ISSN 2395-1621

Botnet Detection With Randomized Traffic Investigation

[#1]Jyoti P. Yewale, [#2]S. B. Chaudhari

[1]jyotiyeawale266@gmail.com
[2]sbchaudharitrinity@gmail.com

[#12]Department of Computer Engineering,

Trinity College of Engineering and Reasearch,
Kondhawa-Saswad Road, Pune, India.

ABSTRACT

At present, the most serious demonstration of advanced malware is botnet. Botnet is widespread malware and it arises commonly in today's cyber crime, which results in serious threats to our network. It is a collection of compromised computer (bot), which is remotely controlled by BotMaster (BotHerder) under a common command and control (C&C)infrastructure. The Command and control is used to distribute commands to the bot to perform malicious activity such as information capturing, form grabbing, sending Spam mails, Distributed Denial-of-service (DDOS) attacks etc. Therefore it is required to detect the botnet in order to provide secure network service. The proposed work is aimed at detecting and deactivating P2P DDOS bot, Zeus bot and ToR bots by applying certain steps. First step is identifying Bot by monitoring network traffic behavior. Second step is used to detect Bot by identifying most access port information along with its count. And last step is deactivating Bot activity from victim machine by using Port block and removing registry keyentry through programming.

Keywords— Botnet, Bot, Communication topologies, c&c erver, DDOS bot, Zeus toolkit, ToR.

ARTICLE INFO

Article History

Received: 2nd January 2018

Received in revised form :

2nd January 2018

Accepted: 6th January 2018

Published online :

7th January 2018

I. INTRODUCTION

The term *bot* is derived from "ro-bot "which is a combination of '*roBOTNETwork'*. 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. Botnets are collections of compromised computers (Bots) which are remotely controlled by its originator (BotMaster) under a common Command-and-Control (C&C) infrastructure [1][2][3]. BotMaster is the computer, used by the attacker to issue commands that are relayed to the bots via the controllers. Once the bot code is installed into the compromised computers, the computer becomes a bot or zombie [12]. The main difference between Botnet and other kind of malwares such as worm and virus is that, botnet has the existence of C&C infrastructure. The C&C allows Bots to receive commands and malicious capabilities as devoted by BotMaster, whereas the main activity of malware is attacking the infected host. According to the C&C channel there are two different models of Botnet topologies one is centralized and other one is decentralized communication model. In Centralized communication approach, one central point is in-charge for exchanging commands and data between BotMaster and Bots. Advantage of this model is that it has Small message latency, due to this BotMaster can easily arrange botnet and launch attacks [2, 4]. Disadvantage ofthis model is that, C &C server is critical point because all connections happen through the C&C server [2, 4]. In other words, we can also say that, C&C server is the weak point in this model. If somebody manages to detect and eliminate the C&C server, the entire Botnet will become useless and ineffective. The C&C server runs on certain network services such as IRC (Internet Relay Chat) channels and HTTP. To overcome disadvantage of centralized model, attackers started to build alternate botnet.

II. LITERATURE REVIEW

Jin Zhigang, Wang Ying discovered, in IEEE 2012 [1], defines Semi-Distributed topology inP2P Botnet Detection and the main idea behind this paper is to find abnormality of botnet computer by using sociality analysis, which is branch

of data mining and traffic characteristics analysis by using Radial basis function of neural network. By using this technique Researchers has Discovered Photbot.

Hossein Rouhani, AzizahBt Abdul Manaf [2] explains the concept of P2P botnet Detection based on IRC (Centralized) communication topology. The main idea behind this paper ispassive network traffic monitoring. The model consists of filtering, application classifier, traffic monitoring, and analyzer. Hossein Rouhani, AzizahBt Abdul Manaf, [4] defines another technique to detect P2P Botnetbased on Traffic monitoring by using similar communication pattern and for Traffic monitoring researchers have used open source tool such as ARGUS (Audit record Generation& Utilization Tool).

