LAB 3

IDA Pro Analysis

Under the direction of
Dr. Samuel Liles

Table of Contents

Abstract

This lab is focused on introducing IDA Pro Analysis Tool and getting familiar with it. The lab is going to use the application to do dynamic analysis of the malware while being isolated from the internet. The Practical Lab 5.1 will be carried out to answer the questions provided.

The Computer Anti-virus was disabled as part of the instructions to enable the download and extract of the files being used. This lab is intended to lay grounds for further labs in the course.

Keywords: IDA Pro, Digital Investigation, Forensic Evidence, Malware Analysis.

Lab 3 Lab 3 IDA Pro Analysis

Steps of the process

Preparing the LAB

The Computer was rebooted, anti-virus was disabled, and the appropriate files were downloaded. Different Images of VM were installed. Installation of different windows environment such as XP, 7 and 8.1. Programs needed have been downloaded and snapshots of the process have been taken.

LAB 5-1

Applications & Tools

The following application was used to forensically examine the files. The following descriptions have been captured from the developer's website and manuals.

IDA is the Interactive DisAssembler: the world's smartest and most feature-full disassembler, which many software security specialists are familiar with (Hex-Rays SA, 2014).

Issues or problems

No Issues or problems were encountered.

Conclusions

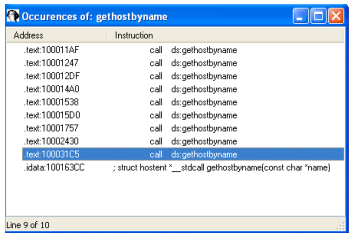
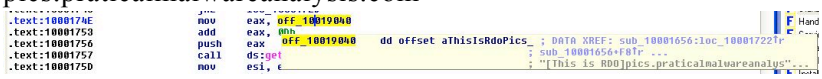
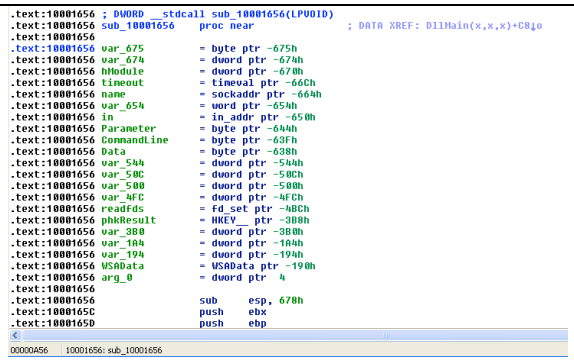
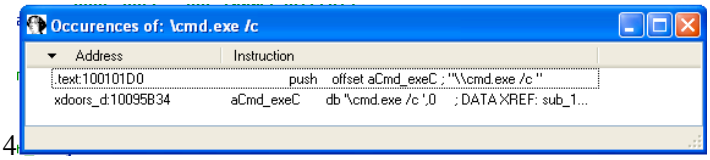
The Lab identified how IDA Pro could be used to help explore the malwares. The tool showed binary information about the malware studied.

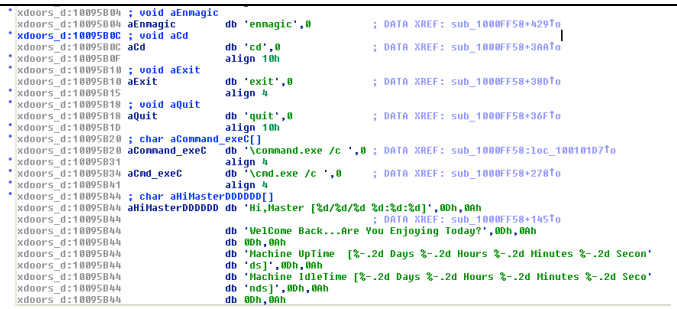
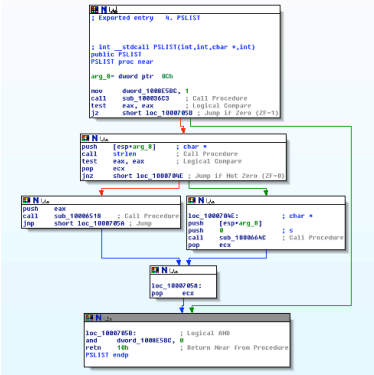
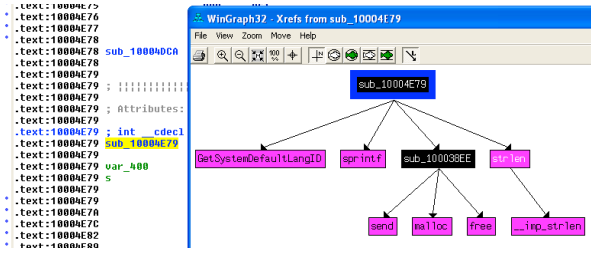
Case studies

