ISSN: 2321-8169
61 – 64

Different Techniques to Detect Botnet

Mitali Lade, Dr. J. W. Bakal, K. Jayamalini
Student, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, India
Principal, Shivajirao S. Jondhale College of Engineering, Mumbai University, Thane, Maharashtra, India
Assistant Professor, Department of Computer Engineering, Shree L. R. Tiwari College of Engineering, Mumbai University, Thane, Maharashtra, India

Abstract:- Botnets are now considered as one of the most serious security threats. In contrast to previous malware, botnets have the characteristics of command and control (C&C) channel. Botnets usually use existing common protocols, eg IRC, HTTP and in protocol conforming manners, this makes the detection of botnet C&C a difficult problem. In this paper we tend to proposed 3 techniques specifically signature based detection, firewall IP blocking and anomaly based detection so as to detect bot and provide secure network services to the users.

Keywords- *Bots, Bot implementation, Bot control, signature based detection, firewall IP blocking, Anomaly based detection*.

*****

I. Introduction

Network security is a critical issue and a challenge to professional system developers in means of protection against miscellaneous attacks aimed at any resource that is of interest to the attacker. Over the years with the increasing number of computer systems connected to the global Internet, even the average users must be aware of the external threats. Therefore, it is 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 must be acknowledged and valued in order 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" which is a combination of '*ro**BOTNET**work'*. Bot is a generic term used to describe a script or set of scripts designed to perform predefined functions in automated 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.

II. Bots

2.1 Definition of a Bot

Since we explore ways that a bot can be changed in order to defeat detection, we need some baseline notion of what constitutes a bot. A bot (I) participates in a command-and-control (C&C) network, through which the bot receives commands (II) which cause the bot to carry out attacks. We do not impose temporal constraints on when the attack must be carried out relative to command receipt nor do we constrain command format. Our bot definition is more general than the one proposed in [9], which required (explicitly or implicitly) that botnet attacks be performed in a coordinated fashion and be network-detectable.

2.2 Bot Implementations

A typical bot implementation consists of two independent engines: a C&C-communication-protocol processor and a *command interpreter*, which interprets and executes bot commands, i.e., implements the bot's protocol. Fig 1 provides an abstraction of the structure of current malicious bots, which live at the application layer of the TCP/IP stack. A bot protocol message (i.e., command) is generally encapsulated as the payload of a C&C communications protocol message. A bot's *command syntax* encodes the actions the bot can perform as well as the ways in which each can be invoked (i.e., the parameters).

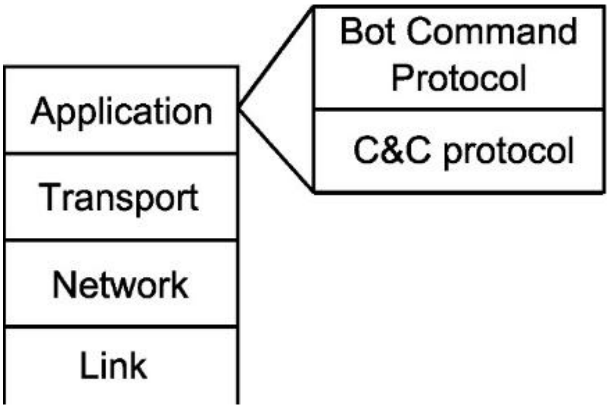

Fig 1: Historically, bots live at the application layer of the TCP/IP stack, which can be further subdivided into the C&C and bot command layers.

2.3 Botnet Control

Botnet control is achieved through a *C&C network*, which consists of the: *C&C protocol*, which defines communication format, *network topology*, which identifies who talks to whom, and *rendezvous point*(RP), the location to which commands are delivered. The historical view of botnets is that they are *tightly controlled*: the bot master sends a command that is received and executed by all listening bots more or less immediately [10], e.g., IRC botnets which have latency on the order of seconds. Peacomm [11]'s use of P2P for C&C demonstrates a looser control model which has higher latency since commands percolate through a distributed network as bot's poll for them.

III. Problem Statement

The objective of Botnet Detection is to provide security against bot. In both centralized and distributed botnets, bots are coordinated through the C&C channel which is control by BotMaster. The BotMaster sends the pre-programmed command to the Target Machine, and then Target (victim) Machine starts sending its periodic information to the BotMaster via Command and Control (C&C) infrastructure. To make the botnet detection more difficult BotMaster started use of low latency anonymous communication to hide botnet with a C&C server. Currently active Bots are hiding their identity. So it is necessary to detect and deactivate Botnet to provide secure network service to the internet users.

