Malware Analysis
Fall 2015
Lab 04 - Debugging Concepts and Tools

The textbook and slides talk about using Ollydbg and Windbg for debugging. These tools are somewhat out of date, and there are better alternatives that come with FLARE. We would recommend using x64dbg or x32dbg, depending on the binary you're analysing.

Lab_04-1.malware
This sample uses an anti-analysis technique that we will discuss later on in the course. The anti-analysis technique makes static analysis harder. Using dynamic analysis is highly recommended!

1. (5%) Set a breakpoint at 0x00401092, what is this sample calling?

2. (5%) What is being called at 0x004010A6? What is the callee doing?

3. (5%) What is sub_401360 doing? What about sub_401372 and sub_401388?

4. (15%) What Windows API functions did the sample import?

5. (10%) How did you find the Imported functions?

6. (10%) What does this sample do?