A Review on Botnet Detection Techniques

Mitali Lade
Department of Computer Engineering
Shree L. R. Tiwari College of Engineering
Mumbai University, Thane, Maharashtra, India

Dr. J. W. Bakal
Shivajirao S. Jondhale College of Engineering
Mumbai University, Thane, Maharashtra, India

K. Jayamalini
Department of Computer Engineering
Shree L. R. Tiwari College of Engineering
Mumbai University, Thane, Maharashtra, India

Abstract— Botnets are still thought of because the most serious malware and it arises normally in today's cyber crime, which results in serious threats to our network. Botnet could be a collection of compromised computer (bot) ,that is remotely controlled by BotMaster (BotHerder) under common command and control (C&C) infrastructure. The Command and control is used to distribute commands to the bot to perform malicious activity like info capturing, form grabbing, sending Spam mails, Distributed Denial-of-service (DDOS) attacks etc. so it is required to detect the botnet so as to provide secure network service

Keywords—*Botnet Detection Techniques, Command & Management Channel, Communication Topologies*

*****

I. Introduction

Network security could be a critical issue and a challenge to professional system developers in means of protection against miscellaneous attacks aimed toward any resource that's of interest to the attacker. Over the years with the increasing number of computer systems connected to the worldwide internet, even the average users should be aware of the external threats. Therefore, it's necessary to take some kind of precautions in order to protect themselves from these threats such as installation of antivirus, keeping the system up-to-date etc. However, from a business or an organization's point of view, security assessments are of a greater importance and should be acknowledged and valued so as to form the security policies that are associated with an organization or a business.

The most serious demonstration of advanced malware [1] is Botnet. The term bot is derived from "ro-bot" that could be a combination of 'roBOTNETwork'. bot is a generic term used to describe a script or set of scripts designed to perform predefined functions in automatic fashion. Botnet is most widespread and occurs commonly in today's cyber attacks. As a result, it creates serious threats to network assets and organization's properties.

1.2 Lifecycle of Botnet: Bots sometimes distribute themselves across the net by searching for vulnerable and unprotected computers to infect. once bot finds associate degree unprotected pc, they infect it so send a report back to the BotMaster. The bot keep hidden till they are conversant by their botmaster to preform associate degree attack or task. Fig.1 shows working of Botnet Detection Life cycle. Flow of life cycle is as given in following steps:

1. BotMaster uses a zombie (exploit machine) to send primary infection to the victim machine
This can be done in form of sending email attachments.

2. Victim downloads the attachment and installs it on its
machine so it gets compromised.

3. The malicious bot program that has been installed onto victim's machine opens network ports
for enabling secondary infection.

4. The victim machine downloads the secondary infection
through which the machine becomes the a part of the botnet.

5. The victim machine is now programmed to periodically send
its status information to the bot.

6. Bot controller sends a reply back to the victim and also sends
new commands from BotMaster

7. . BotMaster sends commands to the bot controller which in turn passes to all the victim machine.

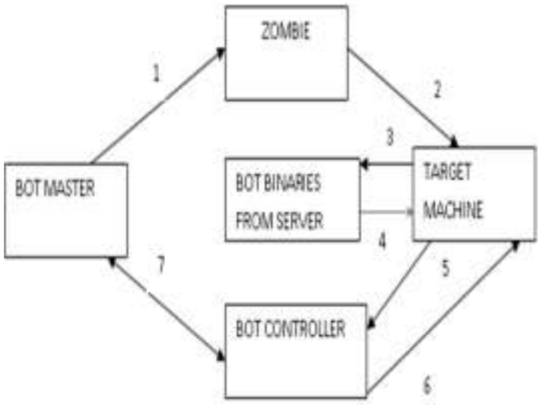

Fig. 1: Botnet Life Cycle

1.2 Purpose of Botnet: it's wont to perform following criminal action;

- Computer frauds and scams
- Cyber-attacks and hacking services transaction
- Cyber warfare and cyber undercover work
- Stealing data (credentials, personal)

- Spying and following (capturing digital camera shots, key stroke logging)
- Hijacking (replicating user actions on a machine)
- Performing malicious internet activity (sending

spam, operating as proxies, infecting alternative machines etc.) and many more

II. BOTNET DETECTION TECHNIQUES

There are two main existing techniques to detect botnet they're as follows[2],[3],[4].

