ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Experimental Analysis of Network Based Malware and Spam Prediction and Declining Model

R.Vimalasree, P.Ponvasan M.E

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathi Village, Amaravathipudur, Karaikudi, Tamilnadu, India

Assistant Professor, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathi Village, Amaravathipudur, Karaikudi, Tamilnadu, India

ABSTRACT: The main objective of this system is to detect the compromised machines in a network that are used for sending spam messages, which are commonly referred to as spam zombies and harmful malwares. As well as to develop an effective malware/spam zombie detection system named Secured and Portable Optimistic Tool (SPOT). This system is intended to design a tool which can effectively identify the malware/spam messaged over a network. As well as this system is used to identify the compromised machines in a network, which are used for sending spam messages and are commonly referred to as spam zombies and harmful malwares. In this approach a new procedure is developed, which can act as an effective malware/spam zombie detection system, called Secured and Portable Optimistic Tool (SPOT). The proposed approach has two major contributions, those are: (a) It is a network-based tool that does not need to be installed on a device, unlike anti-virus software that can be subverted by malware and (b) Results demonstrate that the network based tool is capable of accurately detecting a class of malware that does not generate Wi-Fi network traffic or highly disguises its Wi-Fi network traffic.

KEYWORDS: Mobile Malware, Bring Your Own Device (BYOD), Wi-Fi network traffic, malware.

I. INTRODUCTION

In the present network scenario most of the machines are affected by means of its compromization, the network attacks mainly focusing this kind of compromised machines in a network, those machines allows the malicious things into the machines easily without any stopping measurements, these malicious things are usually termed as Spam Zombies. Comprehensive features of spamming botnets (networks of compromised machines concerned in spamming) founded scheduled the experimented unsolicited mails conservative at a huge e-mail overhaul contributor expand a device for system administrators to automatically notice the bargained systems in their grids in an connected method. The close by produced retiring messages in a network in general cannot offer the collective big level spam sight necessary by these approaches. SPOT is intended based on a statistical technique called Sequential Probability Ratio Test (SPRT), that can be used to experiment between two suggestions (in our case, a machine is compromised against the machine is not compromised), as the proceedings (in our case, outgoing messages) happen in sequence. SPRT reduces the predictable amount of explanations necessary to arrive at a conclusion among all the chronological and non chronological statistical tests with no better fault rates. This means that the SPOT finding system can recognize a

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

compromised machine rapidly both the false positive and false negative chances of SPRT can be surrounded by user definite thresholds.

The ubiquity of mobile devices within enterprise networks opens new avenues of risk. Enterprises that provide a "bring your own device (BYOD)" environment for its employees or provide guest wireless environments require security managers to monitor wirelessly networked devices where users have the freedom to install any software desired on the device that they own. It is possible that users may inadvertently execute trojanized applications on their devices. In this scenario, malware that either: (1) does not source Wi-Fi network traffic (e.g., it may use bluetooth, or SMS messages for malicious activity), or (2) highly disguises its Wi-Fi network traffic, has ample opportunities to penetrate the network; therefore, the goal of security managers would be to identify the malware immediately and quarantine the infected devices to avoid widespread compromise.
Unfortunately, hostbased malware detection methods (including mobile device managers, MDM) are less trustworthy than they once were. So, an effective network intrusion detection system (NIDS) that is Application Aware should be employed to monitor network traffic and device-level activity in BYOD or guest environments. However, standard NIDS (e.g., Snort) do not possess enough detection capabilities (i.e., are not Application Aware) to address this need. The research presented in this paper investigates this challenge. Using a small test-bed of real applications (i.e., six legitimate applications and eleven malicious applications), we demonstrate the feasibility of an Application Aware Network-based Mobile Malware Monitor (N3M) for BYOD and guest wireless networks using two different Android devices (i.e., HTC Incredible S and Google Nexus S smartphones). Using our custom metric, which is based on taking several measurements and claiming malware only when the majority of measurements are seen as malicious by the classifier, our results yield no false positives/negatives.

