International Journal of Engineering Research and General Science Volume 6, Issue 1, January-February, 2018
ISSN 2091-2730

Botnet Detection Based on Passive network traffic monitoring

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 have become one of the main threats to Network security. Botnets have been used to stage denial of service attacks, spam campaigns, stealing user passwords and other malicious activities. Detecting botnets has become an important priority for network security. The proposed paper is going to focus on three techniques namely Signature based detection, Firewall IP Blocking and Anomaly based detection to detect bot and give the comparison of these techniques and also try to give better efficient result.

Keywords- signature based detection, firewall IP blocking , Anomaly based detection

I. Introduction

Nowadays, the most serious manifestation of advanced malware is Botnet. to create distinction between Botnet and different kinds of malware, we've to comprehend the thought of Botnet. For a better understanding of Botnet, we've to understand 2 terms initial, bot and BotMaster and then we can properly define Botnet. bot - bot is actually short for robot that is also known as as Zombie. it's a new form of malware [1] installed into a compromised computer which can be controlled remotely by BotMaster for executing some orders through the received commands. after the bot code has been installed into the compromised computers, the computer becomes a bot or Zombie [2]. Contrary to existing malware like virus and worm which their main activities focus on attacking the infecting host, bots can receive commands from BotMaster and are used in distributed attack platform.

BotMaster - BotMaster is also referred to as BotHerder, is a person or a group of person that control remote Bots. Botnets- Botnets are networks consisting of large number of Bots. Botnets are created by the BotMaster to setup a private communication infrastructure which might be used for malicious activities like Distributed Denial-of-Service (DDoS), sending large amount of SP AM or phishing mails, and alternative nefarious purpose [3] [4] [5]
[6].

The main difference between Botnet and other kind of malwares is that the existence of Command-and-Control (C&C) infrastructure. The C&C allows Bots to receive commands and malicious capabilities, as devoted by BotMaster. the first generation of Botnets utilized the IRC (Internet Relay Chat) channels as their Common-and-Control (C&C) centers. The centralized C&C mechanism of such Botnet has made them vulnerable to being detected and disabled. Therefore, new generation of Botnet which might hide their C&C communication have emerged, Peer-to-Peer (P2P) based Botnets. The P2P Botnets don't suffer from a single point of failure, because they do not have centralized C&C servers [6][7]. Recently researches have proposed some approaches and techniques [8][9] [10] [11] [12] [13] for detecting Botnets. Majority of these approaches are developed for detecting IRC or HTTP based Botnets [8][9] [13].

II. Problem Definition

The botnet has become a most threatening phenomenon and shown its harmful effect on network communities over the last decade. Researchers, law-enforcement authorities, businesses, and individuals have started to discover methods to combat this malicious threat. Botnet detection is currently an ongoing challenge for researchers and organizations. Botnets are considered moving targets, which means all the aspects of botnets including detection, mitigation, and response are changing over time; therefore, no mitigation or detection technique offers a permanent solution. Similarly, different types of stakeholders, for instance, enterprises, governments, networks, and Internet service providers (ISPs), have different ways and goals to address the issue of botnets. Moreover, with the

advent of new technologies and increase in the knowledge base, the expertise of bot masters is improving in evading botnet detection techniques and trying to rally sophistication for the command and control (C&C) architecture. [14]

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.

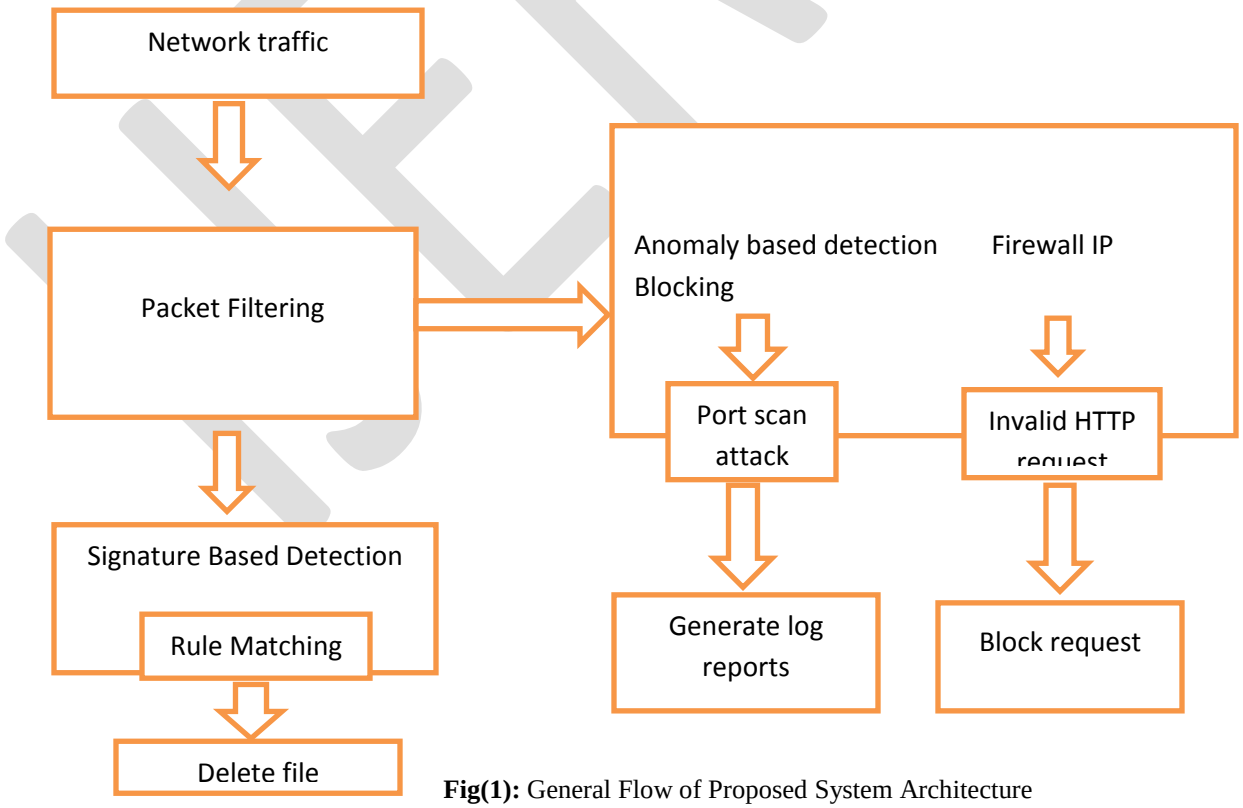
In this project, we focus on three techniques to detect bots: Signature Based Detection, Firewall IP Blocking and Anomaly based detection in order to provide secure network services to the users. This project is based on client server architecture. Initially in the first technique named signature based 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).

