Ahmad KARIM, Rosli Bin SALLEH, Muhammad SHIRAZ, Syed Adeel Ali SHAH, Irfan AWAN, Nor Badrul ANUAR, 2014. Botnet detection techniques: review, future trends, and issues. *Journal of Zhejiang University-SCIENCE C (Computers & Electronics)*, **15**(11):943-983. [doi:10.1631/jzus.C1300242]

Botnet detection techniques: review, future trends, and issues

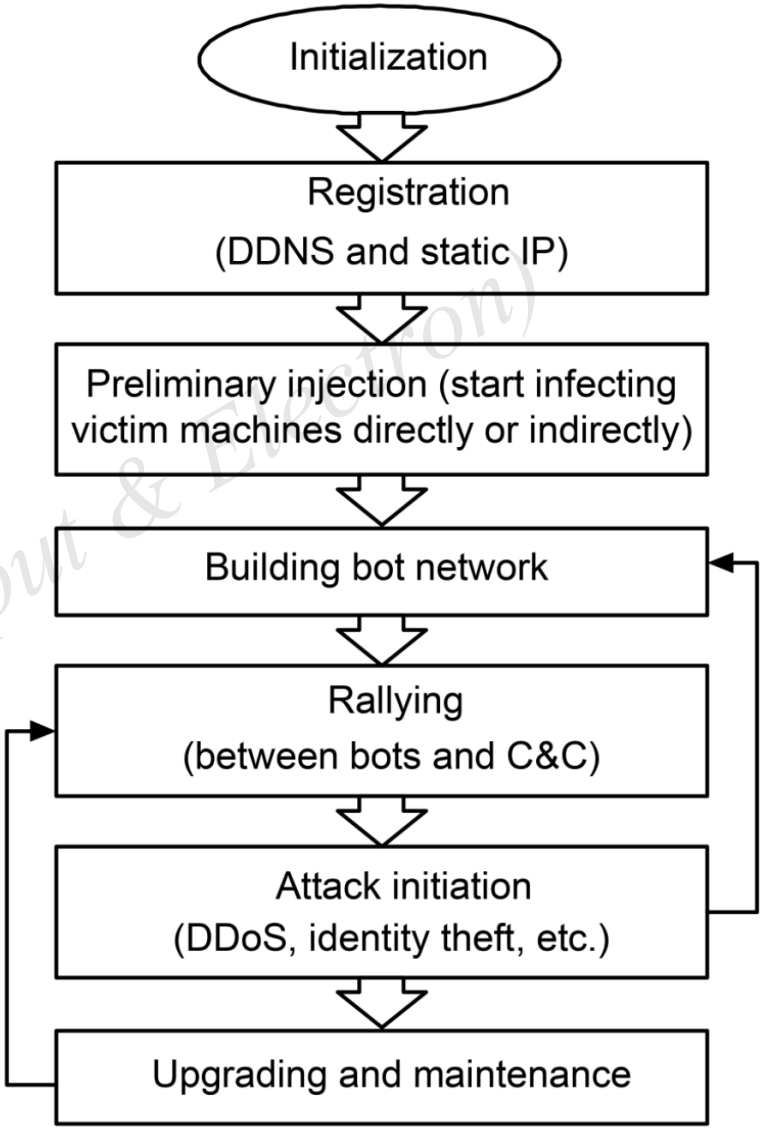
Key words: Botnet detection, Anomaly detection, Network security, Attack, Defense, Taxonomy

