Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detecting Spam Zombies Using Spot Tool By Monitoring Outgoing Messages

Ar.Arunachalam
Asst.Prof (Department of CSE)
Bharath university Chennai. India

V.Vevek
B.Tech Student (Department of CSE)
Bharath university Chennai. India

V.Yogeswaran
B.Tech Student (Department of CSE)
Bharath university Chennai.India

Abstract--In the internet Compromised machines are the key security threats; it is used to spread various security attacks like spamming and spreading malware.That spamming activitys provides a key incentive to recruit the more number of compromised machines,so we developed an effective spam zombies detection system for detecting an compromised machine in a network.SPOT is called Sequential Probability Ratio Test.It is an spam zombie detection system by monitoring outgoing messages. which has bounded false positive and false negative error rates. In addition, we also compare 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, and show that SPOT outperforms these two detection algorithms.

Keyword: spam zombies,compromised machine,spot

I. INTRODUCTION

It is most complicated work to find the large number of compromised machines on the internet.That machines have been increasingly used to spread different security attacks like spamming and spreading malware.using that spamming activity the attackers can recruit more number of compromised machine in a network.identifying andcleaning compromised machines in a network is an most challenged work for system administrators.so we detecting the compromised machine which are sending spam messages in a network.SPOT is an tool which are using to detect the compromised machine.it is an sequential probability ratio test.we develop the SPOT detection system to assist system administrator in automatically identifying the compromised machine in their network.In addition SPOT only needs small number of observation to detect compromised machine.we also design and study two other spam zombie detection algorithm based on number of spam message and percentage of spam message forwaded by internal machines.

II. RELATED WORK

Unsolicited commercial email, commonly known as spam, has become a pressing problem in today's Internet. In this paper we re-examine the architectural foundations of the current email delivery system that are responsible for the proliferation of email spam. We argue that the difficulties in controlling spam stem from the fact that the current email system is fundamentally sender-driven and distinctly lacks receiver control over email delivery. Based on these observations we propose a Differentiated Mail Transfer Protocol (DMTP) [4]. Botnets are now the key platform for many Internet attacks, such as spam, distributed denial-of-service (DDoS), identity theft, and phishing. Most of the current botnet detection approaches work only on specific botnet command and control (C&C) protocols (e.g., IRC) and structures (e.g., centralized), and can become ineffective as botnets change their C&C techniques. In this paper, we present a general detection framework that is independent of botnet C&C protocol and structure, and requires no a priori knowledge of botnets (such as captured bot binaries and hence the botnet signatures, and C&C server names/addresses). We start from the definition and essential properties of botnets. We define a botnet as a coordinated group of malware instances that are controlled via C&C communication channels[7]. We present a new kind of network perimeter monitoring strategy, which focuses on recognizing the infection and coordination dialog that occurs during a successful malware infection. BotHunter is an application designed to track the two-way communication flows between internal assets and external entities, developing an evidence trail of data exchanges that match a state-based infection sequence model. BotHunter consists of a correlation engine that is driven by three malware-focused network packet sensors, each charged with detecting specific stages of the malware infection process, including in bound scanning, exploit usage, egg downloading, outbound bot coordination dialog, and outbound attack propagation [8]. Botnets are now recognized as one of the most serious security threats. In contrast to previous malware, botnets have the characteristic of a command and control (C&C) channel. Botnets also often use existing common protocols, e.g., IRC, HTTP, and in protocol-conforming manners. This makes the detection of botnet C&C a challenging problem. In this paper, we propose an approach that uses network-based anomaly detection to identify botnet C&C channels in a local area network without any prior knowledge of signatures or C&C server addresses. This detection approach can identify both the C&C servers and infected hosts in the network. Our approach is based on the observation that, because of the pre-programmed activities related to C&C, bots within the same botnet will likely demonstrate spatial-temporal correlation and similarity [9]. An analysis of real-

world botnets indicates the increasing sophistication of bot malware and its thoughtful engineering as an effective tool for profit-motivated online crime. Our analysis of source code and captured binaries has provided insight about [10].

