ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Tracking Down and Simulating Camouflaging Worm Behavior

[1]Praveen Kumar Relangi, [2]G.Sasi Bhushana Rao
[1,2]Dept. of CSE, BVC Engg. College, Odalarevu, Allavaram Mandal, AP, India

Abstract
Active worms continue to pose major threats to the security of today's Internet. This is due to the ability of active worms to automatically propagate themselves and compromise hosts in the Internet. Due to the recent surge of peer-to-peer (P2P) systems with large numbers of users and rich connectivity, P2P systems can be a potential vehicle for the attacker to achieve rapid worm propagation in the Internet. In this paper, we tackle this issue by modeling and analyzing active worm propagation on top of P2P systems, and designing effective defense strategies within P2P systems to suppress worm propagation. In particular: (1) we define two P2P-based active worm attack models: an offline P2P-based hit-list attack model and an online P2P-based attack model; (2) we conduct a detailed analysis on the impacts of worm propagation on top of P2P-based systems, and study the sensitivity of worm propagation to various P2P system and attack-related parameters; (3) finally, we propose defense strategies within the P2P system to combat worms. Based on extensive numerical analysis and simulation data, we demonstrate that P2Pbased active worm attacks can significantly enhance worm propagation, and important P2P related parameters (system size, topology degree, host vulnerability, etc.) have significant impacts on worm spread. We also find that our proposed defense strategies can effectively combat worms by rapidly detecting and immunizing infected hosts.

Keywords
Worm, Camouflage, Anomaly Detection, P2P

I. Introduction

Active worms pose major threats to the security of today's Internet. Being self-propagating and self-replicating, active worms can propagate in an automated fashion without human intervention from infected hosts to other vulnerable hosts in a network. Propagation of active worms in the Internet enables one to control thousands of hosts, launch distributed denial of service attacks, access confidential information, destroy valuable data, etc. [1–4]. Due to the recent surge of many popular peer-to-peer (P2P) systems with a large number of users and connectivity, P2P systems can potentially be a powerful vehicle for attackers to launch active worms and achieve rapid worm propagation in the Internet. In this paper, we tackle this issue by modeling and analyzing active worm propagation on top of P2P systems, and designing effective defense strategies within the P2P system to suppress worm propagation P2P computing has been becoming an active area for Internet scale resource sharing and cooperation. The recent surge of P2P applications can be observed by following statistical data collected on November 3, 2004: there are a total of 2,256,612 users in the FastTrack P2P system, 2,401,835 users in the eDonkey P2P system, 1,258,775 users in the Warez P2P system, and 600,926 users in the Gnutella P2P system [10]. These numbers are still increasing. We believe that P2P systems, being highly popular can become a powerful vehicle for attackers to rapidly propagate worms in the Internet. Some incidents in the recent past have indicated this. Examples are the Igloo and MyDoom worms that spread across KaZaA P2P system through P2P file sharing [11-12]. P2P-based worm propagation can be one of the best facilitators for Internet worm attacks due to the following reasons;

1. Compromising P2P systems with a large number of registered hosts can rapidly accelerate Internet worm propagation, as hosts in P2P systems are real and active;
2. Since hosts in P2P systems maintain a certain number of neighbors for routing purposes, worm infected hosts in the P2P system can easily propagate
the worm to their neighbors, which continue the worm propagation to other hosts and so on;
3. Some hosts in P2P systems may have insecure network and system environments (e.g., home networks);
4. P2P hosts install various application specific software, and any vulnerability in such software can enhance their risk of being infected. Our goal in this paper is to quantitatively understand the impacts of worm propagation on top of P2P systems, and design defenses within the P2P system to combat worm propagation. The highlights of this paper are:

1. We formally define two P2P-based worm attack models: an offline P2P-based hit-list attack model, and an online P2P-based attack model. We identify the important P2P system-related and attack- related parameters in the modeling of the attacks.
2. We conduct a detailed analysis to analyze the performance of the attack models (in terms of the number of hosts infected), and the impacts of various P2P system-related and attack-related parameters on attack effects. Our analysis and experimental data demonstrate that P2P-based worm attacks can significantly worsen attack effects. The parameters including P2P size, topology degree, host vulnerability, etc. have important impacts on attack effects. We also observe that attack effects are more pronounced in the case of unstructured P2P systems compared to structured P2P systems.
3. We design and evaluate defense strategies within the P2P system to combat worms. Our strategy consists of P2P hosts performing two tasks: worm detection and rapid immunization. To detect worms, we incorporate the methodologies of trend-based and threshold-based worm detection schemes. We prove that P2P-based worm attacks have clearly identifiable exponential propagation trends, which enables rapid and accurate worm detection within P2P systems. For immunization, we incorporate the methodology of active immunization-based schemes, and analyze its effectiveness in rapidly immunizing hosts in P2P systems. Our experimental data clearly demonstrate the effectiveness of our defense strategies in rapidly detecting worm attacks and reducing the number of infected hosts. We observe that the trend-based scheme performs favorably compared to the threshold-based scheme in terms of both detection time and detection accuracy. We also observe that active immunization-based schemes can rapidly suppress worm propagation and contain their spread.

II. Background and Related Work

A. Active Worms

Active worms are similar to biological viruses in terms of their infectous and self-propagating nature. They identify vulnerable computers, infect them and the worm-infected computers propagate the infection further to other vulnerable computers. In order to understand worm behavior, we first need to model it. With this understanding, effective detection and defense schemes could be developed to mitigate the impact of the worms. For this reason, tremendous research effort has focused on this area Active worms use various scan mechanisms to propagate themselves efficiently. The basic form of active worms can be categorized as having the Pure Random Scan (PRS) nature. In the PRS form, a worm-infected computer continuously scans a set of random Internet IP addresses to find new vulnerable computers. Other worms propagate themselves more effec- tively than PRS worms using various methods, e.g., network port scanning, email, file sharing, Peer-to-Peer (P2P) networks, and Instant Messaging (IM). In addition, worms use different scan strategies during different stages of propagation. In order to increase propagation efficiency, they use a local network or hitlist to infect previously identified vulnerable computers at the initial stage of propagation. They may also use DNS, network topology and routing information to identify active computers instead of randomly scanning IP addresses. They split the target IP address space during propagation in order to avoid duplicate scans studied a divide-conquer scanning technique that could potentially spread faster and stealthier than a traditional random-scanning worm. Formulated the problem of finding a fast and resilient propagation topology and propagation schedule for Flash worms. Studied the worm propagation over the sensor networks. Different from the above worms, which attempt to accelerate the propagation with new scan schemes, the Camouflaging Worm (C-Worm) studied in this paper aims to elude the de- tection by the worm defense system during worm propagation

B. Detection of Worm

In order to rapidly and accurately detect Internet-wide large scale propagation of active worms, it is imperative to monitor and analyze the traffic in multiple locations over the Internet to detect suspicious traffic generated by worms. The generic worm detection framework that we use in this paper consists of multiple distributed monitors and a worm detection center that controls the former. The monitors are distributed across the Internet and can be deployed at hosts, router, or firewalls etc. Each monitor passively records irregular port-scan traffic such as connection attempts to a range of invalid IP addresses (IP addresses not being used) and restricted service ports. Periodically, the monitors send traffic logs to the detection center. The detection center analyzes the traffic logs and determines whether there is suspicious scans to restricted ports or to invalid IP addresses. If such uncommon scans are detected, the detection center determines that there is a wide-spreading worm propagation on the Internet. The worm detection schemes used in the detection center rely on the analysis of globally collected scan traffic data. Specifically, they study the traffic volume to detect the existence of wide-spreading worms. Some of these schemes use the variance of traffic volume or the exponentially increasing trend of traffic volume to identify large-scale worm propagations. Besides the above detection schemes that are based on the global scan traffic monitoring, there are other worm detection schemes such as sequential hypothesis testing for detecting worm-infected hosts, DSC (Destination-Source Correlation) for detecting a worm in local networks, content-based worm signature. In contrast, our spectrum-based detection scheme uses frequency domain analytical techniques to capture the wide spreading worm propagation.

