ISSN:2249-5789
S Preetha, International Journal of Computer Science & Communication Networks,Vol 2(2), 190-193

Modeling and Detection of Camouflaging Worm using IP Traceback

S.Preetha
Department of Information Technology
Sri Venkateswara College of Engineering
Sriperumbudur, Tamilnadu
Preethas.s42@gmail.com

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. 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. The characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and non-worm traffic (background traffic). The 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 observations, designed a novel spectrum-based scheme to detect the C-Worm. 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, the extensive performance evaluations on proposed spectrum-based detection scheme. The performance data clearly demonstrates that our scheme can effectively detect the C-Worm propagation. Furthermore, show the generality of spectrum-based scheme in effectively detecting not only y the C-Worm, but traditional worms as well.**

Keywords-DDoS, SFM, PSD, C-WORM, Networks

I. Introduction

Many real-world worms have caused notable damage on the Internet. These worms include “Code-Red” worm in 2001, “Slammer” worm in 2003 , and “Witty”/ “Sasser” worms in 2004 . 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. A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. In a typical DDoS attack, a hacker (or, if you prefer, cracker) begins by exploiting a vulnerability in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple -- sometimes thousands of -- compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service. While the press tends to focus on the target of DDoS attacks as the victim, in reality there are many victims in a DDoS attack -- the final target and as well the systems controlled by the intruder. Although the owners of co-opted computers are typically unaware that their computers have been compromised, they are nevertheless likely to suffer degradation of service and malfunction. Both owners and users of targeted sites are affected by a denial of service. Yahoo, Buy.com, RIAA and the United States Copyright Office are among the victims of DDoS attacks. DDoS attacks can also create more widespread disruption. In October 2010, for example, a massive DDoS attack took the entire country of Myanmar offline. A computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army. Both Kaspersky Labs and Symantec have identified botnets -- not spam, viruses, or worms -- as the biggest threat to Internet security.

A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion. Computers that are co-opted to serve in a zombie army are often those whose owners fail to provide effective firewalls and other safeguards. An increasing number of home users have high speed connections for computers that may be inadequately protected. A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation. At a certain time, the zombie army "controller" can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.

The computers that form a botnet can be programmed to redirect transmissions to a specific computer, such as a Web site that can be closed down by having to handle too much traffic - a distributed denial-of-service (DDoS) attack - or, in the case of spam distribution, to many computers. The motivation for a zombie master who creates a DDoS attack may be to cripple a competitor. The motivation for a zombie master sending spam is in the money to be made. Both of them rely on unprotected computers that can be turned into zombies. According to the Symantec Internet Security Threat Report, through the first six months of 2006, there were 4,696,903 active botnet computers.

In this paper Camouflaging worm (c-worm short) is modeled.The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. Thereby, the effects of C-Worm camouflages its propagation from existing worm detection systems based on analyzing the propagation traffic generated by worms. 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. A novel spectrum-based scheme to detect the C-Worm. 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. The performance data clearly demonstrates that scheme can effectively detect the C-Worm propagation. The generality of our spectrum-based scheme in effectively detecting not only the C-Worm, but traditional worms as well.

II.RELATED WORK

On July 19, 2001, more than 359,000 computers connected to the Internet were infected with the Code-Red (CRv2) worm in less than 14 hours. The cost of this epidemic, including subsequent strains of Code-Red,[11] is estimated to be in excess of $2.6 billion. Despite the global damage caused by this attack, there have been few serious attempts to characterize the spread of the worm, partly due to the challenge of collecting global information about worms. Using a technique that enables global detection of worm spread, we collected and analyzed data over a period of 45 days beginning July 2nd, 2001 to determine the characteristics of the spread of Code-Red throughout the Internet. In this paper, we describe the methodology we use to trace the spread of Code-Red, and then describe the results of our trace analyses. We also qualified the effects of DHCP on measurements of infected hosts and determined that IP addresses are not an accurate measure of the spread of a worm on timescales longer than 24 hours. Finally, the experience of the Code- Red worm demonstrates that wide-spread vulnerabilities in Internet hosts can be exploited quickly and dramatically, and that techniques other than host patching are required to mitigate Internet.

A mathematical model derived from empirical data of the spread of Code Red I in July, 2001. We discuss techniques subsequently employed for achieving greater virulence by Code Red II[8] and Nimda. In this context, we develop and evaluate several new, highly virulent possible techniques: hit-list scanning (which creates a Warhol worm), permutation scanning (which enables self-coordinating scanning), and use of nternet sized hit-lists (which creates a flash worm). We then turn to the to the threat of surreptitious worms that spread more slowly but in a much harder to detect “contagion” fashion. We demonstrate that such a worm today could arguably subvert upwards of 10,000,000 Internet hosts. We also consider robust mechanisms by which attackers can control and update deployed worms. In conclusion, we argue for the pressing need to develop a “Center for Disease Control” analog for virus and worm-based threats to national cyber security, and sketch some of the components that would go into such a Center. Slammer worm spread so quickly that human response was ineffective. As it began spreading throughout the Internet, the worm infected more than 90 percent of vulnerable hosts within 10 minutes, causing significant distruption to financial, transportation, and government institutions. We tracked slammer spreading behavior via network telescope technique a large address, which is monitored for unusual activity. Ideally these address ranges are unused but routed, which eliminates all normal activity.

