Volume 5, Issue 10, October-2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Modelling and Detection of Camouflaging Worm at an Advance Level

Kinjal S. Thaker
Student, M.E., Computer Engineering Department,
KITRC, 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 Camouflaging 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 detection 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 detection metrics and real-world traces as background traffic, we conduct extensive performance evaluations on our proposed spectrum-based detection 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.

***Keywords:** Worm, camouflage, anomaly detection, PSD, SFM*

I. INTRODUCTION

Active worm’s is like a Trojan horse they effects your internal files without coming into your observation. Active worm’s refers to harmful software program that spreads itself on the internet to infect other computers. Active worms propagate by damaging computer systems and by using infected computers to spread the worms in an automated fashion [7]. A worm is a computer program that has the capacity to copy itself from machine to machine [3]. The propagation of the worm is based on exploiting dangerously of hosts on the Internet. Many real worms have arranged much damage on the Internet [4]. The worms include various names like Nimda, Morris, Code Red, Slammer, Witty and Sasser [5]. Large numbers of computers has infected by many active worms and recruit them as bots or zombies, which are interconnected together to form botnets [1]. These active worms will cause following infections,

- launch massive Distributed Denial-of-Service (DDoS) attacks that disrupt the Internet utilities [9],
- access confidential information that can be misused through large-scale traffic sniffing, key logging ,identity theft, etc.
- destroy data that has a high monetary value [9], and
- distribute large-scale unsolicited advertisement emails (as spam) or software (as malware).

C-worm has power to intelligently manipulates its scan traffic volume over time. Camouflaging worm (C-Worm) is a complex type of active worm which attempts to remain hidden by sleeping (suspending scans) it defendant when it is under observation [3]. The Propagation model of C-Worm is accurately understand and analyzed in both time and frequency domains. We observe that although the C-Worm scan traffic shows no observable trends in the time domain, it exposes a distinct pattern in the frequency domain [4]. The C-Worm has a self-propagating nature similar to traditional worms, i.e., it specify to rapidly infect as many assailable computers as possible. The C Worm is rather different from traditional worms in which it camouflages any observable trends in the number of infected computers over time [5].

II. WORM DETECTION

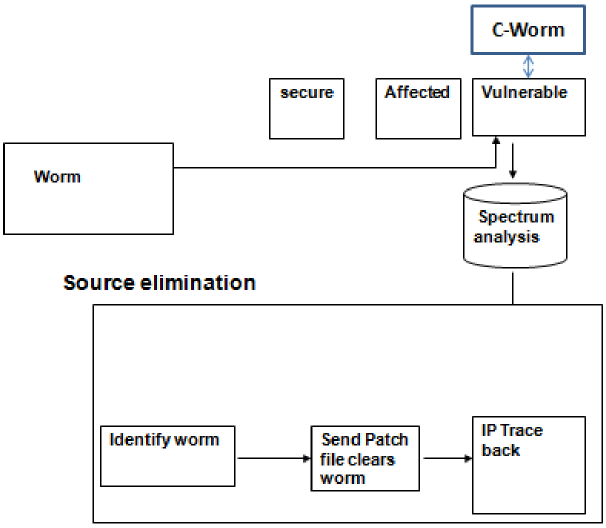
The research that has been about for the past many years to detecting of worms. This kind of research is mandatory to protect IT systems by preventing vicious code from entering into our network .Worm detection method are grouped into two categories: “host based” detection and “network based” detection[8]. Host based detection systems detect worms by monitoring, collecting, and analyzing worm nature on end-hosts. In contrast, network-based detection systems detect worms initially by monitoring, collecting, and analyzing the scan traffic (messages to identify vulnerable computers) generated by worm attacks [1]. Since worms are venomous programs that follows on these computers, analyzing the behaviour of worm executables plays a important role in host-based detection systems. However, while exposurity exist and pose virus of large-scale damage, it is critical to also focus on network-based detection[4]. Host based detection systems are observe that the scan traffic in the hosts they are available. C-Worms identified and prevented whose main purpose is transmitting from one system to another system and damage the whole communication system.

