Modeling and Detection of Disguising Worm

[1]S.Hima Bindu
M.Tech Student
CSE Department
Prakasam Engg College
Kandukur, AP.

[2]K.Srujana
Associate. Professor
CSE Department
Prakasam Engg College
Kandukur, AP.

[3]S.Sreenivasulu
Head of the Department
CSE Department
Prakasam Engg College
Kandukur, AP.

Abstract

As Internet and its technologies are improving with rapid pace, there are security threats growing with same pace. The malicious software such as worm is causing such threats to IT systems linked to information super highway. A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Computer virus or Worm can spread to hard disk whenever an infected computer program or system is used and the uninfected disk is accessed.

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. 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.

Index Terms—Worm, camouflage, Anomalydetection, PSD, SFM.

1. Introduction

Traditional Worms are more threats to the Internet and also would produce lot of Overall Network Traffic. It is very easy to identify the Traditional Worm as it increases the Overall Traffic of the Network Significantly. If a system is affected by worm it is cleared by using antivirus software. But if the operating system of a system gets affected by worm it is impossible to clear it. So we use special technique called spectrum based method to detect the worm and control the worm using Discrete Mathematical model. In most of the existing system, when an operating system is affected by a worm it has to be formatted and a new operating system should be installed. If worm were found out and cleared user might not know about the source node which sent the worm file. This is major disadvantage in the existing systems.

The proposed system models the camouflaging worm (C- Worm), in which the behavior is hidden and its action is implicitly kept secret. So this process of detecting the c-worm is not possible using the usual traditional worm detection techniques as well as ip trace back systems. C- Worm is it scans all the ip present in the network first then identifies the number of protected systems, number of worm affected systems, and number of vulnerable systems. C-Worm rather focusing all the ip, instead it focuses only the vulnerable systems, because thesesystems are the target of c-worm.

Many real-world worms have caused notable damage 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:

1. Launch massive Distributed Denial-of-Service (DDoS) attacks that disrupt the Internet utilities [5],
2. Access confidential information that can be misused [6] through large-scale traffic sniffing, key logging, identity theft, etc.,
3. Destroy data that has a high monetary value and
4. Distribute large-scale un solicited advertisement Emails (as spam) or software.

Nevertheless, the attackers are crafting attack strategies that intend to defeat existing worm detection systems. In particular, "stealth" is one attack strategy used by a recently discovered active worm called "Atak" worm [7] and the "self-stopping" worm [8] circumvent detection by hibernating with a predetermined period.

Camouflage worm is modeled and spectrum based approach is used for the detection of C-Worm. The project 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 and effectively detecting not only the C-Worm, but traditional worms as well and prevention of C-Worm using mathematical model with particular references of C-Worm.

2. Proposed Method

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

2.1 Power Spectral Density

Power Spectral Density the distribution of worm detection data need to transform from time domain to frequency domain. The C-worm is modeled in such a it increases the CPU usage memory. Using Power spectral Density some time period is added and its correspond method Spectral Flatness Measure which scans the background traffic of C-worm and non worm traffic in that specified time period. PSD describes how the power of time series is distributed I the frequency domain. The SFM of PSD is defined as the ratio of geometric mean to arithmetic mean of the coefficient of PSD. In statistical signal processing and physics, the spectraldensity, power spectral density (PSD), or energy spectral density (ESD), is a positive real function of a frequency variable associated with a stationary stochastic process, or a deterministic function of time, which has dimensions of power per hertz (Hz), or energy per hertz. It is often called simply the spectrum of the signal. Intuitively, the spectral density measures the frequency content of a stochastic process and helps identify periodicities.