A) Honeynet: It's used to track and collect information of malicious activity. Honeynet is a set of Honeypots. A honeypot is by design insecure computational system that is placed in network with the objective of detection and capturing traffic from botnets. however Honeynet is usually used to understand the botnet characteristics but don'tnecessarily detect botnet and bot infection.

B) Passive network traffic monitoring: This method is useful to identify existence of botnet. Passive network traffic monitoring is classified into five different techniques they're as follows; signature-based, anomaly based, DNS based, Mining, and Network based.

i) Signature-based detection technique

This technique is employed for detection of known bots. Detection of bots is based on previous knowledge about the botnet and malwares. so this solution is not feasible for unknown bots. Zero day attack can't be detected by this method. Rishi and Snort [3] tools are used to detect known bots and can applicable just for IRC protocol.

ii) Anomaly-based detection technique

Anomaly-based detection technique is based on several traffic anomalies like high network latency, high volumes of traffic, traffic on unusual ports, and unusual system behavior that might indicate the presence of malicious bot. Advantage of this method is that, it's used to detect unknown bot. Disadvantages of this method is that, it's used only for IRC protocol and it's not used to identify botnet C&C traffic because C&C traffic is not with high volume and doesn't cause high network latency.

iii) DNS based detection technique

This technique relies on DNS information generated by botnet. so it's possible to detect botnet DNS traffic by DNS monitoring by using the same principles of the anomaly based detection techniques. this method will simply track DNS traffic anomalies. it's used to detect domain name with unusually high or temporally intense of DDNS query.

iv) Mining based

Mining based detection technique is used to detect the botnet by mining multiple log files. it's used to identify Botnet C&C traffic. this method includes machine learning process, classification of data, and clustering to detect botnet. Disadvantage of this method is that, it's difficult to detect botnet C&C traffic.

v) Network based

Network based detection technique is used to detect unknown, encrypted as well as protocol (IRC, http or P2P) and structure based botnet. This technique tries to detect Botnet by monitoring network traffics. Network based is classed in to two techniques; first technique is Active Monitoring; this technique intentionally injects test packets on to network to observe the flow of network traffic. Advantage of this technique is that the response time to detect malicious agents is less, it is simple technique and a drawback of this technique is; it will increase network traffic with additional packets sent to suspicious machines. Second technique is passive monitoring; it simply observes data traffic that is already on the network instead of injecting artificial traffic and look for suspicious communications (from bots and C&C servers).

III. BOTNET COMMUNICATION TOPOLOGIES

According to the C&C channel there are two different models of Botnet topologies one is centralized (IRC and HTTP) and alternative one is decentralized communication model (P2P).

In Centralized communication approach, one central point is in-charge for exchanging commands and information between BotMaster and Bots. Advantage of this model is that it has small message latency, due to this BotMaster will easily arrange botnet and launch attacks [2]. Disadvantage of this model is that, C &C server is critical point because all connections happen through the C&C server [2]. In other words, C&C server is the weak point in this model. If someone manages to detect and eliminate the C&C server, the entire Botnet can become useless and ineffective. The C&C server runs on certain network services like IRC (Internet Relay Chat) channels and HTTP. Researchers have proposed some of the centralized based botnet detection tools, like Rishi, BotSniffer, and BotMiner etc.

