ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

A Survey on Botnet Detection Based On Anomaly and Community Detection

Vorsu Yadigiri [1] , Nalla Abhishek [2] , Kurma Sailesh [3] Mudireddy Uday Kiran [4]

Assistant Professor, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India [1]

B.Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India [2]

B.Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India [3]

B.Tech Student, Department of Computer Science & Engineering, Guru Nanak Institutions, Hyderabad, India [4]

ABSTRACT: Botnets are the foremost common vehicle of cyber-criminal activity. They're used for spamming, phishing, denial-of-service attacks, brute-force cracking, stealing non-public data, and cyber warfare. A botnet may be a range of net computers that, though their homeowners are unaware of it, are got wind of to forward transmissions (including spam or viruses) to alternative computers on the web. During this paper, we have a tendency to propose a two-stage approach for botnet detection. the primary stage detects and collects network anomalies that are related to the presence of a botnet whereas the second stage identifies the bots by analyzing these anomalies.

KEYWORDS: Optimization, Anomaly detection, cyber-security, Botnets, social networks, random graphs

I. INTRODUCTION

Internet services are increasing in popularity and many new online services appear every day. The attacker's interest may thus be converted from curiosity to economic benefit. Attackers utilize different types of malware to accomplish their goals. Among the diverse types of malware, the Botnet is considered to be the most dangerous means of performing online crimes A Botnet network contains Bots, which are computers infected by malware such as Trojan horses, backdoors or worms without the user permission. The Botmaster remotely manages a Botnet through a C&C channel Recently, Botnets have been sold and rented in an underground market by Botmasters for commercial profit. They can begin many cyber-crimes: creating phishing web pages, carrying out massive amounts of spam emails, stealing sensitive user's information and generating DDoS attacks the scale of Botnet contaminations worldwide makes the detection of Botnet activity an important task. Botnet detection has been a significant subject in the cyber security domain for the last decade. Despite concerted efforts reported in the literature degrade the malicious activities of Botnets, the diversity of Botnet structures and protocols creates from the Botnet detection a demanding task for the cyber-security society.

II. EXISTING SYSTEM

In the existing system we are using bot graph technique we need flow clustering-based analysis approach to identify hosts that are mostly likely running P2P applications. in this we are sending the message to the user without protection due to this attacker may It is mainly due to the fact of that the traffic profile a bot-compromised host might be completely distorted by the legitimate P2P application which is running on it simultaneously. The main disadvantages of this process is due to the centralized command and control server. Servers are that they represent a single point of failure.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

III. PROPOSED SYSTEMS

In the proposed systems we are using Coarse grained botnet detection. in this process message to the peers is sending through scanning and with protection the message is divided in to packets in this technique and transfer to the user if the attacker attacks any of it he could get the whole information about the message in this it is having two process active and the deactivate state in the active state we can give protection and in deactive we can no give protection advantage of this process. We also identify the performance bottleneck of our system and optimize its scalability. We presented a novel botnet detection system that is able to identify stealthy botnets, whose malicious activities may not be observable.

IV. BOTNET THREATS

A Botnet is more dangerous than previous more traditional threats such as worms and viruses. The Honeynet project listed many kinds of Botnet attacks, including such as DDoS, Spam, Stealing information and Exploiting resources. Moreover, that Botnets can be exploited in several kinds of cybercrimes

i. DISTRIBUTED DENIAL OF SERVICE

The DDoS is one of the most potent threats produced by Botnets. The massive number of members in a Botnet network gives the DDoS considerable destructive power. The Botmaster uses the Botnet network to take down the victim system of control as the Bots members send huge numbers of requests to this system. In addition, some massive Botnet scan even be harmful to Internet Service Providers (ISPs).

ii. SPAM

Spam is an operation where an overwhelming quantity email messages containing advertisements or malicious links are sent to a large number of users. A Botnet is the best choice for an attacker use as a tool to send spam emails. The spam attacks start by sending commands to the Bots from Botmaster before they begin sending spam email to the victim's address. In this case, the detection approaches that used a blacklist technique become useless and hereby hard to detect a real attacker. identified Botnets as the major cause of email spam problems. In a study which set out to determine the source of email spam, found that the Botnets were responsible for 79% of spam email received at the University of Washington.

