Tracing outgoing mails with AAA using SPRT algorithm

Shree Vardhini B[1], Syeda Tahreem Azeez[2], Johnpaul C I[3]

[12]B.E, Dept. of ISE, NIE, Karnataka, India
[3]Assistant professor, Dept. of ISE, NIE, Karnataka, India

---***---

Abstract - *"Compromised" is one way of telling that someone or something has maliciously broken into the computer without the knowledge or permission. The number of compromised machines which are used to send spam mails have increased and become an issue in organizations. The spam mails consume unnecessary network bandwidth and hence wastage of it due to spamming. Leading to a concern in the organizations and managements to identify and block them inside the network of an organization. Another concern is to prevent the growing Attack by Insiders which has resulted in reduced reputation of the organizations which is the major impact. Thereby, making it a necessity for the organizations to have a system to validate users and to detect spam mails that are of great need in the society.*

***Key Words*: compromised, spam mails, wastage of network bandwidth, attack by insiders, reputation of an organization.**

1. INTRODUCTION

The E-mail traffic consists of uninvited voluntary messages called Spam. Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc are called spam. They cause unnecessary usage of bandwidth. Email spam is given in other terms as junk email or unsolicited bulk email. By selecting the links in spam email may cause users to fraud sites. These fake websites include phishing web sites or sites that are hosting malware. It takes high cost for the organizations to reduce the spam mails by installing spam filters and still not able to achieve the complete result.

An insider attack is a malicious attack perpetrating the network or computer system by a person with authorized system access. Attacks by Insiders have caused a major hurdle in the organizations. So it is of major concern for system administrators to identify it and block the spammers in the network. Spamming provides a key for attackers to recruit the large number of compromised machines. The challenge exists on the internet regarding the huge count of compromised machine which are being used to send spam mails and other security attacks which include spamming and spreading malware, distributed denial of service (DDOS) attacks. Searching and removing compromised machines in a network still remains a serious trail for system administrators of network of all sizes.

2. LITERATURE SURVEY

Email messages are received at a large email service provider, the aggregate global characteristics of spamming botnets including the size of botnets and the spamming patterns of botnets [1] have been investigated by two recent studies, These studies have provided vital insights into the aggregate global characteristics of spamming botnets by clustering spam messages received at the provider into spam campaigns using embedded URLs and near-duplicate content clustering, respectively. We have to focus on the detection of the compromised machines in a network that are involved in the spamming activities, commonly known as spam zombies[1] as the spamming provides a key economic incentive for attackers to recruit the huge number of compromised machines. SPOT is an effective and efficient system in self detecting compromised machines in the network [3] as the dissertation shows. When we compared spam detection algorithms, the performance of SPOT with two other spam zombie detection algorithms based on the number and percentage of spam messages forwarded by internal machines, respectively, it has been observed that SPOT outperforms those two detection algorithms [3]. In AAA concept, it is said to be efficient for network management and security in a network [2], part of whose mechanism which we have to apply in the project. In AAA system architecture, a set of security mechanisms for real-time secondary market services have been proposed. In this architecture [2], the problems of authenticating and authorizing secondary users, synchronizing a group of secondary devices, managing handoff, and detecting non authorized spectrum usage are figured out. As a module of this procedure it is used to prevent not authorized users from sending data from the network.

3. PROPOSED SYSTEM

Proposed system aims at detection of spam zombies that are involved in spamming activities.

It consists of two servers: Authentication server, Mail server. The authentication server does the process of authentication, authorization and accounting (AAA concept). Authentication server checks whether the user is authenticated and authorized to send the mails and the log of emails sent is maintained by accounting. Mail server runs SPRT algorithm which detects spam mails and every detected spam mail is blocked by it but the spammer is notified as the mail has been sent. For every spam mail sent a record is maintained.

Four modules are involved: Staff machine, Authentication server, Mail server, Admin.