In this project, we focus on three techniques to detect bots: Signature Based Detection, Firewall IP Blocking and Anomaly based detection in order to provide secure network services to the users. This project is based on client server architecture. Initially in the first technique named signature based detection we are checking that whether the internal bot is infecting our system or not. For that purpose, signature of some known bots calculated from the content of bot file and that signatures are store in the database. When the technique scans for detecting bot, it computes the signatures of file that present in the system according to contents of the file and compare that signature with the signature present in the database. If signature of calculated file is match with the database present, then it declares that file as an infected file and delete that particular file. The way to create signature for bot is to use hash algorithm (md5, sha_1).

There are some blacklisted sites which may damage our system. The organization named IANA (Internet Assign Number Authority) has considered some of the sites as blacklist. For that purpose, in the second technique named firewall IP blocking, a HTTP request coming through firewall is a bot then we are blocking that IP.

In the third technique we are checking whether the network traffic is high and if so we analyze the source and if the source is invalid we are blocking it. In this we are applying port scan attack ie the IP will be scanned and log reports will be generated.

IV. Related work

There are several techniques for detection of botnets. However, there are 2 essential techniques for botnet detection: setting up honeynets and passive network traffic monitoring [2]. Several papers mentioned about using honeynets for botnet detection [3][4][5][6]. But we've got to take into thought that honeynets cannot detect bot infection most of the times and is just good for understanding botnet characteristics. For identifying the existence of botnets within the network, passive network traffic monitoring is useful.

This technique can be classified into signature based detection, anomaly based detection, DNS based and mining based. Signature based detection techniques will simply be used for detection of recognized botnets. Therefore, this solution isn't useful for unknown bots. Anomaly based detection techniques attempt to detect botnets based on several network traffic anomalies like high network latency, high volumes of traffic, traffic on unusual ports and unusual system behavior that would indicate presence of malicious bots within the network [7]. DNS based detection techniques are based on DNS information generated by a botnet.

As mentioned before, bots normally begin connection with C&C server to get commands. In order to access the C&C server bots carry out DNS queries to locate the particular C&C server that is generally hosted by a DDNS (Dynamic DNS) provider. Therefore, its possible to detect botnet DNS traffic by DNS monitoring and detect DNS traffic anomalies [6][8].

