Module 07

Software Goes Undercover

Malware - Software Goes Undercover

Malware is a term that is often used to refer to malicious programs and software that are intended to harm a computer. These malware programs can corrupt a computer. Some of them are relatively harmless, only attempting to slow down the speed of the hard drive. Some, however, are much more harmful.

ICON KEY


Important Information

Quiz


CPTE Labs


Course Review

Lab Objectives

The objective of this lab is to help students learn how to create viruses and worms.

In this lab, you will learn how to:

- Create viruses using tools
- Create worms using worm generator tool

Lab Scenario

A computer virus attaches itself to a program or tile enabling it to spread from one computer to another, leaving infections as it travels. The biggest danger with a worm is its capability to replicate itself in your environment, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat.

Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack. The attacker would normally serve to transport multiple attacks in one payload. The attacker can launch a Dos attack or install a backdoor and maybe even damage a local system or network systems.

Since you are a Penetration Testing Engineer, the IT director instructs you to test the network for any viruses and worms that damage or steal the organization's information. You need to construct viruses and worms and try to inject them in a Windows 7 virtual machine and check whether they are detected by antivirus programs or able to bypass the network firewall.

Lab Environment

This lab requires:

- Window Server 2008, Windows 7 running in virtual machine as guest machine

- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Virus and Worms

A virus is a self-replicating program that produces its own code by attaching copies of it onto other executable codes. Some viruses affect computers as soon as their codes are executed: others lie dormant until a predetermined logical circumstance is met. Computer worms are malicious programs that replicate, execute, and spread across network connections independently without human interaction. Most worms are created only to replicate and spread across a network consuming available computing resources. However, some worms carry a payload to damage the host system.

Lab Tasks

Recommended labs to assist you in creating Viruses and Worms:

- **Lab 1: Creating a virus using the JPS Virus Maker tool**
- **Lab 2: Virus analysis using IDA Pro**

Lab Analysis

Analyze and document the results related to the lab. Give your opinion on your target's security posture and exposure through public and free information.

Lab 1

Creating a Virus Using the JPS Virus Maker Tool

JPS Virus Maker Tool

JPS Virus Maker is a tool to create viruses. It also has a feature to convert a virus into a worm.

You can create your virus without knowledge of coding.

Lab Scenario

Select all options you want with your virus and then click on create Virus. It will create an effective virus. There are many options which your virus will perform on a victim's computer system. Your virus will able to hide itself from the process list and it will disable many Windows functions.

This tool can create any type of virus depending on what you demand. You can make the virus shut down the computer, restart the interface, freeze the screen, or anything else you demand it to do, with over 50 options. The file could be created as a .jpg, .exe file or any other type, with capabilities as you commanded.

The objective of this lab is to help students learn and understand how to create viruses and worms.

Lab Resources

To run this lab, you will need the following:

- JPS Virus Maker located on Desktop
- Run this tool on Windows 7
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

ICON KEY


Important Information

Quiz


CPTE Labs


Course Review

Lab Tasks

Task 1

Make a Virus

1. Launch your Windows 7 Virtual machine. **Note: Take a Snapshot of VM before doing these steps.**
2. Launch the JPS Virus Maker tool from Desktop. Installation is not required for JPS Virus Maker. Double-click and launch the jps.exe file.
3. The JPS (Virus Maker 3.0) window appears.

