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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Malware Distribution in Large Scale Network

Dhende Kapil N, Prof. Bere S.S

PG Scholar, Dept. of Computer Engineering, DGOIFOE, Bhigwan, Pune, India

Dept. of computer Engineering, DGOIFOE, Bhigwan, Pune, India

ABSTRACT: Malware is a 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 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 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.

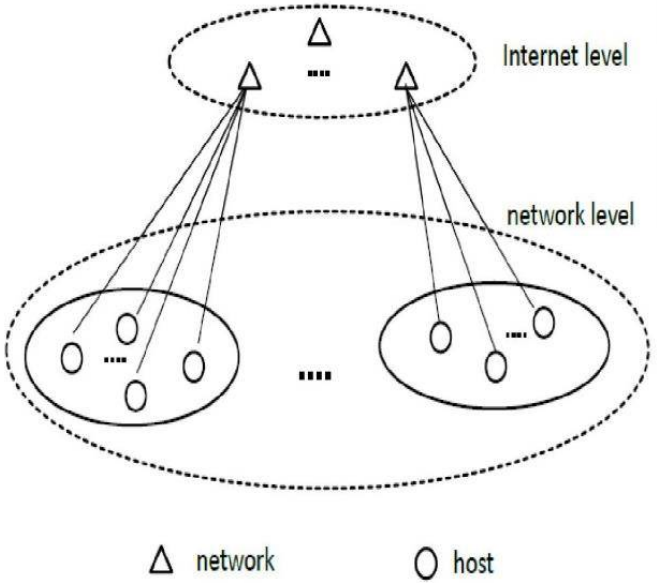

Fig: System Architecture

The epidemic theory plays a leading role in malware propagation modeling. 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

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. RELATED WORK

Time zones play an important and unexplored role in malware epidemics. To understand how time and location affect malware spread dynamics, we studied botnets, or large coordinated collections of victim machines (zombies) controlled by attackers. Over a six month period we observed dozens of botnets representing millions of victims. We noted diurnal properties in botnet activity, which we suspect occurs because victims turn their computers off at night. Through binary analysis, we also confirmed that some botnets demonstrated a bias in infecting regional populations. Clearly, computers that are offline are not infectious, and any regional bias in infections will affect the overall growth of the botnet. We therefore created a diurnal propagation model. The model uses diurnal shaping functions to capture regional variations in online vulnerable populations. The diurnal model also lets one compare propagation rates for different botnets, and prioritize response. Because of variations in release times and diurnal shaping functions particular to an infection, botnets released later in time may actually surpass other botnets that have an advanced start. Since response times for malware outbreaks is now measured in hours, being able to predict short-term propagation dynamics lets us allocate resources more intelligently. We used empirical data from botnets to evaluate the analytical model.
The popularity and adoption of smart phones has greatly stimulated the spread of mobile malware, especially on the popular platforms such as Android. In light of their rapid growth, there is a pressing need to develop effective solutions. However, our defense capability is largely constrained by the limited understanding of these emerging mobile malware and the lack of timely access to related samples. In this paper, we focus on the Android platform and aim to systematize or characterize existing Android malware. Particularly, with more than one year effort, we have managed to collect more than 1,200 malware samples that cover the majority of existing Android malware families, ranging from their debut in August 2010 to recent ones in October 2011. In addition, we systematically characterize them from various aspects, including their installation methods, activation mechanisms as well as the nature of carried malicious payloads. The characterization and a subsequent evolution-based study of representative families reveal that they are evolving rapidly to circumvent the detection from existing mobile anti-virus software. Based on the evaluation with four representative mobile security software, our experiments show that the best case detects 79.6% of them while the worst case detects only 20.2% in our dataset. These results clearly call for the need to better develop next-generation anti-mobile-malware solutions.
Security breaches and attacks are critical problems in today's networking. A key-point is that the security of each host depends not only on the protection strategies it chooses to adopt but also on those chosen by other hosts in the network. The spread of Internet worms and viruses is only one example. This class of problems has two aspects. First, it deals with epidemic processes, and as such calls for the employment of epidemic theory. Second, the distributed and autonomous nature of decision-making in major classes of networks (e.g., P2P, ad- hoc, and most notably the Internet) call for the employment of game theoretical approaches. Accordingly, we propose a unified framework that combines the N-intertwined, SIS epidemic model with a no cooperative game model. We determine the existence of Nash equilibrium of the respective game and characterize its properties. We show that its quality, in terms of overall network security, largely depends on the underlying topology. We then provide a bound on the level of system inefficiency due to the no cooperative behaviour, namely, the "price of anarchy" of the game. We observe that the price of anarchy may be prohibitively high; hence we propose a scheme for steering users towards socially efficient behaviour.
When the probability of measuring a particular value of some quantity varies inversely as a power of that value, the quantity is said to follow a power law, also known variously as Zipf's law or the Pareto distribution. Power laws appear widely in physics, biology, earth and planetary sciences, economics and finance, computer science, demography and the social sciences. For instance, the distributions of the sizes of cities, earthquakes, solar flares, moon craters, wars and people's personal fortunes all appear to follow power laws. The origin of power-law behavior has been a topic of

