Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Botnet: Understanding Behavior, Life Cycle Events & Actions

P. S. Lokhande *
Asst. Professor (IT),
MGMCET, Navimumbai, India

B. B. Meshram
Professor (Computer Engg.),
VJTI, Matunga, Mumbai, India

Abstract*— This paper examines botnet behavior and provides the basis for the development of an application tool used to investigate the properties of botnets in large-scale networks. Botnets are breaching security and data safety and are used by hackers for initiating various cyber-attacks. Botnet causes various problems such as information search and theft, denial of service attack, sending SPAM e-mail, and so on. The purpose of this paper is to study basic details of security threats that users of Internet are facing from malicious botnets. There is a need to develop effective mechanism for detecting and mitigating the malicious behavior of botnets. This study helps: (i) To understand behavior of bots and Botmaster. (ii) To study botnet topologies, behavior, lifecycle events and actions; and (iii) to study preventive steps to stop the botnet attacks.

***Keywords*— Botnet, Bot, Botnet Maker, Botmaster, Botnet Detector, Zombie, IRC, DDoS, Spam, Internet Security, Bot Hunter, WebSecurity**

1.0 INTRODUCTION

The dictionary meaning of Bot is "(Computing) an automated program for doing some particular task, often over a network [1].

A botnet is a common term derived from the phrase robot network. A bot is simply an automated computer program. One can gain the control of your computer by infecting them with a virus or other malicious code gives the access. Botnets are one of the most sophisticated and popular types of cybercrime today. They allow attackers to take control of many computers at a time, and turn them into "zombie" computers, which operate as part of a powerful "botnet" to spread viruses, worms, generate spam, and commit other types of online crime and fraud. Botnets generally use DDoS type of attack against an Ecommerce sites. Computers contain information that is incidental to the crime such as a database containing the payment receipts list [2]. Some of their uses include launching distributed denial-of-service (DDoS) attacks, sending spam, Trojan and phishing email, illegally distributing pirated media, serving phishing sites, performing click fraud, and stealing personal information, among others. Due to their sheer volume, diverse capabilities, and robustness they pose a significant and growing threat to the Internet as well as enterprise networks [3]

1.1 Botnet Background

Many botnet families have their roots in beneficial utilities that were developed to manage Internet Relay Chat (IRC) networks. IRC is a real-time Internet chat protocol, designed for group (manyperson -to-manyperson) communication. IRC was designed to provide Internet users around the world with a casual way of communicating with each other in text–based discussion forums called *channels*. A typical IRC network is comprised of a number of servers in various locations. Channels are administered by channel operators, who can take actions such as muting or ejecting unruly users. To extend the functionality of IRC, some channel operators used automated scripts—the original IRC bots—to perform functions such as logging channel statistics, running games, and coordinating file transfers. As the popularity of IRC communities grew and the number of servers increased, so did the number of conflicts between users, which led to battles over the control of popular channels. IRC is structured so that when all of the designated channel operators disconnect from a channel, another member of the channel is automatically assigned as the new operator. In an effort to gain control of a channel, some malicious users created scripts that could perform denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks against IRC servers. By targeting the server used by a specific channel operator, these scripts could force the operator offline so that the attacker or someone else could gain operator status. Eventually, these same bots were used to target individual users. One of the earliest malware families to make use of IRC as a means of *command and control* (C&C) was a mass-mailing worm called Win32/PrettyPark, which appeared in 1999. [5]

1.2 How a botnet works?

Bots gain access into a person's computer in many ways. Bots distribute themselves over the network by finding highly vulnerable, unprotected computers to infect. When they find an unprotected computer, they infect the computer and then communicate to their master (Botmaster). They will stay hidden until they are instructed to carry out a particular task. Most botnets are designed as distributed-design systems, with the main botnet operator (Botmaster) issuing command instructions directly to a small number of systems. These machines propagate the command instructions to other

compromised machines (zombie machines), usually via Internet Relay Chat (IRC) . The most common type of self propagating malware technique, being used in the past for some time now was the IRC Based Botnet. [7]

The components of a typical botnet include a server program, client program for operation, and the malicious program that embeds itself on the victim's machine (bot). All three of these usually communicate with each other over a network and may use encryption for stealth and for protection against detection or intrusion into the botnet controlled network [8].

