Library for Static Analysis of PE Malware

by Katja Hahn

Master Thesis

HTWK Leipzig

Fakultät Informatik, Mathematik und Naturwissenschaften

First Assessor: Prof. Dr. rer. nat. habil. Michael Frank (HTWK Leipzig)
Second Assessor: Max Mustermann

Leipzig, September 2014

Contents

List of Figures

List of Tables

List of Acronyms

DLL dynamic-link library
DRV legacy system driver

EXE executable

FON font

PE Portable Executable

SYS real mode device driver

VM Virtual Machine

Chapter 1

Introduction

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.

At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum. sanctus sea sed takimata ut vero voluptua. est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat.

Consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus.

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo

Chapter 2

Malware Taxonomy

2.1 Behavioural Malware Types

Usually malware analysts make guesses about the malware's behaviour and shape their further analysis to confirm (or refute) these guesses. This approach helps to speed up the analysis. [2, p. 3] Hereafter is an overview to the different types of malware depending on its behaviour.

Definition 1 (Downloader) *A* downloader *is a piece of software that downloads other malicious programs. (cf. [2, p. 3])*

Definition 2 (Rootkit) *A* rootkit *is a software that has the purpose of hiding the presence of other malicious programs or activities. (cf. [2, p. 4])*

A rootkit may conceal login activities, log files and processes. Rootkits are often coupled with backdoor functionality (see definition 3).

Definition 3 (Backdoor) *A* backdoor *allows access to the system by circumventing the usual access protection mechanisms. (cf. [2, p. 3])*

The backdoor is used by the attacker or other malicious programs to get access to the system later on.

Definition 4 (Launcher) *A* launcher *is a software that executes other malicious programs. (cf. [2, p. 4])*

A launcher mostly uses unusual techniques for running the malicious program in the hopes of providing stealth.

Definition 5 (Spam-sending malware) Spam-sending malware *uses the victim's machine to send spam. (cf. [2, p. 4])*

Attackers use this kind of malware to sell their spam-sending services.

Definition 6 (Information stealer) *An* information stealer *is a malicous program that reads confidential data from the victim's computer and sends it to the attacker. (cf. [2, p. 4])*

Examples for information stealers are: keyloggers, sniffers, password hash grabbers [2, p. 3] and also some kinds of deceptive malware. The latter makes the user input confidential data by convincing the user that it provides an advantage. An example for a deceptive information stealer is a program that claims to add more money to the user's Paypal account; actually it sends the Paypal credentials the user puts into the program to the attacker's e-mail server.

Definition 7 (Botnet) *A* botnet *is a collection computer programs on different machines that recieve and execute instructions from a single server.*

While some botnets are used legally, malicious botnets are installed without consent of the computer's owners and may be used to perform distributed denial of service attacks or for spam-sending (see definition 5).

Definition 8 (Scareware) Scareware *tries to trick a user into buying something by frightening him. (cf. [2, p. 4])*

A typical scareware example is a program that looks like an antivirus scanner and shows the user fake warnings about malicious code found on the system. It tells the user to buy a certain software in order to remove the malicious code.

Definition 9 (Virus) *A* virus *recursively replicates itself by infecting or replacing other programs or modifying references to these programs to point to the virus code instead. A virus possibly mutates itself with new generations. (cf. [4, p. 27, 36])*

A typical virus is executed if the user executes an infected host file.

Definition 10 (Worm) *"*Worms *are network viruses, primarily replicating on networks." [4, p. 36]*

Typically worms don't need a host file and execute themselves without the need of user interaction. [4, p. 36] But there are exceptions from that: e. g. worms that spread by mailing themselves need user interaction. A worm is a subclass of a virus by definition 10.

2.2 Mass Malware and Targeted Malware

Malware is not only classified by behaviour, but also by the attacker's goals. If the malware was designed to infect as many machines as possible, it is a *mass malware*. A *targeted malware* on the other hand was written to infect a certain machine, organization or company.

Chapter 3

Detection by Antivirus Software

Chapter 4

Malware Hiding Techniques

Chapter 5

Malware Analysis

Definition 11 "Malware analysis *is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it." [2, p. xxviii]*

5.1 Malware Analysis Techniques

Static Analysis

Definition 12 Static analysis *is the examination of a program without running it. [2, p. 2]*

Static analysis includes e. g. viewing the file format information, finding strings or patterns of byte sequences, disassembling the program and subsequent examination of the intructions.

Dynamic Analysis

Definition 13 Dynamic analysis *is the examination of a program while running it. [2, p. 2]*

Dynamic analysis includes e. g. observing the program's behaviour in a Virtual Machine (VM) or a dedicated testing machine or examining the program in a debugger.

Chapter 6

Portable Executable Format

The Portable Executable (PE) is a file format for executables and object files used by Microsoft products. Some examples for PE file types are dynamic-link library (DLL), font (FON), legacy system driver (DRV), real mode device driver (SYS) and EXE files.

PortEx extracts the information from the PE format to assist in analysing malware. Therefore knowledge about the PE format is neccessary to understand the inner workings of the library PortEx.

