ASURVEY ON MODELING AND DETECTION OF CAMOUFLAGING WORM

M.Nandhini
Department of Computer Science
Pondicherry University, Puducherry

INTRODUCTION

A worm is "a program that propagates itself over a network, reproducing itself as it goes." Unlike viruses, which have to attach themselves to a particular program, like an email client, worms are self contained. An active worm refers to a malicious software program that propagates itself on the Internet to infect other computers. The propagation of the worm is based on exploiting vulnerabilities of computers on the Internet. Many real-world worms have caused notable damage on the Internet. These worms include "Code-Red" worm in 2001, "Slammer" worm in 2003, and "Witty"/"Sasser" worms in 2004.

Many active worms are used to infect a large number of computers and recruit them as bots or zombies, which are networked together to form botnets. These botnets can be used to: (a) launch massive Distributed Denial-of-Service (*DDoS*) attacks that disrupt the Internet utilities (b) access confidential information that can be misused, through large scale traffic sniffing, key logging, identity theft etc (c) destroy data that has a high monetary value (d) distribute large-scale unsolicited advertisement emails (as spam) or software (as malware). There is evidence showing that infected computers are being rented out as "Botnets" for creating an entire black-market industry for renting, trading, and managing "owned" computers, leading to economic incentives for attackers. Researchers also showed possibility of "super-botnets," networks of independent botnets that can be coordinated for attacks of unprecedented scale[3].

For an adversary, super botnets would also be extremely versatile and resistant to counter measures. Due to the substantial damage caused by worms in the past years, there have been significant efforts on developing detection and defense mechanisms against worms.

A network based worm detection system plays a major role by monitoring,

collecting, and analyzing the scan traffic generated during worm attacks. In this system, the detection is commonly based on the self propagating behavior of worms that can be described as follows: after a worm-infected computer identifies and infects a vulnerable computer on the Internet, this newly infected computer will automatically and continuously scan several IP addresses to identify and infect other vulnerable computers.

As such, numerous existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns[4],[5].

In this paper ,a new class of active worms, referred to as Camouflaging Worm (C-Worm in short) is explored . The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. The organization of this paper is as follows. Section 2 describes about some techniques used and approaches proposed about C- Warm have been surveyed and are listed in the Sections 3 to 6 and concluded with conclusion in Section 7.

I. Techniques Used

Power Spectral Density (PSD)

Spectral Flatness Measure

To obtain the PSD distribution for worm detection data, there is a need to transform data from the time domain into the frequency domain. To do so, a random process can be to model the worm detection data. The flatness of PSD is measured to distinguish the scan traffic of the C-Worm from the normal non worm scan traffic. For this, SFM is introduced (Spectral Flatness Measure), which can capture anomaly behavior in certain range of frequencies. SFM is defined as the ratio of the geometric mean to the arithmetic mean of the PSD[6],[7].

SFM is a widely existing measure for discriminating frequencies in various applications, such as voiced frame detection in speech recognition. In general, small values of SFM imply the concentration of data at narrow frequency spectrum ranges. C-Worm has unpreventable recurring behavior in its scan traffic; consequently its

SFM values are comparatively smaller than the SFM values of normal non worm scan traffic. For detecting C-Worms, a sliding window to capture a noticeably higher concentration at a small range of spectrum is introduced. When such noticeably concentration is recognized, SFM within a wider frequency range is derived. It has been observed that the SFM value for the C-Worm is very small.

II. Moore, Shannon and Brown(2002)

Moore, Shannon and Brown developed the methodology to trace the spread of Code-Red throughout the Internet. They examined the properties of the infected host population, including geographic location, weekly and diurnal time effects, top-level domains and ISPs. Also the effects of DHCP on measurements of infected hosts were explained and determined that IP addresses are not an accurate measure of the spread of a worm on timescales longer than 24 hours.

In their work, they extracted the IP addresses and found that the same 23 addresses sequence is predicted in packet trace data. After extracting, the IP addresses probed by the worm are compared to the hosts to identify the infected hosts. They classify the infected hosts using the DNS name of each host and a hand-tuned set of regular expression matches into some categories and also used Ixia's IxMapping service to determine the latitude, longitude, and country of each IP address infected with the worm. The experimental data and the results characterize the spread of the Code-Red worms and examined the properties of infected host population, and finally determined the rate at which infected hosts are repaired.

