Universitatea POLITEHNICA din București

Facultatea de Automatică și Calculatoare,
Catedra de Calculatoare

LUCRARE DE DIPLOMĂ

Analiza aplicaţiilor de tip malware

Conducător Științific:
As.dr.ing. Laura Gheorghe

Autor:
Cristian Condurache

București, 2013

University POLITEHNICA of Bucharest

Automatic Control and Computers Faculty,
Computer Science and Engineering Department

BACHELOR THESIS

Malware Analysis

Scientific Adviser:
As.dr.ing. Laura Gheorghe

Author:
Cristian Condurache

Bucharest, 2013

Maecenas elementum venenatis dui, sit amet vehicula ipsum molestie vitae. Sed porttitor urna vel ipsum tincidunt venenatis. Aenean adipiscing porttitor nibh a ultricies. Curabitur vehicula semper lacus a rutrum.

Quisque ac feugiat libero. Fusce dui tortor, luctus a convallis sed, lacinia sed ligula. Integer arcu metus, lacinia vitae posuere ut, tempor ut ante.

Abstract

Malware is currently a major security threat for computers and smartphones, with efforts being taken into improving malware detectors with behavior-based detection. In order to classify applications, malware detectors need some form of malicios behavior specification which are usually identified manually by researchers. We present a Linux implementation of the malspec-mining algorithm which automates this process. This algorithm recognizes such specifications by comparing known malicious and benign applications. The output consists of behavior patterns, which are specific to the inputted malware and that do not occur in benign applications.

Keywords: behavior-based detection; malspec-mining algorithm; malicious behavior; kernel programming

Contents

List of Figures

List of Tables

Chapter 1

Introduction

From large corporations to the average user, computer and network environment security is an important necessity to which malware is a threat. Malware, or malicious software, is software programmed and used by attackers in order to gain access to private computers, to obtain sensitive information or to simply disrupt normal computer operation.

Currently, malware written for Windows operating systems are more common than those written for Linux. Considering that operating systems which are based on the Linux kernel, such as Android, are are becoming more wide-spread, we can assume that attackers might change their target. This supports the need for developing better tools for Linux malware analysts and improving malware detection methods.

Appendix A

Project Build System Makefiles

A.1 Makefile.test

```
# Makefile containing targets specific to testing

TEST_CASE_SPEC_FILE=full_test_spec.odt
API_COVERAGE_FILE=api_coverage.csv
REQUIREMENTS_COVERAGE_FILE=requirements_coverage.csv
TEST_REPORT_FILE=test_report.odt


# Test Case Specification targets

.PHONY: full_spec
full_spec: $(TEST_CASE_SPEC_FILE)
        @echo
        @echo "Generated␣full␣Test␣Case␣Specification␣into␣\"$^\""
        @echo "Please␣remove␣manually␣the␣generated␣file."

.PHONY: $(TEST_CASE_SPEC_FILE)
$(TEST_CASE_SPEC_FILE):
        $(TEST_ROOT)/common/tools/generate_all_spec.py --format=odt
            -o $@ $(TEST_ROOT)/functional-tests $(TEST_ROOT)/
            performance-tests $(TEST_ROOT)/robustness-tests
#


# ...
```

Listing A.1: Testing Targets Makefile (Makefile.test)

Bibliography