



ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Malicious Programs Analysis Propagation In Online Social Networks

R. Regan, J. Renuka Devi and V.Sanmugasundhari

Department of Computer Science and Engineering University College of Engineering, Panruti

ARTICLE INFO

Article history:

Article Received : 12 January 2015

Revised: 1 May 2015

Accepted: 8 May 2015

Keywords:

ABSTRACT

In the real world, email is a basic service for computer users, while email malware possess the critical security threats. The technique of email malware will be highly effective. Email malware focuses on modeling the proliferation dynamics which is a fundamental technique for developing counter measures to reduce email malware's spreading speed and prevalence. Modern email malware exhibits two new features, reinfection and self-start. Reinfection is an infected client when sends out hostile copies whenever this client visits the malevolent hyperlinks or attachments. Self-start refers to the behavior that malware starts to spread whenever concession computers are recommence. In the literature, several models are proposed for email malware proliferation but they cannot accurately model the proliferation dynamics of modern email malware. The spreading procedure can be epitomized by a susceptible-infected-immunized (SII) process. The proposed model can precisely present the repetitious spreading process caused by reinfection and self-start and effectively overcome the associated computational challenges. The results show our model provides the estimation accuracy.

© 2015 AENSI Publisher All rights reserved.

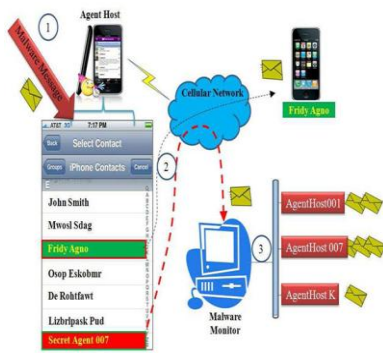
To Cite This Article: R. Regan, J. Renuka Devi and V. Sanmugasundhari., Malicious Programs Analysis Propagation In Online Social Networks. *Aust. J. Basic & Appl. Sci.*, 9(21): 35-38, 2015

INTRODUCTION

Malware short for malicious software, is any software used to disrupt computer operation gather sensitive information, or gain access to private computer systems (Fossi, M. and J. Blackbird, 2011). It can appear in the form of executable code, scripts, active content, and other software with the escalating growth of communication and information systems, a new term and acronym invaded the digital world called as malware. It is a general term, which stands for malicious software and has many shapes (codes, scripts, active content and others). It has been designed to achieve some targets such as, collecting sensitive data, accessing private computer systems, even sometimes harming the system. The malware can reach the systems in different ways and through multiple media; the most common way is the downloading process from the internet, once the malware finds its way to the systems, based on the functions of the malware the drama will begin. In some cases, the malware will not totally harm the system, instead affect the performance and creates overload process; in case of spying, the malware hides itself in the system, which cannot be detected by the anti-virus software, these hidden malware send critical information about the computer to the

source. Based on the above challenges, it is critical to carry out an in-depth analysis to understand the malware for better. 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. Then, 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.

Corresponding Author: R. Regan, Department of Computer Science and Engineering University College of Engineering, Panruti
E-mail: reganr85@gmail.com



1. Malware Propagation:

Many studies and researches focused on studying the malware propagation in the digital world, communications and computer networks, some of the modeling and experimental procedures have been followed to study the effect of malware and the way it propagates in these fields, in addition to this, the studies cover some concepts and techniques related to malware detection (Zou, C.C., 2007). The malware propagation concept refers to the electronic method, by which, malware is transmitted to an information system, platform or device it seeks to infect for example the malware can propagate through PDF files and access the host unless the user disable the JavaScript in PDF reader.

2. System Overview:

For present an email worm simulation model that accounts for the behaviors of email users, including email checking time and the probability of opening an email attachment. The observations of email lists suggest that an Internet email network follows a heavy-tailed distribution in terms of node degrees, and model it as a power law network. To study the topological impact, compare email worm propagation on power law topology with worm propagation on two other topologies: small world topology and random graph topology. The impact of the power law topology on the spread of email worms is mixed: email worms spread more quickly than on a small world topology or a random graph topology, but immunization defense is more effective on a power law topology. Propose and solve the problem using non-linear dynamical systems and fixed point stability theorems. To provide a closed form formula that, surprisingly, depends on only one additional parameter, the largest eigen value of the connectivity matrix (Wen, S., 2013). To illustrate the accuracy of our analysis on realistic and real settings, like mote sensor networks from Intel and MIT, as well as Gnutella and P2P networks. To analyze the social structure and user activity patterns of this network, and confirm that it is a typical online social network, suggesting that conclusions drawn from this specific network can be translated to other online social networks. The extensive trace-driven simulation to study the impact of initial infection, user click probability, social structure, and activity

