RANDOMISED TRAFFIC PATH ANALYSIS AND FORMATION FOR DETECTING DISTRIBUTED DENIAL OF SERVICE BOTNET ATTACKS

M.Maheswari, Madhana Gopal Bhavani, Tanya Aggarwal

Abstract*: Botnets are most commonly used in cyber- criminal activity. They're used for spamming, phishing, denial-of-service attacks, stealing non-public data, and cyber warfare. A botnet may be a range of net computers that, though their homeowners are unaware of but have gotten wind of, forward transmissions (including spam or viruses) to alternative computers on the web. There is 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:Intrusion, Coarse grained ,Botnet, DDOS

I. INTRODUCTION

Security plays an important role in the world of networking. The data that is sent from one system to another system has to travel through many actions of attacks. A perfect security system has to accomplish these tasks . Intrusion detection, prevention and mitigation are the techniques that are conquering the world of security. When these system work accordingly to fight a threat , perfect security system is established. Also Intrusion detection system when combined with machine learning algorithm would give a more robust system .In this paper we have discussed how a botnet detection happen in our proposed methodology

II.LITERATURE SURVEY

The Literature Survey has been done on DDOS attacks.

- **DDOS Attacks with Randomised Trafficinnovation: Botnet Identification Challenges and Strategies (2017)**:Botnets are used to attack the high traffic network so that regular users are unable to access the network. To prevent such attacks, it is important to differentiate the regular users from the bots. This paper suggests a few contributions:

  1) The bots keep looking for vulnerabilities in the network, so the paper suggests an abstract model for DDoS which would do the same 2) an algorithm which will keeps looking to provide an estimate on the bots that are looking to attack the network 3) setting up a testing environment to verify the above suggestions

- P2P AS BOTNET COMMAND AND CONTROL: A DEEPER INSIGHT (2006):

  This paper suggests using P2P concepts to improve botnets. Even though there has been a lot of research on P2P protocols, scalability and availability of content, there isn't much regarding shifting command and control from using protocols like http to botnets becoming command and control which makes them very difficult to detect.

- **EXPERIENCES IN MALWARE BINARY DEOBFUSCATION (2007):**
  Malware creators use varied methods to stop automated reverse engineering and static analysis efforts. One of the popular methods is code obfuscators where they rewrite the original code to a different form which does the same functionality but evades the regular malware detection.

- **Internet Traffic Classification Using Bayesian Analysis Techniques (2005):**
  Classifying the network traffic is very much needed for activities like monitoring the network security, taking stock of all the activities, maintaining quality, feedback to the network operators for long term protection. This classification of network traffic is done using Naive Bayes estimator.

- NOVEL METHODS FOR INTRUSION DETECTION (2006):

Analysing large amounts of data flowing through a network requires identifying anomalies in patterns. Parallel computing is one way that is now being used to identify such patterns, thanks to cloud computing models. This paper suggests a new method called Bot Graph to detect spamming of email providers.

III.REQUIREMENTS GATHERING:

- Functional Requirements:
  1. Differentiating between regular and dangerous P2P activity in computers.
  2. Detecting the dangerous P2P activities in the system and therefore, the infecting bot.
  3. Detecting the peers to which the bot is always

connected.

4. Using Coarse grained algorithm to detect the IP address of the Botmaster from all the other peers the bot connects to.

- Non Functional Requirements:
  1. Platform independence.
  2. The software will run in the background without interrupting the normal activities that take place in the system.
  3. User friendly interface.

IV. RISK FACTORS

Risk factors might include anything related to the product that could reduce its performance, speed, reliability.

- Low risk factors involve delay of hardware and software resources and data migration.
- Medium risk factors involve security issues from the system side by mishandling software.
- High risk involves system owner not participating in system change and if they compromise on quality.