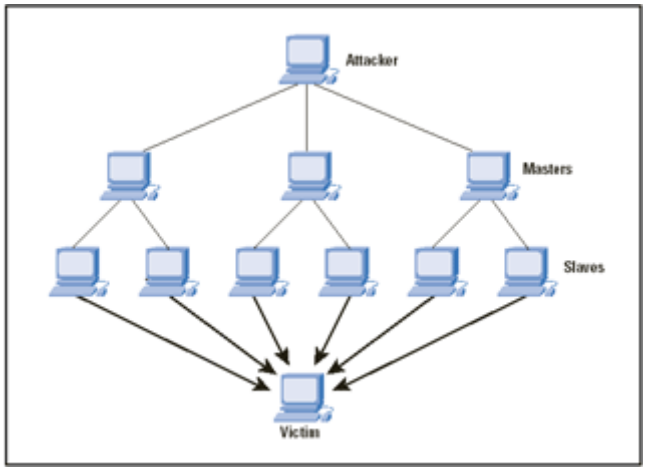

Fig 2.1: Working of botnet using DDoS Attack [9] Source CISCO The Internet Protocol Journal

Originally, botnets were used for distributed denial of service (DDoS) attacks. (See Figure 2.1). When infecting a target computer, the bots connect to IRC servers on a predefined channel as visitors and waited for messages (i.e. commands) from the Botmaster. The Botmaster could come online at any time, view the list of bots, send commands to all zombie (infected) computers at once, or send a private message to one zombie machine. This is an example of a centralized botnet [4]. (See figure 2.2)

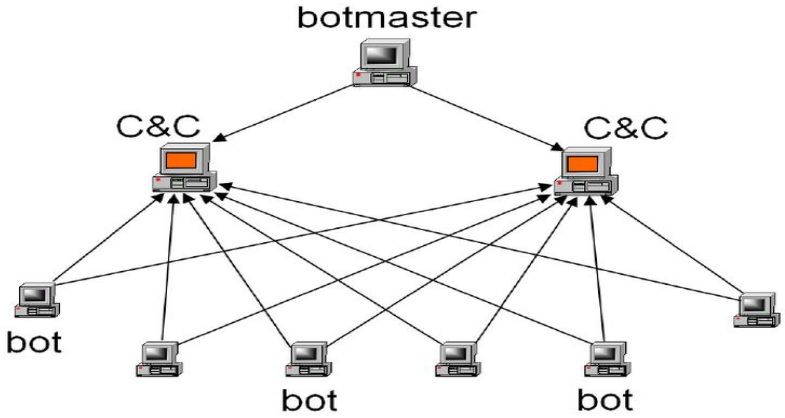

Fig 2.2 C&C issues commands to Bots [4]

1.3 How are botnets used?

Botnets can be used by cyber criminals to conduct a wide range of criminal activity, from sending spam to attacking government networks.

i) Sending spam: This is the most common use for botnets. Experts estimate that over 80% of spam is sent from zombie computers. It should be noted that spam is not always sent by botnet owners: botnets are often rented by spammers.

It's the spammers who understand the real value of botnets. According to Kasprasky Lab data, an average spammer makes $50,000 – $100,000 a year [10].

ii) Blackmail: The second most popular method of making money via botnets is to use tens or even hundreds of thousands of computers to conduct DDoS (Distributed Denial of Service) attacks. This involves sending a stream of false requests from bot-infected machines to the web server under attack. As a result, the server will be overloaded and consequently unavailable. As a rule, cyber criminals demand payment from the server's owner in return for stopping the attack.

iii) Anonymous Internet access: Cyber criminals can access web servers using zombie machines and commit cyber crimes such as hacking websites or transferring stolen money.

iv)Phishing: Addresses of phishing pages are often blacklisted soon after they appear. A botnet allows phishes to change the addresses of phishing pages frequently, using infected computers as proxy servers. This helps conceal the real address of the phishes' web server.

v) Theft of confidential data: A bot used to create a zombie network can download another malicious program, e.g., a password stealing (PSW) Trojan, and infect all the computers on the botnet with it, providing cyber criminals with passwords from all the infected computers. Stolen passwords are sold or used for mass infections of web pages [10].

