International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Dynamic Detection of Vigorous Worm in Infected Host

C. Ajitha[1], K. Kirubanantha Valli[2]

[1,2]Assistant Professor/CSE, Unnamalai Institute of Technology, TamilNadu, India

ABSTRACT

The Internet has developed to give many benefits to mankind. The access to information being one of the most important. Worms cause major security threats to the Internet. Worms are software components that are capable of infecting a computer and then using that computer to infect another computer. The cycle is repeated, and the population of worm-infected computers grows rapidly. Smart worms cause most important security threats to the Internet. The ability of smart worms spread in an automated fashion and can flood the internet in a very short time. A new class of smart worms, referred to as Camouflaging worm (C-Worm in short). C-worm is different from traditional worm. C-worm intelligently manipulate its scan traffic volume over time. Motivated by observations, we designed a novel Spectrum Based detection Scheme to detect the C-worm. This scheme uses 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. This scheme is effectively detecting not only the C-worm but traditional worms as well. The goal is to prevent, detect and delete the smart worms as well as traditional worms.

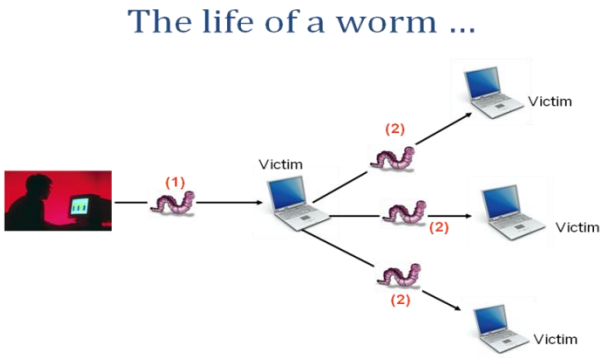
I. INTRODUCTION:

The term **"WORM"** was coined by John Bruner in his novel **"The Shockwave Rider"** in 1975. **What is Virus?** Virus is a computer program that copies itself from one computer to another. . **What is Worm?** A computer worm is much like a virus but does not need any help from a person to spread. Computer worms spread from computer to computer via network.

What is Difference between Virus and Worm?

VIRUS	**WORM**
A virus is a program that is designed to spread from file to file on a single PC.	A worm is designed to copy itself (intentionally move) from PC to PC, via networks, internet etc.
it does not intentionally try to move to another PC.	A worm does not need a host file to move from system to system, whereas a virus does.
it must replicate, and execute	worms spread more rapidly than

itself to be defined as a virus	viruses.



Worm attack in Computer

The Life Cycle of a Simple Worm

- ❖ Scanning for a victim.
- ❖ Exploiting the victim.
- ❖ Cloning itself onto the victim.
- ❖ Running the clone to further spread infection.
- ❖ Stealth techniques used to hide itself.

The smart worms spread in an automated fashion and can flood the internet in a very short time. A new class of smart worms, referred to as Camouflaging worm (C-Worm in short). C-worm is unseen worm, has ability to increase its scan traffic volume over time. The C-Worm hides its propagation from existing worm detection systems based on analyzing the propagation traffic generated by worms. Stealth is a strategy used by a recently discovered active worm called "Atak" worm and "self-stopping" worm. Worm might also use the evasive scan and traffic morphing technique to hide the detection. C-worm is similar to "Atak" Worm. During scanning this worm goes to sleeping mode to avoid detection after scan is finished it starts its self-propagating nature to infect other computers. Fast propagating worm is easy to detect rather than slow propagating worm. Difficult to detect the C-worm because its action is kept secret. First, C-worm scans all the ip's present in the network. Then it identifies the number of immune systems, number of worm infected system and number of vulnerable systems. C-worm focusing only vulnerable ip system rather focusing all the ips. The detection scheme monitors the traffic process continuously, if smaller amount of traffic of c-worm is identify and detected by the spectrum approach. This approach uses Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) is to distinguish the C-Worm traffic from background traffic. Spectrum detection scheme effectively detect and prevent not only the C-worm it will detect and prevent traditional worms also.