V.PROPOSED METHODOLOGY:ARCHITECTURE

Coarse grained detection of P2P bots: Bots are programs that are used for doing malicious profitable activities.They are important to the botmaster, who will try to use bots as much as possible. This is especially true for bots connected P2P because, to have a botnet (network of bots),Firstly, we use supervised learning to differentiate malicious and benign P2P activity. The Naive- Bayes classifier is used to classify malicious threats. The classification is done with accordance to the requests, which the P2P activity in question, sends to its other peers. This is called Fine grained detection. Once a malicious threat is detected, the extensive communication between the peers (botmaster and the bots) can be used to trace the IP address of the botmaster since the bot present in the system will always be connected to the botmaster. The time they remain connected peer to peer depends upon how long the infected system is online. This completes the coarse grained detection of the P2P bots

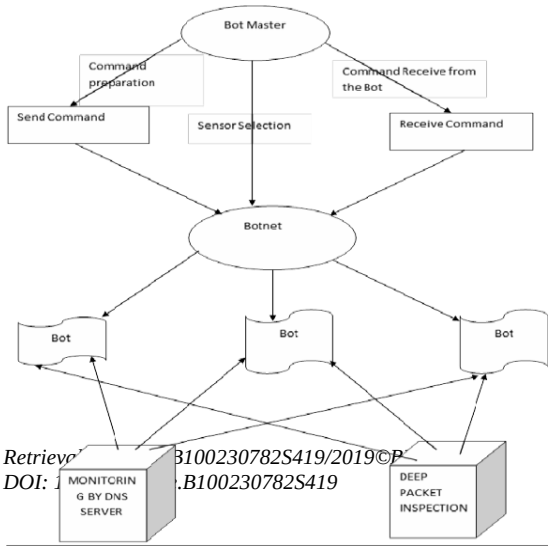
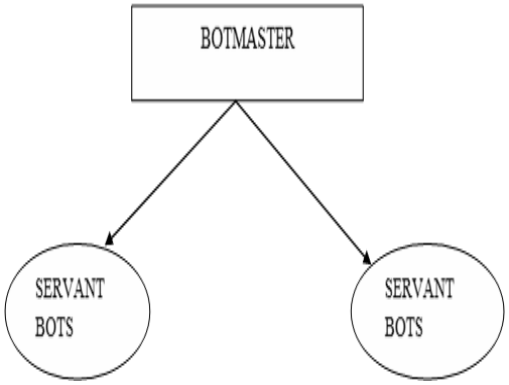


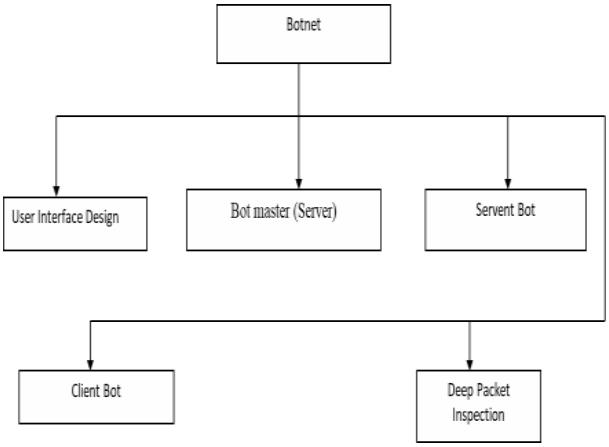
Fig: Proposed Architecture diagram of the system

VI.DATA FLOW DIAGRAM

Level 0:



Level 1:



VII. RESULTS AND DISCUSSION:

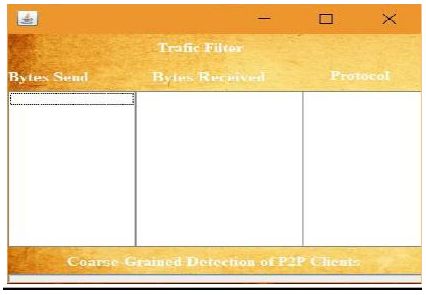


Fig:1.2 Send and receive details of Bytes

The above screenshot illustrates about the bytes sending and receiving details using the coarse grained detection of P2P clients

