**A Project Report**

**On**

**Building a System for P2P Botnet Detection**

**Submitted to**

**VISVESVARAYA TECHNOLOGICAL UNIVERSITY**

**BELGAUM - 590 014, KARNATAKA**



**in partial fulfillment of the requirement for the award of**

**Bachelor of Engineering**

**during 8th semester of**

**Computer Science and Engineering**

**Under the guidance of**

**A.M.PRASAD**

**Associate Professor, Department of Computer Science and Engineering**

**Submitted by**

**Anushka Godha 1DS10CS013**

**Bhansali Amith Kumar Jain 1DS10CS022**

**Neeraj Karamchandani 1DS10CS051**

**2013-2014**



**Department of Computer Science and Engineering**

**Bangalore-560078**

**Dayananda Sagar College of Engineering**

**VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM**

**DAYANANDA SAGAR COLLEGE OF ENGINEERING**

**Shavige Malleshwara Hills, Kumaraswamy Layout, Bangalore-560078**

**Department of Computer Science & Engineering**



**CERTIFICATE**

This is to certify that the project report entitled **“Building a System for P2P Botnet Detection”** is a bonafide work carried out by **Anushka Godha [1DS10CS013],** **Bhansali Amith Kumar Jain [1DS10CS022] and Neeraj Karamchandani [1DS10CS051]** in partial fulfillment for the VIII SEM, **Bachelor of Engineering** in Computer Science and Engineering of the **Visvesvaraya Technological University, Belgaum** during the year 2013-2014. The project report has been approved as it satisfies the academic requirements in respect of Project Work prescribed for Bachelor of Engineering Degree.

Dr. Ramesh Babu D.R Dr. A.N.N.MURTHY

Professor & HOD Principal

Dept of CSE,DSCE DSCE

Bangalore Bangalore

**Signature Signature**

…………………………… …………………………..

**Name of the Examiners Signature with date**

1…………………………. ……………………………

2 …………………………. ……………………………

**ACKNOWLEDGEMENT**

A successful project is a fruitful culmination of efforts by many people, some directly involved and some others who have quietly encouraged and extended support from the background.

A project is not complete if one fails to acknowledge all these individuals who have been instrumental in the successful completion of the project.

We express our sincere gratitude to **Dr. A. N. N. MURTHY**, Principal of our college, DSCE, for his advice and guidance that helped us to complete this project with success.

We would like to begin by expressing our profound and sincere gratitude to our guide **A. M. Prasad**,Associate Professor and Project Coordinator, Department of Computer Science and Engineering for his excellent and timely guidance, constant encouragement, strive for perfection and with relentless support that helped us to make critical decisions during the course of the project

We thank our institution, **Dayananda Sagar College of Engineering** without which our project would have been a distant reality.

|  |  |
| --- | --- |
| Anushka Godha | [ 1DS10CS013 ] |
| Bhansali Amith Kumar Jain | [ 1DS10CS022 ] |
| Neeraj Karamchandani | [ 1DS10CS051 ] |

**ABSTRACT**

A “botnet” consists of a network of compromised computers controlled by an attacker (“botmaster”). Recently, botnets have become the root cause of many Internet attacks including much dreaded DDOS attacks. Traditionally botnet were using a centralized server for communicating but now a days Botnet have started using P2P technology as P2P botnets are harder to track and takedown as they have no single point of faliure. Growing popularity of P2P botnets compels to find proper countermeasures but existing defence mechanisms hardly catch up with the speed of botnet technologies.

In this project we propose novel botnet detection system. We first identify P2P traffic from normal traffic by means of clustering based approch, then we use a profiling scheme to build a statistical fingerprints and to estimate their active time to detect stealthy P2P botnet even if they are overlapped with legitimate P2P traffic (e.g. torrent) with high accuracy.

**CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **1.** |  | **INTRODUCTION** | **1-5** |
|  | 1.1 | MOTIVATION | 3 |
|  | 1.2 | OBJECTIVE OF THE WORK | 4 |
|  | 1.3 | PROBLEM STATEMENT | 4 |
|  | 1.4 | METHODOLOGY ADOPTED | 5 |
|  | 1.5 | ORGANIZATION OF THE REPORT | 5 |
| **2.** |  | **LITERATURE SURVEY** | **6-9** |
| **3.** |  | **BOTNET** | **10-16** |
|  | 3.1 | FORMATION | 12 |
|  | 3.2 | TYPES OF ATTACK | 13 |
|  | 3.3 | LIFECYCLE OF A BOTNET | 14 |
|  | 3.4 | BOTNET CONTROL & COMMUNICATION ARCHITECTURE | 15 |
| **4.** |  | **SYSTEM ANALYSIS** | **17-22** |
|  | 4.1 | EXISTING SYSTEM | 18-21 |
|  | 4.1.1 | BOTMINER | 18 |
|  | 4.1.2 | NETWORK STREAM ANALYSIS | 18 |
|  | 4.1.3 | MULTI-PHASED FLOW MODEL | 19 |
|  | 4.1.4 | NODE BEHAVIOR DETECTION | 19 |
|  | 4.1.5 | NETWORK BEHAVIOR ANALYSIS & DATA MINING | 20 |
|  | 4.1.6 | ASSOCIATION BETWEEN COMMON NETWORK | 20 |
|  | 4.1.7 | USER BEHAVIOR SOCIALITY & TRAFFIC ENTROPY FUNCTION | 21 |
|  | 4.1.8 | DATA MINING | 21 |
|  | 4.2 | THE PROPOSED SYSTEM | 22 |
| **5.** |  | **SOURCE CODE** | **23-51** |

|  |  |  |  |
| --- | --- | --- | --- |
| **6.** |  | **SCREENSHOTS** | **52-59** |
| **7.** |  | **VERIFICATION AND VALIDATION** | **60-62** |
|  | 7.1 | UNIT TESTING | 61 |
|  | 7.2 | WHITE BOX TESTING | 61 |
|  | 7.3 | BLACK BOX TESTING | 62 |
| **8.** |  | **CONCLUSION** | **63-64** |
| **9.** |  | **REFERENCES** | **65-66** |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| 4.2.a. | PICTORIAL REPRESENTATION OF PROPOSED SYSTEM | 18 |
| 6.1.a. | SCREENSHOT OF NODE\_1 | 45 |
| 6.1.b. | SCREENSHOT OF SEND IN NODE\_1 | 45 |
| 6.1.c. | SCREENSHOT OF VIEW IN NODE\_1 | 46 |
| 6.2.a. | SCREENSHOT OF NODE\_2 | 46 |
| 6.2.b. | SCREENSHOT OF SEND IN NODE\_2 | 47 |
| 6.2.c | SCREENSHOT OF VIEW IN NODE\_2 | 47 |
| 6.3.a | SCREENSHOT OF ROUTER | 48 |
| 6.3.b | SCREENSHOT OF TRANSACTION IN ROUTER | 48 |
| 6.3.c | SCREENSHOT OF FIND\_BOTNET IN ROUTER | 49 |
| 6.3.d | SCREENSHOT OF CLUSTER\_FORMATION | 49 |
| 6.3.e,f | SCREENSHOT OF BOTNET\_DETECTION | 50 |
| 6.3.g | SCREENSHOT OF BOTMASTER DETECTION | 51 |
| 6.4 | SCREENSHOT OF BOTMASTER | 51 |