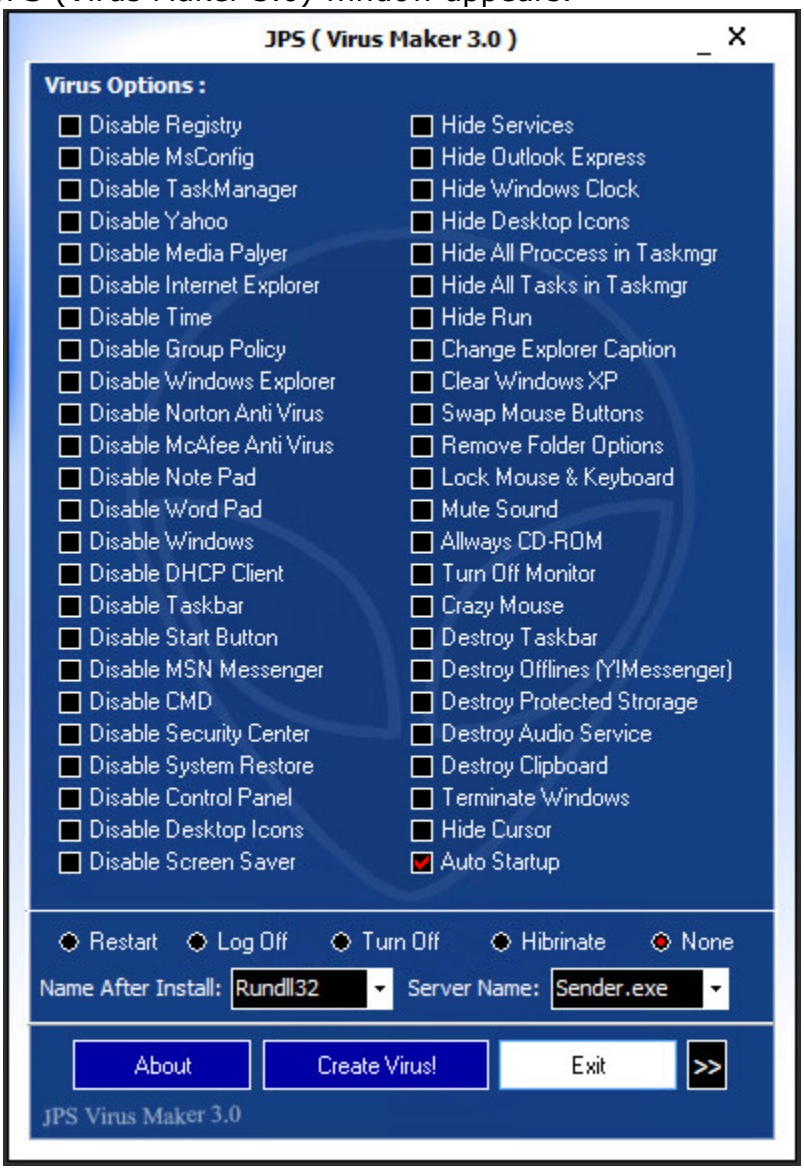


Figure: 1.1- JPS Virus Maker main window

Note: Take a Snapshot of the virtual machine before launching the JPS Virus Maker tool.

The option, Auto Startup is always checked by default and start the virus whenever the system boots on.

This creation of a virus is only for knowledge purposes; don't misuse this tool

A list of names for the virus after install is shown in the Name after Install drop-down list.

Figure: 1.2- JPS Virus Maker main window with options selected

4. Select one of the radio buttons to specify when the virus should start attacking the system after creation.

A list of server names is present in the Server Name drop-down list. Select any server name.

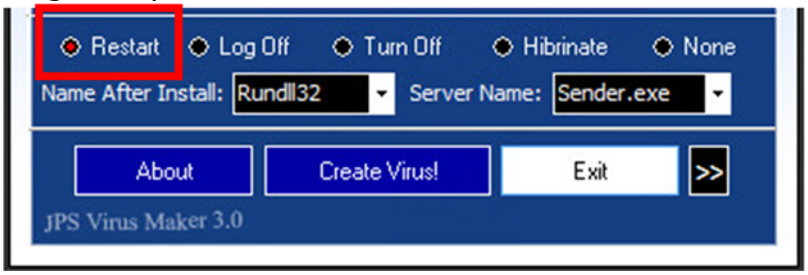


Figure: 1.3- JPS Virus Maker main window with restart selected

5. Select the name of the service you want to make the virus behave like from the *Name after Install* drop-down list.

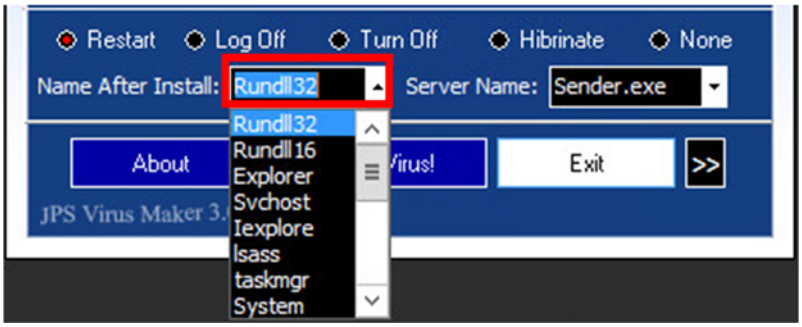


Figure: 1.4- JPS Virus Maker main window with Install options

6. Select a server name for the virus from the *Server Name* drop-down list.

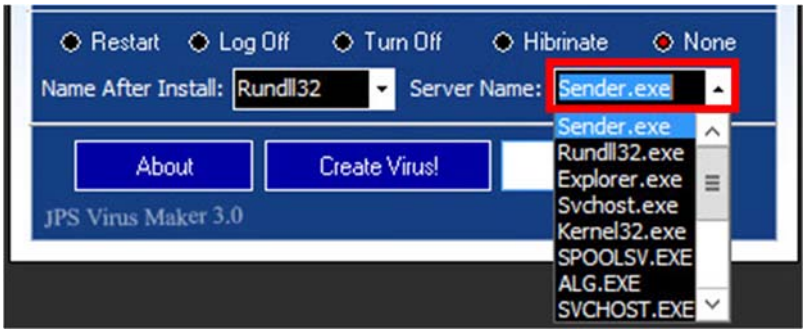


Figure: 1.5- JPS Virus Maker main window with Server Name options

Don't forget to change the settings for every new virus creation. Otherwise, by default, it takes the same name as an earlier virus.

7. Now, before clicking on Create Virus! change setting and virus options by clicking the  icon.

Figure: 1.6- JPS Virus Maker main window with Settings options

Task 1

Make a Virus

8. Here, you see more options for the virus. Check the options and provide related information in the respective text field.