PSD is a very useful tool it identify oscillatory signals in your time series data and want to know their amplitude. For example let assume the operating a factory with many machines and some of them have motors inside. It detects un wanted vibrations from somewhere. It might be able to get a clue to locate offending machines by looking at PSD which would give you frequencies of vibrations. PSD is still useful even if data do not contain any purely oscillatory signals. For example, the sales data from an ice-cream parlor, you can get rough estimate of summer sales peak by looking at PDF of your data. The quite often compute and plot PSD to get a "feel" of data at an early stage of time series analysis. Looking at PSD is like looking at simple time series plot except that we look at time series as a function of frequency instead of time. Here, it could say that frequency is a transformation of time and looking at variations in frequency domain is just another way to look at variations of time series data. PSD tells that at which frequency ranges variations are strong and that might be quite useful for further analysis. The concept and use of the power spectrum of a signal is fundamental in electrical engineering, especially in electronic communication systems, including radio communications, radars, and related systems, plus passive [remote sensing] technology.

For every PSD the c-worm traffic shows less SFM and this is the evidencethat the camouflaging worm hides itself and whenreported this is known to others as well. The scan traffic of the C-worm could be based on the port number of IP address. It uses both based on the requirement. The experiments reveal that our schemes are effective whencompared with many existing worm detection systems. Moreover, we also used many metricssuch as DR (Detection Rate) and DT (Detection Time) and MIR (Maximal Infection Ratio) in order to evaluate the efficiency of the proposed schemes.

2.2 Spectral Flatness Measure (SFM)

We measure the flatness of PSD to distinguish the traffic of the C-Worm from the normal non-worm scan traffic. For this, we introduce the SFM, which can capture anomaly behavior in certain range of frequencies. The SFM is defined as the ratio of the geometric mean to the arithmetic mean of the PSD coefficients[9]. SFM is a widely existing measure discriminating frequencies in various applications, such as voiced frame detection in speech recognition [9].

In general, small values of SFM imply the concentration ofdata at narrow frequency spectrum ranges. Note that the 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. To be useful in detecting C-Worms, we introduce a sliding window to capture a noticeably higher concentration at a small range of spectrum. The SFM fig shown below

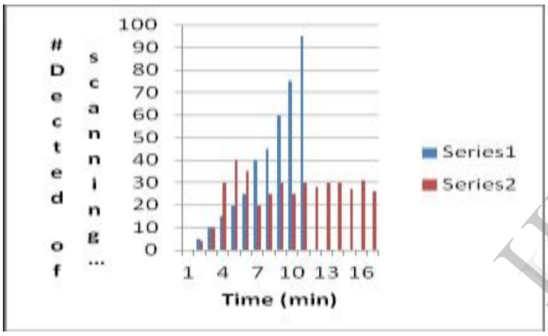


Fig. 1: PDF of SFM on normal non-worm traffic

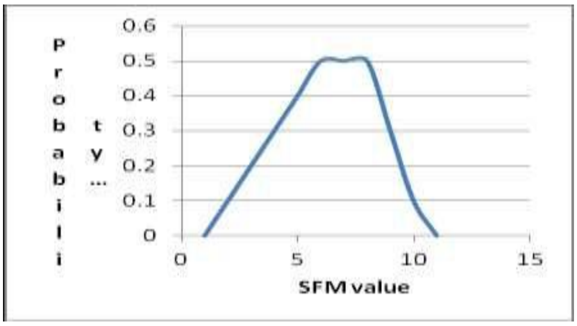


Fig. 2: Number of Detected Scanning Hosts on C Worm

3. System Architecture

3.1 C-worm

Camouflaging Worm (C Worm).The C-Worm has thecapability to intelligently manipulate its scan traffic volume over time, there by camouflaging its propagation from existing worm detection systems. The C-Worm has a self-propagating behavior similar to traditional worms, i.e, it intends to rapidly infect as many vulnerable computers as possible. However, the C Worm is quite different from traditional worms in which it camouflages any noticeable trends in the number of infected computers over time. The camouflage is achieved by manipulating the scan traffic volume of worm-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 detection schemes.

