On Detecting Camouflaging Worm

Wei Yu[1], Xun Wang[2], Prasad Calyam[3], Dong Xuan[2], and Wei Zhao[1]
[1] Dept. of Computer Science, Texas A&M University,
College Station, TX 77843
{weiyu, zhao}@cs.tamu.edu
[2] Dept. of Computer Science and Engineering,
The Ohio State University, Columbus, OH 43210
{wangxu, xuan}@cse.ohio-state.edu
[3] OARnet, The Ohio State University,
Columbus, OH 43210
pcalyam@oar.net

Abstract

Active worms pose major security threats to the Internet. In this paper, we investigate a new class of active worms, i.e., Camouflaging Worm (C-Worm in short). The C-Worm has the capability to intelligently manipulate its scan traffic volume over time, thereby camouflaging its propagation from existing worm detection systems. We analyze characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and non-worm 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 non-worm traffic. We conduct extensive performance evaluations on our proposed detection scheme against the C-Worm. The performance data clearly demonstrates that our proposed scheme can effectively detect the C-Worm propagation.

1 Introduction

An active worm refers to a malicious software program that propagates itself on the Internet to infect other hosts. The propagation of the worm is based on exploiting vulnerabilities of hosts on the Internet. Many real worms have posed much 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]. Since worms may infect a large number of hosts in a relatively short period of time, worms could potentially be used to: (i) launch massive Distributed Denial of Service (*DDoS*) attacks that disrupt the Internet utilities [4], (ii) access confidential information that can be abused [5], and (iii) destroy data that has a high monetary value [6]. There is even evidence showing infected hosts are being rented out as "Botnets" for attacks on Internet e-businesses [7].

Due to the substantial damage caused by worms in the past years, there have been significant efforts on developing defense mechanisms against worms. Detection of worms is one of the most important tasks in defense against them, which usually is based on the behavioral features of worms. The typical self-propagating behavior of a traditional worm can be described as follows: After a worm instance identifies and infects a vulnerable host on the Internet, this newly infected host [1] will automatically scan the IP addresses to identify other vulnerable hosts and infects them in a similar manner. Most existing detection schemes are based on a tacit assumption that each worm infected host keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been widely believed that the worm scan traffic volume and the worm infected host number show exponentially increasing patterns [2][8][9][10][11]. However, worms are evolving and some recently seen smart-worms contradict such assumption by reducing their propagation speed to avoid detection. For instance, the "Atak" worm attempts to avoid detection by hibernating (i.e., with-holding propagation) during its propagation. The smart-worms that adopt attack strategies similar

[1] In this paper, we interchangeably use the terms - *worm infected host* and *worm instance*.

to that of the "Atak" worm could collectively cause serious damage on the Internet without being detected. Therefore, it is very important to understand such smart-worms in order to defend against them.

In this paper, we conduct a systematic study on a new class of such smart-worms denoted as *Camouflaging Worm* (C-Worm in short). The C-Worm has a self-propagating behavior similar to traditional worms, i.e., it intends to rapidly infect as many vulnerable hosts as possible. However, the C-Worm is quite different from traditional worms in a way that it camouflages any noticeable trends in the number of infected hosts over time. The camouflage is achieved by manipulating the scan traffic volume of worm infected hosts. 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 worm detection schemes [12][13][14]. We note that the propagation controlling nature of the C-Worm (and similar smart-worms such as "Atak") cause a slow down in the propagation speed. However, by carefully controlling its scan rate, the C-Worm can still achieve its ultimate goal of infecting as many hosts as possible before being detected.

We comprehensively analyze the propagation model of C-Worm in both time and frequency domains. We observe that although the C-Worm scan traffic shows no noticeable trends in the time domain, it demonstrates a distinct pattern in the frequency domain. Specifically, there is an obvious concentration within a narrow range of frequencies. This concentration within a narrow range of frequencies is inevitable since the C-Worm adapts to the dynamics of the Internet in a recurring manner for manipulating its overall scan traffic volume. The above recurring manipulations involve steady increase followed by a decrease in the scan traffic volume, such that the changes do not manifest as any trends in the time domain or such that the scan traffic volume does not cross thresholds that could reveal the C-Worm propagation.

Based on above observation, we adopt frequency domain analysis techniques and develop a detection scheme against wide-spreading of the C-Worm. Particularly, we develop a novel spectrum-based detection scheme that uses the *Power Spectral Density* (*PSD*) distribution of scan traffic volume in the frequency domain and its corresponding *Spectral Flatness Measure* (*SFM*) to distinguish the C-Worm traffic from non-worm traffic (background traffic). Our frequency domain analysis studies use the real-world Internet traffic trace provided by SANs Internet Storm Center (*ISC*) [15] [2]. Our results reveal that the non-worm traffic (e.g. port-scan traffic for port 80, 135 and 8080) has relatively larger *SFM* values for their *PSD* distributions. Whereas, the C-Worm traffic shows comparatively smaller *SFM* value for its respective *PSD* distribution.

