A NOVEL APPROACH FOR DETECTING SMART CAMOUFLAGING WORM

JEEVAAKATIRAVAN[1], D.HEMAPRIYADHARSHINI[2], C.CHELLAPAN[3] R.DHANALAKSHMI[4]
Assistant Professor [1], PG Scholar [2], Professor[3]
[1,2]Velammal Engineering College, Anna University, Chennai, India.
[4,3]Anna University, Chennai, India
E-mail: jeevaakatir@gmail.com

ABSTRACT

Active Worms wreak havoc by exploiting security loopholes and flaws in software design to propagate from one machine to another. Active Worms are different than a traditional virus in that they don't spread by modifying programs on a single system, but rather by searching for and implanting destructive code onto other systems automatically. In this paper, we propose a novel approach for detecting an intricate type of smart worms called C-Worms. Camouflaging worms (C-Worms) falls under the new category of active worms which conceals its presence by blending with the environment in such a way that it looks analogous to the normal data packet of the network. Thus the propagation of C-Worms and its traffic pattern cannot be determined by the existing worm detection schemes. To countermeasure the C- Worm, we design a new worm detection scheme called Controlled Packet Transmission (CPT) technique where the background traffic is monitored as a function of time. Furthermore, we employ Centralized Worm Detector (CWD) algorithm based on digital signature technique to authenticate each node and monitor the network. Using the CWD algorithm, malicious C-Worm nodes are discarded and the recovered network is monitored. The performance graph obtained experimentally clearly proves that our detection scheme can effectively detect the C-Worm propagation.

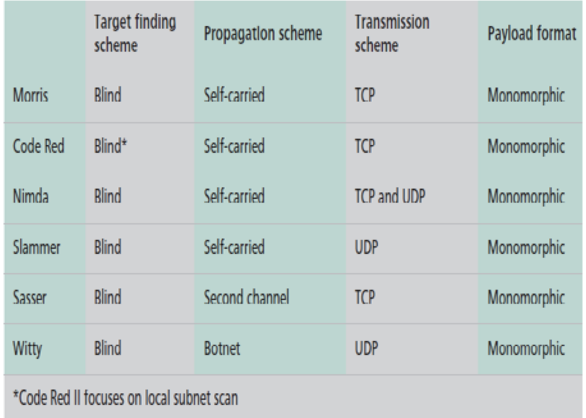
Keywords: *Active worm, Camouflaging worm, Controlled Packet Transmission, Centralized Worm Detector*

1. INTRODUCTION

When internet has become a common household facility and when millions and millions of people from all over the whole world are hooked to this massive worldwide network increase of computer worms is not a rare thing that happens on the internet nowadays. A worm is a computer program that has the ability to copy itself from machine to machine. A worm usually exploits some sort of security hole in a piece of software or the operating system. Based on the spreading nature, worms can be classified as passive worms and active worms. A passive worm does not search for victim machines. Instead, it either waits for potential victims to contact the worm or rely on user behavior to discover new targets. Although potentially slow, passive worms produce no anomalous traffic patterns during target discovery, which potentially makes them highly stealthy.

A. Active Worms

An active worm refers to a malicious software program that propagates itself on the internet to infect other computers. An active worm such as Code Red or the original Morris worm takes advantage of a security hole in a server. It scans through the Internet, looking for machines running that service. Then it tries to break into that service. If successful, it infects the target machine with another copy of itself. Over a period of several hours, it goes from an initial machine to Internet wide contamination. For an active worm to infect a machine, it must first discover that the machine exists. In traditional active worms, each worm instance takes part in spreading worm attack by scanning and infecting other vulnerable hosts in the internet.