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

debate in the scientific community for more than a century. Here we review some of the empirical evidence for the existence of power-law forms and the theories proposed to explain them.
Many network phenomena are well modeled as spreads of epidemics through a network. Prominent examples include the spread of worms and email viruses, and, more generally, faults. Many types of information dissemination can also be modeled as spreads of epidemics. In this paper we address the question of what makes an epidemic either weak or potent. More precisely, we identify topological properties of the graph that determine the persistence of epidemics. In particular, we show that if the ratio of cure to infection rates is larger than the spectral radius of the graph, then the mean epidemic lifetime is of order log n, where n is the number of nodes. Conversely, if this ratio is smaller than a generalization of the isoperimetric constant of the graph, then the mean epidemic lifetime is of order ena, for a positive constant a. We apply these results to several network topologies including the hypercube, which is a representative connectivity graph for a distributed hash table, the complete graph, which is an important connectivity graph for BGP, and the power law graph, of which the AS-level Internet graph is a prime example. We also study the star topology and the Erdos-Renyi graph as their epidemic spreading behaviors determine the spreading behavior of power law graph.

III. SYSTEM ARCHITECTURE

Malware propagation modeling has been extensively explored. proposed a number of models for malware monitoring at the early stage. They pointed out that these kinds of model are appropriate for a system that consists of a large number of vulnerable hosts; in other words, the model is effective at the early stage of the outbreak of malware, and the accuracy of the model drops when the malware develops further. As a variant of the epidemic category, Sellke, Shroff and Bagchi proposed a stochastic branching process model for characterizing the propagation of Internet worms, which especially focuses on the number of compromised computers against the number of worm scans, and presented a closed form expression for the relationship.

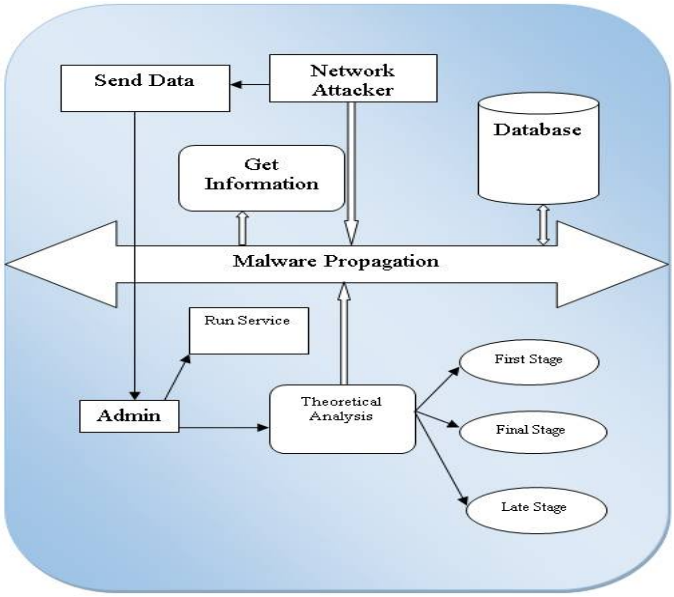

Fig 1: System Architecture

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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IV. MODULE

Network Formation:
Research on complex networks has demonstrated that the number of hosts of networks follows the power law. People found that the size distribution usually follows the power law, such as population in cities in a country or personal income in a nation

Malware Propagation:

1) **Early stage:** An early stage of the breakout of a malware means only a small percentage of vulnerable hosts have been compromised, and the propagation follows exponential distributions.
2) **Final stage:** The final stage of the propagation of a malware means that all vulnerable hosts of a given network have been compromised.
3) **Late stage:** A late stage means the time interval between the early stage and the final stage.