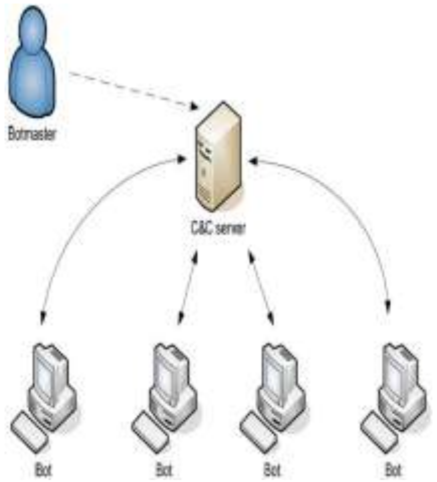

Fig. 2: Centralized Model

To overcome disadvantage of centralized model, attackers began to build alternate botnet communication system that is much difficult to detect and destroy. Hence the attackers have decided to find amodel that doesn't suffer from central point of failure because they do not have centralized C&C server [2]. Thus, attackers exploit the concept of Peer-to-Peer (P2P) based decentralized communication model that makes the detection process significantly difficult. Researchers have proposed some of the P2P based Botnet detection tools, like BotMiner [4]. There are several bots came into the picture from year 1998 who was working under IRC, http and P2P protocol such as RBOT, Phatbot, BitTorrent SDbot, Direct Connect, Zeus and many more.

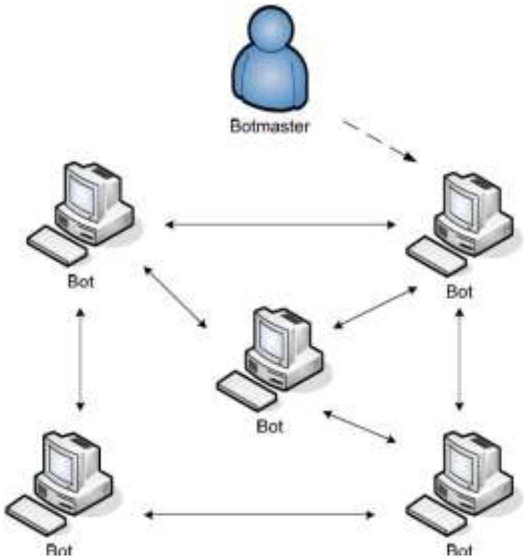

Fig. 3: Decentralized Model

IV CONCLUSION

Botnets pose a significant and growing threat against cyber-security as they provide a key platform for several cybercrimes like Distributed Denial of Service (DDoS) attacks against critical targets, malware dissemination, phishing, and click fraud. Despite the long presence of malicious botnets, only few formal studies have examined the botnet problem and botnet research is still in its infancy. This paper studies botnet detection techniques. In this paper botnet detection techniques based on passive network traffic monitoring are classified into five categories including network based, signature based, anomaly-based, DNS- based, and mining-base.

ACKNOWLEDGMENT

I would wish to express my gratitude to my guide Dr. J.W Bakal and my co-guide Prof. K. Jayamalini for her instructive comments and valuable guidance. I am also grateful to all faculties of computer Engineering department, my colleagues and family for their encouragement and constant support.

REFERENCES

[1] J. Zhang, Perdissci, W. Lee, X. Luo, and U. Sarfraz, “Building a scalable System for Stealthy P2P- Botnet Detection,” IEEE Trans. Inf. Forens. Security, vol. 9, no. 1, Jan. 2014, pp. 27-38.

[2] Y. Mane and K. Devadkar, “P2P Botnet Detection Using Network Security,” in Proc. INTERFACE 2014 TEQIP-II Sponsored 3rd Int. Conf. on Network Infrastructure Management Systems, Mumbai, Jun. 2014.

[3] H. Nair and V. Ewards S, “A Study on Botnet Detection Techniques,” *Int. J. of* Scientific and Research *Publication*, vol. 2, no. 4, Apr. 2012, pp. 1-3.

[4] A. Karim, R. B. Salleh, M. Shiraz, S. A. A. Shah, I. Awan, and N. B. Anuar, “Botnet Detection Techniques: Review, Future Trends and Issues,” Springer, *Journal of Zhejiiang University- Science C (Computer & Electronics)*, vol. 15, no. 11, Nov.2014, pp. 943-983.

[5] Ruchi Dhole, Prof. Shobha Lolge, “*A Survey of Botnet Detection Techniques and Research Challenges”* International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 1, January 2016.