Effects of worms:

1. Causes the computer to run very slowly such that the system may even possibly crash.
2. Will make it difficult to save and create new files.
3. Will delete the files on the host system.
4. Can cause encryption of important files.
5. Will access confidential information and destroy the existing data

II. RELATED WORK

Active worms have been a persistent security threat on the Internet. They spread in an automated fashion and can flood the Internet in a very short time. The basic function of active worms is that they identify the vulnerable computers, infect them and worm infected computers propagate the infection to other vulnerable computers. Pure Random Scan (PRS) is the basic form of active worms. In the PRS form, a computer that is infected by worms, scans a set of random IP addresses to find vulnerable computers. Worms make use of different scan strategies during their propagation like DNS, network topology and routing information to identify the vulnerable computers instead of scanning the IP addresses. One form of worm that is different from other worms because they manipulate the scan traffic over time in order to avoid being detected. Worms can be detected by many mainly two types of detection categories which are Host based detection and Network based detection while the former is used to detect worms by monitoring, collecting and analyzing worm behaviors on host ends, the latter detects worms by monitoring, collecting and analyzing the scan traffic which is set of messages to identify the vulnerable computers. The overall scan for a C-Worm should not be too slow or too fast so that is not detected and delay rapid damage on the internet. Besides the mentioned detection schemes, there are other detection methods like sequential hypothesis testing and payload based worm signal detection.

Worm can be detected by algorithms like Destination Source Correlation (DSC) and Honey Stat. DSC is the first behavioral based model to detect worms. It is based on the worm behavior in terms of infection pattern and scanning pattern. DSC is used to detect zero-day scanning worms with a high detection rate and low false positive rate. It focuses on the infection relation and tracks the real infected host for best response. Overall, it is used to improve the quality of data stream. The Honey Stat algorithm, on the other hand uses a system that provides a way to track the short term infection behavior used by worms. It uses honeypots to generate a highly accurate alert system with low false positive rates.

Active worms spread rapidly in a short span of time so it is essential for modeling the spread of active worms. The propagation of worms can be characterized by the Analytical Active worm propagation (AAWP) model and comparing this model with the Epidemiological model and Weaver's Simulator to characterize the spread of worm effectively. The AAWP model is used to characterize the propagation of worms that employ random scanning and understand the spread of worms that employ local subnet scanning. It detects the worms with a larger hitlist in a shorter period of time even though they spread at a faster rate. There are a few basic differences between the AAWP model and the Epidemiological model which are: While, the Epidemiological model uses a continuous time differential equation, AAWP model is based on the discrete time model. Furthermore, the Epidemiological model neither considers the patching rate nor the time that it takes for the worm to infect a machine but the AAWP model does.

Worms cause many problems in today's network because they spread very rapidly. So, it is essential to use a detection method that gives a faster response. Thus an automatic detection method is used for a faster response. This detection method uses an approach that makes use of behavioral signatures. A behavioral signature describes aspects of any particular worm's behavior that are common

across the manifestations of a given worm and that span its nodes in temporal order. It can be used to detect classes of worms and common worm implementations and designs, even if worm has never been seen before. This approach makes use of signature-based intrusion detection. It focuses on detecting patterns at a higher level of abstraction. Ideally, the patterns are inherent behaviors of worm spread and distinct from normal network traffic. The frequency of and interrelationships between behaviors improve detection accuracy. Behavioral signatures are valuable because they describe classes of worms without needing to know the specifics of a worm in prior.