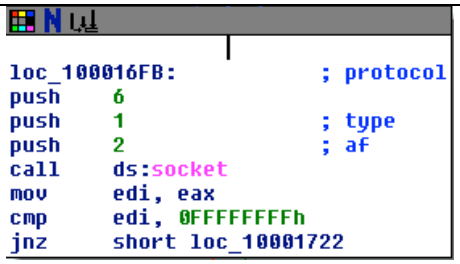
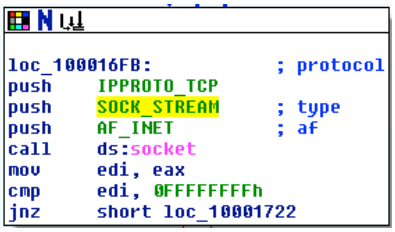
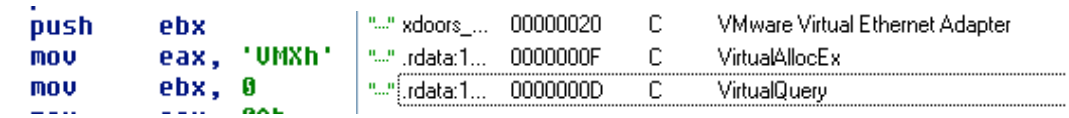
No Case studies was given with this lab.

Review questions

Lab 5-1

Answers	Lab05-01.EXE
1	Location is in .text:1000D02E .text:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)
2	Location is in.idata:100163CC
3	Using Find we get 10 results one of which is the actual function which means there are 9 calls for the function gethostbyname as shown in the graph bellow 
4	As shown in the image the DNS request will call for pics.praticalmalwareanalysis.com 
5	21 variables have been found 
6	There is only 1 argument in the function which is arg_0 as shown in the graph above
7	It was found in two locations .text:100101D0 & xdoors_d:10095B34 
8	It looks like it creates a command line session and greeting the person with Hi, Master and providing information about the PC upTime and idleTime.

	
9	It gets the OS version using GetVersionExA
10	If it was successful it will provide the WorkTime/s for the command shell created for the remote user.
11	The pList provides two different results as shown by the tree structure in the graph both provide information about a single service/process that is running or all that is running. 
12	I would name it GetSysLang 
13	On the first level it calls the following function, strncpy, _strnicmp, CreateThread & strlen. On the 2nd level it calls, the following functions are examples and not all functions being called; WinExec, Sleep, gethostbyname, inet_addr,atoi, inet_ntoa, connect,memset,send,socket,GetTickCount,recv,CloseHandle,memcmp,GetProcAddress, LoadLibraryA.
14	Backtracking both variables atoi & off_10019020 we get 30 * 1000 = 30,000 milliseconds = 30 seconds of sleep
15	The three parameters are 6,1,& 2

	
16	The three parameters are IPRoto_TCP, SOCK_Stream, AF_INET as shown in the graph 
17	Yes there are several strings available that are related to VMware as shown in the graphs bellow. 
18	Data that has no meaning and cannot be understood! However it could be encrypted!
19	No python add on was available
20	Right Click and Selecting 'S' will show the following info .data:1001D988 a1UUU7461Yu2u10 db '-1::',27h,'u<&u!=<&u746>1::',27h,'yu&!',27h,'<;2u106:101u3:',27h,'u'
21	Could not run the program since no python available

References

Hex-Rays SA. (2014, July). *Freeware Download Page*. Retrieved from https://www.hex-rays.com/index.shtml