ANALYZE BOTNET ACTIVITY BY IDENTIFY THE DIFFERENCE BETWEEN NORMAL AND ABNORMAL DNS TRAFFIC

AHMAD SYAFIQ B. JUWAINI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS*

JUDUL : ANALYZE BOTNET ACTIVITY BY IDENTIFY THE DIFFERENCE BETWEEN NORMAL AND ABNORMAL DNS TRAFFIC

SESI PENGAJIAN : 2009 / 2010

Saya AHMAD SYAFIQ BIN JUWAINI

(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
___/___	TIDAK TERHAD	

(TANDATANGAN PENULIS)
Alamat tetap : 47-11-16,MENARA ORKID, BANDAR BARU SENTUL, 51000 KUALA LUMPUR.
Tarikh : 25/06/2010

(TANDATANGAN PENYELIA)
DR. MOHD FAIZAL BIN ABDOLLAH
Nama Penyelia
Tarikh : 25/6/10

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

ANALYZE BOTNET ACTIVITY BY IDENTIFY THE DIFFERENCE BETWEEN NORMAL AND ABNORMAL DNS TRAFFIC

AHMAD SYAFIQ B. JUWAINI

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2010

DECLARATION

I hereby declare that this project report entitled

ANALYZE BOTNET ACTIVITY BY IDENTIFY THE DIFFERENCE BETWEEN NORMAL AND ABNORMAL DNS TRAFFIC

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENTS : _____ Date : 25/06/2010

(AHMAD SYAFIQ B. JUWAINI)

SUPERVISOR : _____ Date : 25/6/10

(DR. MOHD. FAIZAL ABDOLLAH)

DEDICATION

To my beloved parents, thank you for giving me opportunity to further my study until I can finish my study.

To my helpful lecturer, thank you for the guidance from the beginning until the end of the final project.

To my dear friends, thank you for all support that had be given to me to finish my study and final project.

ACKNOWLEDGEMENTS

I would like to thank Dr Mohd. Faizal Abdollah for guiding me during this project implementation period that takes about seven months to successfully done.

I would also like to thank my beloved parents that always giving me support and motivation to complete my final project and complete study.

Finally, I would to all my friends and persons that involved during this project development process until it complete.

ABSTRACT

This project is focus on the difference between normal DNS traffic and abnormal DNS traffic that made by the botnet. Botnet is software robot that is hardcoded by the botmaster or owner of the bot that has mission need to be accomplished. Victim of the botnet will faced consequence such as denial of service. This project analyzed the DNS traffic by focus on the numbers of query response. Query response for normal DNS traffic is less than the botnet DNS traffic because botnet like to contact its server more frequently than the normal DNS traffic. To get the network traffic, lab had been setup based on network setup configuration that had been planned for this project. Server was used to capture the network traffic and some workstations used to run the botnet for botnet DNS traffic and windows update for normal DNS network. There are some techniques to detect botnet, in this project detection of botnet is using anomaly-based technique. Network traffic will be captured for both botnet DNS network and normal DNS network. Three different network traffic had been captured which were botnet DNS network, normal DNS network and combination of botnet and normal DNS network. From the captured network traffic, analysis had been made and criteria involved were time the botnet active, number of NXDomain and CNAME rcode for the query response and the time interval for the botnet request at the DNS server. To get clear information to the DNS query response, graph was created for all the botnet DNS traffic and normal DNS traffic in the analysis phase. To confirmed output in the analysis phase, testing had been made to compare it. Conclusion for the project is to conclude that the project met all objectives that had been planned before or not.

