ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Approach for Malware Extension in LSN

B.Komali, MCA
Lecturer,
Dept of Computer Science,
Sri Durga Malleswara Siddhartha Mahila kalasala,
Vijayawada, A.P., India.

R.Aruna, MCA
Lecturer,
Dept of Computer Science,
P.B.Siddhartha College of Arts and Science,
Vijayawada , A.P., India.

Abstract:
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 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. 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:
Large-Scale Networks, Susceptible-Infected (SI), Malware Propagation, Modelling, security.

I. INTRODUCTION:

Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Reign, or it may be designed to cause harm, often as sabotage (e.g., Stunt), or to extort payment (CryptoLocker). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software,] including computer viruses, worms, trojanhorses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. Malware is often disguised as, or embedded in, non-malicious files. Spyware or other malware is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics. An example of such software, which was described as illegitimate, is the Sony rootkit, a Trojan embedded into CDs sold by Sony, which silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying; it also reported on users' listening habits, and unintentionally created vulnerabilities that were exploited by unrelated malware.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Malware authors target bugs, or loopholes, to exploit. A common method is exploitation of a buffer overrun vulnerability, where software designed to store data in a specified region of memory does not prevent more data than the buffer can accommodate being supplied. Malware may provide data that overflows the buffer, with malicious executable code or data after the end; when this payload is accessed it does what the attacker, not the legitimate software, determines. Early PCs had to be booted from floppy disks; when built-in hard drives became common the operating system was normally started from them, but it was possible to boot from another boot device if available, such as a floppy disk, CD-ROM, DVD-ROM, or USB flash drive. It was common to configure the computer to boot from one of these devices when available. Normally none would be available; the user would intentionally insert, say, a CD into the optical drive to boot the computer in some special way, for example to install an operating system. Even without booting, computers can be configured to execute software on some media as soon as they become available, e.g. to auto run a CD or USB device when inserted.

II. PROBLEM STATEMENT:

EXISTING 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. The epidemiology models are more focused on the number of compromised hosts and their distributions, and they have been explored extensively in the computer science community.
- Zou et al. used a susceptible-infected (SI) model to predict the growth of Internet worms at the early stage.
- Gao and Liu recently employed a susceptible-infected-recovered (SIR) model to describe mobile virus propagation.

DISADVANTAGES OF EXISTING SYSTEM:

- One critical condition for the epidemic models is a large vulnerable population because their principle is based on differential equations.
- As pointed by Willinger et al. the findings, which we extract from a set of observed data, usually reflect parts of the studied objects. It is more reliable to extract the-oretical results from appropriate models with confirmation from sufficient real world data set experiments.

PROPOSED SYSTEM:

- In this paper, we study the distribution of malware in terms of networks (e.g., autonomous systems, ISP domains, and abstract networks 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 a malware, we calculate how many networks have been compromised based on the SI model.
- Secondly, for a compromised net-work, we calculate how many hosts have been compromised since the time that the network was compromised.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ 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.

III. RELATED WORK:

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-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

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.

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 .

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.

IV. LITERATURE REVIEW:

1) Information-theoretic view of network aware malware attacks

Smartphones are pervasively used in society, and have been both the target and victim of malware writers. Motivated by the significant threat that presents to legitimate users, we survey the current smartphone

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

malware status and their propagation models. The content of this paper is presented in two parts. In the first part, we review the short history of mobile malware evolution since 2004, and then list the classes of mobile malware and their infection vectors. At the end of the first part, we enumerate the possible damage caused by smartphone malware. In the second part, we focus on smartphone malware propagation modeling. In order to understand the propagation behavior of smartphone malware, we recall generic epidemic models as a foundation for further exploration. We then extensively survey the smartphone malware propagation models.

Disadvantage:

It only discusses the behavior of malwares.

2) Modeling and automated containment of worms

Self-propagating codes, called worms, such as Code Red, Nimda, and Slammer, have drawn significant attention due to their enormously adverse impact on the Internet. Thus, there is great interest in the research community in modeling the spread of worms and in providing adequate defense mechanisms against them. In this paper, we present a (stochastic) branching process model for characterizing the propagation of Internet worms. The model is developed for uniform scanning worms and then extended to preference scanning worms. This model leads to the development of an containment strategy that prevents the spread of a worm beyond its early stage. Specifically, for uniform scanning worms, we are able to 1) provide a precise condition that determines whether the worm spread will eventually stop and 2) obtain the distribution of the total number of hosts that the worminfects. We then extend our results to contain preference scanning worms. Our strategy is based on limiting the number of scans to dark-address space. The limiting value is determined by our analysis. Our automatic worm containment schemes effectively contain both uniform scanning worms and local preference scanning worms, and it is validated through simulations and real trace data to be nonintrusive.