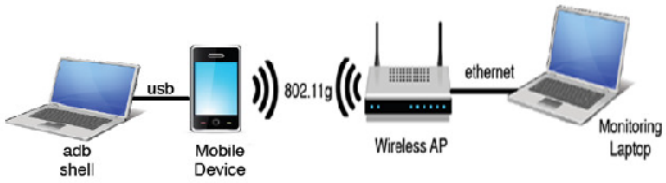

Fig. 1. Mobile Device Malware Evaluation Apparatus

II. SYSTEM IMPLEMENTATION

A. AUTHORIZATION AND AUTHENTICATION

In this Authorization and Authentication module, which is used to allow the user to register his/her identity into the system with proper attributes as well as the authentication scheme checks the e-mail-id and password. If these two fields are valid, the account is authenticated, otherwise block the user to proceed further. The User Authorization and Authentication module is one of most popular and important factor to enter into the required portals and applications. This enhanced authentication and authorization norms module allows the user to register and authenticate themselves into the system with proper identities such as Name, Mobile Number, E-Mail-Id, address, Username and Password and so on. Once the authorization and authentication processes are done, the users have specific rights to proceed into the application and access all the features present into it.

B. SENDING MESSAGES

This Sending Message module allows a single person to send one or more mails to other person. The proposed approach aims to filter the incoming mails are either spam or non-spam. Spam means the more copies of the single message are send as well as it contains more than number of specified lines in the messages received.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

C. SPOT DETECTION

In this SPOT detection module allows to capture the system attributes and sender identity while composing messages. After the mail received by recipient end, the incoming mails are applied to filtering process. Further in this process, the mail content is filtered based on Count Threshold and finally to produce the result of filter in detailed manner. In this CT Detection module to set the threshold value Cs. Cs denotes the fixed length of spam mail. Also to count the number of lines in each mail. If the each mail, counts are greater than equal to threshold value then mark those mails are spam/malware mail.

D. PERCENTAGE THRESHOLD ANALYZER

In this Percentage Threshold Analyzer module administrator is allowed to set threshold value. (a) Ca- specifies the minimum number of mail that machine must send. (b) P- specifies the maximum spam mail percentage of a normal machine. This module is used to compute the count of total mails and the count of spam/malware mails of machine. As well as to check this count of total mails are greater than equal to Cs and the count of malware/spam mails are greater than equal to P, if it's true these mails are considered as a malware/spam mail.

III. LITERATURE SURVEY

New Security Perspectives around BYOD - A. Scarfo - 2012. [1] The dramatic growth of cloud computing services and mobility trends, in terms of 3/4G availability and smart devices, is creating a new phenomenon called "Consumerization" that affects the consumers habits in all facets of the their life. Also during the working time people prefer to stay in their consumer environment because that's their comfort zone. A collateral phenomenon is called BYOD (Bring Your Own Device), that means the employees use their own devices also during their working time. These changing of habits represent an opportunity and a challenge for the enterprises. The opportunity is related to two main aspects: the productivity increase and the costs reduction. In a BYOD scenario the end users would pay totally or partially the devices and would work independently from time and location. On the opposite side, the new scenario bring some risks that could be critical. The use of devices for both personal and working activities opens to new security threats to face for IT organization. Also, the direct comparison between public cloud services for personal use and company's IT services could be a frustrating user experience, that's because of the public cloud services are often almost more effective and usable than typical IT company's services. The aim of this work is presenting a brief survey about the emerging methods and models to approach the BYOD phenomenon from the security point of view.

Android Malware Detection via a Latent Network Behavior Analysis - T. Wei, C. Mao, A. Jeng ,H. Lee ,H. Wang, and D. Wu - 2012. [2]The rapid growth of smartphones has lead to a renaissance for mobile application services.
Android and iOS now as the most popular smartphone platforms offer a public marketplace respectively, the Android Market and App Store- but operate with dramatically different approaches to prevent malware on their devices. In Android platform, developer not only can directly deliver their apps on the Android market without strict review process, but also is capable to put the non-official verified apps marketplace (i.e., Applanet, AppBrain and so on). In this study, we purpose an automatic Android malware detection mechanism based on the result from sandbox. We leverage network spatial feature extraction of Android apps and independent component analysis (ICA) to find the intrinsic domain name resolution behavior of Android malware. The proposed mechanism that identifies the Android malware can achieve in automatic way. For evaluation the proposed approach, the public Android malware apps dataset and popular benign apps collected from Android Market are used for evaluating the effectiveness in analyzing the grouping ability and the effectiveness of identifying the Android malware. The proposed approach successfully identifies malicious Android Apps close to 100% accuracy, precision and recall rate.