Camouflaging worm is very difficult to detect and prevent compared to the other worms because they manipulate the scan traffic over time in order to avoid being detected. Existing worm detection schemes will not be able to detect c-worm scan traffic patterns. It is very important to understand the smart-worms and develop new countermeasures to defend against them. Existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns. To detect the worm they use sequential hypothesis testing and payload-based worm signature detection scheme, this schemes is not used to detect the unseen worms i.e. smart worms. In previous study to model the worm they used stochastic epidemic model, makes it difficult to derive insightful results that could be used to contain the worm. To detect the presence of a worm by detecting the trend, not the rate of the observed illegitimate scan traffic.

III. PROPOSED SYSTEM

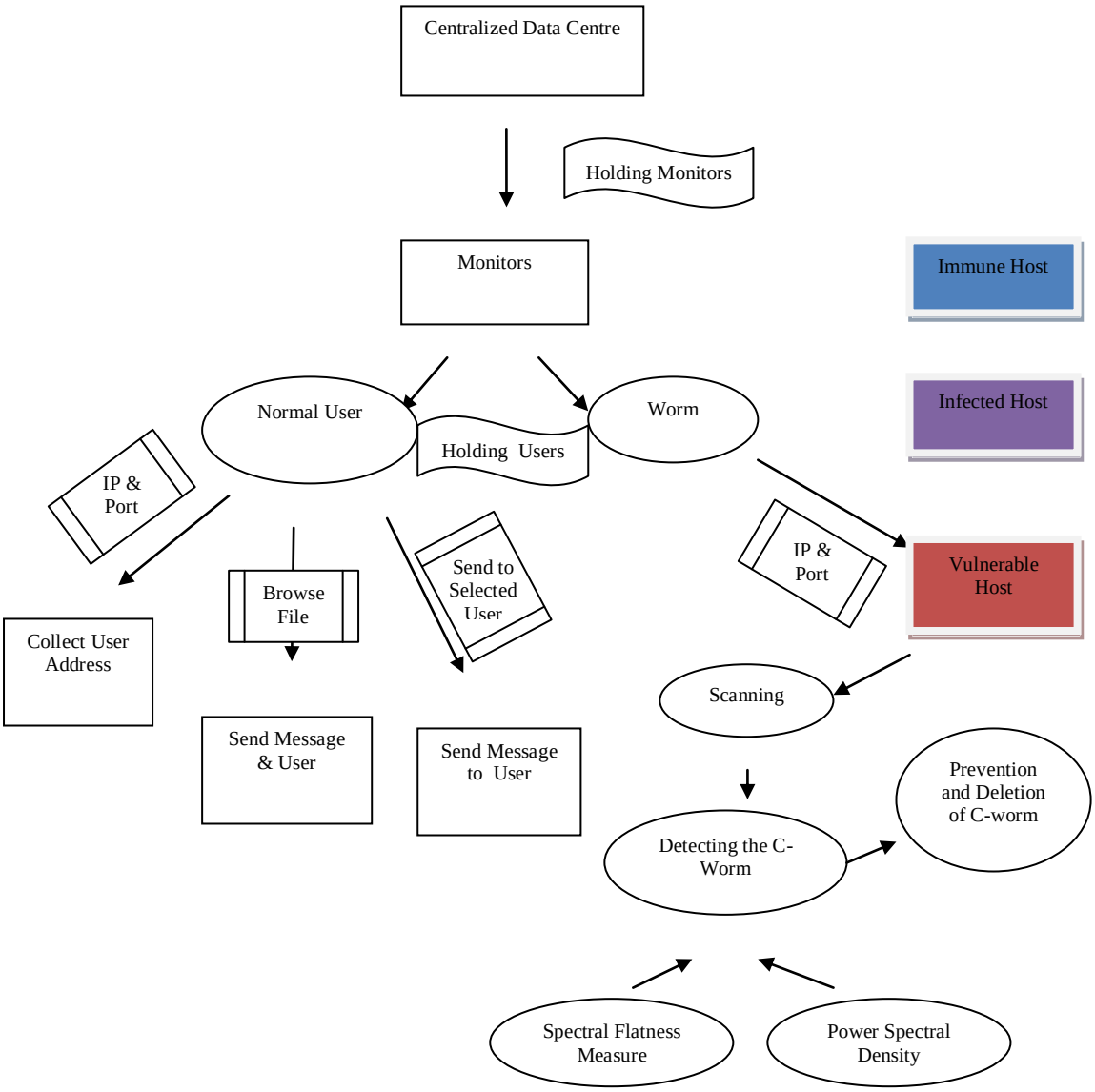
Proposed system models smart worms referred to as Camouflaging Worm. C-worm is different from traditional worm, ability to increase its scan traffic volume over time. A novel to detect C-worm Spectrum Based Detection scheme. Worm detection scheme that are based on the global scan traffic monitor by detecting traffic anomalous behaviour.To define several new metrics, Maximal Infection Ratio (MIR) is the one to quantify the infection damage caused by a worm before being detected. Other metrics include Detection Time (DT) and Detection Rate (DR) used. Mathematical model Analytical Active Worm Propagation (AAWP), which characterizes the propagation of worms that employ random scanning. To identify and detect the C-worm by the spectrum approach. This approach uses Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) is to distinguish the C-Worm traffic from background traffic. It is used to detect and prevent not only the C-worm as well as Traditional worm.

