Paradigmatic and Exploration of Blind Worm

Yellamandaiah Gogula[1], E.Jhansi Rani[2]
[1]Pursuing M.Tech(CSE), [2]Asst. Professor, Department of Computer Science Engineering, Nalanda Institute of Engineering & Technology,Siddharth Nagar, Sattenapalli, Guntur., Affiliated to JNTUK, Kakinada, A.P., India.

Abstract—Active worms pose major security threats to the Internet. This is due to the ability of active worms to propagate 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. In this paper, we investigate a new class of active worms, referred to as Tarnen Worm (C-Worm in short). The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. Thereby, the C-Worm camouflages its propagation from existing worm exploration systems based on analyzing the propagation traffic generated by worms. We analyze characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and non-worm traffic (background traffic). We observe that these two types of traffic are barely distinguishable in the time domain. However, their distinction is clear in the frequency domain, due to the recurring manipulative nature of the C-Worm. Motivated by our observations, we design a novel spectrum-based scheme to detect the C-Worm. Our scheme uses the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to distinguish the C-Worm traffic from background traffic. Using a comprehensive set of exploration metric s and real-world traces as background traffic, we conduct extensive performance evaluations on our proposed spectrum-based exploration scheme. The performance data clearly demonstrates that our scheme can effectively detect the C-Worm propagation. Furthermore, we show the generality of our spectrum-based scheme in effectively detecting not only the C-Worm, but traditional worms as well.

Index Terms —Worm, Glitch Exploration.

1 INTRODUCTION

An active worm refers to a hateful software program that propagates itself on the Internet to infect other computers. The broadcast of the worm is based on exploiting vulnerabilities of computers on the Internet. Many real-world worms have caused notable harm on the Internet. These worms include “Code-Red” worm in 2001 [1], “Slammer” worm in 2003 [2], and “Witty”/“Sasser” worms in 2004 [3]. 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 [4]. These botnets can be used to: (a) launch very big Distributed Denial-of-Service (DDoS) attacks that disrupt the Internet utilities [5], (b) access private information that can be misused [6] through large scale traffic sniffing, key logging, identity theft etc, (c) tear down data that has a high financial value [7], and (d) distribute large-scale unsolicited advertisement emails (as spam) or software (as malware). There is evidence showing that contaminated 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 [4], [8], [9]. Researchers also showed possibility of “super-botnets,” networks of independent botnets that can be coordinated for attacks of unprecedented scale [10]. For an adversary, super botnets would also be extremely versatile and resistant to countermeasures.

The remainder of the paper is organized as follows. In Section 2, we introduce the background and review the related work. In Section 3, we introduce the propagation model of the C-Worm. We present our spectrum-based exploration scheme against the C-Worm in Section 4. The performance evaluation results of our spectrum-based exploration scheme is provided in Section 5. We conclude this paper in Section 6.

2 BACKGROUND AND R ELATEDWORK

2.1 Active Worms

Active worms are similar to biological viruses in terms of their infectous and self-propagating nature. They identify helpless computers, infect them and t he 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 exploration and defense schemes could be developed to mitigate the impact of the worms. For this reason, wonderful research effort has focused on this area.

Different from the above worms, which attempt to accelerate the propagation with new scan schemes, the Tarnen Worm (C-Worm) studied in this paper aims to elude the exploration by the worm defense system during worm propagation. Closely related, but orthogonal to our work, are the evolved active worms that are polymorphic in nature. Polymorphic worms are able to change their binary representation or signature as part of their propagation process. This can be achieved with self-encryption mechanisms or semantics preserving code manipulation techniques. The C-Worm also shares some similarity with stealthy port-scan attacks. Such attacks try to find out available services in a target system, while avoiding exploration. It is accomplished by decreasing the port scan rate, hiding the origin of attackers, etc. Due to the nature of self-propagation, the C-Worm must use more complex mechanisms to manipulate the scan traffic volume over time in order to avoid exploration.