Automated Remote Repair for Mobile Malware - Y. Nadji, J. Giffin, and P. Traynor - 2011. [3] Mobile application markets currently serve as the main line of defense against malicious applications. While marketplace revocations have successfully removed the few overtly malicious applications installed on mobile devices, the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

anticipated coming flood of mobile malware mandates the need for mechanisms that can respond faster than manual intervention. In this paper, we propose an infrastructure that automatically identifies and responds to malicious mobile applications based on their network behavior. We design and implement a prototype, Airmid, that uses cooperation between in-network sensors and smart devices to identify the provenance of malicious traffic. We then develop sample malicious mobile applications exceeding the capabilities of malware recently discovered in the wild, demonstrate the ease with which they can evade current detection techniques, and then use Airmid to show a range of automated recovery responses ranging from on-device firewalling to application removal.

Host-Based Intrusion Detection for Advanced Mobile Devices - M. Miettinen, P. Halonen, and K. Hatonen - 2012. [4] New security threats emerge against mobile devices as the devices computing power and storage capabilities evolve. We address in this paper the issue of augmenting current intrusion detection approaches with host-based intrusion detection models for mobile devices. We show that host-based approaches are required, since network-based monitoring alone is not sufficient to encounter the future threats. We outline some of the data types on mobile devices that could be used to construct intrusion detection models, and finally propose a framework for mobile device intrusion detection.

Exploiting temporal complex network metrics in mobile malware containment - J. Tang, C. Mascolo, M. Musolesi, and V. Latora - 2011. [5] Malicious mobile phone worms spread between devices via short-range Bluetooth contacts, similar to the propagation of human and other biological viruses. Recent work has employed models from epidemiology and complex networks to analyse the spread of malware and the effect of patching specific nodes. These approaches have adopted a static view of the mobile networks, i.e., by aggregating all the edges that appear over time, which leads to an approximate representation of the real interactions: instead, these networks are inherently dynamic and the edge appearance and disappearance are highly influenced by the ordering of the human contacts, something which is not captured at all by existing complex network measures. In this paper we first study how the blocking of malware propagation through immunisation of key nodes (even if carefully chosen through static or temporal betweenness centrality metrics) is ineffective: this is due to the richness of alternative paths in these networks. Then we introduce a time-aware containment strategy that spreads a patch message starting from nodes with high temporal closeness centrality and show its effectiveness using three real-world datasets. Temporal closeness allows the identification of nodes able to reach most nodes quickly: we show that this scheme reduces the cellular network resource consumption and associated costs, achieving, at the same time, complete containment of malware in a limited amount of time.

Using Network Traffic to Remotely Identify the Types of Applications Executing on Mobile Devices - L. Watkins, C. Corbett, B. Salazar, K. Fairbanks, and W.H. Robinson - 2013. [6] In an effort to ultimately develop a network-based mobile device resource monitor, we demonstrate the feasibility of remotely detecting the types of applications (i.e., CPU intensive, I/O intensive or non-CPU intensive) actively executing on a mobile device. The distinguishing characteristic of this method is its uncanny ability to remotely infer the types of applications executing on a mobile device when there is no native network traffic being generated from it. To do this, we inconspicuously solicit network traffic from the mobile device by pinging it. Then we capture the timestamps of the ICMP replies, calculate the average inter-packet spacing, and finally use a Neural-Fuzzy Classifier (NFC) that has been previously trained on CPU intensive, I/O intensive, and non-CPU intensive correlated network traffic to discern between the three application types. The NFC acts as a dynamic threshold by grouping the training patterns into clusters and uses these clusters to create membership functions to separate future patterns of each type. We evaluate several Android and Apple devices, and we show that our approach is feasible for Android mobile devices. The key to this method is CPU throttling (when the on-demand governor is used), which scales the CPU performance according to the needs of the presently executing applications in an effort to save power. We exploit CPU throttling to extract embedded delays from solicited ICMP network traffic. Our results show that our method is at least 95 % effective in remotely detecting the types of applications executing on Android mobile device.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

IV. SYSTEM ANALYSIS

A. Existing System

Compromised Machines having more affection from spam zombies and it is the easiest medium to spread malwares across various systems in a network. Major security challenge on the Internet is the existence of the large number of compromised machines. Such machines have been increasingly used to launch various security attacks including spamming and spreading malware, DDoS, and identity theft. They are often used to launch various security attacks such as spamming and spreading malware, DDoS, and identity theft. A major security challenge on the Internet is the existence of the large number of compromised machines.

