I J C T A, 9(14) 2016, pp. 6455-6461

Spoofed Attack Detection and Defence for Botnet Attacks Using HSMM

Soundary Deep Kaur[*] and L. Kavisankar[**]

ABSTRACT

Botnet plays a crucial role in cyberspace recent days. Botnet server do the botnets attack under the radar so as to hide their spiteful bustle action. This condition makes it hard to trackback the server from where these attacks comes. To check the level of difficulty of these botnet attacks,a website has been selected. To understand and manage this problem,a website has been selected. To understand and manage this problem,a website and its behavior has been taken into account. For solving this purpose hidden semi markov model is used. This model predicts on the set of observations the legitimate behavior of user in the network. Mostly its not easy to carry out a mimicking attacks and legitimate attacks. The main objective of this project is to perform a study of genuine attacks and botnet attacks in the cyberspace from the attackers as well as from defenders side of perspective. This research can be used in different applications and also in other research fields.

INTRODUCTION

Botnet attacks are handled by either an individual or a group of an organization to target computer which are information systems, computer networks in big firms and personal computers. Botnet attacks can install spyware at the victim side to hack the system and to destroy the infrastructure of entire system. Botnet attacks in a very short period of time have become quite advanced and dangerous in the cyberspace.

BOTNET

A botnet is an army of interconnecting programs that communicates with other computer systems to make them part of their army in order to perform illegal tasks in cyber world. These illegal tasks starts with internet reply chat channel, by sending spam email to victim and then continuously sending DDoS attacks. Robot and network collectively known as botnet. The army of zombies is formed with the help of distributing malicious software on victim and soon these victims becomes a part of botnet army. Once the system is hacked computer performs so many tasks over the internet, Many crimes and deceit in the cyberspace is done with the help of Botnet and hence, Botnet are used by hackers to send out spam email messages in the cyberspace to attack computers and servers. When the computer processing becomes slow it is the indication that the computer processing becomes slow it is the indication that the computer has become a part of Botnet army.

Botnet means an organization of computers which can be referred to internet reply chat(IRC) bots but actually Botnet is related to a group of computers that are recruited when a malicious software is sent from one computer to other computers without the knowledge of user. All the programming and working of bots in the botnet is handled with the help of IRC in order to complete some wicked purposes. All the works and processes to different bots is sent by command and control(c&c) server which is called as the backbone of this server. The Botnet operator programming is done with the help of protocols which is more practiced

[*] Post Graduate Student

[**] Assistant Professor, Department of Computer Science and Engineering, SRM UNIVERSITY, Chennai-603203, India, *E-mail: soundaryadeepkaur57@gmail.com*

from scratch. There is a server program and a client program for different operations in these protocols that helps in communicating and then connecting the client on the victim's computer. All these types of communication which is done on a network uses a unique way of sending data which is known as the encryption strategy for stealth and also, it can be used for the protection purpose for the detection into the botnet.

SPOOFED ATTACK

The application layer DDoS attack is the spoofed attack. It spoofs the user's computer behavior in cyberspace i.e. how many websites the user opens and which website the user opens in a day. Legitimate behavior of false sites is always a problem for intrusion detection system in cyber world. E.g. the time period taken for a page request, how many pages are browses in a session. Study of spoofed attacks and detection from client program and server program i.e. from both sides, as attackers and also as defenders, which would be the significant extension based on this work. The Botnet programmers predict that legitimate behavior of user's computer in browsing web can be checked with the help of few things which are as follows:-The webpage which is most famous in user's search,The user takes some time interval during requesting a web page,In a session a number of pages browses by a user. In place of these above three informational keys pieces based on the research three distributions are used. Meanwhile it is difficult for Botnet programmer to meet the sufficient number of request of web pages in cyberspace so that it looks like legitimate attack if an adequate number of bots are active than a Botmaster with the help of one bot can stimulate one legitimate user along with using the knowledge of web browsing behavior.

Cyberattacks are becoming very popular these days and therefore, internet has become a big part of life which is used to send,receive,share and get the information all over the world which can be used in government offices, companies and individuals spoofed attacks on websites reward attacks financially. Some detection and defence strategies are used in place for DDoSattacks[1].

RELATED WORK

In this session,a brief description of the approach of spoofing attacks and its detection is explained.A bot that has investegated after ten days is a new type of bot which is known as"TORPIG". It has found most of the data has been infected more than 180 thousand infection and approximately 70GB of data. At the time when botnets were "hijacked" and studied previously, the torpig botnets because of some certain properties makes the analysis of data interesting[4]. During the estimation of bot, it is found that botnet size can reach 350,000 members. To predict the size of botnet, mainly two methods are explained in this paper[5].

