



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



Borland Delphi v6.0 - v7.0

Aspack v2.12

Aspack Detección Heurística

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

006EE001	60	PUSHAD
006EE002	E8 03000000	CALL QKsmtpSe.006EE008
006EE007	E9 EB045045	JMP 45CBE4F7
006EE00C	55	PUSH EBP
006EE00D	C3	RETN
006EE00E	E8 01000000	CALL QKsmtpSe.006EE014
006EE013	EB 5D	JMP SHORT QKsmtpSe.006EE072

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

Registers (FPU)	
EAX	00000000
ECX	0012FFB0
EDX	7C91E4F4 ntdll.KiFastSystemCallRet
EBX	7FFD6000
ESP	0012FFA4
EBP	0012FFF0
ESI	FFFFFFFF
EDI	7C920208 ntdll.7C920208
EIP	006EE002 QKsmtpSe.006EE002

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

Address	Hex dump
0012FFA4	08 02 92 7C Ff
0012FFB4	00 60 FD 7F Ff
0012FFC4	67 70 81 7C 08
0012FFD4	FD 4B 54 80 C8
0012FFE4	C0 9A 83 7C 70
0012FFF4	00 00 00 00 00

Le damos Run o F9, y nos para:

006EE3A9	8985 A8030000	MOV DWORD PTR SS:[EBP+3A8],EAX
006EE3AF	61	POPAD
006EE3B0	75 08	JNZ SHORT QKSmtpSe.006EE3BA
006EE3B2	B8 01000000	MOV EAX,1
006EE3B7	C2 0C00	RETN 0C
006EE3BA	68 BC0C6500	PUSH QKSmtpSe.00650CBC
006EE3BF	C3	RETN

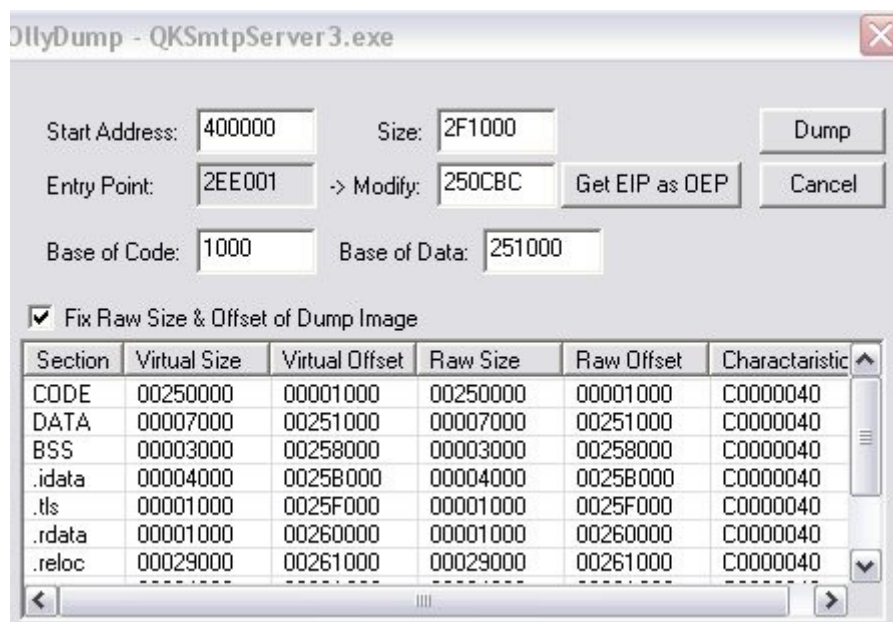
Pulsamos F8, hasta haber pasado el retorno, ya estamos en el OEP.

00650CBC	55	PUSH EBP
00650CBD	8BEC	MOV EBP,ESP
00650CBF	83C4 F0	ADD ESP,-10
00650CC2	53	PUSH EBX

Ya podemos quitar el Breakpoint.