V. Design flow of project

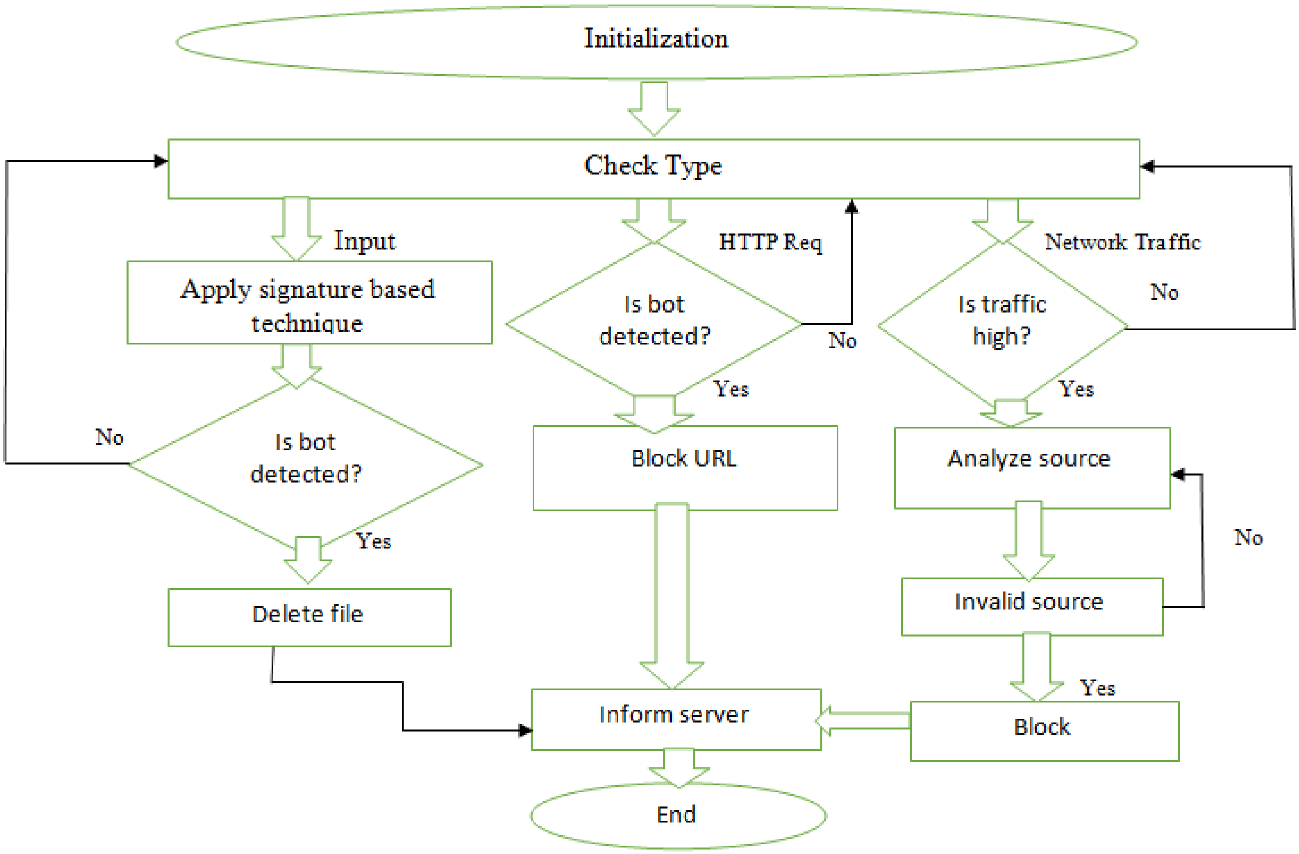

Fig 2: flowchart of our proposed detection techniques

VI. Design Details

Our proposed flowchart is based on passively monitoring network traffics. Fig 2 shows the flowchart of our proposed Botnet detection system, which consist of three techniques: signature based detection, firewall IP blocking and anomaly based detection. In the very first technique we are checking whether our system is infected by the internal bot and is so we are deleting that file. In the second technique we are blocking all the blacklisted IPs inorder to secure our system from bots. In the third technique we are checking whether the network traffic is high and if so we analyze the source and if the source is invalid we are blocking it. In this we are applying port scan attack ie the IP will be scanned and log reports will be generated.

Basically bots can infect our system either internally or through external IP or through invalid source analyzed by the network traffic. So detecting and deleting bots is necessary in order to have a secure network services. According to our proposed flowchart initially we are checking the type of bot ie whether that bot is infecting internally or externally. If the type of bot is input, then we are applying signature based detection technique and scanning our system and if bot is detected we delete that file and inform the server. Again if we are getting an HTTP request which is a bot than we are blocking the request coming from those IPs and inform the server. And in the last technique we are checking whether the network traffic is high or not and if the network traffic is high we analyze whether the source is valid or invalid and if the invalid source is found we block that source and inform the server.

VII. Conclusion

In this paper, we have discussed the flow of our proposed research work for detection of bots. We have taken the overview of what exactly is bot? how it is implemented and what are the botnet controls. We have even gone through the different techniques which we have applied to detect the bots.

Acknowledgments

I owe a deep gratitude towards my honourable guide, Dr J. W. Bakal. He rendered his valuable guidance with a touch of inspiration and motivation. I would like to thank Prof.K. Jayamalini, my co-guide who extended every facility and helped me for completing this paper. I would also like to thank my principal, Dr. S. Ram Reddy for his moral 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] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P. Roberts, K. Han, "Botnet Research survey ". in Proc. 32nd Annual IEEE International conferences on computer software and applications(COMPSAC)2008.page 967-972

[3] M.A Rajab, J. Zarfoss, F. Monrose, and A Terzis, "A multifaceted approach to understanding the Botnet phenomenon," 6th ACM SIGCOMM on Internet Measurement Conference, IMC 2006, 2006, pp.41-S2.

[4] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understandinng, detecting, and disrupting Botnets," Proc. of Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'OS), June 200S.

[5] Ramachandran, Anirudh, and Nick Feamster. "Understanding the network-level behavior of spammers." ACM SIGCOMM Computer Communication Review. Vol. 36. No. 4. ACM, 2006.

[6] Choi, Hyunsang, et al. "Botnet detection by monitoring group activities in DNS traffic." Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on. IEEE, 2007.

[7] Saha, Basudev, and Ashish Gairola. "Botnet: an overview." *CERT-In White Paper, CIWP-2005-05* 240 (2005).

[8] RVillamarin-Salomon and J.C. Brustoloni, "IdentifYing Botnets using Anomaly Detection Techniques Applied to DNS Traffic," in proceeding 5th IEEE Consumer Communications and Networking confernce. (CCNC 2008), 2008, pp. 476-481

[9] Gu, Guofei, et al. "BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection." *USENIX security symposium*. Vol. 5. No. 2. 2008.

[10] Strayer, W. Timothy, et al. "Detecting botnets with tight command and control." *Local Computer Networks, Proceedings 2006 31st IEEE Conference on*. IEEE, 2006.

[11] Grizzard, Julian B., et al. "Peer-to-Peer Botnets: Overview and Case Study." *HotBots* 7 (2007): 1-1.