David Moore, Geoffrey volkier and Stefan Savage developed network telescope[10] to understand distributed denial of service attacks, which generate a considerable amount of “backscatter”, or response to packets with randomly forged source addresses. Modeling the spread of active worms can help us understand how active worms spread, and how we can monitor and defend against the propagation of worms effectively.

In this paper, author present a mathematical model, referred to as the Analytical Active Worm Propagation (AAWP) model,[12] which characterizes the propagation of worms that employ random scanning. We compare our model with the Epidemiological model and Weaver’s simulator. Our results show that our model can characterize the spread of worms effectively. Taking the Code Red v2 worm as an example, we give a quantitative analysis for monitoring, detecting and defending against worms. Furthermore, we extend our AAWP model to understand the spread of worms that employ local subnet scanning. To the best of our knowledge, there is no model for the spread of a worm that employs the localized scanning strategy and believe that this is the first attempt on understanding local subnet scanning quantitatively.

III. PROPOSED ARCHITECTURE DESIGN

In most of the existing system, 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. As a result the operating system has to be formatted and a new operating system only 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 Worm Behavior is monitored and compared with the Previous Behavior of Worms, so that Traditional Worm Detection Method is adopted to kill the worm from the network. Network Traffic is also monitored so that to identify the Worm presence in the network. 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.

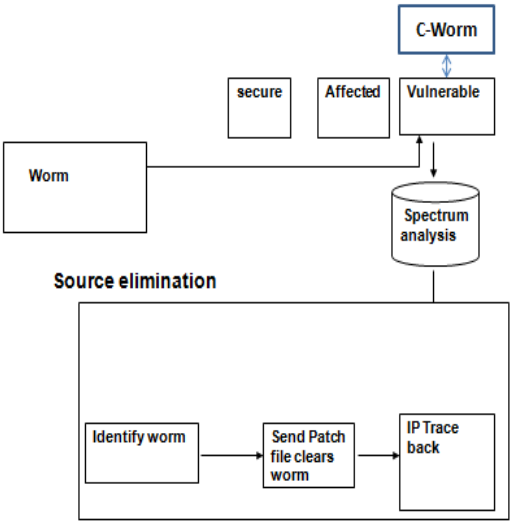

Figure 1: Source Elimination

The worm infected computer identifies and infect vulnerable computer. This newly infected computer will automatically scan several IP addresses to identify and infect other vulnerable computers. The C-worm is different from traditional worms in which it camouflages any noticeable trends in the number of infected computers. The Major Advantage of the 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, number of Vulnerable Systems. C-Worm rather focusing all the IP, instead it focuses only the Vulnerable Systems, because these systems are the Target of C-Worm. The Main aim of C-Worm is 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 infection 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. The C-worm and non worm network traffic is need to analyze. In this paper the spectrum based scheme is used to distinguish the non worm and the C-worm traffic. The Power Spectral Density and its corresponding Spectral Flatness Measure is used, the PSD distribution for worm detection data the data need to transform data from the time domain into the frequency domain. The C-worm can be detected only in frequency domain. The SFM values are comparatively very small than the SFM values of normal non worm scan traffic. Thus the worm is identified and alerts the system. Each and every time of scan it scan the un occupied IP address. When the worm is detected the patch file is used to clear the worm. The IP trace back is used to find the source node which propagates the worm and eliminates such type of system from the network.

A. Spectrum Based Analysis

Worm which is the malicious software program that propagate itself on the Internet. It self-replicating computer program which uses a computer network to send copies of itself to other nodes without any intervention. In spectrum based detection, the distribution of PSD and its corresponding SFM are used to distinguish the C-Worm scan traffic from the non worm scan traffic. The C-worm which doesn't show any noticeable trend and detecting c-worm is very difficult. The Spectrum based detection schemes which detect the C-Worm very easily. The Power Spectral Density which shows it work only in time domain but C-Worm can be detected only in frequency domain. Spectral Flatness Measure is the correspond method of Power spectral Density and by using this C-worm and the difference of their traffic level is detected. The central step in devising our source separation algorithm is the choice of a measure describing the complexity of an audio scene. Given such a measure, it is possible to evaluate it for several combinations of input sounds and choose the combination that gives the lowest complexity score. The measure used in the approach of the spectral flatness measure. It measures how much the energy at a given time is spread in the spectrum, giving a high value when the energy is equally distributed and a low value when the energy is concentrated in a small number of narrow frequency bands. The spectral flatness measure is computed from the spectrum as the geometric mean of the Fourier coefficients divided by the arithmetic mean.

