UNIVERSITI TEKNOLOGI MARA

ANALYZING BOTNET ACTIVITIES
AND NEFARIOUS ATTEMPT IN
CORPORATE & HOME USER NETWORK

MUHAMMAD SAUFI B. HJ BAHARUDIN

2007277904

Thesis submitted in fulfillment of the requirements for

Bachelor of Science (Hons) Data Communication and Networking

Faculty of Computer and Mathematical Sciences

May 2009

ACKNOWLEDGEMENT

By the name of ALLAH, the Most Gracious and Most Merciful.

First of all, Alhamdulillah, praise Allah for His Almighty and Graciousness. By Allah bless, I be able to finish this project and the report in the dateline time.

Special thanks to my supervisor, Pn. Shapina Bt. Abdullah for her guidance, support, encouragement and constructive criticism that I had been receiving for the preparation of this thesis. I never forget all the experience during doing this project. I also wish to express my sincere appreciation to project coordinator, Encik Adzhar B. Abd Kadir and Ms Raihana Bt. Md Saidi for his guidance from the beginning until end of this semester.

I would also like to say my heartiest appreciation to my lovely family, my parents; Tn Hj Baharudin, Pn Hjh Zaini, my siblings for everything they have done to me throughout my days in MARA University of Technology.

Finally, my deepest appreciation goes to Saharudin B. Saat, Kamal Azharan B. Azman, Ashwati Bt Yusoff, Mohd Syafuan B. Salim and to all my friends that support me during my project implementation either. Not to forget, all the IT department staff, Pn. Salmah. Thanks for their support, comments and advice. Finally to all parties in participation and commitment in making these project successful

Special thanks to all of you.

ABSTRACT

Botnet is a collection of compromised computer usually handled by bot herder which controlled it remotely. Internet security has become the most crucial issue in communication. The rashness of internet towards our daily life has turn into a threat that can easily obtain our information with just one click. By using massive attack of zombie, the attackers launch a *distribution denial of services* (*ddos)* against home users or corporate networks which is one of the common dangerous attacks. To create this army of zombie internet hosts, attackers typically infect machines of home users that having broadband access to internet, corporate networks maintained by universities & small enterprises, with remotely controlled Trojans. Usually, for whom who get infected by bot are typically had a low internet security awareness and limited resources to defend their internet infrastructure. This study will focus in Faculty of Computer and Mathematics Sciences, MARA University of Technology, Shah Alam for corporate network while home user network cover using WiMAX service provider. The purpose of this study is to increase understanding of the capabilities present in bot malware and analyzing activities of botnets. This analysis is done to find out the possibility of botnet attacks in every single internet access in FSKM and home users network. . The objective is to capture data in both FSKM and home user network and simulate it by using Snort. FSKM network are monitored by capturing all the inbound and outbound data traffic and those data will be analyze in different standalone platform. The result of this study will show the type of botnet activity and how it propagates the pattern of the activity in which will be use further for prevention development as well as build solid foundation of knowledge regarding botnet.

TABLE OF CONTENTS

CHAPTER 3 RESEARCH METHODOLOGY