A. Foot Print: Overall size of the botnets in a network can be estimated i.e. infected population can be determined. But, then also it cannot predict or determine the actual capacity, a method known as CCDF is used.

B. Live Population: It shows the live bots present in between victim and c&c server i.e. c&c channel, it helps to show the actual capacity. Filtrate the infected bots by joining c&c channel FDPM method is followed by IP trace back so as to find the real source of attacking packets. It usually predicts

   a) No. of resources in one trace back

   b) The time period of the false positive rate

   c) No. of packets needed to trace one source.

The main characteristics of FDPM 1.Flexibility 2.Keep changing its marking rate[7]. Its difficult to trackback the source of attacks because of the memory less features of the internet routing mechanism. Entropy variation can be used to find out source of the attack. It basically shows the difference between

legitimate and DDoS attacks traffic[8]. To detect and discard spoofed IP packets HCF(Hop-Count-Filtering) is used which builds an accurate IP-to-hop-count(IP2HC) mapping table. It is easy to deploy HCF, as no support from underlying network is required in it. It's done through analysis using network measurement data,[9]. 90% of spoofed IP packets can be identified and discards with the help of HCF with a very small collateral damage [10]. With the help of graphical tests authentication is provided in kill-bots and it differs from the systems that also use graphical tests. First, an intermediate stage is used to find out the IP addresses to ignore the test by kill-bots. Second, a test is send by kill-bots to check client's answer and also unauthenticated clients cannot access the sockets, worker processes and TCBS[11]. The most vicious form of DDoS is the flash-crowd attacks. Human behavior modeling helps in defense against flash-crowd attacks and also tells the differences between DDoS bots and human users. Graphical puzzle is the very recent approach to human-vs-bot differentiation [12],which are annoying and insufficient to users, moreover defense against bots are highly transparent. There are mainly three aspects of human behavior. a) with the help of learning many already chosen features of human interaction dynamics, request dynamics and detection of bots which exhibits higher aggressiveness. b) with the help of learning, user requests in accordance with the transitional probabilities along with request semantics and also detection of some bots that generates low probability sequences but valid. C) with the help of server replies it has the ability to process visual cues[13]. In DDoS, attackers and detectors plays spy-on-spy game. Attackers are spoofing network traffic patterns to disable the detection algorithms that are basically dependent on some features. Botnets use controlled functions during attacking on the victim and that's the reason the attack flows to the victim always share some more or new functions and properties. Whether it's a DDoS attack or legitimate access can be easily fixed by comparing the distance with the threshold i.e. if it is less than threshold then the possibility arises it's a DDoS attack and if it is larger than it's a legitimate access.

PROPOSED WORK

A study of spoofing attacks and detections from the client side as well as from the server side, as attackers and defenders has been made, which is actually the significant extension on preliminary work.Although, it's not easy to reach the accurate condition for certain spoofing attacks, such as flash crowd attack[12,14]. From certain set of observations it is found that botmaster can stimulate this attack in terms of statistics. So, basically with the sufficient number of active bots, a botmaster can use one bot to behave like a legitimate user using the knowledge of web browsing behavior of target victim.

BOTNET ARCHITECTURE

The main work of botmasters and various cyber criminals is to add more and more bots in its army without the knowledge of users and also these bots should be hidden to principal security firms, it is obvious these attackers or botmasters are trying their best to exploit social media platforms. These botmasters or attackers have keen interest in number of services from gaming to payments, the main reason behind this is mostly the users plays online games and do online payments, which realizes more or less complex fraud schemes. Social networking and botnet has a very strict relationship. On the other hand, this situation is becoming very common[15]. To control the various infected machines botmasters are using many social network platforms, typically these attackers create some fake accounts that sends encrypted messages to victims to make them believe its not fake. The main principle of this Botnet architecture is that the army of bots present in the social network is very difficult to detect.

CLIENT ARCHITECTURE AND UPDATE

Whenever the client opens a website registration is done by the client on the website and hence, this information can be findanytime in the database. Including the personal information login,password and many more the client can upload images also and client is the victim here in this case.The different web

pages that are accessed by client is the target websites. This work is done for the observation point count the number of HTTP request that are sent to the client on a specific web page for the given interval of time and to differentiate the browsing behavior of a legitimate web user or viewer

CLIENT BROWSING BEHAVIOR

The browsing behavior of client is captured and then the proxy settings in the web browsing by client is changed. In the proxy settings the IP address of victim is given. The next task is done at the server side and hence, it checks the number of HTTP requests sends to the victim. So, finally all the web pages that are browsed by victim is shown in the Botnet server i.e. the specific HTTP request is shown at the Botnet server. Hence, the specific URL of web pages will be stored at the Botnet server in the Botnet database.