2.2 Worm Exploration

Worm exploration has been intensively studied in the past and can be generally classified into two categories: “host-based” exploration and “network-based” exploration. Host-based exploration systems detect worms by monitori ng, collecting, and analyzing worm behaviors on end-hosts. Since worms are malicious programs that execute on these computers, analyzing the behavior of worm executables plays an important role in host- based exploration systems. Many exploration schemes fall under this category [37], [38]. In contrast, network-based exploration systems detect worms primar ily by monitoring, collecting, and analyzing the scan traffic (messages to identify vulner- able computers) generated by worm attacks. Many exploration schemes fall under this category. Ideally, security vulnerabilities must be prevented to begin with, a problem which must addressed by the programming language community. However, w hile vulnerabilities exist and pose threats of large-scale damage, it is critical to also focus on network-based exploration, as this paper does, to detect wide- spreading worms.

3 PARADIGMATIC OF THEC-WORM

3.1 C-Worm

The C-Worm camouflages its propagation by controlling 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.

3.2 Propagation Model of the C-Worm

To analyze the C-Worm, we adopt the epidemic dynamic model for disease propagation, which has been broadly used for worm propagation Paradigmatic [2]. Based on existing results [2], this model matches the dynamics of real worm propagation over the Internet quite well. For this reason, similar to other publications, we adopt this model in our paper as well. Since our investigated C-Worm is a novel attack, we modified the original Epidemic dynamic formula to model the propagation of the C-Worm by introducing the P (t) - the attack probability that a worm-infected computer participates in worm propagation at time t. We note that there is a wide scope to notably improve our modified model in the future to reflect several uniqueness that are relevant in real-world practice.

3.3 Effectiveness of the C-Worm

We now demonstrate the effectiveness of the C-Worm in evading worm exploration through calculating P (t). Given random selection of M c, we generate three C-Worm attacks (viz., C-Worm 1 ,C-Worm2 and C-Worm 3) that are characterized by different selections of mean and variance magnitudes for M C. In our simulations, we assume that the scan rate of the traditional PRS worm follow a normal distribution S n = N (40 , 40) (note that if the scan rate generated by above distribution

is less than 0 , we set the scan rate as 0). We also set the total number of vulnerable computers on the Internet as 360,000, which is the total number of infected computers in "Code-Red" worm incident.

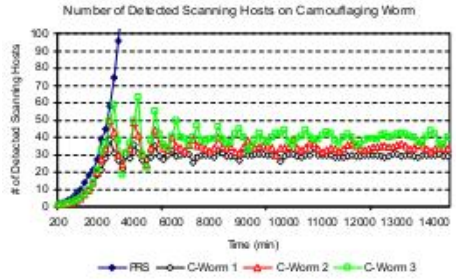

Fig. 1. Observed infected instance number for the C-Worm and PRS worm

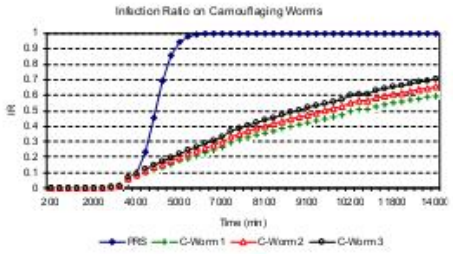

Fig. 2. Infected ratio for the C-Worm and PRS-Worm

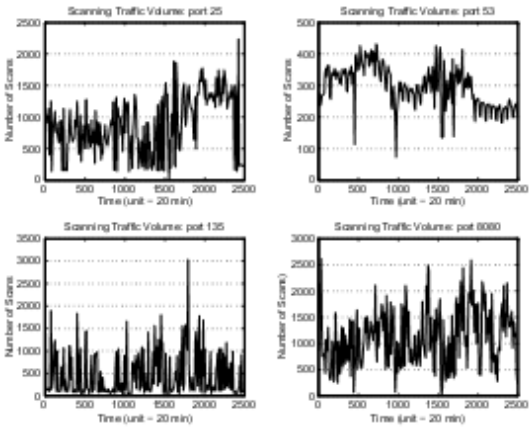

Fig. 3. Observed infected instance number for back-ground scanning reported by ISC

3.4 Discussion

In this paper, we focus on a new class of worms, referred to as the Tarnen worm (C-Worm). The C-Worm adapts their propagation traffic patterns in order to reduce the probability of exploration, and to eventually infect more computers. The C-Worm is different from polymorphic worms that deliberately change their payload signatures during propagation. For example, MetaPHOR and Zmist worms intensively change their payload signature to hide themselves from exploration schemes that rely on expensive packet payload analysis.