III. C-Worm Modeling the Behavior

The C-Worm camouflages its propagation by controlling its scan traffic volume during its propagation. The simplest way to manipulate scan traffic volume is to randomly change the number of worm instances conducting port scans. However, this method may not be able to elude detection. The reason is that the overall C-Worm scan traffic volume still shows an increasing trend with the progress of worm propagation and as more and more hosts are being infected, they in turn take part in scanning other hosts. Due to these facts, the C-Worm needs to introduce a feed-back loop control for regulating its propagation speed according to its propagation status. As such, in order to effectively evade detection, the overall scan traffic for the C-Worm should be comparatively slow and variant enough to not show any notable increasing trends over time. On the other hand, a very slow propagation of the C-Worm is also not desirable, since it delays rapid damage to the Internet. Hence, the C-Worm needs to adjust its propagation so that it is neither too fast to be easily detected, nor too slow to delay rapid damage on the Internet. To regulate the C-Worm scan traffic volume, we introduce a control parameter called attack probability. We assume that a worm attacker wants to manipulate scan traffic volume so that the number of worm instances participating in the worm propagation follows a random distribution

IV. Performance Evaluation

In the following, we report results of our experiments in evaluating the impacts of P2P-based worm attacks, the sensitivity of worm propagation to various attacks and P2P system parameters, and the performance of our worm defense in containing worm propagation.

A. Evaluation Methodology

1. Evaluation Metrics

We broadly classify our metrics into two types: attack related and defense related. Our attack-related metric in this paper is the infection ratio over time, which quantifies the speed of worm propagation. Specifically, it is the ratio of the total number of infected hosts to the number of vulnerable hosts over time. The higher this value is, better is the attack performance. The hosts include those in the Super-P2P and the Non-P2P systems. There are two defense related metrics we evaluate here. The first is the worm detection time, defined as the time taken to successfully detect a worm attack to the P2P system. Obviously, if the detection time is smaller, the defense performance is better. The second metric is once again the ratio of the number of infected hosts to the number of vulnerable hosts over time. However, this parameter here is measured with our defense in place. Ideally, we expect the ratio to go down with defense.

2. Evaluation Systems

We represent our evaluation systems using a tuple of the form, We point out that in our simulations here, we consider hosts in the P2P systems which have the same vulnerability as other hosts in the Internet. In reality, hosts in the P2P system are likely to be more vulnerable (due to file sharing, downloading malicious software,

etc.). As such, the impacts of worm propagation on P2P systems may be far worse than what we show here in our simulations. The term means that the corresponding parameters are variables in our performance evaluations. We use both numerical analysis and discrete-time simulation to obtain performance data. Our results are averaged by 200 simulation runs with the same input parameters but different seeds for random number generator. In the following, we report our performance results. Due to space limitations, we only present a limited number of cases here. However, we found that the conclusions we draw generally hold for many other cases we have evaluated. The data obtained from analytical derivations in Sections III, and IV, are represented by dotted lines, while data obtained from simulations are represented by solid lines. In all data reported, the data obtained from our analytical results is in very good agreement with our simulation data.