Filtering Malware Detection:
Distribution of coexist multiple malware in networks. In reality, multiple malware may coexist at the same networks. Due to the fact that different malware focus on different vulnerabilities, the distributions of different malware should not be the same. It is challenging and interesting to establish mathematical models for multiple malware distribution in terms of networks. The two layers in both layers are sufficiently large and meet the conditions for the modelling methods. In order to improve the accuracy of malware propagation, we may extend our work to layers. In another scenario, we may expect to model a malware distribution for middle size networks

Performance Evaluation:
We have to note that our experiments also indicate that this data does not fit the power law. For a given Android malware program, it only focuses on one or a number of specific vulnerabilities. Therefore, all smartphones share these vulnerabilities form a specific network for that Android malware.

Advantage:
Our rigorous analysis, we find that the distribution of a given malware follows an exponential distribution at its early stage, and obeys a power law distribution with a short exponential tail at its late stage, and finally converges to a power law distribution.

V. EXPERIMENTAL RESULT

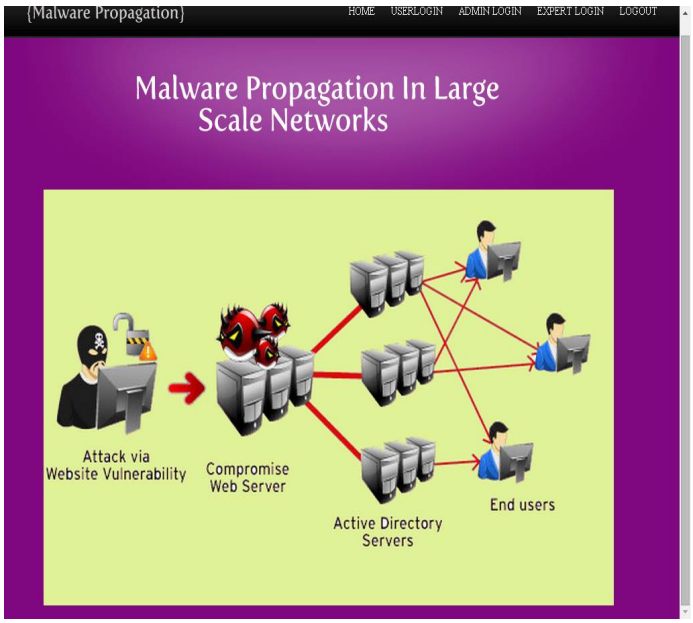

Fig 3: Home Page

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Fig 4: Admin Login

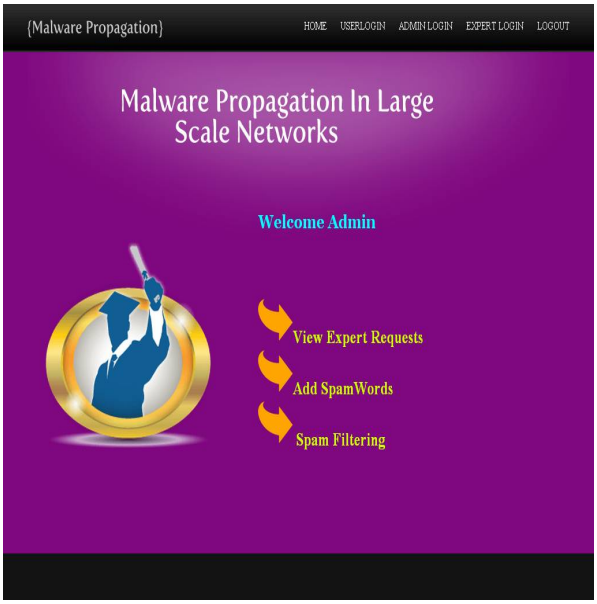

Fig 5: Admin Activity

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Fig 6: User Registration

Fig 7: User Activity

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

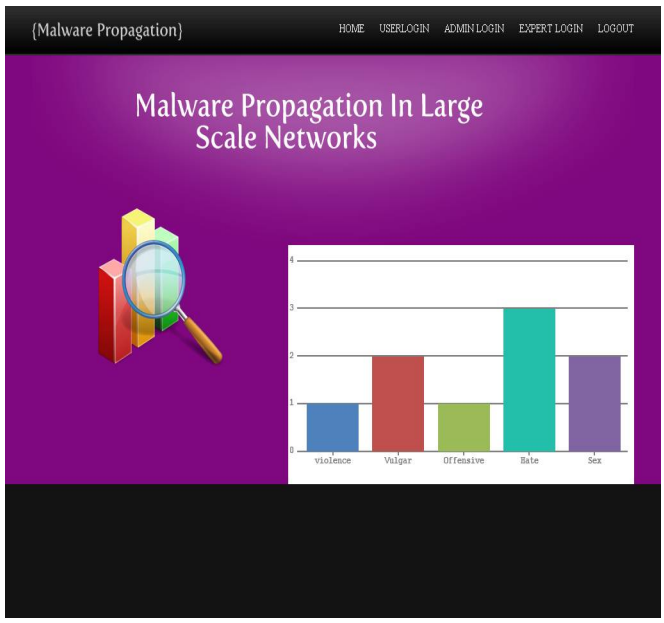

Fig 8: Result

VI. CONCLUSION

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 stage, respectively. 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.

ACKNOWLEDGMENT

I want to thank all people who help me in different way. Especially I am thankful to my guide "**Prof. Bere S.S**" for him continuous support and guidance in my work. Also, I would like thank our PG coordinator **"Prof. Priyadarshi Amrit"**.Lastly, I thank to "**CPGCON-16"** who have given opportunity to present my paper.