Disadvantage:

- It is not possible to prevent undesired messages. No matter user who propose them.

3) An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks

While multi-hop broadcast protocols, such as Trickle, Deluge and MNP, have gained tremendous popularity as a means for fast and convenient propagation of data/code in large scale wireless sensor networks, they can, unfortunately, serve as potential platforms for virus spreading if the security is breached. To understand the vulnerability of such protocols and design defense mechanisms against piggy-backed virus attacks, it is critical to investigate the propagation process of these protocols in terms of their speed and reachability. In this paper, we propose a general framework based on the principles of epidemic theory, for vulnerability analysis of current broadcast protocols in wireless sensornetworks . In particular, we develop a common mathematical model for the propagation that incorporates important parameters derived from the communication patterns of the protocol under test. Based on this model, we analyze the propagation rate and the extent of spread of a malware over typical broadcast protocols proposed in the literature. The overall result is an approximate but convenient tool to characterize a broadcast protocol in terms of its vulnerability to malware propagation.

Disadvantage:

- It use the access control techniques to block Malware.

4) A large-scale empirical study of conficker:

Conficker is the most recent widespread, well-known worm/bot. According to several reports, it has infected about 7 million to 15 million hosts and the victims are still increasing even now. In this paper, we analyze Conficker infections at a large scale, about 25 million victims, and study various interesting aspects about this state-of-the-art malware.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

By analyzing Conficker, we intend to understand current and new trends in malware propagation, which could be very helpful in predicting future malware trends and providing insights for future malware defense. We observe that Conficker has some very different victim distribution patterns compared to many previous generation worms/botnets, suggesting that new malware spreading models and defense strategies are likely needed. We measure the potential power of Conficker to estimate its effects on the networks/hosts when it performs malicious operations. Furthermore, we intend to determine how well a reputation-based blacklisting approach can perform when faced with new malware threats such as Conficker.

We cross-check several DNS blacklists and IP/AS reputation data from Dshield and FIRE and our evaluation shows that unlike a previous study which shows that a blacklist-based approach can detect most bots, these reputation-based approaches did relatively poorly for Conficker. This raises a question of how we can improve and complement existing reputation-based techniques to prepare for future malware defense? Based on this, we look into some insights for defenders. We show that neighborhood watch is a surprisingly effective approach in the case of Conficker.

Disadvantage:

- Providing this service is not only a matter of using previously defined web content mining techniques for a different application, rather it requires to design ad-hoc classification strategies.

CONCLUSION & FUTURE SCOPE:

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 modelling 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. 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.

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 Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 635–647.

[2] 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 Proc. 1st Conf. 1st Workshop Hot Topics Understanding Botnets, 2007, p. 5.

[3] D. Dagon, C. Zou, and W. Lee, “Modeling botnet propagation using time zones,” in Proc. 13th Netw. Distrib. Syst. Security Symp., 2006.

[4] P. V. Mieghem, J. Omic, and R. Kooij, “Virus spread in networks,” IEEE/ACM Trans. Netw., vol. 17, no. 1, pp. 1–14, Feb. 2009.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[5] Cabir. (2014). [Online]. Available: http://www.f-secure.com/en/ web/labs_global/2004-threat-summary.

[6] Ikee (2014) [Online] Available: http://www.f-secure.com/vdescs/ worm_iphoneos_ikee_b.shtml

[7] Brador. (2014). [Online]. Available: http://www.f-secure.com/vdescs/
brador.shtml

[8] 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, Oct. 2005.

[9] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," IEEE Trans. Mobile Comput., vol. 12, no. 3, pp. 529–541, Mar. 2013.

[10] D. J. Daley and J. Gani, Epidemic Modelling: An Introduction. Cambridge, U.K. Cambridge Univ. Press, 1999.

[11] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 2, pp. 925–941, 2014.