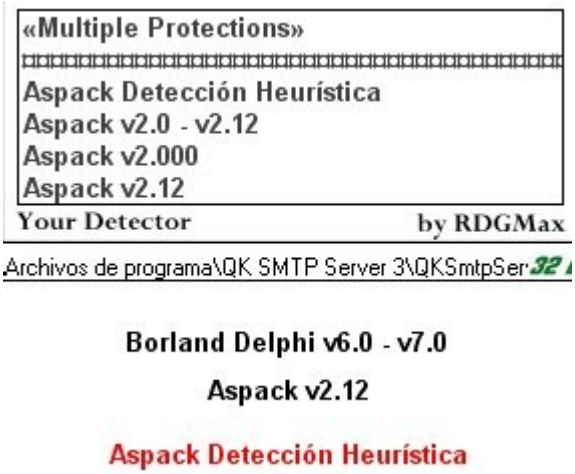
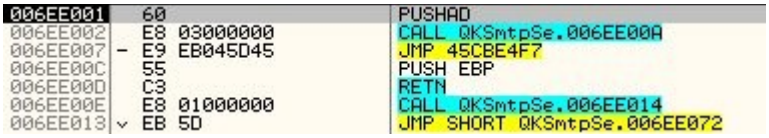
Victima	Qk smtp server 3
Url	http://www.qksoft.com
Herramientas	Rdg, Olly, ImportReconstructor
Fecha	19 – Abril - 2012
Cracker	Alberto Fernandez
Dificultad	ninguna

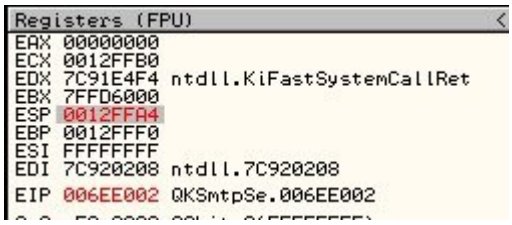
Bueno, pues según Rdg Packer Detector, como se ve en la imagen es un Aspack v2.12



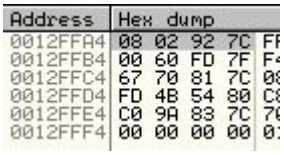
Lo cargamos en Olly, y nos encontramos con la típica entrada.



Pasamos el PUSHAD con F8, vamos a la sección de Registers y en ESP, botón derecho del ratón pulsamos en Follow in Dump.

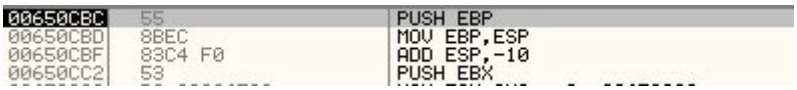


Vamos a la sección del Dump, seleccionamos el registro y con el botón derecho del ratón seleccionamos Breakpoint Hardware, on access dWord.



Le damos Run o F9, y nos para:

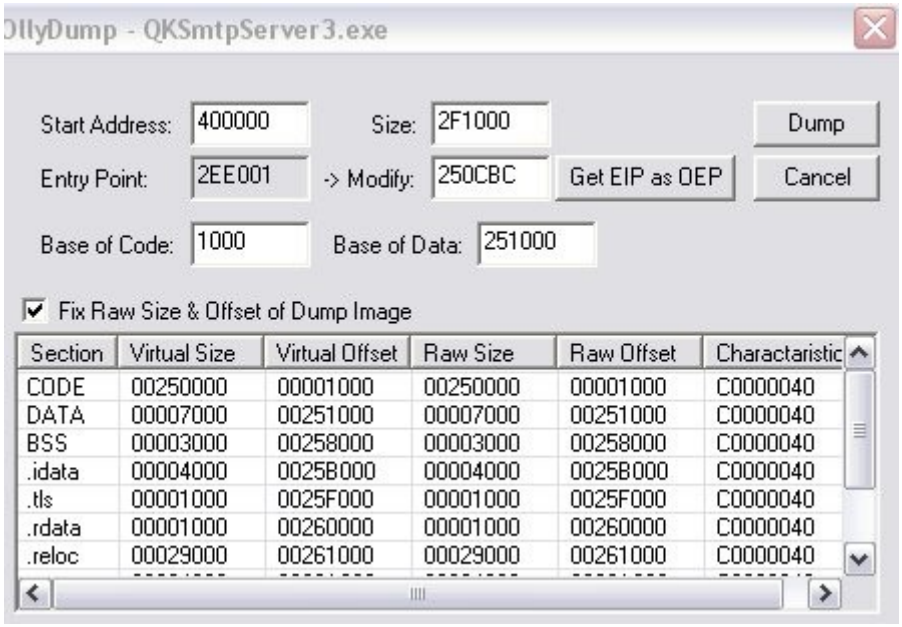
Pulsamos F8, hasta haber pasado el retorno, ya estamos en el OEP.



