IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. V (Sep – Oct. 2014), PP 28-33
www.iosrjournals.org

P2P-BDS: Peer-2-Peer Botnet Detection System

Navjot Kaur[1], Sunny Behal[2]
[1](CSE Department, Shaheed Bhagat Singh State Technical Campus, Ferozepur, India)
[2](CSE Department, Shaheed Bhagat Singh State Technical Campus, Ferozepur, India)

Abstract: *Internet has become an inevitable part of our lives. While internet offers a mass of useful services which makes communication easier and faster than ever, it presents some threats too along the way. Over the last few years, botnet has risen to become the primary source for various internet attacks such as DDos attacks, spamming, phishing etc. Accordingly, a great deal of research has focused on methods to detect and extenuate the effects of botnets. In this paper, we have analyzed the feasibility of outgoing and incoming traffic i.e. intrusions and extrusions, to detect P2P based botnets. We present an approach that uses a network perimeter mentoring system called bothunter. As a part of the research work, a botnet detection system for peer to peer botnets called P2P-BDS has been proposed.*

Keywords: *Attacker, Bot, Botmaster, Extrusion, Intrusion, IRC, peer to peer, Zombie*

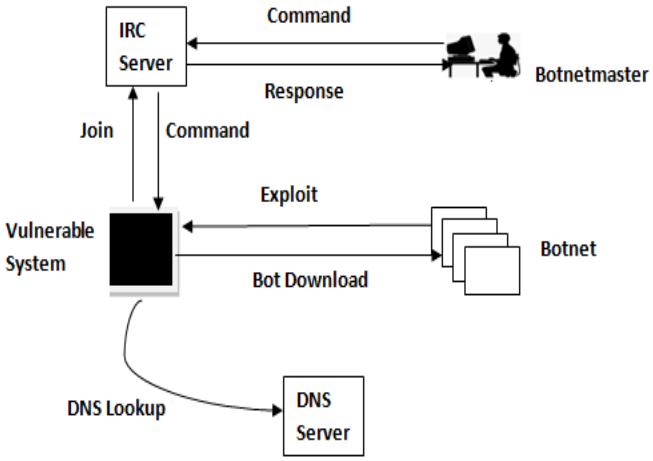
I. Introduction

Now a days various threats to internet security are emerging in the world. Among these threats botnets are treated as most widespread and dangerous threats which occur mostly in today's internet attacks [1, 2]. The term bot also known as zombie is the abbreviation of the term software robot [3] that are used to perform various set of automated functions which is triggered by the various commands. Botnets are the network of vulnerable machines under a common control of central server that is controlled by the single or small group of attackers known as botmaster [4], usually for financial profit or to launch attacks on network [5]. Botmaster takes advantage of compromised system that allows malicious code to be installed on machine without the knowledge of the owners. All vulnerable machines connect to the central server and wait for the botmaster's command. Botnets are different from all other malwares in the way that they follow the command and control approach [6]. To detect and mitigate botnets various researchers developed the set of techniques [7, 8, 9, 10]. From the study of literature [11], We have various kinds of C&C based servers such as centralized based C&C server,P2P based C&C server, Hybrid C&C server, Random C&C server. Botnets can cause a big damage on revenues [12]. One in 5 financial companies estimates outages will affect their revenues by $50k per hour .CNBC reports that in 2013 US banks are the targets of largest wave of botnets ever, were knocked offline for 249 days. 249*50,000=$12,450,000[13]. Botnets not only effect the revenues, but also effects the resources allocation to the customers. Botnets are also responsible for DDos attacks which cause a loss of service to user [14]. Therefore there is a great demand for the detection of the botnets to protect the network from malicious attacks. In this work. we proposed a network based botnet detection system for the detection of malicious attacks occurs in network.

1.1 Working of IRC based Botnet

Botnets have different phenomenon from the previous generation of malwares. Unlike the previous malwares in which a worm is the self-propagating software that infects the compromised system, botnet uses the different scenario. Botnets are based on C&C (Command and Control) phenomenon in which they firstly connect to the C&C server from which they receives the commands they are supposed to run as shown in figure 1.