III.Moore, Paxson, and Savage(2003)

Moore, Paxson and Savage investigated about the Slammer worm spread so quickly that human response was ineffective. In January 2003, it packed a benign payload, but its disruptive capacity was surprising. Slammer (sometimes called Sapphire) was the fastest computer worm in history. As it began spreading throughout the Internet, the worm infected more than 90 percent of vulnerable hosts within 10 minutes, causing significant disruption to financial, transportation, and government institutions and precluding any human-based response. They described about how slammer achieved its rapid growth, analyze the portions of the worm to study some of its flaws, and looked at their defensive effectiveness against it and its successors.

IV. Chen, Gao and Kwiat(2003)

Chen, Gao and Kwiat has presented a mathematical model, referred to as the Analytical Active worm Propagation (AAWP) model to analyze the characteristics of the spread of active worms. The AAWP model use deterministic approximation and it gives more realistic results when compared to Epidemiological model. The AAWP model can be used to simulate the Code Red v2 worm with some parameters. In their work, extended the AAWP model to the LAAWP model to understand the spread of active worms using local subnet scanning. The distribution of the hit list can affect the local subnet scanning policy. When the hit list is concentrated in some subnet, the spread of active worms is slowed down. In the LAAWP model, the vulnerable machines are assumed to be evenly distributed in every subnet.

V. Wei Yu, Sriram Chellappan, Xun Wang and Dong Xuan(2005)

Wei Yu, Sriram Chellappan, Xun Wang and Dong Xuan addressed the impacts of worm propagation on top of Peer-to-Peer (P2P) systems and designed effective defense strategies within the P2P system to combat worm propagation. Three aspects have used to combat worms viz., defined two P2P-based attack models such as an offline P2P-based hit-list attack model (OPHLS) and an online P2P-based attack model (OPS) and identified the important P2P system-related and attack-related parameters in modelling of the attacks , conducted detailed analysis to study the impacts of P2P-based active worm propagation and demonstrate that P2P-based worm attacks can significantly worsen attack effects. The parameters such as P2P size, topology degree, host vulnerability, etc. also have important impacts on attack effects and design and evaluate defense strategies within the P2P system to rapidly detect worms and immunize hosts.

In their work, the strategy consists of P2P hosts performing two tasks: worm detection and rapid immunization. To detect worms, they incorporated the methodologies of trend-based and threshold-based worm detection schemes and proved P2P-based worm attacks have clear identifiable exponential propagation trends that enables rapid and accurate worm detection within P2P systems. For immunization, the methodologies of active immunization-based schemes are incorporated. The experimental data demonstrate the effectiveness of our defense strategies in rapidly detecting worm attacks and reducing the number of infected hosts. It is observed from the results that

the trend-based scheme performs favourably compared to the threshold-based scheme in terms of both direction time and detection accuracy and active immunization-based schemes can rapidly suppress worm propagation and contain their spread.

VI. Summary and Conclusion

Active worms pose major security threats to the Internet and it is propagated in an automated fashion as they continuously compromise computers on the Internet. Active worms evolve during their propagation and thus pose great challenges to defend against them. The spread of Code-Red worm in Internet is increasing day by day. To combat worms, many methodologies and defence strategies have been proposed by many researchers. This Literature survey examines the different methodologies used to detect and combat worms.

REFERENCES

1. Zesheng Chen, Lixin Gao, Kevin Kwiat, " Modeling the Spread of Active Worms ", IEEE Infocom 2003
2. Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao," Modeling and Detection of Camou?aging Worm", IEEE Ttransactions on dependable and secure computing ,vol. 8, No. 3, May-June 2011.
3. T. Sanders, "Botnet Operation Controlled 1.5m Pcs Largest Zombie Army Ever Created", http://www.vnunet.com/vnunet/news/2144375/botnet-operation-ruled-million, 2005.
4. M. Garetto, W.B. Gong, and D. Towsley, "Modeling Malware Spreading Dynamics," in Proc. Of IEEE INFOCOM, Mar. 2003.
5. C.C Zou, W. Gong, and D. Towsley, "Code-Red Worm Propagation Modeling and Analysis," In proc. 9th ACM Conf. Computer and Comm. Security (CCS), Nov. 2002.
6. Zdnet, "Smart Worm Lies Low To Evade Detection", 2010.
7. J. Ma, G.M.Yoelker, and S. Savage, "Self-Stopping Worms," in Proc. ACM workshop Rapid Malcode (worm), Nov. 2005.