OULUN YLIOPISTO
UNIVERSITY of OULU

FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Ilkka Sovanto

EVALUATING SIGNATURELESS NETWORK DETECTION METHODS

Master's Thesis
Degree Programme in Computer Science and Engineering
Month 2016

Sovanto I. (2016) English title. University of Oulu, Degree Programme in Computer Science and Engineering. Master's thesis, 10 p.

ABSTRACT

This is a sample abstract. **Keywords: sample, keywords**

Sovanto I. (2016) Suomenkielinen nimi. Oulun yliopisto, tietotekniikan tutkinto-ohjelma. Diplomityö, 10 s.

TIIVISTELMÄ

Esimerkkitiivistelmä

Avainsanat: esimerkki, sanoja

TABLE OF CONTENTS

ABBREVIATIONS

LAN	local area network
IP	Internet protocol
GUI	graphical user interface
HTTP	hypertext transfer protocol
UDP	user datagram protocol
CPU	central processing unit
RAM	random-access memory
FTP	file transfer protocol
WWW	world wide web
API	application programming interface
NAT	network address translation
CLI	command line interface
DPI	dots per inch

1. INTRODUCTION

- INTRODUCTION: The Setting - bird eye's view - the challenge to be tackled / thing to be be improved in general
- INTRODUCTION: Past research done
- INTRODUCTION: Gap in knowledge/problem not yet solved
- INTRODUCTION: Purpose and method of this work
- INTRODUCTION: More detailed description what was done
- INTRODUCTION: Results acquired
- INTRODUCTION: Analysis and limitations of the results (Mostly relocate to Conclusions)
- INTRODUCTION: Value (Mostly relocate to Conclusions)

The purpose of this thesis is to investigate the state of the art of signatureless detection methods of malicious network traffic. This type of traffic is typically generated by a piece of malware installed on a compromised machine. The prime example of malicious traffic we wish to detect is the so called beaconing traffic where the malware periodically contacts a command & control server to check in and request tasks to execute. In this work we assume the point of view of a security analyst responsible for defending a network belonging to a reasonably sized company.

The best understood and currently most widely deployed approach to detect malware communications is using an intrusion detection system that leverages previously crafted signatures. This works quite well when facing known threats and information about them is being shared effectively between various defenders.

A more problematic scenario arises when tasked to detect a lesser known or perhaps even uniquely tailored piece of malware for which no pre-existing signatures are possible. In this work we will explore various proposed methods from previous research to categorise them and give an estimate on their feasibility and the repeatability of the claims they make. In order to facilitate this, a semi-automated testing system is set up, emulating a continuous integration work flow. This allows other contributors to easily add more detection methods and thus expand the breadth of the survey.

2. IMPLEMENTING SOMETHING

Your implementation.

3. TESTING SOMETHING

Your testing.

4. DISCUSSION

Your discussion.

5. CONCLUSION

The best thesis evar.

6. REFERENCES