**Take Test: Homework4**

**QUESTION 1**

Lab Step 14:  What three files are added during execution of the malware?

C:\Windows\Prefetch\WINDOWS LIVE MESSENGER.EXE-5F1931EE.pf

C:\Windows\msnsettings.dat

C:\pas.txt

**QUESTION 2**

Lab Step 16:  What does the pas.txt file contain and what do you think its purpose is?

pas.txt contains victim’s logon credentials, such as username and password. Its purpose is hackers use them to hack victim’s Windows Live Messenger.

msnsettings.dat contains an exe file named msnmsgr.ex and its purpose is trying to get something during the login, configuration.

**QUESTION 3**

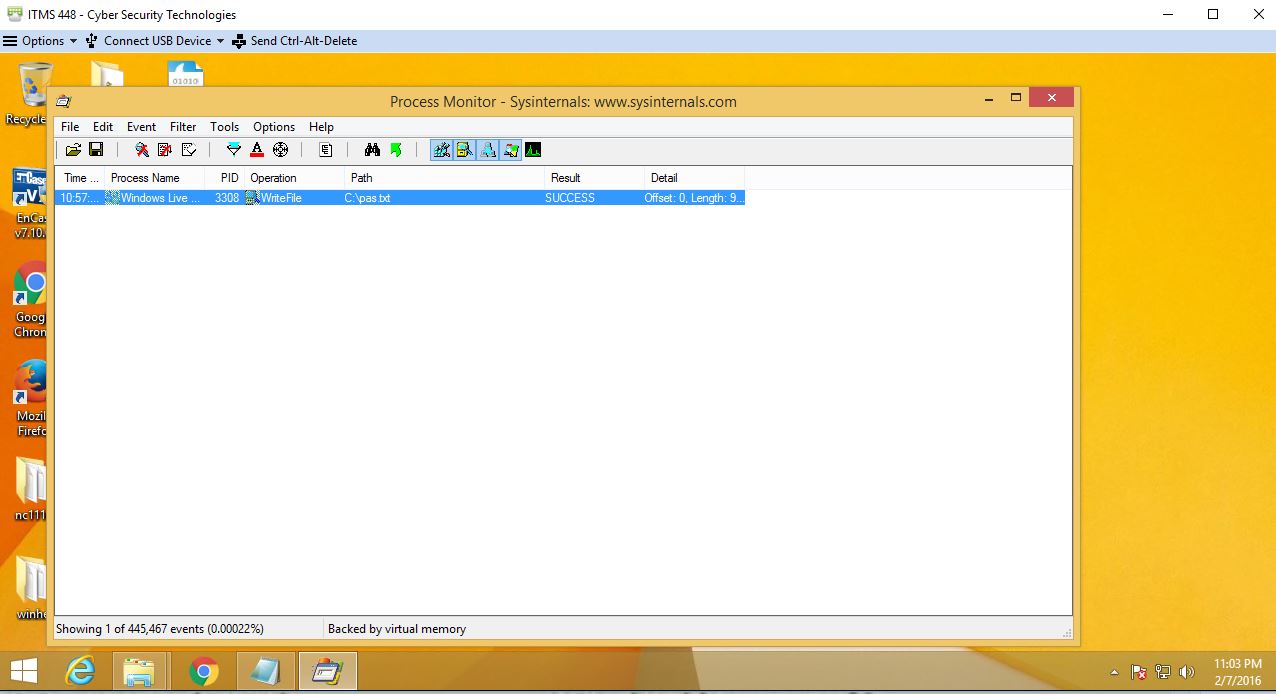
Lab Step 19:  What are the main differences between the msnsettings file that the malware placed after execution and the msnsettings file from the CFO's computer?

The malware add something in it. In this case, the first difference is the first line. It changed from "hello" to "test."

The second difference happened after executing msnmsgr.exe. Adding things are gsmtp185.google.com and mastercleanex@gmail.com.

**QUESTION 4**

Lab Step 30:  Upload a screenshot of Procmon after the completion of step 29.



**QUESTION 5**

Lab Step 37:  What is the name of the service that uses port 25 and what does that service do?

The server is PracticalMalwareAnalysis.com which uses Port 25 for SMTP to send out some information, maybe emails.

