



Victima	Qk smtp server 3
Url	http://www.qksoft.com
Herramientas	Ollly
Fecha	20 – Abril - 2012
Cracker	Alberto Fernandez
Dificultad	ninguna

Aprovechando la imagen del tutorial anterior, vemos como Rdg Packer Detector, nos muestra que está programado en Delphi.



**Borland Delphi v6.0 - v7.0**

**Aspack v2.12**

**Aspack Detección Heurística**

Al ejecutarlo nos muestra



Pulsamos en el botón Register, haber que nos pide, introducimos los datos nombre y numero.



Pulsamos el botón Register y nos muestra:



Ya estamos, lo mismo de siempre, nunca nos dan un número de registro válido.

Bueno, al tajo. Lo cargamos en Olly, sin perden el tiempo pulsamos el botón derecho del ratón, Search for All referenced text Strings, directamente podemos observar dos entradas muy interesantes:

0064F414	MOV EDX,QKSmtSe.0064F4BC	ASCII "\\Software\\BW\\QK SMTP Server 3\\Reg"
0064F428	MOV EDX,QKSmtSe.0064F4E8	ASCII "Name"
0064F448	MOV EDX,QKSmtSe.0064F4F8	ASCII "RegCode"
0064F4BC	ASCII "\\Software\\BW\\QK "	
0064F4CC	ASCII "SMTP Server 3\\Re"	
0064F4DC	ASCII "g",0	
0064F4E8	ASCII "Name",0	
0064F4F8	ASCII "RegCode",0	
0064F724	MOV EDX,QKSmtSe.0064F8A0	ASCII "\\Software\\BW\\QK SMTP Server 3\\Reg"
0064F737	MOV EDX,QKSmtSe.0064F8CC	ASCII "Name"
0064F746	MOV EDX,QKSmtSe.0064F8DC	ASCII "RegCode"
0064F7DA	MOV ECX,QKSmtSe.0064F8EC	ASCII "(Unregistered)"

Un poco más arriba nos muestra unas entradas que realmente no nos sirven para nada:

0064AF26	ASCII "TfrmEnterRegiste"	
0064AF36	ASCII "r"	
0064AF42	ASCII "QKRegisterForm"	
0064AF8D	MOV EAX,QKSmtSe.0064B020	ASCII "Please enter registration name?"
0064AFC8	MOV EAX,QKSmtSe.0064B048	ASCII "Please enter registration code?"
0064B020	ASCII "Please enter reg"	
0064B030	ASCII "istration name?",0	
0064B048	ASCII "Please enter reg"	
0064B058	ASCII "istration code?",0	
0064B1C0	DD QKSmtSe.0064B3FA	ASCII 0F,"TfrmUnregPrompt"

y esto otro:

0064B4C4	MOV EDX,QKSmtSe.0064B604	ASCII "Your evaluation copy has expired!"
0064B51E	MOV EDX,QKSmtSe.0064B604	ASCII "Your evaluation copy has expired!"
0064B54F	PUSH QKSmtSe.0064B630	ASCII "Your evaluation copy will expire in "
0064B561	PUSH QKSmtSe.0064B660	ASCII " days..."
0064B583	PUSH QKSmtSe.0064B630	ASCII "Your evaluation copy will expire in "
0064B595	PUSH QKSmtSe.0064B674	ASCII " day..."
0064B604	ASCII "Your evaluation "	
0064B614	ASCII "copy has expired"	
0064B624	ASCII "t",0	
0064B630	ASCII "Your evaluation "	
0064B640	ASCII "copy will expire"	
0064B650	ASCII " in ",0	
0064B660	ASCII " days..."0	
0064B674	ASCII " day..."0	
0064B7D8	DD QKSmtSe.0064BA8F	ASCII 0A,"TFormAbout"

Nos colocamos sobre la línea 0064F724, pulsamos 2 veces sobre ella, subimos hasta la entrada de la rutina y le colocamos un breakpoint o F2, que es la que nos interesa.

