Conceptual Study of Botnet

[1] Dr.Jitendra Singh Chauhan, [2] Mr. Devendra Suthar, [3] Mr. Sandeep Bordia
[1]Associate professor & Head of Department, [2, 3]Assistant professor
Department of Computer Science & Engineering, Aravali Institute of Technical Studies, Udaipur, India
Email - [1]chauhan.jitendra@live.com, [2]dev_arya123@yahoo.com, [3]sandeep11d@gmail.com

Abstract: *with the rapid increment of data and variation in various technologies of the Internet communication has been accompanied by a rapid increment in the prevalence of intrusions and attacks. However, it is found that now a days there is a significant change in motivation for malicious activity has taken place over the past several years: from vandalism and recognition to the financial gain. Here is a new network known as BOTNET. The bot herder will send commands to the droves of compromised systems, which will gleefully obey. In this paper we study on various features of botnet.*

Keywords: *Botnet, C & C architecture, Content Delivery Networks (CDN), Domain Name System (DNS).*

1. INTRODUCTION OF BOTNET:

Botnet is a new concept in which a software which introduces viruses, worms, Trojan horses and root kits for propagation and hostile integration into a foreign system, providing the functionality of the compromised system to the attacker.

It provides a various features implementation to a controlling entity corresponding it which may be command-and-control server which is under the control of bot-masters or bot-headers, who are responsible to give commands using this server.

These days for cybercrime Botnets plays a major role. Without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal. [1]

One class of botnet architecture that is beginning to emerge uses peer-to-peer protocol, because of its decentralized control design, is expected to be more resistant to strategies for countering its disruptive effects.

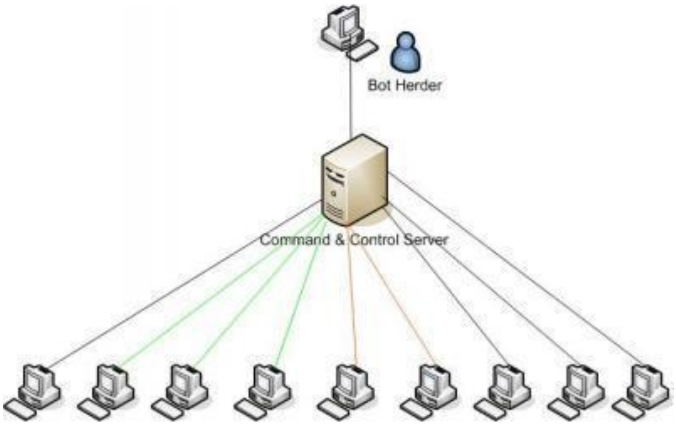

Fig: 1 Botnet network

2. CHARACTERISTICS OF BOTNET:

Bots has the most important characteristic that they form a network by connecting back to a central server after successfully compromising with the host system, and resulting in forming a network. This network is the so-called botnet. It provides a various features implementation to a controlling entity corresponding it which may be command-and-control server which is under the control of bot-masters or bot-headers, who are responsible to give commands using this server. The motivation for these activities is driven mostly by the financial interests of the bot-masters [2].

A. *Component of botnet structure:* The most important part of a botnet is the so-called command-and-control infrastructure (C&C). The instructions sets and their functionality widely vary with the operations they are going to perform. The only way to control bots is using C&C infrastructure. For efficient operation of bots they are required to maintain a stable connection.

Decentralised C&C Architecture: In decentralised command-and-control architectures, loosely coupled links between the bots enable communication within the botnet and provide the basis for its organization. Peer-to-peer botnets is the terminology used for this type of botnets, which represents the corresponding network model name. Also in other case, upon communication the revision number of bots will be exchanged and leads older bots to be updated to the newer version. This process will leads to the localisation of the bot-master almost impossible. This provides a high degree of anonymity. It is very difficult to monitoring and follow such activities. There is at least one known case, the Spam Through botnet [3] in which as a backup channel peer-to-peer functionality was used.

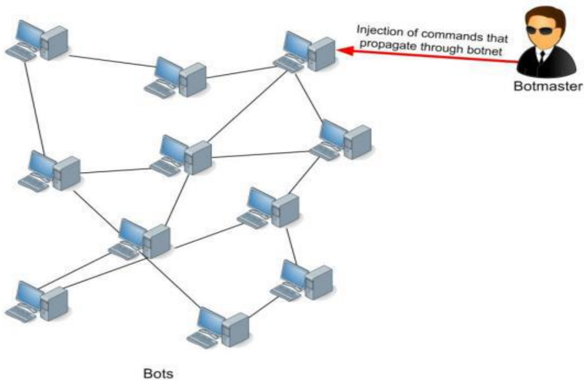

Fig 2 Decentralised C&C architecture

B. *DNS for Botnet:* For centralised approaches, the Domain Name System (DNS) has an important role, as it allows changes to the C&C infrastructure to be performed dynamically. While using DNS the command-and-control server is used to resolve DNS to its corresponding IP address. The new concept called fast- flux compared with Content Delivery Networks (CDN), is shown in figure 3.