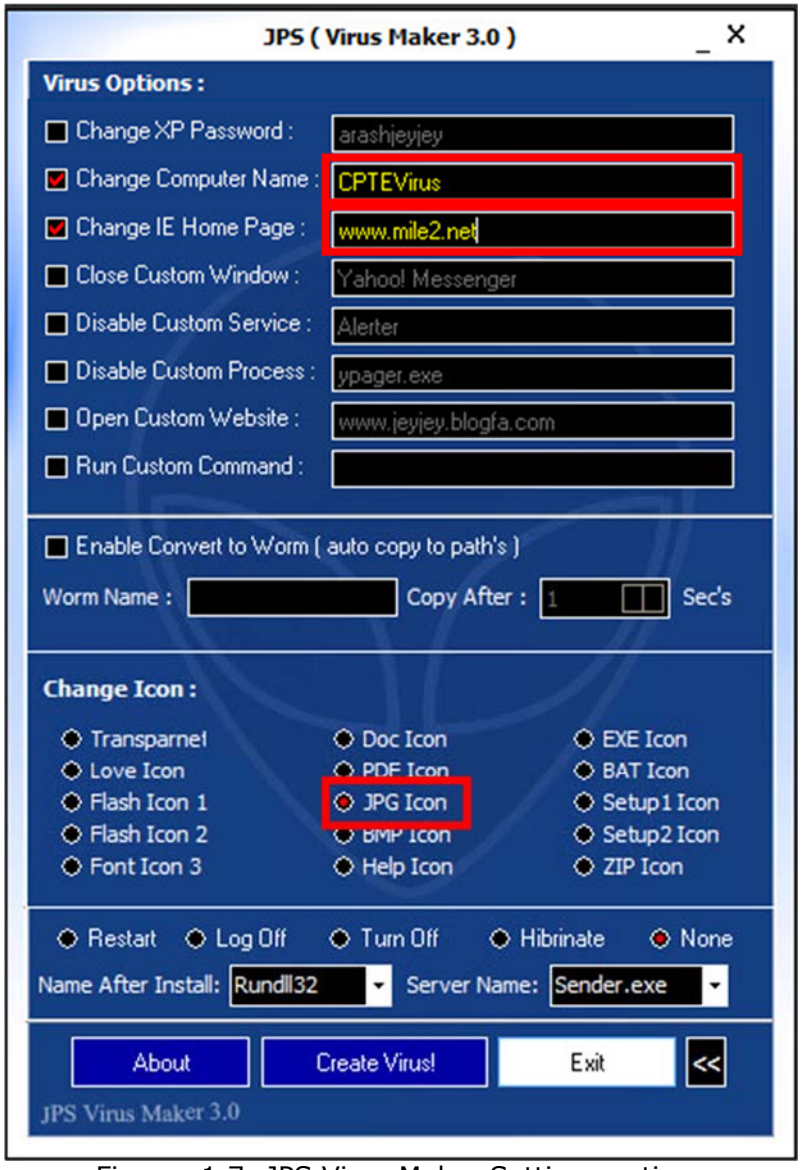


Figure: 1.7- JPS Virus Maker Settings options

You can select any icon from the change icon options. A new icon can be added apart from those on the list.

9. You can change the **Windows password**, **IE home page**, **close custom window**, **disable a particular custom service**, etc.
10. You can even allow the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox and provide a **Worm Name**.
11. For the worm to self-replicate after a particular time period, specify the time (in seconds) in the **Copy after** field.
12. You can also change the **virus icon**. Select the type of icon you want to view for the created virus by selecting the radio button under the **Change Icon** section.

Make sure to check all the options and settings before clicking on Create Virus!

Features
Change XP Password
Change Computer Name
Change IE Home Page
Close Custom Windows
Disable Custom Service
Disable Process
Open Custom Website
Run Custom Command
Enable Convert To Worm
- Auto Copy Server To Active Padi With Custom
Name & Time
Change Custom Icon For
your created Virus (15 Icons)