DISADVANTAGES OF EXISTING SYSTEM

(a) Normal Machine could not identify several security attacks such as spamming and spreading malware, DDoS, and identity theft.
(b) Security challenges are high based on the internet, because it exists large number of compromised machines.
(c) Performance is poor in case of speed and accessibility.

B. Proposed System

In this approach, we focus on the detection of the compromised machines in a network that are used for sending spam messages, which are commonly referred to as spam zombies and harmful malwares. In proposed system to develop an effective malware/spam zombie detection system named Secured and Portable Optimistic Tool (SPOT). SPOT is used to monitoring outgoing messages of a network. SPOT is designed based on a statistical method called Sequential Probability Ratio Rest (SPRT). SPOT is designed to prevent the malwares and zombies with the help of Advanced Fuzzy C-Means (A-FCM), which is based on the FCM. SPOT is designed based on a powerful statistical tool called Sequential Probability Ratio Test, which has bounded false positive and false negative error rates.

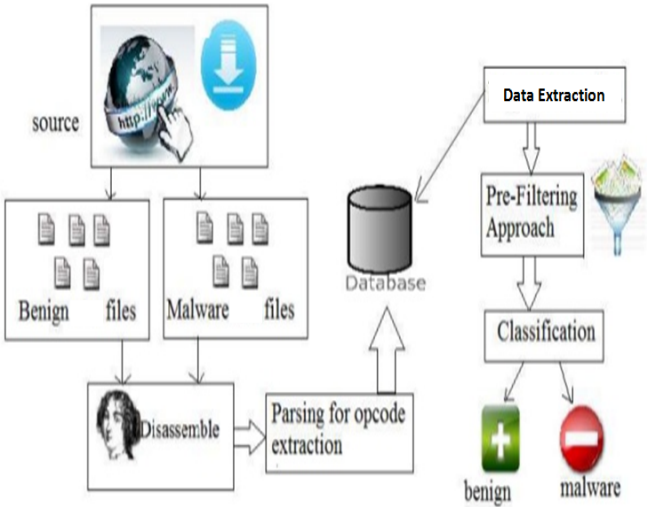

Fig.2 Proposed System Architecture Design

ADVANTAGES OF PROPOSED SYSTEM

(a) Flexible Accessing with proper Access Control facilities
(b) The proposed scheme is more secured, advanced and efficient.
(c) SPOT is introduced to provide efficient and secured Message Transmission over Network environment.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

V. RESULTS AND DISCUSSION

In this section, we provided the simulated results of entire project with its practical proofs. The following figure shows the User Registration Scenario.

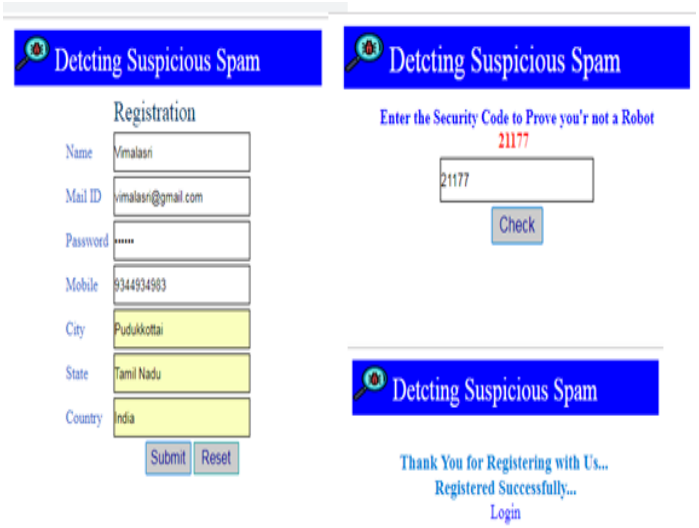

Fig.3 Registration

The following figure illustrates the User Authentication view of the proposed system.