0064F6A8	55	PUSH EBP
0064F6A9	8BEC	MOV EBP,ESP
0064F6AB	51	PUSH ECX
0064F6AC	B9 04000000	MOV ECX,4
0064F6B1	6A 00	PUSH 0
0064F6B3	6A 00	PUSH 0
0064F6B5	49	DEC ECX

En la linea 64F414 de las references text strings, si se quiere se puede colocar un punto de ruptura, aunque no es necesario, que nos manda a:

0064F3C8	55	PUSH EBP
0064F3C9	8BEC	MOV EBP,ESP
0064F3CB	83C4 F0	ADD ESP,-10
0064F3CE	53	PUSH EBX
0064F3CF	33D2	XOR EDX,EDX

Pulsamos F9 o le damos run, nos sale la ventana de registro, así que introducimos los datos que hemos introducido antes, pulsamos F9 y nos para en 0064F6A8:

0064F6A8	55	PUSH EBP
0064F6A9	8BEC	MOV EBP,ESP
0064F6AB	51	PUSH ECX
0064F6AC	B9 04000000	MOV ECX,4
0064F6B1	6A 00	PUSH 0
0064F6B3	6A 00	PUSH 0
0064F6B5	49	DEC ECX
0064F6B6	75 F9	JNZ SHORT QKSmtpSe.0064F6B1
0064F6B8	51	PUSH ECX
0064F6B9	874D FC	XCHG DWORD PTR SS:[EBP-4],ECX
0064F6BC	53	PUSH EBX
0064F6BD	56	PUSH ESI
0064F6BE	57	PUSH EDI
0064F6BF	8BF1	MOV ESI,ECX
0064F6C1	8BFA	MOV EDI,EDX
0064F6C3	8945 FC	MOV DWORD PTR SS:[EBP-4],EAX
0064F6C6	8B5D 08	MOV EBX,DWORD PTR SS:[EBP+8]
0064F6C9	33C0	XOR EAX,EAX
0064F6CB	55	PUSH EBP
0064F6CC	68 83F86400	PUSH QKSmtpSe.0064F883
0064F6D1	64:FF30	PUSH DWORD PTR FS:[EAX]
0064F6D4	64:8920	MOV DWORD PTR FS:[EAX],ESP
0064F6D7	8BCE	MOV ECX,ESI
0064F6D9	8BD7	MOV EDX,EDI
0064F6DB	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]
0064F6DE	E8 65FFFFFF	CALL QKSmtpSe.0064F648

La call que está en 0064F6DE, es la responsable de comprobar si nuestro numero es valido y de generarlo, así que entraremos directamente ahí.

0064F648	55	PUSH EBP
0064F649	8BEC	MOV EBP,ESP
0064F64B	6A 00	PUSH 0
0064F64D	53	PUSH EBX
0064F64E	56	PUSH ESI
0064F64F	8BF1	MOV ESI,ECX
0064F651	8BDA	MOV EBX,EDX
0064F653	33C0	XOR EAX,EAX
0064F655	55	PUSH EBP
0064F656	68 99F66400	PUSH QKSmtpSe.0064F699
0064F658	64:FF30	PUSH DWORD PTR FS:[EAX]
0064F65E	64:8920	MOV DWORD PTR FS:[EAX],ESP
0064F661	85DB	TEST EBX,EBX
0064F663	74 04	JE SHORT QKSmtpSe.0064F669
0064F665	85F6	TEST ESI,ESI
0064F667	75 04	JNZ SHORT QKSmtpSe.0064F66D
0064F669	33DB	XOR EBX,EBX
0064F66B	EB 16	JMP SHORT QKSmtpSe.0064F683
0064F66D	8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]
0064F670	8BC3	MOV EAX,EBX
0064F672	E8 71D2FFFF	CALL QKSmtpSe.0064C8E8
0064F677	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]
0064F67A	8BC6	MOV EAX,ESI
0064F67C	E8 F3ABDBFF	CALL QKSmtpSe.0040A274
0064F681	8BD8	MOV EBX,EAX
0064F683	33C0	XOR EAX,EAX
0064F685	5A	POP EDX
0064F686	59	POP ECX
0064F687	59	POP ECX
0064F688	64:8910	MOV DWORD PTR FS:[EAX],EDX
0064F68B	68 A0F66400	PUSH QKSmtpSe.0064F6A0
0064F690	8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]
0064F693	E8 985ADBFF	CALL QKSmtpSe.00405130
0064F698	C3	RETN

La linea 0064F672 es la call responsable de generar el número de serie y de enseñarnos el formato que debe tener, aunque no es necesario entrar dentro de ella, ya que, nada más pasar sobre ella en la siguiente linea nos muestra el número de serie que nos corresponde.



