BABEŞ BOLYAI UNIVERSITY, CLUJ NAPOCA, ROMÂNIA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
SPECIALIZATION COMPUTER SCIENCE IN GERMAN

Cloud based malicious PDF Detection using Machine Learning

– Diploma thesis –

Author
Viorel GURDIS

2020

Abstract

Text of abstract. Short info about: project relevance/importance, inteligent methods used for solving, data involved in the numerical experiments; conclude by the the results obtained.

Contents

List of Tables

List of Figures

List of Algorithms

Chapter 1

Introduction

1.1 Context

1.2 Motivation

1.3 Paper structure and original contributions

Chapter 2

Scientific Problem

2.1 Problem definition

2.2 Background processes in Microsoft Windows

2.3 Filesystem monitoring

2.4 Analyzing PDF File Structure

2.5 Machine Learning for Malware Detection

2.6 Benefits of Cloud Computing

Chapter 3

Related work

3.1 Cloud based malware detection

3.2 Machine Learning for detecting malicious PDF

Chapter 4

Proposed approach

4.1 Dataset

4.2 Proof of Concept

4.2.1 Feature Extraction

4.2.2 Classification Techniques

4.2.3 Performance Evaluation

4.2.4 Experiment

4.3 Used technologies

4.3.1 Microsoft .NET Framework

4.3.2 PDF Tools and Metasploit Framework

4.3.3 Python Flask

4.3.4 Scikit-learn Machine Learning Library

4.3.5 ReactJS Framework

Chapter 5

Application

5.1 Design

5.2 Windows Service

5.3 Cloud API

5.4 Dashboard Interface

Chapter 6

Conclusion and future work

Bibliography