iii. STEALING INFORMATION

A Botmaster employs Bots to collect secret information from victim hosts by using techniques such key logging, reading log files and screen capture. For example, the SDBot is a type of Botnet which employs a key logging technique to gather user's sensitive information. This can then be sold to others in order to perform illegitimate actions In addition, the Zeus Bot's main tools use key logging methods to steal credit card information and private bank accounts, which allows the Botmaster to extract passwords and usernames from a bank web page, emails, and social network accounts Moreover, this Bot exploits the Windows application program interface (API) to extract private user information before the web browser can encrypt it.

iv. EXPLOITING RESOURCES

Bot hosts are controlled to perform illegal activities. For example, the Bot uses the victim's computer to visit a website periodically to increase the number of website visitors without the user's permissions. In addition, they can be used to cast fake votes or to grow the number of followers on Twitter and Facebook.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

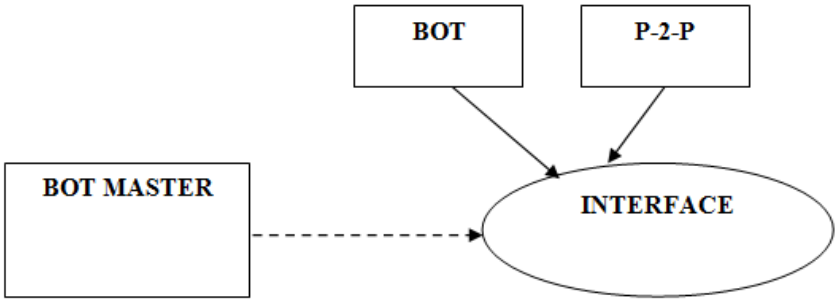
Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

V. MODULES

i. USER INTERFACE DESIGN

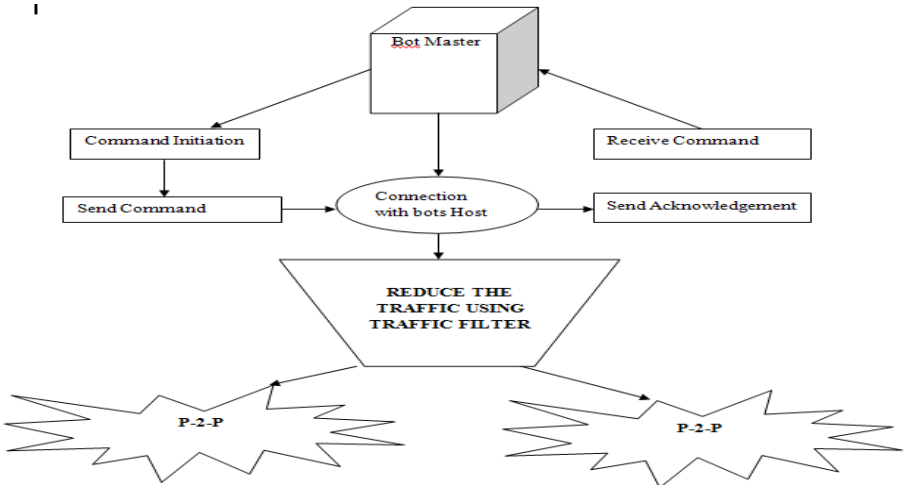
In this module of Botnet detection we design the windows for the project. These windows used to send a message from one user to another. We use the Swing package available in Java to design the User Interface to provide graphical user interface to peer.



a) User interface design

ii. DE-ACTIVATE TRAFFIC

The Traffic Filter component aims at the filtering out network traffic that is unlikely related to P2P communications. This is accomplished by passively analyzing DNS traffic, and identifying network flows whose destination IP addresses are previously resolved in the DNS responses. Specifically, we leverage the following feature: P2P clients usually contact their peers directly by looking up IPs from a routing table for the overlay network, rather than resolving a Domain name.



b) De-activate traffic

iii. COARSE GRAINED PEER-TO-PEER DETECTION

This component is responsible for detecting P2P clients by which analyzing the remaining network flows after the Traffic Filter component in the process. For each host within the monitored network we identify two flow sets, which are the flows related to successful outgoing TCP and UDP connections, respectively. We consider as successful

