International Journal of Technology and Engineering System (IJTES)
Vol 7. No.1 2015 Pp. 81-85
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

SPATIAL – TEMPORAL MODELING ON PROPAGATION OF MALWARE ON E-MAIL

M.SUBRAMANIYAN [1], R.THAMIZHAZHAGAN [2], A.VIGNESH [3], MR.R.VIJAYABHARATHI [4]
[1], [2], [3]UG Scholar, B.E. Computer Science and Engineering.
[4]Assistant Professor, Dept. of CSE.
MRK Institute of Technology, Kattumannarkoil.
Email:subramaniyanganapathy93@gmail.com,vimalvignesh64@gmail.com, thamilramcse@gmail.com

ABSTRACT

Nowadays email becomes basic service for all computers users. There are some critical threads imposed by email malware in recent years. So it necessary to Modeling the propagation dynamics of email malware becomes a fundamental technique for predicting its potential damages and developing effective countermeasures. Comparing the modern email malware with earlier version, modern email malware having two new features called reinfection and self-start. Reinfection refers to the malware behavior that the modern email malware send out malware copies whenever any healthy or infected recipients open certain files.Self-start refers to the malware behavior that an email malware starts to spread whenever compromised user computers restart or certain files are visited. In the literature several models are proposed for email malware propagation, but they did not take into account the above two features. Malware is a malicious software that disrupt the network performance, gather sensitive information, gain access to system, etc. To address this problem we introduce a virtual node in this paper. In this paper we overcome the two new features of modern email malware and more aggressive to spread in the network.

Index Terms:Email malware, network security.

1.INTRODUCTION

In real world, email is basic service for all computer users. However email malware possess critical security threads. Malware is a software designed to attack and damage, disable, or disrupt computers, computer systems, or networks. Hackers often take advantage of website security flaws, also known as vulnerabilities, to inject malware into existing software and systems with consequences that can range from the relatively begin like annoying pop-up windows in a web browser to the severe, including identity theft and financial ruin. A malware email is sent to the victim and appears like as though it was sent by somebody the recipients trusts. Once the victim click the malicious hyperlinks or malicious attachment then the computer will be compromised, and the compromised computer will start to infect new targets found in its email address list immediately. For example the compromising computer users that the received mails with malicious hyperlinks and attachments were from the trusted source.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 few works reported to model email malware propagation. Previous works assume that the user infected and send email malware copies only once, no matter whether or not the user visits a malicious hyperlink or attachment again. However the modern email malware is farmore aggressive to spread in network the before by introducing two new propagation features. First feature is reinfection i.e., an infected users send out the malware copies whenever the user visits the malware hyperlinks or attachments. Second feature is self-start i.e., a user sends out malware copies when certain events are triggered. In previous works they did not take the two new features into account, and hence cannot accuratelyestimate the propagation of modern email malware. In this paper we try to overcome these features and reduce the propagation speed.

II.RELATED WORKS:

There have been substantial efforts in modeling the propagation dynamics of Internet malware in the last decade. First, to model the epidemic spreading on topological networks, early researchers adopt differential equations to present the propagation dynamics of malware. However, as discussed in [3], the differential models [20], [32], and [34] greatly overestimate the spreading speed due to the "homogeneous mixing "assumption. Additionally, Zhou et al. [3] and GAO Et Al. [5] on simulations to model the spread of email malware. Their simulation models avoid the "homogeneous mixing "problem but cannot provide analytical propagation studies. The works [4], [8], [21], [23] propose mathematical models, which have captured the accurate topological information.Wen et al. [8] further addressed the temporal dynamics and the spatial dependence problem in the propagation modeling.

However, all these models cannot present the reinfection and self-start processes of modern email malware. The Works in [21], [22], [23] focus on threshold conditions for malware fast extinction on the Internet. Their works study the final stable state of epidemic spread based on SIS models, whereas we study the transient propagation dynamics of modern email malware.

Second, there are some works which characterize the propagation dynamics of isomorphic malware, such as P2P malware [33], mobile malware [36], [37] and malware on online social networks [28], [29]. R. Thomas and M. Coates [33] adopt differential equations to present the propagation of P2P malware through a P2P network. The models [36], [37] are proposed for the mobile environment by presuming nodes meet each other with a probability. These works assume all individual devices are homogeneously mixed, and thus, they are unlikely to work in the real mobile environment. The models [28], [29] present the propagation ofonline social malware by simulations. Since these models [28], [29], [33], [36], [37] are based on no reinfection, they cannot be adopted topresent the propagation of modern email malware.

