Lab - Delivering Malware

The goal of this lab is to get hands-on experience analyzing malicious office documents. While you can certainly use any analysis resources available, you do need to provide direct evidence from the macro code to support your analysis.

Password for the lab files: Fall2021!

Lab files:

*Sample 1:*

*MD5 (sample1.bin) = f23acd80b83b3bc1ea1503e94e1831f8  
 sample1.pcap*

*Sample 2:*

*MD5 (sample2.bin) = 8c6a5130470766c6c8f7098c1b907250*

*Sample 3:*

*MD5 (sample3.bin) = 1b0fbd5e0af361058a8115b941232e34*

*Sample 4:*

*MD5 (sample4.bin) = b107f3235057bb2b06283030be8f26e4*

For each sample, provide detailed analysis of the macros and any other supporting functionality to determine their purpose (that is, what did they do) and any key IOCs. Also, identify what type of malware the document was attempting to drop.

For each sample, provide additional answers per the guidance that follows:

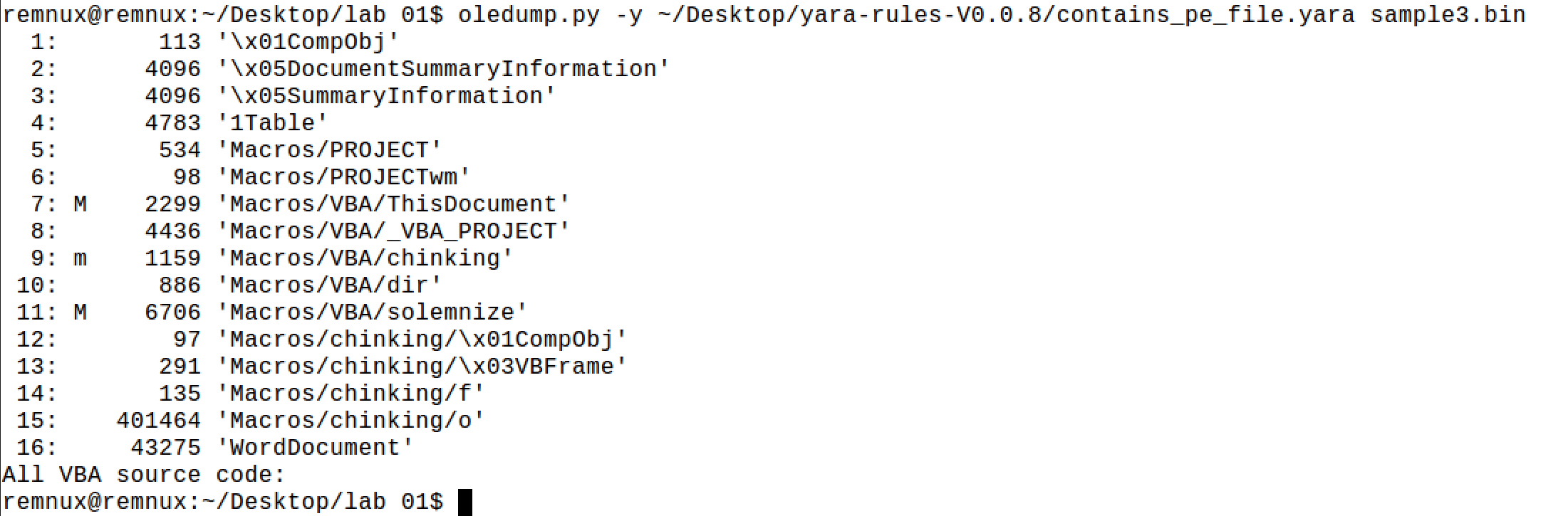
**Sample 1:**

1. This sample uses *certutil*, what is the purpose?
2. This sample executes a DLL, where is this stored or retrieved from?
3. What host does this maldoc attempt to retrieve a payload from? What type of malware is it attempting to drop?

**Sample 2:**

1. Nothing additional

**Sample 3:**

1. This document contains embedded content - demonstrate the usage of a Yara rule to detect a PE file in the document. Then describe why it was unable to find the embedded content.  
     
   

**Sample 4:**

1. Provide detailed analysis of how this document uses the Windows API and for what purpose.

**Deliverables**

Turn in a Word document (no macros) or PDF with your lab report.