Xin Yang
xy213

Report of Homework 5

Lab06-01.exe

1. The only subroutine sub_401000 calls InternetGetConnectedState to get the web connection status, then set eax to 1 if it's connected or 0 if not. Also, it will call sub_40105F write the result message like "Success: Internet Connection\n" or "Error 1.1: No Internet\n" into a file. It's an if structure.
2. This subroutine calls _stbuf and _ftbuf, and sub_401282, which is used to initialize and flush the buffer for print, based on the contents of sub_401282, we can infer it's a printf function.
3. The main function is trying to get into a sub_401000 function, which will return 1 if connected to the Internet, and return 1 if not connected to the Internet, and write the corresponding message into a file. Then taking the returned value from sub_401000, the main would return the same result.

Lab06-02.exe

1. The first subroutine called by main is sub_401000. What it does is the same as the one in Lab06-01.exe: return the Internet status as 1 if connected, 0 if not and write the message into file.
2. 0x40117F did the same thing as the sub_40105F in the previous file. It calls _stbuf and _ftbuf, and calls sub_4013A2, which is a printf.
3. It's sub_401040. In this subroutine, it will first open an URL http://www.practicalmalwareanalysis.com/cc.htm with User-agent as Internet Explorer 7.5/pma. If failed to open the URL or failed to read file or failed to get the command, it will call sub_40117F to write the error message and set al register to 0. There are multiple if branches in this subroutine.
4. This subroutine opens the webpage and calls InternetReadFile to read the webpage, then compare the contents with "<!—", to extract the comment of html.
5. There are two network-based indicators, one is the url of "http://www.practicalmalwareanalysis.com/cc.htm", another is the user-agent, which is "Internet Explorer 7.5/pma".
6. This malware first will determine whether the machine is connected to the Internet, if connected, try to download the webpage and read it. If successfully opened, it will compare the buffer with "<!--", which is the beginning part of comments of html, then print the extracted information as "Success: Parsed command is %c\n", and at last it would sleep for 60000 milliseconds, which is 1 minute.

Lab06-03.exe

1. The sub_401130 is new in this malware's main function.
2. It takes a char variable and a string variable. By tracing back, we can find the char variable is the extracted information from the opened url. The string variable stores the argv, which is the name of the malware.
3. The basic structure is a switch sentence, along with the jump cases.
4. This function can take actions according to the command extracted from the url. It can print error messages, create a directory, copy file, delete file, set a key in the registry, or set the program to sleep for 100 seconds.

5. There is a directory “C:\\Temp\\cc.exe” and a registry location “Software\Microsoft\Windows\CurrentVersion\Run”.
6. This program will first check the Internet status, and try to open and download the webpage same as in the previous one, and extract the commands in the comment, then take actions according to the exact instruction, including set a registry key, create a directory, copy a file, delete a file, sleep for 100 seconds and print the error messages.

Lab06-04.exe

1. The sub_401000 is to check the Internet status, sub_401040 is to download and extract the information in the url, sub_4012B5 is the printf function, sub_401050 contains the switch cases.
2. There is a for loop in the main function, where [ebp + var_C] is the flag variable. This variable will be initialized at first and checked at the beginning of each loop, then be added one at the end of the loop.
3. This malware uses the %d to pass an argument into the string “Internet Explorer 7.50/pma%d”, then calls the _sprintf function
4. This program will run at least 1440 minutes because it will run 1440 rounds defined by the comparison of [ebp + var_C] with 1440, and in each round it will sleep for 60 seconds if successfully parsed the contents in the comment.
5. The network-based indicators are similar to the previous one. It has a User-agent “Internet Explorer 7.50/pma%d” and the url “http://www.practicalmalwareanalysis.com/cc.htm”. The difference is that here the user agent will contain the minutes that this program has been running as an argument.
6. This malware will similarly check the Internet status, then try to download and extract the information hidden in the html comment, then goes into a loop which will loop 1440 times, and each time will sleep for 60s, and pass the round number as argument and send as user-agent. This loop will take actions according to the information extracted from comment including set a registry key, create a directory, copy a file, delete a file, sleep for 100 seconds and print the error messages.