III.EXISTING SYSTEM:

Choosing email as the spreading carrier of malware is not a new technique in the last decade. Early versions of email malware, compromised user will send out malware emails only once, after which the user will not send out any further mail. But the modern emails malware has two features. In the existing system they are taken account the two new feature. They are not giving any spreading procedure. However, modern email malware is far more aggressive in spreading throughout the email network. We characterize its propagation with two kids of new mechanism, namely reinfection and self-start.

3.1 Disadvantages:

- ❖ Previous technology does not consider the spreading procedure.
- ❖ Malwares are easily spread our e-mail and as well as local system also.

4. PROPOSED SYSTEM:

We propose a new analytical model to capture the interactions among the infected email users by asset of difference equations, which together describe the overall propagation of the modern email malware. We introduce a new concept of virtual ode to address the underestimation in previous work, which can represent thesituation of user sending out one more round of malware copies each time this user gets infected. Generally it is common for the malware email to reuse the themes but with slight variations on the body of the message and the attachments names. This trick increases the possibility for a user to be infected and particularly prompts the spreading efficiency of the modern reinfection email malware.

4.1. VIRTUAL NODE:

For modern email malware recall that the compromised user may send out malware email copies to neighbors every time the user visitsthose malware hyperlinks and attachments. Malware e-m ails are send out when certain events like computer restart are triggered. We introduce the new node called the virtual node to denote the possible spreading if user visits the second malware email. We also use the virtual node to denote the possible spreading if user visits the third malwareemail. Nodes and topology information are the basic elements for the propagation of modern email malware. A node in the topology represents a **user in the email network. All nodes in networks are** initially susceptible. Since infected users will send out malware copies where they are compromised, node I transits from the susceptible state to the active state after the user of node i gets infected. The infection probability is denoted by v (i, t). The user is infectious at the active state. When a user is infected but bot infected the node transits to the dormant state. The virtual node can store the characteristics and behavior of malicious node when the hyperlinks are clicked or the malicious attachments are opened. Generally the malicious attachments are appears like they are form the recipients who are trust to the users.

4.2. Advantages:

- To control the malware spreading in email.
- Using virtual node to dodge the malware.
- Especially designed for worm and macro viruses

5. SYSTEM ARCHITECTURE:

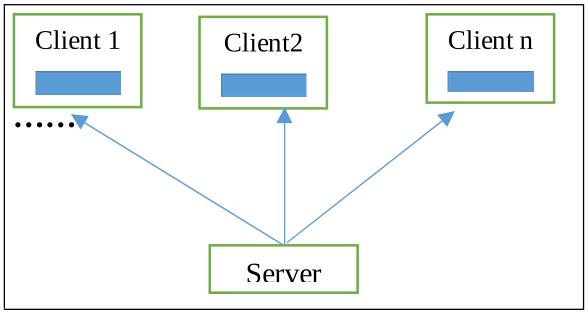


Fig1.1:e-mail client server model

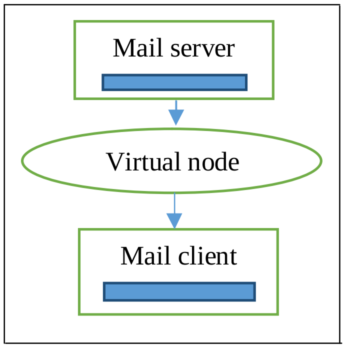


Fig1.2:Access mail though virtual node

6. NATURE OF WORK:

The proposed system consider the two new features of the modern email malware. The virtual node can detect the malicious attachment. The virtual can store the behavior and characteristics of the malware and updated. If any new malware comes when user click the hyperlink or open malicious attachment then the virtual node can store this. The proposed model have four modules. They are as follows:

- Network formation.
- Attacker performance.
- Detection of malicious user.
- Data transfer through virtual node.

7. MODULES DESCRIPTION:

7.1. Network formation:

The network is formed by set of nodes and each of them are identified by a unique ID called N1, N2, N3 …Nn. The nodes are the basic element for propagation of modern email malware. A node in the topology represents a user in the email network. The user may send mail at any time and other user opens the mail at any time.

7.2. Attacker Performance:

The malware is the malicious software that can disrupt the computer operation, gather sensitive information, gain access to the system, and disrupt the network performance. The modern email malware send out the malware copies whenever the compromised user click the malicious attachment or hyperlinks.

