© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Malware Avoidance Using Two Epidemic Layers

R. Siddarth, T. M. Sounderarajan Mothilal, P. Sathish Saravanan
Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

Malware are malicious software programs deployed by cyber attackers to compromise computer. The solution to this problem is desperately desired by cyber defenders as the network security community does not yet have solid answers. The main scope of our project to investigate how malware propagate in networks from a global perspective. We propose a two layer malware propagation model to describe the development of a given malware at the Internet level. Compared with the existing single layer epidemic models, the proposed model represents malware propagation better in large-scale networks. We propose a two layer malware propagation model to describe the development of a given malware at the Internet level. Compared with the existing single layer epidemic models, the proposed model represents malware propagation better in large-scale networks

Keywords: Malware, Malware Propagation, Two Layers, Power Law, Supervised Classification

I. INTRODUCTION

Malware are malicious software programs deployed by cyber attackers to compromise computer. These Malwares are being created at an alarming rate in order to gain political and financial rewards. These malwares are sent to infect the whole network and gain confidential information.

The systems that are affected by these Malwares are called as bots. The action against these malwares can be taken only when the propagation pattern, the behaviour pattern of the malwares are studied.

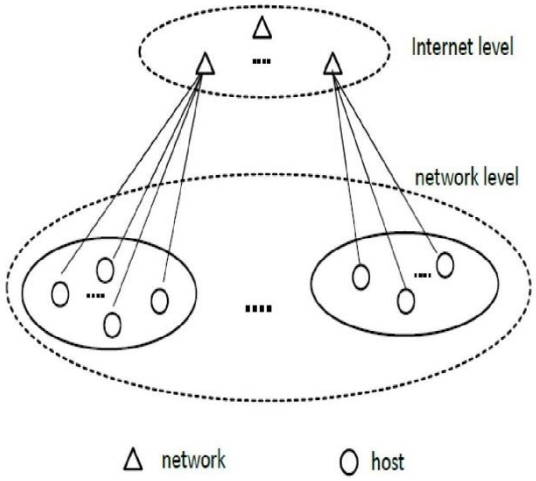

Figure 1: System

We don't have a proper understanding of the size of the Malware, the Bot distribution. Hence, it is very difficult to design a protective system.

The epidemic theory plays a leading role in malware propagation modelling. The current models for malware spread fall in two categories: the epidemiology model and the control theoretic model. The control system theory based models try to detect and contain the spread of malware. One critical condition for the epidemic models is a large vulnerable population because their principle is based on differential equations.

At present, we are using a single epidemic layer for this purpose. This is not very considerable when there is a large network. So now we propose a two layer epidemic model.

This works better as it is capable on focusing on a large scale network. The Upper layer focuses on the large scale network while the lower layer focuses on the hosts of this network. We find the malware distribution in terms of networks varies from exponential to power law with a short exponential tail, and to power law distribution at its early, late, and final stage, respectively.

II. METHODS AND MATERIAL

The Proposed Model

We propose a two layer malware propagation model to describe the development of a given malware at the Internet level. Compared with the existing single layer epidemic models, the proposed model represents malware propagation better in large-scale networks.

The distribution of malware in terms of networks (e.g., autonomous systems, ISP domains, who share the same vulnerabilities) at large scales. In this paper, we use the SI model, which is the simplest for epidemic analysis.

We are proposing a two layer epidemic model technique over the existing single layer epidemic model technique in this paper.

Two layer epidemic model: the upper layer focuses on networks of a large scale networks, for example, domains of the Internet; the lower layer focuses on the hosts of a given network.

We find the malware distribution in terms of networks varies from exponential to power law with a short exponential tail, and to power law distribution at its early, late, and final stage, respectively.