Ya podemos quitar el Breakpoint.

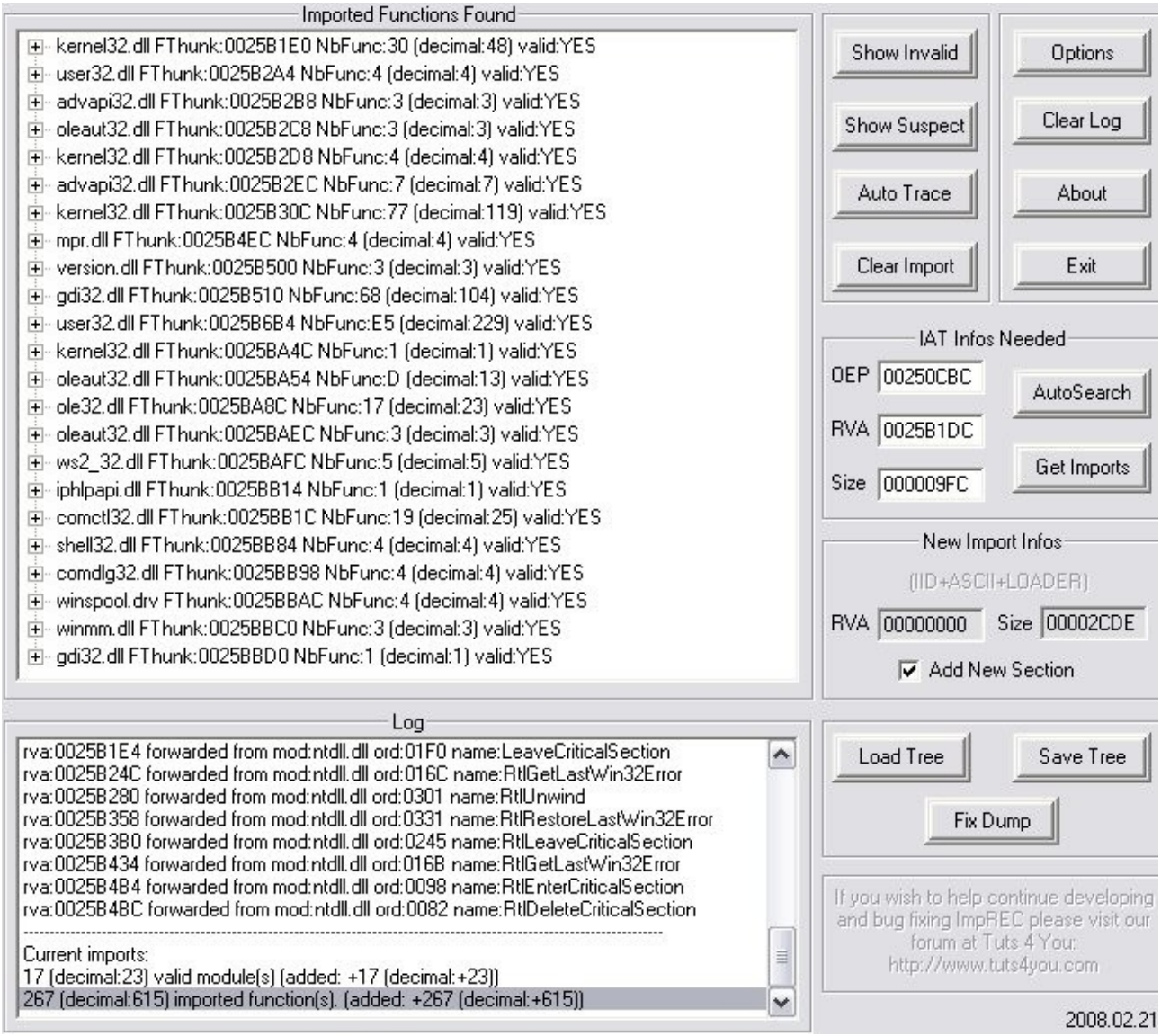
Apuntamos el dato que vamos a necesitar 00650CBC le restamos la imageBase 400000 y nuestro oep será: 00250CBC

En Plugins, OllyDump, Dump debugged process destildamos la opción Rebuilt import, observamos que coloca los datos como deben estar:



Pulsamos en el botón Get EIP as OEP, y le damos a Dump, le damos nombre al ejecutable.

Abrimos el ImportReconstructor y cargamos el proceso:



Colocamos el OEP que hemos apuntado antes, pulsamos el botón AutoSearch, aceptamos el mensaje, pulsamos Get Imports, al no haber entradas invalidas, ya está resuelto, por supuesto no hay que olvidarse, pulsar el botón Fix Dump seleccionar el archivo que se ha creado antes y guardarlo.

Resuelto.

Gracias a todos.

Alberto Fernandez

20 – abril – 2012