The PE format is described in the *Microsoft Portable Executable and Common Object File Format Specification* [3]

6.1 General Structure

Figure 6.1 illustrates the structure of a PE file. An executable PE file always starts with the MS-DOS Stub. This is an application which is able to run in MS-DOS. The standard MS-DOS stub prints the message "This program cannot be run in DOS mode" and closes right after.

To determine if a file is of a certain file format, signatures are used. The file format signature is usually at the very beginning of the file. Since the PE starts with the MS-DOS stub, which has a file signature itself, the PE signature is placed after. The offset to the PE signature is defined in location 0x3c of the stub, thus enables Windows to properly execute the PE file.

MZ, PE00

Right after the signature follow the COFF File Header, the Optional Header and the Section Table. The COFF File Header contains information about the type of the target machine, the number of sections, a time date stamp that indicates when the file was created, the size of the Optional Header.and flags that indicate file characteristics.

Despite its name the Optional Header is mandatory for image files.Only object files don't need it.

The Section Table describes i. a. characteristics, size, name and location of the sections that make up the rest of the PE file.

make your own picture

6.2 Special Sections

Sections may contain arbitrary information, which is only relevant to the application using them; but some sections have a special meaning. Their format is described in the PE COFF specification [3]. These sections are recognized by entries in the Data Directory Table of the Optional Header. They have typical section names which are also used in the specification to refer to the sections. These names are not mandatory, but a convention. That's why they can not be relied on while trying to find certain sections.

Some of these special sections are described right after.

Import Section

The import section contains data about the

Resource Section

Debug Section

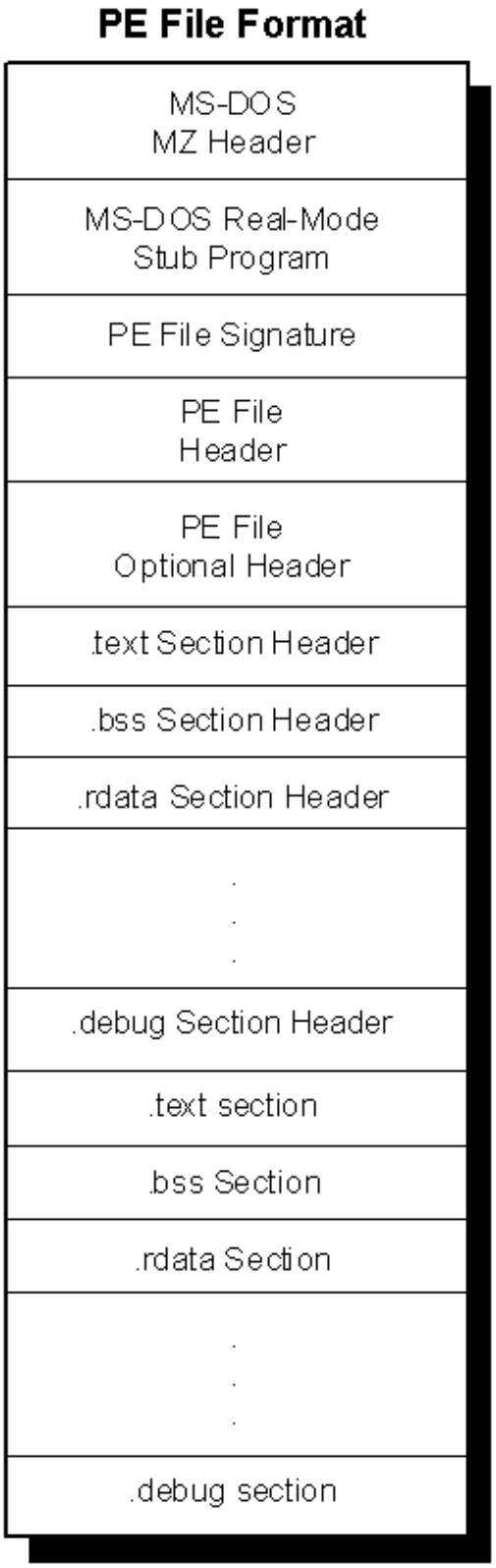

Figure 6.1: Structure of a PE file [1]

Chapter 7

Static Analysis Library

Chapter 8

Evaluation

Chapter 9

Das Competence Information Portal

soll mit Hilfe eines Berichtssystems erleichtert werden. Dazu gehört die Möglichkeit, Mitarbeiter

remove

Bibliography

[1] Kath, Randy: *The Portable Executable File Format from Top to Bottom*. http://www.csn.ul.ie/~caolan/publink/winresdump/winresdump/doc/pefile2.html, 2013.

[2] Michael Sikorski, Andrew Honig: *Practical Malware Analysis*. No Starch Press, Inc., 2012.

[3] Microsoft Cooperation: *Microsoft PE and COFF specification*. http://msdn.microsoft.com/library/windows/hardware/gg463125, 2013.

[4] Szor, Peter: *The Art of Computer Virus Research and Defense*. Addison Wesley Professional, February 2005.

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig, ohne Hilfe Dritter verfasst habe, dass ich keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und Zitate kenntlich gemacht habe. Diese Arbeit ist bislang keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht worden.

Leipzig, den _____ _____

Unterschrift