Lab_06-1

1. 0x00403420
    a. GetCommandLineA gets the command line for the process
    b. GetStartupInfoA populates a struct with process startup info
    c. GetModuleHandleA returns a handle to the file that created the current process (with the used arguments)
2. Solutions:
    a. There appears to be an encoding function at 0x004012ec. It is decoding strings in the data section of the binary
    b. It is repeatedly calling the encoding function in order to decode the aforementioned strings
3. Solutions:
    a. It is calling GetProcAddress to dynamically load library imports after decoding them from the above function
    b. It attempts to load all of the imports. If any fail, it frees the library and returns 0. Otherwise returns 1
4. The program figures out how large the exe will be after loading its headers, then reads in bytes from the end of the file and decodes them. It gets the executable path, then appends a buffer to it.

    It then creates a new process and begins attempting to read/write its memory (sanity checking and maybe dynamic code modifications). It appears to also attempt to check if it's in a sandbox or vm, and might be accessing registry values. Additionally, it may be attempting to switch the mouse buttons or do something similar. The end of the file also appears to have some IRC commands, but I'm not sure what they might be used for.