© 2015 IJIRT | Volume 1 Issue 12 | ISSN: 2349-6002

HTTP Based Botnet Detection Using Characteristic Analysis

Minkesh G. Patel[1], Vinit Gupta[2]
[1]*Hashmukh Goswami College Of Engineering, Vahelal*
Gujarat Technological University, Ahmedabad, India
[2]*Assistant Professor, Hashmukh Goswami College Of Engineering, Vahelal*
Gujarat Technological University, Ahmedabad, India

Abstract **- Botnet as a new technology of attacks is a serious threat to Internet security. Using Rapid development of the botnet, we came across botnet based several protocols. According to the feature of botnet, Markov Model has application in botnet detection and can be used to match with the botnet characteristics. According to the situation and problems of the botnet, the life cycle and behavior characteristics of the botnet have been analyzed. In between, a method of detecting botnet based on this model has been proposed. Finally, we analyzed the experiments and summarized the experimental results, and validated the reliability of the detection method.**

Index Terms **– Botnet, Characteristics, Time To Live, Size Of Packet, Request Per Minute**

I. INTRODUCTION

A botnet is a system of zombie PCs controlled by a solitary element. For the most part, the zombies (Infected Machines) being used of a botnet are contaminated PCs running the Microsoft Windows working framework that have been tainted with a malware. These Infected PCs correspond with other botnet machines by means of the Internet. Most botnets are disseminated configuration frameworks and with the botnet administrator offering directions to just a little number of machines. These machines then spread the directions to other tainted machines, as a rule by means of IRC. The disseminated outline of botnet keeps the disclosure of the controlling PCs. The obscurity that a botnet manages regularly helps the client evade identification and conceivable arraignment.

Botnets are profitable in performing assignments that would be unthinkable given just a solitary IP location, single PC, or a solitary Internet association. As the spam business has get to be gainful, and ISPs normally end administration to endorsers who send spam, botnets were discovered to be a compelling asset for sending spam. Moreover, numerous bargained PCs contain location books of email locations which can be joined into the rundown of locations to send spam to. Botnets are self-spreading and self-organising networks of compromised computers (‘bots') that can be used to perform malicious activities in a coordinated way under control of a botmaster. Botnets can vary in size from hundreds to millions of bots and it is infected by malware ('botagents') and receive commands from the botmaster to carry out malicious activities against bots inside the botnet (internal attacks) or computer systems outside the botnet (external attacks). There are various Examples of malicious activities of botnet which includes stealing sensitive data such as passwords, committing click fraud, manipulating online banking transactions, compromising new hosts to extend the botnet, performing distributed denial-of-service(DDos) attacks, and sending spam or phishing e-mails[6].

An auxiliary goal of the botnet is to discover and taint extra PCs. While this is not viewed as an essential target all by itself, Scaling of the botnet by means of digestion of new PCs helps it perform the essential goals all the more productively. Consequently, this optional goal is frequently the greater part of a botnet's assignments. Numerous PC systems, particularly those utilizing Microsoft Windows PCs running the default settings, characteristically trust different PCs on the same system. Subsequently, a solitary bargained machine on such a system constitutes an assault vector against different machines on the system. Other optional botnet targets incorporate site ad clicking, web program toolbar establishments, key logging, and social bookmarking survey control.

All around related PCs are typically the biggest focuses for botnet administrators hoping to extend their portfolios. College frameworks and even fast broadband-joined PCs are consistently under assault, yet these aren't the old school assaults of a couple of years back, where a human was endeavouring some adventure. These are computerized filtering and profiteering instruments that keep running from existing botnets. No one on the Internet is excluded from these tests, yet in the event that a PC is tainted on a high velocity association, it will get a higher cost.

II. ANALYSIS OF BOTNET CHARACTERISTICS

Both botnet in light of IRC convention and botnet taking into account HTTP convention fit in with botnet taking into account concentrated C/S structure. Their summon and control systems are effective in execution. Notwithstanding, as a concentrated correspondence focus, once the control server is controlled or annihilated by others, the entire botnet will be broke down. With the advancement of P2P innovation, the P2P-based botnet starts to exist. This sort of botnet is unique in relation to that in light of concentrated C/S structure. Case in point, P2P-based botnet has no middle control server. Then again, each casualty in P2P-based botnet can spread and get orders and controls autonomously. So that, there will be little impact to P2P-based botnet if a percentage of the casualties are identified or controlled.

A. Lifecycle of a Botnet

The lifecycle of a typical botnet can be separated into 4 phases: Infection, Bootstrapping and Maintenance , Command & Control , Command Execution as in

1. **Infection**: introductory establishment of botnet malware on target host. this is finished by deceiving clients into running executables to connected to email. By misusing their program shortcoming or abusing the vicinity of security gaps.
2. **Bootstrapping and Maintenance**: every hub needs to perform an arrangement of activities to identify the vicinity of different hubs and unite with them, bot controller must have the capacity to neutralize when its related hubs leave the botnets. Such upkeep operation have a central part in guaranteeing strength.
3. **Command & Control**: botmaster and controller have the need of dependably circulating their command(e.g. by sending the charge begin ddos target=192.133.0.10 or send spam mail layouts bot programming redesigns) to their controlled hubs. that thus to send related results, or current status into back to bot expert.
4. **Command Execution**: particularly concerns the movement of running the got summon on every individual bot this may infer issuing any sort of spontaneous, undesirable or unfriendly activity on the system.

B. Characteristics of Botnet

The HTTP-based botnet distribute a site page as a unified control charge stage. It is secret in correspondence instrument, on the grounds that the bots in HTTP-based botnet visit the incorporated control sites by typical HTTP convention. Nonetheless, there are some sure attributes in the sites which distribute incorporated control orders. Case in point, the incorporated control pages contain some irregular strings or suspicious scripts etc. Also, there are a few similitudes in correspondence messages and correspondence frequencies between bots in HTTP-based botnet and the brought together control site.

III. ARCHITECTURE OF BOTNET

A second center issue for botnet aggressors is the means by which to speak with every bot example. Most assailants would like the capacity to quickly send guidelines to bots additionally don't need that correspondence to be identified or the wellspring of the those summons to be uncovered.

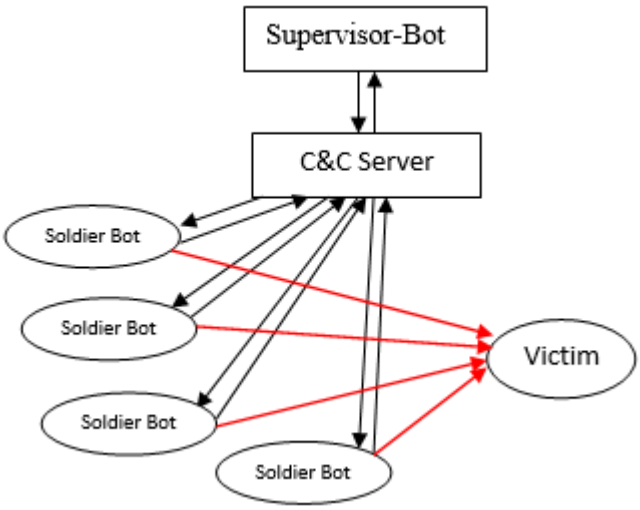

Fig 1 Centralised Botnet Architecture

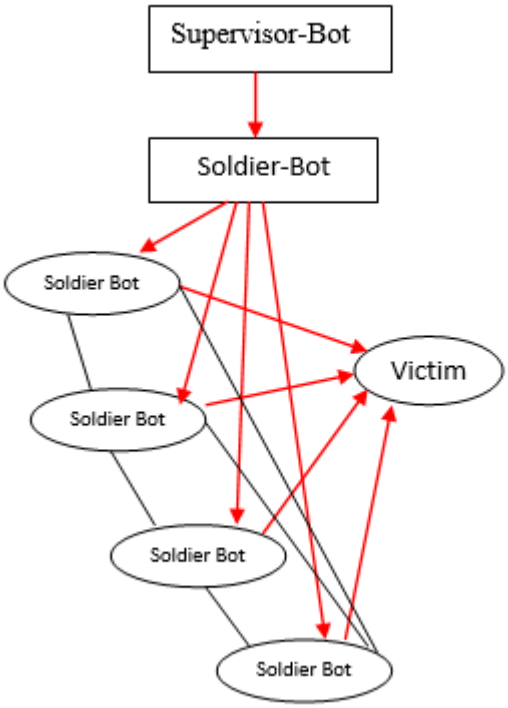

Fig 2 P2P Botnet Architecture

a) **Centralized**: A centralized topology (Fig 1) is portrayed by a main issue that advances messages between customers. Messages sent in a concentrated framework have a tendency to have low idleness as they just need to travel a couple surely understood jumps. From the viewpoint of an assailant, unified frameworks have two noteworthy shortcomings: they can be less demanding to recognize following numerous customers join the same point, and the revelation of the focal area can trade off the entire system[2].

b) **P2P** : Peer to Peer (P2P)(Fig 2) botnet correspondence has a few vital focal points over concentrated systems. Initial, a P2P correspondence framework is much harder to upset. This implies that the bargain of a solitary bot does not so much mean the loss of the whole botnet. Then again, the outline of P2P frameworks is more unpredictable and there are ordinarily no sureties on message conveyance or latency[2].

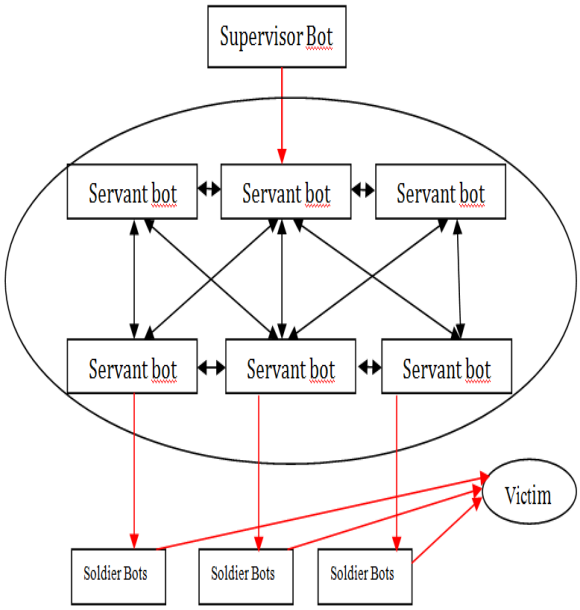

Fig 3 Hybrid Botnet Architecture

c) **Hybrid**: Hybrid(Fig 3) is like P2P where Supervisor-Bot taking care of a P2P correspondence between directors acting like server group. However, a Supervisor-Bot breed, keep data, and keep a hearty BOTNET ready to keep up control of its remaining bots from huge introduction or making it harder through their correspondence movement designs of the system topology of its fighter bot group. Each Supervisor Bot has its own list of associate and does not offer it with others bots for security purposes[2].

IV. DETECTION METHOD

We have given brief idea about architecture and mechanism of botnet. After doing repeated analysis of zeus bot we have come up with three things with which we can catch bot at our server. Those are size of packet, time to live and request per minute.

We have implemented this thing in php language using MYSQL server. We have implemented bot net detection mechanism at server side which analyze each and every request that comes to our sever and we are capturing several details which we required to detect bot. After capturing those details which includes IP address of infected machine as well as normal machine and that bunch of request is analyzed in bot net detection module in which we are referring size of packet, time to live and request per minute. So Here I am taking each of characteristic and mentioned below how I analyzed the http request and pick the threshold value of that.

- **Size of Packet** : When any request comes on the server or on any website it comes through http or https. Https is secured one which we have not considered in our research. We are only experimenting on http request. When somebody land on our site and we are registering him and making him to fill up his details then after clicking on submit all of this data should go to server in the form of packet and using http request. Now this packet is in the form of byte. When normal computer is making request then this packet size may be fixed which we can judge based on its all request and comparing them with other request. Since bot is used for DDos (Distributed denial of service) attack, There may be difference in the packet that is sent by bot. So it is differed from normal packet and its size is more than the normal request size. So we have considered this threshold value of packet size and putting it dynamically in the module.
- **Time to live** : This characteristic state that how much time http request is live. It means call out time of request. This characteristic is also possible parameter of bot because normal request and bot request has difference. Hence we are analyzing this from the request and deciding threshold value of this parameter so that we can detect bot.
- **Request Per Minute** : This characteristic state that how many request comes from one user. We are getting many request on our website if we are having high ranking website so to detect bot request among this request we have decided one more parameter which can be a bot characteristic. In this characteristic we will fetch all the request which is coming from the same ip address or same mac address. We have fetched all of that request and analyzed that and concluded that normal user can request atmost 30(it can varry) request but if there is bot then request is coming at certain interval and it can be more than 30 so we can say that those request might be done from bot computer.

V. EXPERMENT RESULTS

By considering all above mentioned characteristics we have performed experiment by taking 500 http request and 50 bot request so we got following results which represented in table :

Total request in database	500
Total bot request in database	50
Bot detected by base paper algo	37
Bot detected by proposed algo	47(43 actual bots)

Table 3 HTTP requests analysis

Parameter	Detected bot
Time to live	26
Request in a minute	8
Packet size	13
Total	47(43 actual bots)

Table 4 BOT Detected by defined characteristics

VI. CONCLUSION

The number of users connected to the Internet almost doubled in the last five years and it is increasing day by day and This rate is expected to increase in view of technological advancements in the area of wireless communication. However, the remarkable growth in Internet usage is out of proportion to security knowledge of common users. Botnets take cyber attacks to the next level by misusing the aforementioned inconsistency. Botnets make use of variety of mechanisms to compromise users' machines. A botnet treat different itself from other malware in the capability of its compromised machines to establish C&C(Command and Control) with remote server(s) controlled by human misfeasor(s).

We have presented comprehensive classification related to botnet detection. The suspicious hosts are detected by modelling to botnets based on state division with the Markov model which is mentioned in this report and proposed algorithm. According to the Implementation method, We have defined characteristics such as time to live request, size of packet and request per minute and using this we are able to increase the efficiency of botnet detection.

VII. FUTURE WORK

We have proposed few characteristics with which we are able to detect infected pc which are infected with bot. We have taken zeus bot which is open source bot and available for experiments. We have done experiment based on the characteristics which we found while doing reverse engineering of bot. For Future work, There is space to find few more characteristics using which we can improve detection of http based bot.

REFERENCES

[1] Wei WAN, Jun LI," Investigation of State Division in Botnet Detection Model", ICACT2014

[2] Ihsan Ullah, Naveed Khan, Hatim A. Aboalsamh, "SURVEY ON BOTNET: ITS ARCHITECTURE, DETECTION, PREVENTION AND MITIGATION", 978-1-4673-5200-0/13 IEEE 2013

[3] Sheharbano Khatta k, Naurin Rasheed Ramay, Kamran Riaz Khan, Affan A. Syed, and Syed Ali Khayam," A Taxonomy o f Botnet Behavior ,Detection, and Defense" , IEEE COMMUNICAT IONS SURVEYS & TUTORIALS, VOL . 16, NO. 2, SECOND QUART ER 2014

[4] Lei Cao and Xiaofeng Qiu, "Defence Against Botnets: A Formal Definition and a General Framework", IEEE Eighth International Conference on Networking, Architecture and Storage 2013

[5] Esraa Alomari**, Selvakumar Manickam*, B. B. Gupta***, Parminder Singh*, Mohammed Anbar*,"Design, Deployment and use of HTTP-based Botnet (HBB) Testbed", ICACT2014

[6] Timo Schiess,Harald V ranken," Counter Botnet Activities in the Netherlands", ICITST-2013

[7] Liming Huan, Yang Yu, Liangshuang Lv, Shiying Li, Chunhe Xia," A Botnet-Oriented Collaborative Defense Scheme Description Language", 978-1-4799-2548-3/13/2013 IEEE

[8] Robert F. Erbacher, Adele Cutler, Pranab Banerjee, Jim Marshall," A Multi-Layered Approach to Botnet Detection", USU Research Foundation

[9] Hossein Rouhani Zeidanloo, Azizah Bt Abdul Manaf," Botnet Detection by Monitoring Similar Communication Patterns", Vol. 7/No.3/2010,IJCSIS

[10] Jivesh Govil, Jivika Govil, "Criminology of BotNets and their Detection and Defense Methods", IEEE EIT 2007

[11] Zhaosheng Zhu, Guohan Lu, Yan Chen, Zhi Judy Fu, Phil Roberts, Keesook Han," Botnet Research Survey", 0730-3157/08/2008 IEEE

[12] Sajjad Arshad, Maghsoud Abbaspour,Mehdi Kharrazi,Hooman Sanatkar," An Anomaly-based Botnet Detection Approach for Identifying Stealthy Botnets", 978-1-4577-2059-8/11/2011 IEEE

[13] N.S.Raghava, Divya Sahgal, Seema Chandna," Classification of Botnet Detection Based on Botnet Architechture", 978-0-7695-4692-6/12/2012 IEEE

[14] ByungHa Choi, Sung-kyo Choi, Kyungsan Cho," Detection of Mobile Botnet Using VPN", 978-0-7695-4974-3/13/2013 IEEE

[15] Kazumasa Yamauchi, Yoshiaki Hori, Kouichi Sakurai," Detecting HTTP-based Botnet based on Characteristic of the C&C session using by SVM", 978-0-7695-5075-6/13/2013 IEEE

[16] Hachem Guerid,Karel Mittig,Ahmed Serhrouchni," Collaborative Approach for Inter-domain Botnet Detection in Large-scale Networks", 978-1-936968-92/3/2013 ICST

[17] S.S.Garasia,D.P.Rana,R.G.Mehta," HTTP BOTNET DETECTION USING FREQUENT PATTERNSET MINING", Volume-2, Issue-3, 619 – 624/2012 IJESAT