CMPSC 443 Lab: Malware Analysis 1

Lab Description

Student name:

Preparation

Start VM

Click Windows “Start” ➔ type “Ollydbg” ➔ start the Windows VM (if it is the first time using it, it may perform a new installation, which will take a while).
This Windows VM will be used in later labs. However, since the lab uses VM player that does not have the snapshot feature. We will not be able to take snapshots, and revert the VM to previous state. Therefore, we will NOT analyze those nasty malware that causes vital damage to the system. That being said, most malware we play with can be safely removed from the system.

Tools

Download and install the following tools in the VM for basic static analysis

- PEstudio – another good tool to collect information from PE files http://www.softpedia.com/get/Programming/Other-Programming-Files/PeStudio.shtml
- PEview: https://www.aldeid.com/wiki/PEView
- PEid: https://www.aldeid.com/wiki/PEiD
- resource hacker: http://angusj.com/resourcehacker/
- Dependency walker: http://www.softpedia.com/get/System/File-Management/Dependency-Walker.shtml

Resource

Common Windows functions reference – available on Canvas.

Tasks

For the given four malware samples, you need to answer a set of questions with **basic static analysis techniques**. Your answers should be concise.

Sample Lab01-01.exe (in-class demo)

1. Upload the files to http://www.VirusTotal.com/ and view the reports. Does either file match any existing antivirus signatures?
2. When were these files compiled?
3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?
4. Do any imports hint at what this malware does? If so, which imports are they?
5. Are there any other files or host-based indicators that you could look for on infected systems?
6. What network-based indicators could be used to find this malware on infected machines?
7. What would you guess is the purpose of these files?

Task 1 - Sample Lab01-02.exe

1. Upload the Lab01-02.exe file to http://www.VirusTotal.com/ . Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?

Task 2 - Sample Lab01-03.exe

1. Upload the Lab01-03.exe file to http://www.VirusTotal.com/ . Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?

Task 3 - Sample Lab01-04.exe

1. Upload the Lab01-04.exe file to http://www.VirusTotal.com/ . Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.
3. When was this program compiled?
4. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
5. What host- or network-based indicators could be used to identify this malware on infected machines?
6. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

Submission

- Put all your answers into a single pdf or word file.