Furthermore, we demonstrate the effectiveness of our spectrum-based detection scheme in comparison with existing worm detection schemes. Our evaluation data clearly demonstrate that our spectrum-based detection scheme achieves much better detection performance against the C-Worm propagation compared with existing detection schemes.

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

2 Background and Related Work

2.1 Worm Behavior

The basic form of active worms is the Pure Random Scan (PRS) worm, where a worm infected host continuously scans a set of random Internet IP addresses to find new vulnerable hosts. There are several variants of the PRS worm such as local subnet scan worm [10] and hit-list scan worm [9]. Both of these worms attempt to speed up their propagation by increasing the probability of successful scanning. However, it is hard to achieve large scale of worm propagation using pure local subnet scan or hit-list scan strategy due to their limitations in finding large number of vulnerable hosts. Consequently, PRS scan strategy is still widely adopted in worms and other strategies are used to speed up the worm propagation at different stages during the propagation.

To analyze the C-Worm, we adopt the epidemic dynamic model for disease propagation, which has been extensively used for worm propagation modeling [2][8][10]. Particularly, the epidemic dynamic model assumes that any given host is in one of the following states: immune, vulnerable, or infected. An immune host is one that cannot be infected by a worm; a vulnerable host is one that has the potential of being infected by a worm; an infected host is one that has been actually infected by a worm. The simple epidemic model for a finite population of traditional PRS worms can be expressed as,

$$\frac{dM(t)}{dt} = \beta \cdot M(t) \cdot [N - M(t)], \tag{1}$$

where $M(t)$ is the number of infected hosts at time t; $N(= T \cdot P_1 \cdot P_2)$ is the number of vulnerable hosts on the Internet; T is the total number of IP addresses on the Internet; P_1 is

[2] *ISC* monitors and collects port-scan traffic data from around 1 million IP addresses spanning several thousands of organizations in different geographical regions.

Table 1. Notations

Notation	Definition
T	Total number of IP addresses on the Internet
N	Total number of vulnerable hosts on the Internet
S	Average scan rate of a worm infected host (Number of scans that a worm infected host can launch in a unit time interval)
$P(t)$	The attack probability that a worm infected host participates in worm propagation at time t
PRS	Pure Random Scan (worm infected hosts continuously scan randomly selected Internet IP addresses to find new vulnerable hosts)
β	The pairwise scan rate of worm propagation (e.g., $\beta = \frac{S}{T}$)
P_1	Probability that an arbitrary IP address is assigned to a host on the Internet
P_2	Probability that an arbitrary host on the Internet is vulnerable to worm infection
P_m	Ratio of the number of IP addresses monitored by the worm detection system to the total number of Internet IP addresses
$M(t)$	Number of infected hosts at time t on the Internet
$M_A(t)$	The number of observed worm instances by the worm detection system at time t
M_C	Control setting for the C-Worm to manipulate overall scan traffic volume
$\bar{M}(t)$	Estimation of $M(t)$ at time t
$X(t)$	Random variable representing the number of unique source IP address in the scan traffic at time t
W_s	Detection sampling window
W_d	Detection sliding window including q continuous detection sampling windows
$R_X[L]$	Auto-correlation of worm detection time series of length L
PSD	Power Spectral Density
SFM	Spectral Flatness Measure, i.e., the ratio of geometric mean to arithmetic mean of the PSD coefficients
$\psi(R_X[L])$	PSD (power spectral density) as *Discrete Fourier transform* of auto-correlation $R_X[L]$

the ratio of the total number of hosts on the Internet over T; P_2 is the ratio of total number of *vulnerable* hosts on the Internet over the total number of hosts on the Internet; $\beta = \frac{S}{T}$ is called the pairwise infection rate [16]; S is the scan rate defined as the number of scans that an infected host can launch in a given time interval. We assume that at $t = 0$, there are $M(0)$ hosts being initially infected and $N - M(0)$ hosts being susceptible to further worm infection. Table 1 lists all the important notations used in this paper.

2.2 Worm Detection

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 [15][17]. 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 [13]. Some of these schemes use the *variance* of traffic volume [14] or the exponentially increasing *trend* of traffic volume [12] 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 [18], DSC (Destination-Source Correlation) for detecting a worm in local networks [19], content-based worm signature [20]. In contrast, our spectrum-based detection scheme uses frequency domain analytical techniques to capture the wide-spreading worm propagation.

3 Modeling of C-Worm

3.1 C-Worm

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* $P(t)$ for each worm instance. $P(t)$ is the probability that a C-Worm instance participates in the worm propagation (i.e., scans and infects other hosts) at time t. Our C-Worm model with the control parameter $P(t)$ is generic. $P(t) = 1$ represents the cases for traditional worms, where all worm instances actively participate in the propagation. For the C-Worm, $P(t)$ need not be a constant value and can be set as a time varying function.

