



Spam Zombie Detection and Blocking with Efficient Content Filtering and User Feedback Mechanism

Amarish Chaudhari

PG student of Department of
Information Technology, SKNCOE,
Pune, India

Ravi Apare

Assistant Professor of Department of
Information Technology, SKNCOE,
Pune, India

Abstract— *The spam zombie detection and blocking with the efficient content filtering and user feedback mechanism is one of the online detection techniques. The system identifies the spam messages and blocks the sender of such messages. Zombie is single compromised machine within the network. The network of such compromised systems is called as a botnet. This system is based on the functionality of SPOT monitoring system which continuously monitors the outgoing messages within the network. The SPOT monitoring system makes the use of the strong statistical tool known as a Sequential Probability Ratio Test.*

Keywords—: *bot, botnet, content filtering, sequential probability ratio test, spam, spam detection, zombie, Zombie Detection System.*

I. INTRODUCTION

The compromised system is responsible for the vital cyber-attacks within the network. A weak system is always vulnerable to all the kinds of attacks. Such a compromised system within the network is a zombie system or also known as a bot. The network of the bots is also known as a botnet. Botmaster is a system which has a monopoly over the network. All the compromised systems work as per the instructions given by this Botmaster.

The Command and Control Channels (C&C) [4] provide the medium for the communication in between the bots. Several illegal activities are performed on the distributed platform provided by these Command and Control Channels.

The Spam Zombie Detection system [10] prefers the intrusion detection system approach for detecting the bots within the botnets. Malwares are responsible for converting the weak systems into the zombie systems by spreading the infection within the network. Generally bots perform the searching, distribution and sign on operations to compromise the other systems within the network [4].

There are two types of botnet architectures:

There are two types of the botnet architectures:

Command and Control Botnet Architecture

It is also known as the centralised architecture. It is like chat like communication between the Botmaster and the bots [4].

Peer to Peer Botnet Architecture

It can remain undetected for long time because the centralised C&C architecture is absent [4].

The detection system requires the global characteristics of the spamming botnets e.g. spamming patterns of the botnets [9]. With the help of this information, the admin can automatically detect the zombie systems in their networks in an online manner.

The detection system has SPOT monitoring system which continuously monitors the outgoing messages from the network [10]. The system uses the statistical tool which is known as the Sequential Probability Ratio Test mechanism [7].

The content filtering mechanism identifies the spam messages in the incoming mails and reports to the SPOT system. The SPOT system then blocks the sender of such a system so that the spammer cannot send any messages further within the network.

The system has virus detector mechanism to detect the viruses in the attachment of incoming mails. The file scanner system scans the attached files for the spamming patterns. The user feedback mechanism is used to help the user to report to the SPOT system against the non-spam but the unwanted messages.

II. RELATED WORK

Zhenhai Duan, Peng Chen, Fernando Sanchez, Yingfei Dong, Mary Stephenson, Jamnes Barker [10] has established the SPOT observing system which makes the use of the statistical method Sequential Probability Ratio Test established by Theo J.H.M. Eggen [7].

Xiacong. Yu^{1,2}, Xiaomei Dong¹, Ge Yu¹, Yuhai Qin², Dejun Yue¹ [8] has settled the BotMiner system which is bot protocol and structure self-governing which categorizes the flows founded on the related communication designs and similar malicious motion patterns.

GuofeiGu, Junjie Zhang, and Wenke Lee [2] established the BotSniffer system that discovers the Bots within the botnets that have spatial temporal relationship and resemblance. It discovers the spatial communication similarity to find the botnets.

GuofeiGu, Phillip Porras, VinodYegneswaran, Martin Fong, Wenke Lee [3] settled the BotHunter system which is a “Dialog Relationship Tactic” which primarily identifies the infection and then coordinates the conversation that happens during the successful malware infection. It discovers compromised machines by correlating the IDS conversation trace in a network.

III. EXISTING SYSTEM

The current system is generally the Spam Zombie detection techniques. The system is concerned only with spotting the spam zombies or botnets. These systems do not deliver any blocking appliance which will constrain the spam zombies systems from sending the spam messages within the network. Some of the systems are having big budget. Some systems depend upon the user defined edge value for determining whether the message is a spam or not. The current system only implements the check on spam messages and do not check for the viruses. The present system does not offer user feedback mechanism for reporting spam mails to the SPOT monitoring systems.

