

Malware Meta Crawler for MASS

MA-INF 3309 - Malware Analysis
Lab Report
Winter Semester 2016.17
University of Bonn

Ehab Qadah

April 21, 2017

Table of Contents

1	Introduction.....	3
2	Related Work + foundation	3
3	System Overview	3
4	System Implementation.....	3
5	Evaluation performance + number of samples	3
6	Conclusion + future work.....	3

Abstract. On a daily basis, new malware samples are discovered in. This makes the software vulnerabilities analysis one of the top concerns for organizations. The automatic identification of vulnerable software inside the organization is fundamental to avoid cyber-attacks. In this paper, we discuss two techniques to automatically monitor software vulnerabilities using open standards and public vulnerability information repositories, and alternative method to identify a vulnerable software using information obtained from social media platforms.

1 Introduction

state general introduction about the malware analysis and need for the crawler, motivation of topic.

brief overview of the report structure.

2 Related Work + foundation

- about mass - general overview of malware analysis - other people work - mal-trieve -Raypicker - malware resource were used
- foundation like tool were used python + mass apiclient

3 System Overview

- idea +problem - formal algorithmic description - process flow diagram or any sort of charts

4 System Implementation

- how the idea + problem is realized + code snippet - not code docs

5 Evaluation performance + number of samples

- state what do you like to find and how? - state performance metric like time, memory usage, etc. - environment setup - present the results - conclude findings

6 Conclusion + future work

- briefly sumup what was include/done -state the overall achievement -state the future work

References

1. Symantec. Internet Security Threat Report, Vol. 21 <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>, 2016.