BOTMASTER ARCHITECTURE

The botmaster architecture is basically designed to check the activities of client side i.e. it checks the victim's browsing behavior. How many times a web page is opened and for how much time interval. The information is stored at the botnet server. So, all the web pages that are accessed by clients is stored data in the botmaster page.

IMPLEMENTATION

Botmaster observes the legitimate behavior of user in browsing web pages. Reffering an IP to spoof an IP address is not a difficult task because many of the users shares same IP and only some people uses some other IP's carrying much more weight in terms of visitors than others. IRC is used for command and control by many Bots off ramp TCP port 6667 which is basically used to detect few bot commands in IRC.Once a web browsing page is decided bots sends the page request to the victim and then download the web page into the victim's system without displaying it

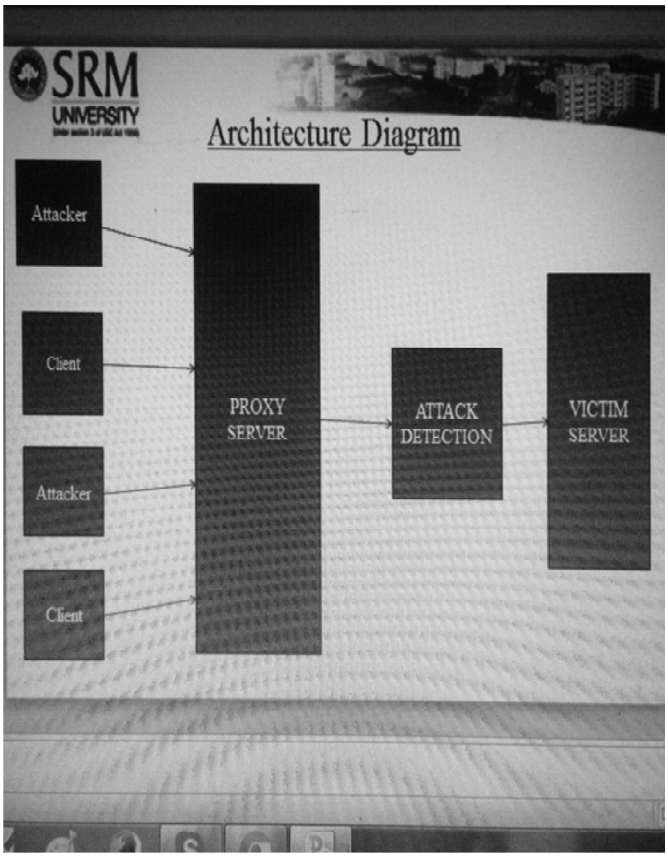

DIAGRAM (ARCHITECTURE DESIGN)

Algorithm 1. The mimicking attack algorithm

1. Observe the target website and check out the browsing parameter which are dynamically related to the website αz, q, αp, λ, μl, n(t).
2. Initialize all the parameters of the hidden semi-markov model.
3. From a set of active bots take n(t) bots, {bots}t and run these bots independently.
4. For each bot {bot}t do
5. Initialize a random number rnd.
6. Generate an initial page with rnd.
7. Browsing length L will be decided for the bot with rnd.
8. If j<=1;

   While j=L do

   - Submit the request and discard

   Then

   - Wait for the time interval decided
   - With the help of rnd.

     a. I=j+1;

     b. Initialize the new page request following the hidden semi-markov model.
9. Remove the checked Bot from set {bots}t.

End.

Algorithm 2. The mimicking detection algorithm

1. Make a profile of R(t) for a fixed interval of time period.
2. Check the flow correntropy of page request flows against R(t), and denoted by Vf(n(t)).
3. While{true}do

Compute the volume of the page requests of the website, which is denoted as R(t)

While{R'(t) >=R(t)}do

a. Follow statistical characteristics,

Some request flows for some sufficient sample points.

b. Measure the flow correntropy of page request V'f(t);

c. Δvf(t)=|vf(t)-v'f(t)|;

d. If Δvf(t) is sufficient then,

It is mimicking attack;

Else

Do nothing;

End

End

RESULT

On a new web page the client will login with the new username and password and this web page is the victim web page and once the web page is opened all the details of client will be stored in the database.

Botmaster will check the information about the client and its browsing behavior and will store the data in the botmaster database. Basically, two more attacks are included in proposed method.

- Mimicking attack
- DDoS attack
- Flash crowd attack
- Phishing attack

A number of requests at the same time is sent to the client system so as to hack the system, which is done by flash crowd attack.

All the login information i.e. necessary passwords are hacked by phishing attack.

And, finally when the server finds that there is some changes in the browsing behavior which means some attacks by the third party is taking place. So, server will notify the victim about these changes by sending the messages.

