International Journal of Applied Sciences, Engineering and Management
ISSN 2320 – 3439, Vol. 07, No. 06, November 2018, pp. 52-57

Malware Prevention using Two Layers Protection

Tangellapalli Madhuri[1], K. Raghu[2]
[1]PG Scholar, Nova's Institute of Technology, Eluru Andhra Pradesh, India.
[2]Asst.Professor, Nova's Institute of Technology, Eluru Andhra Pradesh, India.
Email: *madhucse547@gmail.com, kraghu@gmail.com*

Abstract: Malware is pervasive in networks, and poses a critical threat to network security. However, we have very limited understanding of malware behavior in networks to date. In this paper, we investigate how malware propagates in networks from a global perspective. We formulate the problem, and establish a rigorous two layer epidemic model for malware propagation from network to network. We formulate the problem, and establish a rigorous two layer epidemic model for malware propagation from network to network. Based on the proposed model, our analysis indicates that the distribution of a given malware follows exponential distribution, power law distribution with a short exponential tail, and power law distribution at its early, late and final stages, respectively. 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, Modeling, Power law, Epidemic Model*

Introduction

Malware are malicious software programs deployed by cyber attackers to compromise computer systems by exploiting their security vulnerabilities. Motivated by extraordinary financial or political rewards, malware owners are exhausting their energy to compromise as many networked computers as they can in order to achieve their malicious goals. 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.

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 models is a large vulnerable population because their principle is based on differential equations.

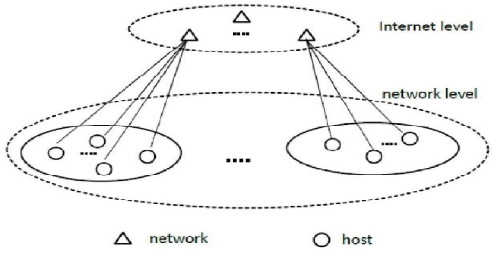

Fig-1: System Architecture

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. gathering protocols. It uses a chain structure.

The goal is to develop a routing structure and an aggregation scheme to reduce energy consumption and deliver the aggregated data to the base station with minimal delay while balancing energy consumption among the sensor nodes. The simulation results of the hierarchical extension of PEGASIS show the

improvement over schemes such as LEACH. HEED (Hybrid Energy-Efficient Distributed clustering), it selects cluster heads depending on node residual energy. It achieves uniform cluster head distribution over the network. HEED almost guarantee connectivity of clustered among the wireless sensor networks. The cluster heads utilize the spatio-temporal correlation to minimize the readings for energy saving. However, traditional single-head clustering schemes may not be suitable with MU-MIMO. So this paper proposes a load-balanced multi-head clustering algorithm to maximize the network lifetime

Literature Survey

"Modeling botnet propagation using time zones,". D. Dagon, C. Zou, andW. Lee
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.

"Dissecting android malware: Characterization and evolution,". Y. Zhou and X. Jiang
The popularity and adoption of smart phones has greatly stimulated the spread of mobile malware, especially on thepopular 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 malwareand 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 evolvingrapidly 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 antimobile malware solutions.

Protecting against network infections: A game theoretic perspective,". J. Omic, A. Orda, and P. V. Mieghem
Security breaches and attacks are critical problems in today's networking. A key-point is that the security of each hostdepends 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 dealswith epidemic processes, and as such calls for the employment of epidemic theory. Second, the distributed andautonomous 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 combinesthe 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.

"Power laws, pareto distributions and zipf's law,". M. E. J. Newman,
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 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.

Related Work

The basic story of malware is as follows. A malware programmer writes a program, called bot or agent, and then installs the bots at compromised computers on the Internet using various network virus-like techniques. All of his bots form a botnet, which is controlled by its owners to commit illegal tasks, such as launching DDoS attacks, sending spam emails, performing phishing activities, and collecting sensitive information. There is a command and control (C&C) server(s) to communicate with the bots and collect data from bots. In order to disguise himself from legal forces, the botmaster changes the url of his C&C frequently, e.g., weekly. An excellent explanation about this can be found in [1]. With the significant growing of smartphones, we have witnessed an increasing number of mobile malware. Malware writers have develop many mobile malware in recent years. Cabir [5] was developed in 2004, and was the first malware targeting on the Symbian operating system for mobile devices. Moreover, it was also the first malware propagating via Bluetooth. Ikee [6] was the first mobile malware against Apple iPhones, while Brador [7] was developed against Windows CE operating systems.