The worms which is found by network based systems to use different approach. For scanning systems they use IP addresses and then try to spread themselves [8]. In the Internet there must be a specified condition to detect worms such as Cyber centre , network telescope and SANSISC. The detections systems can be spreads across WWW in order to successfully found the current existence of worms successfully. Such network based detection systems has ability of examine the scan traffic so worms and remembering them [8]. Besides the above detection schemes that are based on the global scan traffic monitor by detecting traffic abnormal behaviour, there are other worm detection and defence schemes like sequential hypothesis testing for detecting worm-infected computers and payload-based worm signature detection. Different plan of attack described in spite of above, we believe that detecting widely scanning abnormal behaviour continues to be a useful weapon against worms, and that, in practice, miscellaneous defence has advantages [1].

III. MODELLING OF C-WORM

3.1 C-WORM

The C-Worm camouflages its spreads by managing scan traffic volume during its propagation. The easiest way to control scan traffic volume is to randomly change the number of worm in case of conducting port scans. The modelling of C-Worm is based on our observations that have been made after some study. The C-worm block diagram is shown in fig. [9]



The primary research unveil that the C-Worm is different from other worms though it has similarities with normal worms. The ordinary worms perform scan traffic in order to duplicate themselves and also spreads from one system to another system in a network environment. The same is espouse by C-Worms also. However, there are two observations made clearly[10]. The first observation is that, the C-Worm scan traffic involves IP addresses and port numbers and scan traffic is not same from ordinary worms. In second observation, the difference between scan traffic of C-worms and ordinary worms is cannot find by detection of system in terms of frequency domain. In time domain they looks like same. The second observation also bring out that it is necessary to differentiate the C-Worm traffic from other worm's traffic only in frequency domain. The control parameter in our model is general in nature and its value is 1 indicating traditional worms and other value for C-Worms. The process of modelling camouflaging worm consisting following characteristics are followed [9].

- The traffic of C-worm is like non-worm traffic in terms of time domain. This means that the scan traffic of the normal worm and C-worm is same over a period of time.
- C-Worm does not show any tendency while its spreading so as to hide its presence effectively.
- The average traffic of Worm is adequate to model the C-Worm propagation model faster in order to cause rapid damage on the Internet [9].

3.2 PROPAGATION MODEL OF C-WORM

To study about the C-Worm, we take up the epidemic dynamic model for disease propagation, which has been extended to use for worm propagation modelling.

Since our inquire about C-Worm is a novel attack, we altered the real epidemic dynamic formula to model the propagation of the C-Worm by presenting the P(t)—the attack probability that a worm-infected computer participates in worm propagation at time t [1]. We notice that there is a broad scope to especially improve our updated model in the future to reflect some characteristics that are applicable in real- world practice Particularly, the epidemic dynamic model presumes that any given computer is in one of the following stages: immune, vulnerable, or infected. An immune computer is one that cannot be infected by a worm; a vulnerable computer is one that has the existing in possibility of being infected by a worm; an effected computer is one that has been effected by a worm [9]. C-Worm is not same propagation model as compared to traditional PRS worms due to its P(t) parameter.

$$\frac{dM(t)}{dt} = \beta . M(t) . [N – M(t)] \qquad (1)$$

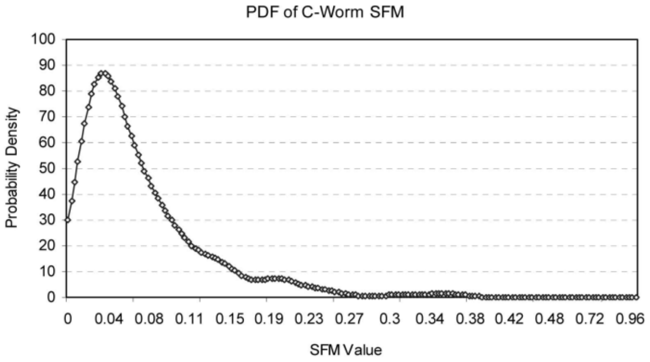
where M(t) is the number of effected computers at time t, N = (T . P1. P2) is the number of vulnerable computers on the Internet; T is the total number of IP addresses on the Internet; P1 is the ratio of the total number of computers on the Internet over T; P2 is the ratio of total number of susceptible to attacks on computers on the Internet over the total number of computers on the Internet; β = S/V is called the pair wise infection rate; and S is the scan rate known as the number of scans that an infected computer can run in a given time interval. We assume that at t = 0, there are M(0) computers being initially effected and N –M(0) computers being susceptible to further worm infection[1].