B. P2P-Based Worm Attack Performance Results

We first compare different attack models to see their impacts. We then study the sensitivity of worm propagation for different attack models to important P2P system parameters. All data shown start at time 35, as the infection ratio is very small (close to 0) in the time interval [0,35] due to very small number of infected hosts compared to the large number of vulnerable hosts initially. (1) Performance comparison of all attack models. Fig. 1 shows the data on the performance of various attack models ver time. The parameters are hSYS; ATT; ;i, where SYS and ATT have default values. The attack models are shown in the legend in Fig. 1. We report both analytical and simulations data. The term A in the legend represents the data obtained for the corresponding attack model using our analytical derivations. For the case where the attack model is just mentioned in the legend, the data shown is the simulation data for the corresponding attack model. From Fig. 1, we can make the following observations: (a) The P2P-based attack models overall outperform the PRS attack model. For example, in the fast propagation phase of the worm (from simulation time 40–60), P2P-based attack models can achieve a minimum of 100–300% performance increase over the PRS attack model, highlighting the impacts of P2P-based worm propagation. (b) The OPHLS attack model achieves the fastest propagation compared to online-based attack models. The reason is that IP addresses of all P2P hosts (attack hit-list) are obtained prior to attacks in the OPHLS model, which enables rapid worm propagation. In our simulations, we do not consider the time taken for the worm attacker to obtain the P2P hit-list. In this paper, we study impacts during the phase of worm propagation on P2P systems. The phase where the hit-list is obtained is orthogonal to worm propagation. The attacker does not pursue any attack during this phase. The attacker can offline obtain the hit-list by means of P2P crawler tools,

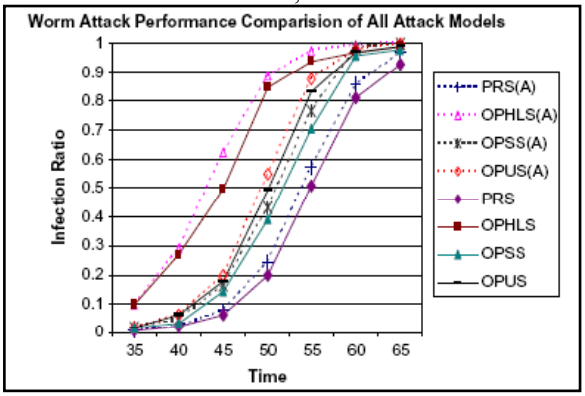

Fig. 1: Performance Comparision of all Attack Models

information published on web sites, etc. The time during collection may take days, weeks, or even months, depending on the attackers approach, resources, P2P host dynamics, etc. It is too difficult, if not impossible to model the phase of hit-list collection, and is not our focus here. (2) Attack performance vs. P2P system size. Fig. 2, shows the sensitivity of infection ratio over time under two P2P system sizes (number of hosts in the Super-P2P system).

When P2P system size increases, the attack performance becomes consistently better for all attack models. This is because, when the P2P system size increases, the probability that a scan hits the vulnerable hosts increases, consequently increasing the number of infections. (3) Attack performance vs. P2P topology degree. Recall from our analysis in Section III, that demonstrated the importance of structured/ unstructured property of P2P systems on worm propagation (which is function of topology degree).

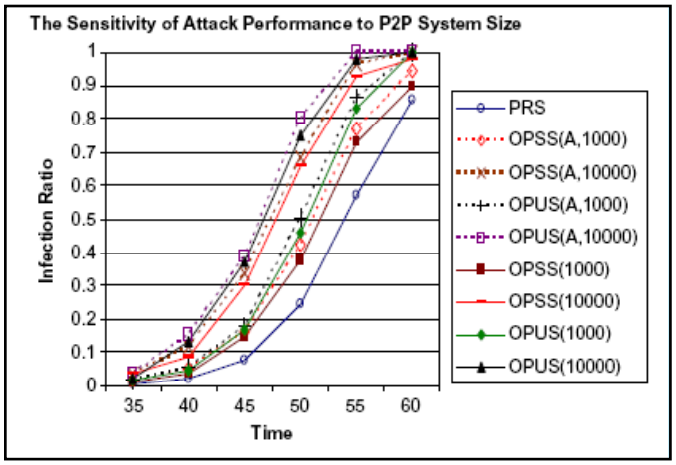

Fig. 2: Attack Performance vs. P2P System Size

C. Worm propagation Module

Worm scan traffic volume in the open-loop control system will expose a much higher probability to how an increasing trend with the progress of worm propagation. As more and more computers get infected, they, in turn, take part in scanning other computers. Hence, we consider the Cworm as a worst case attacking scenario that uses a closed loop control for regulating the propagation speed based on the feedback propagation status.