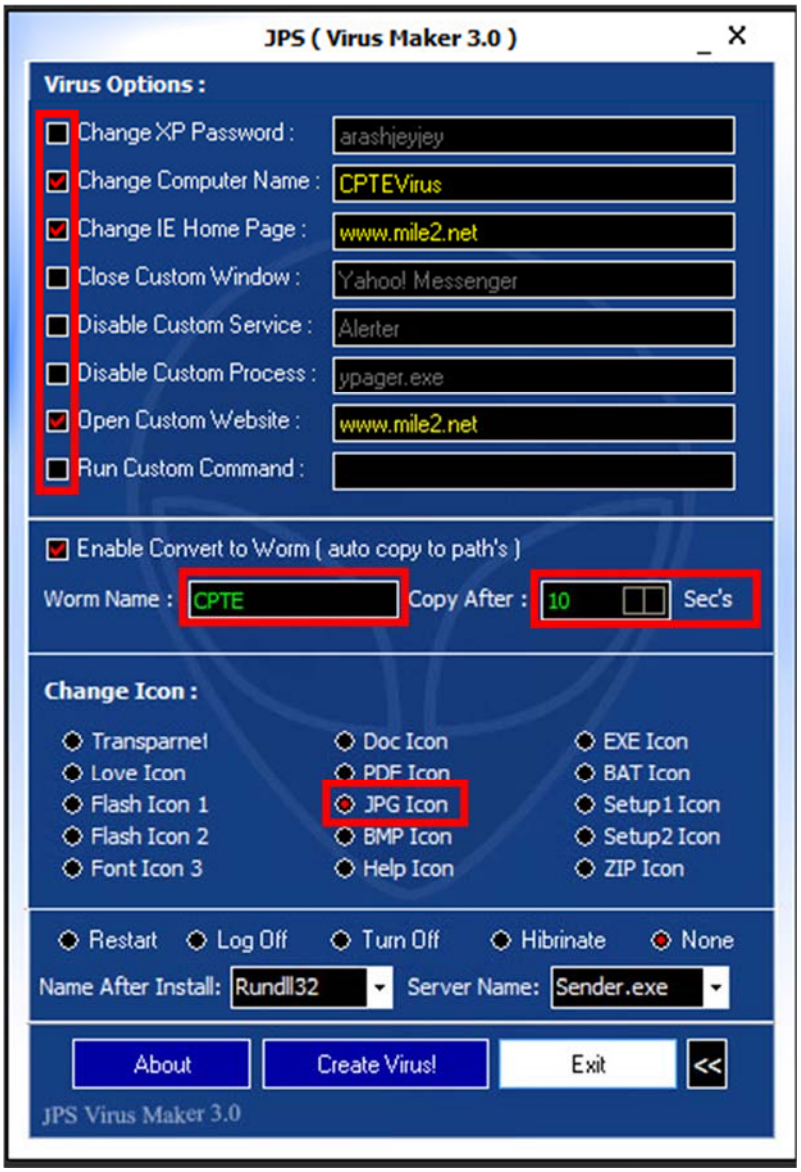


Figure: 1.8- JPS Virus Maker Settings options

13. After completing your selection of options, click **Create Virus**!

Figure: 1.10- JPS Virus Main windows with Create Virus! Button

14. A pop-up window with the message Server Created Successfully appears. Click OK.
15. The newly created virus (server) is placed automatically in the same folder as jps.exe but with name **Sender.exe**.
16. Now pack this virus with a binder or virus packager and send it to the victim machine. ENJOY!

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

Tool / Utility	Information Collected / Objectives Achieved
JPS Virus Maker Tool	To make Virus: • Disable Yahoo • Disable Internet Explorer • Disable Norton Antivirus • Disable McAfree Antivirus • Disable Taskbar • Disable Security Restore • Disable Control Panel • Hide Windows Clock • Hide All Tasks in Task.mgr • Change Explorer Caption • Destroy Taskbar • Destroy Offline (Y!Messenger) • Destroy Audio Services • Terminate Windows • Auto Setup

Quiz

1. Infect a virtual machine with the created viruses and evaluate the behavior of the virtual machine.
2. Examine whether the created viruses are detected or blocked by any anti-virus programs or anti-spyware.

Lab 2

Virus Analysis Using IDA

IDA Pro Overview

The IDA Disassembler **and Debugger** is an interactive, programmable, extendible, multi-processor disassembler hosted on Windows, Linux, or Mac OSX. IDA has become the de-facto standard for the analysis of hostile code, vulnerability research and COTS validation. See this executive overview for a summary of its features and uses.

In addition to being a disassembler, IDA is also a powerful and versatile debugger. It supports multiple debugging targets and can handle remote applications via a "remote debugging server".

ICON KEY


Important Information

Quiz


CPTE Labs


Course Review

Lab Scenario

Virus, worms, or Trojans can erase your disk, send your credit card numbers and passwords to a stranger, or let others use your computer for illegal purposes like denial of service attacks. Hacker mercenaries view Instant Messaging clients as their personal banks because of the ease by which they can access your computer via the publicly open and interpretable standards.

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

Lab Resources

To run this lab you need the following:

- IDA Pro located on Desktop
- Run this tool on Windows 7
- Administrative privileges to run tools
- Web browser with Internet access

Lab Duration

Time: 15 Minutes

Lab Tasks

Note: The Windows 7 VM should be configured to allow the IDA demo to run. If it says the the demo is expired, change the date on your VM to approximately 1 year before. This can be done from a command prompt with the command **date 8/21/2014**

1. Go to **Windows 7** Virtual Machine.
2. Install IDA Pro, which is located on Desktop
3. Double-click the file called idaq64.exe. The IDA License window appears. Click I **Agree**.
4. Click the New button in the Welcome window.

Task 1

IDA Pro

Read the License Agreement carefully before accepting.