III. CONCEPT

In this project, we will develop a spam zombie detection system, named SPOT, by monitoring outgoing messages. SPOT is designed based on a statistical method called Sequential Probability Ratio Test (SPRT) which has bounded false positive and false negative error rates.

IV. ALGORITHM

A. Spot Detection Algorithm

SPOT is designed based on the statistical tool SPRT. In the context of detecting spam zombies in SPOT, we consider H1 as a detection and H0 as normality. That is, H1 is true if the concerned machine is compromised, and H0 is true if it is not compromised. In addition, we let Xi =1 if the ith message from the concerned machine in the network is a spam, and Xi = 0 otherwise.

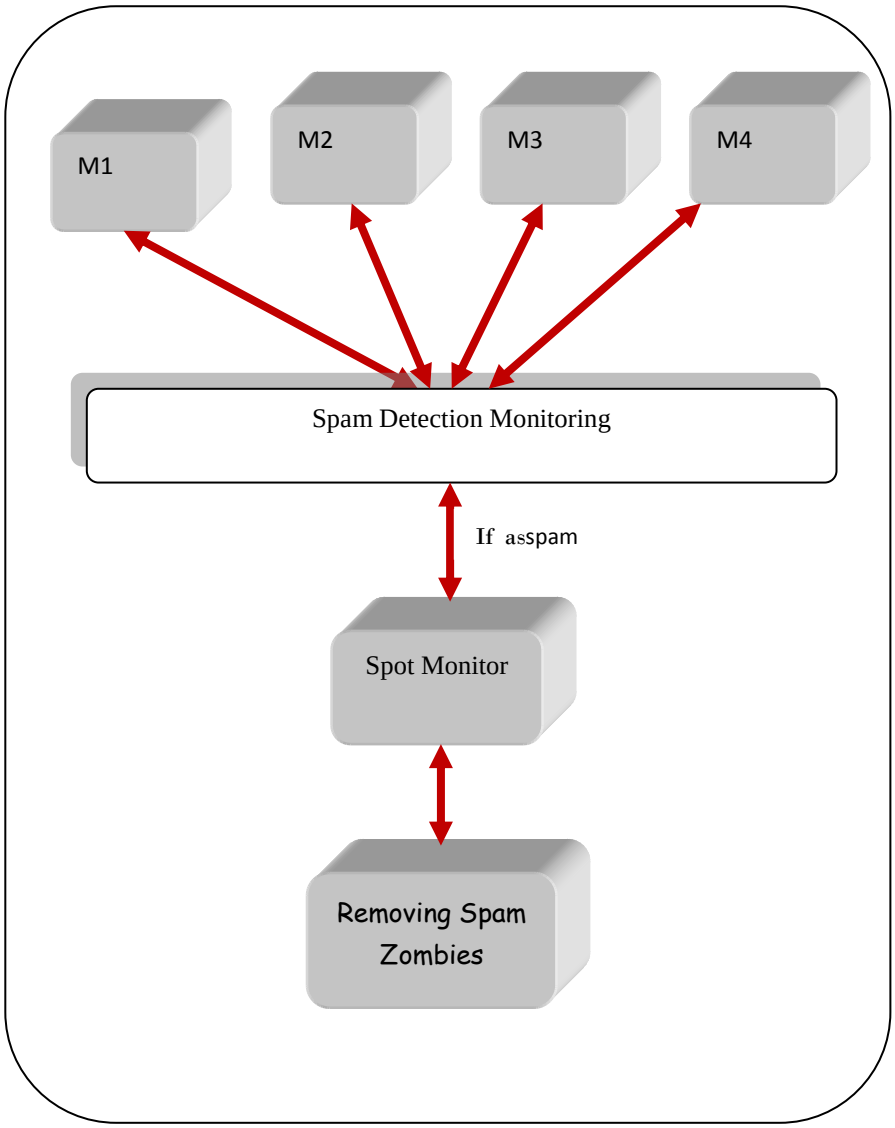
B. Spam Count and Percentage-Based Detection Algorithms

We present two different algorithms in detecting spam zombies, one based on the number of spam messages and another the percentage of spam messages sent from an internal machine, respectively. We refer to them as the count-threshold (CT) detection algorithm and the percentage-threshold (PT) detection algorithm.