The basic overall system architecture of this model is given below:

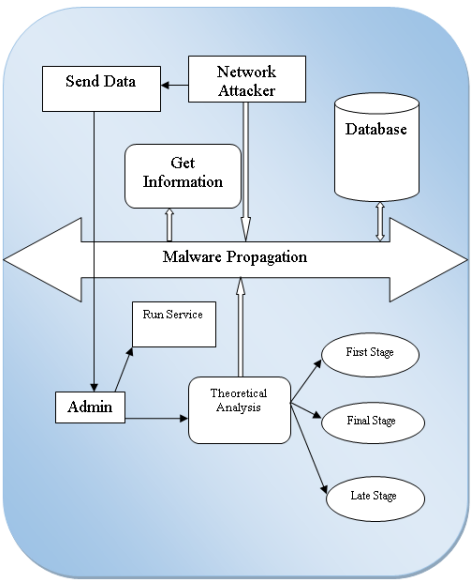

Figure 2: The basic overall architecture

The protectors mentioned in the architecture diagram are normally police squads and night guards.

III. RESULTS AND DISCUSSION

The implementation can be gone through in a stage-wise method as follows.

A. Authentication

If you are the new user or admin going to access their page then they have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.
Network Attacker

In this stage, we compromise as many networked computers in order to achieve our malicious goals. So we are giving some service to the networked computers. By using our service we can get their information here itself.

B. Network Admin

In this stage, we are viewing all requested messages if the service satisfied we are replying to the particular user. Then we will get the service from that user.

C. Malware Propagation

In this module, we are running the service which is getting from the user. Then we will see the performance about the service. At the same time we can see how the service is reducing our system performance.

D. Theoretical Analysis

In this module we are analysing all services, like first stage, final stage, late stage respectively, then we will create the document for reference.

IV. CONCLUSION

We perform a restricted analysis based on the proposed model, and obtain three conclusions:

- The distribution for a given malware in terms of networks follows exponential distribution,
- Power law distribution with a short exponential tail and,
- Power law distribution at its early, late, and final stages.

In order to examine our theoretical findings, we have conducted extensive experiments based on two real-world large-scale malware, and the results confirm our theoretical claims.

V. FUTURE ENHANCEMENT

Our future work will focus on supervise the malware propagation in networks. By using this technique, network user can aware of the malware propagation.

Then admin can view the malware propagation details in graphical format. At the same time admin can permanently block the defender IP address. After blocking the defender can't communicate to anyone. By using this technique we can easily escape from the malware.

VI. REFERENCES

[1] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," in CCS '09: Proceedings of the 2009 ACM conference on computer communication security, 2009.

[2] D. Dagon, C. Zou, andW. Lee, "Modeling botnet propagation using time zones," in Proceedings of the 13 th Network and Distributed System Security Symposium NDSS, 2006.

[3] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging," in Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, 2007.

[4] D. Dagon, C. C. Zou, and W. Lee, "Modeling botnet propagation using time zones," in NDSS, 2006.

[5] A. M. Jeffrey, xiaohua Xia, and I. K. Craig, "When to initiate hiv therapy: A control theoretic approach," IEEE Transactions on Biomedical Engineering, vol. 50, no. 11, pp. 1213–1220, 2003.

[6] R. Dantu, J.W. Cangussu, and S. Patwardhan, "Fast worm containment using feedback control," IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 2, pp. 119–136, 2007.

[7] S. H. Sellke, N. B. Shroff, and S. Bagchi, "Modeling and automated containment of worms," IEEE Trans. Dependable Sec. Comput., vol. 5, no. 2, pp. 71–86, 2008.

[8] P. De, Y. Liu, and S. K. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks," IEEE Trans. Mob. Comput., vol. 8, no. 3, pp. 413–425, 2009.

[9] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms (extended version)," IEEE Trans. Mob. Comput., vol. 8, no. 3, pp. 353–368, 2009.

[10] C. C. Zou, W. Gong, D. Towsley, and L. Gao, "The monitoring and early detection of internet worms," IEEE/ACM Trans. Netw., vol. 13, no. 5, pp. 961–974, 2005.