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] P. V. Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," IEEE/ACM Transactions on Networking, vol. 17, no. 1, pp. 1–14, 2009.
[6] Cabir, http://www.f-secure.com/en/web/labs global/2004- threat-summary.
[7] Ikee, http://www.f-secure.com/vdescs/worm iphoneos ikee b.shtml.
[8] Brador, http://www.f-secure.com/v-descs/brador.shtml.
[9] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," IEEE Communications Surveys and Tutorials, in press, 2014.
[10] Z. Chen and C. Ji, "An information-theoretic view of network-aware malware attacks," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 530–541, 2009.
[11] 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," IEEE Trans. Mob. Comput., vol. 12, no. 3, pp. 529–541, 2013.
[18] D. J. Daley and J. Gani, Epidemic Modelling: An Introduction. Cambridge University, 1999.
[19] W. Willinger, D. Alderson, and J. C. Doyle, "Mathematics and the internet: A source of enormous confusion and great potential," Notices of the Ameriacan Mathematical Socieity, vol. 56, no. 5, pp. 586–599, 2009.
[20] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in IEEE Symposium on Security and Privacy, 2012, pp. 95–109.
[21] S. Shin, G. Gu, A. L. N. Reddy, and C. P. Lee, "A largescale empirical study of conficker," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 676–690, 2012.
[22] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in Internet Measurement Conference, 2006, pp. 41–52.
[23] A. J. Ganesh, L. Massouli´e, and D. F. Towsley, "The effect of network topology on the spread of epidemics," in INFOCOM, 2005, pp. 1455–1466.
[24] J. Omic, A. Orda, and P. V. Mieghem, "Protecting against network infections: A game theoretic perspective," in INFOCOM'09, 2009.
[25] R. L. Axtell, "Zipf distribution of u.s. firm sizes," Science, vol. 293, 2001.
[26] M. Mitzenmacher, "A brief history of generative models for power law and lognornal distributions," Internet Mathematics, vol. 1, 2004.
[27] M. Newman, Networks, An Introduction. Oxford University Press, 2010.
[28] Z. K. Silagadze, "Citations and the zipf-mandelbrot's law," Complex Systems, vol. 11, pp. 487–499, 1997.
[29] M. E. J. Newman, "Power laws, pareto distributions and zipf's law," Contemporary Physics, vol. 46, pp. 323–351, December 2005.
[30] L. Kleinrock, Queueing Systems. Wiley Interscience, 1975, vol