Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Critical Investigation of Botnet

By Rathod R.P., Bhalchandra P.U., Dr. Khamitkar S.D & Lokhande S.N.
SRTM University's Sub Center, Latur (MS), India

Abstract - A Botnet is a network of compromised hosts, called as bots that are used for malicious activity. These bots are then controlled by single master termed as Botmaster. A Botmaster may inject commands though any bot to launch DDoS attack. In this paper, we have demonstrated the behavior of Botnet on network in real time Internet environment.This will be helpful for researcher to detect the different types of emerging Botnet.

Keywords : *network security, botnet, denial of service attack.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

A Critical Investigation of Botnet

Rathod R.P. [α], Bhalchandra P.U. [σ], Dr. Khamitkar S.D [ρ] & Lokhande S.N. [ω]

Abstract - A Botnet is a network of compromised hosts, called as bots that are used for malicious activity. These bots are then controlled by single master termed as Botmaster. A Botmaster may inject commands though any bot to launch DDoS attack. In this paper, we have demonstrated the behavior of Botnet on network in real time Internet environment. This will be helpful for researcher to detect the different types of emerging Botnet.

Keywords : network security, botnet, denial of service attack.

I. Introduction

A Botnet is large group of compromised hosts known as bots. Symantec [1] defines a bot as "Bots are similar to worms and Trojans, but earn their unique name by performing a wide variety of automated tasks on behalf of their master". The bots are also known as zombies. . The Botnet are used for different attacks such as DDoS, spamming, phishing, sniffing, etc. These bots are controlled by a Botmaster through the command & control (C&C) mechanism as shown in figure 1. Based on this C&C mechanism Botnet can classified into IRC, P2P and HTTP Botnet.

II. Command & Control (C&C) Mechanism

The Botmaster uses the C&C mechanism to control the bots .This mechanism states the how Botmaster to assign the commands to the bots. The C&C mechanism classified into centralized, P2P, IRC, and HTTP.

a) Centralized

This is the most widely used mechanism by the Botmaster. In this mechanism, a central server is used communication with bots. The commands are downloaded by the bots known as pull or sent to bots known as push. In push style the bots directly controlled by the Botmaster. While, in case of pull style Botmaster does not have direct control bot has to received the commands by interacting with C&C server periodically [2]. The IRC and HTTP protocols are widely used by this mechanism.

b) P2P Mechanism

As the name implies there is no central server. The bot acts as client and server to form Botnet; hence the detection is harder compared to other Botnet. If one bot is removed still other bots continue the communication which gives more flexibility for Botnet.

Author α : SRTM University's Sub center, Latur (MS), India.
E-mail : srtmun.parag@gmail.com
Authors σ ρ ω : School of Computational Sciences, SRTM University, Nanded, MS, India.

c) IRC (Internet Relay Chat)

This is the most popular and old mechanism used by the Botnet. The bots are connected to IRC server using IRC protocol. Bots communicates though push mechanism and they chats with each other with the help of commands.

d) HTTP

Here the commands are not sent directly to the bots, instead it leaves malicious program on a web server and bot uses the pull mechanism for commands.

III. Botnet Existence Phases

a) Preliminary Infection and Transmission

Botnet are formed though a vulnerable hosts. The Botmaster gain the access of infected host using different techniques such as operating system or application vulnerability. The Botmaster also uses the websites, emails as a spreading channel. When the user click on website link of opens an email the bot get installed on a victim's machine and become part of Botnet. [3]

b) C&C Server Actions

When the bot get installed on the Botmaster uses the pull or push methods for communication with bots. The C& C server controls the bots though IRC channel. The bot get connected to IRC server with a nickname and then it join to Botnet.

c) Accepting Instructions

When the bot joins the IRC Server Botmaster sends instructions to the bots. These instructions include commands which are used for various malicious activities or attacks.

d) Disseminations using other hosts

The Botnet spread though the vulnerable hosts, so the Botmaster uses C&C server to search such a host to become a part of Botnet.

IV. Case Study: IRC Botnet

IRC Botnet is the most popular Botnet which uses the centralized mechanism to control the bots. This Botnet uses the IRC channel for communication and controlling the bots. We have tested in a secure environment to avoid infection to other unwanted hosts.

We have used a bot which performs different tasks and attacks such as port scanning, port scanning, UDP flood, TCP flood, http flood, SQL flood etc.

When the bot connect to IRC server he/she joins the channel where other users are already login by nicknames. When a user submits the messages to IRC server publically the other user can see her/his messages on the channel [4]. IRC include list of channels a user can join any channel though an IRC chat client by channel name.

IRC server commonly uses the port 6667 where user gets joined to IRC server. The channel administrator handles all the users. The user can use the commands as follows:

1. JOIN: Joins a channel
2. PASS: set or send a password
3. QUIT: Exit a channel
4. SEND: Send the file to another IRC user
5. RAW : Will do the raw scan
6. JUMP: Jump to another IRC server
7. QUIT: Quit the channel

a) Experiment Setup

Our experiment consists of one IRC server hosted on cloud server with Ubuntu 12.04 and two dummy servers working as bot all are connected in real time Internet environment as shown in following figure 1. We have installed packet capturing tool 'tcpdump' on these servers. The client is installed with Xchat software for joining the channels on IRC server.

