International Journal of Computer and Communication Technology

Volume 7 | Issue 4 Article 10

October 2016

SMART WORMS DEFENSE AND DETECTION

DASARI NAGARAJU
CSE Dept, JNTUA College of Engineering, Anantapur, Andhra Pradesh, India, raj2dasari@gmail.com

C. SHOBA BINDU
CSE Dept, JNTUA College of Engineering, Anantapur, Andhra Pradesh, India, shobabindhu@gmail.com

SMART WORMS DEFENSE AND DETECTION

DASARI NAGARAJU[1] & C. SHOBA BINDU[2]

[1,2]CSE Dept, JNTUA College of Engineering, Anantapur, Andhra Pradesh, India
E-mail : raj2dasari@gmail.com, shobabindhu@gmail.com

Abstract - There are several worm attacks in the recent years, this leads to an essentiality of producing new detection technique for worm attacks. In this paper we present a spectrum based smart worm detection scheme, this is based on the idea of detection of worm in the frequency domain. This scheme uses the power spectral density of the scan traffic volume and its corresponding flatness measure to distinguish the smart worm traffic from background traffic. This scheme showed better results against the smart worms and also for the c-worm detection.

Keywords *- security, worm, and detection*

I. INTRODUCTION

Smart worms are malicious software that can self – propagate across the internet, i.e., compromise vulnerable hosts and use them to attack other victims. Since the early stage of the internet, worms have caused enormous damage and been a significant security threat. For example, the Morris worm infected 10% of all hosts in the internet in 1988. The Code Red worm compromised at least 359,000 hosts in one day in 2001 [1], and the Storm botnet affected the tens of millions of hosts in 2007.

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. In this paper, we conduct a systematic study on smart worms. The smart worms have a self propagating behavior similar to traditional worms. The smart worms are quite different from traditional worms in which it manipulates any noticeable trends in the number of infected computers such a manipulation of the scan traffic volume prevents exhibition of any exponentially increasing trends or even crossing of thresholds that are tracked by existing system [2], [3].

Based on the observation, we adopt frequency domain analysis technique and develop a detection scheme against wide-spreading of the smart worms; particularly we develop a spectrum based detection scheme that uses the power spectral density distribution of scan traffic volume in the frequency domain and its corresponding spectral flatness measure to distinguish the smart worm traffic from non worm traffic [4].

We define the metrics to evaluate the performance; the metrics are Detection time and Detection rate. Our evaluation data clearly demonstrate that spectrum based detection scheme achieves much better performance against the smart worm propagation.
The remainder of this paper is organized as follows. In Section 2, we introduce the spread of smart worms. In Section 3, we introduce the smart worm propagation model. In Section 4, we introduce the spectrum based detection scheme against the smart worms. In Section 5, the performance evaluation and the results of our detection scheme is provided. We conclude the paper in Section 6.

II. SPREAD OF SMART WORMS

In this section, we describe how smart worms spread, then introduce the parameters used in the spread of smart worms. Finally, we present pure random scanning model.

When a smart worm is fired into the Internet, it simultaneously scans many machines in an attempt to find a vulnerable host to infect. When it finally finds its prey, it sends out a probe to infect the target. If successful, a copy of this worm is transferred to this new host. This new host then begins running the worm and tries to infect other machines. During the worm's spreading process, some machines might stop functioning properly, forcing the users to reboot these computers or at least kill some of the processes that may have been exploited by the worm. Then these infected machines become vulnerable machines again, and are still inclined to further infection. When the worm is detected, people will try to slow it down or stop it. A patch, which repairs the security hole of the machines, is used to defend against worms. When an infected or vulnerable machine is patched, it becomes an invulnerable machine.

III. SMART WORM PROPAGATION MODEL

To understand the characteristics of smart worms, we adopt the epidemiological model, which has been extensively used for worm propagation modeling [5]. This model matches the dynamics of real worm propagation over the hosts quite well.

