# Multi-phase IRC Botnet & Botnet Behavior Detection Model

Aymen AlAwadi
aymen@tmit.bme.hu

# Content

1. Introduction
2. Understanding botnet problem
3. Solution
4. Botnet specification
5. Module design
6. Process flows of the model
7. Module implementation
8. Validation testing
9. Summary

# 1. Introduction

Botnet problem:

- Bot: is a malicious software like the common computer viruses and worms, can be distributed either by itself or by Trojan insertion.
- Bots can threaten the existing services and resources. Bots can easily evade AV tools.
- Bots implementing command-and-control (C&C) which is used by the botmaster to direct and update the bots through communication protocol like (IRC or HTTP).

# 1. Introduction

## Botnet Architecture:

- Botnet is a group of bots mainly have two kinds of architecture, centralized and P2P.

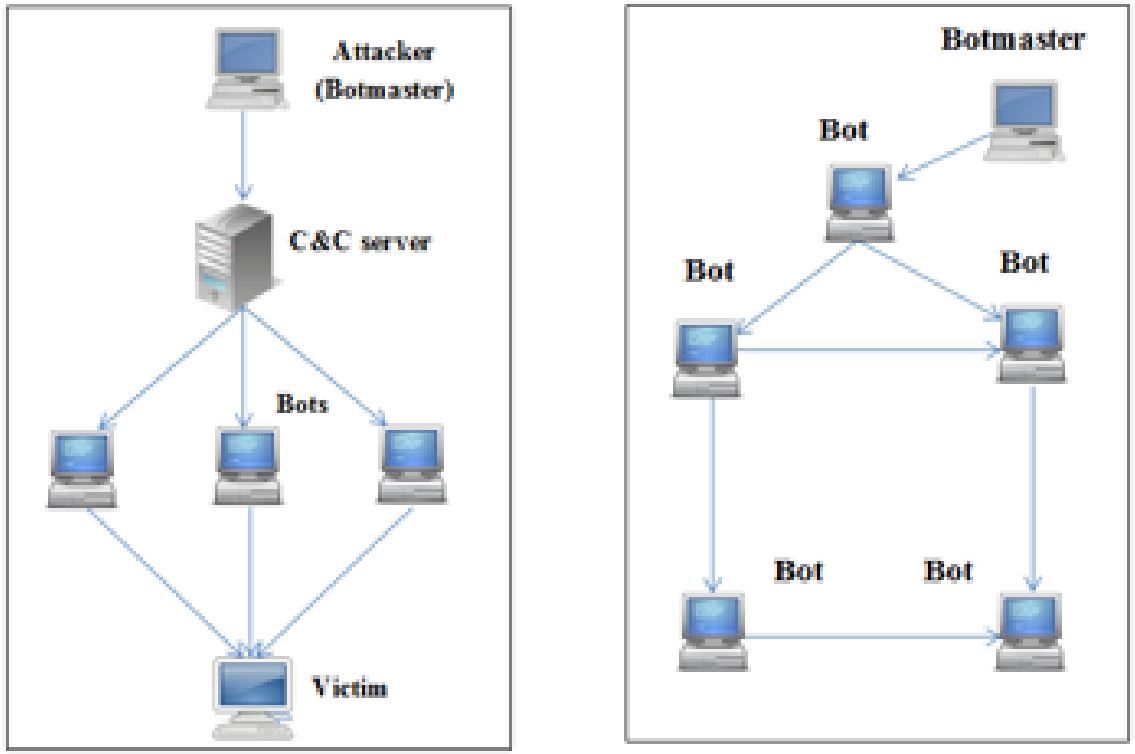


Fig. 1 Botnet architecture

# 2. Understanding Botnet

- Botnet life cycle

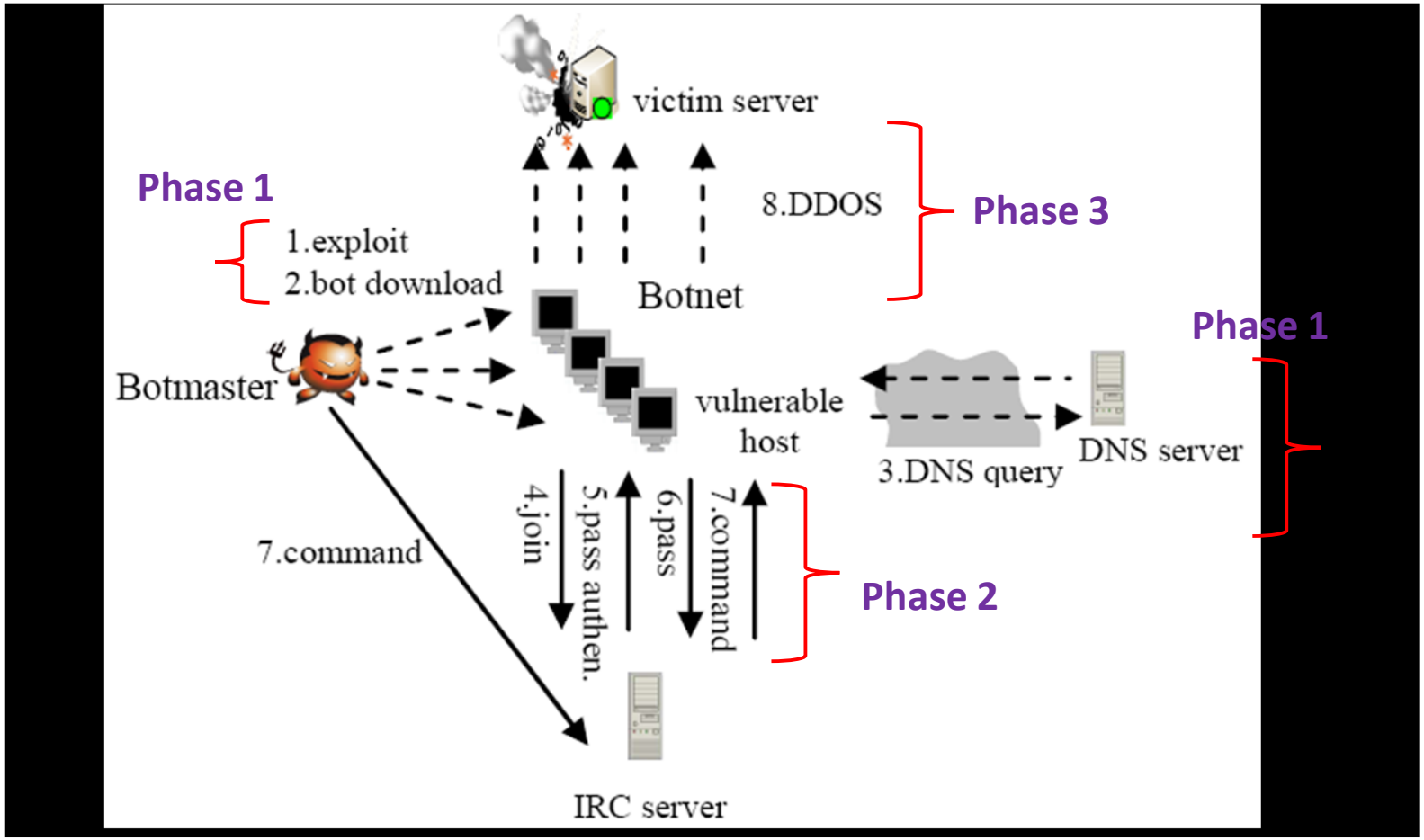


Fig. 3: Common life-cycle for IRC botnet (Lu and Ghorbani, 2008)

# 2. Understanding Botnet

- Global Botnet Threat Activity Map

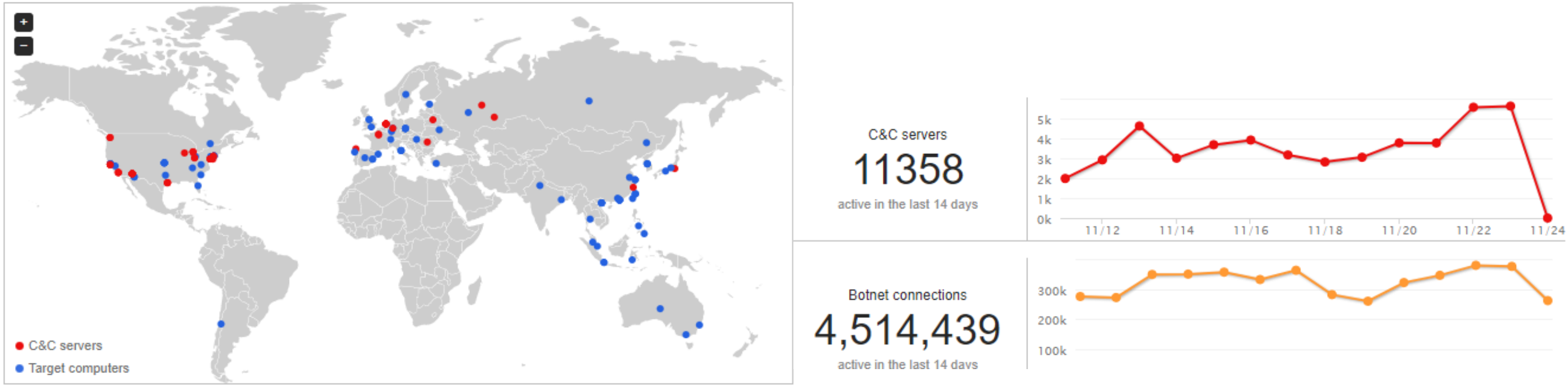


Fig. 3 Current botnet map distribution (trend micro, 2017)

# 3. Solution

- We proposed a model for IRC botnet and botnet behaviors detection based on botnet life-cycle phases.