4 DETECTING THEC-WORM

4.1 Design Rationale

In this section, we develop a novel sp ectru m-based exploration sch e me . Recall that the C-Worm goes undetected by exploration schemes that try to determine the worm propagation only in the time domain. Our exploration s cheme captures the distinct pattern of the C-Worm in the frequency domain, and thereby has the potential of effectively detecting the C-Worm propa- gation.

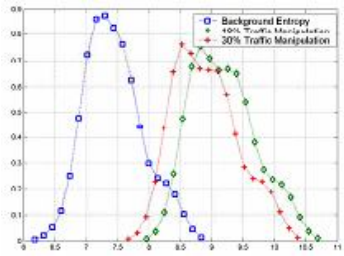

Fig. 4. Manipulation of attack target distribution entropy

The large SFM values of normal non-worm scan traffic can be explained as follows. The normal non-worm scan traffic does not tend to concentrate at any meticulous frequency since its random dynamics is not caused by any recurring phenomenon. The small value of SFM can be reasoned by the fact that the power of C-Worm scan traffic is within a narrow-band frequency range. Such concentration within a narrow range of frequencies is unavoidable since the C-Worm adapts to the dynamics of the Internet in a recurring manner for manipulating the overall scan traffic volume.

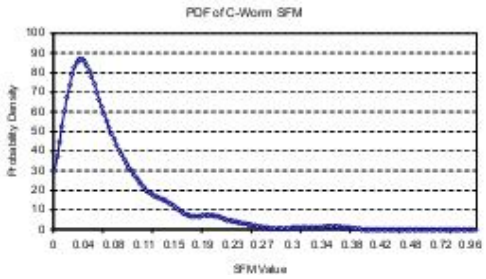

Fig. 5. PDF of SFM on C-Worm traf fi c

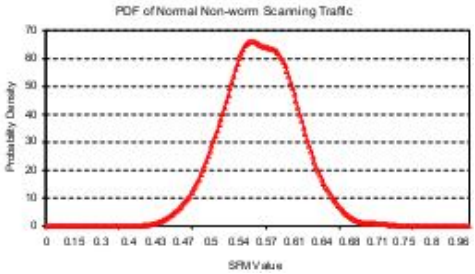

Fig. 6. PDF of SFM on normal non-worm traffi c

4.2 Spectrum-based Exploration Scheme

We now present the details of our spectrum-based exploration scheme. Similar to other exploration schemes, we use a "destination count" as the number of the unique destination IP addresses targeted by launched scans during worm propagation. To understand how the purpose count data is obtained, we recall that an ITM system collects logs from distributed monitors across the Internet.

4.2.1 Power Spectral Density (PSD)

To obtain the PSD distribution for worm exploration data, we need to transform data from the time domain into the frequency domain.

4.2.2 Spectral Flatness Measure (SFM)

We measure the flatness of PSD to distinguish the scan traffic of the C-Worm from the normal non-worm scan traffic.

4.2.3 Exploration Decision Rule

We now describe the method of applying an appropriate exploration rule to detect C-Worm propagation.

Notice that even if the C-Worm monitors the port-scan traffic report, it will be hard for the C-Worm to make the SFM similar to the background traffic. This can be reasoned by two factors. First, the low value of SFM is mainly caused by he closed-loop control nature of C-worm. The attentiveness within a narrow range of frequencies is unavoidable since the C-Worm adapts to the dynamics of the Internet in a recurring manner for manipulating the overall scan traffic volume.

5 PERFORMANCE EVALUATION

In this section, we report our evaluation results that illustrate the success of our spectrum-based exploration scheme against both the C-Worm and the PRS worm in comparison with existing representative exploration schemes for detecting wide-spreading worms. In addition, we also take into consideration destination distribution based exploration schemes and evaluate their performance against the C-Worm.

5.1 Evaluation Methodology

- Evaluation Metrics
- Simulation Setup

5.2 Performance of Exploration Schemes

We assess our proposed spectrum-based exploration scheme by comparing its performance with three existing delegate traffic volume-based exploration schemes. The first scheme is the volume mean-based (MEAN) exploration scheme which uses mean of scan traffic to detect worm propagation [2]; the second scheme is the trend-based (TREND) exploration scheme which uses the increasing trend of scan traffic to detect worm broadcast [19]; and the third scheme is the victim number variance based (VAR) exploration scheme which uses the variance of the scan traffic to detect worm propagation [21].

