**Lab: Debugging**

**Overview**

The goal of this lab is to practice debugging. Debugging assembly is a skill that requires continuous practice; the more you practice, the more you become familiar with assembly blocks, and with different debugging techniques.

You are free to choose whatever debugging tool you like. You can try a couple of different tools to see which one works best for you.

Before you start looking at the details, I want to remind you some of the rules of reverse engineering by revisiting some of the things we discussed in the first lecture:

* Don’t get caught in details!
* You don’t need to understand 100% of the code
* Focus on key features

Please analyze the first two samples in the lab’s archive, which you can download from Canvas, and answer the following questions regarding the samples. You may want to use other tools in addition to a debugger, such as our basic static and dynamic analysis tools and IDA, to analyze the samples, and that is encouraged.

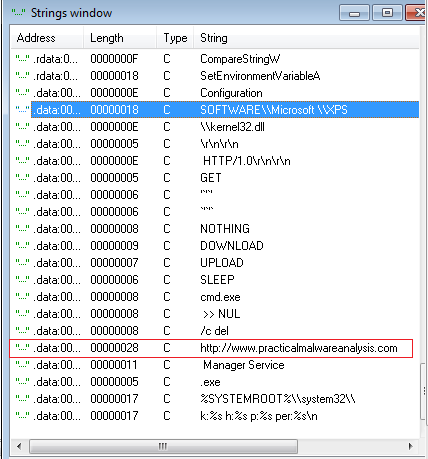
**\*\*\* Remember to snapshot your VM and double-check that it is on an isolated network (e.g. an “internal network” in VirtualBox) before loading any sample in a debugger! \*\*\***

**Sample 1:**

|  |
| --- |
| Q1-1. How can you get this malware to install itself?  ------------------------------------------------------------------------------  Just run the program without arguments, and then the file had gone. I think it is deleted itself.  I tried again with arguments like ‘-in aaaa’ after disabling password check function. But it seems like nothing happens and I am not sure it’s installed or not.    ------------------------------------------------------------------------------  Q1-2. What are the command-line options for this program? What is the password requirement?  ------------------------------------------------------------------------------  I can notice 4 arguments of this program. 00402AF0 is the address of a main function and if you go to the address, we can see the arguments operations.  -in  -re  -c  -cc    And the password is ‘abcd’ and it’s a bit hard to figure out the meaning of the codes.  First, it is comparing argument size with 4. If it’s not, it will jump to other address. If it’s 4, and then proceed.    This image is where code is comparing first 2 arguments. The first check is straightforward. It is comparing 61h ASCII code. The Second one is a little bit tricky, it is subtracting second one to first one and then it compares the value to 1. Since ‘a’ and ‘b’ is apart from each other by 1, so we can know it is trying to find ‘b’. The third and fourth character comparing is similar.      ------------------------------------------------------------------------------  Q1-3. How can you use OllyDbg to permanently patch this malware, so that it doesn’t require the special command-line password?  ------------------------------------------------------------------------------  At address 402510(which is a password check function), I changed assembly code to ‘MOV EAX,1 RET’ to return always 1.  Click right mouse button and choose ‘Binary -> Edit’. And you can edit binary value and put this binary value. ‘B8 01 00 00 00 C3’ which means that ‘MOV EAX,1 RET’  After editing, click right button again and choose ‘Copy to executable’ and you can save what you’ve changed so far.    ------------------------------------------------------------------------------  Q1-4. What are the host-based indicators of this malware?  ------------------------------------------------------------------------------  I thinks there are 2 indicators which show that it is a host-based malware.  When I look into the ‘Strings window’ of IDA, I can see ‘SOFTWARE/Microsoft/XPS’ and ‘%SYSTEMROOT%/system32’.  I think it is trying to do something on the victim computer.(Copying a file or making a registry key or something)    ------------------------------------------------------------------------------  Q1-5. What are the different actions this malware can be instructed to take via the network?  ------------------------------------------------------------------------------  I found several commands this malware could execute at address 402020.  SLEEP  UPLOAD  DOWNLOAD  CMD  NOTHING    ------------------------------------------------------------------------------  Q1-6. Are there any useful network-based signatures for this malware? |

------------------------------------------------------------------------------

‘http://www.practicalmalwareanalysis.com’



------------------------------------------------------------------------------