The proposed model includes 2 phases.

- The proposed method would be used to detect IRC bots based on botnet phase 2 and botnet behaviors based on botnet phase 3.

- The detection method is depending on spatial-temporal correlation and similarities strategy.

- We evaluated the model accuracy and efficiency.

# 4. Botnet specification

For IRC Botnet detection:

- Phase 2 of botnet life-cycle (Bot initial communication) – (NICK and C&C response message (PRIVMSG)). (Phase 1 (part 1 & 2) on the proposed model).

For Botnet behavior detection:

- Phase 3 for Botnet attacks behaviors. (attacks or any malicious activities). Phase 2 on the proposed model.

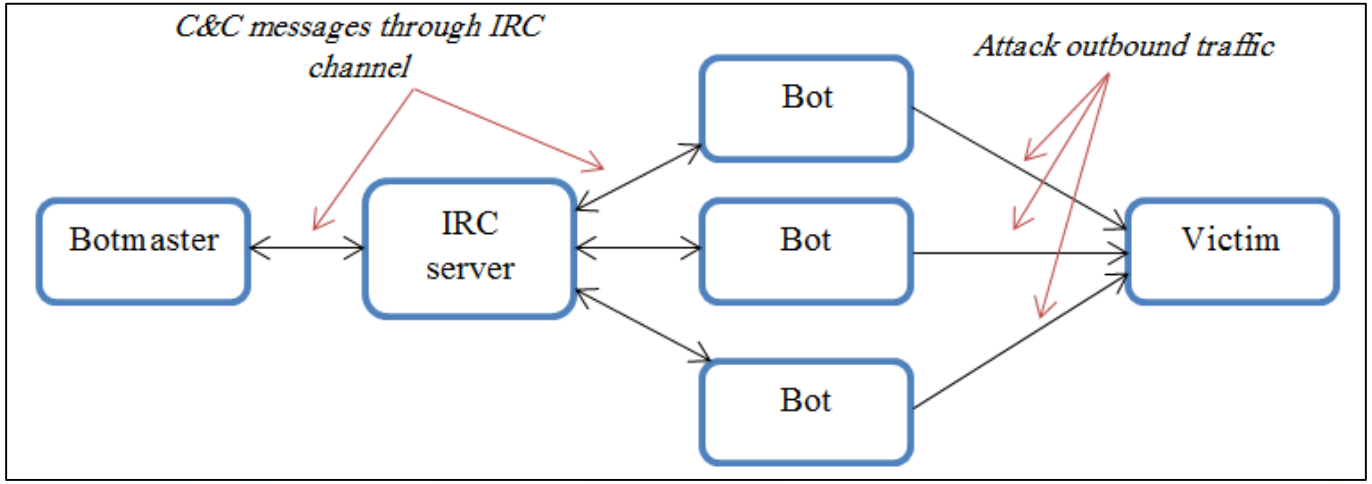


Fig. 4 Common architecture of IRC botnet

# 5. Module design

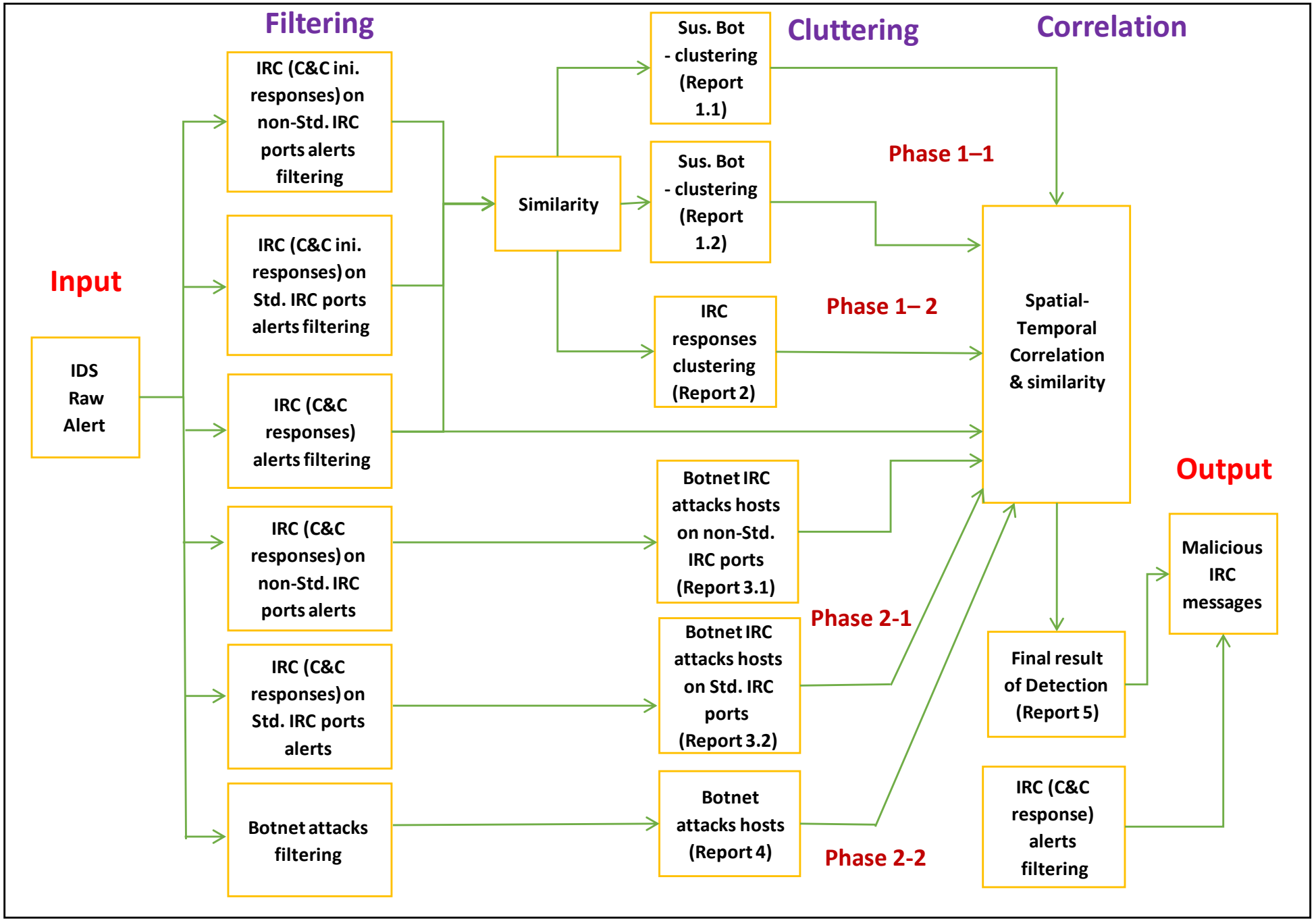


Fig. 5 The phases and the Process Flows Modes of the Model

# 5. Process Flows of the Model

- There are two process flows on the purposed model to track the IRC botnet activities.
- **Coherent mode**: representing the IRC responses messages that related to initial IRC bot activities. Phase 1 and continue with the result of phase 2.

- **Non-coherent mode**: representing the IRC responses messages which are not related to the initial IRC activity. Phase 1 – part 2 and continue with the results of the phase 2.

- The filtering stage is depending on filtering the C&C responses that are directed to the same IRC server with same (destination IP, destination port and timestamp).

# Module implementation

# 6. Module implementation (Module testing)

The detection efficiency and accuracy of the proposed model have been evaluated with three case studies and multiple botnet scenarios.

1. Virtual machines by using Vmware with real botnets.

2. Dataset like DARPA 2000-Windows NT Attack Data Set.

3. CAIDA DDoS Attack 2007 Dataset.

# 6.1 Module implementation (Module testing)

## Case Study 1:

The main objective of first case study is:

- To show different situations of existing botnet inside the monitored network with different intervals of monitoring time.

- To achieve this case study, we had three IRC botnet scenarios inside the Vmware environment.

# 6.1 Module implementation (Module testing)

## Case study 1:

1. Botnet scenario 1: Detecting multiple kinds of bots in initial IRC activity.
2. Botnet scenario 2: Detecting multiple kinds of bots in middle of IRC activity.
3. Botnet Scenario 3: Detecting single bot members at different situations.

