Malware Meta Crawler for MASS

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

Ehab Qadah

April 25, 2017

Table of Contents

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

In last decade, the usage of the Internet has increased and adopted all sectors of business and industry as result of the digital revolution. On the other hand, the wide usage of Internet creates a new opportunities for Cyber criminals to perform their malicious activities such as information theft and espionage. Malicious Software (malware) is a common way to perform cyber attacks that can be in different forms such as worm, virus, Trojan and spyware [1]. According to Symantec, in 2015, 431 million of new malwares were discovered [2], which means over one million per day. To protect the Internet's users the malware researchers community try hardly to study these malwares, in order to build the counter measures and detect the new malware software or their malicious behavior, using different malware analysis techniques like static or dynamic analysis of malware samples [3].

In this work, we provide malware crawler that contentiously retrieve new malware samples (e.g., malware domains, URLs and binary files) from different on-line sources and repositories , and submit them to MASS server to build a comprehensive database of malicious software, to make the malware samples continuously available in one place, which helps the malware researchers in their studies.

The remainder of this report is organized as follows. In Section 2, we present the related work and fundamental background . Section 3 presents the general system overview. In Section 4 we give the implementation details. Section 5 provides the evaluation results. And finally, Section 6 gives the overall conclusion and future work.

2 Related Work + foundation

- about mass - general overview of malware analysis - other people work - maltrieve -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 perfomance 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 - measure the difference time between submission time between samples.

References

1. Kienzle, Darrell M., and Matthew C. Elder. "Recent worms: a survey and trends." Proceedings of the 2003 ACM workshop on Rapid malcode. ACM, 2003.
2. Symantec. Internet Security Threat Report, Vol. 21 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, 2016.
3. Egele, Manuel, et al. "A survey on automated dynamic malware-analysis techniques and tools." ACM Computing Surveys (CSUR) 44.2 (2012): 6.