Resisting Proxy Based Spoofing Attacks

S. Adithya jones
PG Student, Department of Computer Science & Engg
P.B College of Engineering, Tamil Nadu, India

***Abstract*--**Botnets are the main drivers of cyber attacks, such as distributed denial of service (DDoS), information phishing and email spamming. These attacks are pervasive in the Internet, and often cause great financial loss. Motivated by huge financial or political reward, attackers find it worthwhile to organize sophisticated botnets for use as attack tools. There are numerous types of botnets in cyberspace, such as DSNXbot, evilbot, G-Sysbot, sdbot, and Spybot. A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. A Flash Crowd (FC) is a large surge in traffic to a particular Web site causing a dramatic increase in server load and putting severe strain on the network links leading to the server, which results in considerable increase in packet loss and congestion. In order to simulate the legitimate behaviour of a web browser, we need three key pieces of information: web page popularity of the target website, web page requesting time interval for a user, and number of pages a user usually browses for one browsing session. In this project we show Mimicking attack and phishing attack. We propose a second order statistical metric for the detection purpose. To detect flash crowd attacks when the sufficient number condition is not met by botnet owners.

Keywords: *Mimicking, flash crowd attack, detection, second order metrics.*

I. INTRODUCTION

Discriminating flash crowd attacks from genuine flash crowds has been explored for approximately a decade. Previous work has focused on extracting DDoS attack features, followed by detecting and filtering DDoS attack packets using the known features. However, these methods cannot actively detect DDoS attacks. The current popular defence against flash crowd attacks is the use of graphical puzzles to differentiate between humans and bots. This method involves human responses and can be annoying to users. Another common method is detecting anomalies by modeling legitimate behavior, in which Markov models are the popular tools. Xie and Yu used the hidden semi-Markov model, and Awad and Khalil employed the all-Kth Markov model to describe web browsing dynamics. Oikonomou and Mirkovic tried to discriminate mimicking attacks from real flash crowds by modeling human behavior.

This behavior based discriminating methods work at the application layer, and is therefore limited to the potential victim's location. An ideal detection method should be feature independent and work on a large scale, e.g. at the network layer. Mimicking attacks and detections from both sides, as attackers and defenders, which is a significant extension based on our preliminary work in. From the botnet programmers' perspective, in order to simulate the legitimate behavior of a web browser, we need three key pieces of information: web page popularity of the target website, web page requesting time interval for a user, and number of pages a user usually browses for one browsing session. Based on the research on web browsing dynamics, there are three distributions in place for the three key pieces of information. The properties of the Internet we use in this paper are reliable. If botmasters have a sufficient number of active, then each bot can simulate one legitimate user using the three statistical distributions. However, it is hard for botnet owners to meet the sufficient number condition for certain mimicking attacks, such as flash crowd attacks. We demonstrate that botmasters can simulate a flash crowd successfully in terms of statistics. With a sufficient number of active bots, a botmaster can use one bot to simulate one legitimate user using the knowledge of web browsing dynamics.

II. RELATED WORK

A. MIMICKING

Botnets have become major engines for malicious activities in cyberspace nowadays. To sustain their botnets and disguise their malicious actions, botnet owners are mimicking legitimate cyber behavior to fly under the radar. This poses a critical challenge in anomaly detection. In this paper, we use web browsing on popular web sites as an example to tackle this problem. First of all, we establish a semi-Markov model for browsing behavior. Based on this model, we find that it is impossible to detect mimicking attacks based on statistics if the number of active bots of the attacking botnet is sufficiently large (no less than the number of active legitimate users). However, we also find it is hard for botnet owners to satisfy the condition to carry out a mimicking attack most of the time. With this new finding, we conclude that mimicking attacks can be discriminated from genuine flash crowds using second order statistical metrics. We define a new fine correntropy metrics and show its effectiveness compared to others. Our real world data set experiments and simulations confirm our theoretical claims. Furthermore, the findings can be widely applied to similar situations in other research fields.