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

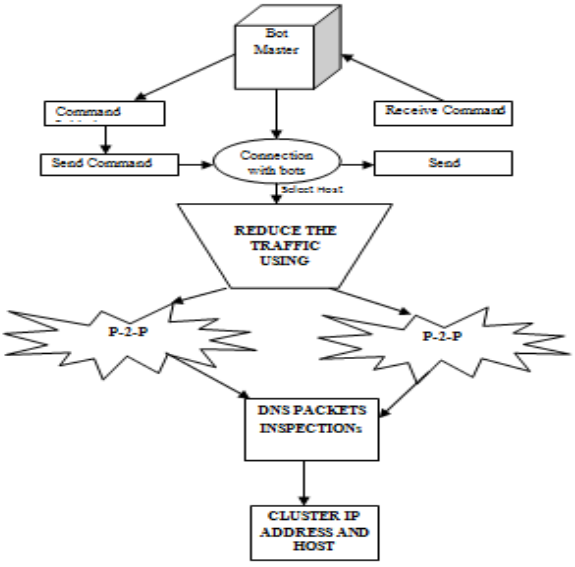
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

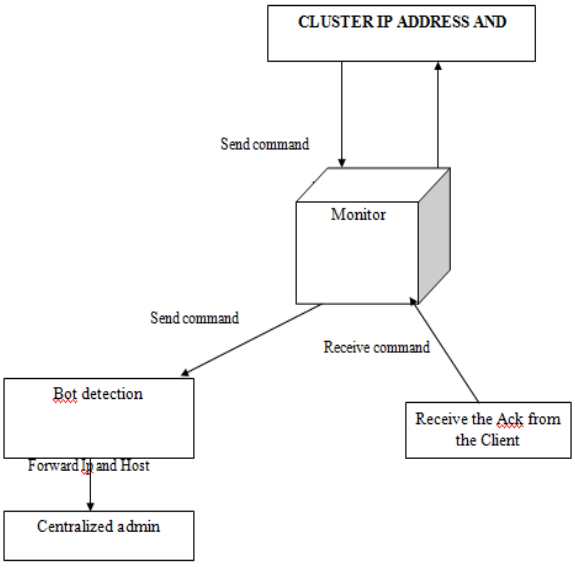
those TCP connections wit1h a completed, Acknowledgement handshake, and those UDP (virtual) connections for which there was at least one "request" packet and a consequent response packet.



c) Coarse grained peer-to-peer detection

iv. COARSE GRAINED BOT DETECTION

Since bots are malicious programs used for performing the profitable malicious activities, they represents valuable assets for the botmaster, which will intuitively tries to maximize utilization those bots. This is particularly true for P2P bots because in order to have functional overlay in network (the botnet), a sufficient number of peers needs to be always online. In other words, we can say that the active time of a Bot should be comparable to the active time of the underlying compromised system.



d) Coarse grained bot detection

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

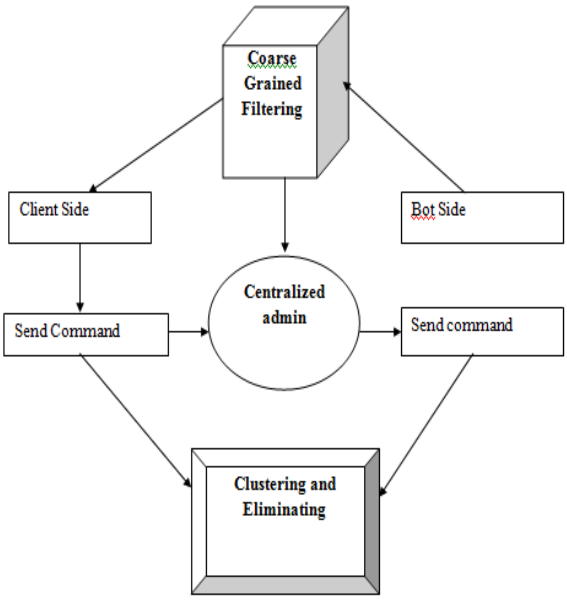
(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

v. CLUSTERING AND ELIMINATING

The distance between two flows can be defined as the Euclidean distance of that two corresponding vectors. After that We can apply a clustering algorithm for performing the partition the set of flows into a number of clusters. Each of the obtained clusters of flows represents the group of flows which are of similar size. For each we consider the set of destination IP addresses that is related to the flows in the clusters.



e) Clustering and eliminating

VI. SYSTEM ARCHITECTURE

The systems architecture establishes the basic structure of the system which defines the essential core design features and elements that provide the framework. The systems architect mentioned provides the architects views of the user's vision. Above diagram user first login to the account then he can upload or download a file which are available in server.

