LABS

**Lab 7-1**

Analyze the malware found in the file ***Lab07-01.exe*.**

Questions

1. How does this program ensure that it continues running (achieves persistence) when computer is restarted?
2. Why does the program use a mutex?
3. What is a good host-based signature to use for detecting this program?
4. What is a good network-based signature for detecting this malware?
5. What is the purpose of this program?
6. When will this program finish executing?

**Lab 7-2**

Analyze the malware found in the file ***Lab07-01.exe*.**

Questions

1. How does this program achieve persistence?
2. What is the purpose of this program?
3. When will the program finish executing?

**Lab 7-3**

Analyze the malware found in the file ***Lab07-03.exe*.**

**Lab 7-1 Solutions**

**Short Answers**

**Lab 7-2 Solutions**

**Short Answers**

1. This program only executes once. It does not persistence.
2. This program displays a webpage to the user.
3. Program exits after displaying the webpage.

Detailed Analysis

In basic static analysis, no string stands out to us. However, there is a one Unicode String that ***http://www.malwareanalysisbook.com/ad.html*** .We can also see the important import to the program.

**CoCreateInstance**

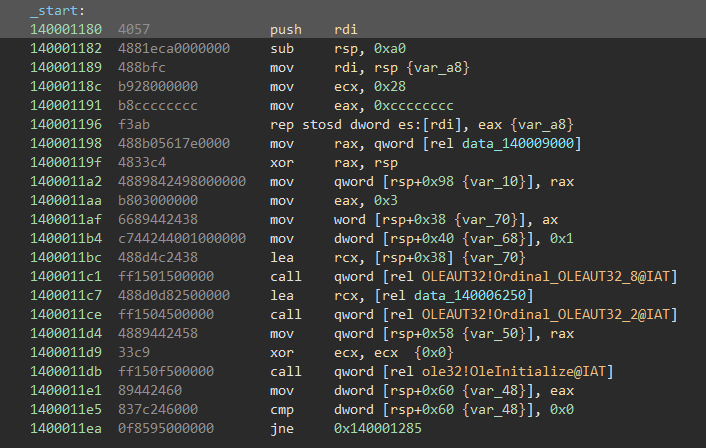
**OleInitialize**

**Oleuninitialize**

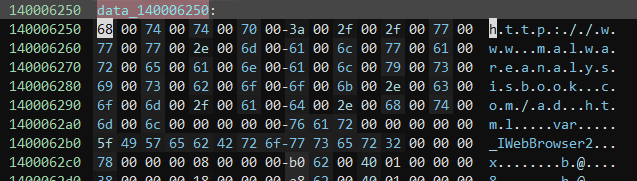
These functions are windows COM object related, ***CoCreateInstance*** and ***Oleinitealizw*** are particularly used in a Com object functionality.

In the Dynamic analysis, when it runs it opens internet browser in this case Internet Explorer and opens a webpage. There is no evidence of the program modifying the system to run on system restart.

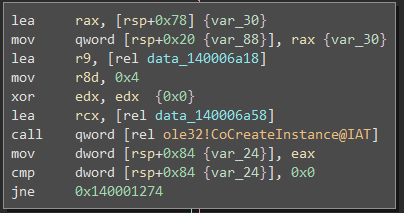
Now we can analyze the code in Binary Ninja. We go to the \_start method and we see the following disassembly.



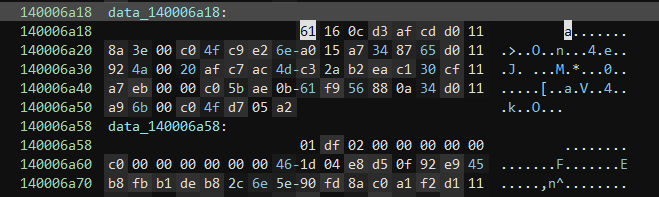
The first thing the malware does it to create a String that hold the URL that it will visit at the end of the program, The URL is stored at the address 0x140006250. Upon inspecting the address we can see the String ***http://www.malwareanalysisbook.com/ad.html*** . The malware initialize the COM object with use of OleInitialize.



If initialize successfully it will obtain a pointer to the COM object by running the CoCreateInstance and which is stored at the address of 1400062b0 (\_IWebBrowse2). The following picture show the disassembly graph of the sub routine.



To determine what COM functionality is being used, we need to examine the interface identifier (IID) and class identifier (CLSID). Clicking on the data\_140006a18 and data\_140006a58 we can identify *CLSID 0002DF01-0000-0000-C000-000000000046* and *IID D30C1661-CDAF-11D0-8A3E-00C04FC9E26E.*  To determine which program will be called, check the registry for the CLSID, or IID, the CLSID is for Internet Explorer and IID id for IWebBRowser2. The following image shows the IID and CLSID at their respective addresses.



After the call to Navigate, there are some cleanup function that are being called to before the program end. The program does not install itself for persistently and it does not modify the system. It simply displays a onetime advertisement.

**Lab 7-3 Solutions**

**Short Answers**