IV. SYSTEM ARCHITECTURE DESCRIPTION

The Main framework of the worm detection model consists of a centralized data center which acts as a server and is used to collect traffic logs from distributed monitors in a timely manner. The server uses a specified port number to accept the connection from the monitors. The centralized data center then distributes the report logs to all the users connected to the network further generating reports. The monitors are distributed across the internet and records the scan traffic. The monitor then sends the traffic logs (IP addresses not used) to the detection center.

Based on the scan traffic, worms are detected. The IP and port numbers are scanned. If the user is a normal user, then the user address is collected based upon the scan of IP address and port and the message intended to the selected recipient or user is sent. If the worms are detected based on the monitor analysis, then the IP address and port of targeted systems are scanned and the vulnerable computers are affected by the worms.

V. SYSTEM ARCHITECTURE



VI. MODULE DESCRIPTION:

i. MODELING OF THE C-WORM:

We need to model a C-worm for testing purposes. There are several features that characterize a worm which are: a) The Speed of spread, b)Strategies of spread, c) Payload of the worm, d) Vulnerabilities The worm is modelled by using a dynamic model for the worm propagation. The model assumes that the host can be in the any of the three states which are: immune, vulnerable or infected. An immune host is one that cannot be infected by the worm. Vulnerable host is that which can be infected

by a worm and an infected host is that which cannot be infected by a worm. The C-worm is modelled in such a way that it increases the CPU usage memory. Since the C-Worm camouflages its propagation, we need to change the number of worm instances conducting the port scans thus manipulating the scan traffic volume. We should model the C-Worm in such a way that it's neither too slow nor too fast so that it's not easily detected and does not delay rapid damage on the internet.

ii. WORM PROPAGATION MODULE:

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, consider the C-Worm as a worst case attacking scenario that uses a closed loop control for regulating the propagation speed based on the feed back propagation status.

iii. BRANCHING PROCESS MODULE:

To the problem of combating worms, we have developed a branching process model to characterize the propagation of Internet worms. Unlike deterministic epidemic models studied in the literature, this model allows us to characterize the early phase of worm propagation.

iv. SCANNING :

The computer infected by worms keeps scanning the internet and propagates itself at the highest possible speed. The scanning is done based on the networks IP addresses and ports. A local network is used to infect the vulnerable computers at their initial stages of propagation. When one computer gets infected by the worm, they take part in thus scanning other computers to detect the vulnerable computers. C-Worms are being scanned in a definite randomized and time related pattern. They scan a specific target space that consists of a set of IP addresses. The C-Worm is designed in such a way that it manipulates the scan traffic.

v. DETECTION OF THE C-WORM:

Detection of the worms is one of the most important tasks and it based on the behavioral features of the worms. Since C-Worms camouflage their propagation, based on the scan traffic, they are very difficult to detect. So, we adopt frequency domain analysis techniques in order to prevent the wide spreading of the C-Worm. Particularly, we use the spectral-based detection schemes which are the a) PSD(Power Spectral density) in the frequency domain and b) Spectral Flatness Measure(SPM) to distinguish the C-Worm traffic from non-worm traffic.