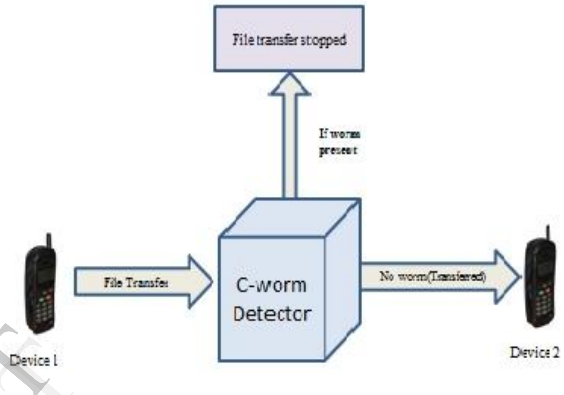


Figure.3 Block diagram of worm detection system

Fig.3 shows the block diagram of worm detection system. It consists of c-worm detector , devices .The device1 will start sending files to device2 ,while transferred c-worm detector is in between them ,which will check the existence of worm , if present stop sending files else send it to other device 2.c worm detector is main system which will wok based on various data mining algorithms of classification. This paper investigates new techniques to detect worms. Initially at first when worm will start affecting, it will find target first in order to attack or spread itself. Once target is find out, it will start propagation by using either any technique of propagation. So device 1 will transfer a file to c-worm detector module.

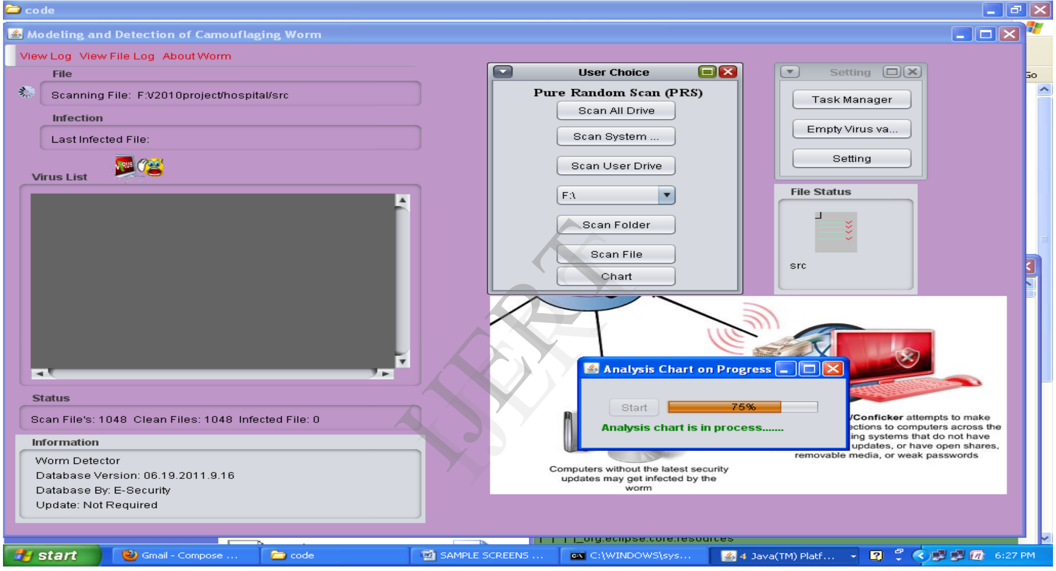
This module will detect the worm, if there is no worm, it will directly pass file to device 2, otherwise if worm is present, it will stop transfer of file. Here In this paper new spectrum based detection scheme is introduced. It consists of Centralized data center, Monitor, User. The data center will collect all traffic logs from various network monitors foridentifying worms by their own IP address. The monitors will record all traffic and send it to data center when needed. The data center will collect traffic logs from monitors across internet. The data center then analyzes collected traffic logs and publishes reports to system users.

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 extensively used for worm propagation modeling [10], [11]. Based on existing results [10], [11], this model matches the dynamics of real-worm propagation over the Internet quitewell. 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 characteristics that are relevant in real-world practice.

4. Result Analysis

Worm scan traffic volume in the open-loop control system will expose a much higher probability to show 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 C-worm as a worst case attacking scenario that uses a closed loop control for regulating the propagation speed based on the feedback propagation status.



Scanning File: F:V2010project/hospital/src

Last Infected File:

Scan File's: 1048 Clean Files: 1048 Infected File: 0

Worm Detector
Database Version: 06.19.2011.9.16
Database By: E-Security
Update: Not Required

Analysis chart is in process.......