This study is arranged in to two tasks. The first task was to learn the behavior of bots and botnet controllers. This helps us understand the behavioral patterns of botnets. The second task is to use this information to study botnet topologies, lifecycle events and actions.

This paper is organized in following manner. Section 2 presents Botnet background information. Section 3 reviews literature related to Botnet. Section 4 Focuses on Life Cycle of Botnet and Botnet Detection, Prevention and Destruction presented in section 5. Section 6 present conclusions and recommendations for future work respectively.

2.0 MOTIVATION

Literature review discusses the current research that has been published about botnets. We first identify the motivations behind building and operating botnets and how these motivations have evolved over time. Then, we discuss the current research on how to track and disable botnets.

2.1 Botnet Motivation: Botnet Commerce

Attackers have developed a number of different ways to make money with botnets,. Bot-herders might choose to attempt these activities individually, or they might return to a black market forum and advertise the services of the new network. These black market forums are online communities that bring sellers of malware and services together with interested buyers [5].

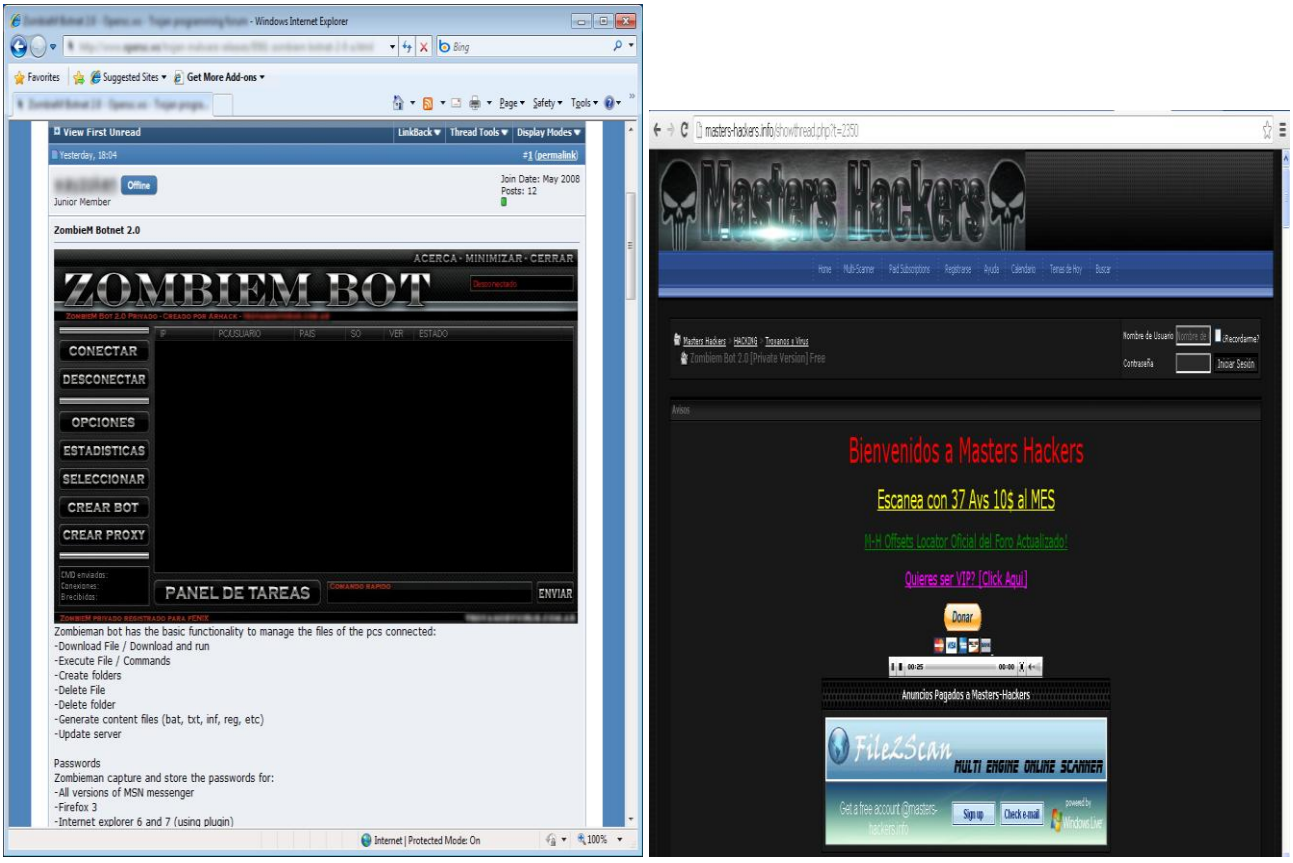

Fig 2.1: Criminals Sell botnet S/W and Services in online Blackmarket

