ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

INTEGRATED IMPLEMENTATION OF MODELING, PROPAGATION AND DETECTION OF WORMS IN OUTBOX OF ATTACKER

V.B.Anitha*, D.Durai kumar

* M.Tech-Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

Associate Professor &Head , Dept. of Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

ABSTRACT

There are many critical security threats posed in the malware. Modeling their propagation dynamics and detecting the malware are the main essential for prediction of the potential damages. The malwares could cause the computer to be compromised. Malware / worms is modeled and propagated into other computers to compromise those. A new folder virus and shutdown virus are created and their behavior are analyzed and stored in the server. The user is infected in the active state. Once a user node infected it becomes compromised. It starts sending a worm file to rest of its neighbor nodes to which it is attached in the network. There is no sender end filtration of malware worm's .In order to address this in this paper we proposed to scan the content of the mail. After analysis of the behavior of the worms patches are distributed to kill the worms. Finally the sever analyze the data if there is any malware content then they filtered at the sender end itself in order to prevent the penetration of the worms.

KEYWORDS: Network Security, Malware, Modeling, Propagation Dynamics.

INTRODUCTION

The malware cause problem in the recent years. Worms are one of the most potent threats to Network security. Worms are one of the most ill defined concepts. Worms have the unique ability to mimic. They can infect a host and then choose a medium to propagate to a neighboring host. Generally, the intent of the worm is assumed to be malicious. These malicious worms will make the computer as a compromised one. The attacker send a worm file to the victim .The victim believe that it was send by a trusted recipient .When the victim enter in to the worm file and download the file means then the computer become a compromised one and it start to send the worm file to other nodes which it has been in contact . The information like contact lists contained in the victim's machine. Only once one node is infected it will spread out the worm file .If a user starts infecting at the moment they will infect other user system.

They are motivated to provide the analysis of spreading speed and performance of every worms propagation models. The network topology will define how the computers within the network are arranged and connected to each other. It's used to determine the worm propagation and overall spreading scale. The spreading of worms is incredibly fast because they are highly connected in hub. The speed of the worm propagation is measured using mathematical models and they are used to describe the dynamics of the worm propagation. The email user periodically checks their newly arrived messages and is lured to open those which are actually worm copies. The first feature is "newfolder", the infected computer will create a new folder which as folder inside a folder .The second feature is "shutdown", the computer system will automatically shut down while the attacker send the infectious file. The compromised system will be in a susceptible and active state the patches are distributed to make the compromised system to a immunized state. The researcher mainly focuses on the modeling and propagation dynamics of the malware. To reduce and avoid the worm spreading and affecting the computer they should be detected at the sender end itself.

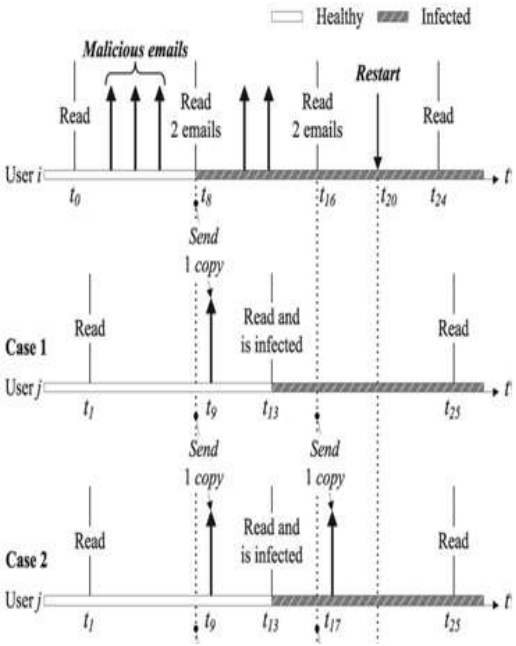
PROBLEM STATEMENT

The propagation of the worms and malware are not the new technique. The compromised user sends the worm file once to the other user. If the user visits or click on the worm file then the system will be a compromised

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

computer system. In the previous models only modeling and propagation is done. In this the new folder and shut down worm mechanisms are modeled and propagated. Then these worm file are detected in the receiver end only. In order to detect the worm file in sender end itself. The newfolder worm indicates that it will create a folder inside a folder. The shutdown worm wills automatically shutdown the compromised system.