CONCLUSION

By using some methods of classification and exactly identifying how to use the correct technique for a specific type of botnet. The most effective botnet detection are IRC based. In this project, firstly client uploads the data and then this data is stored in the client database. Along with the login and password details the client can upload images to the server also and hence, here system which is used by client is the victim. The web pages that are accessed by client on internet is the target websites. This is done for the observation work. There are many critical attacks in the cyberspace which is done by the army of botnets and handled by command and control server in which the whole information is stored in botmaster database. Botmaster reviews the different activities performed by the client on the internet and catches information of number of different websites opened by client in a day and out of these websites, the most frequent site which is used by client is taken into account by the botmaster and hence, with the help of this site, botmaster generates flash crowd attacks and mimicking attacks. When the server finds that there is something wrong in the client's system then it immediately checks the client's system and sends a message that your system is in danger. Sometimes, the server bans client's system from accessing internet. Once a message is sent by the server to victim, victim immediately checks the problem that is taken place in system and try to resolve it. Although, its not easy to detect the attacks very easily but with the help of hidden semi-markov model these attacks can be detected with some set of observations.

REFERENCES

[1] Carl, G., G. Kesidis, R. Brooks and S. Rai, 2006. "Denial-of-service attack detection techniques," IEEE Internet Computing, 10(1); 82-89.

[2] *http://en.wikipedia.org/wiki/Botnet.*

[3] Ianelli, N. and A. Hackworth, 2006. "Botnets as vehicle for online crime,".

[4] Stone-Gross, B., M. Cova, L. Cavallaro, B. Gilbert, M.Cova, L. Cavallaro, B. Gilbert, M. Szyydlowski, R. Kemmerer, C. Kruegel and G. Vigna, 2009. "Your botnet is my botnet: Analysis ofa botnet takeover," in Proceedings of the 2009 ACM Conference on Computer Communication Security.

[5] Rajab, M.A., J. Zarfoss, F. Monrose and A. Terzis, 2007. "My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging,"

[6] A.P., 2007. ACM Computing Survey, "An IP Traceback System to Find the Real Source of Attacks".39(1).

[7] International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, "EntropyBased Detection of DDOS Attacks". Volume-1, Issue 5, November 2011.

[8] Yu, S., W. Zhou, S. Guo and M. Guo, 2013. "Adynamical deterministic packet marking scheme forddostraceback," in Proceedings of the IEEEGlobecom.

[9] Wang, H., C. Jin and K.G. Shin, 2007. IEEE/ACMTrans. Netw.,."Defense against spoofed ip trafficusing hop-count filtering," 15(1): 40-53.

[10] SrikanthKandula Dina Katabi, MIT {kandula,dina} @csail. mit .edu, "Botz4Sale: Surviving OrganizedDDoS Attacks That Mimic Flash Crowds" MatthiasJacob Princetonmjacob@princeton.edu, ArthurBerger MIT/Akamai awberger@mit.edu.

[11] Oikonomou, G. and J. Mirkovic, 2009. "Modelinghuman behavior for defense against flash-crowdattacks," in Proceedings of the 2009 IEEE Conferenceon Computer Communication.

[12] Jung, J., B. Krishnamurthy and M. Rabinovich, 2002."Flash crowds and denial of service attacks:Characterization and implications for cdns andweb sites," in Proceedings of the WWW. IEEE,pp: 252-262.

[13] Yu, S., W. Zhou and R. Doss, 2008. IEEECommunicationsLetters, "Information Theory BasedDetection Against Network Behavior MimickingDdos Attack," 12(4): 319-321.

[14] Yu, S., G. Zhao, S. Guo, Y. Xiang and A. Vasilakos,2011. "Browsing behavior mimicking attacks on popular websites,"in INFOCOM Workshops.

[15] Yu, S., S. Guo and I. Stojmenovic, 2012. "Can we beat legitimate cyber behavior mimicking attacks from botnets," in Proceedings of INFOCOM, pp:3133-3137.

[16] Duan, Z., X. Yuan and J. Chandrashekar, 2008. "Controlling ip spoofing through interdomain packet filters," IEEE Trans. Dependable Sec. Comput., 5(1): 22-36.

[17] Peng, T., C. Leckie and K. Ramamohanarao, 2007. "Survey of network-based defense mechanisms countering the dos and ddos problems," ACM Computing Survey, 39(1).

[18] Shui Yu, 2013. Senior Member, IEEE, Song Guo, Senior Member, IEEE and Ivan Stojmenovic, Fellow, IEEE, "Fool me if you can:Mimicking attack and anti-attacks in cyber space" IEEE transactions on computers, 2013.