7.3. Detection of malicious user:

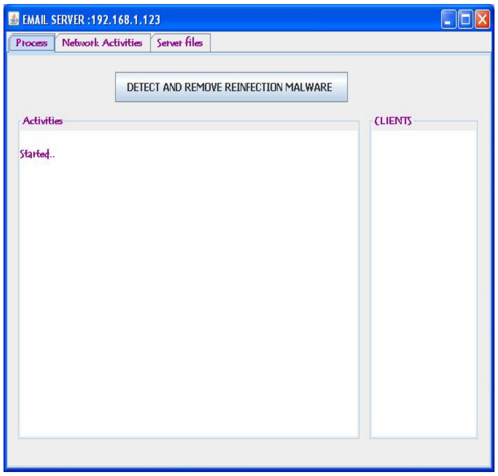
The proposed system can detect the malicious hyperlinks and attachments. When the legitimate user try to communicate to server at the time the attacker can hack the message. The virtual node identify them.

7.4. Data transfer through virtual node:

Virtual node can represent the situation of the user sending out one or more round of malware copies each times user gets infected. The virtual node detect the malicious attachments. When the malicious attachments are transfer again it detect. This reduce the speed of propagation.

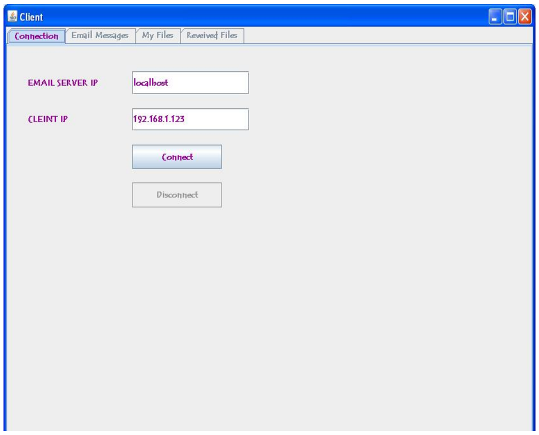
8. RESULTS:

The result obtained from the implementation using java, WAMP server shown below.


EMAIL SERVER :192.168.1.123
Process
Network Activities
Server files
DETECT AND REMOVE REINFECTION MALWARE
Activities
CLIENTS

Started..

Fig8.1: Server window



EMAIL SERVER IP: localhost

CLEINT IP: 192.168.1.123

Fig8.2: Client window

9. CONCLUSION:

In this paper we propose a new model for the propagation of modern email malware. This model is able to address the two critical problems of the unsolved in previous model called reinfection and self-start. By introducing the virtual node we present the model to reduce the propagation speed and overcome the two features of modern email malware. The results are shown by implementing using java. Finally we are interested in studying the distribution of multiple copies of malware in large scale networks. We need to seek the appropriate model to address this problem in large scale networks.

10.FUTURE WORK:

In future we can implement this concept in large type viruses like as Trojans, Inkgen, Hosting viruses etc. So we can able to make the malware free network and to avoid the lot of cybercrime activities and can be applied to large scale networks.

11. REFERENCES:

[1] M. Fossi and J. Blackbird, "Symantec Internet Security ThreatReport 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 SimulationStudy of the Propagation and Defense of Internet E-Mail Worms,"IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105118,Apr.-June 2007.

[4] Z. Chen and C. Ji, "Spatial-Temporal Modeling of Malware Propagationin 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 VirusPropagation in Email Networks: Experimental Evaluation andAnalysis," Knowledge and Information Systems, vol. 27, pp. 253-279,2011.

[6] S. Wen, W. Zhou, Y. Wang, W. Zhou, and Y. Xiang,"LocatingDefense Positions for Thwarting the Propagation of TopologicalWorms," IEEE Comm. Letters,vol. 16, no. 4, pp. 560-563, Apr. 2012.

[7] J. Xiong, "Act: Attachment Chain Tracing Scheme for Email VirusDetection and Control," Proc. ACM Workshop Rapid Malcode(WORM '04), pp. 11-22, 2004.

[8] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia,"Modeling Propagation Dynamics of Social Network Worms,"IEEE Trans. Parallel and Distributed Systems, vol.24, no. 8, pp. 16331643,Aug. 2013.

[9] (1999) Cert, advisory ca-1999-04, Melissa Macro Virus, http://www.cert.org/advisories/CA-1999-04.html, 2009.

[10] Cert, Advisory ca-2000-04, Love Letter Worm,
http://www.cert.org/advisories/CA-2000-04.html, 2000.

[11] M. Calzarossa and E. Gelenbe, Performance Tools
And Applicationsto Networked Systems: Revised
Tutorial Lectures. Springer-Verlag,2004.

