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 or file io, here we have a file pointer, and based on the contents of sub\_401282, we can infer it’s basically a write into file operation.
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 does file writing operations.
3. It’s sub\_401040. In this subroutine, it will first open an URL ﻿<http://www.practicalmalwareanalysis.com/cc.htm> using agent of 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. If successfully opened, it will compare the buffer with “<!--”, which is the beginning part of comments of html, if yes, then put [ebp+var\_20C] into al and return.
4. There are multiple if branches in this subroutine.