Computer Science 491/691
Malware Analysis
Homework 1
Assigned: February 4, 2019
Due: February 11, 2019

Name: Sai Sasaank Srivatsa Pallerla
ID: HG13015

How to turn this in for grading: You can edit your answers right into this file. Email it to the TAs as (will be) described in class. Make sure your name appears in the body of the document. Give to us with a name of the form LastnameFirstname.HW1.word.

Download and extract hw1.7z on a virtual machine. The password to the zip file is "infected", without the quotes. The file contains hw1_1.infected and hw1_2.infected, which are malware samples. **Do NOT run them!**

Hint: Chapter 1 and Appendix A of your Practical Malware Analysis textbook are very useful references! Other parts of your textbook may be helpful as well!

## Part 1: hw1_1.infected

**1) What is the MD5 of hw1.7z? What is the MD5 of hw1_1.infected?**
MD5 of hw1.7z – 777b0dc4b07bc3db3084dc4dc4da0d4b215
MD5 of hw1_1.infected – 0d07363187dcda999e1a6e750ed7a57a

**2) How many antivirus engines on VirusTotal detect the file hw1_1.infected as malicious?**
55/69 engines detected the file hw1_1.infected as malacious

**3) When was hw1_1.infected compiled? How did you find this information?**
Compilation TimeStamp – 2017:07:04 19:19:53 +1:00
PMA describes that the PE file Header has information such as Imports, Exports, Time Date Stamp, Sections, Resources. When the file is uploaded into virustotal.com TimeStamp can be found in Exif File Tool Metadata.

**4) Investigate the Windows API functions that hw1_1.infected imports. List two functions that suggest that hw1_1.infected can check whether it is being debugged.**

1. IsDebuggerPresent - Determines whether the calling process is being debugged by a user-mode debugger.
2. OutputDebugStringW – Send a string to the debugger to display.
3. FlushInstructionCache – Flushes the instruction cache for the specified process.

**6a) List any string in hw1_1.infected that appears to be a file name.**
Output.111742493.txt
Loader.exe
98nHU.sys

**6b) List any string in hw1_1.infected that appears to be a domain name.**
cn.bing.com

**6c) One of the strings in hw1_1.infected is a registry key that is commonly used to give malware persistence. What is this string?**
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Run

**6d) List any string in hw1_1.infected that appears to be a user agent.**
User agent: Mozilla/5.0 <Windows NT 6.3; Trident/7.0; rv:11.0> like Gecko

**6e) List any string in hw2_1.infected that appears to be a Program Database (pdb) string.**
C:\User\W?\Downloads\kur\Redir\Bin\main_64.pdb

**Part 2: hw1_2.infected**

**1) What is the MD5 of hw1_2.infected?**
MD5 - 70a2fd5bd44482de36790309079fd9ac

**2) How many antivirus engines on VirusTotal detect the hw1_2.infected as malicious?**
55/69 antivirus engines on Virustotal detected the hw1_2.infected as malicious.

**3) Describe three features of hw1_2.infected that indicate that it is packed. What packer was used to pack hw1_2.infected?**

1. Virtual Size: 90112 and the Raw size is 0 – indicator of packing
2. Total of only 5 imports (unusual) - low number of imports is an indicator of packing.
3. Entropy of UPX1 is 7.87 – Entropy > 7 is an indicator of packing

Packer Pack: UPX 0.89.6 – 1.02 / 1.05 – 2.90 -> Markus & Laszlo

**4) Unpack hw1_2.infected. Describe how you unpacked it. What is the md5 of the unpacked file?**
Download UPX from upx.sourceforge.net
Copy the .exe file and hw1_2.infected to C drive
To run the .exe file use upx.exe command in command prompt
To unpack the file use upx -d hw1_2.infected.
MD5 of the unpacked file: b6d5449653396a74b9bcffd00b28a9fe

**5) How many resources are contained within hw1_2.infected? One of these resources is suspicious - do your own analysis and describe why it is.**
There are three resources in hw1_2.infected, the third resources looks suspicious because it is very long when compared to the first two resources, when inspecting the file using resource hacker you see number of windows API and lastly it is an executable code.

**Extra Credit:**

**Investigate the Windows API functions that hw1_1.infected imports. A combination of the imported functions suggests that the malware can perform a certain covert malware launching technique. What is the name of this technique? List all of the imports that suggest the malware can perform it.**
Name of the Covert Malware launching Technique: *Process Injection*

- VirtualAllocEx
- WriteProcessMemory
- LoadLibrary
- CreateToolhelp32Snapshot
- Process32First
- Process32Next
- OpenProcess
- CreateRemoteThread
- WriteProcessMemory