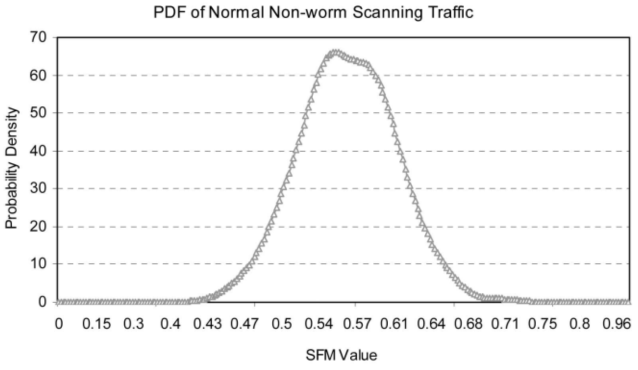
C-Worm has a different propagation model compared to traditional PRS worm due to its P(t) parameter. Consequently, Formula (1) needs to be also written as[9],

$$\frac{dM(t)}{dt} = \beta . M(t) . P(t) . [N – M(t)] \qquad (2)$$

3.3 EFFECTIVENESS OF C-WORM

The system has huge capacity in its working and detecting the C-Worm propagation. We get the veracious result in the form of graph and examine the infected instance number for the C-Worm and PRS Worm. It gives a elaborated report of infected ratio of the C-Worm and PRS Worm and also gives examined result of infected instance number for background scanning report by ISE in the form of graphs[9].





IV. PROPOSED METHOD (ALGORITHM)

In this proposed method mainly we can use two methods those are power spectral density (PSD) distribution of the scan traffic volume and its corresponding spectral flatness measure (SFM).

4.1 POWER SPECTRAL DENSITY(PSD)

Power Spectral Density is the apportioning of worm detection data require to transform from time domain to frequency domain. Using Power spectral Density sometimes interval is added and its correspond method Spectral Flatness Measure which scans the background traffic of C-worm and non worm traffic in that limited time period. PSD describes how the power of time series is distributed I the frequency domain [6]. we use a random process X(t); t €(0, n) to model the worm detection data. Assuming

X(t) is the source count in time period [t – 1] (t € [1,n])we define the autocorrelation of X(t) by [1],

$$Rx(L) = E [X(t) \ X(t + L)] \qquad (3)$$

In (3), Rx(L) is the correlation of worm detection data in an interval L.If a recurring conduct exists, a Fourier transform of the autocorrelation function of Rx(L) can bring out such demeanour. Thus, the PSD function of the scan traffic data is intended to using the Discrete Fourier Transform (DFT) of its autocorrelation function as follows [4]

PSD is a very useful tool to identify analogue signals in your time series data and want to know their amplitude. The concept and application of the power spectrum of a signal is fundamental in electrical engineering, particularly in electronic communication systems, including radio communications, radars, and related systems, plus passive [remote sensing] technology [6].

For every PSD the c-worm traffic shows less SFM and this is the proof that the camouflaging worm hides itself and when reported this is also known to others. The scan traffic of the C-worm could be based on the port number of IP address. Moreover, we also used many metrics such as DR (Detection Rate) and DT (Detection Time) and MIR (Maximal Infection Ratio) in order to measure the efficiency of the proposed schemes [6].

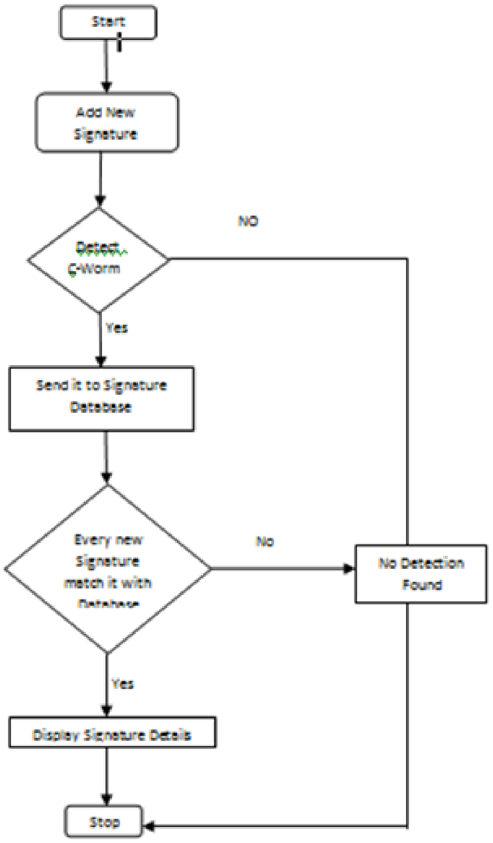
4.2 SPECTRAL FLATNESS MEASURE (SFM)