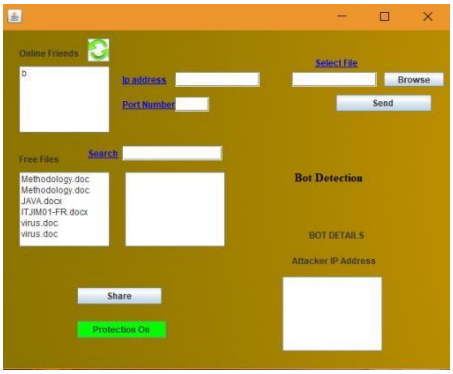


Fig 1.3 Details of file or data transfer

The details of the system that is sending the data or file to the other system

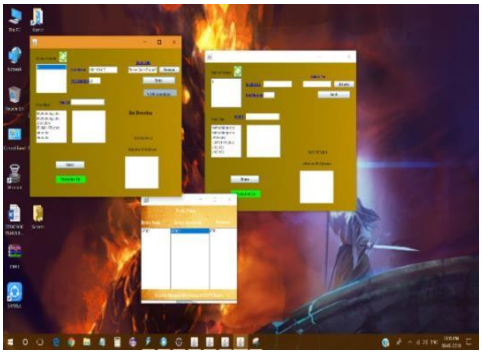


Fig 1.4 Setting the protection mode: ON

The overall picture of the details of the system that is sending and receiving the files with protection ON.

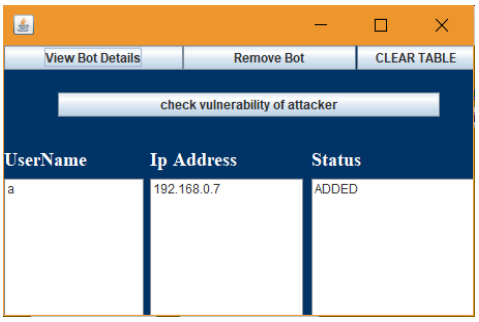


Fig 1.5 Entire the details of BOT

Also the admin can view the entire details of the BOT that is generated , and its IP Address.

VIII. CONCLUSION

In this paper we provided an overview of the kind of attack each node will be affected by, how the bots in the botnet communicate and co-ordinate and what they do to the target system under the command of the botmaster. The method used to mitigate the attacks and identify the source of the attack, coarse grained technique, is also briefly explained. It is worth mentioning that it is impossible to continuously keep up with new techniques that attackers use, to mask the mal intentions of the files with which they attack .The proposed system needs the dataset to be regularly updated.

IX. REFERENCES:

[1]S. Stover, D. Dittrich, J. Hernandez, and S. Dietrich, “Analysis of the storm and nugachetrojans: P2P is here,” in Proc. USENIX, vol. 32. 2007, pp. 18–27.
[2.] P. Porras, H. Saidi, and V. Yegneswaran, “A multi-perspective analysis of the storm (peacomm) worm,” Comput. Sci. Lab., SRI Int., Menlo Park, CA, USA, Tech. Rep., 2007. P. Porras, H. Saidi, and V. Yegneswaran. (2009). Conficker C Analysis [Online]. Available: http://mtc.sri.com/Conficker/addendumC/i ndex.html
[3]. G. Sinclair, C. Nunnery, and B. B. Kang, “The waledac protocol: The how and why,” in Proc. 4th Int. Conf. Malicious Unwanted Softw., Oct. 2009, pp. 69–77.
[4]. R. Lemos. (2006). Bot Software Looks to Improve Peerage [Online]. Available: http://www.securityfocus.com/news/1139 0
[5]. Y. Zhao, Y. Xie, F. Yu, Q. Ke, and Y. Yu, “Botgraph: Large scale spamming botnet detection,” in Proc. 6th USENIX NSDI, 2009, pp. 1–14.
[6]. G. Gu, R. Perdisci, J. Zhang, and W. Lee, “Botminer: Clustering analysis of network traffic for protocol- and structureindependent botnet detection,” in Proc. USENIX Security, 2008, pp. 139–154.
[7]. T.-F. Yen and M. K. Reiter, “Are your hosts trading or plotting? Telling P2P filesharing and bots apart,” in Proc. ICDCS, Jun. 2010, pp. 241–252.
[8]. S. Nagaraja, P. Mittal, C.-Y. Hong, M. Caesar, and N. Borisov, “BotGrep: Finding P2P bots with structured graph analysis,” in Proc. USENIX Security, 2010, pp. 1–16.
[9]. J. Zhang, X. Luo, R. Perdisci, G. Gu, W. Lee, and N. Feamster, “Boosting the scalability of botnet detection using adaptive traffic sampling,” in Proc. 6th ACM Symp. Inf., Comput. Commun. Security.