# **Lab 9 Report**

1. Name: Student ID:
2. Analyze the Lab06-01.exe

What is the major code construct found in the only subroutine called by main?

What is the subroutine located at 0x40105F?

What is the purpose of this program?

1. Analyze the Lab06-02.exe

What operation does the first subroutine called by main perform?

What is the subroutine located ar 0x40117F?

What does the second subroutine called by main do?

What type of code construct is used in this subroutine?

Are there any network-based indicators for this program?

What is the purpose of this malware?

1. Analyze the Lab06-03.exe

Compare the calls in main to Lab6-2’s main method. What is the new function called from this main?

What parameters does this new function take?

What major code construct does this function contain?

What can this function do?

Are there any host-based indicators for this malware?

What is the purpose of this malware?

1. Analyze the Lab06-04.exe

What is the difference between the calls made from the main method in Lab6-3 and 6-4?

What new code construct has been added to main?

What is the difference between this lab’s parse HTML function and those of the previous labs?

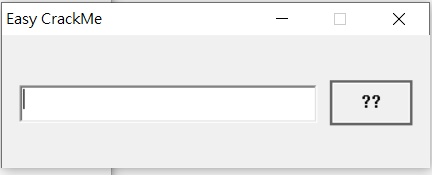
How long will this program run? (Assume that it is connected to the Internet)

Are there any new network-based indicators for this malware?

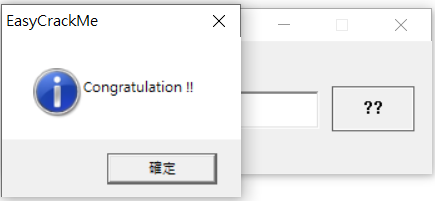
What is the purpose of this malware?

1. Please analyze Easy\_CrackMe.exe. (Use IDA PRO)

After you run the exe file, you will see an input box like



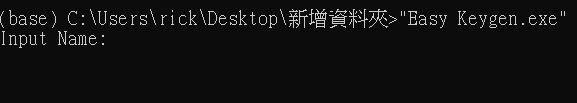
Please Find the correct Password and you will get the correct response.



A:

1. Please analyze Easy\_Keygen.exe. (Use IDA PRO)

You need to run the exe file in cmd like



In this case, you need to enter the Input Name and Input Serial. If Name and Serial are matched, you will get correct response. Please find the Input Name when the Input Serial is 5B134977135E7D13.



A: