July – Sep © 2019 Transactions; 6(23): 1307-1313

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Review Report

An overview on architecture of botnet and techniques towards the botnet detection

Ramesh Gadde [1] and Dr. Suresh Pabboju [2]

Corresponding Author:
gadde.ramesh@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.6.23(2)2019

Manuscript:
Received: 02nd July, 2019
Accepted: 10th Aug, 2019
Published: 15th Sep, 2019

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

As of late, botnets are the most radical of all digital attacks and turning into the major issue towards cloud computing. Botnets are the system of various traded off PCs and/or cell phones. These gadgets are contaminated with vindictive code by botmaster and controlled as gatherings. The assailants utilize these botnets for criminal exercises, for example, DDoS, click extortion, phishing, spamming, sniffing activity and spreading new malware. The main issue is how to recognize these botnets? It turns out to be all the more fascinating for the analysts identified with digital security? This focuses us to compose an audit on botnets, its architectural structure and detection techniques.

Keywords: botnet architecture, bots, botmaster, botnet attacks, botnet, detection techniques.

[1] Research Scholar, [1 2] Department of Computer Science and Engineering,
[1] Osmania University, Hyderabad, Telangana, India -500 007.
[2] Professor & Head, Department of Information Technology,
[2] Chaitanya Bharathi Institute of Technology (Autonomous),
[2] Gandipet, Hyderabad, Telangana, India - 500 075.

IJRA - Year of 2019 Transactions:
Month: July - September
Volume – 6, Issue – 23, Page No's:1307-1313
Subject Stream: Computers

Paper Communication: Author Direct

Paper Reference Id: IJRA-2019: 6(23)1307-1313

DOI: 10.17812/IJRA.6.23(2)2019

International Journal of Research and Applications
July - Sep © 2019 Transactions 6(23): 1307-1313

eISSN : 2349 – 0020
pISSN : 2394 – 4544
www.ijraonline.com

COMPUTERS REVIEW REPORT

An overview on architecture of botnet and techniques towards the botnet detection

Ramesh Gadde [1] and Dr. Suresh Pabboju [2]

[1] Research Scholar, [1 2] Department of Computer Science and Engineering,
[1] Osmania University, Hyderabad, Telangana, India -500 007.
[2] Professor & Head, Department of Information Technology,
[2] Chaitanya Bharathi Institute of Technology (Autonomous),
[2] Gandipet, Hyderabad, Telangana, India - 500 075.
[1] gadde.ramesh@gmail.com, [2] plpsuresh@gmail.com

ABSTRACT

As of late, botnets are the most radical of all digital attacks and turning into the major issue towards cloud computing. Botnets are the system of various traded off PCs and/or cell phones. These gadgets are contaminated with vindictive code by botmaster and controlled as gatherings. The assailants utilize these botnets for criminal exercises, for example, DDoS, click extortion, phishing, spamming, sniffing activity and spreading new malware. The main issue is how to recognize these botnets? It turns out to be all the more fascinating for the analysts identified with digital security? This focuses us to compose an audit on botnets, its architectural structure and detection techniques.

Keywords: botnet architecture, bots, botmaster, botnet attacks, botnet, detection techniques.

1. INTRODUCTION

The sharp increment of the web in the past period performed to have encouraged a development in the events of online attacks [1]. At the advanced time web is turning into the basic need of everybody. Today age is the period of cloud computing, which encourage the clients to access and store the information through cloud. Cloud computing is a portrayal for empowering all over the place, great, on-demand organize access to an open, private and cross breed shared pool of computing assets like stockpiling, administrations, server, systems, and application.

These administrations can be given least administration endeavors and rapidly. Gadgets which are associated with the web are these days under the danger of various attacks performing through PC noxious programming's [2] [3]. The cloud servers can be gotten to through web, the more utilization of cloud computing drives the cloud computing toward the more digital attacks.

Botnet is one of the preeminent perilous danger to the digital security [4] in these all. Botnet is the blend of two terms, Bot stands for Robot and Net stands for Network, the gathering of traded off contaminated web associated gadgets are called botnet.

Botnet give the one-to-numerous relationship instrument amongst command and control server and bots that is the reason the botmaster utilize botnet for commercial, digital attacks and so on. Once a gadget is contaminated with noxious code, it turns into the piece of a botnet, and begin working for the botmaster without knowing to the end client. Botnet spread itself an opportunity to time by trading off an ever increasing number of gadgets as cell phones, PCs, PCs and diverse servers. The quantities of digital attacks which are found in the web these days, most clients are influenced by these attacks are performed through botnet. Botmaster can perform diverse sort of cybercrime like DDoS, click misrepresentation, phishing extortion, key logging, bit coins extortion, spamming, sniffing

activity, spreading new malware, google AdSense mishandle with bots[6].

These days the botnet is turning into the base of all cybercrime which is performed through the internet [7] [8]. Botmaster utilize distinctive strategies to taint a client gadget to make it bot (zombie) like drive by download , email and pilfered programming's are the most widely recognized method for attacks[9][10]. As per the past research loads of the detection approaches have been proposed. Be that as it may, a large portion of them are centered on the disconnected detection of botnet; still we have to center around the constant detection [11].

The current botnet detection techniques are order into two principle bunches given as Honeynets Based Detection Technique and Intrusion Detection System [12]. Specialists center on the digital security to identify botnets attacks and keep cloud servers from the botnet attacks. Yet inquire about on botnet detection is juvenile, and need more research to enhance information security in cloud computing.

In the rest of the areas of this paper, we display writing audit, botnet life cycle, architectures, detection techniques, future work and conclusions.

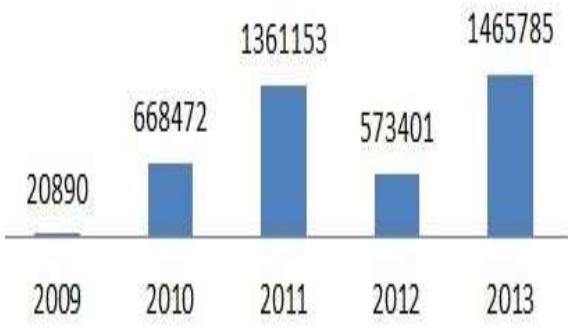

Fig 1: Botnet Drones Attack in Malaysia [14].

The record general cases performed by botnets are DDoS, click misrepresentation, phishing extortion, key logging, bitcoins extortion, spamming, sniffing activity, spreading new malware, google AdSense manhandle, secret word stealer and mass data fraud with bots [6].

Like worms proliferation the botnet additionally spread itself, comparatively like infection, botnet likewise keep it escaped detection. Botnet has a coordinated control and command framework that is the reason it assault comparative various standardization unaccompanied devices. It goads with a high tainted by botnet, bots are otherwise called a zombie that is the reason a botnet is additionally called zombie network.

Cyber criminals begin thinking initial 1990 to make a botnet for the sake of entertainment, however later their brain was completely changed to make a botnet for benefit. Egg drop was the principal botnet made in 1993 [13]. Gtbot and Spybot were made in 2000.

Essentially unique sorts of botnets are made in various vacancy with more propel techniques and marks, to secure these botnets from cyber-security. As per MYCERT (Malaysian Computer Emergency Response Team) measurements report of most recent five years demonstrates that the botnet rambles attacks are expanded with a high ratio [14].

2. BOTNET LIFE CYCLE

At the point when the botmaster needs to contaminate another casualty gadget, for this botmaster ought to experience legitimate stages, beginning disease, optional infusion, association, sending malignant code and support and refreshing. Initial a botnet taint new gadget associated with the web, at that point it infuse some pernicious code utilizing distinctive conventions like Hyper Text Transfer Protocol (HTTP), FTP and P2P. After effectively infusing the pernicious code, the casualty gadget consequently make an association with officially existing command and control server. Once a malignant code is infused to the casualty gadget then it turns into a zombie. In the fourth step the botmaster send commands the bot armed force through the command and control server [15] [6]. This performs vindictive exercises as indicated by the commands which the casualty gadget gets from the command and control servers [16]. The last advance is to keep up and refresh the zombie dynamic constantly, it send updates to the zombie gadgets time to time [17] [18].

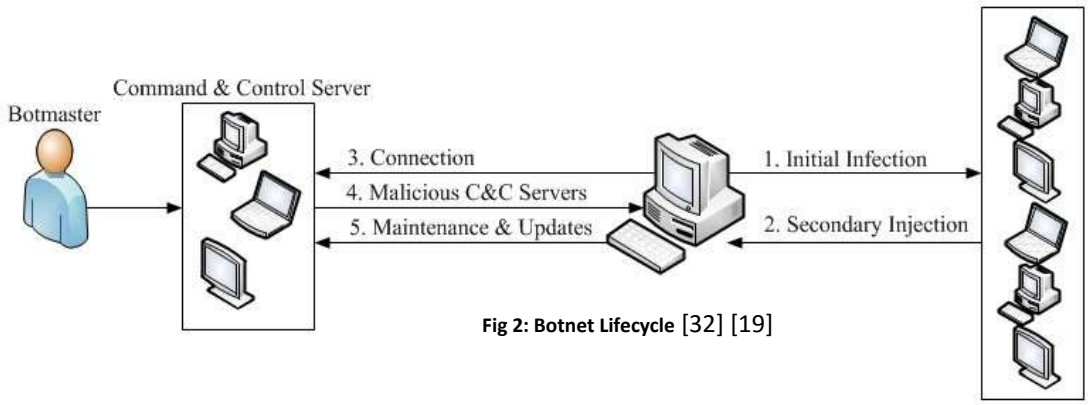

Fig 2: Botnet Lifecycle [32] [19]

3. BOTNET ARCHITECTURES

The route through which the individual bots frame a botnet are grouped into three classes as indicated by their architectures. In this paper we present a few strategies for arranging the botnet architectures, and likewise the favorable circumstances and weaknesses are clarifying here.

a) **Centralized Architecture:**

Centralized Botnet architecture is the most straightforward to control and oversee by the botmaster. In concentrated architecture the botmaster control and regulate every one of the bots in a botnet from a solitary essential issue called command and control server (C&C Server). Along these lines it's implying that in concentrated botnet architecture every one of the bots are get commands and answer to an essential issue called C&C server. There are two kinds of topologies utilized as a part of unified botnet architecture; names are star topology and progressive topology. The key conventions are utilized as a part of unified architecture are web hand-off talk (IRC) and Hyper Text Transfer Protocol (HTTP) [6][19] [20].

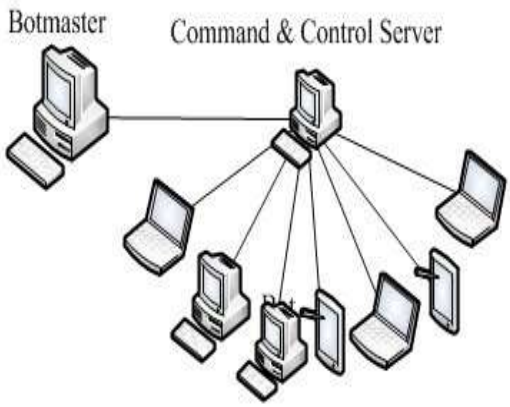

Fig 3: Centralized Botnet Architecture [19] [32] [31]

Administration and checking of botnet is simple due to one essential issue. The botmaster straightforwardly speak with bots basically and rapidly. In the brought together architecture the outline is less perplexing; while message inertness and survivability is low. The primary cons of brought together architecture are the disappointment chances is more than other architecture.

b) **Decentralized Architecture:**

In decentralize or distributed architecture there is no single element in charge of controlling the bots in a botnet. There are in excess of one C&C server which speak with bots. The detection of such a botnet which utilizing decentralized architecture is harder as contrast with incorporated architecture.

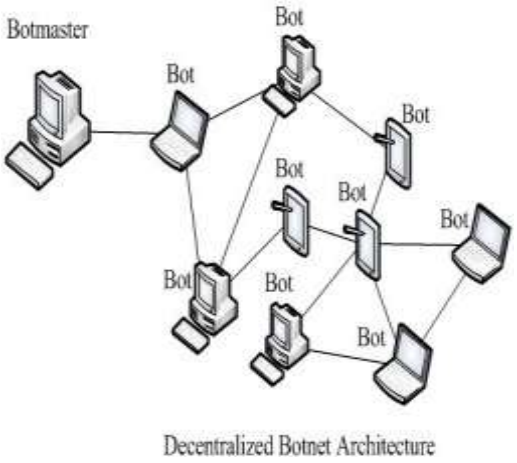

Fig 4: Architecture of Decentralized Botnet [19] [32] [31]

Decentralized architecture in view of the shared conventions. As contrast with concentrated architecture the plan of distributed architecture is more unpredictable, detection of botnet have

such architecture is harder than other botnet. Additionally message inertness and survivability is high than brought together botnet architecture.
In decentralized architecture the disappointment chances are less as contrast with brought together architecture in light of the fact that on the off chance that one command and control server moves toward becoming disappointment then the other C&C server can oversee and screen the botnet [22].

c) **Hybrid Architecture:**

Hybrid architecture is the blend of both incorporated and decentralized architecture. In hybrid architecture there are two sorts of bots, one is hireling and the other is customer bot [24]. The bots are associated with the hybrid botnet it is possible that they are customer or hireling. Observing and detection of botnet having hybrid architecture are harder than botnet having brought together and decentralized architectures; while the outline isn't much perplexing.

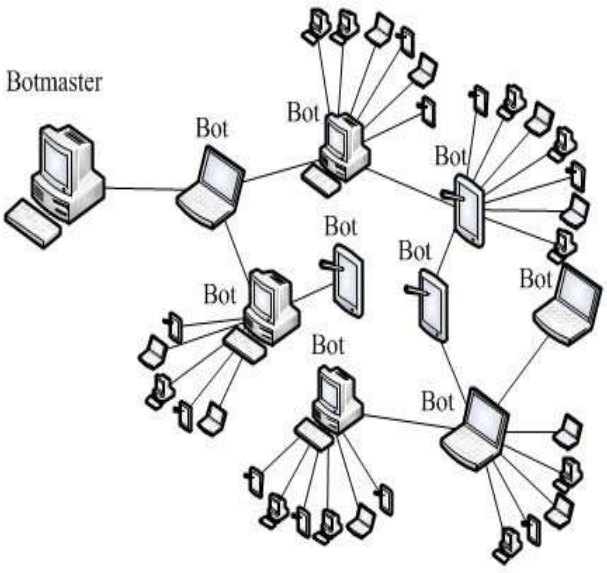

Fig 5: Hybrid Botnet Architecture

4. BOTNET DETECTION TECHNIQUES

Botnet detection is the most imperative undertaking to enhance the cyber-security against different cyber-attacks happens in web these days. As indicated by the past research botnet detection techniques can be arranged into two classifications honeynets detection techniques and interruption detection techniques [12] [25] [26]. Interruption detection system is additionally partitioned into sub-classifications.

Honeynets & Honeypots Based Detection System: Honeynets and Honeypots both are indicating the end client gadgets. These end clients PC's are the most ideal approach to gather basic data about the cyber-attacks. This end client PC is simple for botmaster to assault and bargain, since it's extremely powerless against malevolent attacks. The cyber-security gathering will have the capacity to make great detection techniques under the gathered data about the botnet attacks through these honeynets. As indicated by the past research the botnet change their mark time to time due to the security reason and honeynets are critical for understanding these botnet properties [27][28]. In honeynets detection procedure honeywall is vital, which is utilized for observing, gathering, changing and controlling correspondence over the honeypots.

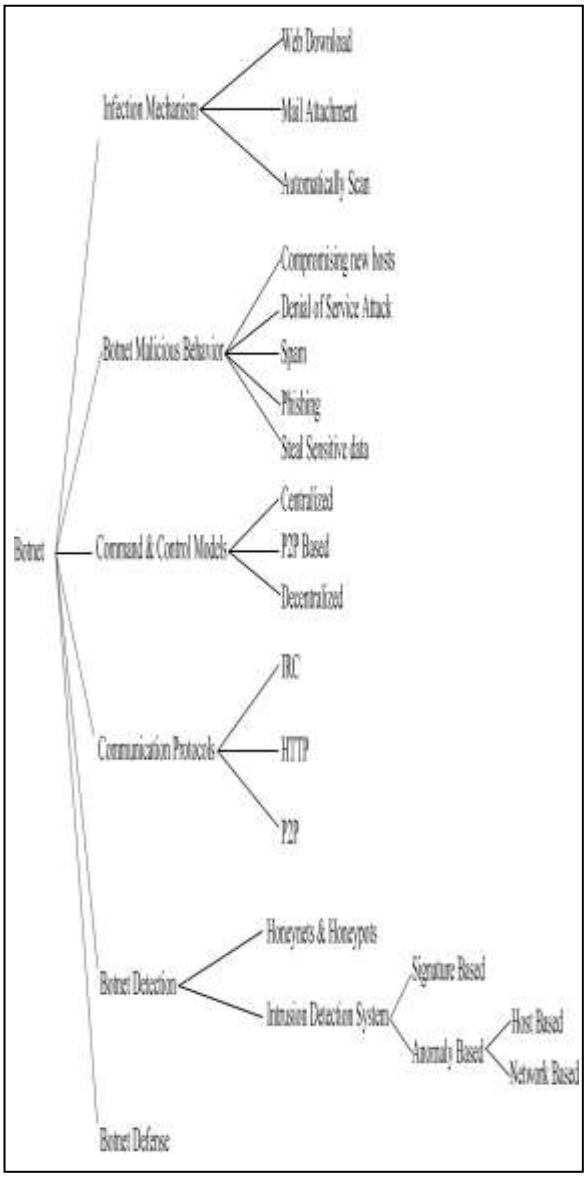

Fig 6: Botnet Taxonomy [31] [20]

i) **IDS (Intrusion Detection System):**

Intrusion detection system is utilizing for checking the movement stream for the pernicious exercises of a network. Amid the activity on the off chance that it discovered some noxious assault it specifically advise the PC system or the head of the system. IDS have likewise the abilities to make a move against such malevolent exercises to hinder the activity originating from the infection contaminated system. There are two sorts of interruption detection system one is signature based and the other is anomaly based.

ii) **Signature Based Detection:**

In signature based botnet detection system the malware known as the parcel arrangements or the transportation of the bytes arrangement in looking for network [29]. The key favorable position of this detection procedure is that signatures are so easy to develop and acknowledge in the event that you recognize what network execution you're attempting to discover. This system is excessively basic and straightforward and create. The Botmaster change signatures of each assault with time in light of the fact that to make a botnet assault more secure from the bot contaminated machines[29][30].

iii) **Anomaly Based Detection:**

This strategy centers on the possibility of basis for network execution. Anomaly based botnet detection strategy can acknowledge just that network exercises or activity which is indicated by the heads or which is encourage by the chairman or both in the progress. In this strategy the control ought to be characterized ahead of time for every convention and each to be tried for precision. It recognizes those occasions which not identified with the bolster or acknowledged model of execution. Anomaly based detection strategy is somewhat costly as per calculation yet it is more secure than signature based detection system. This strategy has likewise a few weaknesses in which the principle cons is meaning of guidelines is exceptionally troublesome. For various conventions there are distinctive guidelines are characterized, which are all the more difficult activity. Anomaly based system is additionally have some impediment about the time and checking the bot tainted machines [29] [31]. This system is additionally sorted into network and host based detection techniques.

5. CONCLUSION AND FUTURE WORK

The expanding in number of web clients turns out to be twofold over the most recent couple of years. The more utilization of web drives the clients to the cloud computing, while the more utilization of cloud computing drives the cloud computing to the cyber-attacks. Botnet is one of the greatest cyber-assault these days. It separates itself from other malware being able to influence other machine to trade off for a cyber-assault. Botnet engender itself an opportunity to time, and change its shape and signature likewise with time. Still quarter of the all web associated PCs and cell phones are the piece of botnet making diverse kinds of criminal exercises without knowing to the end clients. In this paper we introduce detail of botnets, attacks, its distinctive kinds of architectures, and detection techniques. In every one of the three distinct architectures it utilizes diverse conventions as given in detail. Still detection of botnet is juvenile; specialists need to accomplish more research on this territory.

However in future the scientist can do explore on the anomaly based botnet detection, making base as high network dormancy, correspondence on surprising and regular ports, which demonstrate the malware.

REFERENCES

1) E. Alomari, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers : Classification and Art," vol. 49, no. 7, pp. 24– 32, 2012.
2) M. Thapliyal, N. Garg, and A. Bijalwan, "Botnet Forensics : Survey and Research Challenges," no. April, 2013.
3) F. Carpine and S. Maria, "Online IRC Botnet Detection utilizing a SOINN Classifier," pp. 1351– 1356, 2013.
4) R. A. Rodr, I. Omez, G. M. A-plant, and P. Garc, "Study and Taxonomy of Botnet Research through Life-Cycle," vol. 45, no. 4, 2013.
5) I. Ullah, N. Khan, and H. a. Aboalsamh, "Overview on botnet: Its architecture, detection, counteractive action and alleviation," 2013 tenth IEEE Int. Conf.

networking, Sens. Control, pp. 660– 665, Apr. 2013.
6) S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: An overview," Comput. Networks, vol. 57, no. 2, pp. 378–403, Feb. 2013.
7) "Botnets the New Threat Landscape White Paper [Threat Control] - Cisco Systems."
8) M. Zahid, A. Belmekki, and A. Mezrioui, "another architecture for identifying DDoS/savage compelling assault and decimating the botnet behind," 2012 Int. Conf. Multimed. Comput. Syst., pp. 899–903, May 2012.
9) W. Paper, "Life structures of a Botnet."Microsoft Security Intelligence Report," vol. 15, 2013.
10) W. Xianghua and C. Lijun, "Investigation and Design of Botnet Detection System," 2012 Int. Conf. Comput. Sci. Serv. Syst., pp. 947– 950, Aug. 2012.
11) X. Zang, A. Tangpong, G. Kesidis, and D. J. Mill operator, "Botnet Detection Through Fine Flow Classification," no. 0915552, pp. 1– 17, 2011.
12) C. Batt, "Eggheads," Food Microbiology, vol. 16, no. 3. p. 211, Jun-1999. "Malaysian Computer Emergency Response Team.".
13) M. Feily, A. Shahrestani, and S. Ramadass, "A Survey of Botnet and Botnet Detection," 2009 Third Int. Conf.
14) Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications", Volume 1, Issue 1, and Jan-Mar 2014 [ISSN: 2349-0020].
15) H. Choi, H.Lee, H. Lee, H. Kim, Botnet Detection by Monitoring Group Activities in DNS Traffic,7th IEEE International Conference on Computer and Information Technology (CIT 2007).
16) G. Gu, J.Zhang, and W. Lee, BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic, 15th Annual Network & Distributed System Security Symposium, 2008.
17) S. Ji, C.Im, M. Kim, H. Jeong, "Botnet Detection and Response Architecture for Offering Secure Internet Services," 2008 International Conference on Security Technology, pp.101- 104, 2008.
18) K.Takemori,Y. Miyake, C. Ishida, I.Sasase,A SOC Framework for ISP Federation and 18 Gu-Hsin Lai , Chia-Mei Chen1, and Ray-Yu Tzeng2, Chi-Sung Laih2, Christos Faloutsos3 Attack Forecast by Learning Propagation Patterns, Intelligence and Security Informatics, Vol.23, No.24, pp.172 - 179,2007
19) R. Villamarín-Salomón and J. Carlos Brustoloni, Bayesian bot detection based on DNS .traffic similarity, Proceedings of the 2009 ACM symposium on Applied Computing, 2009,p.p 2035-2041.
20) Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1, Jan-Mar 2014 [ISSN: 2349-0020].
21) A. Wald. Sequential Analysis. Dover Publications, 2004.
22) Wang, Wallace (2004-10-25). "Instant Messaging and Online Chat Rooms: Internet Relay Chat (IRC)". Steal this File Sharing Book (1st Ed.). San Francisco, California: No Starch Press. pp. 61 – 67. ISBN 1-59327-050-X.
23) Claire Elliott, "Botnets: To what extent are they a threat to information security?" Information Security Group, Royal Holloway, University of London, Technical Report 15, 2010. pp: 79-103, www.sciencedirect.com.
24) Maryam Feily, Alireza Shahrestani, Sureswaran Ramadass "A Survey of Botnet and Botnet Detection" Third International Conference on Emerging Security Information, Systems and Technologies, University of Malaysia, 2009. pp: 268-273.
25) Hossein Rouhani Zeidanloo, Mohammad Jorjor Zadeh, shooshtari, Payam Vahdani Amoli, M. Safari, Mazdak Zamani "A Taxonomy of Botnet Detection Techniques" University of Technology Malaysia, 2010 IEEE, pp: 158-162.
26) Kuochen Wang, Chun-Ying Huang, Shang-Jyh Lin, Ying-Dar Lin "A fuzzy pattern-based filtering algorithm for botnet detection" 2011 Elsevier B.V. All rights

reserved, pp: Computer Networks 55 (2011) 3275–3286.

27) Hossein Rouhani Zeidanloo, Azizah Bt Manaf, Payam Vahdani, Farzaneh Tabatabaei, Mazdak Zamani "Botnet Detection Based on Traffic Monitoring" International Conference on Networking and Information Technology- University of Technology Malaysia, 2010. pp: 97-101.
28) Chunyong Yin, Ali A. Ghorbani "P2P Botnet Detection Based on Association between Common Network Behaviors and Host Behaviors" 2011 IEEE, pp: 5010-5012.
29) David Zhao , Issa Traore , Bassam Sayed , Wei Lu , Sherif Saad , Ali Ghorbani , Dan Garant "Botnet detection based on traffic behavior analysis and flow intervals" 2 University Of Victoria , Canada ª 2013 Elsevier Ltd. All rights reserved. pp: computers & security 39 (2013) 2 -16.
30) Paul Sroufe, Santi Phithakkitnukoon, Ram Dantu, and João Cangussu" Email Shape Analysis for Spam Botnet Detection" University of North Texas,USA, ©2009 IEEE, pp: 1-2.
31) Dan Garant, We i L u "Mining Botnet Behaviors on the Large-scale Web Application Community" Keene State College, Keene, NH USA, © 2013 IEEE Computer Society, and pp: 185-190.
32) Tao Wang, Shun-Zheng Yu "Centralized Botnet Detection by Traffic Aggregation" SUN YAT-SEN University Guangzhou, China, © 2009 IEEE Computer Society, pp: 86-93.
33) Wen-Hwa Liao, Chia-Ching Chang "Peer to Peer Botnet Detection Using Data Mining Scheme "2010 IEEE Trancations.
34) Hyunsang Choi, Hanwoo Lee, Heejo Lee, Hyogon Kim "Botnet Detection by Monitoring Group Activities in DNS Traffic" Seventh International Conference on Computer and Information Technology, Korea University-2007, pp: 715-720.
35) H. Choi, H.Lee, H. Lee, H. Kim, Botnet Detection by Monitoring Group Activities in DNS Traffic,7th IEEE International Conference on Computer and Information Technology (CIT 2007).
36) G. Gu, J.Zhang, and W. Lee, BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic, 15th Annual Network & Distributed System Security Symposium, 2008.
37) S. Ji, C.Im, M. Kim, H. Jeong, "Botnet Detection and Response Architecture for Offering Secure Internet Services," 2008 International Conference on Security Technology, pp.101- 104, 2008.
38) K.Takemori,Y. Miyake, C. Ishida, I.Sasase,A SOC Framework for ISP Federation and 18 Gu-Hsin Lai , Chia-Mei Chen1, and Ray-Yu Tzeng2, Chi-Sung Laih2, Christos Faloutsos3 Attack Forecast by Learning Propagation Patterns, Intelligence and Security Informatics, Vol.23, No.24, pp.172 - 179,2007.
39) R. Villamarín-Salomón and J. Carlos Brustoloni, Bayesian bot detection based on DNS .traffic similarity, Proceedings of the 2009 ACM symposium on Applied Computing, 2009,p.p 2035-2041.
40) A. Wald. Sequential Analysis. Dover Publications, 2004.
41) Sumalatha Bandela, Ramesh Gadde and Dr. Suresh Pabboju "Survey on Cloud computing Technologies & Security threats" in International Journal of Research and Applications April – June © 2015 Transactions, eISSN: 2349-0020 & pISSN: 2394-4544 Volume-2, Issue-6, pp: 296-308. DOI: 10.17812/IJRA.2.6 (53)2015.
42) Wang, Wallace (2004-10-25). "Instant Messaging and Online Chat Rooms: Internet Relay Chat (IRC)". Steal this File Sharing Book (1st Ed.). San Francisco, California: No Starch Press. pp. 61 – 67. ISBN 1-59327-050-X.
43) "Top Threats to Cloud Computing V1.0", Cloud Security Alliance, March 2010. http://www.cloudsecurityalliance.org/.