In order to achieve its camouflaging behavior, the C-Worm needs to obtain an appropriate $P(t)$ to manipulate its scan traffic. Specifically, the C-Worm needs to regulate its overall scan traffic volume such that: (i) it is similar to non-worm scan traffic in terms of the scan traffic volume over time, (ii) its does not exhibit any notable trends such as an exponentially increasing pattern or any mono-increasing pattern even when the number of infected hosts is (exponentially) increasing over time, and (iii) the average value of the overall scan traffic volume is sufficient to make the C-Worm propagate fast enough in order to cause rapid damage on the Internet.

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 with mean $\bar{M}_C$. This $\bar{M}_C$ can be regulated in a random fashion during the worm propagation in order to camouflage the propagation of C-Worm. Correspondingly, the worm instances need to adjust their attack probability $P(t)$ in order to ensure that the total number of worm instances that launch the scans is approximately $\bar{M}_C$.

To regulate $\bar{M}_C$, it is obvious that $P(t)$ has to be decreased over time since $M(t)$ keeps increasing during the worm propagation. We can express $P(t)$ using a simple function as follows: $P(t) = \frac{\bar{M}_C}{\bar{M}(t)}$, where $\bar{M}(t)$ represents the estimation of $M(t)$ at time t. From the above expression, we know that the C-Worm needs to obtain the value of $\bar{M}(t)$ (as close to $M(t)$ as possible) in order to generate an effective $P(t)$. Here we discuss one approach for the C-Worm to estimate $M(t)$. The basic idea is as follows: A C-Worm could estimate the percentage of hosts that have already been infected over the total number of IP addresses as well as $M(t)$, through checking a scan attempt is a *new hit* (i.e., hitting an uninfected vulnerable host) or a *duplicate hit* (i.e., hitting an already infected vulnerable host). This method requires each worm instance (i.e., infected host) to be marked by a watermark which indicates that this host has been infected. Thus, when a worm instance (say for example, host *A*) scans one infected host (say for example, host *B*), then the host *A* will detect such watermark, and thereby know that host *B* has been infected. Through checking such watermarks during the propagation, a C-Worm infected instance can estimate $M(t)$. This method is similar to the one used by the self-stopping worm [21].

3.2 Propagation Model of C-Worm

C-Worm has a different propagation model compared to traditional PRS worms because of its $P(t)$ parameter. Consequently, Formula (1) needs to be rewritten as,

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

Recall that $P(t) = \frac{\bar{M}_C}{\bar{M}(t)}$, $\bar{M}(t)$ is the estimation of $M(t)$ at time t, and assuming that $\bar{M}(t) = (1+\epsilon) \cdot M(t)$, where ϵ is the estimation error, the Formula (2) can be rewritten as,

$$\frac{dM(t)}{dt} = \frac{\beta \cdot \bar{M}_C}{1+\epsilon} \cdot [N - M(t)]. \qquad (3)$$

With Formula (3), we can derive the propagation model for C-Worm as $M(t) = N - e^{-\frac{\beta \cdot \bar{M}_C}{1+\epsilon} \cdot t}(N - M(0))$, where $M(0)$ is the number of infected worm instances at time 0. Assume that the worm detection system can monitor P_m ($P_m \in [0, 1]$) of the whole Internet IP address space. The probability that at least one scan from a worm infected host (it generates S scans in unit time on average) will be observed by the detection system is $1 - (1 - P_m)^{P(t) \cdot S}$. We define that $M_A(t)$ is the number of worm instances that have been observed by the worm detection system at time t, then there are $M(t) - M_A(t)$ unobserved infected instances at time t. At the worm propagation early stage,