**QUESTION 6**

Lab Step 38:  After you hit "Sign In" in the malware, what is the malware trying to do based on the traffic you see in FakeNet going out on port 25?  What information is being sent and by what means?

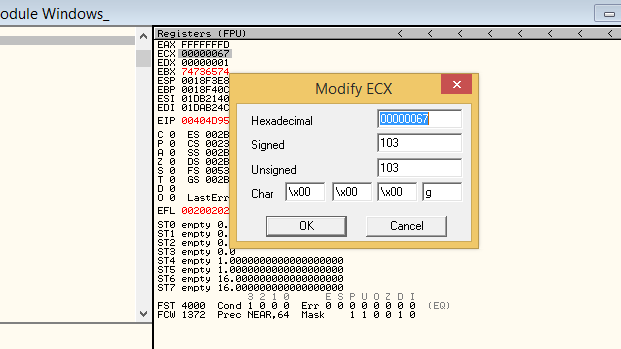
The malware is trying to collect the user's email address and password after the user hit "Sign In" in the malware.

Then, the malware mail the information from yourpassword@password.com to mastercleanex@gmail.com.

**QUESTION 7**

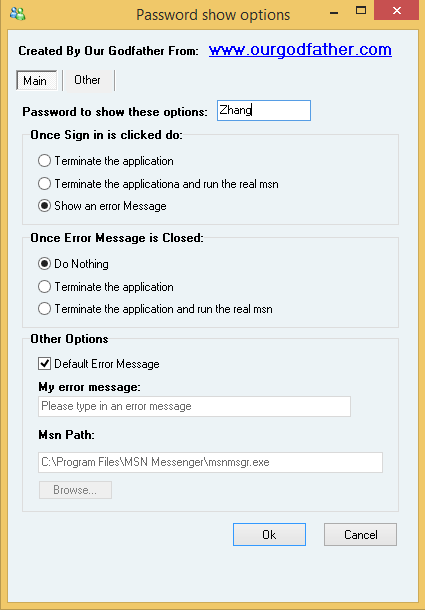
\*\*Extra Credit Question:

Lab Step 62:  Upload the image file of the Modify ECX window showing "g" as the last character from the prior step to answer this question.



**QUESTION 8**

Lab Step 69:  In the secret menu, change the "Password to show these options" value to your last name.  Then, using the Windows snipping tool from the Windows 8 VM, take a screen capture of only the secret menu showing your last name in the XP VM and save it.  Upload that image file to answer this question.



**QUESTION 9**

Lab Step 70:  Your boss would like to know the results of your analysis of this malware.  Write a 1 to 1.5 page 12pt font double spaced report letting her know of your findings.  Your report should be uploaded in either .doc, .docx, orpdf format.  Be sure to include an introduction, all of the main facts from your analysis, and a conclusion.

**QUESTION 10**

Lab Step 71:  Your boss would like to know how users can determine if they are using the real Windows Live Messenger application or this malicious version.  Explain how users could tell the difference.

If you could not enter your Windows Live Messenger after logging in your account, it must be a malware. The malicious version will show some error message and tell you could not enter your account after you submit the “Sign in” button. When you tried to quit this application, the malware will attempt to connect to a website and may perform an additional redirect to a malicious page. You may see fakeAV, a notice that your java is out of data, VMware Flash Optimizer, etc.

**QUESTION 11**

An isolated analysis environment for testing malware is optional most of the time.

 True

 False

### QUESTION 12

1. What does RegShot do?

|  |  |  |
| --- | --- | --- |
|  |  | Deletes registry keys. |
|  |  | Alters registry keys. |
|  |  | Can be used to take a snapshot of the Windows registry and compare it against a later snapshot to look for any changes that may have occurred. |
|  |  | Can be used to take a snapshot of the Windows RAM and compare it against a later snapshot to look for any changes that may have occurred. |

### QUESTION 13

1. What type of file was Laine.lora from the lecture?

|  |  |  |
| --- | --- | --- |
|  |  | A keylogger. |
|  |  | A rootkit. |
|  |  | Ransomware |
|  |  | A compressed archive containing three files. |

### QUESTION 14

1. What is the main difference between static and dynamic malware analysis?

It is if execute the malware or not. Static analysis will evaluate the executable without executing it but dynamic analysis will evaluate the executable during execution.