IV. PROPOSED SYSTEM

The functionality of the proposed system is categorized into the following sections:

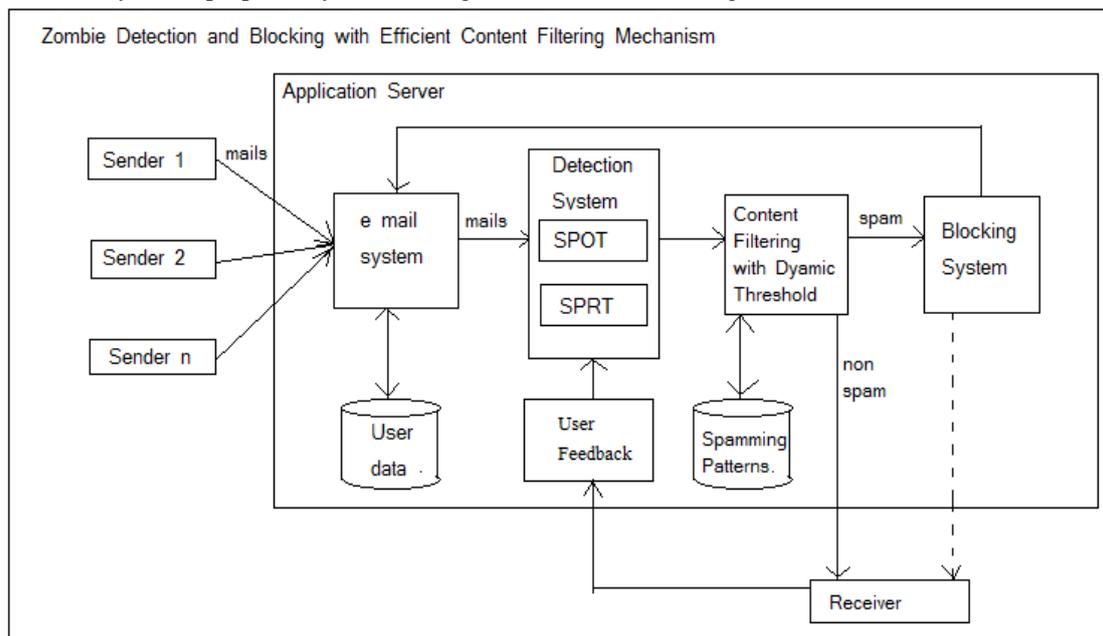


Fig.3 Architecture of the proposed system

1. Mailing System

The mailing system is planned in such way that the user data will be easily available to the administrator of the system. Thus we can manage the information related to the users of the system such as username, password, user id, IP address of the user. The system will store the user information in the own database maintained at the server [1].

2. Detection System

2.1 Sequential Probability Ratio Test

The SPRT algorithm [7] observes the incoming messages in the similar series they arrive at the server. The system has two hypotheses to test, the system is compromised and the system is not compromised. SPRT has the desirable features such as it reduces the probable number of observations with the minor error rates. The false positive error rate and false negative error rate of the system can be selected by the administrator as a threshold. Thus, SPRT helps the recognition system to recognize the spam zombie systems quickly, within the network [10].

2.2 SPOT monitoring system

The working of the monitoring system is largely reliant on the SPRT. The SPOT system first of all registers the IP address of the message as the message reaches the system. The SPOT system calculates the log value of the corresponding probability ratio and brings up to date its value every time a message arrives with the identical IP address. The SPOT system endlessly observes the normal machines within the network as the machines may have chances of getting infected at any time [10].

The detection system takes the four, user defined constraints:

α and β as desired false positive and false negative rates and θ_0 as the probability of a message being spam from normal system and θ_1 as probability of a message being spam from zombie system.

The SPRT considers the desired error rates and draws out the conclusion.

3. Content Filtering with Dynamic Threshold

The spam content filter positioned at the detection system is used to check the message contents. The spam content filtering algorithm mainly categorizes the spam and non-spam messages [6]. We are sustaining a dynamic threshold value which will be valuable for spotting the spam mails even if a spammer sends the very small messages.

4. Blocking System

After the system is acknowledged as the compromised system, the blocking system adds it to the list of the potential zombie systems. The administrator of the system will then have privileges to block the system that has been found as a zombie system. Thus, the blocking of the compromised system will not permit the user of such a blocked zombie system to send any message to any other system within the network [5].

5. User Feedback

The spammer may intend to send the non-spam messages to the user but these messages may be completely meaningless and nonsense messages. In that case the system doesn't detect the spam messages as they do not contain any spamming pattern. Then the user feedback mechanism may provide the user to report the mails as the spam mails. If more than half of the receivers of such messages report to the system then the sender of the messages gets blocked.

V. RESULTS AND DISCUSSIONS

Following the Bar chart that shows the comparison of the current system with the projected system grounded on the number of the observations essential to identify the zombie system. As the quantity of observations rises the bar grows straight up and the end of the bar specifies the recognition of the zombie system on that day. The chart grows horizontally as the quantity of the repetitions for the both the present and projected systems grows. In the chart below b shows the results of present system while the c shows the results of the projected system.