Figure

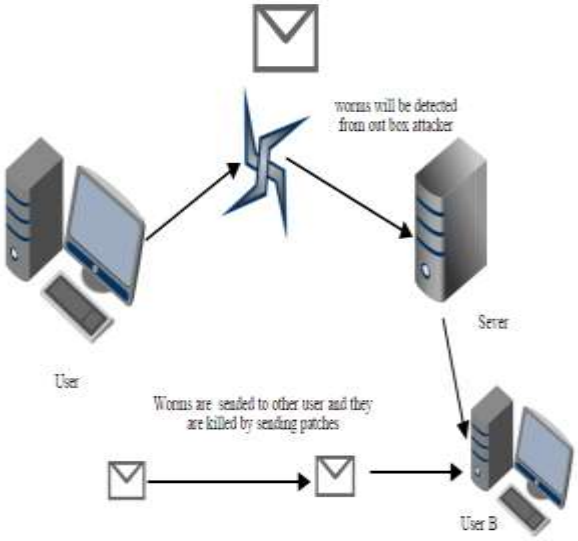


Recipient user j's behavior for different types of malware. User i read two of three malware file at t8 and then restarts at t20. Case 1: New folder; Case 2: shut down malware.

RELATED WORK

SYSTEM MODE

Figure



Architecture for worm propagation and detection

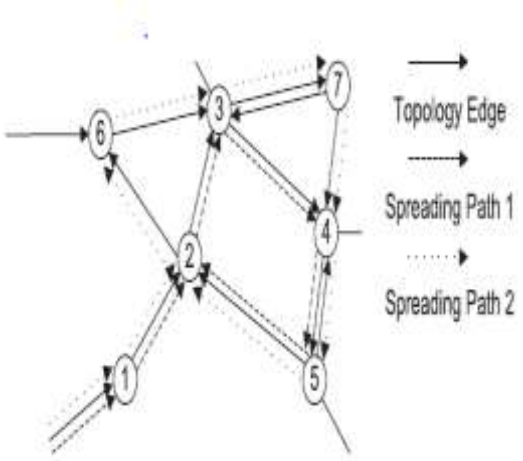
The worm is a program which will self propagated around the network .The worms like shutdown and new folder are created and they are modeled and propagated .The attacker send a malware/worm file to userB .If already the system is a compromised then the sever will send the patches to convert the active state to immunized state .In order to detect the worm in the sender end itself ,the sever checkout the file by content analysis if there are any malware /worm fill in the sender side. Then the sever model the worm and distribute the patches according to the worm behavior so that the worm file will be detected and destroy in sender outbox. According to this penetration of the worms will be avoided.

NETWORK DEPLOYMENT

Nodes are the main elements for modeling and propagation of the malware. These network topologies are created to avoid the security issues. Network has many number of node details. The node in the each topology presents a user in the network.

Figure

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114



Worms spread in a small episode of a network. Paths 1 and 2 are two examples for the propagation in the topology.

The random variable $X_i(t)$ denote the state of a node i at discrete time t. Connection details are maintained. In the network topology there are two states healthy and infected, each and every worms will be in this state they will be converted to the immunized state in the network. Dormant state is that a user is infected but not yet infectious.

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

We propose employing an M by M square matrix with elements pij to describe a topology consisting of M nodes, as in

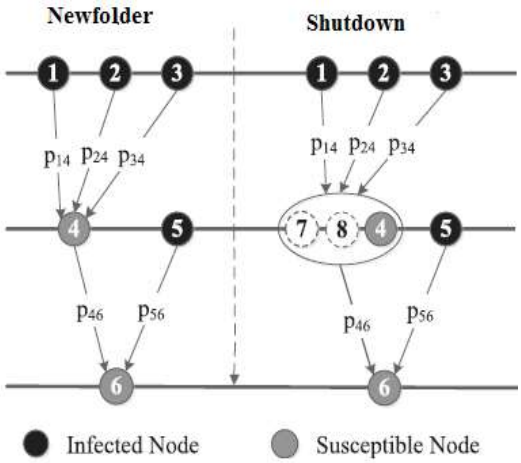
Formulae:

$$\begin{pmatrix} p11 & \cdots & p1M \\ \vdots & \ddots & \vdots \\ pM1 & \cdots & PMM \end{pmatrix} p_{ij\in[0,1]}$$

MODELING OF WORMS

The attacker creates worms file like new folder, shutdown, Bat, Exe .The worm's files which are created are modeled and their behavior are analyzed. The modeling is done by these models like susceptible - infected (SI) models, susceptible-infected-susceptible (SIS) models and susceptible-infected-recovery (SIR) models .The modeling is done in the compromised computer.

Figure



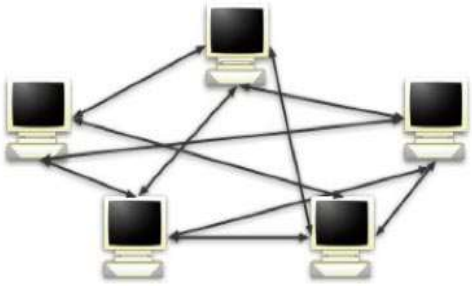
An example to explain nodes in the newfolder case and the shutdown case.