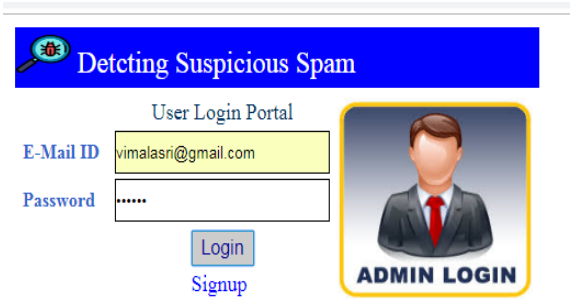

Fig.4 User Authentication

The following figure illustrates the Message Composing view of the proposed system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

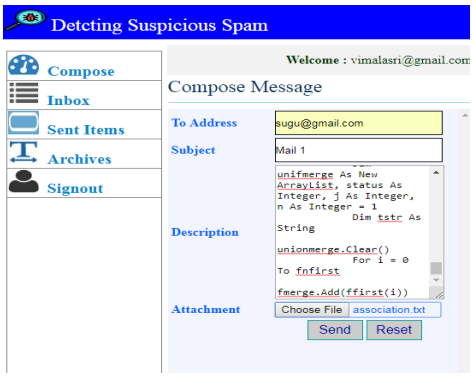

Fig.5 Compose Message

VI. CONCLUSION AND FUTURE WORK

The Sequential Probability Ratio Test tool is used to develop the simple and statistical SPOT which is used to detect the spamming activities in the attacked machines. With the help of SPOT we can detect false positive and false negative error rates compare to the earlier ones. It reduces the number of interpretations which is involved in the detection of spam zombies. We have identified a threat that makes the trust-worthiness of host-based methods questionable and demonstrated that there is a class of malware not detectable by standard IDS like Snort. As a solution, we have introduced SPOT with N3M, emulated its operation, and explained the resulting data.

As future work, we will look closer at mobile application memory usage and definitively determine the contribution of application memory usage on network traffic. Also, we will further test the use of N3M and black/white listing for multi-core Android devices and Apple iOS-based devices. Finally, we will evaluate the performance of N3M with hundreds of malware samples and legitimate applications.

REFERENCES

[1] A. Scarfo, “New Security Perspectives around BYOD”, In The Proceedings Of The International Conference On Broadband, Wireless Computing, Communication and Applications, 2012.
[2] M. Bradley, “What is guest network?”, Mitchell Bradley, http://compnetworking.about.com/b/2009/03/03/what-is-a-guestnetwork.htm.
[3] Texas Instruments Embedded Processors Wiki Website, Accessed June 2017: http://processors.wiki.ti.com/index.php/TI-Android-GingerBread-2.3.4-DevKit-2.1_PortingGuides
[4] T. Wei, C. Mao, A. Jeng ,H. Lee ,H. Wang, and D. Wu, “Android Malware Detection via a Latent Network Behavior Analysis”, In The Proceedings Of The International IEEE Conference on Trust, Security and Privacy in Computing and Communications, 2012.
[5] Y. Nadji, J. Giffin, and P. Traynor, “Automated Remote Repair for Mobile Malware”, In The Proceedings Of The Annual Computer Security Applications Conference (ACSAC), 2011.
[6] M. Miettinen, P. Halonen, and K. Hatonen, “Host-Based Intrusion Detection for Advanced Mobile Devices”, In The Proceedings Of The International IEEE Conference on Advanced Information Networking and Applications (AINA), 2006.
[7] J. Tang, C. Mascolo, M. Musolesi, and V. Latora, "Exploiting temporal complex network metrics in mobile malware containment," In The Proceedings Of The IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011, pp. 1-9.
[9] L. Watkins, C. Corbett, B. Salazar, K. Fairbanks, and W.H. Robinson, “Using Network Traffic to Remotely Identify the Types of Applications Executing on Mobile Devices” In The Proceedings of IEEE Mobile Security Technologies (MoST), May 2013.
[10] SANS Computer Forensics Website Accessed June 2017: http://computer-forensics.sans.org/blog/2012/04/09/is-anti-virus-reallydead-a-real-world-simulation-created-for-forensic-data-yieldssurprising-results.
[11] G. Holmes; A. Donkin and I.H. Witten (1994). "Weka: A machine learning workbench". In The Proceedings of The Second Australia and New Zealand Conference on Intelligent Information Systems, 1994.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

[12] M. Sami, A. Hassanien, N. El-Bendary, and R. Berwick, "Incorporating Random Forest Trees with Particle Swarm Optimization for Automatic Image Annotation", In The Proceedings Of The IEEE Federated Conference on Computer Science and Information Systems, pp.763- 769, 2012.
[13] Google Play Website, Accessed June 2017: https://play.google.com/store/apps
[14] Smali Website, Accessed June 2017: https://code.google.com/p/smali/.
[15] WEKA 10-Fold Cross Validation Website, Accessed June 2017: http://www.cs.waikato.ac.nz/ml/weka/mooc/dataminingwithweka/transcripts/Transcript2-5.txt