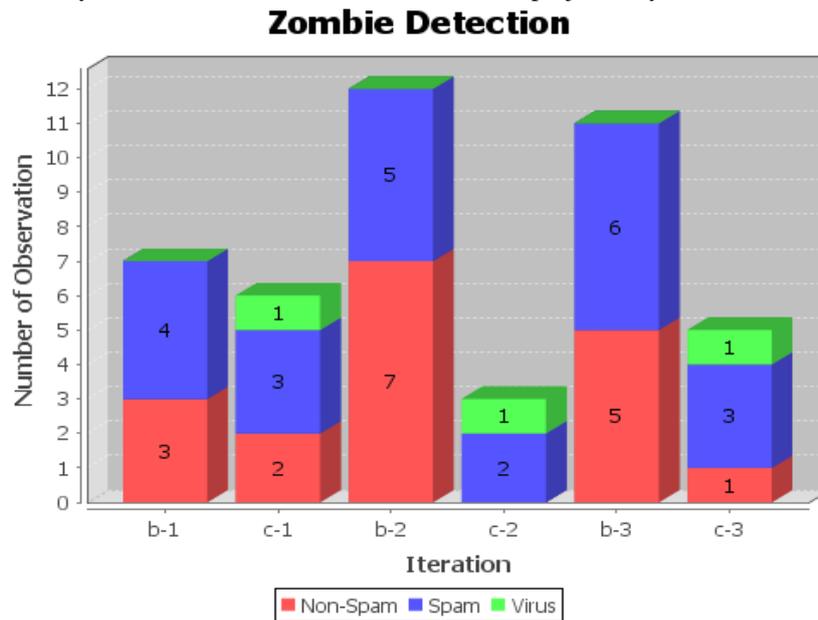


Fig 4 Bar chart showing comparison

VI. CONCLUSION

Thus, the planned system discovers the spam messages with the help of an efficient content filtering mechanism. The content filtering algorithm has a dynamically preserved threshold value which will notice the spam messages independent of the size of the messages. Thus, the SPOT monitoring system will identify the spam zombie system even if the spammer is sending very small messages. Thus, the overall detection system will identify the spam mails and the sender of spam mails with a smallest number of observations. The blocking system then blocks the spam zombie system so that it cannot further send the messages to any other system within the network. The proposed system also checks for the virus attachments and scanning the contents of attachments. The proposed system provides the user feedback mechanism that helps the users to report the system about the nonsense unwanted messages.

ACKNOWLEDGEMENT

I am very thankful to my guide for guiding me and heartily thankful to IJARCSSE for giving me such a wonderful opportunity for publishing my paper.

REFERENCES

- [1] Abhinav Pathak, Syed Ali Raza Jafri and Y. Charlie Hu, 2009, "The Case for Spam-Aware High Performance Mail Server Architecture," 29th IEEE International Conference on Distributed Computing Systems.
- [2] Guofei Gu, Junjie Zhang, and Wenke Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," School of Computer Science, College of Computing Georgia Institute of Technology.
- [3] Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong, Wenke Lee, Aug. 2007, "BotHunter: Detecting Malware Infection through IDS-Driven Dialog Correlation," Proc. 16th USENIX Security Symposium, Boston, MA.
- [4] Hossein Rouhani Zeidanloo, Mohammad Jorjor Zadeh shooshtari, Payam Vahdani Amoli, M. Safari, Mazdak Zamani, 2010, "A Taxonomy of Botnet Detection Techniques," Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference on (Volume:2).
- [5] J. E. Schmidt, July 2006, "Dynamic port 25 blocking to control spam zombies," in Proceedings of First Conference on Email and Anti-Spam (CEAS).
- [6] Jiansheng Wu 1, Tao Deng 2, 2008, "Research in Anti-Spam Method Based on Bayesian Filtering," IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application.
- [7] Theo J.H.M. Eggen, 2008, "The Sequential Probability Ratio Test in Educational Testing," Cito Arnhem.
- [8] Xiaocong. Yu^{1,2}, Xiaomei Dong¹, Ge Yu¹, Yuhai Qin², Dejun Yue¹, 2010, "Botminer: Data-adaptive Clustering Analysis for Online Botnet Detection," Computational Science and Optimization (CSO), 2010 Third International Joint Conference on (Volume:1).
- [9] Yinglian Xie, Fang Yu, Kannan Achan, Rina Panigrahy, Geoff Hulten+, Ivan Osipkov, 2008, "Spamming Botnets: Signatures and Characteristics," SIGCOMM.
- [10] Zhenhai Duan, Peng Chen, Fernando Sanchez, Yingfei Dong, Mary Stephenson, Jamnes Barker, 2012, "Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE Transactions Dependable And Secure Computing Vol.9, No.2.
- [11] Amarish Chaudhari, Ravi Apare, "Spam Zombie detection and Blocking Mechanism," International Journal of Institute of Research and Journal, published in the proceedings of 10th International Conference, 25th December 2013.
- [12] Amarish Chaudhari, Ravi Apare, "Spam Zombie detection and Blocking with Efficient Content Filtering Mechanism," Post Graduate Conference for Information Technology (iPGCON 2014), SKNCOE in association with Cyber Times International Journal of Technology and Management, Volume 7, Issue 1, April 2014.