As Internet users began to shop and do the banking transaction online, the nature of malware shifted from disrupting service to exploiting these technologies for financial gain. Malware may be used to steal sensitive information such as credit card numbers, social security numbers, and passwords. It sends the information harvested to the Botmaster. The Botmaster may use the information for further attacks or may sell it to other criminals. Other criminals may use the information for nefarious activities including identity theft. (See Figure 2.2)

Primary motivation for operating a botnet is the money that can be earned from sending *spam email*. Ferris Research has found that email spam costs businesses over $130 billion a year worldwide—$42 billion in the U.S. alone [11]. Another popular source of income for online criminals is the installation of advertising software, known as adware, on victim systems. Many adware software companies offer monetary incentives for installing their software [3]. Phishing schemes are also a major revenue generator for botnet operators.

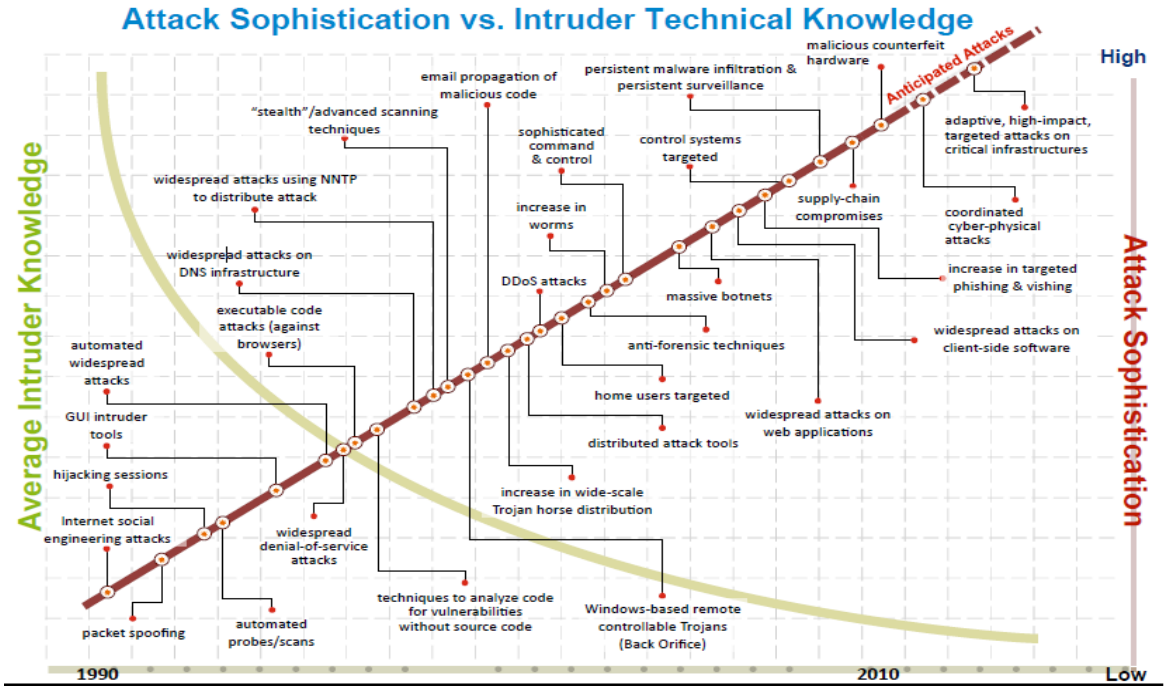

Fig 2.2 Attack sophistication vs. Intruder Technical Knowledge, Source: Software Engineering Institute, Carnegie Mellon-2010

2.2 Detecting Botnets

As the botnet problem arises, security experts have begun to develop ways to detect and monitor the behavior of botnets to gather intelligence that might prove useful in future research.

Detecting malicious activity on a network is difficult. The attacker can hide their presence on a machine and only become active under certain conditions. Some vendors publish their findings about detecting botnets but this information is not always enough to effectively track, disrupt, or mitigate botnets.