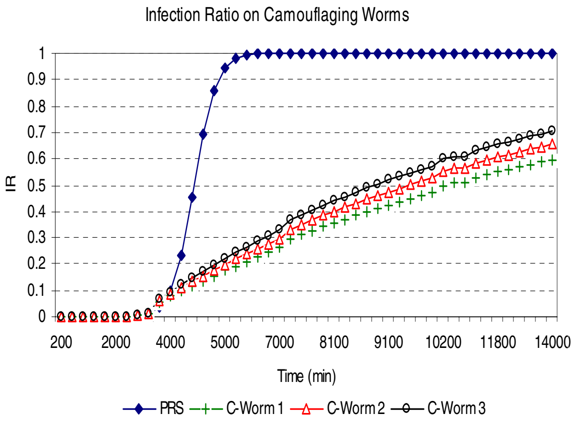

Figure 1. Infected ratio for C-Worm and PRS worm

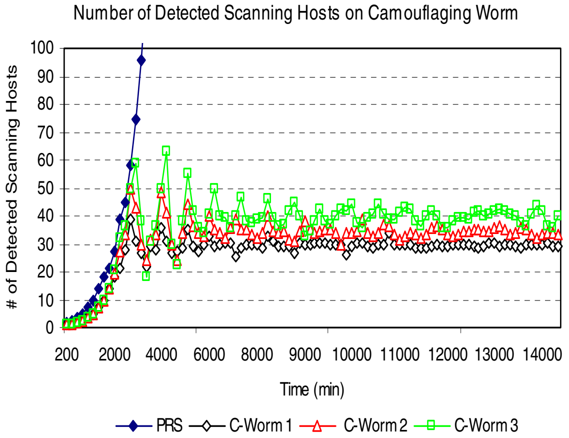

Figure 2. Observed infected instance number for C-Worm and PRS worm

$M(t) - M_A(t) \simeq M(t)$. The expected number of newly observed infected instances at $t + \delta$ (where δ is the interval of monitoring) is $(M(t) - M_A(t)) \cdot [1 - (1 - P_m)^{P(t) \cdot S}] \simeq M(i)[1 - (1 - P_m)^{P(t) \cdot S}]$. Thus, we have $M_A(t + \delta) = M_A(t) + M(t)[1 - (1 - P_m)^{P(t) \cdot S}]$. Using simple mathematical substitutions, the number of worm instances observed by the worm detection system at time t is,

$$M_A(t) = P(t) \cdot M(t) \cdot P_m = \frac{P_m \cdot \bar{M}_C}{1 + \epsilon}. \qquad (4)$$

3.3 Effectiveness of C-Worm

We now demonstrate the effectiveness of C-Worm in evading worm detection through controlling $P(t)$. We define the worm *Infection Ratio* (IR) as the ratio of the number of infected hosts over the total number of vulnerable hosts. Given random selection of $\bar{M}_c$, we generate three C-Worm attacks (viz., C-Worm 1, C-Worm 2 and C-Worm 3) that are characterized by different selections of mean and variance magnitudes for $\bar{M}_C$. In our simulations, we assume that the scan rate of 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 hosts on the Internet as $360,000$ which is the total number of infected hosts in “Code-Red” worm propagation [1].

Fig. 1 shows the infection ratio for the PRS worm and the above three C-Worm attacks. Fig. 2 shows the observed number of worm instances over time for the PRS worm and the above three C-Worm attacks. These simulations are for a worm detection system discussed in Section 2.2 that covers a 2^{20} IPv4 address space on the Internet. The reason for choosing 2^{20} IP addresses as the coverage space of the worm detection system is due to the fact that the SANs *Internet Storm Center* (ISC) has similar coverage space [15]. For the C-Worm, the trend of observed number of worm instances over time ($M_A(t)$) (defined in Formula (4)) is much different from that of the traditional PRS worm as shown in Fig. 2. This clearly demonstrates how the C-Worm successfully camouflages its increase in the number of worm instances ($M_A(t)$) and avoids detection by worm detection systems that expect exponential increases in worm instance numbers during large-scale worm propagation.

From above Figs. 1 and 2, we also observe that the C-Worm is still able to maintain a certain magnitude of scan traffic so as to cause significant infection on the Internet. As a note regarding the speed of C-Worm propagation, we can observe from Fig. 1 that the C-Worm takes around 10 days to infect 75% of total vulnerable hosts in comparison with the 3.3 days taken by a PRS worm. Hence, the C-Worm could potentially adjust its propagation speed such that it is still effective in causing wide-spreading propagation, while avoiding being detected by the worm detection schemes.

The C-Worm shares similarity with other stealthy port-scan attacks. Such attacks find out available services on a target system, while trying to avoid detection [22][23]. They slow down the port-scan rate and hide the origin of the attacker. Due to the nature of self-propagation, the C-Worm has to use more sophisticated mechanisms to manipulate the scan traffic volume over time in order to avoid detection. The stealth port-scan attacks were only briefly discussed in [22][23], while we comprehensively study the C-Worm modeling and its detection in this paper. We discussed the “Atak” worm in Section 1 and mentioned that it is similar to the C-Worm since it tries to avoid detection, when it suspects it is being detected by anti-worm software. However, the “Atak” worm differs from the C-Worm because, it at-