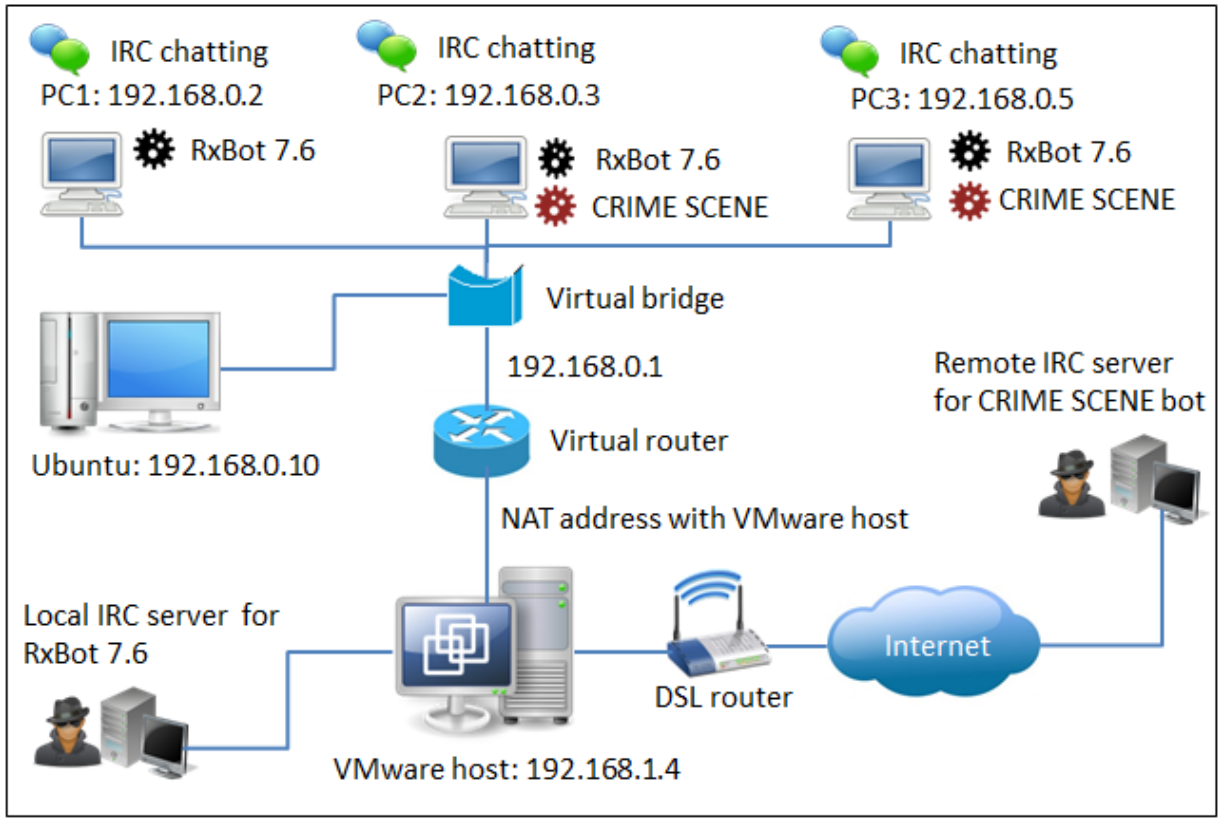


Fig. 6: VMware testbed environment

# 6.2 Module implementation (Module testing)

**Case study 2:**

Windows NT Attack DARPA 2000 Network Traffic Data Set.

- The chosen data set does not contain any kind of botnet, but it has normal IRC chatting traffic that comes with many Windows NT attacks.
- The main objective is to show that the proposed model can pass normal IRC chatting on IRC port 6667 without any botnet false positive result.
- This data set contains two flows from two networks; one for Inside and one for Outside network.

# 6.3 Module implementation (Module testing)

**Case study 3:**

CAIDA DDoS Attack 2007 DataSet

- This data set includes TCP-based DDoS attack to certain victim with responses from that victim to the attackers.

- The main objective is to evaluate the proposed model to detect botnet behavior (attack) which is happening regardless to the type of botnet communication protocol.

# Validation testing

# 7. Validation testing

- The proposed model will be evaluated regarding detection accuracy and the model execution performance.
- The detection accuracy will be measured by evaluating the achieved objectives for each case study and scenario.

- The model performance will be measured by evaluating the average execution time of the proposed model to achieve the objectives.

# 7.1 Validation testing

Case study1-Botnet Scenario1:

Botnet scenario 1: Detecting multiple kinds of bots in initial IRC activity

results and discussion:

| Total Alerts | IRC MSG | IRC % of total alerts | Normal IRC | Malicious IRC | % Normal IRC to total IRC | % Malicious IRC to total IRC | IRC Bots | Detected IRC Bots |
|---|---|---|---|---|---|---|---|---|
| 10,259 | 324 | 3% | 142 | 182 | 44% | 56% | 5 | 5 |

Table 1: Results of IRC Botnet Scenario 1

The achieved objectives:

- All of the infected IRC bots (the 5 bots) have been detected and their current state was accurate except one bot.
- The proposed model was able to detect IRC botnet members that work in different IRC ports with different destination IP addresses.