ABSTRAK

Projek ini fokus kepada perbezaan di antara trafik DNS yang normal dan trafik DNS yang tidak normal di mana ia di lakukan oleh *botnet*. *Botnet* adalah perisian robot yang dikodkan oleh *botmaster* atau pemilik *bot* tersebut yang mempunyai misi untuk dilakukan. Mangsa kepada *botnet* akan menghadapi akibat seperti kekangan pada servis. Projek ini menganalisa trafik DNS dengan fokus kepada bilangan respon diberi kepada permintaan. Bilangan respon kepada permintaan daripada trafik DNS yang normal adalah kurang berbanding bilangan yang dilakukan oleh *botnet* kerana *botnet* suka menghubungi pelayan mereka lebih kerap berbanding trafik DNS yang normal. Untuk mendapat trafik rangkaian, makmal telah dikonfigurasi berdasarkan kepada perancangan yang telah dilakukan untuk projek ini. Pelayan digunakan untuk menangkap trafik rangkaian dan beberapa komputer digunakan untuk menghidupkan *botnet* untuk trafik DNS *botnet* dan computer juga digunakan untuk servis *windows update* untuk trafik DNS yang normal. Terdapat beberapa teknik untuk mengesan *botnet,* pendekatan yang digunakan untuk mengesan *botnet* di dalam projek ini adalah teknik *anomaly-based.* Trafik rangkaian akan ditangkap untuk kedua-dua rangkaian DNS *botnet* dan rangkaian DNS yang normal. Tiga jenis trafik rangkaian yang berbeza yang akan ditangkap adalah rangkaian DNS *botnet,* rangkaian DNS yang normal dan gabungan antara rangkaian DNS *botnet* dan rangkaian DNS yang normal. Analisa akan dilakukan berdasarkan kepada trafik rangkaian yang telah ditangkap dan kriteria yang terlibat adalah masa *botnet* aktif, bilangan NXDomain dan CNAME *rcode* untuk respon kepada pertanyaan dan waktu untuk *botnet* menghubungi pelayannya di pelayan DNS. Untuk mendapatkan gambaran yang lebih jelas untuk respon pertanyaan DNS, graf direka untuk rangkaian *botnet* dan juga rangkaian yang normal di dalam fasa analisa. Percubaan dilakukan untuk membuat perbandingan data di antara analisa dan juga data percubaan. Sebagai kesimpulan, kesemua objektif untuk projek ini tercapai dengan sempurna.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACRONYM	WORD
Botnet	Robot Network
Botmaster	Owner of a bot
DNS	Domain Name System
DDNS	Dynamic Domain Name System
NXDomain	Non-Existent Domain
CNAME	Canonical Name
DDoS	Distributed denial-of-service
C&C	Command and Control
IRC	Internet Relay Chat
P2P	Peer to Peer
IP	Internet Protocol
LAN	Local Area Network
RCODE	Reply Code
SPAN	Switched Port Analyzer
NetBIOS	Network Basic Input/Output System
Email	Electronic mail
IOS	Internetwork Operating System
QoS	Quality of Service

CHAPTER I

INTRODUCTION

1.1 Project Background

When the internet become more efficient, provide more reliable services and can store private data, it will attract the intruder to attack them using many types of method depends on the mastermind of the attacker. In today environment, botnet is considered as major problem to the internet because it is harmful and can cause the network cannot function or botnet capable to sniff secret information of user on the internet. Botnet is difficult to stop and detect because it is control by the botmaster.

Software robots or bots can operate automatically and autonomously meaning that it can be controlled remotely by the developer from its server that is from another network. It also calls as Botnet when it is form a group of them and uses command and control infrastructure. They only do task that command by its server and the aim or objective of attack can be change at any time. One of the most dangerous attacks on the internet is botnet because they can spread itself very fast over the network. It also can make them invisible to make them hard to detect and destroy.

Botnet communicate among them using unique encryption scheme to make sure that they cannot be detected and prevent intruder to enter their network. There are many types of botnet depends on their originator and what are their missions. Botnet will attack the target network or user by using several methods such as denial of service attacks, adware, spyware, fast flux, email spam and so on. Those techniques are differing from each other because each technique has its own implementation method.

Today pattern of the botnet command and control server make Internet Relay Chat (IRC) server to act as their server to control their botnet over the network. Host that had been attacked with the botnet will access the botnet server using their domain name to retrieve command that need to be executed. The DNS servers will response with the request because it does not know that the request is made by botnet and also does not know either the request made by legitimate host or not.

Number of request to resolve domain name at the DNS server made by the botnet at one time is too many if compared with the request made by the legitimate host. This is because botnet will make request for their domain name at the DNS server continuously but legitimate host will make when necessary to resolve their request. Sometimes the DNS server will down because cannot respond with a lot of number at one time.

Aim for this project is to analyze the DNS traffic for the difference between botnet behavior and normal network activity. This project will analyze how many times botnet made request at the DNS server to resolve their domain name for a period of time. Besides that, number of normal network request at the DNS server also will be analyzed and comparison will be made for the two types of requests.

