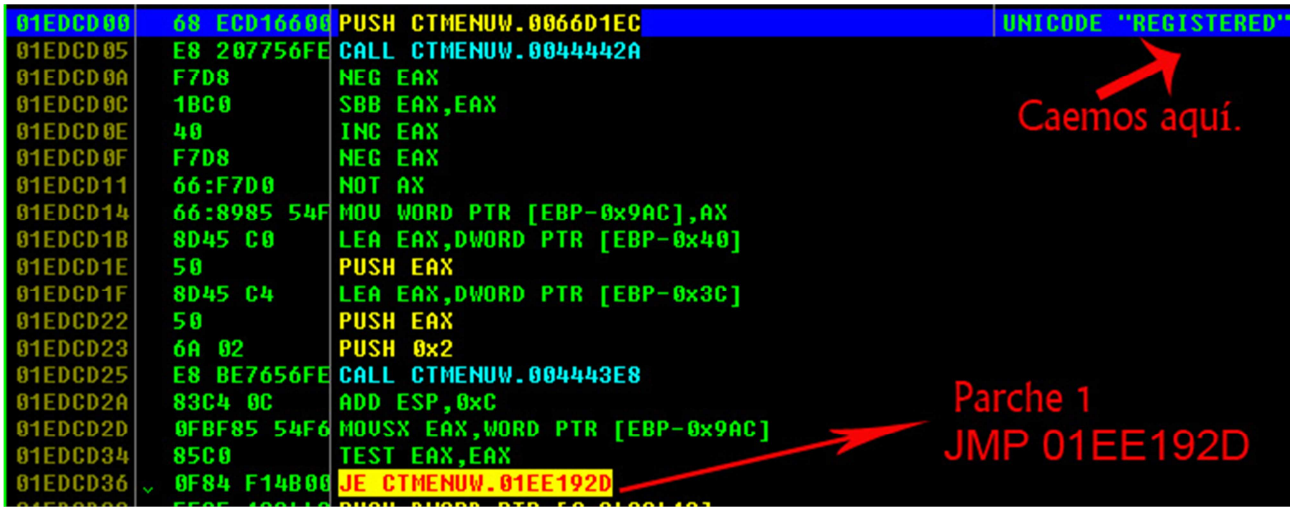
Última versión de Concar: Pero aplica para todas.

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.

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.

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

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

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.

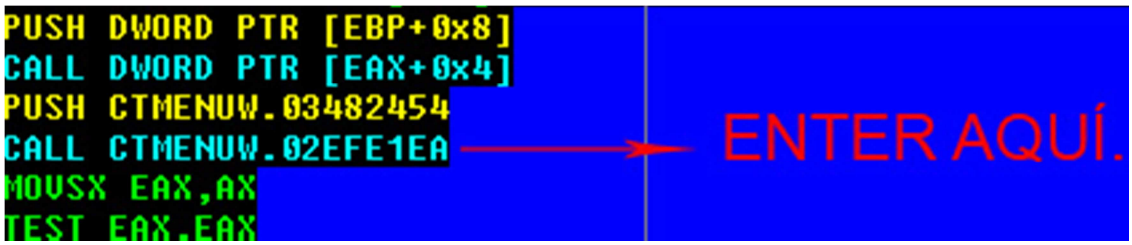
9. Vamos al botón **R** para seguir buscando strings. Recuerda posicionarte desde el principio para buscar en todo el bloque. Clic derecho, buscamos **RK0008** y damos ENTER. Cambiamos el **JE** por **JMP**.

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.

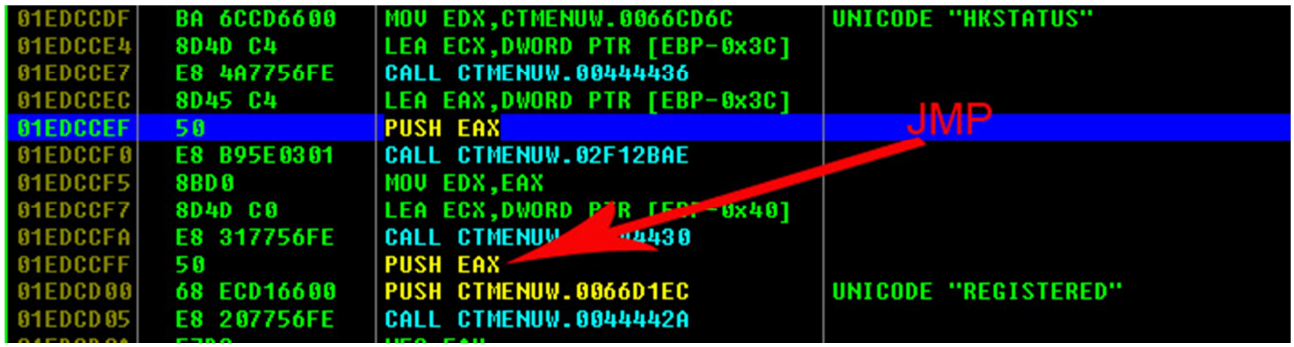


Caemos en un PUSH y lo cambiamos por RET.

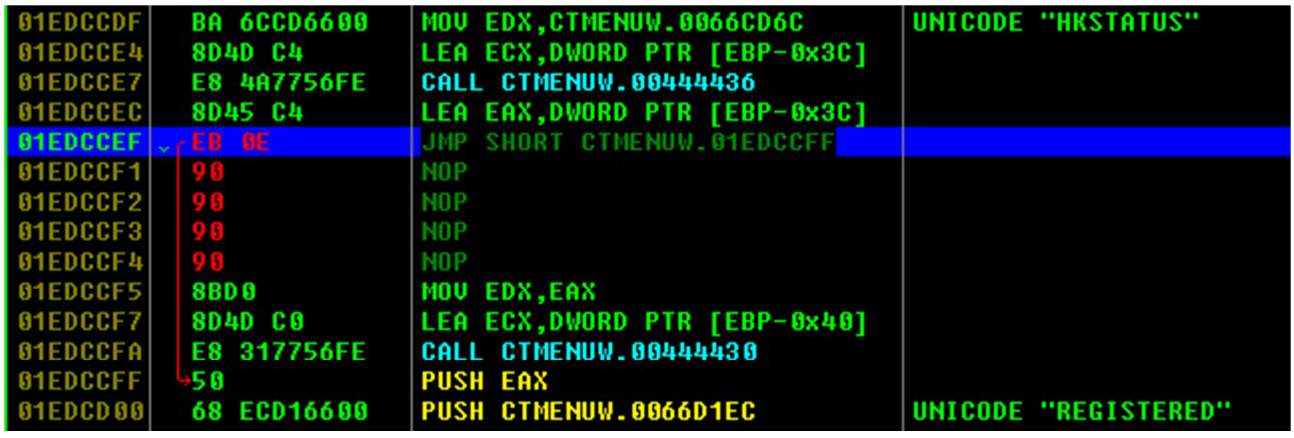
11. Eliminar el tiempo de espera al iniciar CONCAR.

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.



Quedaría así:



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

IvinsonCLS

14/04/2017

Ipadilla63@gmail.com