|  |  |  |
| --- | --- | --- |
| Week | Reverse Engineering Malware | Duration |
| 8 | IDA Pro Practical | 60 mins |

Marks allocation: 10/100 for CA tutorial submission

**Lesson Objectives**

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

Lab files can be found on desktop folder (Labs) on the Windows XP Virtual Machine.

# Lab 01 [60 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**?

Function 0x401000 and 0x401040 is the same as lab 6-2. But 0x401130 is a new function.

**Question 2**

What parameters does this new function take?

This new function take the command character from the HTML comment and argv[0]

**Question 3**

What major code construct does this function contain?

This function major code construct is a “switch” statement with jump table

**Question 4**

What can this function do?

This function can print error message, create directory, copy and delete file, set registry and sleep after 100 second

**Question 5**

Are there any host-based indicators for this malware?

Yes, this is 2 host-based indicators

**Question 6**

What is the purpose of this malware?

This malware first will check if there is internet connection. If there is connection, it will try get the command in the website comment (which start with <!--) than create a directory, copy itself to that directory than delete itself from the old location and add a registry key to user system or sleep for 100 second.