IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 5 (Mar. - Apr. 2013), PP 52-55
www.iosrjournals.org

Monitoring the Spread of Active Worms in Internet

Mr.V.Senthilkumar , M.Tech IT , Mrs.P.Chitrakala, Asst Prof.
Dept. of Information Technology, Hindustan Institute of Technology and Science, Chennai India.

***Abstract*:** *As far as security is concerned compromised system plays a vital role i.e., system connected with a network and which is used to send spamming, malware, identity theft etc. A System is developed mainly to focus on detection of compromised machines which is already being affected by hacker or cracker and used for anti social activities. We have developed an effective solution for detecting compromised system named "SPOT". SPOT uses SPRT (Sequence probability ratio test) which has false positive and false positive error rates. This SPOT is an effective and efficient system in detecting compromised machines in the network. To implement a single remote address corresponds to a malicious scanner which works good in internet environments. The main objective are effectively identifying the spam zombies and Denial of Services attack using SPOT without any botnet spam signatures techniques on the network.*

Keywords- Compromised machines, Malicious scanner, Spam filter, Machine creation, dynamic ip, Spam zombies.

I. Introduction

As the sub product of electronic mail services, spam became a serious issue in penetrating into any mail system and this types of penetration is mainly used by hackers for stealing confidential data without the knowledge of the user. Generally few hackers use worm which is standalone malware computer program that spreads itself in order to spread to other computers. Compromised systems is generally known to be bots and collection of bots controlled by single entity is known as botnets. This type of system comes into picture due to weak security design of SMTP(Simple Mail Transfer Protocol). The ability of spammers to forge email headers often complicates the spam control efforts and makes it hard to locate exact spammers and their location. Also proven that in today's world Compromised systems are basically used for anti-social activities. The main goal is to identify and cleaning compromised systems in the network which are used for spreading malware, spamming etc. The exact nature of the action varies with the domain email worm authors may try to have the target run an executable attachment; spyware authors may want to direct the target to a specific web site for a drive-by download; spammers may want to have the target visit their web site or that of an affiliate. We will refer to email worm authors, spyware authors, and spammers using the generic term "adversary" since they share this common goal. In each case, the goal can be accomplished by sending out bulk email (spam) to potential targets. Improved spam will come from zombie machines. At first blush, this isn't terribly original, but the difference is in how the zombies are used. A zombie machine is not just a throwaway resource, a launching pad for DDoS attacks and spam; a zombie contains a wealth of data.

II. Existing System

In the existing system periodic counting the number of spam messages is used i.e., checking out how much data is being attained in the form of spam is counted but it is not suitable for aggregate large scale spam view . Identifying spam messages had became significant challenge for the system administrator to sort out the solution and the main drawbacks is that sequential detection problem in which it mainly deals when many process is executing continuously the system should withstand in such a way that stability should be maintained but it is impossible in this system. Here AutoRE that identifies botnet host by generating botnet spam signatures from Email. AutoRE is motivated in part by the recent success of signature based worm and virus detection systems. These trends for evading existing detection systems suggest that we need to take a holistic view of various mechanisms and explore the invariable attack features in order to get an upper hand in the spam arms race.

III. Proposed System

The proposed system avoids the main limitations of the existing systems. This system mainly intends to develop an effective spam zombie detection system.