Particularly, the epidemiological model assumes that any given computer is in one of the following states: immune, vulnerable, or infected. An immune computer is one that cannot infect by a worm; a

vulnerable computer is one that has the potential of being infected by a worm; an infected computer is one that has been infected by a worm. The epidemiological model can expressed as,

$$\frac{dn}{dt} = \beta . n . [N - n], \quad (1)$$

Table 1
The parameters for the spread of smart worms

Notation	Explanation
n	The number of infected computers at time t.
N	(=T.p1.p2) the number of vulnerable computers on the internet.
T	
P1	Total number of IP addresses on the internet.
P2	The ratio of total number of computers on the internet over T.
β	Ratio of total number of vulnerable computers on the internet over the total number of computers on the internet Pair wise infection rate.

This epidemiological model works with the principle of disease propagation, which has been used for the worm propagation modeling. It uses a continuous time differential equations.

IV. SMART WORM DETECTION SCHEME

In this section we develop a spectrum based detection scheme. Our detection scheme captures the distinct patterns of the smart worms in the frequency domain, and thereby has the potential of effectively detecting the smart worm propagation.

In order to identify the smart worms propagation in the frequency domain, we use the distribution of Power spectral density (PSD) and its corresponding Spectral flatness measure (SFM) of the scan traffic. Particularly, PSD describes how the power of a time series is distributed in the frequency domain. Mathematically, it is defined as the Fourier transform of the auto correlation of a time series. The time series corresponding to the changes in the number of worm instances that actively conduct scans over time.

4.1 SPECTRUM BASED DETECTION

We know present the details of spectrum based detection scheme. Similar to other detection schemes [6], [7], we use the destination count as the number of unique destination hosts targeted by launching scans during worm propagation. The distribution of PSD and its corresponding SFM are used to distinguish the smart worm scan traffic and non worm scan traffic. In our detection scheme, the detection data is further processed in order to obtain its PSD and SFM. In the following we detail how the PSD and SFM are determined during the processing of the detection data.

4.1.1 Power Spectral Density (PSD)

To obtain the PSD distribution for worm detection data, we need to transform the data from time domain into the frequency domain. To do so, we use source count Z (t) is obtained by counting the unique hosts. Assuming that Z (t) is the source count in the time period [t-1, t] (t ϵ[1, n]), we define the auto-correlation of Z (t) by

$$C_x(L) = M[Z(t)\, Z(t + L)]. \quad (2)$$

In formula (2), $C_x(L)$ is the correlation of worm detection at time interval L. if a recurring behavior exists, a Fourier transform of auto correlation function reveal such behavior. The discrete Fourier transform of the auto correlation for the function is given as follows,

$$\psi(C_x[L], P) = \sum_{n=0}^{N-1} (C_x[L]) \cdot e^{-j2\pi Pn/N} \quad (3)$$

Where P=0, 1… N-1.

As the PSD inherently captures any recurring pattern in the frequency domain, the PSD function shows a comparatively even distribution across a wide spectrum range for the normal non-worm scan traffic.

4.1.2 Spectral Flatness Measure (SFM)

We measure the flatness of PSD to distinguish the scan traffic of the smart worm from the normal non worm scan traffic. For this we introduce the Spectral Flatness Measure which can capture anomaly behavior in certain range of frequencies [8], [9]. The SFM is defined as the ratio of the geometric mean to the arithmetic mean of the PSD coefficients. it can be given as,

$$SFM = \frac{[\Pi_{k=1}^{n} S(f_k)]^{\frac{1}{n}}}{\frac{1}{n}\sum_{k=1}^{n} S(f_k)} \quad (4)$$

Where $S(f_k)$a PSD coefficient is for the PSD obtained from the results in Formula (3), SFM is a widely existing measure for discriminating frequencies in various applications.

V. PERFORMANCE EVALUATION

In this section, we report our evaluation results that illustrate the effectiveness of our spectrum based detection scheme against both the smart worms and the c-worm.