Corresponding author: Ahmad Karim
E-mail: ahmadkarim@um.edu.my

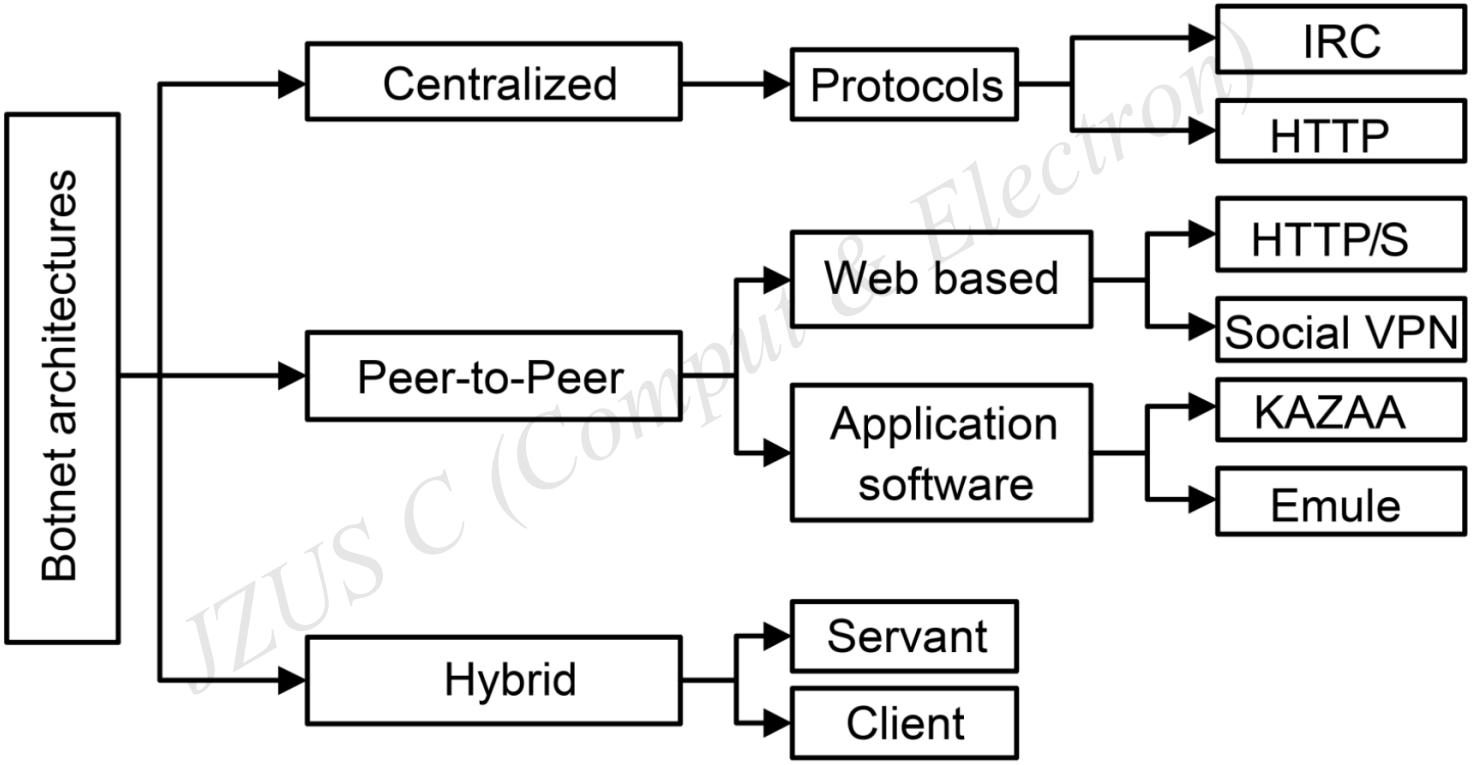
Introduction

- The botnet phenomenon supports a wide range of criminal activities, including distributed denial of service (DDoS) attacks, click fraud, phishing, malware distribution, spam emails, and building machines for illegitimate exchange of information/materials.
- It is imperative to design and develop a robust mechanism for improving the botnet detection, analysis, and removal process.
- This paper presents a comprehensive review of the latest state-of-the-art techniques for botnet detection, in addition to figuring out the trends of previous and current research. It provides a thematic taxonomy for the classification of botnet detection techniques and highlights the implications and critical aspects by qualitatively analyzing such techniques.