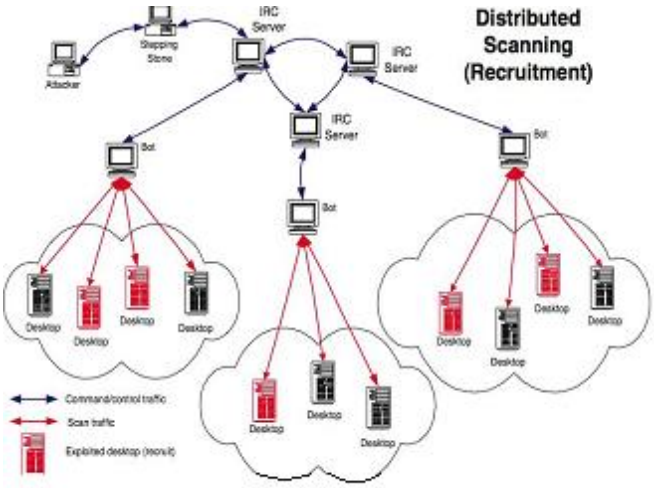

Fig 3.3 Tracking a Botnet

3.0. LIFE CYCLE OF BOTNET

The infected machine is called a zombie. Once a host is infected, it downloads the bot binary source from a remote server and installs automatically. The bot then looks up for the address of IRC servers by DNS Lookups. These IRC servers are called Command and Control (C&C) servers. On obtaining the C&C server's address, the bot then logs into it and authenticates itself as a part of the particular botnet. The bots can then update their bot software; this is usually functionalities added to the bot software, if an update were available and add more C&C servers. IRC servers are used for C&C by bot masters is due to the following reasons.

- •Easy to implement & install i.e. private network can be installed easily.
- •Ease of control i.e. using features like username, passwords.
- •Interactive i.e. two way communication between bot master and zombie machine is possible.

These zombie computers, when it is up and connected to the Internet, will log into the C&C server and wait for bot master's commands. Bot master logs into the C&C and can issue commands for the bots to perform.

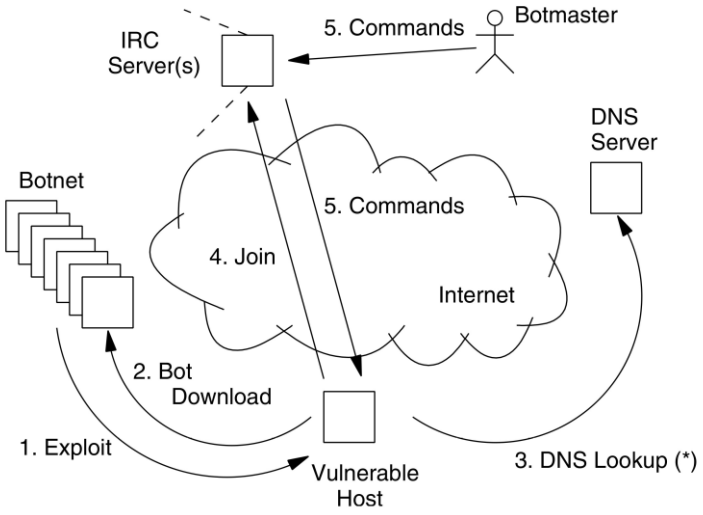

Fig 3.1: Lifecycle- 1 Exploit>Bot download>DNS Lookup>Connect to IRC server>Command from Botmaster [12]

3.1 Types of Botnet

Botnet classification is straight forward, and uses botnet architecture the protocols used to control bots as a basis.

Classification of botnets according to architecture

There are currently only two known types of botnet architecture.

i) Centralized botnets. In this type of botnet, all computers are connected to a single command-and-control center or C&C. The C&C waits for new bots to connect, registers them in its database, tracks their status and sends them commands selected by the botnet owner from a list of bot commands. All zombie computers in the botnet are visible to the C&C. The zombie network owner needs access to the command and control center to be able to manage a centralized botnet.