Firstly a botmaster exploits the vulnerabilities on the victim host, after that victim host downloads the bot binary and contacts the IRC server address by resolving the DNS name and then victim joins the IRC server to receive the commands from the botmaster [15].This research work uses the advanced botnet life cycle model given in [16].



Fig, 1. Working of IRC based botnet

1.2 Life Cycle of a Botnet

Figure 2 describes the typical botnet infection dialog model. In the infection dialog model, the infection begins with an external to internal communication flow that contains the inbound scanning or bot scanning (E1) or a direct inbound exploit (E2). When the victim host has been completely compromised, then this host downloads a binary instance of the bot (E3). After the full binary instance of the bot is executed, it will have two paths type I and type II [16].In the type I bot, the victim host directly moves to the outbound scan (E5). Whereas in type II bots, the infected host moves to the C&C server communication (E4) then it will move to the outbound scanning.

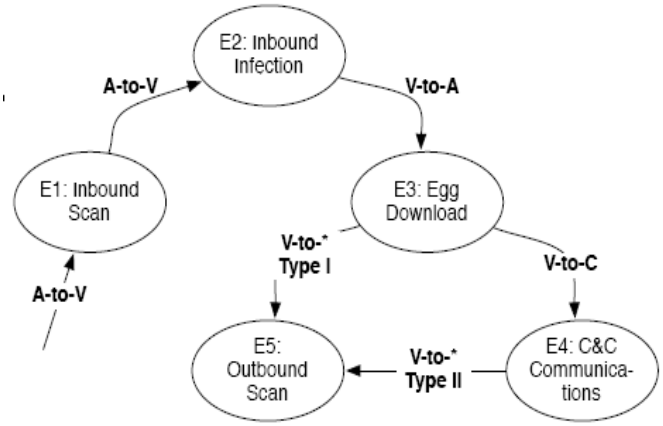


Fig. 2. Life cycle of a typical Botnet

Most of the botnet detection and mitigation techniques developed by various authors are based on centralize C&C sever. In these type of servers by locating the central server and destroying it, one can easily remove or shutdown the whole botnet [17]. In response to this botmasters have developed new generation botnets known as Peer -2-Peer botnets to make their botnets more resilient.

In these type of botnets the communication doesn't heavily depend on a few selected servers. Destroying a single or even a number of bots will not necessarily lead to the destruction of an entire botnet [11]. Therefore dealing with such botnets is a challenging task, still some techniques to detect these botnets have been proposed [18, 19, 20]. Our primary contribution to this paper is:

- To develop a new kind of traffic monitoring technique which focus on detecting the peer-2-peer botnet infection by analyzing outbound and inbound traffsic.
- To use the existing open source and freely available software to develop a network based detection system of peer-2-peer botnet based attacks.

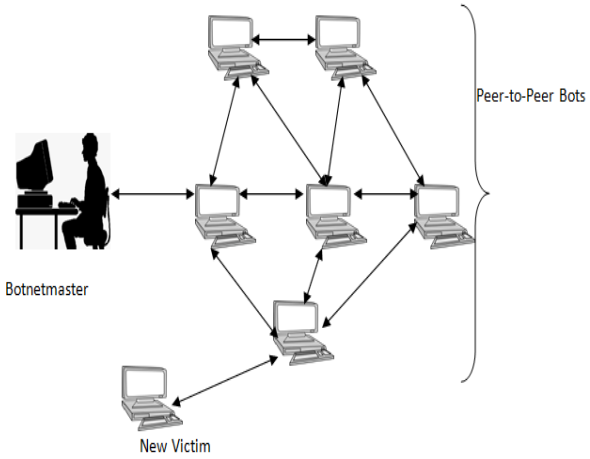


Fig. 3: Peer-2-Peer based botnet

The remaining sections of the paper are as follows: Section II and Section III classify the proposed work and methodology of botnet detection system. Section IV describes the experimental setup of proposed work. Section V classifies the various results obtained by monitoring the traffic and the last section concludes the work done by defining the future scope of the system.

