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 ii

List of Tables iii

List of Acronyms v

1 Introduction 1

2 Malware Taxonomy 4

3 Detection by Antivirus Software 6

4 Malware Hiding Techniques 7

5 Malware Analysis 8
5.1 Malware Analysis Techniques 8

6 Static Analysis Library 9

7 Evaluation 10

8 Das Competence Information Portal 11

Bibliography 13

List of Figures

List of Tables

List of Acronyms

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

Malware is grouped into different types depending on its behaviour. 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. [1, p. 3]

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

Definition 2 (Rootkit) Rootkit

Definition 3 (Backdoor) *A* backdoor *allows access to the system by circumventing the usual access protection mechanisms. (cf. [1, 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. [1, p. 4])*

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

Definition 5 (Spam-sending malware) *A* spam-sending malware *uses the victim's machine to send spam. (cf. [1, 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. [1, p. 4])*

Examples for information stealers are: keyloggers, sniffers, password hash grabbers [1, p. 3] and also deceptive malware, which makes the user input confidential data by convincing the user that it provides an advantage. An example for the latter 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) botnet

Definition 8 Scareware *tries to make the user pay or buy something by frightening him. (cf. [1, p. 4])*

Definition 9 (Virus) *A* virus *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. [2, p. 27, 36])*

Definition 10 (Worm) worm

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.

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." [1, p. xxviii]*

5.1 Malware Analysis Techniques

Static Analysis

Definition 12 Static analysis *is the examination of a program without running it. [1, 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. [1, 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

Static Analysis Library

Chapter 7

Evaluation

Chapter 8

Das Competence Information Portal

soll mit Hilfe eines Berichtssystems erleichtert werden. Dazu gehört die Möglichkeit, Mitarbeiter inklusive ihrer Fähigkeiten, Standorte und Lebensläufe zu suchen. Führungskräfte können so geeignete Kandidaten finden, um interne Stellen zu besetzen. *Arbeitsnahe und -integrierte Maßnahmen zur Kompetenzentwicklung* werden indirekt unterstützt, indem der Bedarf ermittelt und die Planung realisiert werden kann.


remove

Bibliography

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

[2] 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