*International Journal of Engineering Research and Modern Education (IJERME)*
*ISSN (Online): 2455 - 4200*
*(www.rdmodernresearch.com) Volume I, Issue I, 2016*

# DETECTION OF E-MAIL MALWARE USING BLOOM FILTER TECHNOLOGY

**G. Robert Arul* & K. Adlin Suji****

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Associate Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

**Abstract:**

*In Today's Internet Mail Server Spam delivery is the most common issue. In the Receiver Side only Most of the modern spam-filtering Techniques are deployed. They are good at filtering spam for end users, but spam messages still keep wasting Internet bandwidth and the storage space of mail servers. This work is therefore intended to detect and nip spamming bots in the bud. We use the Bro intrusion detection system to monitor the SMTP sessions in a university campus, and track the number and the uniqueness of the recipients' email addresses in the outgoing mail messages from each individual internal host as the features for detecting spamming bots. Due to the huge number of email addresses observed in the SMTP sessions, we store and manage them efficiently in the Bloom filters.*

**Index Terms:** Network Security, Simple Mail Transfer Protocol (SMTP) & Bloom Filtering

## 1. Introduction:

In the real world, email is a basic service for computer users, while email malware poses critical security threats. For a number of years, the propagation of email malware has followed the same modus operandi. A viral email is sent to the victim and appears as though it was sent by somebody the recipient trusts. The subject is also related to the recipient's business area. Once the victim is tricked into either clicking the malicious hyperlinks or opening the attachments inside such an email, the computer will be compromised.

The compromised computer will start to infect new targets found in its email address lists immediately. To prevent email malware, scientists have spared no effort to dissuade people from opening unexpected hyperlinks and email attachments. However, the success of recent new email malware, such as "Here you are" indicates that those education measures are not very successful. A key reason is because social engineering is a tried-and-true technique in the context of security.

For example, by convincing computer users that the received emails with malicious hyperlinks and attachments were from a trusted source, the technique of email-borne malware will be highly effective and is still widely adopted by current malware authors Current research on email malware focuses on modeling the propagation dynamics which is a fundamental technique for developing countermeasures to reduce email malware's spreading speed and prevalence.

There are a few works reported to model email malware propagation. Previous works same that a user can be infected and send out malware copies only once, no matter whether or not the user visits a malicious hyperlink or attachment again. Real instances are those early email malware like Melissa in and Love letter in, which will check whether a victim has been compromised before the infection. However, modern email malware is far more aggressive to spread in network than before by introducing two new propagation features.

First feature is "reinfection", i.e., an infected user sends out malware copies whenever this user visits the malicious hyperlinks or attachments. Second feature is "self-start", i.e., an infected user sends out malware copies when certain events (like PC restart) are triggered. Researchers in stated that a user can be infected multiple times. However, their model assumes that an infected user could send out only one malware copy each time the user checks emails, even if the user visits more than one malicious hyperlinks or attachments. In short, previous works id not takes the two new features into account, and hence, cannot accurately estimate the propagation of modern email malware.

The major contributions of this paper are listed below; here propose a new analytical model to capture the interactions among the infected email users by a set of difference equations, which together describe the overall propagation of the modern email malware. Here introduce a new concept of virtual nodes to address the underestimation in previous work, which can represent the situation of a user sending out one more round of malware copies each time this user gets infected. We perform empirical and theoretical study to investigate why and how the proposed SII model is superior to existing models.