II. Related Work

The proposed work uses the Botnet detection system called a Bothunter proposed in paper [16]. BotHunter is a network defensive system driven by Snort which is an open source software [21] and fits in our approach of monitoring the traffic in both ways i.e. inbound and outbound. Bothunter focus on monitoring of two way communication between the internal and external flow of network. It is based on the algorithm called network dialog correlation, in which it correlates the inbound intrusion alarms with outbound communication patterns that are highly indicative of successful local host infection [22]. We present our experimental results in virtual and live testing environment. In this work we focus on all outgoing and incoming traffic. C. Lussi [23] used the concept of extrusion to detect different types of malware in virtual environment. The author used the network traces of five popular worms to validate the approach but the author proposed only detection system. The work done in paper [23] focuses only on the further propagation of the botnets, while in this work we focus on monitoring the inbound and outbound traffic i.e. extrusions and intrusions to get the clear indication about a successful botnet attack. Sunny Behal [15] has developed N-EDPS i.e. Network based Extrusion Detection and Prevention System to detect certain kind of botnets. Though, they have been able to find number of prominent botnets. However, there is a need to analyze both kind of traffic to detect botnets. We use the signature based detection instead of anomaly based system. The main idea behind the signature based system is to extract the pattern information on the packet and match pattern available in the database of the bots. Whereas in anomaly based system the main goal is distinguish the normal traffic with the abnormal traffic by monitoring the behavior of the system [24, 25]. Apart from the botnet detection tool used in the proposed work, some other botnet based detection tools are also available like Botminer [26], Botsniffer [9], Botfinder [27], Botswat [28], BotInfer [29]. Previous work on botnet detection has mainly focused on identifying infected bot computers based on centralized C&C server .This paper aims to fill this gap by presenting a new approach called Botnet detection system for peer-2-peer based botnets.

III. Methodology Of Proposed Work

We have proposed a system called P2P- BDS as shown in figure 4, which will detect the network from the various malicious attacks caused because of botnets. Here the traffic of the organization will be analyzed for peer to peer bots and the results will be stored in the log file for future references and analysis. In our system, we have included a detection engine that will detect the bot profiles and based on the available signatures it will generate the alerts.

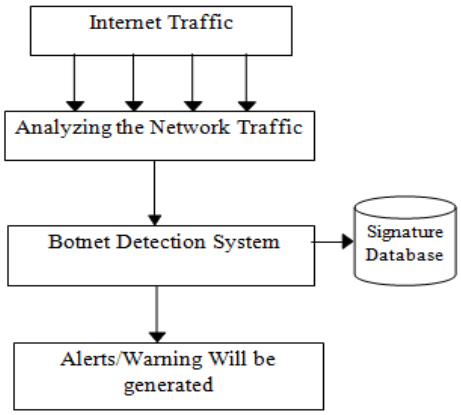


Fig. 4 Proposed methodology of BDS

The signature database of detection system contains number of rules with which we want to generate an alert or a warning. After this we are now able to refine the botnet infected traffic from the normal traffic resulting in botnet free traffic. In our methodology of P2P-BDS we use active IDS (Intrusion detection system) which monitor the packets continuously and detect the botnet attack in real time. Passive IDS can only recognize intrusions however active IDS can detect and respond to them. In the proposed work the Network-based IDS has been used instead of Host-based IDS. A Network-based IPS monitors the network traffic of a particular network whereas a Host-based IPS monitors the operating system, applications, and the host specific network traffic. Signature based detection system is used which is useful to detect an important class of attacks which is characterized by signatures by searching a malicious pattern in the packet. For the development of P2P-BDS we use an open source and free software.

IV. Implementation Of BDPS

The proposed P2P-BDS consist of Detection engine and for the implementation of detection engine we use bothunter as detection engine which is based on an open source snort. The experimental results of BDS are presented in live testing environment. The experimental setup of proposed system is shown in figure 5. We placed the proposed BDS between the SBSSTC network and the internet server to monitor the Internet traffic.