	Target finding scheme	Propagation scheme	Transmission scheme	Payload format
Morris	Blind	Self-carried	TCP	Monomorphic
Code Red	Blind*	Self-carried	TCP	Monomorphic
Nimda	Blind	Self-carried	TCP and UDP	Monomorphic
Slammer	Blind	Self-carried	UDP	Monomorphic
Sasser	Blind	Second channel	TCP	Monomorphic
Witty	Blind	Botnet	UDP	Monomorphic

*Code Red II focuses on local subnet scan

Fig 1: Existing Worm Implementation

B. Camouflaging Worm (C-Worm)

Camouflaging worm (C-Worm) is an intricate type of active worm which attempts to remain hidden by sleeping (suspending scans) when it suspects it is under detection. Worms that adopt such smart attack strategies could exhibit overall scan traffic patterns different from those of traditional worms. Since the existing worm detection schemes will not be able to detect such scan traffic patterns, it is very important to understand such smart-worms and develop new countermeasures to defend against them. 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. We note that the propagation controlling nature of the C-Worm (and similar smart-worms, such as “Atak”) cause a slowdown in the propagation speed. However, by carefully controlling its scan rate, the C-Worm can still achieve its ultimate goal of infecting as many computers as possible before being detected and position itself to launch subsequent attacks.

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 computers as possible. We employ a Controlled Packet Transmission (CPT) for monitoring the network traffic and thereby detecting the C-Worm.

2. RELATED WORK

Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao [1] proposed a mechanism for detecting C-Worms based on analyzing the propagation traffic generated by worms. They analyzed characteristics of the C-Worm and conducted a comparison between its traffic and non-worm traffic (background traffic). Observations show that 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. They designed 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.

Zesheng Chen, Lixin Gao, and Chuanyi Ji [2] focuses on effectiveness of defense systems against active worms. It is vital to provide a basic understanding of how efficient the current systems defend against worms, by what way we determine the effectiveness of a defense system, and the guidelines that can be drawn for developing future defense systems. In their work, they have investigated the performance of different host-based defense systems against active worms using a discrete-time (AAWP) model and shown that the ability of worm propagation is constrained by three parameters: number of vulnerable machines, scanning rate, and time to complete infection. Focusing on the Code-Red-v2-like worm, they have performed a quantitative study on how well a system can slow down the propagation of worms.

Senthilkumar G. Cheetancheri, John Mark Agosta, Denver H. Dash [3] proposed a distributed host based worm detection system which presents a method for detecting large-scale worm attacks using only end-host detectors. These detectors propagate and aggregate alerts to cooperating partners to detect large scale distributed attacks in progress. The properties of the host-based detectors may in fact be relatively poor in isolation but when taken collectively result in a high-quality distributed worm detector. A cooperative alert sharing protocol coupled with distributed sequential hypothesis testing to generate global alarms about distributed attacks.

Wei Yu, Xun Wang, Dong Xuan and David Lee [4] presented a new approach for the effective detection of active worms with varying scan rate. They modeled a new form of active worms called Varying Scan Rate worm (the VSR worm). The VSR worm deliberately varies its scan rate and is able to avoid being effectively detected by existing worm detection schemes. The emerging “Atak” worm belongs to this category of worms. To countermeasure the VSR worm, a new worm detection scheme called attack target distribution entropy based dynamic detection scheme (DEC detection) is designed..DEC detection utilizes the attack target distribution and its statistical entropy in conjunction with dynamic decision rules to distinguish worm scan traffic from non worm scan traffic.

Guofei Gu, Monirul Sharif, Xinzhou Qin, David Dagon, Wenke Lee and George Riley [5] proposed a method for the worm detection, early warning and response based on local victim information. Their work concentrates on a simple two-phase local worm victim detection algorithm, DSC (Destination-Source Correlation), based on worm behavior in terms of both infection pattern and scanning pattern. DSC can detect zero-day scanning worms with a high detection rate and very low false positive rate. DSC does not aim to detect all types of worms.DSC aims to detect scan-based, fast - spreading worms. Further, the infection time for hosts is not very long. In other words, DSC may not effectively detect email worms, very slow scanning worm, or sleeper worms with very slow rates of infection. Compared to the fast spreading worms like SQL slammer and CodeRed, slow spreading worms do less damage to networks and are easier to contain, in part because their slower spread rate allows for human intervention.