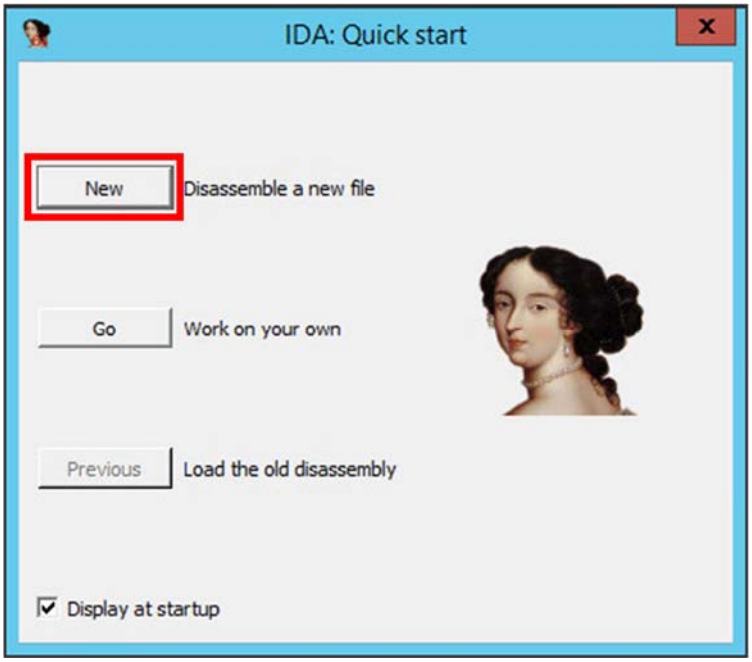


Figure: 2.1- IDA Pro Main Windows

5. A file browser window appears; select Desktop/face.exe

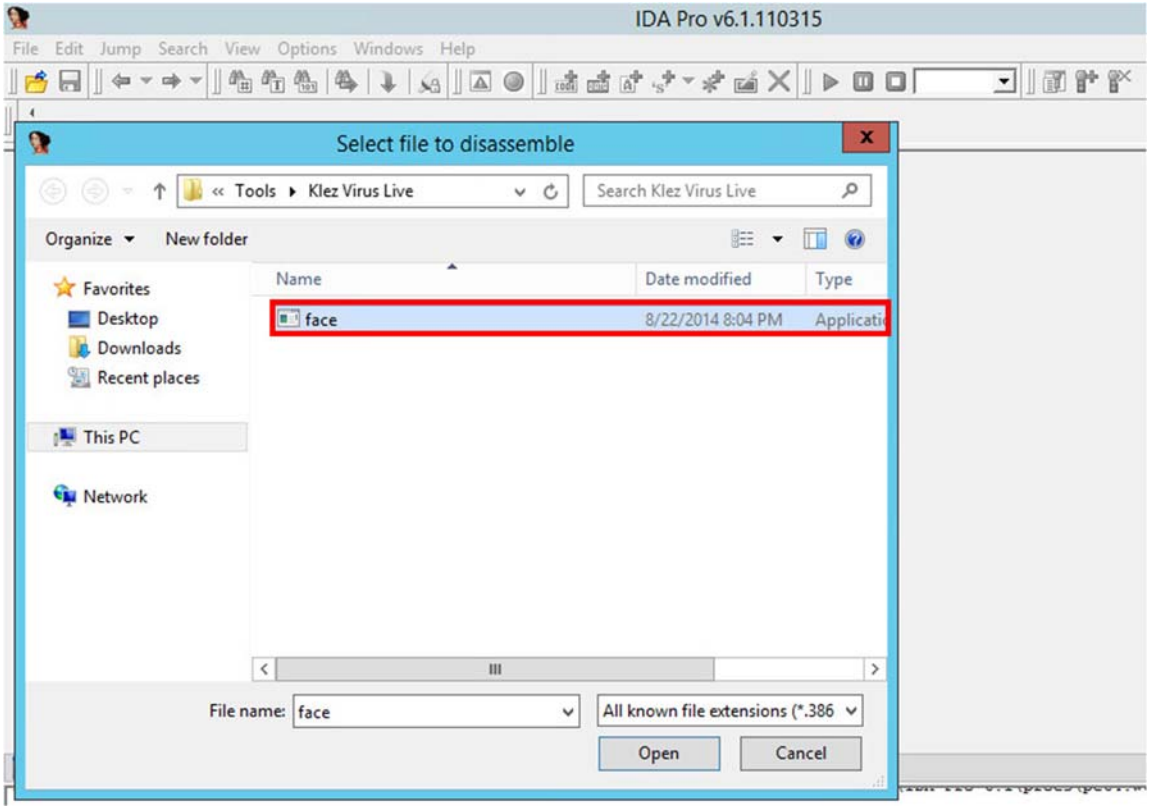


Figure: 2.2- IDA Pro File Browse Windows

6. The **Load a new file** window appears. Keep the default settings and click **OK**

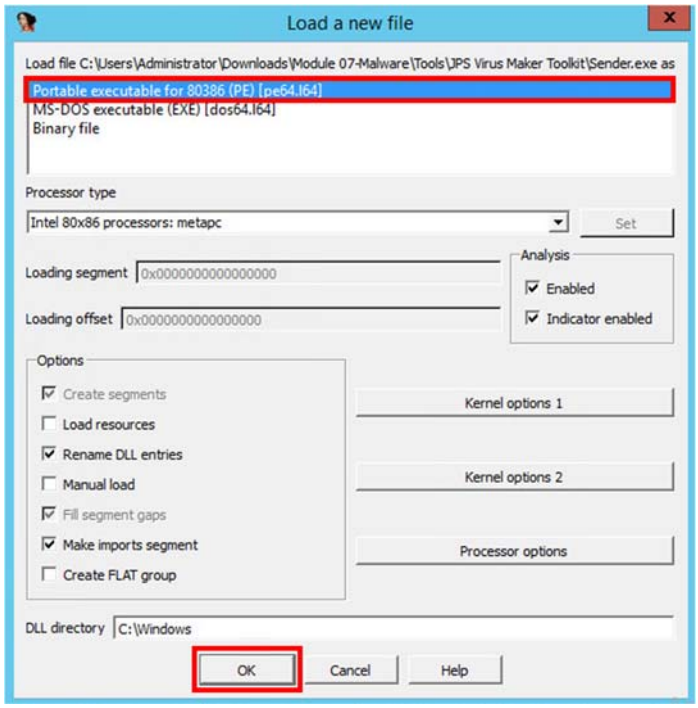


Figure: 2.3- IDA Pro Load a new file Window

7. If any warning window prompts appear, click **OK**.
8. The Please confirm window appears; read the instructions carefully and click **Yes**.
9. The final window appears after analysis.