- Exploration Performance for C-Worm Attacks
- Exploration Performance for Traditional PRS Worms

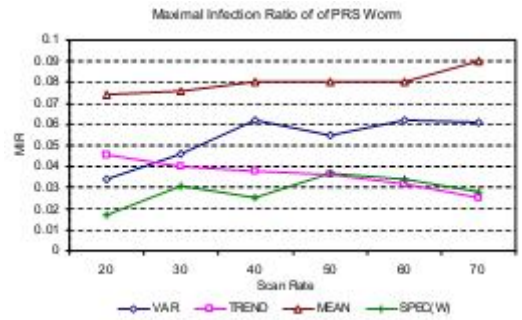

Fig. 7. Maximal Infection Ratio of detection schemesagainst PRS worm

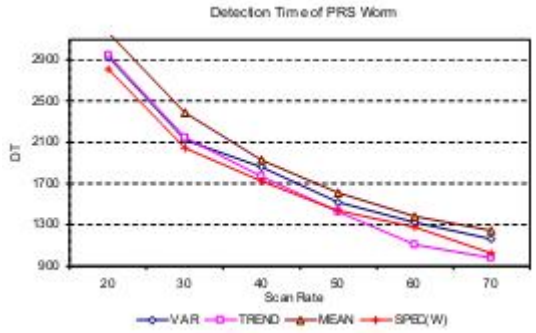

Fig. 8. Detection Time of detection schemes against PRS worm

In view of emphasizing the relative performance of our SPEC and SPEC(W) schemes with the obtainable worm exploration schemes, we plot the MIRand DT results in Figs. 7 and 8 for different scan rates S . We can observe from these figures that the MIRand DT results of our spectrum based scheme (shown only for SPEC(W)) are comparable or better than the existing worm exploration schemes. For a mean scan rate of 70/min, our SPEC(W) scheme achieves a exploration time of 1024 mins, which is faster than that of VAR and MEAN schemes, whose values are 1239min and 1161min, in that order. For the same mean scan rate of 70/min, SPEC(W) achieves a maximal infection ratio of 0 .03, which is comparable to TREND's MIRvalue and is less than 50% of the MIRvalue for the VAR and MEAN exploration schemes. The effectiveness of our spectrum-based scheme is based on the fact that traditional PRS worm scanning traffic shows a constantly rapid increase. Thus, SFM values are relatively small due to PSD concentration at the low frequency bands in the case of the traditional PRS worm scanning.

6 FINALR EMARKS

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

REFERENCES

[1] D. Moore, C. Shannon, and J. Brown, "Code-red: a case study on the spread and victims of an internet worm," in P roceedings of the 2 –th Internet Measurement Wo rkshop (IMW) , Marseille, France, November 2002.
[2] D. Moore, V. Paxson, and S. Savage, "Inside the slammer worm," in IE E E Magaz ine o f S ecur ity and P r ivacy , July 2003.
[3] CERT, CE R T /CC advis or ies, http://www.cert.org/advisories/.
[4] P.R.Roberts, Zotob Arrest Breaks Credit Card Fraud Ring, http: //www.eweek.com/article2/0,1895,1854162,00.asp.
[5] W32/MyDoom. BVirus, http://www.us-cert.gov/cas/techalerts/ TA04-028A.html.
[6] W32. Sircam. Worm@mm , http://www.symantec.com/avcenter/venc/data/ w32.sircam.worm@mm.html.
[7] Wo rm. E xploreZip, http://www.symantec.com/avcenter/venc/data/worm. explore.zip.html.
[8] R. Naraine, Botnet Hunters Search for Com m and and Control Servers , http://www.eweek.com/article2/0,1759,1829347,00.asp.
[9] T. Sanders, B o tnet opera tion contro lled 1. 5m PCs Larges t z o m - biearmy ever created, http://www.vnunet.com/vnunet/news/2144375/ botnet-operation-ruled-million, 2005.
[10] R. Vogt, J. Aycock, and M. Jacobson, "Quorum sensing and self- stopping worms," in Proceedings of 5th ACM Workshop on Recurring Malcode (WO R M), Alexandria VA, October 2007.
[11] S. Staniford, V. Paxson, and N. W eaver, "How to own the internet in yourspare time," in P roceedings of the 11-th U S E NIX Secur ity Sym pos ium(SECURITY), San Francisco, CA, August 2002.