Packet for the botnet and normal network must be captured first before analysis can be made to identify the difference between them. A lab needs to be setup to locate all required node to run the project such as server, workstations, switch, modem and so on. Internet is needed to make the botnet inside the network to request DNS server to resolve their domain name. Not forget the normal network also will be access to the network to make request at the DNS server.

From the botnet captured packet, analyze will be made for number of request at a period and number for DNS respond which is NXDomain. NXDomain means botnet had been made request for domain that not exist in the internet. This happen might because the server has been migrate to new domain name. For the normal network, only number of request made by them will be focused on.

Finally when all required information and data are found and collected, analysis can be made to identify the difference between botnet behavior and normal network activity at the DNS server when communicate with it. Graph of the transaction for both activities at the DNS server will be produced to get clear information about the number of request made and number of reply from the DNS server.

1.2 Problem Statements

Nowadays, internet become not safe anymore because of there are many threat to it such as worm, backdoor, intruder and many more that can give bad effect to the network environment and also the user on the internet that always communicate with each other. One of the most important services on the internet is DNS that provide domain name to IP address translation also had been attacked by one of the threat named botnet.

Botnet will act as legitimate host and request for DNS traffic to access abnormal type of domain name that produce by the botmaster which controller the botnet activity. Botnet will request many number of domain name translation and the continuous request will make the DNS server become busy, after a period the DNS server can down because cannot process a lot of request make by them.

This project will monitor the DNS traffic to detect the normal and abnormal DNS traffic. Normal DNS traffic is network that clean from any botnet and abnormal traffic usually network that contain botnet inside them. From the abnormal traffic, maybe there are request make by the botnet that comes from some of them in some period.

Botnet like to make request at the DNS server with a lot of number at a time compared to the normal network usually make request at the DNS server only when they need and only in small number. This project will analyze the number of request for domain name translation at the DNS server made by the botnet and the normal network for a period of time and then comparison between them will be made.

There are many type of respond DNS server can provide for the request made by the host. Botnet normally will receive respond from the DNS server which is NXDomain because botnet domain name server had migrated to another domain name or it no longer exists. Output will be produced to show the number of NXDomain receive by the botnet from the DNS server for request they had been made before for a period of time.

1.3 Objective

Internet in now era becomes not safer anymore because there are many intruders that try to attack network or host on the internet because of many reasons depends on the attackers. One of the most popular intruders in the network is botnet that can act as legitimate host to make request for DNS query at the DNS server. Every research has their own objective to achieve to ensure they have something to meet and my objectives make research on this topic are stated below, there are:

To study the botnet activity at the DNS server when make transaction by identify the normal and abnormal DNS traffic. When the normal and abnormal DNS traffic identified, how the botnet activity is like about can be know.

To compare the normal DNS traffic and abnormal botnet traffic, when the packet on the network captured, it will contain both normal and abnormal packet. Then this project will compare the differences between them and make comparison based on the packet information.

To study the time interval of the botnet captured packet. When got the abnormal traffic, how many the botnet make request for their domain will be studied by refer to the time interval of the botnet request.

To study what will happen to the specified DNS server when there is botnet activity is running. Rumors said that when botnet attack the DNS server, the server cannot process the entire request make by them because there are too many invalid request that want to resolve not active domain.

1.4 Scope

There are many types of internet intruder but this research will focus only on the botnet. This project will concentrate on the packet that contains normal and abnormal DNS traffic by capturing the entire DNS flow packet on a network. Other than that, this project will also make attention on the botnet activity by focus on how the botnet try to connect to their botmaster.

The packet that will be captured only packet that flow in the security lab and made by the workstation inside the network. Other packet that come from outside the specified location, the packet will not be captured.

Reply code from the DNS server there are many types but this project will only focus on NXDomain only when produce the output. The output will produce a graph that will show the reply from the DNS server for each request.

1.5 Project significance

This project is important for the internet user by define what is botnet is actually about and how does they operate in the network. This project can make they become more cautions with botnet after this by prepare network shield such as firewall for their network to prevent from being entered with this intruder. Besides that it is useful for the network admin to ensure that their DNS server is not being attack by the botnet. When DNS server is being attack by the botnet, the DNS server can become slower and cannot function at optimum because it needs to responds with the not legitimate request. They can always monitor their network flow and take precautions move.