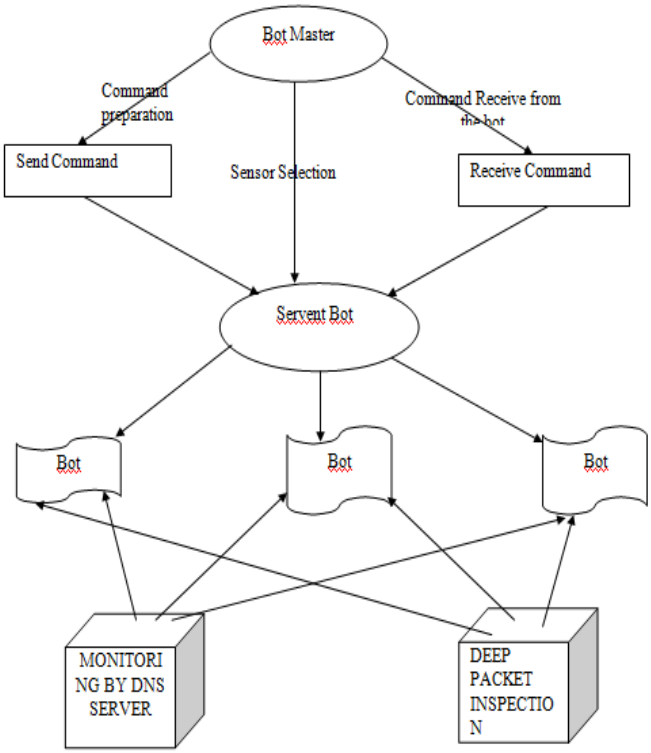
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017



f) System Architecture

VII . CONCLUSION

In this paper, we propose a novel method of botnet detection that consists of two stages. The first stage applies a sliding window to network traffic and monitors anomalies in the network. We propose two anomaly detection methods, both of which are based on large deviations results, for flow and packet level data, respectively. For both anomaly detection methods, an anomaly can be represented as a set of interaction records. Once instances of anomalies have been identified, we proposed a method for detecting the compromised nodes. This is based on ideas from community detection in social networks. However, we devised a refined modularity measure that is suitable for botnet detection. The refined modularity also addresses some limitations of modularity by adding regularization terms and combining information of pivotal interaction measure and SCGs.

ACKNOWLEDGEMENT

We felt great pleasure in submitting this paper on “Botnet Detection based on Anomaly and Community Detection” First and the foremost We , express our deep sense of gratitude, sincere thanks to Asst. Prof. V. Yadgiri for the best support ,opinion, views, comments and thoughts have been really helped us.

REFERENCES

[1] “DDoS Protection Whitepaper,” 2012, http:// www.neustar.biz/enterprise/resources/ddosprotection/ddos-attacks-survey whitepaper#.UtwNR7Uo70o.
[2] W. T. Strayer, R. Walsh, C. Livadas, and D. Lapsley, “Detecting botnets with tight command and control,” in Local Computer Networks, Proceedings 2006 31st IEEE Conference on. IEEE, 2006, pp. 195–202.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

[3] 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, 2008.
[4] G. Stringhini, T. Holz, B. Stone-Gross, C. Kruegel, and G. Vigna, "Botmagnifier: Locating spambots on the internet." in USENIX Security Symposium, 2011.
[5] G. Gu, P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee, "Bothunter: Detecting malware infection through ids-driven dialog correlation." in Usenix Security, vol. 7, 2007, pp. 1–14.
[6] A. Dembo and O. Zeitouni, Large Deviations Techniques and Applications, 2nd ed. NY: Springer-Verlag, 1998. [7] I. C. Paschalidis and G. Smaragdakis, "Spatio-temporal network
anomaly detection by assessing deviations of empirical measures," IEEE/ACM Trans. Networking, vol. 17, no. 3, pp. 685– 697, 2009.
[8] J. Wang and I. C. Paschalidis, "Statistical traffic anomaly detection in time-varying communication networks," IEEE Transactions on Control of Network Systems, vol. 2, no. 2, pp. 100–111, 2015.