# 7.1 Validation testing

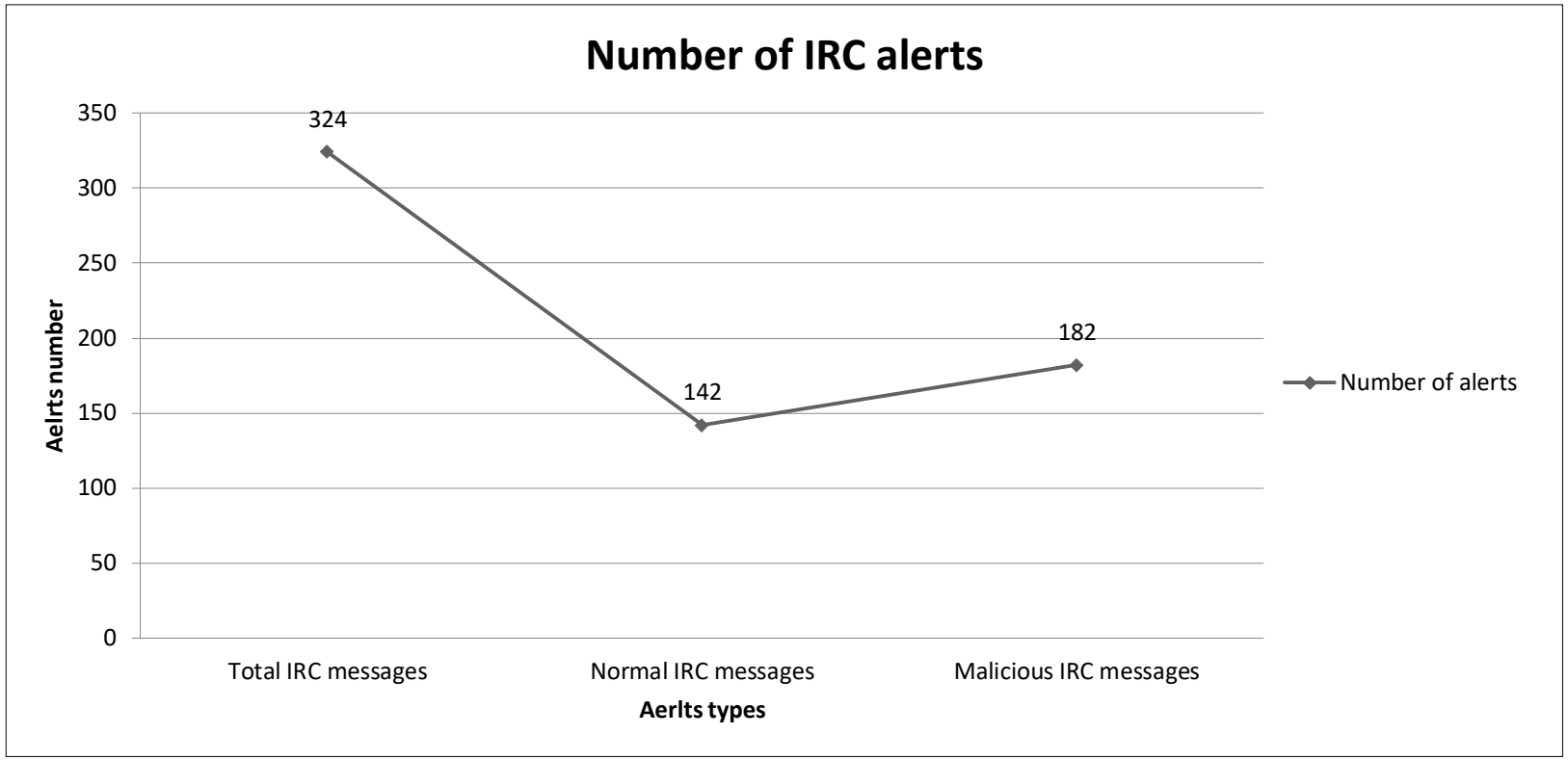


Fig. 7: The filtered normal and malicious IRC alerts compared with the total number of IRC message

- As for performance evaluation, the proposed model took 2 seconds as an average execution time.

# 7.2 Validation testing

Botnet scenario 2: Detecting multiple kinds of bots in middle of IRC activity results and discussion:

| Total Alerts | IRC MSG | IRC % of total alerts | Normal IRC | Malicious IRC | % Normal IRC to total IRC | % Malicious IRC to total IRC | IRC Bots | Detected IRC Bots |
|---|---|---|---|---|---|---|---|---|
| 2,073 | 163 | 8% | 96 | 67 | 59% | 41% | 4 | 4 |

Table 2: Results of IRC Botnet Scenario 2

The achieved objectives:

- Detected IRC bots are in coherent mode or non-coherent mode.
- There were some functional conflicts after rules updating.
- Normal IRC messages for single IRC server have been filtered out.