3. DETECTING THE C-WORM

The C-Worm camouflages its transmission by scheming scan traffic volume during its propagation. The simplest way to manipulate scan traffic volume is to arbitrarily change the number of worm instances performing port-scans. Existing worm detection scheme will not be able to detect such traffic patterns, it is very important to understand such worms and develop new techniques to defend against them. Existing detection schemes depends on an implicit hypothesis that each worm-infected computer keeps scanning the internet and spreads 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. The attackers are using new attack strategies that aim to exploit existing worm detection systems. In particular, “stealth” is one attack strategy used by a recently discovered active worm called “Atak” worm and the “self-stopping” worm evade detection by hiding (i.e., stop propagating) with a fixed period. Worm might also use the evasive scan and traffic morphing technique to hide the detection. In this paper, we have proposed a new detection scheme known as Controlled Packet Transmission (CPT) for detecting such smart worms and monitor the network.

A. Controlled Packet Transmission (CPT) Technique

The controlled packet transmission is used to monitor the network traffic and thus the normal network is differentiated from the network affected by C-Worm. CPT technique has three parameters such as constant energy, constant data rate and constant time delay. As the data rate is maintained constant, the variation from the normal traffic can be clearly determined. By taking time as a function, the traffic is monitored and the graph is plotted for the sent, received and also for the dropped packets. Minimum Time and Maximum Time of packet drop is noted.

B. Network Normal Traffic Analysis

The packet which is sent by the sender traverses the network. In wireless network, there will be a considerable drop during the transmission of packets. The drop of packets is plotted against the time which clearly shows the overall drop in the network. Also the sent packets and received are monitored and their data rate is maintained constant with constant energy. As a result, the overall graph is obtained which compares the drop of the network with the number of sent packets.

