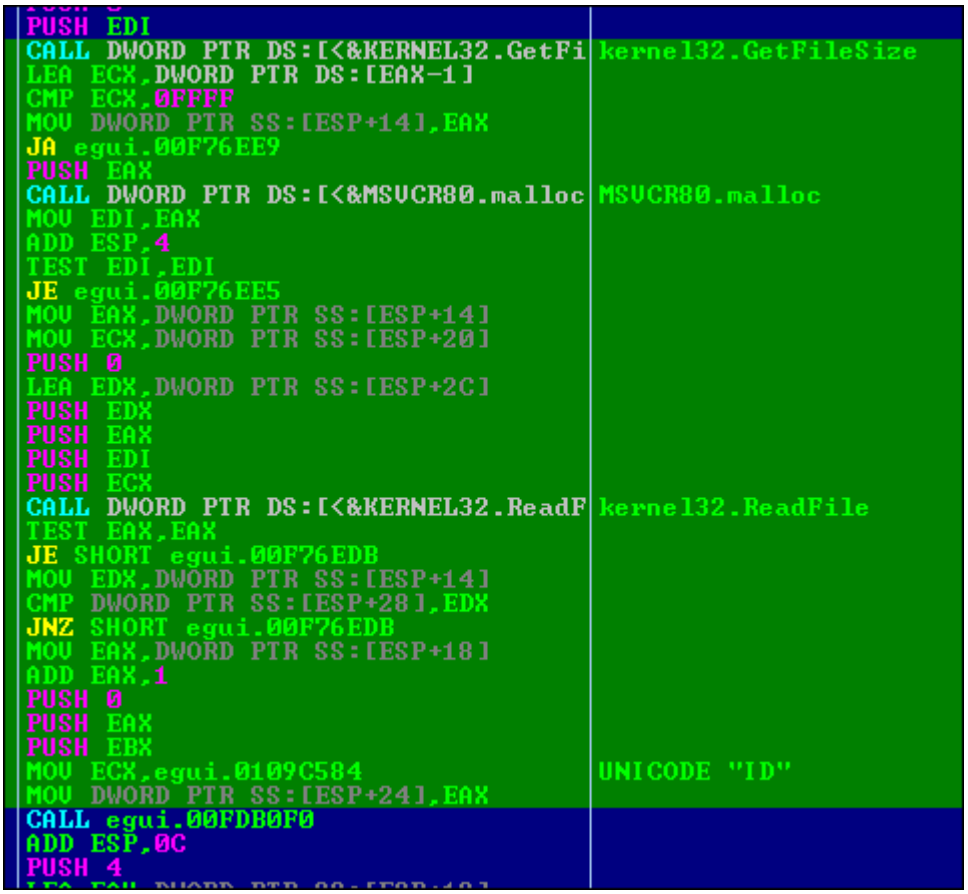
Bien realmente no interesa si ya termino el proceso , ya que pueden ser varios factores y uno de ellos podria ser que es un metodo de proteccion que no deje correr dos procesos del egui.exe , entonces veamoslo en codigo muerto vamos a la seccion de memoria y nos dirigImos a la seccion .code porque sospecho no esta empacado y si no , pues se me ocurre ver las strings (esa casi nunca falla) :P



Bien vemos que no necesitamos estar horas en el pc para encontrar strings que nos ayuden en la busqueda de un ataque que logre dejar full este software , si entramos por donde estan esas , podemos ver que empieza con una rutina que empieza a hacer chequeos de la existencia de una licencia



Bien lo que vemos remarcado en verde es la zona de la que les hablo , no creo que en eso se base toda su proteccion , en algun momento verificara el contenido (eso creo) , asi que si seguimos analizando de rapido el codigo vemos que toma el tamaño de la licencia y depues toma el contenido del archivo y guarda su contenido en un buffer



Asi podemos seguir hasta ver donde estan las comprobaciones del contenido de la licencia y poder crear una licencia valida y generar una ó quizas hasta un generador de licencias validas que eso es algo mas avanzado y seria perfecto pero dependiendo de los algoritmos que use para la comprobacion de

la misma , o hasta algo mas facil y que me gusta mas seria hacer que aunque no tengamos licencia , piense que si tenemos una y que actue como un software competamente registrado , ya que como vimos el software no esta empacado/protegido , y podemos manipularlo a nuestro antojo , lo siguiente seria ver lo de las actualizaciones que hace , pues eso es lo que mas me han comentado algunos amigos que ese problema tienen los activadores que ya existen por la red y es que no actualizan , ese es otro tema ya que debemos encontrar donde esta la rutina que se conecta al server para actualizar y ver de donde depende el chequeo ... sin mas les mando un saludo , me retiro a desayunar ya un poco tarde pero pues ya me intrigaba meterle mano a este soft que seguiremos mas adelante . **Espero pronto tenerles la segunda parte de este reversing sobre el ESET** que a mi parecer tiene al descubierto toda su proteccion y el codigo y esto es un gran problema ya que es mas facil la creacion de un parche o un keygen para dejar expuesto un gran soft de seguridad que aunque ya existan activadores lo que se debe hacer para corregir este tipo de errores es crear un analisis del mismo y reportar el procedimiento haber si asi ya lo corrigen XD, saludos

Alejandro Torres (torrescrack)

e-mail: tora_248@hotmail.com