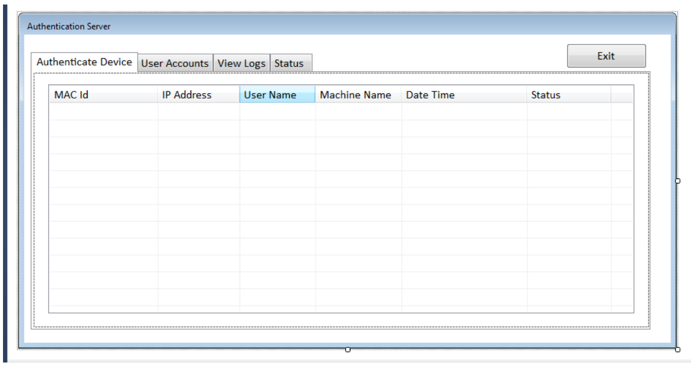
3.1. Staff machine

Staff machine should be registered before sending any mails so it requests Authentication server for the registration. User name, Mac id, Ip address, machine name, date and time are sent in a request packet. It checks the request status from authentication server whether is accepted or rejected. If accepted user is given a private key or else the reason for rejection is viewed to the user. If the user is valid then he can successfully login to the system and can send mails.

3.2. Authentication server

Authentication server accepts the request for registration if the Mac id, IP address, User name, Machine name of the staff machine belongs to the same network and generates a private key to the user and The Status is maintained which shows whether the request is granted or not.

It maintains an XML file which stores the information about user account like user name, email id, password and an option which tells if the user is authorized to send a mail called as "can send". The successful login details are logged in an XML file along with public and private key of that machine.



MAC Id	IP Address	User Name	Machine Name	Date Time	Status

Fig.4.1 User request and login details.

3.3. Mail server

Mail server which is multithreaded redirects the received mails to Authentication server. Sends OTP to the background process which is run in the authentication server for authenticity and authority. If authenticated and authorized, it redirects to mail server and spam detection algorithm called SPRT is run else mail is blocked by the mail server.

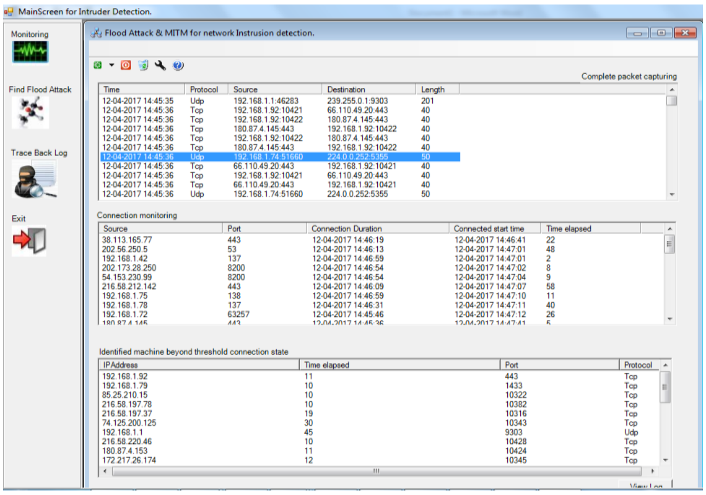
SPRT Algorithm:

Sequential Probability ratio test is a powerful statistical method that is used to test between two hypothesis which in our case is whether the machine is compromised or not as the events (outgoing messages) occur sequentially.

It checks for attachments with virus and if it finds any, it will be deleted. It uses content based filtering methods to check mails which are spam. If found, the mail is blocked from being sent to outside world but the spammer is notified as the mail is sent in order to track his next actions.

When spammer does the flood attack by repeatedly sending the request packets to mail server, the mail server will maintain a graph which depicts the IP address from which the packets have arrived and the count of the packets

When spammer does the flood attack by repeatedly sending the request packets to mail server, the mail server will record the details like time and date, protocol used, source and destination, length of the packet.