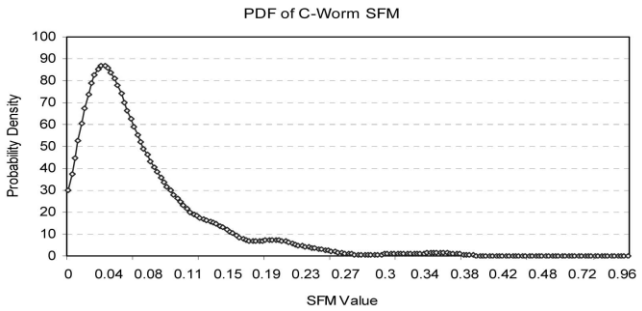

Figure 2: PDF of C-Worm SFM

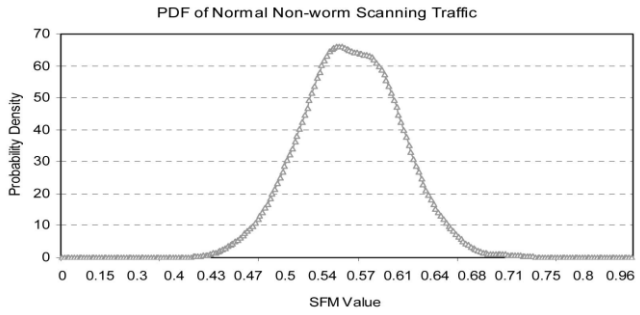

Figure 3: PDF of Normal Non-Worm Scanning Traffic

B. 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 spectral density, 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 detect unwanted 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. Much effort has been expended and millions of dollars spent on developing and producing electronic instruments called "spectrum analyzers" for aiding electrical engineers and technicians in observing and measuring the power spectra of signals. The cost of a spectrum analyzer varies depending on its frequency range, its bandwidth (signal processing), and its accuracy. The higher the frequency range (S-band, C-band, X-band, Ku-band, K-band, Ka-band, etc.), the more difficult the components are to make, and the more expensive the spectrum analyzer is. Also, the wider the bandwidth that a spectrum analyzer possesses, the more costly that it is, and the capability for more accurate measurements increases costs as well.

IV. CONCLUSION

In this paper a new class of smart-worm called C-Worm, which has the capability to camouflage its propagation and further avoid the detection. The investigation 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 observation, a novel spectrum-based detection scheme to detect the C-Worm. The evaluation data showed that a scheme achieved superior detection performance against the C-Worm in comparison with existing representative detection schemes. In this the foundation for ongoing studies of “smart” worms that intelligently adapt their propagation patterns to reduce the effectiveness of countermeasures.

REFERENCES

[1] P.R. Roberts, Zotob Arrest Breaks Credit Card Fraud Ring,http://www.eweek.com/article2/0,1895,1854162,00.asp, 2010.
[2]W32/MyDoom.BVirus, TA04-028A.html, 2010.
[3]W32.Sircam.Worm@mm, /venc/data/w32.sircam.worm@mm.html, 2010.
[4]Worm.ExploreZip, http://www.symantec.com/avcenter/venc/data/worm.explore.zip.html, 2010.
[5] R. Naraine, Botnet Hunters Search for Command and ControlServers, http://www.eweek.com/article2/0,1759,1829347,00.asp, 2010.
[6] T. Sanders, Botnet Operation Controlled 1.5m PCs Largest Zombie Army Ever Created, http://www.vnunet.com/vnunet/news/ 2144375/botnet-operation-ruled-million, 2005.
[7] R. Vogt, J. Aycock, and M. Jacobson, “Quorum Sensing and Self-Stopping Worms,” Proc. Fifth ACM Workshop Recurring Malcode (WORM), Oct. 2007.
[8] S. Staniford, V. Paxson, and N. Weaver, “How to Own the Internet in Your Spare Time,” Proc. 11th USENIX Security Symp. (SECURITY), Aug. 2002.
[9] Z.S. Chen, L.X. Gao, and K. Kwiat, “Modeling the Spread of Active Worms,” Proc. IEEE INFOCOM, Mar. 2003
[10] D. Moore, V. Paxson, and S. Savage, “Inside the Slammer Worm,” Proc. IEEE Magazine of Security and Privacy, July 2003.
[11] M. Garetto, W.B. Gong, and D. Towsley, “Modeling Malware Spreading Dynamics,” Proc. IEEE INFOCOM, Mar.2003.
[12] C.C. Zou, W. Gong, and D. Towsley, “Code-Red Worm Propagation Modeling and Analysis,” Proc. Ninth ACM Conf. Computer and Comm. Security (CCS), Nov. 2002.
[13] Zdnet, Smart Worm Lies Low to Evade Detection, http://news. zdnet.co.uk/internet/security/0,39020375,39160285,00.htm, 2010.
[14] J. Ma, G.M. Voelker, and S. Savage, “Self-Stopping Worms,” Proc. ACM Workshop Rapid Malcode (WORM), Nov. 2005.