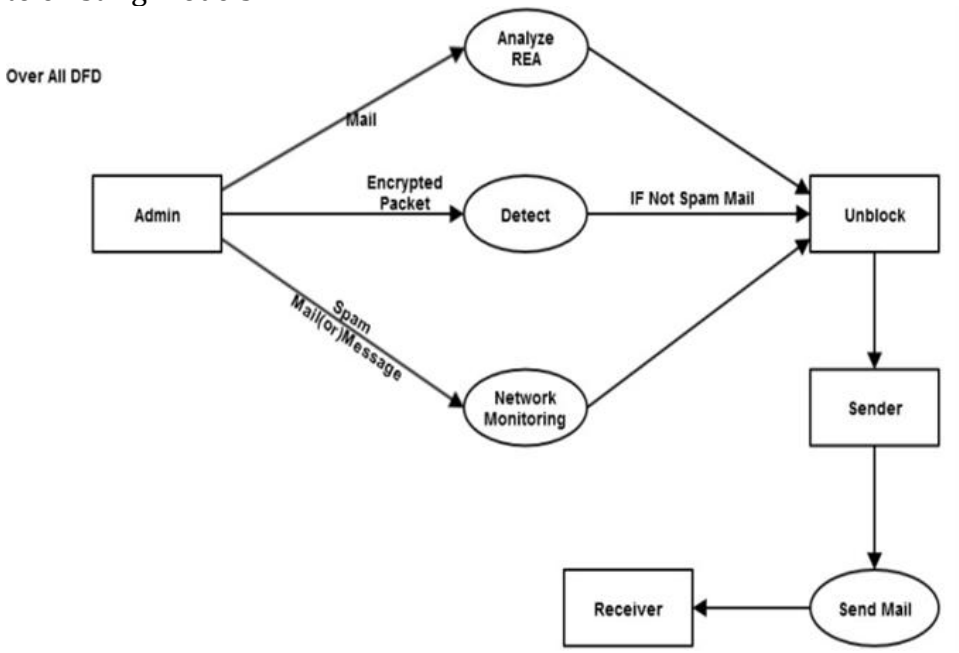


Figure 1: Data Flow Diagram

The reminder of this paper is organized as follows. Section II, describes the Related Works. Section III, describes the Proposed Work. Section IV, describes the Experimental Evaluation and Results. Section V summarizes the Conclusion and Future Enhancement.

## 2. Related Works:

Choosing email as the spreading carrier of malware is not a new technique in the last decade. Early versions of email malware, such as Melissa and Love letter, work in a "naive" way. That is, a compromised user will send out malware emails only once, after which the user will not send out any further malware copies, even if she visits the malicious hyperlinks or attachments again. Take Melissa for example, the malware first checks a specific registry key in the Window OS and the malware will not do anything further when the value of this key suggests that the user has been infected before. In the following, we name this spreading mechanism as non reinjection. However, modern email malware is far more aggressive in spreading throughout email networks than

before. Without checking if a computer has been infected before, modern email malware makes use of every chance to spread itself. We characterize its propagation with two kinds of new mechanisms, namely reinjection and self-start.way of extending the length range of the key shares to increase the attack cost substantially, and do some improvement Original Vanish system.

**3. Proposed Work:**

In Proposed System we are going deploy spam filtering techniques on the sender side itself. Before sending the mail we can able to filter the spam, normally some files come with an extension of .exe and encrypted file sent to the mails. Before this don't have any technique to detect encrypted spam. Using our technique we can neglect the encrypted spam too. This system will improve bandwidth and memory storage. World Net dictionary and short message technique which is used to find the encrypted format text. And finding the spam.

**Advantages:**

- ✓ We use Bloom filters to track the REAs due to a large number of them. Moreover, we also study the cases of spamming through the legitimate mail servers.
- ✓ We present a simple yet effective detection method with high accuracy based on the diversity of REAs. This method is proved to be effective in a real environment.
- ✓ The list of spamming bots is reported to the network administrators in the computer center for them to investigate and crack down the hosts.
- ✓ The detection method also finds account cracking events on mail servers in the campus. The events are critical, and should be detected and cracked down like spamming bots.

**Module:**

- ✓ Compose Mail
- ✓ Detection of Spamming bots
- ✓ Chat
- ✓ Detection of Encrypted Packet
- ✓ Network monitoring
- ✓ Analyze REA's

**Compose Mail:** In this module a single person can send one or more mails to other person, then enter the two mail id and subject body and also add attachment and then click the send button.

**Detection of Spamming Bots:** In this module the bloom filter first checks the subject and body texts, there is any wrong word or unrelated special symbols. If it is presented then block mail and increase count. Otherwise bloom filter get the stream contents from the attachments and generate hash value for all streams. If there is any streams hash value is not find out then automatically consider it is unwanted files, also block this mail.

**Chart:** In this Module users have a number of friends from their circle. If want to contact any friend from these circle then chat / communicate through this e-mail communication network.

**Detection of Encrypted Packet:** In this module the mails and the chat texts are also traveled and then reached the server. For the security reasons files are encrypted and then split as packets and the travel in network. After that server would collect all of the packets and re-assemble then decrypted after that stored in server.

**Network Monitoring:** In this module the spam messages can identify according to the sender`s network. Because every devices has own IP and MAC address which are all

used for access internet. Based on these details an admin collects the counts of blocked mails.

**Analyze REA's:** In this module the spam messages can identify according to Recipient Email Address. If the mail user sends more spam message to more recipients that can be monitored through the sender's mail address or recipient e-mail address .After those monitoring if admin want to block persons then block. After blocking no one use this system for exchange messages.