We measure the flatness of PSD to make out the scan traffic of the C-Worm from the normal non-worm scan traffic. For this, we bring the Spectral Flatness Measure (SFM) [4]. which can catch anomaly behaviour in certain range of frequencies. The SFM is known as the ratio of the geometric mean to the arithmetic mean of the PSD coefficients [6]. It can be declared as,

SFM is a widely existing measure for individual frequencies in different applications such as voiced frame sensing in speech recognition. In general, small values of SFM means that the concentration of data at minute frequencies spectrum ranges [9]. The C-Worm has non solutiable recurring behaviour in its scan traffic; accordingly its SFM values are relatively smaller than the SFM values of normal non worm scan traffic. To be applicable in detecting C-Worms, we present a sliding window to catch a observably higher concentrations at a small range of spectrum. When such observably concentration is accepted, we derive the SFM within a broad frequency range. In above figure we can notice that the SFM value for the C-Worm is very small (e.g., with a mean value of approximately 0.075) [1].

V. PROPOSED NEW ALGORITHM

1. Collect logs from distributed monitors over internet
2. in SDF, find out the detection count over IP addresses.
3. Define the geometric mean
4. Define an arithmetic mean
5. Find the ratio of geometric mean and arithmetic mean of the PSD coefficients
6. Compare values of ratio as SFM with other SFM value.


Start
Add New Signature
Detect C-Worm
NO
Yes
Send it to Signature Database
Every new Signature match it with Database
No
No Detection Found
Yes
Display Signature Details
Stop

VI. CONCLUSION

In this Review paper, 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 analysis and evaluation showed that, although the C-Worm successfully camouflages its spreads in the time domain, its camouflaging nature inevitably manifests as a distinct pattern in the frequency domain. Based on observation, we developed an algorithm to detect the C-Worm. Thus through this paper we have given effective methods to detect the C-Worm and recover the network from C-Worm.

REFERENCES

[1] Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao, Fellow, IEEE Modeling and Detection of Camouflaging Worm VOL. 8, NO. 3, MAY/JUNE 2011

[2] Xiaojun Tong, Miao Zhang, Zhu Wang, Hui Xu, Yang Liu A Novel Anomaly Detection Method for Worms

[3] JEEVAAKATIRAVAN, D.HEMAPRIYADHARSHINI, C.CHELLAPAN, R.DHANALAKSHMI A Novel Approach For Detecting Smart Camouflaging Worm 20th January 2013. Vol. 47 No.2

[4] Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao On Detecting Camouflaging Worm 2006.

[5] Prof. Chavan M.K, Madane P.V Modelling and Detection of Camouflaging worms- A Survey volume 2 Issue 10 October 2012

[6] M.Nagendramma, P.Eswarai, Sk. Ghouse Basha, K.Suma Anusha Modeling and Detection of Cancealing worm Volume 2, Issue 12, December 2012.

[7] Zesheng chen, Lixin Gao, Kevin kwiat Modeling the spread of Active worms IEEE INFOCOM 2003

[8] Michele Garetto, Weibo Gang, Don Towsley Modeling Malware Spreading Dynamics IEEE INFOCOM 2003

[9] Aruna.A , Perumal.S , Dr. A. Muthukumaravel Modeling and detection of Camouflaging Worm Using SDF Volume 2, Issue 4, July 2013

[10] Sushma Mergu, G.Dileep Kumar C-worm Traffic Detection using Power Spectral Density and Spectral Flatness Measure Volume 4, Issue 3 (Sep-Oct. 2012)