Osman salem, Ali Makke,Jeantajer[5] discovered a technique to detect DDOS Attack. Idea behind this paper is that it defines method of Traffic Monitoring and anomaly detection overhigh speed network and the result of analysis of large no of traffic flow is store in Hash table.Alireza shahrestani, Maryam feily, rodina

Ahmad, Sureswaranramadass[3] , shows a technique of traffic monitoring by using Visual network monitoring system to detect botnet traffic in small and medium size network. This system works under Passive Network traffic monitoring system including Visual threat monitoring. This provides interfacing between botnet traffic and visual threat monitoring by HCI (human computer Interface).

Gu et al. has proposed BotSniffer [7] that uses network-based anomaly detection to identify Botnet C&C channels in a local area network. BotSniffer is based on observation that bots within the same Botnet will likely reveal very strong similarities in their responses and activities. Therefore, it employs several correlation analysis algorithms to detect spatial temporal correlation in network traffic with a very low false positive rate [7].

BotMiner [8] is the most recent approach which applies data mining techniques for BotnetC&C traffic detection. BotMiner is an improvement of BotSniffer [7]. It clusters similar communication traffic and similar malicious traffic. Then, it performs cross cluster correlation to identify the hosts that share both similar communication patterns and similar malicious activity patterns. BotMiner is an advanced Botnet detection tool which is independent of Botnet protocol and structure. BotMiner can detect real-world Botnets including IRC-based, HTTP-based, and P2P Botnets with a very low false positive rate [8].

Geobl and Holz [9] proposed Rishi in 2007. Rishi is primarily based on passive traffic monitoring for odd or suspicious IRC nicknames, IRC servers, and uncommon server ports.They use n-gram analysis and a scoring system to detect bots that use uncommon communication channels, which are commonly not detected by classical intrusion detection systems [9]. Disadvantage of this method is, it cannot detect encrypted communication as wellas non-IRC Botnets.

Strayer et al. [10] proposed a network-based approach for detecting Botnet traffic which used two step processes including separation of IRC flows at first, and then discover Botnet C&Ctraffic from normal IRC flows [10]. This technique is specific to IRC based Botnets.

Masud et al. [11] proposed effective flow-based Botnet traffic detection by mining multiple log files. They proposed several log correlation for C&C traffic detection. They categorize an entire flow to identify Botnet C&C traffic. This method can detect non-IRC Botnets [11].

Various bot detection approaches are shown in below figure.

