Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.3, No.13, 2013

Autonomous Botnet Detection

Pragati Chandankhede
Assistant Professor,J.D.I.E.T., Yavatmal
* pragati.211086@gmail.com

Abstract

With the pervasiveness of internet, huge threats have been seen in last few decades. These threats involve the activities for violation of security in terms of integrity, confidentiality, denial of service, authentication. Due to the existence of such threats, there is requirement to defend our immense corporate secret, online banking account details and social networking account accessible via web interface. Over last few decades there is the emergence of botnet within internet. Botnet can be considered as the mass of compromise machine that are under the authority and control of single botmaster. Because of existence of such botnet there arouse intrusion. And hence intrusion detection has turn out to be sphere of influence of information assurance. At the network-level, the research work to detect bots has proceeded along two important area of vertical and horizontal correlation engine. Vertical and local correlation engine have the downside that these systems require prior knowledge about communication channel and it is indispensable to have at least two hosts in the monitored network(s) should be the members of the same botnet. Hence the new autonomous model is proposed by combining the concept of observation of command and responses received. This model will be built in controlled environment with recording of network activity by using subspace and evidence accumulation clustering. Proposed models are helpful for detection of bots in the midst of few false positives.

Keywords: : Intrusion; intrusion detection system; botnet; threat; evidence accumulation; subspace clustering

1. Introduction

Due to the heavy reliance of human being on the technology, today there is the need to take steps in the direction for dealing with their misuse. System are getting more defenseless due to increase of threats within network [5]. For every user there is everywhere threats of attack in today's internet. Along with viruses and worm, malicious botnet has been new security threats within network[1]. The name of bot was derivative of ro-bot which means the script or program that are executed repeatedly and automatically for performing predefined function which is activated by some system infection intentionally. Botnet is the collection of computer which are under the control of person/organization who is usually called as bot master. Botmaster causes the computer system to perform the malicious activities. Mystery of botmaster is that they govern the victim computer by command and control architecture. On the basis of nature of bot are categorized as benevolent bot malicious bot. The bot used for performing legal activities are called as benevolent or kind bot. whereas bot used for performing the activities for malevolent purpose are called as malicious bot. Search engines and sites of online game used the benevolent bot. Example of malicious bot have includes phishing, service operation within network like denial of service.

Botnet detection has been the recent area of interest for the researchers. Before moving on the detection technique, previous work and botnet threats are outline as prime key of concern.

1. Previous work

For text based conferencing, Jeff fisher has created the first bot program which work on many machine in scattered manner.[6] The bot was named as Eggdrop bot and it was based on feature of Internet Relay Chat (IRC). IRC is a teleconferencing system which is well suited for running on many machines in a distributed fashion.

In order to provide secure Communication between the clients, it is required that all servers should be able to transmit a message in precisely one direction all along the network for reaching to any client. The path of a message being delivered should be the shortest path between any two points on the network. As the key aim of IRC is to bring a environment which permits easy and efficient conferencing which is usually one to many in nature. The conferencing of message within IRC is done by using either to list, to group, to host or sever mask, and one message to all.

1. List: The client gives a list of destinations to which the message is to be delivered and the server breaks it up and dispatches a separate copy of the message to each given destination.

2. Group (Channel): If there are multiple user on a server within the same channel(group), the message text is send once to the server and then sent to each client within the group. Consider client 1,2,3 in channel then all the message are sent to the client on channel if it were a private message to a single client.

3. Host / Server mask: In order to provide IRC operators for sending messages to a huge body of related users, host and server mask messages are supplied. These messages are sent to users whose host or server information match that of the mask.

4. One message to all: On a large network of users and servers, a single message can result in a lot of traffic being sent over the network in an effort to reach all of the desired destinations.

As illustrated the way message can be passed among client for broadcasting purpose, and accordingly the conferencing technique of Internet Relay Chat[7] is used in order for the user running an IRC client program connects to an IRC server in an IRC network. Every servers are interconnected and they passes messages from one user to other. Due to the increased popularity among Internet users of IRC, assault (attack) on IRC started. Assault result in misuse as they are used for illegitimate financial gain or deception of user of system. Hence the malicious bot can be thought of the program, running on hosts and which gets booted in hidden way and it is being controlled by command. Size of program is 15KB and it is in compressed form. The zombie can be said to the hosts which run on IRC bot malware program.