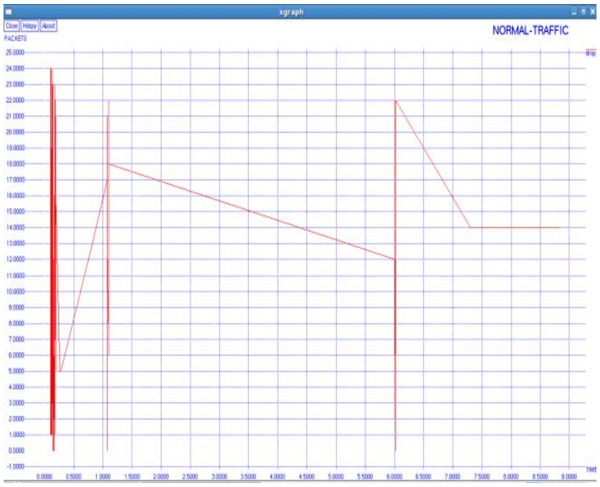


Fig 2: Drop In The Normal Traffic

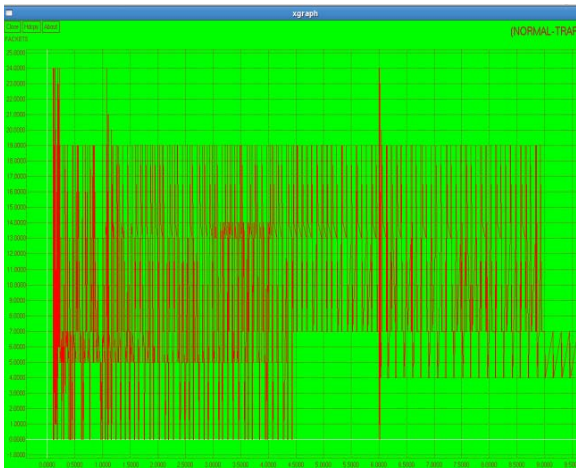


Fig 3: Sent Packets In The Normal Traffic

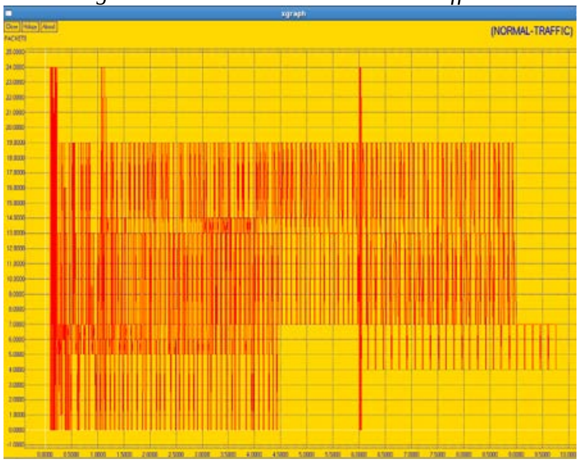


Fig 4: Received Packets In The Normal Traffic

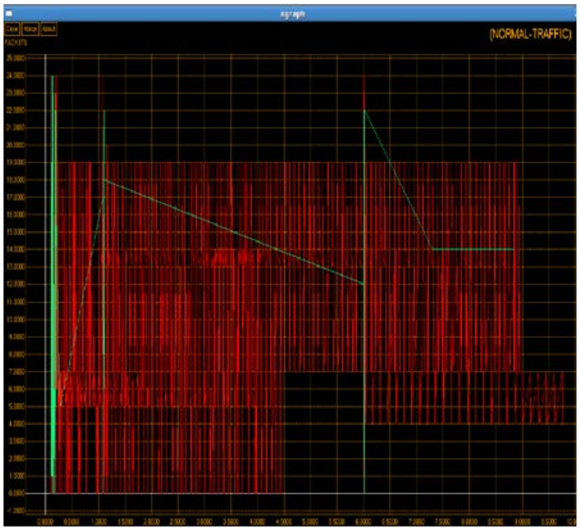


Fig 5: Comparison Between The Drop And Sent Packets In The Network

C. C-Worm Propagation

Camouflaging worms (C-Worms) falls under the new category of active worms which conceals its presence by blending with the environment in such a way that it looks analogous to the normal data packet of the network. Thus the propagation of C-Worms and its traffic pattern cannot be determined by the existing worm detection schemes. Our method of Controlled Packet Transmission (CPT) maintains a table with constant energy, data rate and constant time delay. For example, if the time delay between the packets in the queue is 2ms, the normal node will transfer 2 packets. At the same time, C-Worm will transfer 4 packets. This transmission will vary for time since C-Worm will often move to sleeping mode when it is suspected under detection. So when a constant time delay and constant data rate is maintained, CPT technique monitors the network. The density of the graph at the region where the packet transmission is higher can be clearly demonstrated .By comparing the overall graph of the normal traffic and the C-Worm traffic we detect the presence of C-Worms.