/Conficker attempts to make ...ctions to computers across the ...ing systems that do not have updates, or have open shares, removable media, or weak passwords

Computers without the latest security updates may get infected by the worm

Fig 4: Progressing Analysis Chart

Worms are malicious programs that execute on these computers, analyzing the behavior of worm executables plays an important role in host based detection systems. Many detection schemes fall under this category. In contrast, network-based detection systems detect worms primarily by monitoring, collecting, and analyzing the scan traffic (messages to identify vulnerable computers) generated by worm attacks. Many detection 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, while vulnerabilities exist and pose threats of large-scale damage, it is critical to also focus on network-based detection, as this paper does, to detect wide spreading worms.

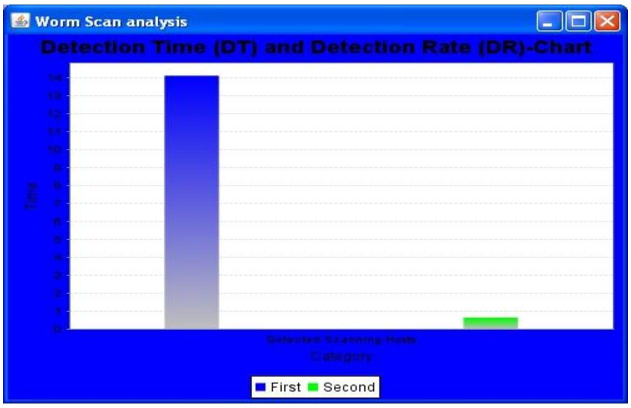


Fig 5: Analysis Chart Comparing Detection Time &Detection Rate

5. Conclusion

We have identified the characteristics of existing and hypothetical worms during the target finding and propagation phase of a worm's life cycle. They are classified based on target finding, propagation, transmission scheme, and payload format. Current detection algorithms are organized based on the categories of signature-based, anomaly-based, or hybrid. We have evaluated the categories against worm characteristics. We have classified current containment schemes based on the methods they use to control the spread of worms. We have also explored the implementations of detection and containment at different network locations and system scopes. Different detection schemes are useful at different levels of implementation. So far, there is no ultimate solution to deal with all existing and hypothetical worms. New attack technologies are being developed every day, and the threat constantly exists.

C-Worm has the capability to camouflage its propagation and further avoid the detection. 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, develop a novel spectrum based detection scheme to detect the C-worm. To perform an evaluation data showing a scheme to achieve superior detection performance against the c-worm in comparison with existing representative detection schemes and to prevent C-worm using mathematical models.

References:

[1] D. Moore, C. Shannon, and J. Brown, "Code-Red: A Case Study on the Spread and Victims of an Internet Worm," Proc. Second Internet Measurement Workshop (IMW), Nov. 2002.

[2]D. Moore, V. Paxson, and S. Savage, "Inside the Slammer Worm," Proc. IEEE Magazine of Security and Privacy, July 2003.

[3] CERT, CERT/CC Advisories, http://www.cert.org/advisories/, 2010.

[4] P.R. Roberts, Zotob Arrest Breaks Credit Card Fraud Ring, www.eweek.com/article2/0,1895,1854162,00.asp, 2010.

[5]W32/MyDoom.B Virus,http://www.uscert.gov/cas/techalerts/TA04-028A.html, 2010.

[6]W32.Sircam.Worm@mm,http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html, 2010.

[7] Zdnet, Smart Worm Lies Low to Evade Detection,http://news.zdnet.co.uk/internet/security/0,39020375,39160285,00.htm, 2010.

[8] J.Ma,G.M. Voelker, and S. Savage, "Self-Stopping Worms,"Proc.ACM Workshop Rapid Malcode (WORM), Nov. 2005.

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

[10] A survey of internet worm detection and containment

[11] D. Moore, V.P axsonand S. Savage, Inside the slammer worm,‖ 2003,vol. 1, pp. 33-39.