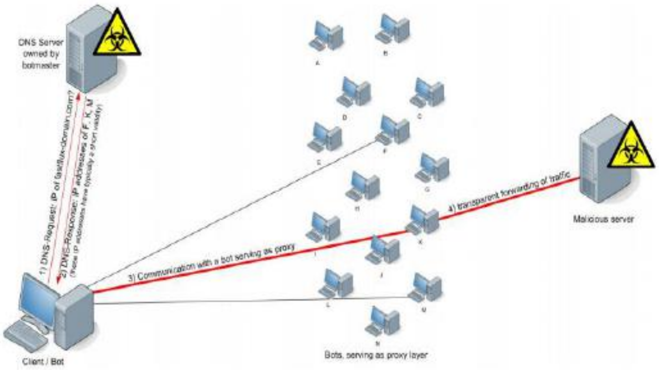
DNS Server owned by botmaster
1) DNS-Request: IP of fastflux-domain.com?
2) DNS-Response: IP addresses of F, K, M (these IP addresses have typically a short validity)
3) Communication with a bot serving as proxy
4) transparent forwarding of traffic
Malicious server
Client / Bot
Bots, serving as proxy layer
A
B
C
D
E
F
G
H
I
J
K
L
M
N

Fig 3: Fast-Flux Service Network

C. *Indirection of Command and Control:* In addition to the approaches mentioned, other technologies have been exploited for botnet command-and-control architectures in order to achieve a certain level 0 indirection.

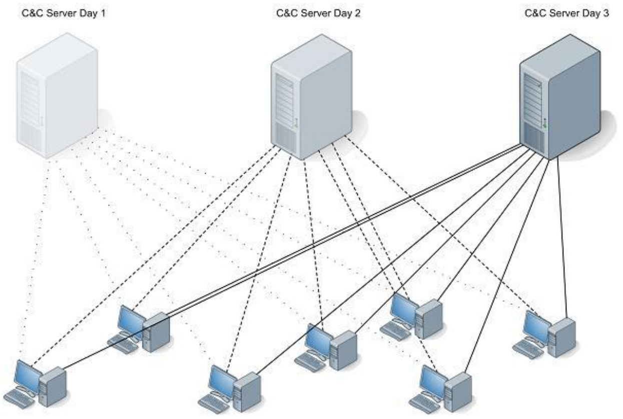

Fig 4: Locomotive Botnet

3. USES OF BOTNET:

Botnet can be referred as a tool, which is used by different people for fulfilling their illegal motives. The most common uses were criminally motivated (i.e. monetary) or for destructive purposes. Various uses of Botnet on behalf of the data captured, are listed below.

1. **Distributed Denial-of-Service Attacks:** A DDoS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming victim’s network bandwidth.
2. **Sniffing Traffic:** Sniffers mainly try to retrieve information like usernames and passwords. If a machine is compromised more than once and also a member of more than one botnet, the packet sniffing allows to gather the key information of the other botnet. Thus it is possible to "steal" another botnet.
3. **Keylogging**: If the compromised machine uses encrypted communication channels then there is no use of network packets on the victim's computer as encryption/decryption medium gets missing. Sensitive information can be easily retrieved by attacker using key-logger.

4. MEASUREMENT AND DETECTION TECHNIQUE:

There are two types of categories of different techniques:

1. *Passive Technique*: This group of passive measurement techniques consists of those where data is gathered solely through observation. Note, however, that passive methods may also limit the amount of data that can be gathered for analysis.

   1.1 Packet Inspection: A popular concept for increasing a network's security is to inspect the network data packets. This works on the basic principal to match various protocol fields, or the payload of a packet, with pre-defined patterns of suspicious content. These patterns are also called detection signatures.

1.2 Analysis of Flow Records: Analysis of flow records ‘can be considered as a technique for tracing network traffic at an abstract level. Instead of inspecting individual packets, as described in the previous section, communication streams are considered in an aggregated form. Typical attributes are: source and destination address; the related port numbers and also the protocol used inside the packets; the duration of the session; and the cumulative size and number of transmitted packets.

1.3 DNS based approaches: When a host has been compromised by a botnet, communication has to be established to either a commanding server or other infected hosts, depending on the botnet infrastructure. Two ways of specifying a firm contact point are available for this purpose: 1. Fixed IP addresses can be integrated into the bot, executable upon distribution. 2. Define a domain name for contact while compromising of the host system. Fast-flux service networks based on the Domain Name System and described in more detail in section 1.2 (Components of Botnet Infrastructures), are a consequent evolution of this approach. The contact information needed to register a domain is usually forged by bot-masters and therefore not usable for investigations.

2. *Active Technique:* The group of active measurement techniques contains approaches that involve interaction with the information sources being monitored.

2.1 Sinkholing: In general, the term sinkholing describes a technical countermeasure for cutting off a malicious control source from the rest of the botnet.

2.2 Infiltration: The infiltration of botnets can be divided into software- and hardware-based techniques. The software based technique monitor traffic to get measurements called control and conduct. The hardware-based technique can be used only if command-and-control server access is possible.

2.3 DNS Cache Snooping: The measurement technique called DNS Cache Snooping [101] is based on the caching property implemented and used by many DNS servers.

5. CONCLUSIONS:

As Networks are growing, problems related to security and data loss has also increased. To overcome these problems a new technique must be designed to prevent those attacks. Botnet is good but it also has some problem regarding security. So this technique should e revised and advanced for preventing future attacks.

REFERENCES:

1. Jeanne Meserve, “Official: International Hackers Going after U.S. Networks,” CNN.com, October 19, 2007, [http://www.cnn.com/2007/US/10/19/cyber.threats/index.html]. Sebastian Springer, “Maj. Gen. Lord Is a Groundbreaker,” *Federal Computer Week,* October 15, 2007, vol. 21, no. 34, p. 44.
2. ITU Study on the Financial Aspects of Network Security: Malware and Spam. ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, 2008.
3. Peer-to-Peer Botnets: Overview and Case Study. Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B., Dagon, D. In: Proceedings of the First Workshop on Hot Topics in Understanding Botnets (HotBots‘07), 2007.
4. Cyberextortion: An Overview of Distributed Denial of Service Attacks against Online Gaming Companies. Paulson, R. A., Weber, J. E. In: Issues in Information Systems, Vol. VII, No. 1-2, 2006.
5. DNS Cache Snooping. Grangeia, L. Research Paper, 2004.