MainScreen for Intruder Detection.
Monitoring
Find Flood Attack
Trace Back Log
Exit
Flood Attack & MITM for network Instrusion detection.
Complete packet capturing
Connection monitoring
Identified machine beyond threshold connection state
View Log

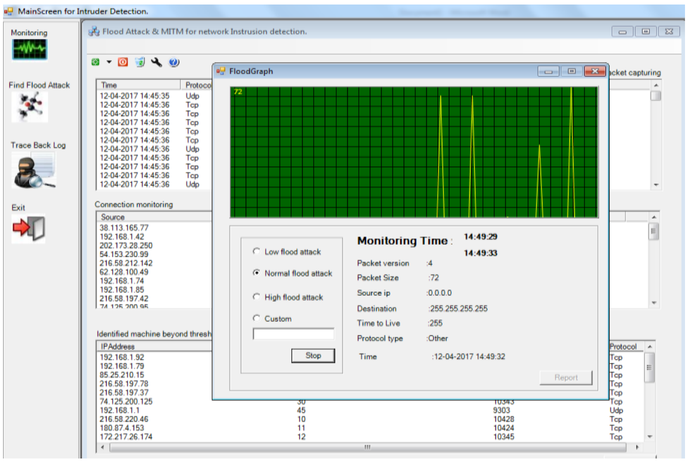
Time	Protocol	Source	Destination	Length
12-04-2017 14:45:35	Udp	192.168.1.1:46283	239.255.0.1:9303	201
12-04-2017 14:45:36	Tcp	192.168.1.92:10421	66.110.49.20:443	40
12-04-2017 14:45:36	Tcp	192.168.1.92:10422	180.87.4.145:443	40
12-04-2017 14:45:36	Tcp	180.87.4.145:443	192.168.1.92:10422	40
12-04-2017 14:45:36	Tcp	192.168.1.92:10422	180.87.4.145:443	40
12-04-2017 14:45:36	Tcp	180.87.4.145:443	192.168.1.92:10422	40
12-04-2017 14:45:36	Udp	192.168.1.74:51660	224.0.0.252:5355	50
12-04-2017 14:45:36	Tcp	66.110.49.20:443	192.168.1.92:10421	40
12-04-2017 14:45:36	Tcp	192.168.1.92:10421	66.110.49.20:443	40
12-04-2017 14:45:36	Tcp	66.110.49.20:443	192.168.1.92:10421	40
12-04-2017 14:45:36	Udp	192.168.1.74:51660	224.0.0.252:5355	50

Source	Port	Connection Duration	Connected start time	Time elapsed
38.113.165.77	443	12-04-2017 14:46:19	12-04-2017 14:46:41	22
202.56.250.5	53	12-04-2017 14:46:13	12-04-2017 14:47:01	48
192.168.1.42	137	12-04-2017 14:46:59	12-04-2017 14:47:01	2
202.173.28.250	8200	12-04-2017 14:46:54	12-04-2017 14:47:02	8
54.153.230.99	8200	12-04-2017 14:46:54	12-04-2017 14:47:04	9
216.58.212.142	443	12-04-2017 14:46:09	12-04-2017 14:47:07	58
192.168.1.75	138	12-04-2017 14:46:59	12-04-2017 14:47:10	11
192.168.1.78	137	12-04-2017 14:46:31	12-04-2017 14:47:11	40
192.168.1.72	63257	12-04-2017 14:45:46	12-04-2017 14:47:12	26
180.87.4.145	443	12-04-2017 14:45:36	12-04-2017 14:47:41	5

IPAddress	Time elapsed	Port	Protocol
192.168.1.92	11	443	Tcp
192.168.1.79	10	1433	Tcp
85.25.210.15	10	10322	Tcp
216.58.197.78	10	10382	Tcp
216.58.197.37	19	10316	Tcp
74.125.200.125	30	10343	Tcp
192.168.1.1	45	9303	Udp
216.58.220.46	10	10428	Tcp
180.87.4.153	11	10424	Tcp
172.217.26.174	12	10345	Tcp

Fig.4.2 Intruder details

It maintains a graph which depicts the IP address from which the packets have arrived and the count of the packets. By plotting graph, the number of observations required to track is reduced which help in monitoring the flood attack.