V. Conclusion

We studied a new class of smart-worm called C- Worm, which has the capability to camouflage its propagation and further avoid the detection. Our investigation showed that, although the C-Worm successfully camouflages its propagation in the time domain, its camouflaging nature inevitably manifests as a distinct pattern in the frequency domain. Based on observation, we developed a novel spectrum-based detection scheme to detect the C-Worm. Our evaluation data showed that our scheme achieved superior detection performance against the C-Worm in comparison with existing representative detection schemes. This paper lays the foundation for ongoing studies of "smart" worms that intelligently adapt their propagation patterns to reduce the effectiveness of countermeasures

References

[1] D. Moore, C. Shannon, J. Brown,"Code-red: a case study on the spread and victims of an internet worm", in Proceedings of the 2-th Internet Measurement Workshop (IMW), Marseille, France, November 2002.

[2] D. Moore, V. Paxson, S. Savage,"Inside the slammer worm", in IEEE Magazine of Security and Privacy, July 2003.

[3] CERT, CERT/CC advisories, [Online] Available: http://www.cert.org/advisories/.

[4] P. R. Roberts,"Zotob Arrest Breaks Credit Card Fraud Ring", [Online] Available: http: //www.eweek.com/article2/0,1895,1854162,00.asp.

[5] W32/MyDoom.B Virus, [Online] Available: http://www.uscert. gov/cas/techalerts/ TA04-028A.html.

[6] W32.Sircam.Worm@mm, [Online] Available: http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html.

[7] Worm.ExploreZip, [Online] Available: http://www.symantec.com/avcenter/venc/data/worm.explore.zip.html.

[8] R. Naraine,"Botnet Hunters Search for Command and Control Servers", [Online] Available: http://www.eweek.com/article2/0,1759,1829347,00.asp.

[9] T. Sanders,"Botnet operation controlled 1.5m PCs Largest zombie".

[11] S. Staniford, V. Paxson, N.Weaver,"How to own the internet in your spare time", in Proceedings of the 11-th USENIX Security Symposium (SECURITY), San Francisco, CA, August 2002.

[12] Z. S. Chen, L.X. Gao, K. Kwiat,"Modeling the spread of active worms", in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.

[13] M. Garetto, W. B. Gong, D. Towsley, "Modeling malware spreading dynamics", in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.

[14] C. C. Zou, W. Gong, D. Towsley,"Codered worm propagation modeling and analysis", in Proceedings of the 9-th ACM Conference on Computer and Communication Security (CCS), Washington DC, November 2002. army ever created, [Online] Available: http://www.vnunet.com/vnunet/news/2144375/ botnet-operation-ruled-million, 2005.

[15] R. Vogt, J. Aycock, M. Jacobson,"Quorum sensing and selfstopping worms", in Proceedings of 5th ACM Workshop on Recurring.

PRAVEEN KUMAR RELANGI, He is Pursuing M. Tech(CSE), From B V C Engineering College, Odalarevu, Allavaram Mandal, East Godavari District, Andhra Pradesh-533201, India. His areas of interest are Network security and Networking applications.

G.SASIBHUSHANA RAO, M. Tech Working as Assoc. Prof, Department of Computer Science Engineering, B V C Engineering College, Odalarevu, Allavaram Mandal, East Godavari District, Andhra Pradesh-533201, India. His areas of interest are Computer Network Security, Image Processing and Data mining.