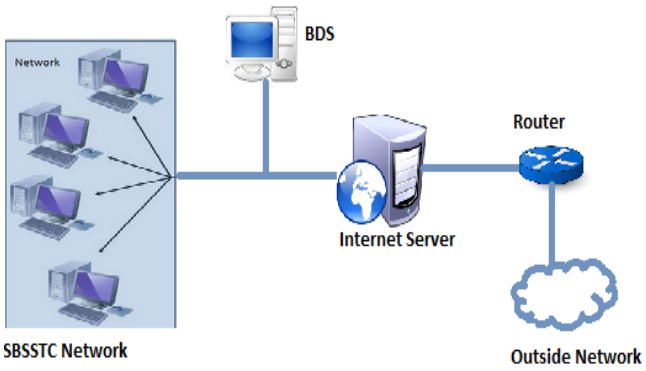


Fig. 5. Experimental Setup of P2P-BDS

V. Results

We placed BDS for four weeks in SBSSTC network as shown in figure 5. We have been able to find 34 infected computers, 24 C&C servers, 28 egg download servers and 36 IP addresses of outbound scanning servers as shown in Table 1. The names of botnets found are shown in the Table 2.

Table 1: Output of BDS

Victim IP addresses	C&C server IP addresses	Egg Download source IP addresses	Outbound scanning system's IP addresses
172.16.2.162	195.216.243.2	174.36.201.82	202.164.142.254
172.16.1.12	199.2.137.252	74.208.64.145	202.227.180.157
172.16.1.20	221.7.91.31	208.43.162.198	202.164.194.229
172.16.1.197	64.94.137.106	69.95.64.198	202.164.142.172
172.16.2.151	65.43.232.379	62.62.101.118	202.227.180.157
172.16.2.153	74.208.164.166	83.68.16.36	202.122.154.150
-	-	-	-
-	-	-	-
172.16.2.176	78.109.24.106	193.136.28.167	202.149.1.162

Table 2:. Botnets Detected

Name of the botnet	Type of the botnet
Kademlia	Peer-2-Peer Bot
Phatbot	Malicious Bot
Nugache	Malicious Bot
Napster	Peer-2-Peer Bot
BitTorrent	Peer-2-Peer Bot
Ares	Peer-2-Peer Bot
Peacomm	Malicious Bot

VI. Conclusion and future scope

Peer-to-Peer botnets have same goals as of centralized C&C botnets. The main difference between both scenarios is that there is no central point of failure in Peer-2-Peer based botnets. In this paper we showed the methodology of botnet detection for botnets with central server to botnet which uses Peer-to-Peer botnets. This research work is based on the concept of monitoring outbound and inbound traffic i.e. Extrusions and Intrusions. As a part of the work we have proposed a system known as P2P Botnet Detection and System using an open source and freely available software. We placed our system in the live environment of SBSSTC for the period of four weeks and during this analysis we are able to find various infected system, C&C servers, egg download source list and outbound scanning servers. The main drawbacks of the proposed system are: Firstly, it is unable to identify the novel botnets. Secondly, it should always update the knowledge base with new signatures which may reduce the performance and thirdly our system is not able to detect the encrypted C&C communication. These drawbacks can be removed if we merge behavior-based detection system with P2P- BDS. In future work, we plan to combine the anomaly based detection and signature based detection for better results. The system can be extended if we add prevention engine which will react to the network from new kinds of botnets like hybrid C&C based botnets.

References

[1] Honeynet Project. Know your Enemy: TrackingBotnets, March 2005. http://www.honeynet.org/ papers/bots.

[2] G. Schaffer, "Worms and Viruses and Botnets, Oh My! : Rational Responses to Emerging Internet Threats", IEEE Security & Privacy, 2006.

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

[4] B. Saha and A, Gairola, " Botnet: An overview," CERT-In White Paper(CIWP)-2005-05,2005

[5] Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., and Zhang, J., 2009. Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. EURASIP Journal on Wireless Communications and Networking, Vol.2009.

[6] N. lanelli, A. Hackworth, "Botnets as a vehicle for online crime," CERT Request for Comments(RFC) 1700, December 2005.

[7] J. R. Binkley and S. Singh. An algorithm for anomaly-based botnet detection. In Proceedings of Second Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'06), pages 43,48 July 2006.

