International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August 2013
ISSN 2229-5518

Automated Layered HTTP Botnet Detection Mechanism

Seena Elizebeth Mathew
ComputerScience and Engineering
Ilahia College of Engineering
Moovattupuzha

Abdul Ali
ComputerScience and Engineering
Ilahia College of Engineering
Moovattupuzha

Abstract— HTTP botnet uses HTTP protocol for compromising another system. This paper proposes robust method of detecting as well as preventing botnet attacks. Distributed denial of service attacks, session attacks, port scanning, HTTP errors are mainly considered in this paper. Detection and prevention based on network level and packet level features of the packets entering to the system. Performance evaluation is done based on precision, F-value and probability. Layered approach reduces the computation and overall time required for the detection by using autonomous and self sufficient layers. Thread model provide more effieciency to the system.

Index Terms— Http Botnet,Firewall,Layered approach.

1 INTRODUCTION

The word Botnet derives from two words rebot and networks. Botnet is a collection of systems (or application programs) communicating with other systems to perform certain tasks. Two types of botnets are there legal botnet and illegal botnet. Legal botnets used for keeping control of IRC channel etc. Illegal botnet are comprise computers whose security defence has been breached and then compromised systems are controlled by the third party through protocols such as IRC (Internet Relay Chat) and HTTP(Hyper Text Transfer Protocol) .Illegal botnet are mainly used for DDoS attacks, misuse of SMTP etc. Bots are created by means of malware Software. Botnet controller sends the infected packet to the system to be compromised with bot as its payload. When the packets reaches the system it logs to the C&C server. Operator provides botnet services to the spammer. Operator instructs the compromised system when it receives the spam messages from the operator

Http botnet uses HTTP protocol. With http protocol and port 80 attacks can not only be masked but also go through the firewall without being detected[1] .Network layer security is the key aspect of internet security mechanisms. Different network security measures are available .Among them layered approach is popular. Layered approach reduces computation and detection time[2].Layered approach ensures availability, confidentiality and integrity[3].

This paper uses mainly four layers DDoS layer, U2R layer, R2L layer. Each layer is independent and autonomous so as to reduce the communication between the layers and trained separately and with no central controller. Layers are deployed sequentially so that attackers can easily be detected and blocked. This paper deals with the use of automated (thread) layered approach for http botnet detection as well for the defence.

When packet enters `the network It captures all the packets in the Network Interface by using Jpcap capture.The probe attacks are aimed at acquiring information about the target network from a source that is often external to the network. Basic connection level features such as the “duration of connection” and “source bytes are noted. For the DoS layer, traffic features such as the “percentage of connections having same destination host and same service” and packet level features such as the “source bytes” and “percentage of packets with errors” are noted. For R2L attacks network level features such as the “duration of connection” and “service requested” and the host level features such as the “number of failed login attempts” are noted. For U2R attack’s features such as “number of file creations” and “number of shell prompts invoked are considered. Firewall filters the packets according to white-list gray list it created. At first firewall initialize the list and then updates the list as per the analysis.

The remainder of the paper are organized as follows. Second section deals with the related works. Third chapter presents the automated layered system along with the architecture. Fourth discusses the implementation of the proposed system. Fifth section concludes the paper as well as profiles some directions for the future work

2 RELATED WORK

The illegal botnet now became the serious threat in network security[4]. Bot net first appeared on the internet by 1993 and called IRC bots, then by 2002 it became P2p bots. HTTP bots came into existence by 2004 onwards. Strength of the Bot net is growing year by year. Different safety measures are taken in each period to prevent botnet attack. In Botnet detection beased on DNS traffic, analysis of traffic is done to check whether the service requesting client is legitimate or not. In the mothod based degree of periodic repeatability, DPR is calculated using standard deviation. The fig below shows the developmental stages.

