

Última versión de Concar: Pero aplica para todas.

<http://www.descargasrealsystems.com/uploads/descargas/CONCAR-CB/CONCAR-CB-RK-v2017.02.zip>

1. Cargar CONCAR en Olly y ejecutarlo hasta que crashee.
2. CTRL+G y vamos a **401000**.
3. Clic derecho – Search for all reference strings, buscamos la palabra **REGISTERED** y le damos ENTER.

01EDCBDD	PUSH CTMENUW.0066CD30	UNICODE "HK Versi"
01EDCCDF	MOV EDX,CTMENUW.0066CD6C	UNICODE "HKSTATUS"
01EDCD00	PUSH CTMENUW.0066D1EC	UNICODE "REGISTERED"

4. Caemos en la zona del primer parche:

01EDCD00	68 ECD16600	PUSH CTMENUW.0066D1EC	UNICODE "REGISTERED"
01EDCD05	E8 207756FE	CALL CTMENUW.0044442A	
01EDCD0A	F7D8	NEG EAX	
01EDCD0C	1BC0	SBB EAX,EAX	
01EDCD0E	40	INC EAX	
01EDCD0F	F7D8	NEG EAX	
01EDCD11	66:F7D0	NOT AX	
01EDCD14	66:8985 54F	MOV WORD PTR [EBP-0x9AC],AX	
01EDCD1B	8D45 C0	LEA EAX,DWORD PTR [EBP-0x40]	
01EDCD1E	50	PUSH EAX	
01EDCD1F	8D45 C4	LEA EAX,DWORD PTR [EBP-0x3C]	
01EDCD22	50	PUSH EAX	
01EDCD23	6A 02	PUSH 0x2	
01EDCD25	E8 BE7656FE	CALL CTMENUW.004443E8	
01EDCD2A	83C4 0C	ADD ESP,0xC	
01EDCD2D	0FBF85 54F6	MOVSX EAX,WORD PTR [EBP-0x9AC]	
01EDCD34	85C0	TEST EAX,EAX	
01EDCD36	0F84 F14B00	JE CTMENUW.01EE192D	

Caemos aquí.

Parche 1
JMP 01EE192D

5. Vamos al botón R para seguir buscando strings:



6. Clic derecho, buscamos **RK0006** y damos ENTER.

01F2AC80	0F84	JE CTMENUW.01F2AF81	Parche 2. JMP 01F2AF81
01F2AC86	C785	MOV DWORD PTR [EBP-0x9C],0x80020004	
01F2AC90	C785	MOV DWORD PTR [EBP-0xA4],0xA	
01F2AC9A	C785	MOV DWORD PTR [EBP-0x8C],0x80020004	
01F2ACA4	C785	MOV DWORD PTR [EBP-0x94],0xA	
01F2ACAE	C785	MOV DWORD PTR [EBP-0xBC],CTMENUW.0066D1EC	
01F2ACB8	C785	MOV DWORD PTR [EBP-0xC4],0x8	
01F2ACC2	68 64	PUSH CTMENUW.00675164	UNICODE "RK0006.Su servicio post venta ha expirado."

Caemos aquí.

7. Vamos al botón **R** para seguir buscando strings:



8. Clic derecho, buscamos **RK0007** y damos ENTER. Caemos en:

```
01F2B303 PUSH CTMENUW.00675424 UNICODE "RK0007.Su servicio post venta esta vencido."
```

Cambiamos ese PUSH por un **JMP** hacia la dirección después del primer **JE**.

Sería **JMP 01F2B540** porque es la línea que está después del primer **JE** a partir del **PUSH** donde caímos. Esto es para eliminar el rectángulo **amarillo** (NAG) que sale al abrir Concar.

01F2B53E	74 14	JE SHORT CTMENUW.01F2B554	→	Primer JE a partir del PUSH.
01F2B540	FF35	PUSH DWORD PTR [0x3482464]	→	El JMP debe saltar aquí.
01F2B546	8B45	MOV EAX,DWORD PTR [EBP+0x8]		

9. Vamos al botón **R** para seguir buscando strings. Recuerda posicionarte desde el principio para buscar en todo el bloque. Clic derecho, buscamos **RK0008** y damos ENTER. Cambiamos el **JE** por **JMP**.