A user-defined threshold parameter Cs specifies the maximum number of spam message that may be originated from a normal machine in any time window. The system monitors the number of spam messages n originated from a machine in each window. If n > Cs, then the algorithm declares that the machine has been compromised.

Let N and n denote the total messages and spam messages originated from a machine m within a time window, respectively, then PT declares machine m as being compromised if N>=Ca and n /N > P, where Ca is the minimum number of messages that a machine must send, and P is the user-defined maximum spam percentage of a normal machine.

V. SYSTEM ARCHITECTURE



VI . MODULE DESCRIPTION

A. User Interface Module

In the user interface module we are creating the end user login page for the mailing system. Each and every machine in the network will get login to the mailing system then only it will forward the mail through the network. Here we are creating the user interface module using the JSP.

B. Spot Module

In the SPOT Module when an outgoing message arrives at the SPOT detection system, the sending machine's IP address is recorded, and the message is classified as either spam or no spam by the (content-based) spam filter. The machines which are all sending the spam message are treated as the compromised System.

C. Count Threshold (CT) Module

The count threshold module is counting the number of the spam messages sent by the compromised system in the network. In the SPOT Monitoring process the IP of the Spam spreading systems are monitored. The number of message sent by the machine in a time interval is counted here. If the one machine count gets increased with it then it will be decided as Spam system.

D. Percentage Threshold (PT) Module

In this module we are monitoring the machines messages. Here we are calculating the number of messages sent by the system and counting the number of the spam messages sent by the compromised system then we are calculating the percentage of spam message sent by the compromised system.

E. Spam Zombie Detection Module

In the spam zombie detection module the SPOT method will give the details about the compromised systems. Here the SPOT monitor system will clean the details about the Spam zombie system. Reset the values of the corresponding compromised system details from the monitoring process.

VII. EXPERIMENTAL AND RESULT

In this project, a mail system machine are involved for the mail transactions. The machine which is entering into the network will be monitored by the SPOT. It will monitor the spam messages sent by the system. if the message exceeded the level in the sense SPOT will do some process and decide that system as Spam Zombie. This detection is based on the outgoing messages. SPOT is a lightweight compromised machine detection scheme.SPOT detection system can identify a compromised machine quickly. It also minimizes the numberof required observations to detect a spam zombie.System administrators can automatically detect the compromised machines in their networks in an online manner

VIII. CONCLUSION

In this project, we developed an effective spam zombies detection system for detecting an compromised machine in a network. SPOT is called Sequential Probability Ratio Test. It is an spam zombie detection system by monitoring outgoing messages. which has bounded false positive and false negative error rates. It also minimizes the number of required observations to detect a spam zombie.so in addition we also design and study two other spam zombie detection algorithm based on number of spam message and percentage of spam message forwarded by internal machines.

REFERENCES

[1] *P. Bacher, T. Holz, M. Kotter, and G. Wicherski, "Know Your Enemy: Tracking Botnets," http://www.honeynet.org/papers/bots, 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] *R. Droms, "Dynamic Host Configuration Protocol," IETF RFC 2131, Mar. 1997.*

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

[5] *Z. Duan, K. Gopalan, and X. Yuan, "Behavioral Characteristics of Spammers and Their Network Reach ability Properties," Technical Report TR-060602, Dept. of Computer Science, Florida State Univ., June 2006.*

[6] *Z. Duan, K. Gopalan, and X. Yuan, "Behavioral Characteristics of Spammers and Their Network Reach ability Properties," Proc. IEEE Int'l Conf. Comm. (ICC '07), June 2007*

[7] *G. Gu, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection," Proc. 17th USENIX Security Symp., July 2008.*

[8] *G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: Detecting Malware Infection through Ids-Driven Dialog Correlation," Proc. 16th USENIX Security Symp., Aug. 2007.*

[9] *G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed System Security Symp. (NDSS '08), Feb. 2008.*

[10] *N. Ianelli and A. Hackworth, "Botnets as a Vehicle for Online Crime," Proc. First Int'l Conf. Forensic ComputerScience,2006.*