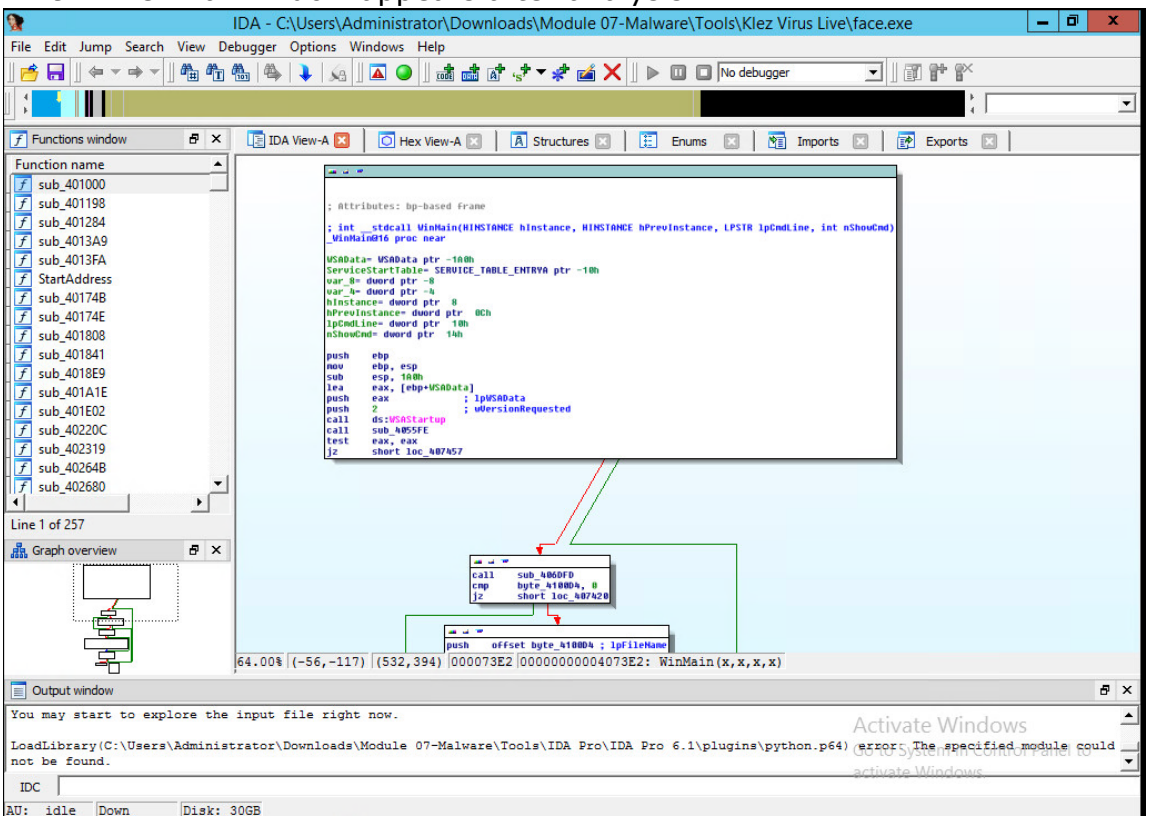


Figure: 2.4- IDA Pro windows after analysis

10.Click **View → Graphs → Flow Chart** from the menu bar

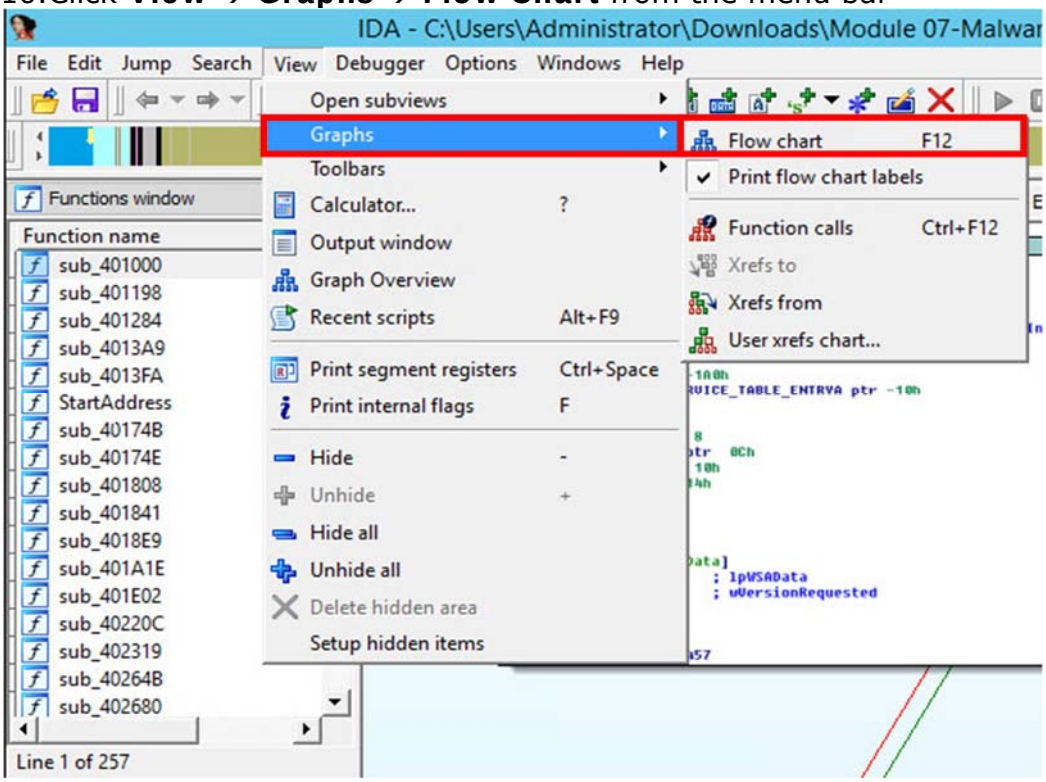


Figure: 2.5- IDA Pro flow chart menu

11.A Graph window appears with the flow; zoom to view clearly.