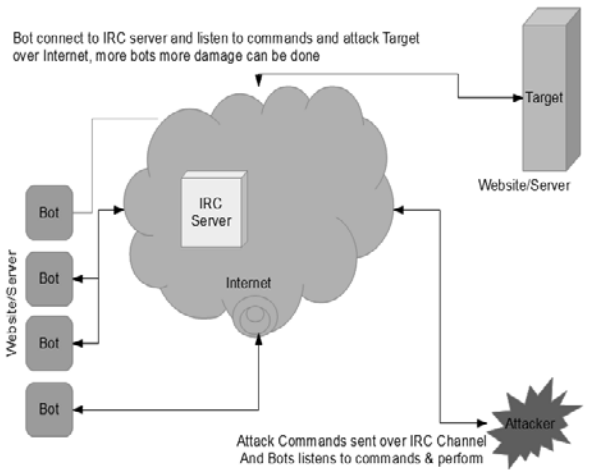

Figure 1 : Experimental Setup for Botnet Attacks

When the user joins a channel on IRC server, he/she become the channel operator. When the bot is setup on victim's machine from IRC server, the Botmaster tries to hide it's identity from IRC Server by using node commands [4]. The user joins the channel by using user name. First we have collected the network traffic with the help of 'tcpdump' and then converted to CSV for further analysis.

We have tested the bot to obtain the actual working of bot and Botmaster. In this experiment bots are controlled by using the commands and launch

We have tested the bot to obtain the actual working of bot and Botmaster. In this experiment bots are controlled by using the commands and launch different attacks. The network traffic contains traffic from IRC to bot and other hosts in the network.

b) Flow Characteristics

Our experiment contains over 260000 packets with the flow characteristics shown in below table1. We have filtered this traffic to separate normal or legitimate and Botnet traffic. During the experiment the protocol hierarchy statistics is shown in the following table 2.

Name of Field	Filed Details
Source	Source IP address
Destination	Destination IP address
Protocol	Name of protocol
Length	Packet Length in bytes
Info	Information about packet

Table 1 : Flow Characteristics

Protocol	% Packets	Packets
Transmission Control Protocol	54.1 %	142640
SSH Protocol	0.10 %	270
Internet Relay Chat	7.50 %	19748
Virtual Router Redundancy Protocol	4.75 %	12524
User Datagram Protocol	7.38 %	19443
Domain Name Service	5.10 %	13441
Drop box LAN sync Discovery Protocol	0.58 %	1534
NetBIOS Name Service	1.43 %	3766
Internet Control Message Protocol	0.02 %	45
IP v6	0.01 %	33
SMB	0.18 %	462
Internet Group Management Protocol	0.16 %	415
Address Resolution Protocol	29.20 %	76943
Logic-Link Control	2.24 %	5907
Spanning Tree Protocol	2.17 %	5715
Cisco Discovery Protocol	0.07 %	192
IP V6	2.10 %	5545
DHCP V6	1.18 %	3098
Domain Name Service	0.84 %	2208
HTTP	0.03 %	66
ICMP v6	0.07 %	173

Table 2 : Protocol Hierarchy Statistics

c) Bot Communication

When the bot join the channel the Botmaster controls the bot, the captured traffic by Wireshark is shown in following figure 2. The victim joins using port 6667. It is observed that the packet length of Botnet traffic is within the range of 50~500 bytes.

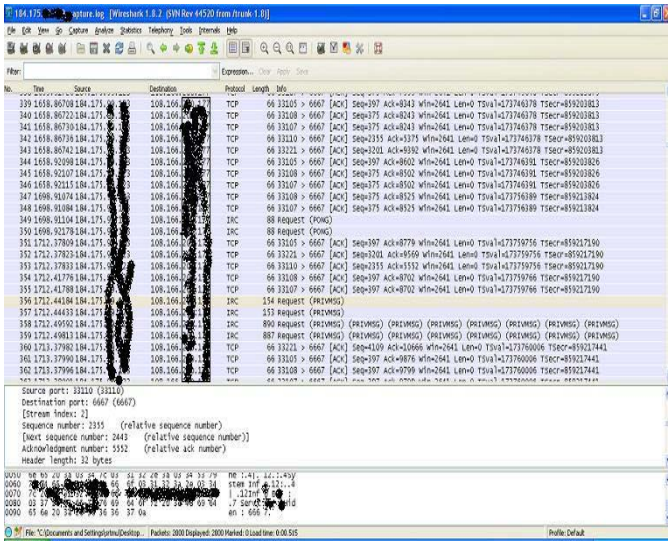

Figure 2 : Result Analysis

V. Conclusion

Botnet are emerging threat with hundreds of millions of computers infected. A study of Zhaosheng Zhu, Northwestern University, USA, shows that about 40% of all computers connected to the internet in the world are infected bots and controlled by attackers. Our paper experimentally shows the behavior and understanding of Botnet attacks. Understanding Botnet, detecting and tracking Botnet, and defending against Botnet is need of time. While Botnet are widespread, the research and solutions for Botnet are still in their infancy.

References Références Referencias

1. Symantec. Crime ware: Bots. http://www.symantec.com/avcenter/cybercrime/bots_page1.html, 2008.
2. Dittrich, D., Dietrich, S.: P2P as Botnet command and control: a deeper insight. Applied Physics Laboratory University of Washington, Computer Science Department Stevens Institute of Technology (2008).
3. S. Racine. Analysis of Internet Relay Chat Usage by DDoS Zombies. Master's Thesis. Swiss Federal Institute of Technology, Zurich. April 2004.
4. M. Overton. Bots and Botnet: Risks, Issues and Prevention. In Proceedings of Virus Bulletin Conference 2005. Dublin, Ireland. October 5-7, 2005.

This page is intentionally left blank