[8] F. Freiling, T. Holz, and G. Wicherski. Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks. In Proc. of 10th European Symposium On Research In Computer Security (ESORICS'05),2005.

[9] G. Gu, J. Zhang, and W. Lee. BotSniffer: Detecting botnet command and control channels in network traffic. In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), February 2008.
[10] A. Karasaridis, B. Rexroad, and D. Hoein. Wide scale botnet detection and characterization. In Proceedings of Hot Topics in Understanding Botnets (HotBots'07), April 2007.
[11] Sunny Behal , Krishan Kumar, " Classification of C & C based Botnet Architectures," International Journal of Engineering & Information Technology, ISSN 0975-5292, Vol. 1(2009), pages 28-32.
[12] "Zeus botnet steals $47M from European bank customers", 2012. http://news.cnet.com/8301-1009_3-57557434-83/zeus-botnet-steals-$47m-from-european-bank-customers/
[13] http://www.neustar.biz/resources/whitepapers/2012-ddos-attacks-report
[14] Sunny Behal, Krishan Kumar, Vishal Arora, "Classification of Flood Based DDoS Attacks," Proceedings of International Conference on Wireless Networks and Embeeded Systems (WECON), Pages 521-524, October 18-19, 2008.
[15] Sunny Behal, Amanpreet Singh Brar, Krishan Kumar, "Signature-based Botnet Detection and Prevention", ISCET, pp.122-127,2010.
[16] Gu, G., Porras, Ph., Yegneswaran, V., Fong, M., Lee, W. "BotHunter: Detecting malware infection through IDS-driven dialog correlation", In 16th USENIX Security Symposium (Security' 07), 2007.
[17] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A multi-faceted approach to understanding the botnet phenomenon. In Proceedings of ACM SIGCOMM/USENIX Internet Measurement Conference, Brazil, October 2006.
[18] Hund, R., Hamann, M., Holz, T.: Towards next-generation botnets. In: EC2ND:European Conference on Computer Network Defense. pp. 33–40. IEEE Computer Society (2008).
[19] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling. Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. In Proceedings of the First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '08), 2008.
[20] Raihana Syahirah Abdullah et al., "Revealing the Criterion on Botnet Detection Technique", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013, Pages 208-215
[21] https https://www.snort.org/
[22] Sunny Behal, Krishan Kumar, "Extrusion: An Outbound Traffic based approach to detect Botnets," International Journal of Information and Telecommunication Technology, Vol. 2, Issue 1,2010, ISSN: 0976-5972, pages 71-76.
[23] Cecile Lussi. Master's thesis on "Signature-based Extrusion detection" ETHZ (TIK), 2008.
[24] Sunny Behal, Krishan Kumar, " A Review on Botnet Defense Mechanisms: Detection, Tracing, Mitigation and Prevention",International Conference on Computer Engineering & Technology, Jodhpur(ICCET-2010), IEEE, 13-14 Nov., 2010, page no. 25-33.
[25] David Zhao, Issa Traore, Bassam Sayed, Wei Lu, Sherif Saad, Ali Ghorbani and Dan Garant, "Botnet detection based on traffic behavior analysis and flow intervals", ELSEVIER, Computers & Security, Vol .39, 2013, pp. 2-16.
[26] Guofei Gu, Roberto Perdisci, Junjie Zhang, and Wenke Lee, "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection". In USENIX Security, 2008.
[27] F. Tegeler, X. Fu, G. Vigna, and C. Kruegel. BotFinder: Finding Bots in Network Traffic Without Deep Packet Inspection. In Proceedings of the 8th international conference on Emerging networking experiments and technologies - CoNEXT '12, pages 349–360, New York, New York, USA, 2012. ACM Press.
[28] A. Nummipuro, "Detecting P2P-Controlled Bots on the Seminar on Network Security, Espoo, Helsinki, 2007.
[29] Dong Guo, Yukun He, Qiang Li , Yuede Ji," BotInfer: A Bot Inference Approach by Correlating Host and Network Information", Spriger.Volume 8147, 2013, pp 356-367