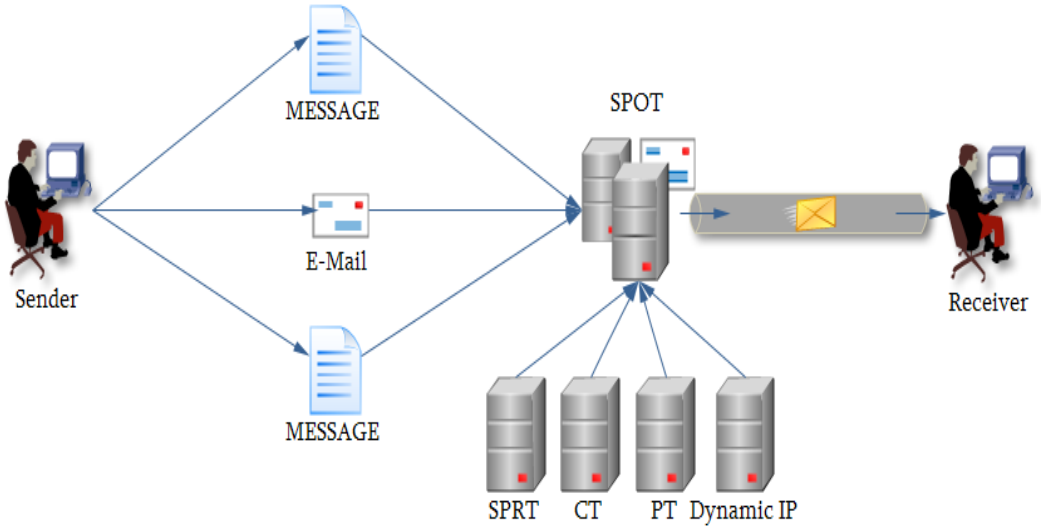


Figure 1. System Architecture

The systems which is used to sense the spam mails i.e. many copies of same mail is send to other systems. The outgoing messages are arrived in SPOT detection .Inside the SPOT there are three blocks Capture IP, Spam Filter, Detection of Spam. Capture IP of the system is done then next the system mails are applied to the spam filter process. Inside the spam filter mail contents are filtered. Next is arriving of detection of spam in which filtered mail are classified either spam or not spam .Then the result of the spam is displayed .Here particular system of the spam comes under compromised machines otherwise remaining mails comes under uncompromised machines.

Next is the process to compare SPOT. Here two different technique are used first is CT (count threshold) and another is PT. CT is fixed length of spam mail where monitor process is enhanced. If each mail is greater than or equal to the threshold values then mails are spam. And in case of PT it has two blocks minimum message threshold and maximum message threshold. And in compute it handles count of total messages and count of spam mail. These counting values are checked. If it is greater , then this mail are spam mail.

A. NETWORK AND TOPOLOGY INVENTION

In the first phase, Network topology deals about arrangements of elements such as nodes and links of a computer. Then the node information and IP address is received with the help of network administrator. Once the node information is received , then network is configured based on certain rules and regulation. Finally after configuring the topology , Network topology is innovated.

B.SPAM ZOMBIES DETECTION MACHINE CREATION

Here in this module the main goal is to create detection machine. Messages generated are send to the spam zombies detection system. Then here an random variable is initiated which randomly generates key. Then check the value for exceeding the range. If it is exceed then it is said to be Zombies. Else the machine is normal which means it is not involved in any malware activity.

C.SPOT DETECTION AND ANALYSIS

SPOT examines the user specified boundary values. Boundary is the user defined threshold where user specifies the limits. Then Random variables arrives along with the message generated from the nodes. Both the above parameter Boundary values and random variables are send to Sequential Probability Ratio Test. Then finally false positive and negative is calculated and analysed. These false positive and negative are error rates by which the actual system can be found out whether it is compromised or not.

D.SPAM COUNT AND ANALYSIS

Here in spam count based detection analysis enhances how to count spam and detect it such that the resultant will be compromised. User had to detect the threshold value as T. Cs specifies the maximum number of spam message received from normal machine. If n exceeds Cs then it is compromised machine else it is not compromised system.

E. SPAM PERCENTAGE BASED DETECTION ANALYSIS

Here we need to fix the threshold value T as in case of count analysis. Let N be total number of spam messages and Ca is minimum number of spam messages. If value of N<Ca and N>P then it implies that it is compromised system.

F. EVALUATION OF DYNAMIC IP ADDRESS

The main goal is to find and analysis the change of IP address. Since hackers used to change IP address dynamically so that it becomes very tough job to find it. Received messages are send to spam detection machine. Detection message also get the IP address of sending message along with the message. Then checking the parameter values of CT and PT with user specified threshold value. If range of CT and PT is greater then T, it is compromised machine else it is reported as normal machines.

