IJDCST @Jan-2015, Issue- V-3, I-2, SW-30
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Modelling and Security with Malware Extension in Large Scale Networks

P.B.V.N.Prasad[1], G.Jameson[2], K.Rambabu[3]

[1]Associate Professor, Dept. of Computer Science & Engineering, MVR College of Engineering & Technology, A.P., India.

[2]Assistant Professor, Dept. of Computer Science & Engineering, MVR College of Engineering & Technology, A.P., India.

[3]Assistant Professor, Dept. of Computer Science & Engineering, MVR College of Engineering & Technology, A.P., India.

Abstract — 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. Malware is pervasive in networks, and poses a critical threat to network security. However, we have very limited understanding of malware behaviour 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. A compromised computer is called a bot, and all bots compromised by a malware form a botnet. Botnets have become the attack engine of cyber attackers, and they pose critical challenges to cyber defenders. In order to fight against cyber criminals, it is important for defenders to understand malware behavior, such as propagation or membership recruitment patterns, the size of botnets, and distribution of bots. 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.

Keywords — ***Large-Scale Networks, Malware Propagation, modelling, security.***

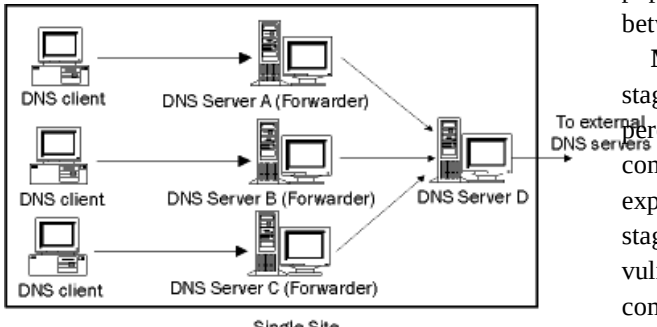
I. INTRODUCTION

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. 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. 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

In this paper ,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.



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-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

Y. Zhou and X. Jiang : **"Dissecting android malware: Characterization and evolution":**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 antimobile-malware solutions.

K Ramachandran, B Sikdar… "Modeling malware propagation in Gnutella type peer to peer networks Parallel and Distributed": A key emerging and popular communication model mostly invented for getting information which is peer-topeer (P2P) networking. To spread of malware in decentralized Gnutella type of peer-to-peer network is needed. The study reveals that the existing bound on the spectral radius governing the possibility of an epidemic outbreak needs to be revised in the context of a P2P network. To formulate an analytical model that reveals the study of mechanics and decentralized Gnutella type of peer network and study the spread of malware on such networks. The show analytically, that a framework which does not incorporate the behavioral characteristics of peers. This in turn results in negatives, an undesirable feature. Thus differentiating the conditions under which the network may reach a malware free equilibrium and validate the theoretical results with numerical simulations.

S Shin, G Gu, N Reddy, CP Lee.A Large Scale Empirical study of conficker". If analyze Conficker infections at a large scale, about 25 million victims, and study various interesting aspects about this state-of-the-art malware. By analyzing Conflicker, the 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. On observing that the Conflicker 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.If measure the potential power of Conficker to estimate its effects on the networks when it performs malicious operations.

V.CONCLUSION

In this paper, malicious nodes may inject some dummy signatures targeting no malware into the network and induce denial-of-service attacks to the defense system. Therefore, security and authentication mechanisms should be considered. From the aspect of malware, since some sophisticated malware that can bypass the signature detection would emerge with the development of the defense system, new defense mechanisms will be required. To studying the distribution of multiple malware on large-scale networks such as only focus on one malware in this paper. It is not a simple linear relationship in the multiple malware.

REFERENCES

[1] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in IEEE Symposium on Security and Privacy, 2012, pp. 95–109.

[2] 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.

[3] 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.

[4] 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.

[5] J. Omic, A. Orda, and P. V. Mieghem, "Protecting against network infections: A game theoretic perspective," in INFOCOM'09, 2009.

[6] R. L. Axtell, "Zipf distribution of u.s. firm sizes," Science, vol. 293, 2001.

[7] M. Mitzenmacher, "A brief history of generative models for power law and lognornal distributions," Internet Mathematics, vol. 1, 2004. [8] M. Newman, Networks, An Introduction. Oxford University Press, 2010.

[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] " A Large Scale Empirical study of conficker" S Shin, G Gu, N Reddy, CP Lee.., volume pp no 3…, IEEE year 2012.