01F2AFAB	0F84	JE CTMENUW.01F2B2AC	→	JMP 01F2B2AC
01F2AFB1	C785	MOV DWORD PTR [EBP-0x9C],0x800		
01F2AFB8	C785	MOV DWORD PTR [EBP-0xA4],0xA		
01F2AFC5	C785	MOV DWORD PTR [EBP-0x8C],0x800		
01F2AFCF	C785	MOV DWORD PTR [EBP-0x94],0xA		
01F2AFD9	C785	MOV DWORD PTR [EBP-0xBC],CTMEN		
01F2AFE3	C785	MOV DWORD PTR [EBP-0xC4],0x8		
01F2AFED	68 78	PUSH CTMENUW.00675378		

Unicode "Contabilidad CONCAR v." ←

Unicode "RK0008.Su servicio post venta ha expirado."

Caemos aquí.

10. Eliminar los **RK0002**. Lo más deseamos por los revendedores de CONCAR. 😊

CTRL+G y vamos a la dirección 401000. CTRL+S y buscamos la secuencia de comandos siguiente:

```
PUSH [EBP+8]
CALL [EAX+4]
PUSH CONST
CALL CONST
MOVSX EAX,AX
TEST EAX,EAX
```

Le damos ENTER a la segunda CALL.

<pre>PUSH DWORD PTR [EBP+0x8] CALL DWORD PTR [EAX+0x4] PUSH CTMENUW.03482454 CALL CTMENUW.02EFE1EA MOVSX EAX,AX TEST EAX,EAX</pre>	ENTER AQUÍ.
--	-------------

Caemos en un PUSH y lo cambiamos por RET.

02EFE1EA	55	PUSH EBP	→ RET
----------	----	----------	-------

11. Eliminar el tiempo de espera al iniciar CONCAR.

Vamos a la primera dirección que encontramos donde está la string **REGISTERED: 01EDCD00**.

Colocamos un JMP donde está el primer PUSH EAX hacia el otro PUSH EAX.

01EDCCDF	BA 6CCD6600	MOV EDX,CTMENUW.0066CD6C	UNICODE "HKSTATUS"
01EDCCE4	8D4D C4	LEA ECX,DWORD PTR [EBP-0x3C]	
01EDCCE7	E8 4A7756FE	CALL CTMENUW.00444436	
01EDCCEC	8D45 C4	LEA EAX,DWORD PTR [EBP-0x3C]	
01EDCCCF	50	PUSH EAX	JMP
01EDCCF0	E8 B95E0301	CALL CTMENUW.02F12BAE	
01EDCCF5	8BD0	MOV EDX,EAX	
01EDCCF7	8D4D C0	LEA ECX,DWORD PTR [EBP-0x40]	
01EDCCFA	E8 317756FE	CALL CTMENUW.00444430	
01EDCCFF	50	PUSH EAX	
01EDCD00	68 ECD16600	PUSH CTMENUW.0066D1EC	UNICODE "REGISTERED"
01EDCD05	E8 207756FE	CALL CTMENUW.0044442A	

Quedaría así:

01EDCCDF	BA 6CCD6600	MOV EDX,CTMENUW.0066CD6C	UNICODE "HKSTATUS"
01EDCCE4	8D4D C4	LEA ECX,DWORD PTR [EBP-0x3C]	
01EDCCE7	E8 4A7756FE	CALL CTMENUW.00444436	
01EDCCEC	8D45 C4	LEA EAX,DWORD PTR [EBP-0x3C]	
01EDCCCF	E8 0E	JMP SHORT CTMENUW.01EDCCFF	
01EDCCF1	90	NOP	
01EDCCF2	90	NOP	
01EDCCF3	90	NOP	
01EDCCF4	90	NOP	
01EDCCF5	8BD0	MOV EDX,EAX	
01EDCCF7	8D4D C0	LEA ECX,DWORD PTR [EBP-0x40]	
01EDCCFA	E8 317756FE	CALL CTMENUW.00444430	
01EDCCFF	50	PUSH EAX	
01EDCD00	68 ECD16600	PUSH CTMENUW.0066D1EC	UNICODE "REGISTERED"

Listo. Como está empacado con Themida, pueden hacer un loader ya que tienen todos los datos necesarios.

IvinsonCLS

14/04/2017

lpadilla63@gmail.com