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.

III. Proposed System Architecture

Following fig(1) shows the proposed system architecture for an efficient technique to detect botnet.



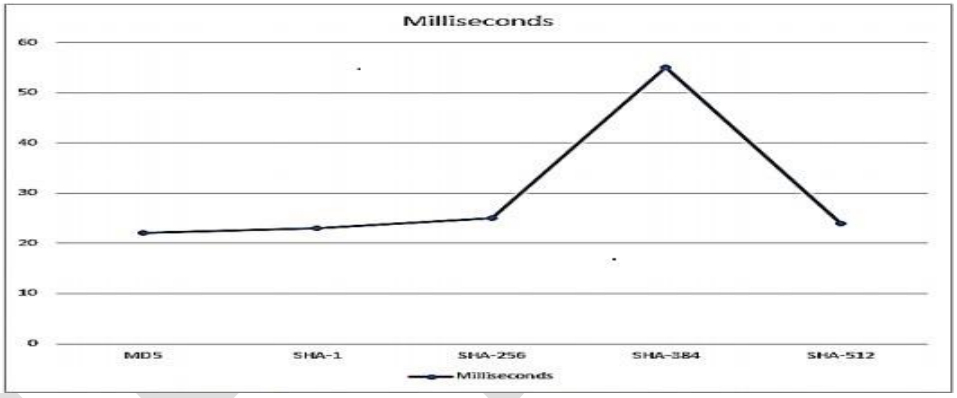
Fig(1): General Flow of Proposed System Architecture

In the proposed system architecture, we have implemented three techniques to detect bot. Signature based detection is very simple and is used to detect known bots. Signature based detection is implemented using MD5 algorithm as compared to SHA algorithm. In this technique signature of some known bots calculated from the content of bots file and that signatures are store in the database. When our script scans the system, 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 our script declares that file as an infected file and delete that particular file. The simple way to create signature for bot is to use hash algorithm (md5, sha). Mainly setup includes Virtual Network Environment Using MS Virtual PC and installed Windows 7.

In our experiments we have used md5 hash algorithm as compared to sha_1. Table 1 shows the comparison between MD5 and SHA.

Keys For Comparison	MD5	SHA
Speed	Faster	Slower
Iterations required	Only 64	80 iterations
Successful attacks so far	Attack reported to some extent	No such attack reported yet
Security	Less	High
Length	128 bits	160 bits

Table 1: Comparison between MD5 and SHA



Fig(2): Performance chart of hashing algorithms [15]

The next technique to detect bot is blocking IPs through firewall. Network firewalls are devices or systems that control the flow of traffic between networks employing different security postures. The network traffic flow is controlled according to a firewall policy. Basically in this technique firewall acts as a doorkeeper which does not allows the access to blacklisted IPs. Client observes the traffic coming through firewall and if the firewall gets to know that if the incoming request is blacklisted IP then that IP is blocked.
In the third technique we are observing whether the ports are performing some malicious activities or not that is the port is attacked by botnet and an alert message and log reports are generated. Nmap (Network Mapper) well known tool is used for port scanning.