B. FLASH CROWD ATTACK

Flash crowd is a sudden, large surge in traffic to a particular Web site– September 11, Ken Starr's report, Victoria's Secret webcast.Denial of Service (DoS) attack is an explicit attempt to prevent legitimate users of a service from using that service – HTTP request flooding, attack to crack password-protected web pages, worm, TCP SYN flooding, etc.

C. DETECTION

Mimicking attacks and detections from both sides, as attackers and defenders, which is a significant extension

based on our preliminary. From the botnet programmers' perspective, in order to simulate the legitimate behavior of a web browser, we need three key pieces of information: web page popularity of the target website, web page requesting time interval for a user, and number of pages a user usually browses for one browsing session (referred to as browsing length). Based on the research on web browsing dynamics, there are three distributions in place for the three key pieces of information.

D. SECOND ORDER METRICS

Measurement has been extensively explored for many years, with researcher inventing many metrics, including first order and second order metrics. For example, mean and the Kullback-Leibler distance are first order metrics, while standard deviation and correntropy are second order metrics. It is not difficult for attackers to exhaust their active bots to generate the same average number of page requests as a flash crowd. Therefore, first order metrics are vulnerable to sophisticated mimicking attacks. However, when the sufficient number condition is not met for attackers, the flow feature of standard deviation or second order statistics will reveal the difference between a genuine flash crowd and a flash crowd attack.

III. PROTOCOL DESIGN DESCRIPTION

System has three modules namely

Modules:

- Client Architecture and Updates.
- BotMaster Architecture.
- Attacks and its Detection.

A. CLIENT ARCHITECTURE AND UPDATES:

In this module, the client registers to the server with necessary information where server verifiers the details provide. Client login their account for uploading files. Client chooses the file and uploads to server where the server stores the file in storage system. Here the client is the victim. The web pages he accessing is the target victim web sites. This work is done for the observation point. We count the number of HTTP requests of each flow for the given time intervals and to describe the browsing behavior of a legitimate web viewer or user.

B. BOTMASTER ARCHITECTURE:

In this Module we have design a web page to observe the potential victim for sufficient time in attack free cases. This training should be taken periodically to update the parameters to reflect the ever changing web browsing behavior. The client Browsing details will be collected in this BotMaster web page. All the web page that the client accessing will be collected in this BotMaster page.

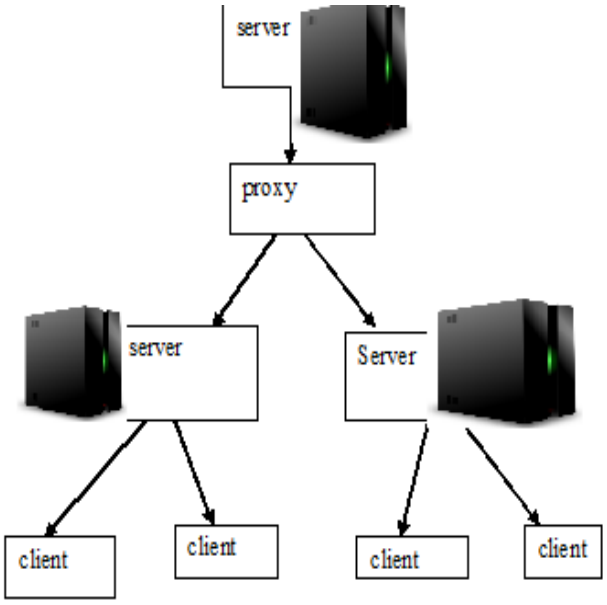

Fig.1. System Overview

C. ATTACKS AND ITS DETECTION:

In this module, using the collected details about victim in the botmaster will successfully generate ddos attack, flash crowd attack, phishing attack and mimicking attack. If we perform any modification in the botmaster page it will automatically reflect in the victim client website. Server detects all the attacks using second order statistical metric detection scheme and block the bot ip address. The client send report (my service is blocked due to attack please revert me) to the server.After analyzing the client report from the server, that particular client ip is released from the blocked list by server. Server gives the instruction about attack and how to prevent it.