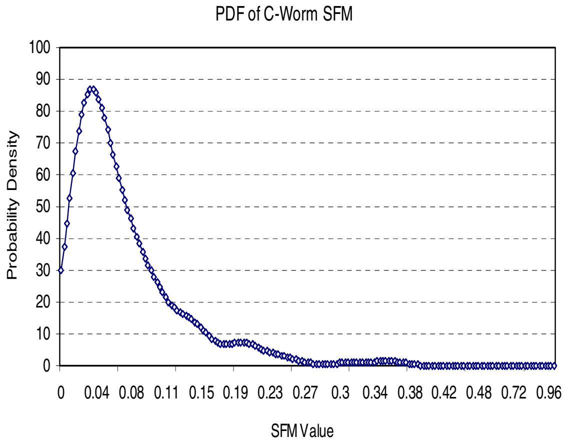

Figure 3. PDF of SFM on C-Worm traffic

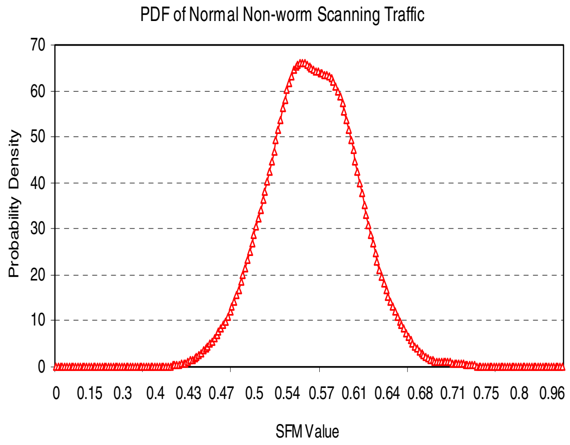

Figure 4. PDF of SFM on normal non-worm traffic

tempts to hide itself only when it suspects its propagation will be detected by anti-worm software. Whereas, the C-Worm proactively camouflages itself *all the time* during its propagation.

4 Detecting the C-Worm

4.1 Design Rationale

In this section, we develop a novel *spectrum-based detection scheme*. Recall that the C-Worm goes undetected by detection schemes that try to determine the worm propagation only in the time domain. Our detection scheme captures the distinct pattern of the C-Worm in the frequency domain, and thereby has the potential of effectively detecting the C-Worm propagation.

In order to identify the C-Worm 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. In our case, the time series corresponds to the changes in the number of worm instances that actively conduct scans over time. The *SFM* of *PSD* is defined as the ratio of *geometric mean* to *arithmetic mean* of the coefficients of *PSD*. The range of *SFM* values is $[0,\ 1]$ and a larger *SFM* value implies flatter *PSD* distribution and vice versa.

To illustrate *SFM* values of both the C-Worm and normal non-worm scan traffic, we plot the *Probability Density Function* (PDF) of *SFM* for both C-Worm and normal non-worm scan traffic as shown in Figs. 3 and Fig. 4, respectively. The normal non-worm scan traffic data shown in Fig. 4 is based on real-world traces collected by the *ISC* [3]. Note that we only show the data for port 8080 as an example, and other ports also show similar observations. From this figure, we know that the *SFM* value for normal non-worm traffic is very small (e.g., *SFM* $\in (0.02,\ 0.04)$ has much higher density compared with other magnitudes). The C-Worm data shown in Fig. 3 is based on 800 C-Worms attacks generated by varying attack parameters defined in Section 3 such as $P(t)$ and $M_c(t)$. From this figure, we know that the *SFM* value of the C-Worm attacks is high (e.g., *SFM* $\in 0.5,\ 0.6$ has high density). From the above two figures, we can observe that there is a clear demarcation range of *SFM* $\in (0.3,\ 0.38)$ between the C-Worm and normal non-worm scan traffic. As such, the *SFM* can be used to sensitively detect the C-Worm scan traffic.

The large *SFM* values of normal non-worm scan traffic can be reasoned with the following fact. The normal non-worm scan traffic does not tend to concentrate at any particular 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 frequency of C-Worm scan traffic is within a narrow-band. 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. In reality, the above recurring manipulations involve steady increase followed by a decrease in the scan traffic volume.

4.2 Spectrum-based Detection Scheme

We now present the details of our spectrum-based detection scheme. Similar to other detection schemes [14][12], we use a “source count” as the basis for worm detection in

[3] The traces used in this paper contain log files which have over 100 million records and the total size exceeds 40 GB.

our spectrum-based detection scheme. The "source count" is the number of the unique sources that launch scans during worm propagation. To understand how the source count data is obtained, we recall that, a worm detection system collects logs from distributed monitors across the Internet. With reports in a sampling window W_s, the source count $X(t)$ is obtained by counting the unique source IP addresses in received logs.

In our spectrum-based detection scheme, the distribution of *PSD* and its corresponding *SFM* are used to distinguish the C-Worm scan traffic from the non-worm scan traffic. In our worm detection scheme, the detection data (e.g., source counter), is further processed in order to obtain its *PSD* and *SFM*. In the following, we give the detail about how the *PSD* and *SFM* are determined during the processing of the detection data.

To conduct spectrum analysis, we consider a detection sliding window W_d in the worm detection system. W_d consists of q (> 1) continuous detection sampling windows and each sampling window lasts W_s. The detection sampling window is the unit time interval to sample the detection data (e.g., the source count). Hence, at time i, within a sliding window W_d, there are q samples denoted by $(X(i-q-1), X(i-q-2), \ldots, X(i))$, where $X(i-j-1)$ $(j \in (1,q))$ is the $j-th$ source count from time $i-j-1$ to $i-j$.