5.1.1 Detection Performance for Smart worms

Table 2 shows detection results of detection scheme against the smart worm. The results have been average over 100 smart worm attacks. From this table we can observe that this detection scheme has

succeeded in find outing the rate of 84% within the time period of 1000 seconds. We evaluate the detection performance of detection scheme against the C-worm. The detection performance has been averaged over the 100 C-worm attacks. We observe that this scheme has succeeded in find outing the rate of 99 % in the case of C-worm attacks within the time period of 1000 seconds.

Table 2
Detection results for the smart worms and c-worm

worms	Detection time(sec)	Detection rate
Smart worms	1000	84%
C-worm	1000	99%

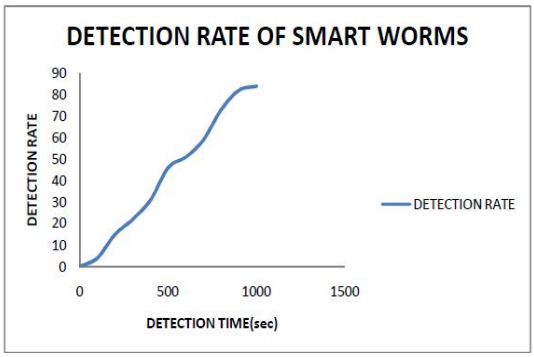

Fig. 1 : Detection Rate of detection schemes against the Smart worms

In view of emphasizing the relative performance of our spectrum based detection scheme, we plot the DT and DR results of smart worms and c-worm in Figs 1 and 2. We can observe from these figures that our spectrum based detection scheme showed better results for smart worms detection and as well as C-worm detection.

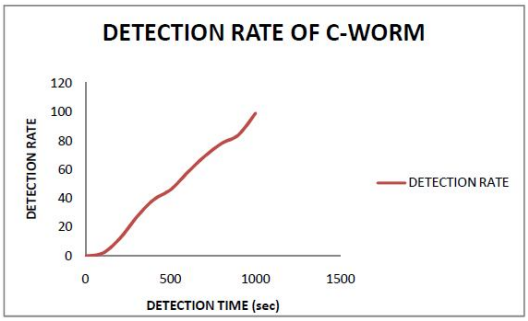

Fig. 2. Detection Rate of detection schemes against the C-worm

VI. CONCLUSIONS

We present the spectrum based detection scheme for the smart worms. Our investigation showed that this detection scheme achieved good performance against the Smart worms and also for the C-worm attacks.

REFERENCES

[1] D. Moore, C. Shanoon, and 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] Z. S. Chen, L.X. Gao, and K. Kwait, “Modelling the spread of active worms,” in proceedings of the IEEE Conference on Computer Communications[INFOCOM], San Fransisco, CA, March 2003.

[3] M. Garetto, W. B. Gong, and D. Towsley, ”Modelling malware spreading dynamics”, in proceedings of the IEEE Conference on Computer Communications[INFOCOM], San Fransisco, CA, March 2003.

[4] Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao, ”Modelling and detection of camouflaging worm,” in Proceedings of IEEE transactions on dependable and secure computing, vol. 8, no. 3, MAY-JUNE2011.

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

[6] C. Zou, W. B. Gong, D. Towsely, and L.X. Gao, “Monitoring and early detection for internet worms,” in Proceedings of the 10-th ACM Conference on Computer Communications Security (CCS), Washington DC, October 2003.

[7] J. Wu, S. Vangala and L. X. Gao, “An effective architecture and algorithms for detecting worms with various scan techniques,” in Proceedings of the 11-th IEEE Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2004.

[8] S. Soundararajan and D. L. Wang, “A schema-based model for phonemic restoration,” Tech. Report, OSU-CISRC-1/04-TRO#, Department of Computer science and Engineering, The Ohio State Univeresity, January 2004.

[9] N. S. Jayant and P.Noll, Digital Coding of Waveforms, Prentice-Hall,1984.

◈◈◈