In 1999 the first malicious IRC bot, called as Pretty Park Worm consist of limited set of features. The feature includes the ability to connect to a remote IRC server, retrieve basic system information e.g. operating system version, login names, email addresses, etc. To command and control using the innovative scheme of IRC has became distinct method. Surrounded by a few years, Botnet can be well thought-out as the collection of infected hosts that are controlled and executed by the master, also called as botmaster. Botmaster force the infected hosts to perform the malicious tasks of Denial of Service (DoS), Distributed Denial of service (DDoS), theft identifying. The technology of using IRC to control a pool of compromised hosts was improved and perfected.

Botnet Threats

Depending on the purpose of attack and attacking tool applied, botnet can reveals major four types of threats as follows:

1. Contaminate new hosts
2. Theft of personal information
3. Spam proxy and phishing
4. Distributed Denial of Service

1.Contaminate new hosts:

In order to Compromise new hosts, botnet either uses one of the method of social engineering or distribution of malicious email for contaminating host. Social engineering technique causes user to execute the malware.[9]. While distribution of email, which is being attached with malware is spread among the several host which in turn infects host.

Simple example to depict how the attack might be carried out . Malicious email are often have the ability to catch the eye of the user by their name, like “check out this picture” or “hurry for sell 50% discount”, at the same instant email might contains the infected attachment which runs automatically when clicking on the email. It might be the windows file.

2. Theft of personal information

on top of the way of to acquiring the latest application and game; the end user undermine confidentiality and integrity of their devices with outdated situational awareness on the latest threat facing them. End user unknowingly exposes critical business data to cybercriminals who manage to infect their devices. Recent DIY android.apk decompiler/ injector, keylogger and traffic packet sniffer are the best techniques for getting lost to the personal information.

3. Spam sending and phishing

Spam sending is a subset of electronic spam which invokes identical message and send it to the various recipients by email. Clicking on links in spam email may send user to phishing web site that are hosting malware. Security researchers in January 2007, observed an assault of spam enclosing subject lines which was related to extreme weather conditions (for example, "230 dead as storms batter Europe"). "ReadMore.exe" attachment accompanied the spam. The attachment infects the recipient’s computer with trojan code, if an unfamiliar recipient tried to open the attachment[10]. Trojan code may includes receiving, installing, and executing updates, using rootkit technology which can hide on the recipient’s machine.

The theft of Phishing depicts the techniques where electronic means are used by attackers to trap recipients by

revealing his confidential information. As an example phishing attack would be an email appearing to be for recipients that ask him to verify credit account transaction. The email is not really from recognized bank but if recipients tag along the link, recipients sign in information can be captured by attacker. Botmaster can command all its bots to perform the task of spam sending and phishing which is controlled by botmaster.

4. Distributed Denial of Service

During a botnet DDoS threat, a particular server can be commanded by botmaster (example: update.microsoft.com). And this technique is adapted via a malicious or anonymous proxy used for a particular date, time and for a duration in order to hide the actual commanding node.

Intrusion detection system for botnet

Detection system can be basically categorized into two major part

1. Signature based detection
2. Anomaly detection

1. Signature based detection technique:

This technique is based on the existing knowledge about the existing botnet, which are usually represented in the form of signature or rule. And in order to detect bot the database for the signature should be updated. Usefulness of this technique lies in the fact that botnet can be identified earliest but at the same instant this technique rellies on the database of bot, hence uncovering the new bot detection is not possible. Also to keeping database up-to-date is also difficult task for any detection system. The technique of signature based detection fails during the case where bot insert dead code, which remains undiscovered by signature based intrusion detection system.

2. Anomaly detection technique:

Anomaly based detection system relies on the normal behavior model, which depicts that certain behavior are called as normal and anything different from the normal behavior is treated as the abnormal or suspicious event. Normal behavior is defined by observing behavior at host level. It is better than signature detection since malicious activities can be identified by this technique. For botnet, high network latency, failed login attempts can be considered as suspicious activities. But the fact of creating such large data of normal behavior and the fluctuating behavior other than normal is difficult task. Also it is not efficient and time consuming.

On the basis of two main detection technique mentioned above, various co-relation engine has been developed that combines the idea of host level and network level behavior.

i) BotSniffer : Main aim of botsniffer is monitoring the various similarities between various activities occurring on C and C server.

ii) Bot Miner : To cluster Similar communication pattern and similar malicious activities for detecting botnet is the main motive of Bot Miner.

iii) Bot Hunter : Evidence accumulation of interior feature and external feature are matched all along various stages, which are in turn matched with state based sequence for botnet detection.

