Computer Science

Opponent(s):

Dennis Eklind, Zeena Yalda

Respondent(s):

Markus Fors, Christian Grahn

An implementation of a DNS-based malware detection system

Opposition Report, C-level

2010:xx

1 A General Evaluation of the Project

In the project, Fors and Grahn have developed the FoG-DMDS program, which is a platform for detecting malware by analysing DNS queries on a network. They seem to have fulfilled the goals they had in the start of the project and the test of the program gave a good result. Since the program uses modules for performing the actual tasks, it will not be outdated in a near future. It is natural to update the modules rather then the program to keep up with the the development of new malwares.

2 Comments on the Project in Relation to the Dissertation

The project to develop FoG-DMDS takes up a very big part of the dissertation. We like the way the dissertation focuses only on the parts of the background that is directly relevant to the project. Only relevant information is given and even though the dissertation is relatively short, we do not feel like any part is missing.

2.1 Title

The title of the dissertation summarizes the dissertation in a very good way. The reader gets a very good idea of what the content of the dissertation will be.

2.2 Dissertation Layout

The dissertation layout is very logical and easy to follow. There is a clear red thread through the introduction, background, implementation, testing and conclusion chapters. But it could have been even better if chapter summarizes were added and a new page was used for every new chapter.

2.3 Scientific Method

The authors have been reading literature and talking to their supervisor to collect the information needed to write the dissertation. It seems like they have chosen trustworthy

sources for their information. Among the references we find several references to different RFC's

2.4 Argumentation and Conclusions

Through the entire dissertation, substantiated arguments and logical conclusions are used

2.5 The Abstract

In the abstract, the authors start with explaining the need for their project and goes on giving a good overview of the project. Reading the abstract gives the reader enough background information to understand the context of any given part of the dissertation.

2.6 Language Aspects

The dissertation includes multiple errors in the choosing of “a” or “an” and grammatical number.

2.7 References and Sources

The references have been carefully chosen and we have no reason to mistrust the sources of the dissertation. It would however have been appropriate to give the date that the website was retrieved also for the two references from The Open Group ([1] and [2]), even though it is unlikely that they will be changed. It could also be easier to find the references if URL-addresses were given also to the RFCs in the reference list.

2.8 General Comments on the Project

The authors have accomplished their task to develop a software for detecting malware by monitoring DNS traffic. They have declared what additional work they would have done if they had enough time. The program uses modules to perform the actual detection and action taking. This makes the program flexible and extendible.

3 Chapter by Chapter Evaluation of the Dissertation

3.1 Chapter 1

The first chapter,named introduction, starts with a brief definition of malware and DNS and DMDS, which are all highly relevant for the dissertation. Since the project is about creating a DMDS which monitors DNS traffic to detect malware. The authors then goes on to describe the core of their project, namely their implementation of a DMDS platform. The chapter ends with an overview of the remaining chapters.

A very good starting chapter. The reader gets a sound introduction to dissertation and will easily be able to follow the red thread through the chapter and the reader will also be helped to follow the red thread through the rest of the dissertation, given such a good overview.

The only thing we miss is a reference to the definitions in the beginning of the chapter.

3.2 Chapter 2

The second chapter is called background. It mainly deals with DNS and malwares. Here we find Figure 1.1, which we would have expected to find in chapter 1. The first part of the chapter gives a good background and explanation of DNS including the distinction between iterative and recursive queries and the four parts of the DNS packet. Details are only given about the part relevant to this project, which is a good idea in a society where the readers rarely have time to read something only vaguely related to the subject.

Unfortunately there seems to be some confusion over the distinction between a DNS packet and a DNS section. We learn on page 8, that a DNS packet consists of four parts: A MAC-header, IP-header, UDP-header and the DNS section. But in Figure 2.4, a DNS packet is shown, consisting of five parts: A DNS Header, Question, Answer, Authority and Additional. This seems to match the description of the DNS section on page 10.

After having described the different formats of the DNS section/packet, the authors describe the term malware and more specifically bots and botnets and spyware/adware. Finally a list of known methods to observe bots and other malicious software using DNS monitoring, is displayed.

The chapter gives a solid background to the specific field area interesting to this thesis.

3.3 Chapter 3

The third chapter describes the software that the authors developed during the project and named it after themselves: Fors-Grahn DMDS (FoG-DMDS). The application is divided into three parts: logging, detection and action. The two later parts use modules to perform the actual tasks, this so it will be easy to plug-in new modules as the malwares gets more sophisticated and depending on specific threats to a system.

The chapter gives very extensive details of the implemented software. Since references are made to specific functions in the code, it would have been easier to follow the text if the source code had been found in the appendix. But it is still a very good description of the software.

3.4 Chapter 4

In this chapter we can read about a test that was conducted to measure the rate of sent DNS queries that FoG-DMDS can handle. Every step of the test is documented in a convincing way and the reached result is that approximately 3000 users can be actively transmitting normal amounts of traffic on the network before the program starts to fall behind.

3.5 Chapter 5

The last chapter is the conclusion. It includes a short summary of the work done and what work should be done in the future, including ideas for other modules. The chapter meets our expectations for a conclusion.

3.6 General Comments on the Dissertation

The first thing we notice when looking at the dissertation is how short it is. But after reading it, it gives a complete impression. The authors have focused on quality rather than quantity.

After reading through the project description, found on the course homepage (http://www.cs.kau.se/stefalfr/dnsdatamining/ 2010-06-06), we found an aspect of the project that is hardly mentioned in the dissertation:

"The project will also consider ethical and privacy aspects of this data mining. This technology can easily be used for surveillance purposes, and the risk for abuse is high."

This document is however only an idea for a Bachelor's project, but we still think this aspect, being as important as it is, should have been mentioned in the dissertation.

The many abbreviations in the dissertation are treated somewhat differently. Sometimes they are explained directly in the text, sometimes with a reference and sometimes the reader has to go to the Glossary t the end to find the meaning of the abbreviation. Some consistency would be appreciated. When the meaning of an expression or an abbreviation is explained in the glossary, it would be good if the reader was informed about this. The glossary should also be alphabetically ordered. Now it seems to be randomly ordered.

4 Final Comments

Markus Fors and Christian Grahn have done a very good job with both their implementation and the dissertation. Except for some spelling mistakes, the dissertation gives a very professional impression and FoG-DMDS appears to be a well thought-out software.