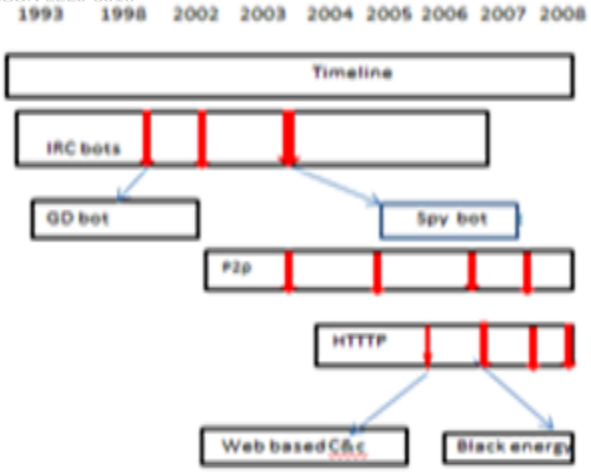

Fig 2.1 History of Malicious Botnet

2.1 DNS Traffic Based Botnet Detection

Botnet detection based on DNS traffic based on analysis of DNS traffic, which forms a group activity in which DNS queries simultaneously sent by distributed bots to DNS server. Bots are sending DNS queries in order to access the C&C channel server[5]. A bot master wants to arrange several C&C servers which can be listed in the bot binary for the stability of the botnet and uses a dynamic DNS (DDNS).Previous domain name of botnet C&C server is blocked, bot master can just moves his botnet to another candidate C&C server[6]. Several features of botnet DNS traffic tis different from legitimate DNS traffic and thus find the botnet.

2.2 Http Botnet Detection Based On Degree Of Periodic Repeatability

Tung-Ming Koo proposed the botnet detection based on the repeatability of the connection. The term Repeatability is the variations in measurements taken by a single entity on an item under the same condition. A measurement is said to be Repeatable when these variation is lower than an agreed threshold. This technique exploited the degree of periodic repeatability (DPR) for detecting http botnet by analyzing the traffic between http server and the clients[1]. For a high periodic repeatability the degree of periodic repeatability is low and for low periodic repeatability the degree of periodic repeatability is high. If DPR of a user is high then that user will be a legitimate user and if DPR of a user is low then that user will probably be b http bot. Fig explains the above scenario. In this figure DPR of the user5 is low therefore user5 probably will be a httpbot.in this way it is able to detect http bot and the particular user behavior can be observer and blocked later

3 PROPOSED SYSTEM

3.1 Automated Layered System Architecture

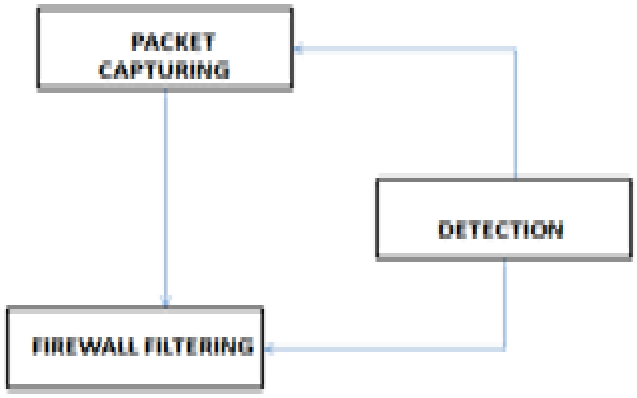

Fig 3.1 Automated Layered system architecture

Packet capturing module captures the packets that are sent from other network to respective network. In Deep packet capture means capturing the packets from the network layer. After capturing the packets are inspected to analyse the contents. Full packet capture means capturing both header and payload part. Header part provides information regarding the payload part along with length and routing information. Payload includes the actual data. In partial packet capturing only header is captured during capturing. After capturing the packet packets are stored in memory and evaluated later. Initially all packets are captured. The proposed system employs filtered capture where packets are captured based on ip address or mac address etc. All packets with ip address in white list are captured without further intervention. Packets with ip address in black list are filtered by the firewall.

Detection module aims at detecting attacks especially DDoS attacks. In DoS attacks the targeted system is flooded with large number of request beyond it can accommodate thus it slows down the system. Therefore traffic level features such as source address, destination address, mac address, ip address traffic rate etc are considered and packet level features such as contents of packets, errors in the packets are considered. Different DDOS attacks this paper considers are request from the client with reset/set request by setting the reset flag, http request with no data, Session hacking, port scanning etc.

- Session hacking refers to the theft of session key that is used to authenticate a session. So that the attacker can unauthorisily access to the information exchanged in the session.
- In session fixation attacker fixes the session key but the parties involved in the session is unaware of it.
- Next one is Session sidejacking here the attacker reads the network traffic by packet sniffing. Once the attacker gets the session key he

can directly access the data without intervention.

- Port scanning is process of scanning the ports. Since data to and from the system goes through the ports administrators uses port scanning for managing the network. Attackers uses port scanning for analyzing the system traffic. Port scanning is mainly used for identifying the active ports and exploiting the service provided by that port .It is done by sending infinite number of request to a large set of ports. Port sweep is yet another variation of port scanning.

The R2L attacks are one of the most difficult to detect as they involve the network level and the host level features. We therefore selected both the network level features such as the "duration of connection" and "service requested" and the host level features such as the "number of failed login attempts" among others for detecting R2L attacks.