All the above technique are used for monitoring the presence of botnet. In favor of better detection result the above system of correlation relies on large amount of data of botnet activities to be traced. Thus the process being time consuming since it requires prior knowledge about command and control channel. Hence the unsupervised autonomous detection of botnet is requisite in order to detect the botnet automatically without any prior knowledge about command and control mechanism or the manner in which bot circulates.

3. Proposed Architecture:

The proposed architecture is designed to detecting bot from the given traffic in unsupervised way the procedure for bot detection is described below in Figure 1.The first important step is to capture the data from different host. The data captured is then aggregated so that bot get connected to its C&C mechanism. Evidences are captured by keeping this process running long enough to observe representative collection of the different bot commands and the activities they trigger. The detection target or evidences are the captured by [2] Evidence accumulation algorithm. The hidden bot detection are captured by applying subspace clustering. The evidence accumulatio algorithm for detecting bot from the traffic is as follows, Consider Input as follows let n d−dimensional patterns;k min - minimum initial number of clusters;.k max - maximum initial number of clusters;N - number of clusterings. For the processing of output K means will be used as the basic alogorithm for processing data.

Initialization: Set obtained from subspace clustering is set to a null n * n matrix.

1. Do N times:

1.1. Randomly select k in the interval [k min; k max].

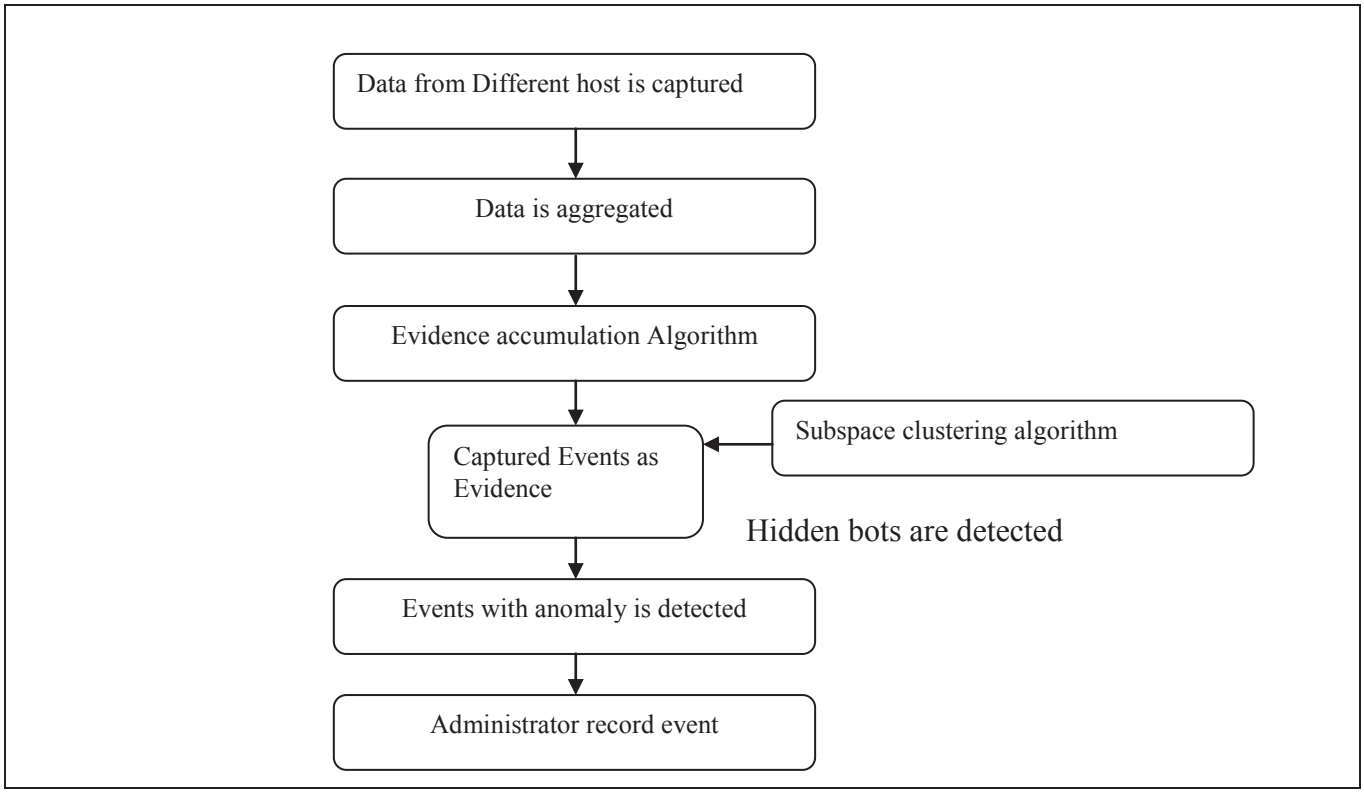

Figure 1 : Proposed architecture

1.2. Randomly select k cluster centers.

1.3. Run the K-means algorithm with the above k and initialization, and produce a partition P .

1.4. Update the subspace set for each pattern pair, (i; j), in thesame cluster in P , set co assoc(i; j)= co assoc(i; j)+1/N

2. Detect consistent clusters in the obtained set and keep it as record for administrator.

Thus the strong clustering techniques is used for unsupervised detection by combination of Sub-Space Clustering and Evidence Accumulation algorithms to identify anomalous bot within the data of traffic flows. And the evidence is then used for administrator record.

Thus the result of the process consist of events as anomaly which are detected bots within the given traffic captured or data from different host. The administrator record those events and exclude those event in future.

4. Conclusion

