Malware Analysis
Fall 2015
Lab 09 - Packers and Unpacking

Please provide your scripts and unpacked binaries

Lab_09-1.malware

1. (1 pts) Is there a name for the packer used to protect this sample?

2. (3 pts) What is OEP?

3. (3 pts) What method did you use to find OEP?

Lab_09-2.malware

1. (2 pts) What are two indicators of this sample being packed?

2. (2 pts) What is this program packed with?

3. (2 pts) What is OEP?

4. (2 pts) What method did you use to find OEP?

5. (5 pts) Write a script (any language) to unpack this program.

6. (2 pts) Remove the nag screen and enable the secret menu item, briefly explain how you did it.

Lab_09-3.malware

1. (10 pts) How did you find OEP?

2. (5 pts) How did you resolve any PE header corruption?

3. (5 pts) How did you fix the import table?