IV. Spot Progression

This SPOT is considered to be best and important part in the detection system. This SPOT works on SPRT(Sequential Probability Ratio Test) i.e., it is the probability of finding sequential spam detection process. SPRT has false positive and false negative error rates. False positive is the one which doesn't consists of spam and false negative is the one which consists of spam . Performance of SPOT is based on number and percentage of spam messages. SPOT minimizes the expected number of observation needed to reach decision among all the sequential and non sequential statistical test with no greater error rates .

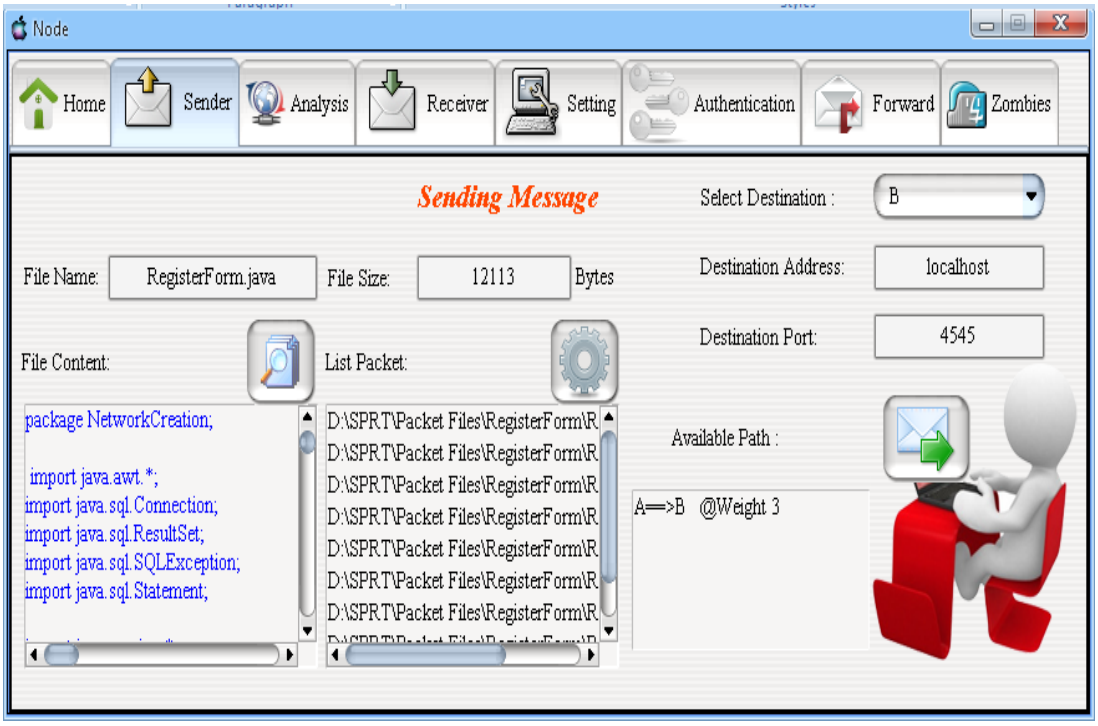
V. Spammers activities blocking

SPOT identify the spam message , analyze the ip address of senders machine. After analyzing the ip address, messages are send to the Network Administrator in order to check the activities such as whether it exceeds the user defined threshold value. If the resultant activity seems to be abnormal condition , it is blocked . Otherwise process continues.

VI. Results

Thus the system is properly detected and analyzed using various techniques mentioned above. An effective and efficient system in automatically detecting compromised machines in the network is achieved successfully. Operation workload is very minimum because using the CT and PT techniques. It effectively identifies any machine sending a single spam message as a compromised machine if a machine sent one outgoing message caring a virus / worms attachment.

.