**4. Experimental Analysis and Results:**

A software application in general is implemented after navigating the complete life cycle method of a project. Various life cycle processes such as requirement analysis, design phase, verification, testing and finally followed by the implementation phase result in a successful project management. System implementation is an important stage of theoretical design is turned into practical system.

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

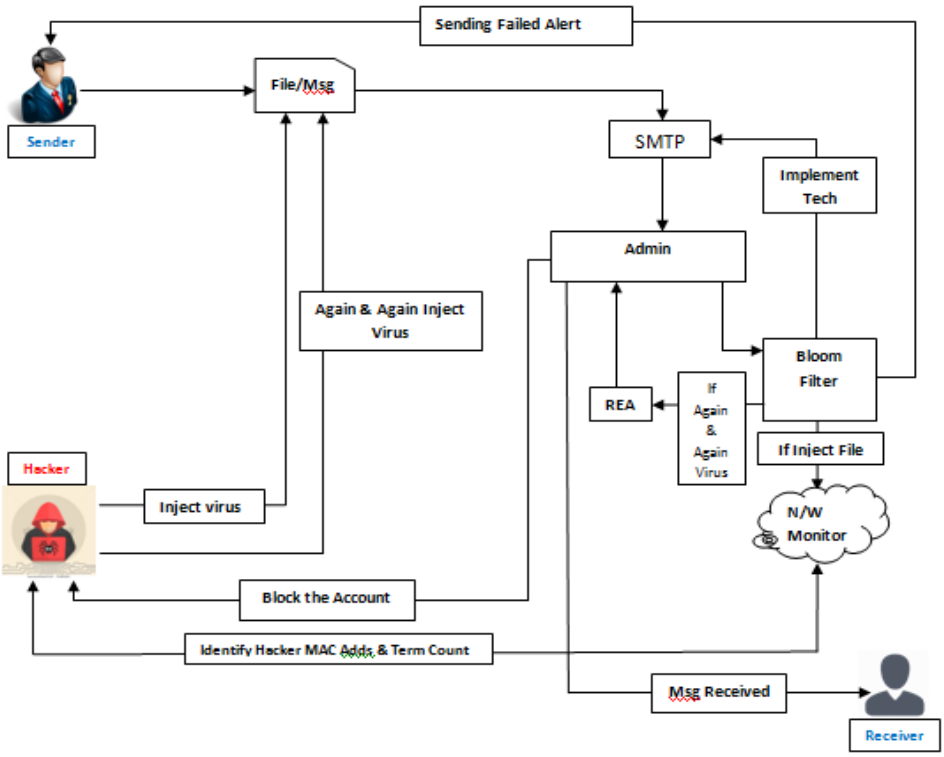


Figure 2: Detection of e-mail malware using bloom filter

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user.

The system that has been developed is accepted and proved to be satisfactory for the user and so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly

and quickly. The final stage is to document the entire system which provides components and the operating procedures of the system.

**Network Based Spamming Bots:**


**Rea Based Spamming Bots:**


## 5. Conclusion:

Here have proposed a novel SII model for the propagation of modern email malware for the independent assumption. I to address two critical processes unsolved in previous models: the reinfection and the self-start. By introducing a group of difference equations and virtual nodes, we presented the repetitious spreading processes caused by the reinfection and the self-start. The experiments showed that the result of our SII model is close to the simulations. For the future work, there are also some problems needed to be solved, such as the independent assumption between users in the network and the periodic assumption of email checking time of users

## 6. Future Enhancement:

The experiments showed that the result of our SII model is close to the simulations. For the future work, there are also some problems needed to be solved, such as the independent assumption between users in the network and the periodic assumption of email checking time of users.

## 7. References:

1. M. Fossi and J. Blackbird, “Symantec Internet Security Threat Report 2010,”

technical report Symantec Corporation, Mar. 2011.

2. P. Wood and G. Egan, "Symantec Internet Security Threat Report 2011," technical report, Symantec Corporation, Apr. 2012.
3. C.C. Zou, D. Towsley, and W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105- 118, Apr.-June 2007.
4. Z. Chen and C. Ji, "Spatial-Temporal Modeling of Malware Propagation in Networks," IEEE Trans. Neural Networks, vol. 16, no. 5, pp. 1291-1303, Sept. 2005.
5. C. Gao, J. Liu, and N. Zhong, "Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis," Knowledge and Information Systems, vol. 27, pp. 253-279, 2011