International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 1 09-Apr-2015,ISSN_NO: 2320-7248

DETECTING AND BLOCKING OF SPAM ZOMBIE MECHANISM

Mankar Aarti, Sardeshpande Sandeep, Shirohiya Mayur, Thigale Shital

Computer & Pune University

ABTRACT:-*A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. These compromised machines send a lot of spam messages on the internet. Such machines result in spamming attacks, DDOS attacks, identity theft which result in different kind of losses to the victim. Spamming botnets is the network of compromised machines involved in spamming. The SPOT, the sequential probability ratio test is used for detecting the compromised machines. SPRT is used since the error rate produced is infinitesimally small and the number of observations required to deciding whether a machine is compromised or not is also small. It helps in observing the outgoing messages from a machine in a network. Out of a large number of machines in a network only a few of them are not compromised. For an instance, out of 440 internal IP addresses SPOT identifies 132 of them as being compromised. This system has been developed for system administrators for monitoring the machines in a network.*

INTRODUCTION:-

A security is a big challenges in the internet. Many machines having security attacks on the compromised machine in network such as spamming,malware,etc.

In this paper, we have focus on such compromised machine which have sending spam messages. Such messages are commonly referred as spam zombies. We have develop a spam zombie detecting system with help of some algorithms like Spam Zombie Detection System(SPOT),Sequential Probability Ratio Test(SPRT).

The remainder of paper is organized as follows: in Section 2, we discuss related work in the area of botnet identification. Section 3, evalutes on detecting of spam zombies. Section 4, tells about the our system. Section 5,concludes the paper.

RELATED WORK:-

In this section,we discussed related work and study about Network based anomaly detection is used to identify botnet [1].And study about techniques used to filter spams by analyzing the email content[2],and also Focus on characterizing spamming botnets by spam server traffic properties [3].

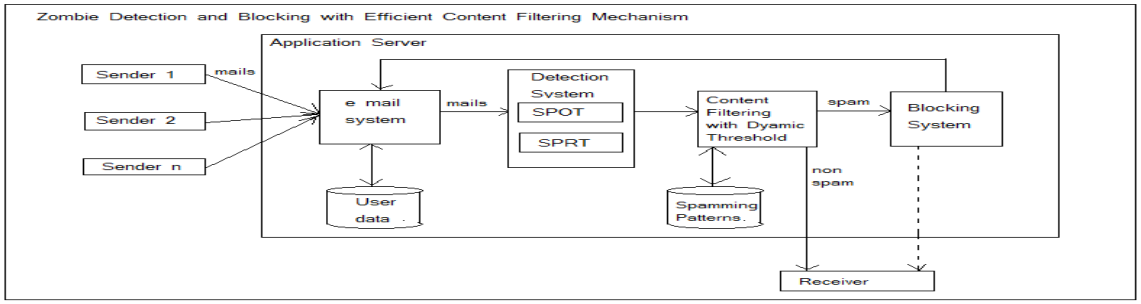
EXITING SYSTEM:-

The system is concerned only with detecting the spam zombies or botnets. These systems do not provide any blocking mechanism which will restrict the spam zombies systems from sending the spam messages within the network. Some of the systems are having higher cost. Some systems depend upon the user defined threshold value for deciding whether the message is a spam or not. The existing system only performs a check on spam messages and do not check for the viruses. The existing system does not provide user feedback mechanism for reporting spam mails to the SPOT monitoring systems.

PROPOSED SYSTEM:-

The Proposed system makes the use of the Content filtering algorithm that filters the outgoing mails into the words and performs the word by word comparison with the stored spamming patterns. If the spamming percentages goes beyond the specifies limit, the system detects the messages as Spam message and sender of that messages gets blocked.The attachment may contain the text file, word files and PDF files with the spamming patterns.

BLOCKED DIAGRAM:-



CONCLUSION:-

The Spam Zombie Detection and blocking Mechanism detects the spam mails by monitoring the outgoing mails. The Spam Zombie Detection and blocking Mechanism uses the Sequential Probability Ratio Test algorithm to detect the spam zombies. The system also provides the blocking mechanism in which if the system is identified as the spam zombie then the user account gets blocked so that he cannot send the spam messages further. The system also provides the virus detector and attachment scanning mechanism.

REFERENCES:-

[1].Guofei Gu,Junjie Zhang, and Wenke Lee “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic.”

[2].Ahmed Khorsi “An Overview of Content-Based Spam Filtering Techniques.”

[3].Yinglian Xie, Fang Yu, Kannan Achan, Rina Panigrahy “Spamming Botnets: Signatures and Characteristics.”