# 7.2 Validation testing

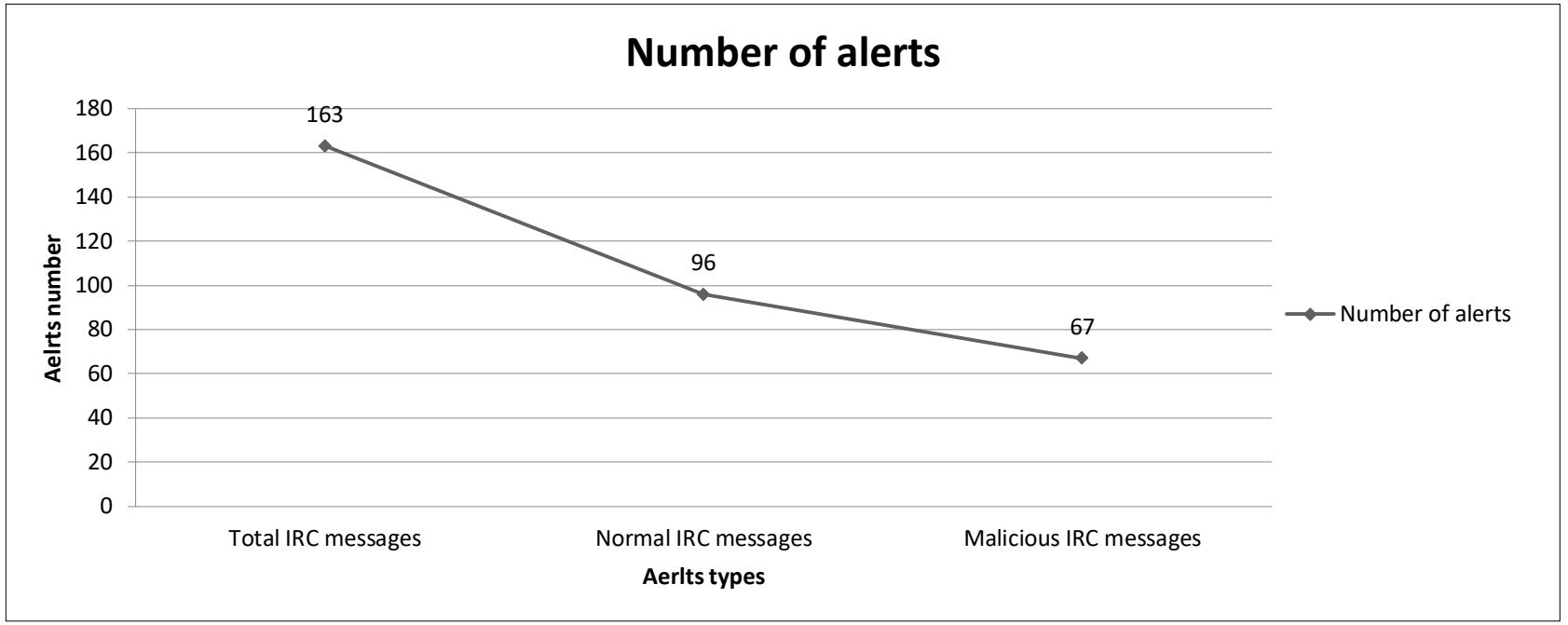


Fig. 8: The filtered normal and malicious IRC alerts compared with the total number of IRC message of the botnet scenario 2

- As for performance evaluation, the proposed model took 0.3 of a second as an average execution time, since there was no botnet attack in this scenario.

# 7.3 Validation testing

Botnet scenario 3: Detecting single bot members at different situations results and discussion:

| Total Alerts | IRC MSG | IRC % of total alerts | Normal IRC | Malicious IRC | % Normal IRC to total IRC | % Malicious IRC to total IRC | IRC Bots | Detected IRC Bots |
|---|---|---|---|---|---|---|---|---|
| 60,989 | 149 | 0.2% | 99 | 50 | 66% | 34% | 3 | 3 |

Table 3: Results of IRC Botnet Scenario 3

The achieved objective:

- Detecting singles IRC botnet member(s) inside the monitoring network even when they were in different situations with different activities (botnet attacks).