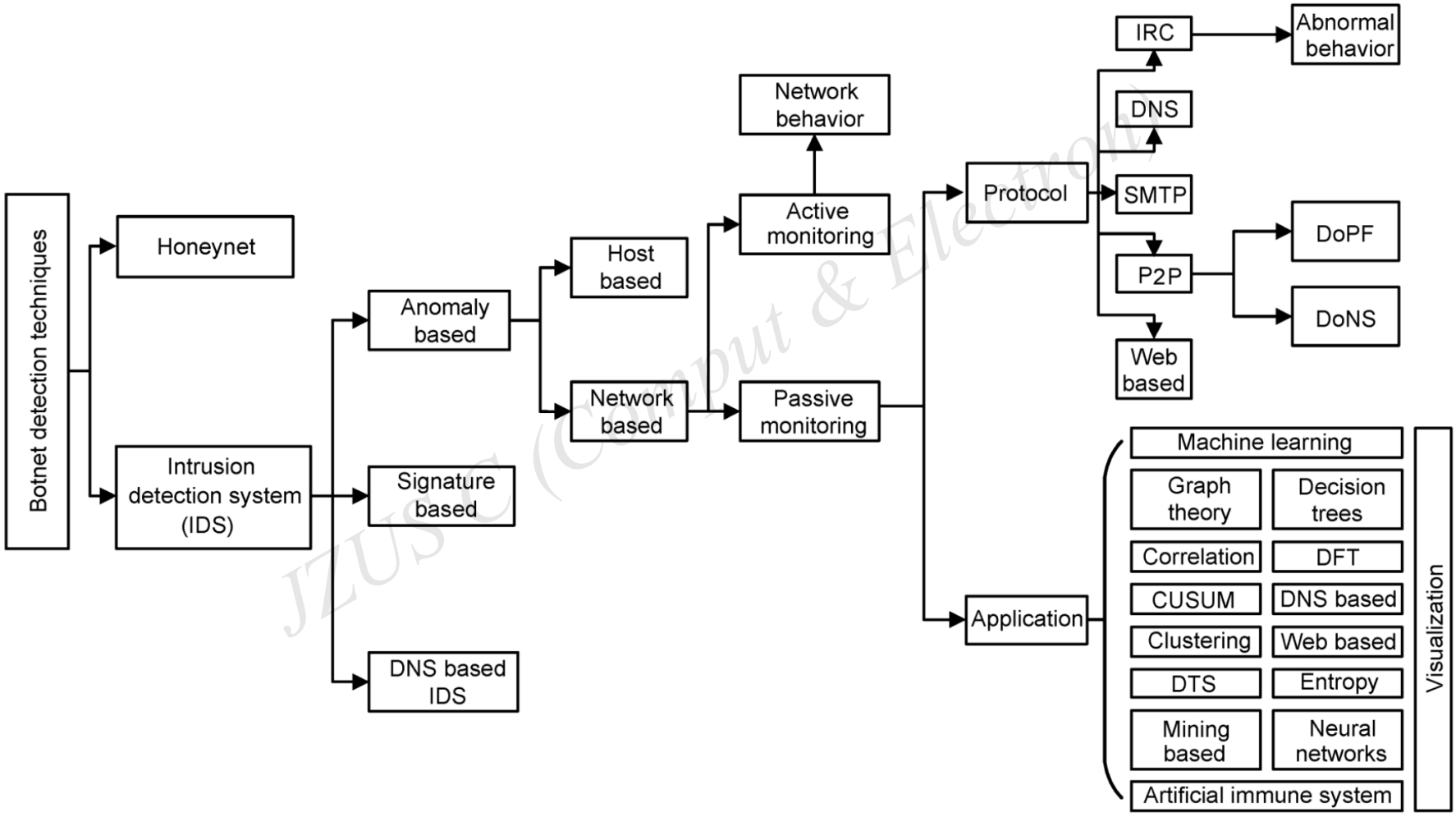
Botnet life cycle



Architecture of a botnet



Taxonomy of botnet



Summary

- We present a comprehensive review of the latest state-of-the-art for botnet detection techniques to figure out the trends of previous and current research and the issues in the botnet detection phenomenon.

- We propose a thematic taxonomy for the classification of botnet detection techniques and highlight the implications and critical aspects through qualitative analysis of such techniques.

- Also, we discuss recent trends towards botnets that are emerging with new technologies and highlight the open challenges in botnet detection for future research.