patterns on malware propagation in online social networks. The models 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 present the propagation of online social malware by simulations (Wood, P. and G. Egan, 2012). Since these models are based on non reinfection, they cannot be adopted to present the propagation of modern email malware. The previous analytical model presented the spreading procedure by an susceptible-infected-susceptible (SIS) process, while it does not consider the new features of modern email malware. These observations become the motivation of work to develop a new analytical model that can precisely present the propagation dynamics of the modern email malware. Since the spreading procedure can be characterized by a susceptible-infected-immunized (SII) process. The major contributions of this paper are listed below: 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. To 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. Perform empirical and theoretical study to investigate why and how the proposed SII model is superior to existing models. Modern email malware exhibits two new features, reinfection and self-start. For address this problem, to derive a novel difference equation based analytical model by introducing a new concept of virtual infected user. 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. The Proposed a novel SII model for the propagation of modern email malware. This model is able 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.

3. Protocol Description:

TCP provides a communication service at an intermediate level between an application programs. The software can issue a single request to TCP and let TCP handle the IP details. IP works by exchanging pieces of information called packets. A packet is a sequence of octets (bytes) and consists of a header followed by a body. The header describes the packet's source, destination and control information. The body contains the data IP is transmitting. TCP detects these problems, requests retransmission of lost data, rearranges out-

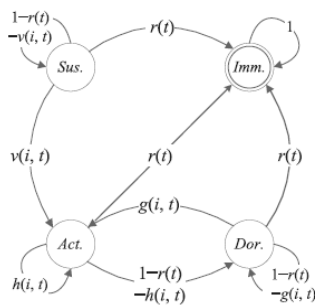
of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. Once the TCP receiver has reassembled the sequence of octets originally transmitted, it passes them to the receiving application. TCP is optimized for accurate delivery rather than timely delivery, and therefore, TCP sometimes incurs relatively long delays (on the order of seconds) while waiting for out-of-order messages or retransmissions of lost messages. TCP is utilized extensively by many of the Internet's most popular applications, File Transfer Protocol, Secure Shell, peer-to-peer file sharing, and some streaming media applications.

4. Implementation Of Sii Model:

SII model is different from SIS and SIR models because both susceptible and infected users can be immunized and never become susceptible again. 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. Let random variable $X_i(t)$ denote the state of a node i at discrete time t . Then, have

$$X_i(t) = \begin{cases} \text{Hea., healthy} & \begin{cases} \text{Sus., susceptible} \\ \text{Imm., immunized} \end{cases} \\ \text{Inf., infected} & \begin{cases} \text{Act., active} \\ \text{Dor., dormant.} \end{cases} \end{cases}$$

The state transition graph of an arbitrary node i in an email network. All nodes in networks are initially susceptible. Since infected users will send out malware copies when 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 not infectious, the node of this user transits to the dormant state. Besides, any user can be compromised again even if the user has been infected before. R represent the infection probabilities of an arbitrary node being at the dormant state and the active state as $g(i,t)$ and $h(i,t)$ respectively. Whatever the state an arbitrary node is at, it may transit to the immunized state. The probability of immunization is denoted by $r(t)$. In fact, if the values of $g(i,t)$ and $h(i,t)$ are equal to zero, any infected node i will stay at the dormant state until the user of this node is immunized.

$$\begin{pmatrix} p_{11} & \dots & p_{1M} \\ \vdots & p_{ij} & \vdots \\ p_{M1} & \dots & p_{MM} \end{pmatrix} p_{ij} \in [0, 1],$$

Where in p_{ij} represents the probability of user j visiting a deceptive malware email received from user i . If p_{ij} is equal to zero, it means the email address of user j is not in the contact list of user i . Therefore, the matrix reflects the topology of an email network.

Virtual Nodes:

For modern email malware, recall that a compromised user may send out malware email copies to neighbors every time the user visits those malware hyperlinks or attachments.[5] Malware emails are also sent out when certain events like computer restart are triggered. Thus, at an arbitrary time t , a user may receive multiple malware email copies from an identical neighboring user who has been compromised. In order to represent the repetitious spreading process of the reinfection and the self-start, introduce virtual nodes to present the k^{th} infection caused by infected users opening the k^{th} malware email copy. The node 1, 2, 3 send malware emails to node 4. When the user of node 4 visits those emails, the user gets infected. If the user of node 4 visits two malware emails, node 4 will send malware email copies twice to node 6. If the user of node 4 visits three malware emails, node 4 will send treble malware email copies to node 6. The spreading process of extra malware email copies is equivalent to two virtual nodes sending a malware copy to node 6.