The attack victors for mobile malware are diverse, such as SMS, MMS, Bluetooth, WiFi, and Web browsing. Peng et al. [8] presented the short history of mobile malware since 2004, and surveyed their propagation models.A direct method to count the number of bots is to use botnet infiltration to count the bot IDs or IP addresses. Stone- Gross et al. [1] registered the URL of the Torpig botnet before the botmaster, and therefore were able to hijack the C&C server for ten days, and collect about 70G data from the bots of the Torpig botnet. They reported that the footprint of the Torpig botnet was 182,800, and the median and average size of the Torpig's live population was 49,272 and 48,532, respectively. They found 49,294 new infections during the ten days takeover. Their research also indicated that the live population fluctuates periodically as users switch between being online and offline. This issue was also tacked by Dagon et al. in [3].

Another method is to use DNS redirection. Dagon et al. [3] analyzed captured bots by honypot, and then identified the C&C server using source code reverse engineering tools. They then manipulated the DNS entry which is related to a botnet's IRC server, and redirected the DNS requests to a local sinkhole. They therefore could count the number of bots in the botnet. As discussed previously, their method counts the footprint of the botnet, whichwas 350,000 in their report. In this paper, we use two large scale malware data sets for our experiments. Conficker is a well-known and one of the most recently widespread malware. Shin et al. [20] collected a data set about 25 million Conficker victims from all over the world at different levels. At the same time, malware targeting on Android based mobile systems are developing quickly in recent years. Zhou and Jiang [19] collected a large data set of Android based malware. In [2], Rajab et al.pointed out that it is inaccurate to count the unique IP addresses of bots because DHCP and NAT techniques are employed extensively on the Internet ([1] confirms this by their observation that 78.9 percent of the infected machines were behind a NAT, VPN, proxy, or firewall). They therefore proposed to examine the hits of DNS caches to find the lower bound of the size of a given botnet.

Proposed Work

In this paper, we study the distribution of malware in terms of networks (e.g., autonomous systems, ISP domains, and abstract net-works of smartphones who share the same vulnerabilities) at large scales. In this kind of setting, we have a sufficient volume of data at a large enough scale to meet the requirements of the SI model. Different from the traditional epidemic models, we break our model into two layers. First of all, for a given time since the breakout of amalware, we calculate how many networks have been compromised based on the SI model. Secondly, for acompromised net-work, we calculate how many hosts have been compromised since the time that the network was compromised.

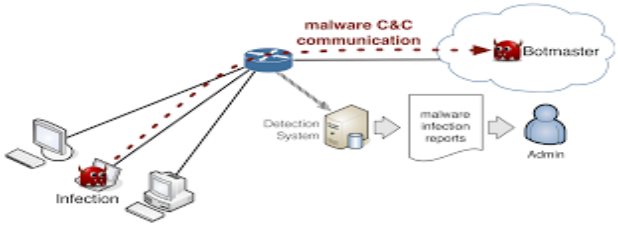

Fig-2: System Architecture of Proposed System.

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

a) 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.
b) Final stage: The final stage of the propagation of a malware means that all vulnerable hosts of a given network have been compromised.
c) 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.
a. 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.

Proposed System

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. In regards to future work, we will first further investigate the dynamics of the late stage. More details of the findings are expected to be further studied, such as the length of the exponential tail of a power law distribution at the late stage. Second, defenders may care more about their own network, e.g., the distribution of a given malware at their ISP domains, where the conditions for the two layer model may not hold. We need to seek appropriate models to address this problem. Finally, we are interested in studying the distribution of multiple malware on large-scale networks as we only focus on one malware in this paper. We believe it is not a simple linear relationship in the multiple malware case compared to the single malware one.

Result and Discussions

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

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.

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.

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.

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

Conclusion

In this paper, we thoroughly explore the problem of malware distribution at large-scale networks. The solution to this problem is desperately desired by cyber defenders as the network security community does not yet have solid answers. Different from previous modeling methods, we propose a 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. This two layer model improves the accuracy compared with the available single layer epidemic models in malware modelling. Moreover, the proposed two layer model offers us the distribution of malware in terms of the low layer networks. 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 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.

Reference

[1] 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] S. Peng, S. Yu, and A. Yang, “Smartphone malware and its propagation modeling: A survey,” IEEE Communications Surveys and Tutorials, in press, 2014.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] P. De, Y. Liu, and S. K. Das, “An epidemic theoretic framework for vulnerability analysis of broadcast protocolsin wireless sensor networks,” IEEE Trans. Mob. Comput., vol. 8, no. 3, pp. 413–425, 2009.
[13] 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.