Attackers do not have an account on the victim machine, hence tries to gain access, these are guess password, ftp write, multi hop etc.

The U2R attacks involve the semantic details that are very difficult to capture at an early stage. Such attacks are often content based and target an application. Hence, for U2R attacks, we selected features such as "number of file creations" and "number of shell prompts invoked," while ignores features such as "protocol" and "source bytes."

An attacker has local access to the victim machine and tries to gain super user privileges; these are buffer overflow, rootkit.

Firewall performs filtering operation based on black list, white list etc[1].

a)Custom white list: Users can initially set their white list with the ip address of the other systems they believe to be reliable or authenticated. For this user keeps a database table consisting of ip address and corresponding status. User can add customarisily ip address to the custom white list so that connection from such system is accepted without intervention.

b)custom blacklist: Initially users can also set their own custom black list with the ip address they feel to be unrealiable. There is a separate status for ip address included in the custom black list. Connection request from the ip address included in black list is filtered without further intervention. So that analysing time can be saved.

c)white list: White list are updated after the analysis of the packets. Packets is checked under differ layers, if packet is legitimate packet then source address in the packet is added in white list. For this also a database table is used with entries for ip address and status.

d)Black list: Black list includes the ip address of the system which has been proven to be an attacker. Connection request from the ip s in the black list is filtered without analysis. Thus time can be saved.

4 CONCLUSION

In this paper we proposed a simple yet practical automated layered approach for http botnet detection. We discussed that such a system would less computational intensive and more accurate. This system focusing mainly on DDOS attacks prevention. Layered approach provides efficiency and reliability and the automation provides robustness. When packet enters `the network It captures all the packets in the Network Interface by using Jpcap captor. The probe attacks are aimed at acquiring information about the target network from a source that is often external to the network. Basic connection level features such as the "duration of connection" and "source bytes are noted.. Hence, for the DoS layer, traffic features such as the "percentage of connections having same destination host and same service" and packet level features such as the "source bytes" and "percentage of packets with errors" are noted. T. We therefore selected both the network level features such as the "duration of connection" and "service requested" and the host level features such as the "number of failed login attempts" among others for detecting R2L attacks. For U2R attacks, we selected features such as "number of file creations" and "number of shell prompts invoked," . Firewall filters the packets according to whitelist gray list it created. Firewall performs filtering operation it makes the attacker to try with another approach. Rather than filtering if it possible to send another packet rather than requested, the attacker can't understand that he has been blocked. Therefore attacker would not go for another approach. Also employ signatures with the packets for better performance.

REFERENCES

[1] Tung-Ming Koo, Hung-Chang Chang,Guo-Quan Wei, "Construction p2p firewall HTTP-Botnet Defence mechanis,".

[2] Dianxiang Xu, Manghui Tu, Michael sanford, Lijo Thomas, Daniel Woodraska, Weifeng Xu, "Automated Security Test Generation With Formal Threat Model," in Magnetism, IEEEtransaction on dependable and secire computing vol 9.

[3] Bonepalli uppalaiah, Nadipally Vamsi Krishna, Renigunta Rajendher, "Layer Based Intrusion Detection Sysytem for Network Security,"

[4] World Economic Forum, "The Internet is Doomed," BBC News, Jan 2007 .

[5] Hyungsang Choi, Hanwoo Lee, Heekoo Lee, Hyorgon Kim, "Botnet Detection By Monitoring Group activities in DNS Traffic," 7th IEEE iccit 7 pp.715-720.

[6] Paul Balford, Vinod Yegneswaran, "An inside Look At The Botnet," 2006..

[7] L. Hubert and P. Arabie, "Comparing Partitions," *J. Classification,* vol. 2, no. 4, pp. 193-218, Apr. 1985. (Journal or magazine citation).

[8] R.J. Vidmar, "On the Use of Atmospheric Plasmas as Electromagnetic Reflectors," *IEEE Trans. Plasma Science*, vol. 21, no. 3, pp. 876-880, available at http://www.halcyon.com/pub/journals/21ps03-vidmar, Aug. 1992. (URL for Transaction, journal, or magzine).

[9] J.M.P. Martinez, R.B. Llavori, M.J.A. Cabo, and T.B. Pedersen, "Integrating Data Warehouses with Web Data: A Survey," *IEEE Trans. Knowledge and Data Eng.*, preprint, 21 Dec. 2007, doi:10.1109/TKDE.2007.190746.(PrePrint)