Zoom to have a better view the detail

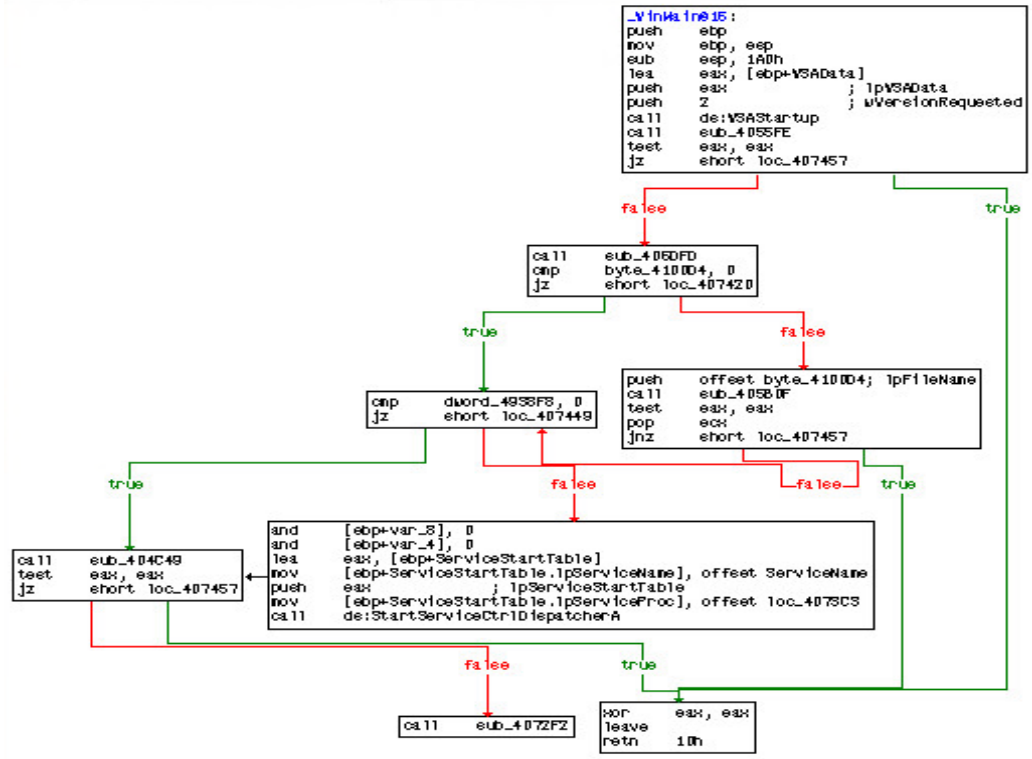
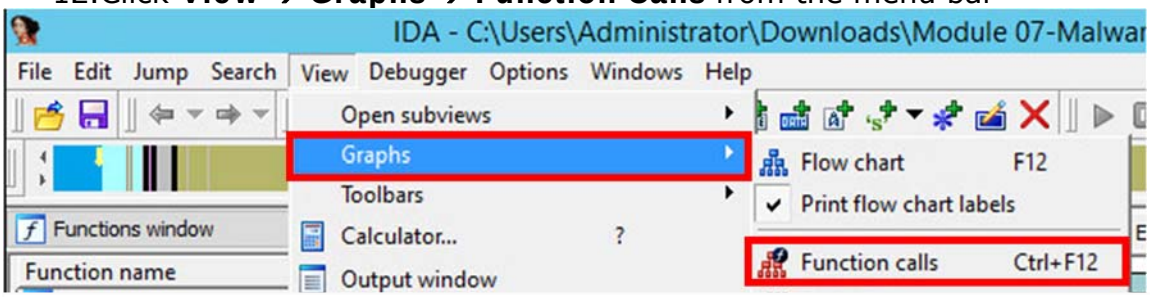


Figure: 2.5- IDA Pro flow chart

Note. You can scroll down to view all the flow charts

Empty input file
The input file doesn't contain any instructions or data. i.e. there is nothing to disassemble. Some file formats allow the situation when the file is not empty but it doesn't contain anything to disassemble. For example, COFF/OMF/EXE formats could contain a file header which just declares that there are no executable sections in the file.