The newfolder worm will create a folder inside a folder. So that there will be more no of folders in the computer. And the second one is shutdown worm will automatically shutdown the compromised system. By the sever will model the behavior of these worm files and store in the sever.

WORMS PROPAGATION

Worms have been widespread because they can travel form one host to another host and network to another network within the contact range. Once the attackers created the worm, they will propagate the worm via network that connected to that system, So that the worm will be spread to other Users Computers. While sending via routing technique like topology-based, small world networks, Random networks.

Figure



Peer-to-Peer Worm Propagation

The User's has to be present within the contact range. The Attacker can send the worm file via Application that was installed in their Computers. And the computer connected with system is compromised so that the worm will easily transfer to the other system

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

and became infectious system .The attacker propagate the worms file to the network which its compromised .After the propagation of the worms the behavior of each and every worms are analysis and prestored in the server.

PATCHES DISTRIBUTION

Once the Server identify worm file was sent to the User's Computer, the Server will provide the patch files to delete the worm file. The patches are created according to each and every worms which has been generated. The patches are small pieces of code created to make the susceptible and active state of system to immunized state. Using an Application the patches will be distributed to the User's Computer automatically to clear the worms. The attacker distribute the worm files into the network .The content of the mail is analysis if there are any spam words in sender outbox then the sever send the patches according to the behavior of the worm file.

AUTOMATIC WORMS DETECTION FROM OUTBOX

Once the attack spread the worm File to other User's Computer the content of the message of the file will be analyzed by the Server to detect whether the file contains that Malicious Behavior or not. The sever maintain a threshold value for the spam words if it exit the range then the sever will consider it as a malicious/worm file, then the server will detect the file as worm file. Once the server detected that the worm file it will not allowed to transfer to receiver end it will be detected and destroy in the sender outbox itself. The detection of worm is done when there is worms\ malware files are present in the sender outbox .The scanning of files are done by the server in the sender outbox.

KILLING WORMS

A worm's data from the sender end itself is filtered. In this, the implementation for both creating of worms and killing of worm is performed. So the worm data is analyzed with pre stored behavior and flittered in the sender end itself in order to prevent worm penetration .The worms which are founded in the sender outbox its killed by sending the patches. By this killing of worms in the sender outbox is done .According to this the penetration of the worm will be avoided.

CONCLUSION

In this we have proposed novel model which can be used to detect the malware worms at sender outbox. In the previous models only the modeling and propagation are done and the detection is done at the receiver end. In this each and every worm is modeled and their behaviors are analyzed and the patches are discovered to kill the worms. The content of the file are scanned in the sender outbox by the content analysis. They maintain a threshold value for every spam word if it exits then the words is considered as a malware worm. Then server transfer the patches to the attacker outbox to destroy it, by this the penetration of worms in the network are avoided.

REFERENCES

1. Cong Jin, Jun Liu, and Qinghua Deng "Network Virus Propagation ModelBased on Effects of Removing Time and User Vigilance"2009.
2. 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.
3. Nuno G. Rodrigues, Ant´onio Nogueira and Paulo Salvador "Fighting Botnets - A Systematic Approach" Instituto de Telecomunicac¸ ˜oes/University of Aveiro Campus de Santiago, 3810-193 Aveiro, Portugal 2012.
4. R. Pastor-Satorras and A. Vespignani, "Epidemic Spreading in Scale-Free Networks," Physical Rev. Letters, vol. 86, pp. 3200-3203,2001.
5. Sheng Wen, Student Member, IEEE, Wei Zhou, Jun Zhang, Member, IEEE,Yang Xiang," Modeling Propagation Dynamics of Social Network Worms" Senior Member, IEEE 2013.
6. Shui Yu, Senior Member, IEEE, Guofei Gu, Member, IEEE, Ahmed Barnawi, Member, IEEE, Song Guo, Senior Member" Malware Propagation in Large-Scale Networks"
7. Stelios Sidiroglou, John Ioannidis, Angelos D. Keromytis, and Salvatore J. Stolfo " An EmailWorm Vaccine Architecture" Department of Computer Science, Columbia University {stelios,ji,angelos,sal}@cs.columbia.edu 2005.
8. Symantec, A-Z Listing of Threats and Risks, http://www. symantec.com/security Response, 2012.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

9. Y. Xiang, X. Fan, and W. Zhu, "Propagation of Active Worms: A Survey," Int'l J. Computer Systems Science and Eng., vol. 24, pp. 157-172, 2009.

10. Yini Wang, Sheng Wen, Yang Xiang, Senior Member, IEEE, and Wanlei Zhou,Senior Member, IEEE,"Modeling the Propagation of Worms in Networks A Survey",201