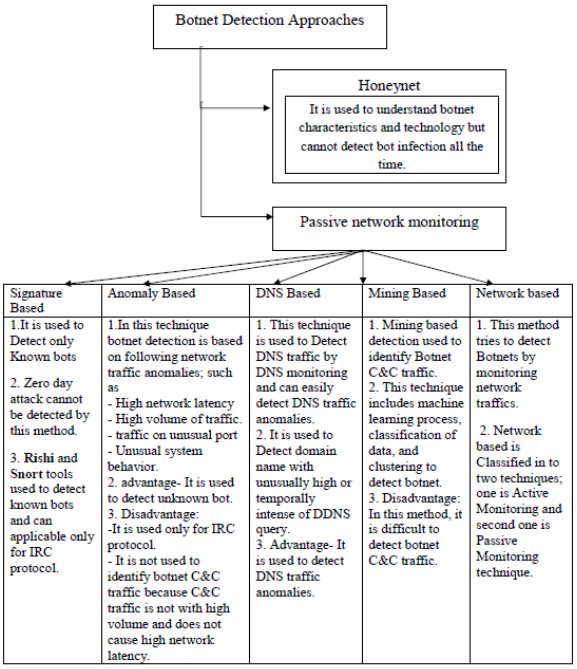

Fig1. Botnet detection approaches

III. PROBLEM DEFINITION

The objective of Botnet detection system is to provide security against bot. In my project, it not only detects victim machines within a monitored network that are part of a botnet, but also deactivating bot from victim machine. This can be done by using passive network monitoring technique. This project mainly focused on detection of victim machine inside traffic monitoring network, not the way internal hosts become infected (e.g., by Spam attachments, remote exploiting, virus).Main goal of the project is to monitor network traffic and gather information about IP, protocol, ports, etc. From this information by applying required algorithms we have to detect the bot pattern or DDOS attack or ToR network and report it to the user. The result analysis is divided into two main activities; first one is to view log report, and second activity is to determine how to detect and deactivate bot programmatically by using proposed algorithm.

IV. EXISTING TOOLS FOR BOTNET DETECTION

Detail description of existing botnet detection tools is as follows:

1. Snort[6]:

Snort is open source Intrusion detection tool. This is used to monitor network traffic to find signature of existing bot.

Advantage:

- It is useful tool to protect the organization network from intrusion.
- It is used to detect only known bots.

Disadvantage:

- Sort tool is not feasible to detect unknown bots.

2. BotSniffer[7]:

BotSniffer is anomaly based botnet detection tool. It is used to identify bot C&C channel in LAN. Bot Sniffer is based on observation that bots within same botnet will likely reveal very strong similarities in their response and activities.

Advantages:

- It uses several correlation algorithms
- It has very low false positive rate.

Disadvantage:

- If botnet traffic is normal traffic, this type of method cannot detect it.
- It is used to detect only IRC and HTTP.

3. BotMiner:[25]

BotMiner is the most recent approach which applies data mining techniques for Botnet C&C traffic detection. BotMiner is an improvement of Bot Sniffer [7].It clusters similar communication traffic & similar malicious traffic. Then, it performs cross cluster correlation to identify the hosts that share both similar communication pattern& similar malicious activity patterns.

Advantage:

- It is used to detect IRC, HTTP and P2P encrypted bot.
- It has low false positive rate.

Disadvantage:

- If the Challenger finds detection framework and implementation of Bot Miner, they might get some ways to avoid detection. For example if challenger does some changes in clustering or in the cross correlation plane.

4. Rishi[9][24] :

Geobl& Hal discover this technique. This method detect only well known bot. Rishiuses IRC bot nickname pattern as signature.

Disadvantage:

- It is not used to detect non IRC bot and encrypted bot.

5. Karasaridis et al[26][28] :

Karasaridis et al has study network flows and detect IRC botnet controllers in a fashion of following steps; in which, the most important one is to identify hosts with suspicious behavior and isolate flow records to/from those hosts.

Disadvantage:

- It is used to detect only for IRC botnet.

V. PROPOSED SYSTEM

The main objective of this project is to provide secure network service, to detect and report DDOS attacks or DDOS bots It is used to detect and deactivate P2P Zeus bot. Detect the ToR network or bots which can affect network as ToR. The system will work as show in below figure.

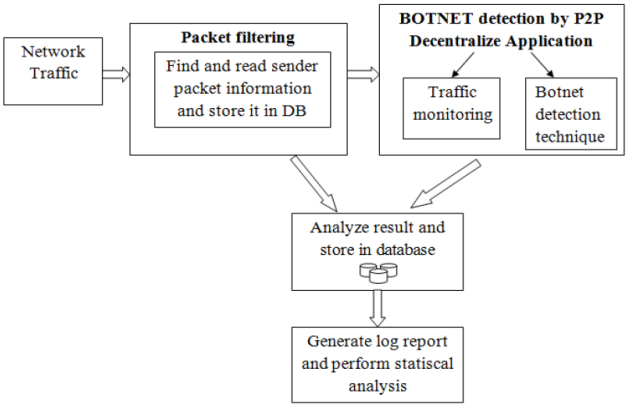

Fig2. System architecture of proposed system

VI. FUTURE SCOPE

In the future, different types of botnets may appear in addition toDDoS, Zeus, ToR botnets as discussed in this project work, so the proposed mechanism can be used as a general approach for the analysis and identification of the traffic flows produced by other types of botnets. In addition, it can also be applied to detect the unknown botnet.

