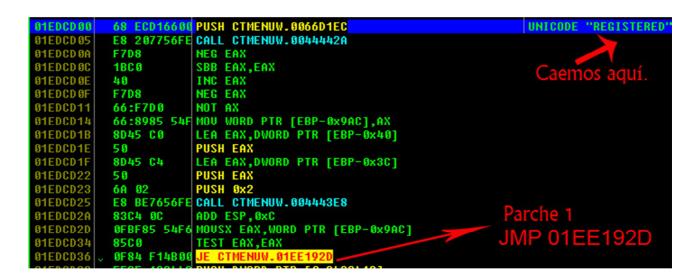
Última versión de Concar: Pero aplica para todas.

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 MOU EDX,CTMENUW.0066CD6C UNICODE "HKSTATUS"
01EDCD00 PUSH CTMENUW.0066D1EC UNICODE "REGISTERED"
```

4. Caemos en la zona del primer parche:



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



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

```
### STEARS | ### OF STEAR | ### OF S
```

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] EI JMP debe saltar aquí.

01F2B546 8B45 MOU 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**.

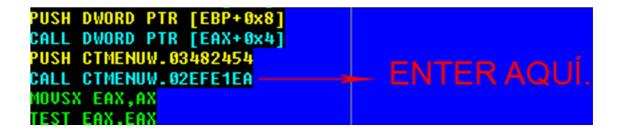


10. Eliminar los **RK0002**. Lo más deseamos por los revendedores de CONCAR. ©

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.



Caemos en un PUSH y lo cambiamos por 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.

```
BA 6CCD6600
                           MOU EDX,CTMENUW.0066CD6C
                                                            UNICODE "HKSTATUS"
01EDCCE4
           8D4D C4
                           LEA ECX, DWORD PTR [EBP-0x3C]
           E8 4A7756FE
                           CALL CTMENUW.00444436
01EDCCE7
01EDCCEC
           8D45 C4
                           LEA EAX, DWORD PTR [EBP-0x3C]
                                                                  JMP
                           PUSH EAX
CALL CTMENUW.02F12BAE
01EDCCEF
01EDCCF0
           E8 B95E0301
01EDCCF5
           8BD 0
                           MOV EDX, EAX
01EDCCF7
           8D4D C0
                           LEA ECX, DWORD PER LED!
                           CALL CTMENUM
                                            ··4430
           E8 317756FE
01EDCCFA
                           PUSH CTMENUW.0066D1EC
01EDCCFF
           50
 1EDCD 00
           68 ECD16600
                                                            UNICODE "REGISTERED"
                           CALL CTMENUW.0044442A
01EDCD 05
           E8 207756FE
```

Quedaría así:

```
BA 6CCD6600
                            MOU EDX,CTMENUW.0066CD6C
                                                               UNICODE "HKSTATUS"
11EDCCDF
                            LEA ECX, DWORD PTR [EBP-0x3C]
01EDCCE4
            8D4D C4
                            CALL CTMENUW.00444436
01EDCCE7
            E8 4A7756FE
                            LEA EAX,DWORD PTR [EBP-0x3C]
JMP SHORT CTMENUW.01EDCCFF
           8D45 C4
01EDCCEC
01EDCCEF
                            NOP
01EDCCF1
                            HOP
01EDCCF2
                            NOP
01EDCCF3
01EDCCF4
                            HOP
01EDCCF5
            8BD 0
                            MOV EDX, EAX
                            LEA ECX, DWORD PTR [EBP-0x40]
01EDCCF7
           8D4D C0
                            CALL CTMENUW.00444430
01EDCCFA
           E8 317756FE
01EDCCFF
           →50
                            PUSH EAX
                            PUSH CTMENUW.0066D1EC
                                                               UNICODE "REGISTERED"
  EDCD 00
           68 ECD16600
```

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

IvinsonCLS

14/04/2017

Ipadilla63@gmail.com