|  |  |  |
| --- | --- | --- |
| Week | Malware Analysis Tools and Techniques | Duration |
| 6 | IDA Pro Practical | 120 mins |

**Lesson Objectives**

Use IDA Pro to recognize and analyse code constructs to understand overall functionality of Assembly Language program.

# Lab 01 [40 mins]

In this lab, you will analyze the malware found in the file *Lab06-01.exe*.

**Question 1**

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

(Hint: look at graph in IDA Pro)

**Question 2**

What is the subroutine located at 0x40105F?

**Question 3**

What is the purpose of this program?

# Lab 02 [40 mins]

Analyze the malware found in the file *Lab06-02.exe*.

**Question 1**

What operation does the first subroutine called by main perform?

**Question 2**

What is the subroutine located at 0x40117F?

**Question 3**

What does the second subroutine called by **main** do?

**Question 4**

What type of code construct is used in this subroutine?

**Question 5**

Are there any network-based indicators for this program?

**Question 6**

What is the purpose of this malware?

# Lab 03 [40 mins]

In this lab, you will analyze the malware found in the file *Lab06-03.exe*.

**Question 1**

Compare the calls in main to Lab 6-2’s **main** method. What is the new function called from **main**?

**Question 2**

What parameters does this new function take?

**Question 3**

What major code construct does this function contain?

**Question 4**

What can this function do?

**Question 5**

Are there any host-based indicators for this malware?

**Question 6**

What is the purpose of this malware?