LAB 1

Practical Malware Analysis

Purdue University
Due Date : 27/08/2014
CNIT 58100 CFM

Under the direction of
Dr. Samuel Liles

Table of Contents

Abstract

In this lab is focused on intruducing new tools and getting familiar with it. The lab is going to use mainly https://www.virustotal.com website that provides scan reports to uploaded files, URLs, and Searches. The Practical exam Lab 1.1 to Lab 1.4 will be carried out to answer the quastions provided.

The Computer Anti-viruse 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: Virustotal, Digital Investigation, Forensic Evidence, Malware Analysis.

Android Acquisition and Analysis

Steps of the process

Preparing the LAB

The Computer was reboated, anti-viruse was diabled, the appropriate files were downloaded.

LAB 1-1

The device was identified as Galaxy S III, and was inspected physically to note down inputs and output of the system. From Figure 1 the following inputs was noted (Pringle, Jbott, & Alex, 2013):

Applications & Tools

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

FTK® Imager,"is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as AccessData® Forensic Toolkit® (FTK) is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence"(AccessData, 2012).

Autopsy®,"is an open source digital investigation tools (a.k.a. digital forensic tools) that run on Windows, Linux, OS X, and other Unix systems. They can be used to analyze disk images and perform in-depth analysis of file systems (such as NTFS, FAT, HFS+, Ext3, and UFS) and several volume system types”(SleuthKit, 2003).

Logical Inspection

The device should be connected via USB and with running FTK Imager a Forensic Image is acquired by stream copying the physical memory. That image is then imported into Autopsy for examination. This is necessary to preserve the evidence and to be able to go back and prove the process or proof the results.

Forensic Examination

The Image was loaded and the following 27 volumes were found as shown in figure 3. In sequence all directories have been expanded and examined for user created files of interests and the following was found.

Issues or problems

when uploading the original file PracticalMalwareAnalysis-Labs.7z to https://www.virustotal.com the following Trojan was reported Trojan.Win32.Siggen4.cypnws

Conclusions

Evidence of stocking and misbehavior such as drug dealing has been found using the images and text massages in the Table 1. A female target with brown hair, white skin, young age has been identified in several pictures some of which has been deleted. A car that could be related to the victim has also been sighted in several pictures including one from the suspect car tailing it. Most events have been established on the last week of August 2013. Text massages found are abusive in nature and could be used to further investigate the suspect on several accounts.

Case studies

No Case studies was given with this lab.

Review questions

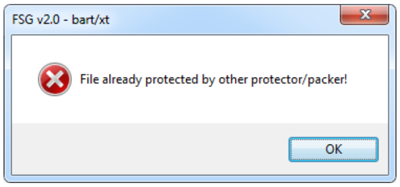
Lab 1-1

Answers	Lab01-01.exe	Lab01-01.dll
1	Yes, Trojan.Rogue	Only one Anti-viruse reported : WS.Reputation.1
2	2010-12-19 16:16:19	2010-12-19 16:16:38
3	Yes , exe extention	Yes, Dll Extention
4	It has MSVCRT.dll That uses the C++ Library	MSVCRT.dll uses C++ Library while WS2_32.dll is used for communcation
5	Linked to Kernal32 which provideds create/copy functinalities	
6	an ip address 127.26.152.13	
7	Copy files and probebly use the network to send it. However, the network address is private. Could be an aggregator point for gathering infomraiton and another module routes it out of the network !?	

Lab 1-2

Answers	Lab01-02.exe
1	Yes, Artemis
2	Packed using UPX and by downloading it and running the UPX -d command the file was unpacked and rescanned
3	ADVAPI32.dll, is used to create services, KERNEL32.DLL, is used to utilize the CPU and create proccesses and threads, WININET.dll is used for internet communicaitons.
4	http//www.malwareanalysisbook.com is a link that was found uding the PEviewer.

Lab 1-3

Answers	Lab01-03.exe
1	Yes, Trojan.ADH
2	No it was protected by the packer  FSG v2.0 - bart/xt File already protected by other protector/packer!
3	KERNEL32.dll was used but not so many functionallities have been listed when using the total
4	Nothing could be seen running PEid or the Resource Hacker

Lab 1-4

Answers	Lab01-04.exe
1	Yes, Downloader
2	Nothing shows that the file has been packed
3	2019-08-30 22:26:59 which is in the future as virustotal website analysis shows.
4	ADVAPI32.dll, affect and change privilages in tokens, KERNEL32.dll, creates /copy/write and excute files
5	Using the PeView System32\wupdmgr.exe was found within the texts under the main section for the file. http://www.practicalmalwareamalysis.com/updater.exe was also found under the Section.rsrc
6	Using virustotal website and scanning the resource extracted urlmon.dll which downloads the file from a URL and KERNEL32.dll which provides the path and executes the file.

References

AccessData. (2012, 03 21). *User Guide.* Retrieved 02 18, 2014, from AccessData: http://marketing.accessdata.com/acton/attachment/4390/f-000d/1/-/-/-/-/file.pdf

Pringle, Jbott, & Alex. (2013). *Battle of the Smartphones*. Retrieved 02 18, 2014, from New Jersey Institute of Technology: http://webdesign.njit.edu/winners/2013/cat2/410/index.php?p=specifications

Samsung. (2013). *GALAXY S III (16GB)*. Retrieved 02 18, 2014, from Samsung: http://www.samsung.com/hk_en/consumer/mobile/mobile-phones/smartphone/GT-I9300MBDTGY-spec

SleuthKit. (2003). *Home*. Retrieved 02 18, 2014, from SleuthKit: http://www.sleuthkit.org/index.php