Malware Analysis
Fall 2015
Lab 06 - Data Encoding and Malware Countermeasures

Lab_06-1.malware

1. (20%) What is the address of the _main function?

    a. What imported function does main call?

        i. What do these functions do?

2. (30%) Looking at the subroutine at 0x00402C6E:

    a. Is there an encoding/decoding function? If so:

        i. What is the address of the function?

        ii. What is being encoded/decoded?

    b. What is the very large basic block doing?

3. (20%) Looking at the subroutine at 0x004023D0:

    a. What are all of the GetProcAddress calls doing?

    b. What does this function do?

4. (30%) In two or three paragraphs, what does this sample do?