LAB3
Xiaoyi Zhou

Lab3-1
Q1: What are this malware's imports and strings?
The file is packed by the format PENinja. The only import we can see is Kernal32.dll->Exitprocess.

C:\> Strings Lab03-01.exe
StubPath
SOFTWAREÄClassesÄhttpÄshellÄopenÄcommandV
SoftwareÄMicrosoftÄActive SetupÄInstalled ComponentsÄ
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWAREÄMicrosoftÄWindowsÄCurrentVersionÄRun
SOFTWAREÄMicrosoftÄWindowsÄCurrentVersionÄExplorerÄShell Folders
AppData

Q2: What are the malware's host-based indicators?
By using Window process explorer, we noticed that "\BaseNamedObjects\WinVMX32" which means the malware create a mutex WinVMX32. We are still interested in how does the malware effect the system. So we can investigate the process monitor and then apply the filter. Here we should realize that RegSetValue and
WriteFile will show the modification made on filesystem and registry. We checked the registry first, we noticed that there are 9 same entries "software\microsoft\cryptogtaphy\RNG\seed", but there was one obviously different entry " software\microsoft\Windows\currentversion\run\vediodriver", the data entry showed windows\system32\vmx32to64.exe. The rest of 9 entries will generate random number and write those numbers to registry. I think the purpose of those 9 entries is to mess up the registry.
Clearly, the register has been changed and written a new entry. The malware run the vmx32to64.exe on the location at Windows\System32. We scan the vmx32to64.exe on Virustotal, we notice that it is identical file with Lab03-01.exe by comparing the MD5 (d537acb8f56a1ce206bc35cf8ff959c0). Therefore, we can make the conclusion that the malware change the registry and copy it self once it is launched. By the way, we can find wmx32to64 at Window process explorer.

Q3: Are there any useful network-based signatures for this malware? If so, what are they?
We can check the network-based signature by check the DLL files at window process explorer. The DLL files like ws2_32.dll and wshtcpip.dll indicate the network function. Moreover, we can check the ApateDNS, the malware is trying to access to

"www.practicalmalwareanalysis.com" after it launched. The Wireshark indicated that the packet was 256 bytes. And the malware used port 443 as source port, 1199 as destination port.

Lab3-2

Q1: How can you get this malware to install itself?
We looked up the export table at PEview first and we found few entries. Install, Servieceman, installA, uninstallA. In this case we can try for both Install an installA. Since installA pairs unistallA, so I assume installA is the command for installation.
We checked the strings as following:
C:\ Documents and Settings\Administration>Strings Lab03-02.dll
There are a lot of strings but we can find something useful, such as IPRIP (the starting service), RegOpenValue, Systemroot\system32\svchost,exe -k netsvcs(really important!the host indication!), Intranet Network Awareness<INA+>, practicalmalwareanalysis.com(network indication).

Q2: How would you get this malware to run after installation?
C:\net start IPRIP
The Intranet Network Awareness (INA+) service is starting.
The Intranet Network Awareness (INA+) service was started successfully.

Q3: How can you find the process under which this malware is running?
Back to question one, "Systemroot\system32\svchost.exe" is the indication. So we checked each svchost.exe at Process Explorer by using DLL panel view. Once we found the Lab03-02.dll entry, we found the process we need.
The svchost.exe with PID 1112 had the Lab03-02.dll.

Q4: Which filters could you set in order to use ProComm to glean information?
We should apply the PID1112 first.
Then we could apply operations such as "RegSetValue" or "WriteFile". The registry has been changed a lot. But in order to view the difference, we should use Regshot to compare the registry. We took the first snapshot before we get everything done, and we took the second snapshot after we install the malware. Then we can compare them. See question five. We focused on key added and value added.
At "key added" filed, we found HKLM\SYSTEM\ControlSet001\Servie\IPRIP
This entry proved that the malware is executed by service IPRIP.
At the "value added filed", we found many entries related to IPRIP, such as HKLM\SYSTEM\ControlSet001\Servie\IPRIP\Parameters\ServiceDll:"C:\Documents and Settings\Administration\Lab03-02.dll", which means the malware has been installed at the host.

Q5: What are the malware's host-based indicators?
In the result of comparison at Regshot, we make sure that the malware was installed. And the Systemroot\system32\svchost.exe is also the host-based indicator.

Q6: Are there any useful network-based signatures for this malware?

We checked the ApateDNA, the malware send request to practicalmalwareanalysis.com. The wireshark told us the packet is 414bytes. Moreover, by using the Wireshark capture, we can learn that the malware was using port 80 as source port and 1128 as destination port.
Based on this lab and the lab03-01, we should set the network analyzer listen on port 80 and 443 since they are the two ports that pose a significant threat to the network.

Lab3-3
Q1: What do you notice when monitoring this malware with Process Explorer?
After I run the Lab03-03.exe file, I notice that it create another process named svchost.exe with PID196, then exit itself quickly. Normally we can see that svchost.exe is under the tree structure of service.exe while the special svchost.exe is not. So we can examine that file for future steps. And I didn't close the file folder of BinaryCollection\Chapter_3L. I also notice that a new log file emerges. The new log file is practicalmalwareanalysis.log. (And it keep updating itself when I was going through the file)

Q2: Can you identity any live memory modification?
Based on the question above, we can examine the PID196 process with process monitor. Since the malware has written new file, the memory should be modified. I found the operations like Writefile, RegQueryValue, RegOpenkey and etc. So the malware definitely changed the registry. We can also check the "memory" under the String tab at Window process explorer. A lot of thing has changed. The content in "memory" option and "image" option are totally different.

Q3: What are the malware's host based indicators?
C:\WINDOWS\System32\svchost.exe file
practicalmalwareanalysis.log file.

Q4: What is the purpose of this program?
I opened the file when I noticed the existence of the file at first place. The file was almost empty (not empty actually. But there were only few words). While I keep doing my work, open the log file again, I found the file has been updated. I keep testing it by doing some simple things, for example I browsed the Internet and just typed the keyboard. The next time I opened the log file, I knew it is a keylogger malware. Moreover, when we examined the memory at String tab, we can noticed that it has alphabet from lowercase a to uppercase Z, which also imply that the malware is a keylogger.

Lab3-4
Q1: What happens when you run this file?
When I run the file, the file exited itself after few seconds. And I tried to run the file using command line, but it still failed to show me any information. So I used PEview and Virustotal to scan the file, I assume that this malware is a downloader. It might download another malware program and upload it via network. The PEview showed the network-based indicator such as http://www.practicalmalwareanalysis.com.

Q2: What is causing the roadblock in dynamic analysis?
The malware disappear at Window process explorer. Therefore, we cannot gain more information from analyzing the detail process. But we can still find it at process monitor. Since the file exit automatically, and it might be a downloader, we apply the filter using the key words like"exit", "delete", "off", "upload", "create", "value", ""and etc. But I didn't find anything valuable. At the end I found the command line to launch the malware at Process Start, and the commend line to delete itself at Process Create.

Q3: Are there other ways to run this program?
The command line doesn't work so far. So I guess we might need to apply another software to dissect and slow down the process when the malware is running, so we can clearly see it by step and step.