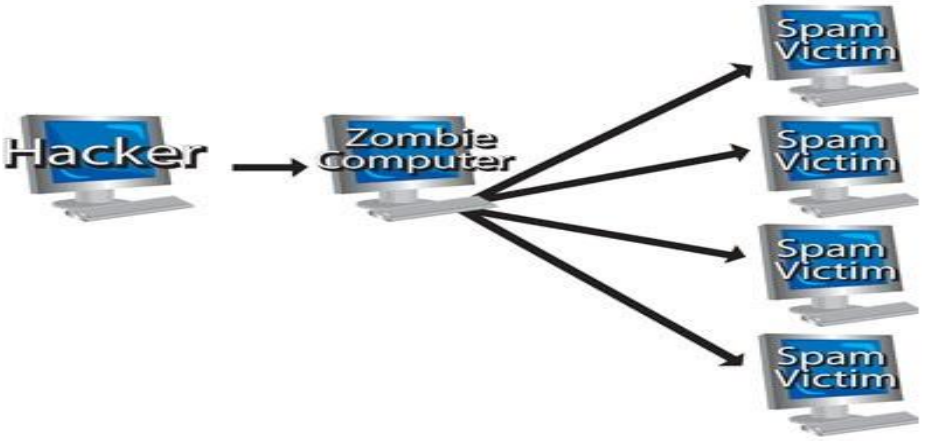


Figure 2.Hacker and spam victim relationship

Hence using malware scanner and SPOT the system had traced out and also analyzed which system is infected and which is not compromised systems.

VII. Conclusion

Once the parameters are learned by the spammers, they can send spam messages below the configured threshold parameters to evade the detection algorithms One possible countermeasure is to configure the algorithms with small threshold values, which helps reduce the spam sending rate of spammers from compromised machines, and therefore, the financial gains of spammers. Spammers can also try to evade PT by sending meaningless "nonspam" messages. Similarly, user feedback can be used to improve the spam detection rate of spam filters to defeat this type of evasions.

More effective spam can be sent by using malware on zombie machines to mine data from email corpora. This allows spam to be sent that automatically mimics legitimate email sent by the real owners of the zombie machines, and our proof-of-concept implementation demonstrates that the result can be convincing even to seasoned users. While this more effective spam has not, to our knowledge, been seen in the wild, there are defensive steps that can be taken now to limit its impact when this spam makes its debut.

As future work we will cross validate the findings using other spam archives; we will also develop more systematic approaches to investigating the inconsistency in spam delivery paths, in addition to the network-level path consistency .Filtering the zombies before the scanner using SPOT.

References

[1] J.S.Bhatia, R.K.Sehgal and Sanjeev Kumar, "Botnet Command detection using Virtual Honeypot," *International journal of Network Security & its applications(IJNSA),* Vol.3, No.5, Sep 2011.

[2] Z. Chen, C. Chen, and C. Ji, "Understanding Localized-Scanning Worms," *Proc. IEEE Int'l Performance, Computing, and Comm. Conf. (IPCCC '07)*, 2007.

[3] Z. Duan, Y. Dong, and K. Gopalan, "DMTP: Controlling Spam through Message Delivery Differentiation," *Computer Networks*, vol. 51, pp. 2616-2630, July 2007.

[4] A. Ramachandran and N. Feamster, "Understanding the Network-Level Behaviour of Spammers," *Proc. ACM SIGCOMM*, pp. 291-302, Sept. 2006.

[5] F. Sanchez, Z. Duan, and Y. Dong, "Understanding Forgery Properties of Spam Delivery Paths," *Proc. Seventh Ann. Collaboration, Electronic Messaging, Anti-Abuse and Spam Conf. (CEAS '10),* July 2010.

[6] Y.Xie, Fang Yu, kannan Achan, Rina Panigrahy, Geoff hulten, Ivan Osipkov," Spamming botnet signature and characteristics," *Microsoft Research*,2008

[7] Xianonam Zang, Athichart Tangpong, George Kesidis and David J.Miller," Botnet detection through fine flow classification," *CSE Dept Technical Report No.CSE11-001*, Jan 2011.