MainScreen for Intruder Detection.
Monitoring
Find Flood Attack
Trace Back Log
Exit
Flood Attack & MITM for network Instrusion detection.
FloodGraph
72
acket capturing
Connection monitoring
Identified machine beyond thresh
Stop
Report

Time	Protoco
12-04-2017 14:45:35	Udp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Udp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Tcp
12-04-2017 14:45:36	Udp

Source
38.113.165.77
192.168.1.42
202.173.28.250
54.153.230.99
216.58.212.142
62.128.100.49
192.168.1.74
192.168.1.85
216.58.197.42
74.125.200.95

○ Low flood attack
● Normal flood attack
○ High flood attack
○ Custom

Monitoring Time : 14:49:29
14:49:33
Packet version :4
Packet Size :72
Source ip :0.0.0.0
Destination :255.255.255.255
Time to Live :255
Protocol type :Other
Time :12-04-2017 14:49:32

IPAddress			Protocol
192.168.1.92			Tcp
192.168.1.79			Tcp
85.25.210.15			Tcp
216.58.197.78			Tcp
216.58.197.37			Tcp
74.125.200.125	30	10343	Tcp
192.168.1.1	45	9303	Udp
216.58.220.46	10	10428	Tcp
180.87.4.153	11	10424	Tcp
172.217.26.174	12	10345	Tcp

Fig.4.3 Graph representing flood attack

3.4. Admin

Admin has the power of control to use the services of the system and configures the authentication server and spot server. It does the task of responding to the user registration request by authenticating the machine, checking the authority of user, approve or reject the user registration request and maintain the blocked IP's of the user.

4. CONCLUSION

Therefore via indicating a graph the times of observations needed can be reduced hence resulting it an efficient system and an effective system. The graph comprises of on y-axis number of times the spam mails sent and on x-axis the IP addresses. This system works well in the domain of dynamic IP address. Spam mails which are sent which use the name and reputation of an organization can be hindered .If the insider of an organization is sending the mails which he is unauthorized and not authenticated to forward continuously, this system selflessly gives birth to a statistical analysis of the instances the same individual who is the insider of the company who is recapitulating the procedure. The AAA will do authorization, authentication and accounting of the spam mails which are sent. There is a hike in efficiency of the system because the SPRT algorithm is not run until the person is authenticated and thus to safeguard the integrity and to impediment spam mails.

5. FUTURE SCOPE

As we are protecting the harm from insiders of the organization .We need to protect the threat from outside the organization .We have to develop a concept in which the system will be protected from the threats from outside the organization .As any person or group of people can send fake emails from outside the organization or sending unwanted mails to a reputed company. A module should be generated in such a way that the emails coming from the outsiders who are a threat to the insiders in the organization and the organization itself should be blocked by various algorithms. Algorithms should be built in order to block unwanted mails and accept the important mails to an organization. So that the emails from fake accounts can be blocked and filter the incoming emails.

REFERENCES

[1] Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez, Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker," Detecting Spam Zombies by Monitoring Outgoing Messages", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012.

[2] "On the architecture of Authentication, Authorization and Accounting for Real time secondary market services" Yihong Zhou, Dapeng Wu and Scott M. Nettles INTERNATIONAL JOURNAL OF WIRELESS AND MOBILE COMPUTING, JAN 2005.

[3] "Detecting Spam Zombies Using Spot Tool By Monitoring Outgoing Messages" INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING, Volume 3, Issue 4, April 2013.

[4] "Tracking of spam mails using SPRT algorithm with AAA" INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY(IRJET), Volume 4, Issue 3, March 2017, S.NO: 405.