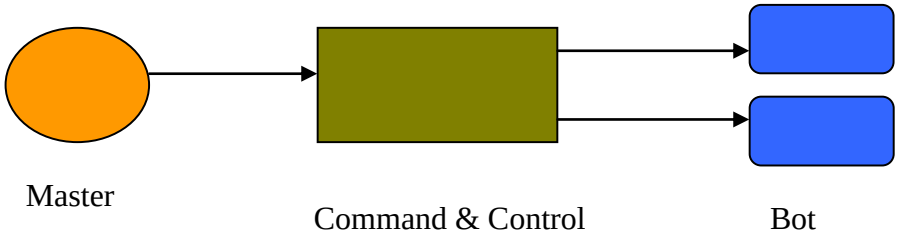

Fig. 3.2: Centralized Topology (C&C)

ii) Decentralized or P2P (peer-to-peer) botnets. In a decentralized botnet, bots connect to several infected machines on a bot network rather than to a command and control center. Commands are transferred from bot to bot: each bot has a list of several 'neighbours', and any command received by a bot from one of its neighbours will be sent on to the others, further distributing it across the zombie network. In this case, a hacker needs to have access to at least one computer on the zombie network to be able to control the entire botnet.

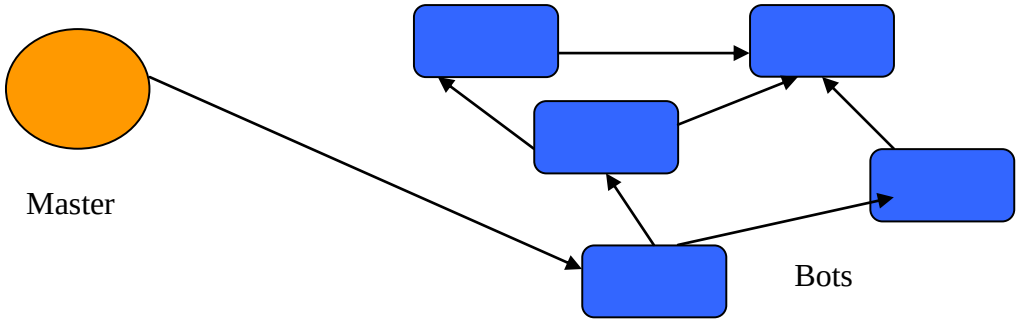

Fig:3.3. Decentralized or P2P (peer-to-peer) botnets

3.2 Classification of Botnets According to Network Protocols

Botnets can be divided into the following classes when classified according to network protocols:

i) IRC-oriented.: bots were controlled via IRC (Internet Relay Chat) channels.

ii) IM-oriented. It uses communication channels provided by IM (instant messaging) services such as AOL, MSN, ICQ etc.

iii) Web-oriented: A bot connects to a predefined web server, receives commands from it and transfers data to it in response.

iv) Other: In addition to the botnet types listed above, there are other types of botnets that communicate via their own protocol that is only based on the TCP/IP stack, i.e., they only use transport-layer protocols such as TCP, ICMP and UDP [14].

4.0 BOTNET DETECTION, PREVENTION AND DESTRUCTION

Defense against bots infection & attack could be classified in three stages prevention, detection & response

i) Detection stage: the measures user and sys-admin could employ to identify a malicious bots activity on machine or in network.

ii) Prevention stage: recommends the measures a user or admin could take to prevent their system or network from bots infection.

iii) Response stage: recommends the action that user, sys-admin could take in response to bots infecting machine or network.

Following are the techniques were identified from a survey of experts among different stakeholders working in the field of botnet mitigation, they are listed as follows.

4.1 Detection Techniques [13]

1) Passive Techniques: In passive techniques data is gathered solely through observation. By monitoring, activities can be tracked without interfering with the environment or tampering with the evidence.

2) Active Technique: approaches that involve interaction with the information sources being monitored

Table 4.1: Botnet detection techniques

Sr. no	Techniques	Types
1	Passive Techniques	Packet Inspection
		Analysis of Flow records: Network data stream. Source and destination address
		DNS based approaches
		Analysis of Spam records
		Analysis of Log files
2	Active Techniques	Sinkholding: Cutting off malicious control source from the rest of botnet.
		Infiltration: Dividing bots in S/W and H/W based techniques
		DNS Cache snooping: DNS server queried for malicious request.