## Interior de la rutina:

0064C8F9	< 75 11	JNZ SHORT QKSmtpSe.0064C90C	
0064C8FB	. 8BC7	MOV EAX,EDI	
0064C8FD	. BA C4C96400	MOV EDX,QKSmtpSe.0064C9C4	ASCII "Error!"
0064C902	. E8 7D88DBFF	CALL QKSmtpSe.00405184	
0064C907	< E9 A6000000	JMP QKSmtpSe.0064C9B2	
0064C90C	> 8BD4	MOV EDX,ESP	
0064C90E	. 8BC6	MOV EAX,ESI	
0064C910	. E8 27FFFFFF	CALL QKSmtpSe.0064C83C	
0064C915	. 8BD5	MOV EDX,EBP	
0064C917	. 8BC4	MOV EAX,ESP	
0064C919	. B9 10000000	MOV ECX,10	
0064C91E	. E8 F964DBFF	CALL QKSmtpSe.00402E1C	
0064C923	. 8BC6	MOV EAX,ESI	
0064C925	. E8 D68ADBFF	CALL QKSmtpSe.00405400	
0064C92A	. F76D 00	IMUL DWORD PTR SS:[EBP],EAX	
0064C92D	. 8A1E	MOV BL,BYTE PTR DS:[ESI]	
0064C92F	. 33D2	XOR EDX,EDX	
0064C931	. 8AD3	MOV DL,BL	
0064C933	. 69D2 9A020000	IMUL EDX,EDX,29A	
0064C939	. 03C2	ADD EAX,EDX	
0064C93B	. 8945 00	MOV DWORD PTR SS:[EBP],EAX	
0064C93E	. 33C0	XOR EAX,EAX	
0064C940	. 8AC3	MOV AL,BL	
0064C942	. F76D 04	IMUL DWORD PTR SS:[EBP+4]	
0064C945	. 6BC0 7B	IMUL EAX,EAX,7B	
0064C948	. 8945 04	MOV DWORD PTR SS:[EBP+4],EAX	
0064C94B	. 8BC6	MOV EAX,ESI	
0064C94D	. E8 AE8ADBFF	CALL QKSmtpSe.00405400	
0064C952	. 33D2	XOR EDX,EDX	
0064C954	. 8A16	MOV DL,BYTE PTR DS:[ESI]	
0064C956	. F7EA	IMUL EDX	
0064C958	. 69C0 D5190000	IMUL EAX,EAX,19D5	
0064C95E	. 0145 08	ADD DWORD PTR SS:[EBP+8],EAX	
0064C961	. 8B5D 00	MOV EBX,DWORD PTR SS:[EBP]	
0064C964	. 035D 04	ADD EBX,DWORD PTR SS:[EBP+4]	
0064C967	. 035D 08	ADD EBX,DWORD PTR SS:[EBP+8]	
0064C96A	. 0FAF5D 0C	IMUL EBX,DWORD PTR SS:[EBP+C]	
0064C96E	. 895D 0C	MOV DWORD PTR SS:[EBP+C],EBX	
0064C971	. 57	PUSH EDI	Arg1
0064C972	. 8B45 00	MOV EAX,DWORD PTR SS:[EBP]	
0064C975	. 894424 24	MOV DWORD PTR SS:[ESP+24],EAX	
0064C979	. C64424 28 00	MOV BYTE PTR SS:[ESP+28],0	
0064C97E	. 8B45 04	MOV EAX,DWORD PTR SS:[EBP+4]	
0064C981	. 894424 2C	MOV DWORD PTR SS:[ESP+2C],EAX	
0064C985	. C64424 30 00	MOV BYTE PTR SS:[ESP+30],0	
0064C98A	. 8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
0064C98D	. 894424 34	MOV DWORD PTR SS:[ESP+34],EAX	
0064C991	. C64424 38 00	MOV BYTE PTR SS:[ESP+38],0	
0064C996	. 895C24 3C	MOV DWORD PTR SS:[ESP+3C],EBX	
0064C99A	. C64424 40 00	MOV BYTE PTR SS:[ESP+40],0	
0064C99F	. 8D5424 24	LEA EDX,DWORD PTR SS:[ESP+24]	
0064C9A3	. B9 03000000	MOV ECX,3	
0064C9A8	. B8 D4C96400	MOV EAX,QKSmtpSe.0064C9D4	ASCII "%.8x-%.8x-%.8x-%.8x"
0064C9AD	. E8 36F5DBFF	CALL QKSmtpSe.0040BEE8	QKSmtpSe.0040BEE8
0064C9B2	> 83C4 40	ADD ESP,40	
0064C9B5	. 5D	POP EBP	
0064C9B6	. 5F	POP EDI	
0064C9B7	. 5E	POP ESI	
0064C9B8	. 5B	POP EBX	

