Lab 9 Report

1. Name: 林靖昀 Student ID: B12902116

2. Analyze the Lab06-01.exe

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

   An if statement.

   What is the subroutine located at 0x40105F?

   printf.

   What is the purpose of this program?

   Check the internet connection and print its status.

3. Analyze the Lab06-02.exe

   What operation does the first subroutine called by main perform?

   Check internet connection.

   What is the subroutine located ar 0x40117F?

   printf.

   What does the second subroutine called by main do?

   Download the webpage from http://www.praticalmalwareanalysis.com/cc.htm, then parse out the comment and return it.

   What type of code construct is used in this subroutine?

   A buffer array used to store the results of InternetReadFile.

   Are there any network-based indicators for this program?

   There are two interesting strings in the program:

   1. http://www.praticalmalwareanalysis.com/cc.htm
   2. Internet Explorer 7.5/pma

   What is the purpose of this malware?

   It checks the internet connection, then attempts to download and parse the comment from http://www.praticalmalwareanalysis.com/cc.htm, if it is successful, it sleeps for 60000ms.

4. 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?

   The function 0x401130.

   What parameters does this new function take?

   The html comment parsed from the previous function, and argv[0], which is the program's name.

   What major code construct does this function contain?

   A switch case.

What can this function do?

Depending on the parsed comment, it can:

1. Create a directory.
2. Copy a file.
3. Delete a file.
4. Set a registry value.
5. Sleep.
6. Print an error message.

Are there any host-based indicators for this malware?

1. Software\Microsoft\Windows\CurrentVersion\Run\Malware
2. C:\Temp\cc.exe

What is the purpose of this malware?

1. Check the internet connection.
2. Parses the command from the html comment.
3. Depending on the command, it can:
    a. Create a directory.
    b. Copy a file.
    c. Delete a file.
    d. Set a registry value.
    e. Sleep.
    f. Print an error message.

5. Analyze the Lab06-04.exe

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

This program calls the 0x401040 function, which is similar to the function in Lab6-3, except it takes an argument. The function is called 1440 times, each time with a different argument, from the number 0 to 1439, after each call depending on the result it either returns, or calls the same two functions as seen in Lab6-3, and sleeps for 1 minute, then continues to the next iteration.

What new code construct has been added to main?

A for loop.

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

It takes an integer argument, and modifies the user agent string with that integer, the format string is as follows:

"Internet Explorer 7.50/pma%d", the argument is inserted here.

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

Depending on the contents of the html, if only counting the sleep time, it will run anywhere between:

0 to 1440 * (60000 + 100000) ms, which is:

0 to 3840 minutes

0 is when the first iteration of the for loop gets an error and returns immediately. This is not entirely accurate since there is still processing time for the other functions such as printing the error message or doing internet operations.

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

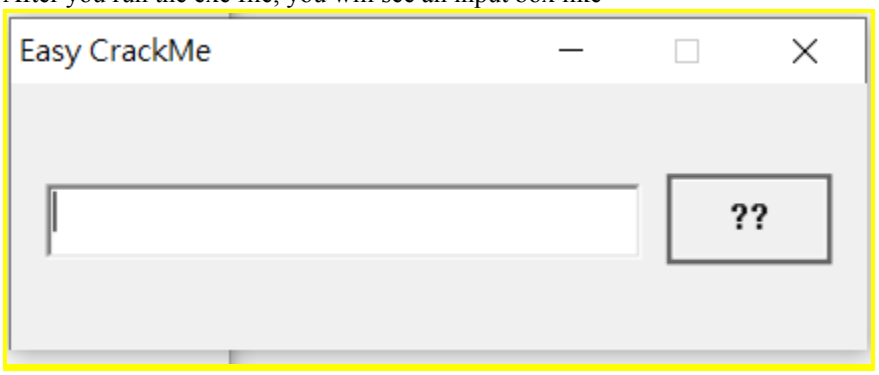
1. The user agent string is different as it is a format string instead:

   "Internet Explorer 7.50/pma%d"

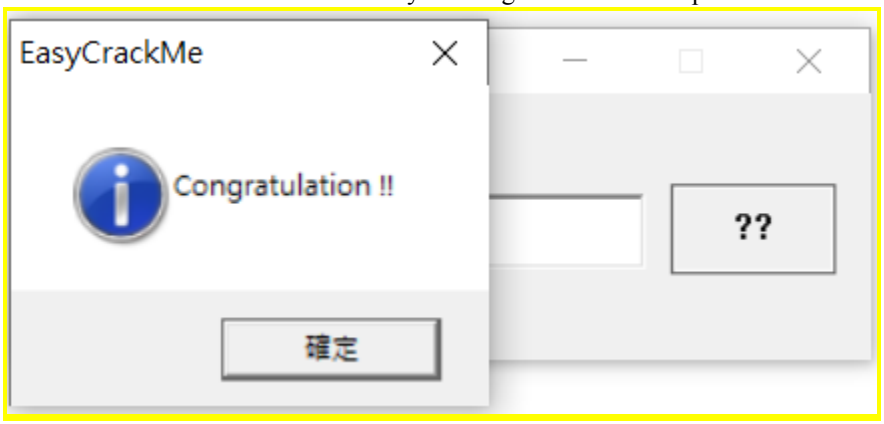
What is the purpose of this malware?

It essentially does the same thing as the one in Lab6-3, except it tries the internet operations with 1440 different user agent names.

6. 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: Ea5yR3versing.

7. 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.


(base) C:\Users\rick\Desktop\新增資料夾>"Easy Keygen.exe"
Input Name:
Input Serial: 5B134977135E7D13
Correct!

A: K3yg3nm3