SPECTRUM BASED:

Spectrum based detection scheme uses Power Spectral Density and Spectral Flatness Measure

a. Power Spectral Density(PSD):

In order to obtain the PDS distribution for detection of worm, We transform the data from time domain into the frequency domain.

We use a random process to model the worm detection data the PSD is used to capture any repeating pattern in the frequency domain and shows a comparatively even distribution across a wide spectrum range for the normal non-worm scan traffic. The PSD of C-Worm scan traffic shows higher concentrations at a certain range of a spectrum.

b. Spectral Flatness Measure(SFM):

The SFM is used to distinguish the scan traffic from the normal non-worm scan traffic. Smaller values of SFM implies concentration of data at narrow frequency spectrum ranges.SFM can capture the anomaly behaviour in certain range of frequencies. It is defined as the ratio of the geometric mean to the arithmetic mean of the PSD coefficients.SFM is widely used in various applications, such as voiced frame detection in speech recognition.

vi. PREVENTION AND DELETION OF C-WORM:

Prevention:

It is always better to prevent the worm from entering rather than getting the computer infected after the worm attacks .Thus, it is important to fix the holes that are being exploited. We therefore develop a mathematical model for prevention of the propagation of the worms. We can also prevent the worm from infecting by using the latest anti-virus software's, firewalling.

Deletion of worms:

If the worms enter the system, then it's necessary to delete the worm before it infects the entire system thus shutting down the entire system and destroying the important data that is present. So, we develop a distinct model that deletes the worms that have infected the system in order to provide security and keep our system secure.

VII. CONCLUSION AND FUTURE WORK:

In this paper, we have analysed and studied a new class of smart worms called C-Worms, which has the capability to camouflage its propagation. It has been thus observed that its Camouflaging nature inevitably manifests as a distinct pattern in the frequency domain. Based on the observation, we have developed the Spectrum based detection scheme which encloses the Power Spectral Density (PSD) scheme and Spectral flatness Measure (SPM) scheme to detect the C-Worm. It has also been observed that the evaluation data showed that our scheme achieved superior detection performance against the C-Worm in comparison with existing worm detection schemes.

As a part of future work for this project, we design discrete mathematical models for the prevention and deletion of the C-Worms that enter the system. Thus, protecting the system and keeping it secure.

References:

1. D.Moore, V.Paxson, and S.Savage, "Inside the Slammer Worm", proc. IEEE Magazine of Security and Privacy, July 2003.
2. Z.S.Chen, L.X.Gao, and K.Kwait, "Modeling the Spread of Active worms," Proc. IEEE INFOCO, Mar. 2003.

3. C.Zou, W.B.Gong, D.Towsley, and L.X.Gao, "Monitoring and Early Detection for Internet Worms". Proc. 10th ACM Conf. Computer and Comm. Security (CCS), Oct. 2003
4. C.C.Zou, D.Towsley, and W.Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worm," IEEE Trans. Dependable and Secure Computing, Vol.4, no.2, pp.105-118, Apr-June 2007
5. X.Wang, W.Yu, A.Champion, X.Fu, and D.Xuan, "Detecting Worms Via Mining Dynamic Program Execution," Proc. IEEE Int'l Conf. Security and Privacy in Comm. Networks (SECURE COMM), Sept 2007.
6. Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan and Wei Zhao, "Modeling and Detection of Camouflaging Worm", IEEE Transactions on Dependable and Secure Computing, Vol.8, No.3, May-June 2011.