5. Theoretical Justification:

The empirical study has shown our SII model is superior to previous models. To provide the theoretical justification in modeling the spreading mechanism and state transition of the propagation.

Superiority In The Spreading Mechanisms:

Recall that modern email malware has two aggressive spreading mechanisms. The first one is caused by the reinfection: any user can be infected again even if this node has been infected before. The second one is the repetitious spreading process caused by the reinfection and the self-start: any infected user spreads malware email copies every time the user visits malware emails or the infected computer restarts.

Superiority In Modeling State Transitions:

The difference among these models is caused by different considerations on the state transition of nodes. SIS models assume infected nodes become susceptible again after recovery. If infected nodes cannot become susceptible again once they are cured, the models are called SIR models. Considering the propagation of modern email malware, after users

clean their infected computers or become more vigilant against a type of malware, they are unlikely to be infected any more. Therefore, SIS models are not appropriate to model the propagation of modern email malware. SIR models may suit for modern email malware, but the real case is that a susceptible user can be immunized directly without being infected at first. Thus, the state transition of our SII model is similar to SIR model except nodes at the susceptible state can directly transit to the immunized state. In order to exclude the impact of other factors, derive the SIS and SIR models on the basis of the SII model. First, a susceptible user can be immunized in SII model, but not in SIR model. Thus, we can revise equation to obtain an SIR model as in

$$P(X_i(t) = Imm.) = P(X_i(t-1) = Imm.) + r(t) \cdot$$

$$P(X_i(t-1) = Inf.).$$

$$P(X_i(t) = Sus.) = (1 - v(t)) \cdot P(X_i(t-1) = Sus.)$$

$$+ r(t) \cdot P(X_i(t-1) = Inf.).$$

The results of SII model decrease more rapidly than SIR and SIS models. Thus, we cannot use traditional SIS and SIR models to model the propagation of modern email malware.

Conclusion:

The proposed a novel SII model for the propagation of modern email malware. This model is able 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, presented the repetitious spreading processes caused by the reinfection and the self-start. Our model greatly outperforms previous models in terms of estimation accuracy.

REFERENCES

- Fossi, M. and J. Blackbird, 2011. "Symantec Internet Security Threat Report 2010," technical report Symantec Corporation.
- Wood, P. and G. Egan, 2012. "Symantec Internet Security Threat Report 2011," technical report, Symantec Corporation.
- Zou, C.C., D. Towsley and W. Gong, 2007. "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms," IEEE Trans. Dependable and Secure Computing, 4(2): 105-118.
- Chen, Z. and C. Ji, 2005. "Spatial-Temporal Modeling of Malware Propagation in Networks," IEEE Trans. Neural Networks, 16(5): 1291-1303.
- Gao, C., J. Liu and N. Zhong, 2011. "Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis," Knowledge and Information Systems, 27: 253-279.
- Wong, C., S. Bielski, J.M. McCune and C. Wang, 2004. "A Study of Mass-Mailing Worms," Proc. ACM Workshop Rapid Malcode (WORM '04), 1-10.
- Wen, S., W. Zhou, J. Zhang, Y. Xiang, W. Zhou and W. Jia, 2013. "Modeling Propagation Dynamics of Social Network Worms," IEEE Trans. Parallel and Distributed Systems, 24(8): 1633-1643.
-, 1999 Cert, advisory ca-1999-04, Melissa Macro Virus, <http://www.cert.org/advisories/CA-1999-04.html>.
- Cert, Advisory ca-2000-04, Love Letter Worm, <http://www.cert.org/advisories/CA-2000-04.html>, 2000.
- Calzarossa, M. and E. Gelenbe, 2004. Performance Tools and Applications to Networked Systems: Revised Tutorial Lectures. Springer-Verlag.
- Serazzi, G. and S. Zanero, 2003. "Computer Virus Propagation Models," Proc. 11th IEEE/ACM Int'l Conf. Modeling, Analysis and Simulations of Computer and Telecomm. Systems (MASCOTS '03), 1-10.
- Rozenberg, B., E. Guides and Y. Elovici, 2009. "SISR: A New Model for Epidemic Spreading of Electronic Threats," Proc. 12th Int'l Conf. Information Security, 242-249.
-, 2001. Cert, Advisory ca-2001-22, w32/sircam Malicious Code, <http://www.cert.org/advisories/CA-2001-22.html>.
- Cert, Incident Note in-2003-03, w32/sobig.f Worm, <http://www.cert.org/incidentnotes/IN-2003-03.html>, 2003.