VII. CONCLUSION

The Internet is persistently threatened by different types of malicious software such as viruses, worm and bots. These malware have a negative impact on both network and personal computers. The effect of attacking the Internet results in network delay due to congestion and wastage of bandwidth. On the other hand, the impact of attacking personal computers can include corrupting user's computers and stealing information. The proposed work is based on anomaly based detection method which is used to Detect and Deactivate bot from the victim machine to provide secure network service.

To detect and deactivate bot we need to monitor network traffic. It is used to get information of most access port along with its count and bar graph. This analysis is used to find Suspicious Port number. All this evaluation is used to Detect and Deactivate bot entry permanently from victim machine by using two different techniques. One is manual method by using command prompt and other is automated method which includes port block and by deleting the registry key entry for bot.

REFERENCES

[1] Jin Zhigang, Wang Ying "P2P botnet detection based on user Behavior sociality & Trafficentropy function". CECNet IEEE 2012, 1953 – 1955

[2] HosseinRouhani, AzizahBt Abdul Manaf," Botnet detection by monitoring similar communication pattern". IJCSIS, Vol. 7, No. 3, 2010

[3] Alirezashahrestani, Maryam feily, rodina Ahmad, Sureswaranramadass,in " Discoveryof invariant bot behavior through visual network monitoring system". IEEE 2010, Page(s):182 – 188

[4] HosseinRouhani, AzizahBt Abdul Manaf, in IEEE 2010 "Botnet Detection based on Traffic Monitoring ".Page(s): 97 – 101

[5] Osman salem, Ali Makke,Jeantajer," Flooding Attack detection in Traffic of backbonenetwork". LCN' IEEE 2011, Page(s): 441 – 449

[6] Snort IDS web page. http://www.snort.org, March 2006.

[7] GuofeiGu, Junjie Zhang, and Wenke Lee. "BotSniffer: Detecting Botnet Command andControl Channelsin Network Traffic." In Proceedings of the 15th Annual Network andDistributed System Security Symposium (NDSS'08), San Diego,CA, February2008.

[8] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysis of network traffic for protocol- and structure independent Botnet detection," in Proc. 17th USENIX Security Symposium, ACM-2008 Pages 139-154

[9] J. Goebel and T. Holz. Rishi: Identify bot contaminated hosts by irc nickname evaluation.In Proceedings of USENIX HotBots'07, 2007

[10] W. Strayer, D. Lapsley, B. Walsh, and C. Livadas, Botnet Detection Based on NetworkBehavior, ser. Advances in Information Security.Springer, 2008, PP. 1-24.

[11] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, K. W.Hamlen, " Flow-basedidentification of Botnet traffic by mining multiple in Proc. International Conference onDistributed Framework& Application,Penang,Malaysia.2008

[12]N.lanelli, A. Hackworth, Botnet as a Vehicle for online Crime, CERT, December 2005

[13] D Stutzbach and R Rejaie, Understanding churn in Peer2to2 Peer networks [A]. In Proc.ACM IMC' 06[C]. 2006. 189-202.

[14] "Exploit on Amnesty pages tricks AV software". The H online. Heinz Heise. 20 April2011. Retrieved 8 January 2011.

[15] Jump up^ Olsen, Stefanie (8 April 2002). "Web surfers brace for pop-up downloads". CNET News.Retrieved 28 October 2010.

[16] abuse.ch: "When a Botmaster goes REALLY mad"References73

[17]Dr,.Laheeb M. Ibrahim, Karan HatimThanoon, 'Detection of Zeus botnet in computernetwork and internet.

[18]http://www.antisource.com/article.php/zeus-botnet-summary