12. Click **View → Graphs → Function Calls** from the menu bar



13. Click **Windows → Hex View-A**

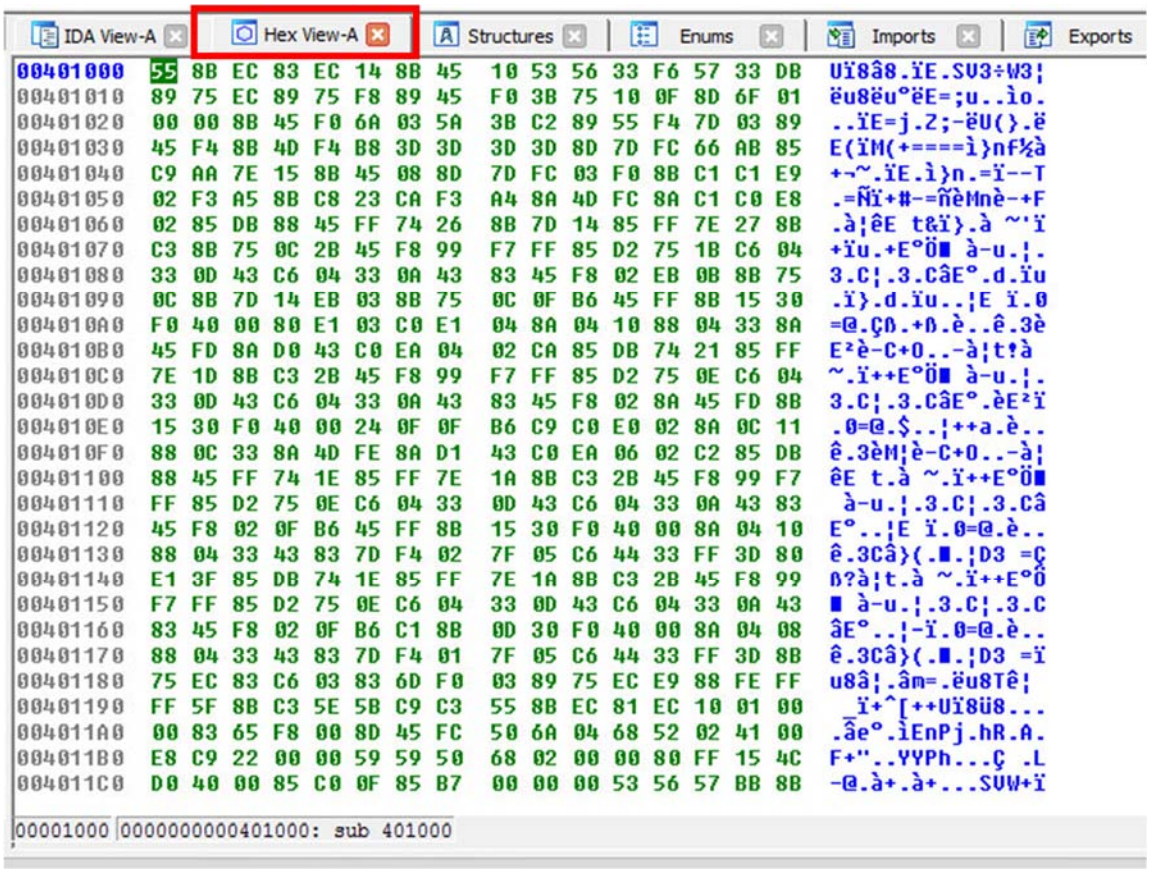


Figure: 2.7- IDA Pro Hex View-A Window

14. Click **Windows → Structures**. The following is a window showing **Structures** (to expand structures click Ctrl and +).

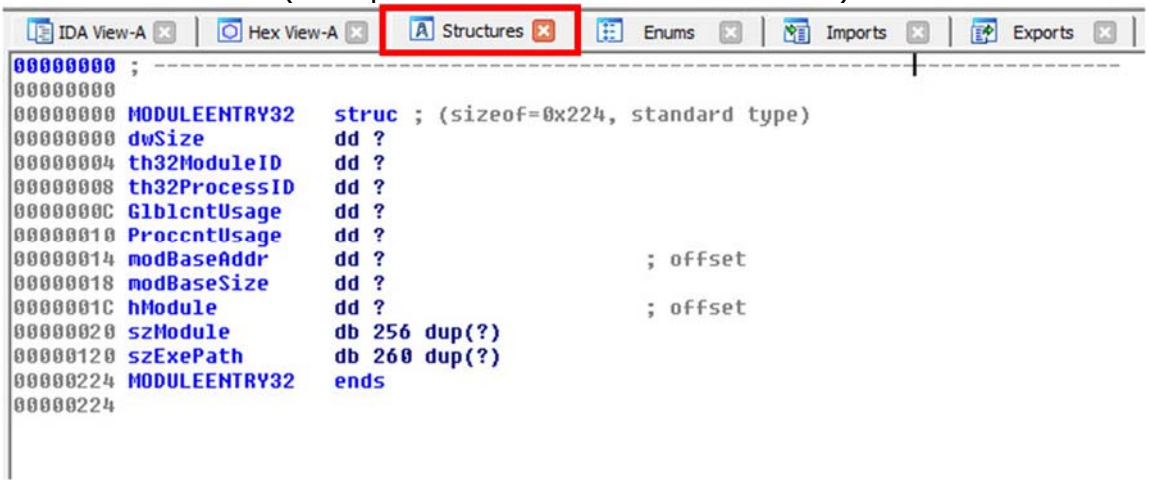


Figure: 2.5- IDA Pro Structures View Window

15. Click **Windows → Enums**

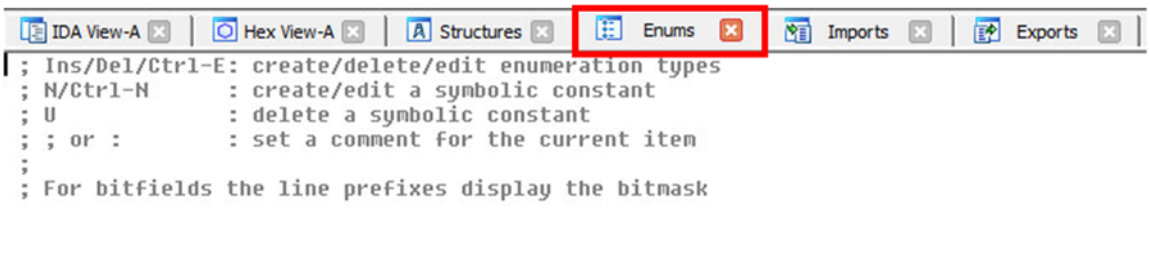


Figure: 2.7- IDA Pro Enum Window

16. Click **Windows → Structures**. The following is a window showing **Structures** (to expand structures click Ctrl and +).

Figure: 2.5- IDA Pro Structures View Window

Lab Analysis

Document all the results and reports gathered during the lab.

Tool / Utility	Information Collected / Objectives Achieved
IDA Pro	**File name :** face.exe **Output:** • View functional calls • Hex view-A • View structures • View enums

Quiz

1. Analyze the chart generated with the flow chart and function calls; try to find the possible defect that can be caused by the virus file.
2. Try to analyze more virus files generated by JPS Virus Maker Toolkit.