4.2.1 Power Spectral Density (PSD)

To obtain the *PSD* distribution for worm detection data, we need to transform data from the time domain into the frequency domain. To do so, we use a random process $X(t), t \in [0,n]$ to model the worm detection data. Assuming $X(t)$ is the source count in time period $[t-1,t]$ $(t \in [1,n])$, we define the auto-correlation of $X(t)$ by

$$R_X(L) = E[X(t)X(t+L)]. \tag{5}$$

In Formula (5), $R_X(L)$ is the correlation of worm detection data in an interval L. If a recurring behavior exists, a *Fourier* transform of the auto-correlation function of $R_X(L)$ can reveal such behavior. Thus, the *PSD* function (also represented by $S_X(f)$; where f refers to frequency) of the scan traffic data is determined using the Discrete Fourier Transform (*DFT*) of its auto-correlation function as follows,

$$\psi(R_X[L], K) = \sum_{n=0}^{N-1} (R_X[L]) \cdot e^{-j2\pi Kn/N}, \tag{6}$$

where $K = 0, 1, \ldots, N-1$.

As the *PSD* inherently captures any recurring pattern in the frequency domain, the *PSD* function shows a comparatively even spread across a wide spectrum range for the normal non-worm scan traffic. Whereas, the *PSD* of C-Worm scan traffic shows spikes or noticeably higher concentrations at a certain range of the spectrum.

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. For this, we introduce the *Spectral Flatness Measure (SFM)*. The *SFM* is defined as the ratio of the geometric mean to the arithmetic mean of the *PSD* coefficients [24]. It can be expressed as,

$$SFM = \frac{[\prod_{k=1}^{N} S(f_k)]^{\frac{1}{N}}}{\frac{1}{N}\sum_{k=1}^{N} S(f_k)}, \tag{7}$$

where $S(f_k)$ is the k^{th} *PSD* coefficient for the *PSD* obtained from the results in Formula (6). *SFM* is a widely existing measure for discriminating frequencies in various applications such as voiced frame detection in speech recognition [24][25]. In general, small values of *SFM* imply the concentration of data at narrow frequency spectrum ranges.

Table 2 shows the mean value of *SFM* based on extensive analysis of non-worm traffic data for some popular ports collected by SANs *ISC*. Overall, we note that the *PSD* distribution of non-worm scan traffic is relatively flat, and thereby results in relatively larger magnitudes of *SFM* values. The above observation can be reasoned due to the fact that normal non-worm scan traffic does not tend to concentrate at any particular frequency since its random dynamics is not caused by any repeating phenomenon. Differently, the C-Worm has unpreventable recurring behavior in its scan traffic and consequently its *SFM* values are comparatively smaller than the *SFM* values of normal non-worm scan traffic. From Fig. 3, we can observe that the *SFM* value for the C-Worm is very small (e.g., with a average value of approximately 0.075).

4.2.3 Detection Decision Rule

We now describe the method of applying an appropriate detection rule to detect large scale propagations of the C-Worm propagation. As the *SFM* value can be used to sensitively distinguish the C-Worm and normal non-worm scan traffic, the worm detection is performed by comparing the *SFM* with a predefined threshold T_r. If the *SFM* value is smaller than a predefined threshold T_r, then a C-Worm propagation alert is generated. The value of the threshold T_r used by the C-Worm detection can be fittingly set based on the knowledge of statistical distribution (e.g., *PDF*) of *SFM* values that correspond to the non-worm scan traffic. If we can obtain the *PDF* of *SFM* values for the C-Worm through comprehensive simulations and even real-world profiled data in the future, the optimal threshold can

Table 2. SFM average values for normal non-worm scan traffic

port	23	25	53	113	139	445	1025	4672	6346	6881	8080	27015
SFM	0.71	0.71	0.95	0.86	0.64	0.67	0.46	0.47	0.45	0.74	0.56	0.65

be obtained by applying the Bayes classification. If the *PDF* of *SFM* values for the C-Worm is not available, based on the *PDF* of *SFM* values of the normal non-worm scan traffic, we can set an appropriate T_r value. For example, the T_r value can be determined by the Chebyshev inequality [26] so as to obtain a reasonable false alarm rate for worm detection. Hence in Section 5, we evaluate our spectrum-based detection scheme against the C-Worm on two cases: (i) the PDF of *SFM* values are known for both the normal non-worm scan traffic and the C-Worm scan traffic, (ii) the PDF of *SFM* values is only known for the normal non-worm scan traffic.

5 Performance Evaluation

In this section, we report our evaluation results that illustrate the effectiveness of our spectrum-based detection scheme against the C-Worm in comparison with popular existing worm detection schemes used for detecting large-scale propagation of worms.