[12] G. Serazzi and S. Zanero, "Computer Virus
Propagation Models,"
Proc. 11th IEEE/ACM Int'l Conf. Modeling, Analysis and Simulations of Computer and Telecomm. Systems
(MASCOTS '03), pp. 1-10, Oct 2003.

[13] B. Rozenberg, E. Gudes, and Y. Elovici, "SISR: A
New Model forEpidemic Spreading of Electronic
Threats," Proc. 12th Int'l Conf.Information Security, pp.
242-249, 2009.

[14] (2001) Cert, Advisory ca-2001-22, w32/sircam
Malicious Code,
http://www.cert.org/advisories/CA-2001-22.html, 2001.

[15] Cert, Incident Note in-2003-03, w32/sobig.f Worm, http:// www.cert.org/incidentnotes/IN-2003-03.html, 2003.

[16] C. Wong, S. Bielski, J.M. McCune, and C. Wang, “A Study of Mass-Mailing Worms,” Proc. ACM Workshop Rapid Malcode (WORM ’04), pp. 1-10, 2004.

[17] D. Moore and C. Shannon, “The Nyxem Email Virus: Analysis and Inferences,” technical report, CAIDA, Feb. 2006.

[18] Symantec, A-Z Listing of Threats and Risks, http://www.symantec.com/security Response, 2012.

[19] C. Zou, Internet Email Worm Propagation Simulator

[22] A.J. Ganesh, L. Massouli, and D.F. Towsley, “The Effect of NetworkTopology on the Spread of Epidemics,” Proc. IEEE INFOCOM’05, pp. 1455-1466, 2005.

[23] D. Chakrabarti, J. Leskovec, C. Faloutsos, S. Madden, C. Guestrin, and M. Faloutsos, “Information Survival Threshold in Sensor and p2p Networks,” Proc. IEEE INFOCOM ’07, pp. 1316-1324, 2007.

[24] Y. Wang, S. Wen, S. Cesare, W. Zhou, and Y. Xiang, “Eliminating Errors in Worm Propagation Models,” IEEE Comm. Letters, vol. 15, no. 9, pp. 1022-1024, Sept. 2011.

[25] H. Ebel, L.I. Mielsch, and S. Bornholdt, “Scale-Free Topology of Email Networks,” Physical Rev. E, vol. 66, no. 3, Sept. 2002.

[26] M.E. . Newman, S. Forrest, and J. Balthrop, “Email Networks and the Spread of Computer Viruses,” Physical Rev. E, vol. 66, no. 3, 2002.

[27] T. Bu and D.F. Towsley, “On Distinguishing between InternetPower Law Topology Generators,” Proc. IEEE INFOCOM ’02, pp. 638-647, 2002.

[28] G. Yan, G. Chen, S. Eidenbenz, and N. Li, “Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications,” Proc. Sixth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’11),, pp. 196-206, 2011.

[29] W. Fan and K.H. Yeung, “Online Social Networks-Paradise of Computer Viruses,” Physica A: Statistical Mechanics and Its Applications, vol. 390, no. 2, pp. 189-197, 2011.

[30] S. Wen, “Topology Generator and Propagation Simulator of Modern Email Malware,” Experement Result, http://www.deakin. edu.au/wsheng/emailpropagation.html, 2012.

[31] G. Eschelbeck, “The Laws of Vulnerabilities,” Proc. BlackHat Conf., 2004.

[32] R. Pastor-Satorras and A. Vespignani, “Epidemic Spreading in Scale-Free Networks,” Physical Rev. Letters, vol. 86, pp. 3200-3203, 2001.

[33] R. Thommes and M. Coates, “Epidemiological Modelling of Peerto-Peer Viruses and Pollution,” Proc. IEEE INFOCOM ’06, pp. 112, 2006.

[34] Y. Moreno, J.B. Gomez, and A.F. Pacheco, “Epidemic Incidence in Correlated Complex Networks,” Physical Rev. E, vol. 68, Sept. 2003.

[35] D.H. Johnson and S. Sinanovic, “Symmetrizing the Kullbackleibler Distance,” technical report, Rice Univ., Houston, TX, 2001.

[36] G. Yan and S. Eidenbenz, “Modeling Propagation Dynamics of Bluetooth Worms (Extended Version),” IEEE Trans. Mobile Computing, vol. 8, no. 3, pp. 353-368, Mar. 2009.

[37] S.M. Cheng, W.C. Ao, P.Y. Chen, and K.C. Chen, “On Modeling Malware Propagation in Generalized Social Networks,” IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011.