

Lab 1: Malware Taxonomy

ITSC 303: Malware Analysis

**EVALUATION**:

|  |  |  |
| --- | --- | --- |
| Question 2.2 | 2pts |  |
| Question 2.3 | 3pts |  |
| Question 3.1 | 3pts |  |
| Question 3.2 | 1pt |  |
| Question 4.1.1 | 5pts |  |
| Question 4.1.2 | 4pts |  |
|  |  |  |
| TOTAL MARK | 18pts |  |

## 

## 2.2 Strings

Without going into detail about how strings are extracted from binaries, run SysInternals **strings.exe** command against the **calc.exe**.

### Question(s) - (2pts)

1. List 2 strings that you found in the sample calc.exe that would not be located in the file c:\windows\system32\calc.exe

**Answer:**

**SHELL32.dll** — Reference to the system shell library.

**msvcrt.dll** — Reference to the C runtime library used by calc.exe

## 2.3 Extraction

### Question(s) - (3pts)

Use windows Explorer to search for all the .pyd and .pyc files in the calc folder.

1. What type of content does the .pyc and .pyd files contain?
2. Are .pyc and .pyd files text files?
3. List 2 of these interesting files:
4. Do the names of these file indicate what the purpose of the file is intended to do?

## 3.1 Extracting Relevant Byte Code Files

### Question(s) - (3pts)

1. After extracting the contents of the .exe files, answer the following question(s).
   1. What are the names of the extracted files?
   2. What filetype(s) were recovered?
      1. An example of a filetype is .txt (for text files).
   3. Show a screenshot of the files extracted.

## 3.2 Decompiling Byte Code

### Question(s) - (1pt)

After decompiling the Byte Code

1. What is the output created by executing the uncompyle command?
2. Show a screenshot of the output.

### 4.1.1 Analyzing calc.exe

### Question(s) - (5pts)

1. Within the Evil Python class, what is the class variable referencing?
2. Describe what the \_\_init\_\_() method is doing. How would this malware be classified based on the presentation slide(s) discussed in class?
3. Describe what the steal\_hives method is doing. How would this malware be classified based on the presentation slide(s) discussed in class?
4. Describe what the steal\_files method is doing. How would this malware be classified based on the presentation slide(s) discussed in class?
5. What file extensions are being referenced by the re.match call?

### 4.1.2 Analyzing resume.pdf.exe

### Question(s) - (4pts)

1. What vulnerability is this malware exploiting?
2. Describe the get\_ips() method. For example:

What does it do? How does it accomplish the task? Does it require any special input?

1. What is being accomplished in the for loop when \_\_name\_\_ == ‘\_\_main\_\_’? How would this malware be classified based on the presentation slide(s) discussed in class?
2. Can you find ASCII strings in the exploit payload? (**Hint:** Look for the class variable value from calc.exe.) How would this malware be classified based on the presentation slide(s) discussed in class?

# Resources

Szor, P. (2005). *The art of computer virus research and defense*. Toronto: Addison-Wesley.