4.1.1 Tools for Botnet Detection

Sr. No	Tools
1	IDS, BotHunter : developed by labs of SRI International, the Army Research Office and the National Science Foundation
2	The network protocol "NetFlow" from Cisco Systems.
3	Snort: Plugins SLADE and SCADE
4	Spam email templates, DNS tracking
5	Honey pots, spamtraps
6	Penetration testing tools

4.2 Prevention Techniques: Preventing a system on Internet from falling victim to a botnet requires a high level of awareness about online security and privacy.

1) Port 25 Blocking: Port no 25 is widely used for spreading spam, thus blocking it will prevent bot spreading.

2) Protecting ISPs customers by implementing walled gardens

3) Infiltration and remote disinfection: Taking control of the infected machine remotely and process the disinfection operation.

4.2.1 Botnet Prevention Tools

Sr. No	Tools
1	Websense,
2	Symantec
3	Cyveillance
4	Kaspersky lab tools

4.3 Response Stage (Countermeasures):

i) Blacklisting botnet: Can be done via real-time push service of ISP
ii) BGP Blackholing: Allows selective black holing
iii) DNS Based countermeasure: DNS Sinkholding, DNSCache Snooping
iv) Packet Filtering on network and application level: Transparent monitoring and detection.

5.0 CONCLUSION AND FUTURE SCOPE

The purpose of this paper is to list down and document Internet Security threats posed by botnets. Today, botnets are among the main sources of illegal income on the Internet and they are powerful weapons in the hands of hackers. Now a day's botnets increasingly spreading over the internet they are becoming easier and easier to use The paper presents a study of technology and methods involved in the design and control of botnets and threats posed by them. The main focus of this paper is Botnet which enfolds all other attacks in one way or the other.

Future Scope

This study was limited to understand the Botnet, their types, mechanisms and various techniques to deal with it. Further research efforts may focus on the following problems to extend this study.

1) Designing the web browser level bot detection, prevention and destroy technique useful for a common man who don't know the IDS, IPS and Honey pot etc.
2) Build data repository of all botnets with respective data samples, which can be used as a sample data to test.
3) Exploring the possibility to design anti-bot application similar to the antivirus used today.

References

[1] Nina Godbole, Sunit Belapure, "Cyber Security : Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", wileyindia, ISBN: 9788126521791, 2013 edition
[2] P. S. Lokhande, B. B. Meshram; "Learning from Past Intrusion Attacks: Digital Evidence Collection to Make E-commerce Systems more secure.", ICL 2009 Proceedings ,Conference ICL2009 September 23-25, 2009 Villach, Austria
[3] Anestis Karasaridis, Brian Rexroad, David Hoeflin, "Wide-scale Botnet Detection and Characterization", AT&T Security and AT&T Labs
[4] Ping Wang Sherri Sparks Cliff C. Zou , "An Advanced Hybrid Peer-to-Peer Botnet", School of Electrical Engineering and Computer Science University of Central Florida, Orlando, FL
[5] Accessed online Microsoft security Intelligence report: http://www.microsoft.com/security/sir/story/default.aspx#!botnetsection_history
[6] Joseph Massi, Sudhir Panda, Girisha Rajappa, Senthil Selvaraj, and Swapana Revankar, "Botnet Detection and Mitigation", Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 7th, 2010
[7] Accessed online: http://what-is-what.com/what_is/botnet.html
[8] Accessed online: http://en.wikipedia.org/wiki/Botnet
[9] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, "Distributed Denial of Service Attacks", The Internet Protocol Journal - Volume 7, Number 4
[10] Vitaly Kamluk, "The botnet business" Securelist, Kaspersky Lab http://www.securelist.com/en/analysis/204792003/The_botnet_business?print_mode=1
[11] Ferris Research (2009), Industry statistics. Retrieved October 31, 2009 from http://www.ferris.com/research-library/industry-statistics/
[12] http://rise.cse.iitm.ac.in/wiki/images/9/98/Botnet_report.pdf
[13] Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder, " Botnets: Detection, Measurement, Disinfection & Defence", European Network and Information Security Agency (ENISA), 2011
[14] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna, " Your botnet is my botnet: analysis of a botnet takeover", In *Proceedings of the 16th ACM conference on Computer and communications security* (CCS '09). ACM, New York, NY, USA, 635-647. DOI=10.1145/1653662.1653738 , http://doi.acm.org/10.1145/165366