5.1 Evaluation Methodology

In order to evaluate the performance of any given detection scheme against the C-Worm, we use the following metrics. The first two metrics are the *Detection Time* (DT) and the *Maximal Infection Ratio* (MIR). DT is defined as the time taken to successfully detect a wide-spreading worm from the moment the worm spreading starts. It quantifies the detection speed of a detection scheme. MIR defines the ratio of infected host number over the total number of vulnerable hosts up to the moment when the worm spreading is detected. It quantifies the damage caused by a worm before being detected. The objective of any detection scheme is to minimize the damage caused by a rapid worm propagation. Hence, MIR and DT can be used to quantify the effectiveness of any worm detection scheme. The higher the values, better the worm attack effectiveness and worse the detection effectiveness. In addition, we use other two metrics called the *Detection Rate* (DR) and *False Alarm Rate* (FAR). DR is defined as the probability that a detection scheme can correctly identify a worm attack. The FAR is defined as the probability that a detection scheme mistakenly identifies a worm attack that does not exist.

In our evaluations, we set the total number of vulnerable hosts on the Internet as $360,000$ [1]. For the scan rate S (number of scans per minute), we set different scan rates for infected hosts (worm instances) [4]. In our evaluation, the scan rates are predetermined and follow a normal distribution $S = N(S_m, S_\sigma^2)$, where S_m and S_σ^2 are in $[(20,\ 70]$, similar to those used in [12].

We simulate the C-Worm attacks by varying the attack parameters such as attack probability ($P(t)$) and the number of worm instances participating the scan ($\bar{M}_C$) defined in Section 3. The $\bar{M}_C$ follows the Gaussian distribution $N(m, \sigma)$ and are changed dynamically by the C-Worm during its propagation. Particularly, for $N(m, \sigma)$, m is randomly selected in $(12000,\ 75000)$ and σ is randomly selected in $(0.2,\ 100)$. We simulate different C-Worm attacks by varying the values of m and σ. The detection sampling window W_s is set to 5 minutes and the detection sliding window W_d is set to be incremental from 80 min to 800 min. The incremental selection of W_s from comparatively small window to large window can adaptively reflect the worm scan traffic dynamics caused by the C-Worm propagation at various speeds. We choose the setting of the detection sampling window to be short enough in order to provide enough sampling accuracy as prescribed by Nyquist's sampling theory. Also, we choose the detection sliding window to be long enough in order to capture adequate information for spectrum-based analysis [24].

In practice, since detection systems analyze port scan traffic which also includes the non-worm scan traffic, we replay the real-world traces as non-worm scan traffic (background noise) in our simulations. In particular, we used the *ISC* real-world trace from 01/01/2005 to 01/15/2005. Note that SANs *ISC* maintained by the SANs Institute have gained popularity in the Internet security community in recent years. *ISC* collects firewall and Intrusion detection system logs, which indicate port-scan trends from approximately 2000 organizations that monitor up to 1 million IP addresses. We choose the scan traffic logs for port 8080 as an example for profiling the non-worm scan traffic.

5.2 Performance of Detection Schemes

We evaluate our proposed spectrum-based detection scheme by comparing its performance with three existing popular worm detection schemes. The first scheme is the volume mean-based (MEAN) detection scheme [13];

[4] Each worm instance may have access to a different set of out-going link bandwidth and local computing resources, which results in different scan rates for the different worm instances.

Table 3. Detection results for the C-Worm

Schemes	VAR	TREND	MEAN	SPEC(W)	SPEC
Detection Rate (DR)	48%	0%	14%	96.4%	99.3%
Maximal Infection Ratio (MIR)	14.4%	100%	7.5%	4.4%	2.8%
Detection Time (DT) in minutes	2367	∞	1838	1707	1460

the second scheme is the trend-based (TREND) detection scheme [12]; and the third scheme is the victim number variance based (VAR) detection scheme [14]. We define our spectrum-based detection scheme as SPEC. We evaluate two flavors of SPEC: one does not have knowledge of any C-Worm attacks or C-Worm scan traffic (denoted by SPEC(W)); and the other does have the knowledge of C-Worm attacks through an off-line training process (denoted by SPEC). For the off-line training, we use 1000 worm attacks that include both the C-Worm (800 C-Worm attacks) and PRS worms (200 PRS worm attacks). For fairness, we set the detection parameters for our SPEC scheme and the other three detection schemes, so that all detection schemes achieve similar false alarm rate FAR below 1%.

Table 3 shows the detection results of different detection schemes against the C-Worm. The results have been averaged over 500 C-Worm attacks. From this table, we can observe that existing detection schemes are not able to effectively detect the C-Worm and its DR values are significantly lower in comparison with our spectrum-based detection schemes (SPEC and SPEC(W)). For example, SPEC achieves the DR of 99%, which is at least $3-4$ times more accurate than the detection schemes such as VAR and MEAN that achieve DR values of only 48% and 14%, respectively.