Justo al pasarla

0064F648	55	PUSH EBP
0064F649	8BEC	MOV EBP,ESP
0064F64B	6A 00	PUSH 0
0064F64D	53	PUSH EBX
0064F64E	56	PUSH ESI
0064F64F	8BF1	MOV ESI,ECX
0064F651	8BDA	MOV EBX,EDX
0064F653	33C0	XOR EAX,EAX
0064F655	55	PUSH EBP
0064F656	68 99F66400	PUSH QKSMTPSe.0064F699
0064F658	64:FF30	PUSH DWORD PTR FS:[EAX]
0064F65E	64:8920	MOV DWORD PTR FS:[EAX],ESP
0064F661	85DB	TEST EBX,EBX
0064F663	74 04	JE SHORT QKSMTPSe.0064F669
0064F665	85F6	TEST ESI,ESI
0064F667	75 04	JNZ SHORT QKSMTPSe.0064F66D
0064F669	33DB	XOR EBX,EBX
0064F66B	EB 16	JMP SHORT QKSMTPSe.0064F683
0064F66D	8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]
0064F670	8BC3	MOV EAX,EBX
0064F672	E8 71D2FFFF	CALL QKSMTPSe.0064C8E8
0064F677	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]
0064F67A	8BC6	MOV EAX,ESI
0064F67C	E8 F3ABDBFF	CALL QKSMTPSe.0040A274
0064F681	8BD8	MOV EBX,EAX
0064F683	33C0	XOR EAX,EAX
0064F685	5A	POP EDX
0064F686	59	POP ECX
0064F687	59	POP ECX
0064F688	64:8910	MOV DWORD PTR FS:[EAX],EDX
0064F68B	68 A0F66400	PUSH QKSMTPSe.0064F6A0
0064F690	8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]
0064F693	E8 985ADBFF	CALL QKSMTPSe.00405130
0064F698	C3	RETN
0064F699	E9 AE53DBFF	JMP QKSMTPSe.00404A4C
0064F69E	EB F0	JMP SHORT QKSMTPSe.0064F690
0064F6A0	8BC3	MOV EAX,EBX
0064F6A2	5E	POP ESI
0064F6A3	5D	POP EBP

Stack SS:[0012F528]=012EF11C, (ASCII "918476EF-B6AE9806-4A866E77-F03134E4")  
EDX=00000000

Apuntamos el número 918476EF-B6AE9806-4A866E77-F03134E4

Pulsamos F9 para que nos salte el error, le damos a aceptar e introducimos los datos que hemos obtenido y nos muestra:



Le damos a Ok, cerramos Olly y ejecutamos el programa, haber que pasa, vamos al about y vemos:



Ya está resuelto.

Gracias a todos.

Alberto Fernandez

20 – abril – 2012