# 7.3 Validation testing

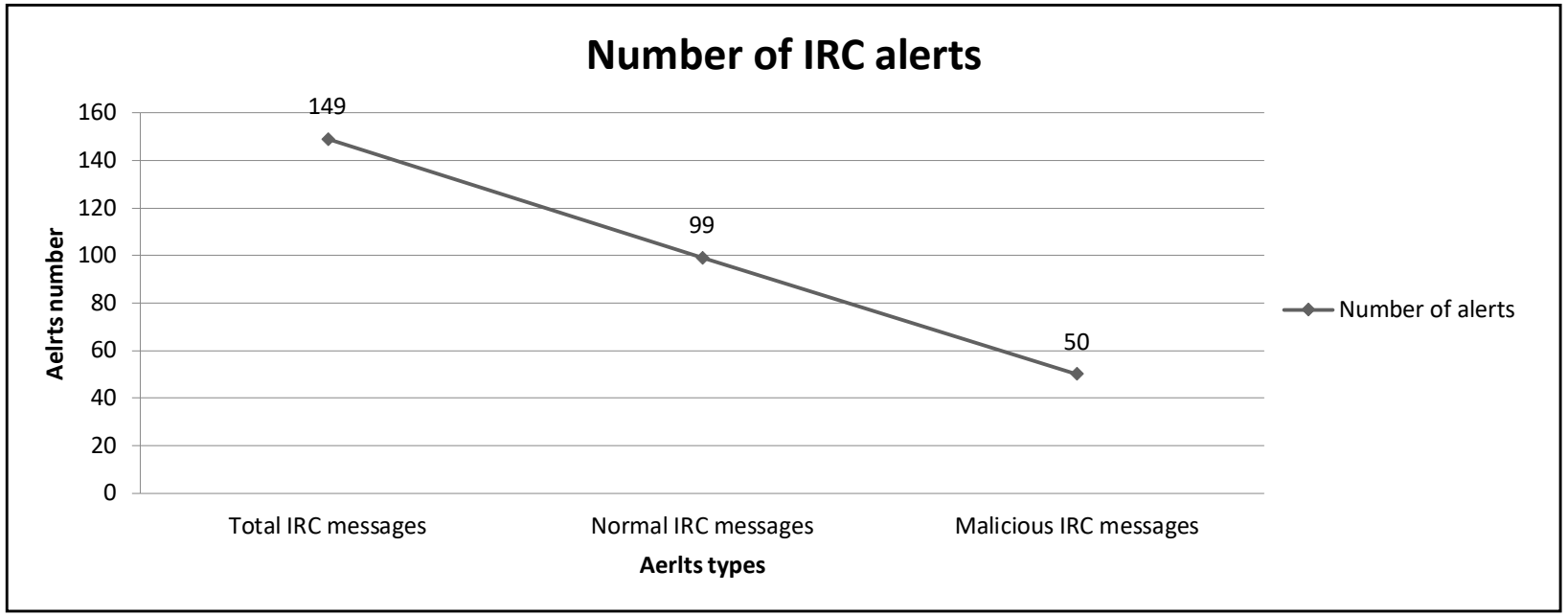


Fig. 9: The filtered normal and malicious IRC alerts compared with the total number of IRC message of the botnet scenario 3

- As for performance evaluation, the proposed model took 28.66 seconds as an average execution time, since there were 59,087 alerts belong to botnet attack.

# 7.4 Validation testing

Case study 2: Windows NT Attack DARPA 2000 Network Traffic:

| No. Alerts | No. of IRC | % IRC msg to No. of Alerts | Normal IRC | Malicious IRC | % Normal IRC to total No. of IRC messages | % Malicious IRC to total No. of IRC | IRC Bots | Detected IRC Bots |
|---|---|---|---|---|---|---|---|---|
| 930 | 35 | 4% | 35 | 0 | 100% | 0% | 0 | 0 |

Table 4: Results of case study 2 for the inside Tcpdump file

The achieved objective:

- False positive botnet behaviors of case study 2 for the Inside Tcpdump file (2 hosts out of 40 hosts inside the network).
- The proposed method took from (0 to 0.3) of a second as average of execution time.

# 7.5 Validation testing

## Case study 3: CAIDA DDoS Attack 2007 Dataset:

| No. Alerts | No. of TCP traffic alerts | %TCP traffic alerts to the total No. of Alerts | No. of Port scanning alerts | %Port scanning to the total No. of Alerts | Detected DDoS Hosts | %Detected DDoS hosts to TCP traffic alerts |
|---|---|---|---|---|---|---|
| 1,033 | 871 | 84% | 160 | 16% | 113 | 13% |

Table 5: Results of IRC case study 3 for CAIDA DDoS Attack 2007 Dataset

The achieved objective:

- The proposed model proved that it was able to detect and verify botnet behaviors even without prior knowledge to the type of the used protocol for botnet communication.
- As for performance evaluation, the proposed model took 0.3 of a second to analyze the alerts.

# 7.6 Validation testing (Comparison)

## Botnet model characteristics

| Approach | Basis | IRC | Flow-Chars | Time | Net-Det | Syntax |
|---|---|---|---|---|---|---|
| BotHunter | Net- | Yes | No | Yes | Yes | Yes |
| BotSniffer | Net- | Yes | No | Yes | Yes | Yes |
| Rishi | Net- | Yes | No | No | No | Yes |
| The proposed model | Net- | Yes | pps | No | Yes | Yes |

Table 6: Comparison of the proposed model with the other approaches based on botnet characteristics

- The flow characteristics are including number of packet per flow (ppf), number of bytes per packets (bpp), number of bytes per second (bps) and number of packets per second (pps) (Lu et al., 2011).

# 8. Summary

1- The main goal of the proposed model is to detect IRC botnet members and botnet behaviors based on that bots, malicious IRC messages will be filtered.

2- The proposed model considers the two botnet life-cycle phases for detection (IRC messages and attacks).

3- The proposed model assigns different status messages to describe the current status of the detected bot (IRC responses messaging and/or attacks).

4. The model evaluation shows that the proposed model was able to detect IRC botnet member(s) with minimum false positive results.

# 9. References


1. Al, Aymen Hasan Rashid, and Bahari Belaton. "Multi-phase IRC Botnet and Botnet Behavior Detection Model." International Journal of Computer Applications 66.15 (2013).
2. Lu, Wei, and Ali A. Ghorbani. "Botnets detection based on irc-community." Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. IEEE, 2008.
3. Lu, Wei, Goaletsa Rammidi, and Ali A. Ghorbani. "Clustering botnet communication traffic based on n-gram feature selection." Computer Communications 34.3 (2011): 502-514.

# Thank you!