This paper provides a review on the various bot threats and intrusion detection system for bot. since the detection system relies on the large amount of data to be traced it is being time consuming process. As a solution the paper presents a system that identifies the anomalous bot evidences and captures those evidences as filter for future bot attack by filtering those record at administrator. It targets the unique characteristic of bots, the fact that they receive commands from the bot master and respond appropriately. Our system observes the behavior of bots executed in a controlled environment, and automatically derives signatures for the commands that a bot can receive, as well as network-level specifications for the responses that these commands trigger. The approach does not requires prior knowledge about the communication channel used by the bot and hence it is being more advantageous.

References

1.A. Karasaridis, B. Rexroad, and D. Hoeflin. Wide-scale Botnet Detection and Characteriza-tion. In Usenix Workshop on Hot Topics in Understanding Botnets (HotBots), 2007.
2. Ana Fred, Anil K. Jain . Evidence Accumulation Clustering base K-Means Algorithm. In IEEE Trans.Pattern Analysis and machine Intelligence , 2(15):926-932,2009.
3. M.Figueiredo, A.K.Jain.Unsupervised learning of finite mixture models.IEEE Trans. Pattern Analysis and Machine Intelligence, 24(3):381-396, 2002.
4. Naveen Davis, Botnet detection using correlated anomalies. In Technical University of Denmark Informatics and Mathematical Modelling,2012.
5. P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. C. Freiling. The Nepenthes Platform: An Efficient Approach to Collect Malware. In International Symposium on Recent Advances in Intrusion Detection (RAID), 2006.
6. Alam, M. & Vuong, A Mobile Agent Based Intrusion Detection System, in second International conference on Communication Systems Software and Middleware, pp. 1-6, ISBN 1-4244-0613-7, Bangalore, January, 2007.
7. C. Abad, J. Taylor, C. Sengul, W. Yurcik, Y. Zhou, and K. Rowe. Log correlation for intrusion detection: A proof of concept. In 19th Annual Computer Security Applications Conference (ACSAC'03), page 255, Washington, DC, USA, 2003. IEEE Computer Society.
8. P. Barford and V. Yegneswaran. An inside look at botnets. Special Work-shop on Malware Detection, Advances in Information Security, Springer Verlag, 2006.
9. J. Oikarinen, D. Reed, "Internet Relay Chat (IRC) Protocol," IETF, Request for Comments (RFC) 1459, May 1993.
10. Raihana Syahirah Abdullah, Mohd Faizal Abdollah, "Revealing the Criterion on Botnet Detection Technique", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013.
11. Jignesh Vania, Arvind Meniya, H. B. Jethva A Review on Botnet and Detection Technique
International Journal of Computer Trends and Technology- volume4, Issue1 2013.
12. Zhang yanyan,Yao Yuan, Study of Database Intrusion Detection Based on Improved Association Rule Algorithm, IEEE. Pages 673-676, 2010.
13. A. K. Jain and R. C. Dubes. Algorithms for Clustering Data . Prentice Hall, 1988.