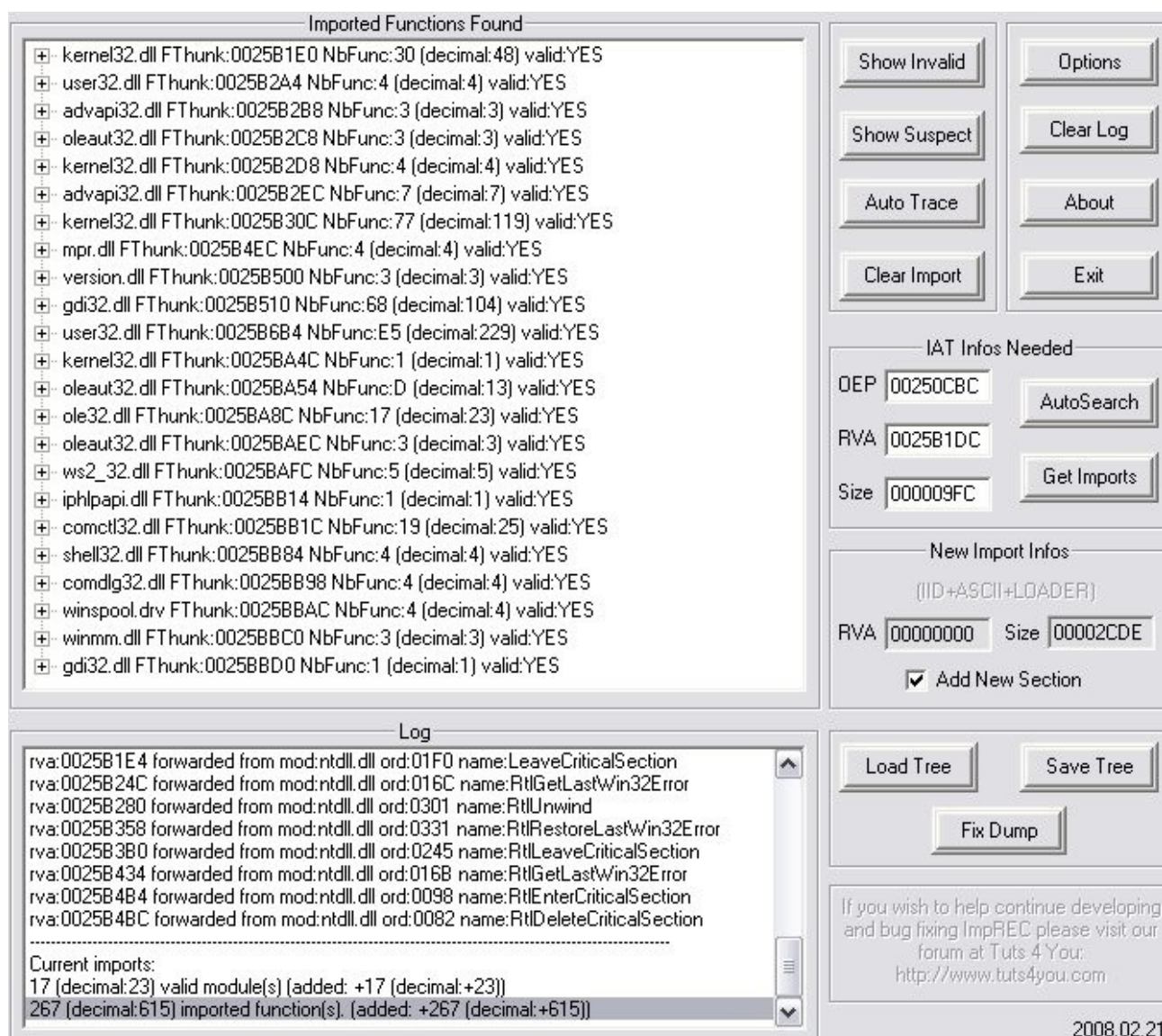
Apuntamos el dato que vamos a necesitar 00650CBC le restamos la imageBase 400000 y nuestro oep será: 00250CBC

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