Malware Analysis
Fall 2015
Lab 02 - Advanced Static Analysis

Lab_02-1.malware

1. (10%) Main function:
    a. What is the address of main?

    b. What does this function do?

        i. What code constructs are used in this function?

        ii. Are there any interesting strings? If so, what are they?

2. (15%) Looking at the subroutine a 0x00401130:
    a. What are the arguments to InternetConnectA? What do they mean?

    b. What does this function do?

        i. What code constructs are used in this function?

3. (10%) Looking at the subroutine at 0x00401000:
    a. What code constructs are used in this function?

    b. What imported functions are called?

    c. What does this subroutine do?

4. (15%) What does this malware do?

Lab_02-2.malware

1. (15%) Main function:
    a. What imported functions are called?

        i. What do these functions do?

        ii. Any interesting strings?

2. (15%) Looking at the subroutine at 0x0040135C:
    a. What imported functions are called?

    b. What code constructs are used here?
    Hint: Look at the 'jmp eax' at 0x00401465, try to guess where that jump could potentially take you

3. (20%) What does this malware do?

    a. What signatures would you propose?
        i. Why are they useful signatures?

        ii. Does the sample create any files? If so, what are they used for?