Our SPEC and SPEC(W) detection schemes also achieve good DT performance in addition to the high DR values indicated above. In contrast, the DT of existing detection schemes have relatively larger values. As a consequence of the DT values, we can see that the C-Worm propagation is effectively contained by SPEC and SPEC(W) as demonstrated by the lower values of MIR for the SPEC and SPEC(W). Since the DR values for the existing detection schemes are relatively small, obtaining low values of MIR for those schemes are not as significant as those for SPEC and SPEC(W). Furthermore, we can notice that the detection performance of the SPEC(W) is worse than the SPEC. This is because the SPEC(W) lacks off-line training knowledge for the C-Worm scan traffic. Nonetheless, the SPEC(W) still performs much better than existing detection schemes.

6 Final Remarks

In this paper, we studied a new class of smart-worms viz., the *Camouflaging Worm* (C-Worm in short), which has the capability to camouflage its propagation. Our analysis and evaluation 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 such observation, we developed a novel spectrum-based detection scheme to detect the C-Worm. Specifically, our spectrum-based detection scheme used the *Power Spectral Density* (*PSD*) distribution of the C-Worm scan traffic volume and its corresponding *Spectral Flatness Measure* (*SFM*) as the key detection feature to distinguish the C-Worm scan traffic from the normal non-worm scan traffic. The evaluation data showed that our scheme achieved superior detection performance against the C-Worm in comparison with existing worm detection schemes.

The war between the malicious attackers who develop new forms of intelligent attacks, and the proactive defenders who develop effective countermeasures, is never ending. We believe that this paper is just a foundation for continuous development of defensive countermeasures for identifying and mitigating smart-worms such as the C-Worm.

Acknowledgments

We thank the anonymous reviewers for their invaluable feedback. This work is partially supported by NSF under grants No. ACI-0329155 and CCF-0546668.

References

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

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

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

[4] *W32/MyDoom.B Virus*, http://www.us-cert.gov/cas/techalerts/TA04-028A.html.

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

[6] *Worm.ExploreZip*, http://www.symantec.com/avcenter/venc/data/worm.explore.zip.html.

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

[8] C. C. Zou, W. Gong, and D. Towsley, "Code-red worm propagation modeling and analysis," in *Proceedings of the 9-th ACM Conference on Computer and Communication Security (CCS)*, Washington DC, November 2002.

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

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

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

[12] C. Zou, W. B. Gong, D. Towsley, and L. X. Gao, "Monitoring and early detection for internet worms," in *Proceedings of the 10-th ACM Conference on Computer and Communication Security (CCS)*, Washington DC, October 2003.

[13] S. Venkataraman, D. Song, P. Gibbons, and A. Blum, "New streaming algorithms for superspreader detection," in *Proceedings of the 12-th IEEE Network and Distributed Systems Security Symposium (NDSS)*, San Diego, CA, Febrary 2005.

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

[15] SANS, *Internet Storm Center*, http://isc.sans.org/.

[16] D. J. Daley and J. Gani, *Epidemic Modeling: an Introduction*, Cambridge University Press, 1999.

[17] V. Yegneswaran, P. Barford, and D. Plonka, "On the design and utility of internet sinks for network abuse monitoring," in *Proceeding of Symposium on Recent Advances in Intrusion Detection (RAID)*, Pittsburgh, PA, September 2003.

[18] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," in *Proceedings of the 25-th IEEE Symposium on Security and Privacy*, Oakland, CA, May 2004.

[19] G. F. Gu, D. Dagon, M. I. Sharif X. Z. Qin, W. Lee, and G. F. Riley, "Worm detection, early warning, and response based on local victim information," in *Proceedings of Proceedings of the 20-th Annual Computer Security Applications Conference (ACSAC 2004)*, Tucson, Arizona, December 2004.

[20] S. Singh, C. Estan, G. Varghese, and S. Savage, "Automated worm fingerprinting," in *Proceedings of the ACM/USENIX Symposium on Operating System Design and Implementation*, San Francisco, CA, December 2004.

[21] G. M. Voelker J. Ma and S. Savage, "Self-stopping worms," in *Proceedings of the ACM Workshop on Rapid Malcode (WORM)*, Washington D.C, November 2005.

[22] Linux.com, *Understanding Stealth Scans: Forewarned is Forearmed*, http://security.itworld.com/4363/LWD010321vcontrol3/page1.html.

[23] Solar Designer, *Designing and Attacking Port Scan Detection Tools*, http://www.phrack.org/phrack/53/P53-13.

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

[25] R. E. Yantorno, K. R. Krishnamachari, J. M. Lovekin, D. S. Benincasa, and S. J. Wenndt, "The spectral autocorrelation peak valley ratio (sapvr) - a usable speech measure employed as a co-channel detection system," in *Proceedings of IEEE International Workshop on Intelligent Signal Processing (WISP)*, Budapest, Hungary, May 2001.

[26] S. Theodoridis and K. Koutroumbas, *Pattern Recognition, Second Edition*, Elsevier Science, 2003.