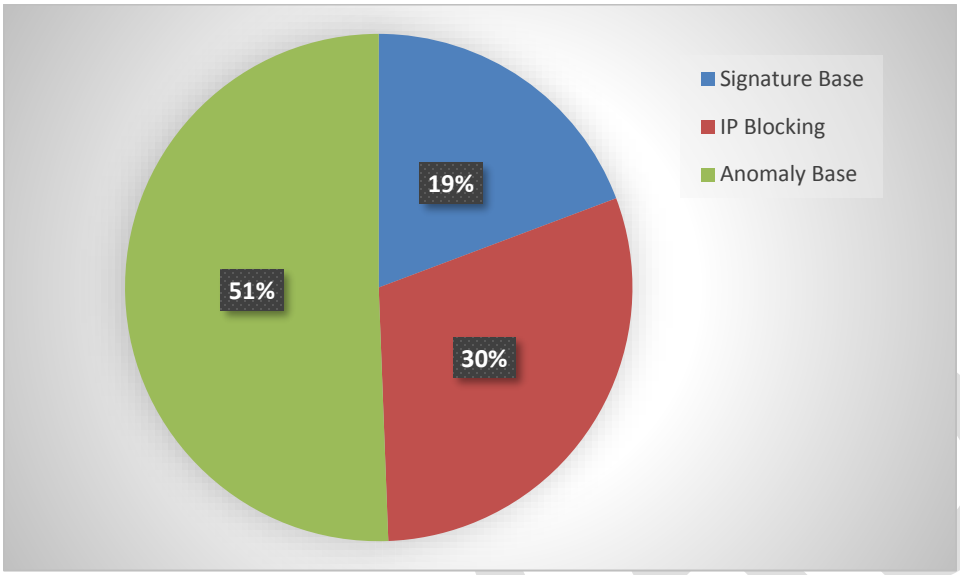
IV. Hardware and software details used for impelementation of proposed system

Python is an interpreted high level programming language for general purpose programming.
Python has a design philosophy that emphasizes code readability and a syntax that allows programmers to express concepts in fewer lines of code notably using significant whitespace.
It provides constructs that enable clear programming on both small and large scales.

1. Python 3.5 (64 bit)
2. Windows 7 (VMWARE) operating system
3. Intel Core i5 processor
4. 64 Bit system bus
5. 8 GB RAM

V. Result Analysis

In this section I would like to discuss result of proposed system. We have defined three techniques namely signature based detection, firewall IP blocking and anomaly based detection to detect bot. Result of it as follows.



Fig(3) : comparison of proposed system with existing system

Fig(3) shows the results of our research work. According to our research our existing technique signature based detection gives 19% efficiency whereas our other technique named firewall IP blocking gives 30% more efficiency compared to existing technique and anomaly based detection gives 51% more. Hence we can say that our research work gives better efficiency and provides secure network service to users.

VI. Conclusion

Botnet detection is a relatively new and a very challenging research area. In this paper we presented three techniques to detect bot. The efficiency of these techniques gives much better results compared to existing techniques. But if we connect two or more number of systems then the speed of our project will decrease. So in the future purpose concept of multithreading should be used to resolve this problem.

VII. 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:

[I] P. Barford and V. Yagneswaran, "An Inside Look at Botnets ". In: Special Workshop on Malware Detection, Advances in Information Security, Springer, Heidelberg (2006).

[2] N. Ianelli, A Hackworth, Botnets as a Vehicle for Online Crime, CERT, December 200S.

[3] 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.

[4] Honeynet project, know your Enemy: tracking Botnets, march 200S. http://www.honeynet. orglpapers/bots

[5] 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.

[6] Zeidanloo, H.R; Manaf, A.A. "Botnet Command and Control Mechanisms ". Second International Conference on Computer and Electrical Engineering,2009. ICCEE. Page(s): S64-S68.

[7] Duc T. Ha, Guanhua Yan, Stephan Eidenbenz, Hung Q. Ngo. "On the effectiveness of structural detection and defense against P2P based Botnet," Proc. of the 39th Annual IEEEIIFIP International Conference on Dependable Systems and Networks (DSN'09), june2009

[8] J. R Binkley and S. Singh. An algorithm for anomaly-based Botnet detection. In Proceedings of USENIX SRUTI'06, pages 43-48, July 2006

[9] J. Goebel and T. Holz. Rishi: identifY bot contaminated hosts by irc nickname evaluation in proceeding of USENIX security symposium (security 2007)

[10] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. BotHunter: Detecting mal ware infection through ids-driven dialog correlation. In proceedings of the 16th USEBIX security symposium (security 2007).

[11] G. Gu, J. Zhang, and W. Lee. BotSniffer: Detecting Botnet command and control channels in network traffics. In proceeding of ISth Annual network and Distributed system security symposioum,2008.

[12] A Karasaridis, B. Rexroad, and D. Hoeflin. Widescale Botnet detection and characterization. In Proceedings of USENIX HotBots'07,2007.

[13] W. T. Strayer, RWalsh, c. Livadas, and D. Lapsley. Detecting Botnet with tight command and control. In Proceeding of the 31th IEEE conference on local computernetwork,2006.

[14] Karim, Ahmad, et al. "Botnet detection techniques: review, future trends, and issues." Journal of Zhejiang University SCIENCE C 15.11 (2014): 943-983.

[15] Gupta, Piyush, and Sandeep Kumar. "A comparative analysis of SHA and MD5 algorithm." architecture 1 (2014): 5.