IV. IMPLEMENTATION AND EVALUATION

In a genuine flash crowd scenario, we are interested to see the various phenomenons in a system viewpoint. For example, for a given point of time, we expect to know the number of total page requests to a web site, and number of requests for a specific web page of the web site. In order to answer these questions, we need one more parameter: the number of active web viewers for a given time point, which we denote as. varies against the time point of a day. Intuitively, there are more web viewers during working time than early morning.Wehave conducted 30 days observation on for every 30 minutes, and found that was stable day after day. We present our observation of on June 1, 2010 of a popular news web site. We find there is significant variation among the number of web viewers. For example, there are less than 100 concurrent viewers at 5 or 6 am, however, it soars to more than 1,000 around 11 or 12am, and is relatively stable in the afternoon and into the middle night, with around 400 viewers. There are many factors that impact, e.g. time zone, holidays, weekdays or weekends. Therefore, it is hard

to have a closed form.However; this does not impact our modeling and analysis. Following the properties of the Pareto distribution, when > , the mean of the viewing time is Therefore, we can obtain an average of frequency (the number of pages a browser reads for a unit of time) as The number of page requests for a given time point , , observed at the server end can be expressed as If we break this down further, for the same scenario, the number of requests for page at time point is Moreover, the duration of a browsing session for a user is dominated by Based on Wald's theorem, the mean of the duration of browsing sessions is Suppose we observe the number of users every (<) time interval, and we have conducted observations, then during this time interval (>), the number of unique users accessing the system is Equation (13) indicates the number of unique bots that a botmaster has to possess in order to carry out a mimicking attack for a duration of . Based on the four parameter semi-Markov model and the analysis, we can make the following conclusion.

V. CONCLUSION

Thus I designed and developed to perform legitimate cyber behavior mimicking attacks from large scale botnets and also able to discriminate mimicking attacks from legitimate cyber events by showing client upload and botmaster response for suspending DDOS attack as a part of mimicking attack. Our future work will follow two directions. First, there are a lot of legitimate network events that do not involve a large number of users. Therefore, botnet owners do have the capability to perform perfect mimicking attacks, such as membership recruitment, performance degradation attacks, and so on. I have a significant interest in addressing this problem by finding new methodologies. Secondly, I are also interested in tackling the problem of botnet owners who may cooperate with each other to establish a super botnet to satisfy the sufficient number condition to execute mimicking attacks.

REFERENCES

[1]. S. Yu, W. Zhou, S. Guo, and M. Guo, "A dynamical deterministic packet marking scheme for DDoS traceback," in Proc. IEEE Global Telecommun. Conf. (Globecom), 2013.

[2]. M. A. Awad and I. Khalil, "Prediction of user's web-browsing behavior: Application of Markov model," IEEE Trans. Syst. Man Cybern. B, vol. 42, no. 4, pp. 1131–1142, Feb. 2012.

[3]. C. A. Shue, A. J. Kalafut, and M. Gupta, "Abnormally malicious autonomous systems and their internet connectivity," IEEE/ACM Trans. Netw., vol. 20, no. 1, pp. 220–230, Feb. 2012.

[4]. S. Yu, S. Guo, and I. Stojmenovic, "Can I beat legitimate cyber behavior mimicking attacks from botnets," in Proc. IEEE Conf. Comput. Commun. (INFOCOM), 2012, pp. 3133–3137.

[5]. Z. Li, A. Goyal, Y. Chen, and V. Paxson, "Towards situational awareness of large-scale botnet probing events," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 175–188, Mar. 2011.

[6]. N. Jiang, J. Cao, Y. Jin, L. E. Li, and Z.-L. Zhang, "Identifying suspicious activities through DNS failure graph analysis," in Proc. IEEE Int. Conf. Netw. Protocols, 2010, pp. 144–153.

[7]. S. Yadav, A. K. K. Reddy, A. L. N. Reddy, and S. Ranjan, "Detecting algorithmically generated malicious domain names," in Proc. Internet Meas. Conf., 2010, pp. 48–61.

[8]. M. Edman and B. Yener, "On anonymity in an electronic society: A survey of anonymous communication systems," ACM Comput. Surv., vol. 42, no. 1, 2009.