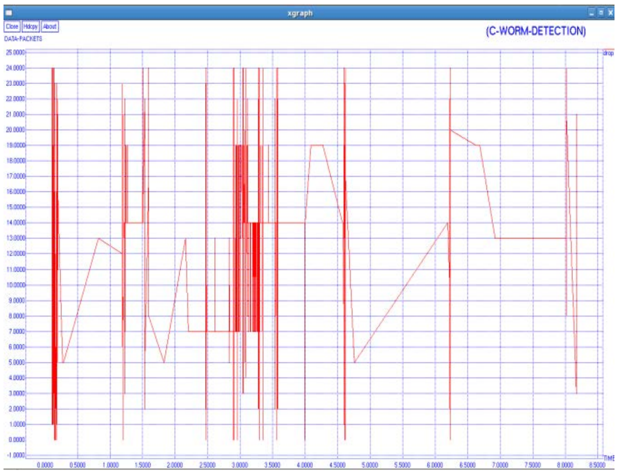


Fig 6: Drop During C-Worm Propagation

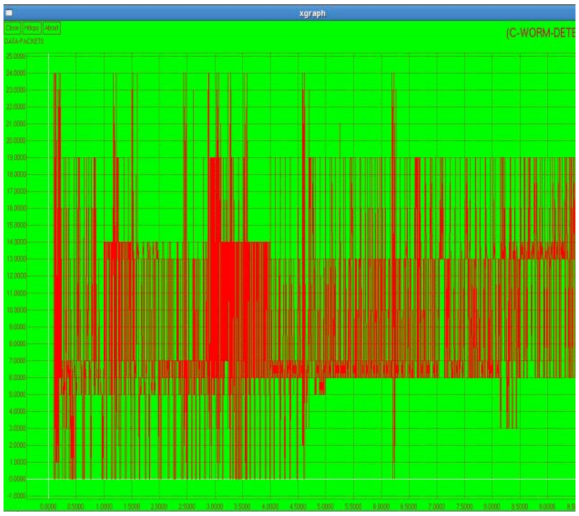


Fig 7: Sent Packets During C-Worm Propagation

Figure 6 and 7 evidently shows the transmission of large number of packets. Also by comparison, the time where the network experienced a drop in the drop graph is compensated by the packet transmission by the C-Worm. It is noted to be an abnormal packet transmission and the graph becomes dense over this time of transmission.

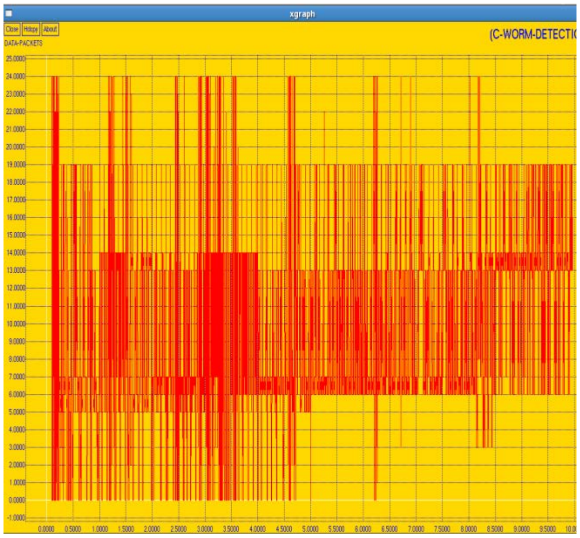


Fig 8: Received Packets During C-Worm Propagation

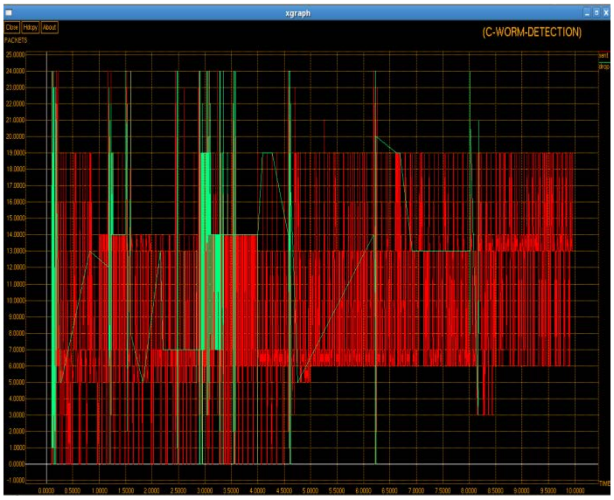


Fig 9: Comparison Between The Drop And Sent Packets During C-Worm

4. RECOVERY OF THE NETWORK

Our CPT technique effectively detects the presence of C-Worms. Our next aim is to detect the C-Worm node and recover the network which is affected by the C-Worms. Hence to accomplish our idea, we have developed a secure and an effective algorithm based on the method of digital signature called Centralized Worm Detector (CWD). CWD enables the authentication of nodes on packet transmission. Using our CWD algorithm, we try to recover the nodes from the C-Worm.

A. Centralized Worm Detector (CWD) Algorithm

CWD algorithm is based on the digital signature technique which authenticates each packet transmitted between nodes. During packet transmission, each node attaches its own digital signature to the packets. Digital Signatures are based on Public Key Technology that uses asymmetric cryptography. Each person's identity is related to a key pair - a private key and a public key. These keys are nothing but mathematical codes generated on your computer. The private key is under its owner's sole control and the public key is distributed to everyone without any risk to security. The private key is used for signing and the public key is used for verification. A Certifying Authority identifies and proofs individuals before issuing digital certificates to them.

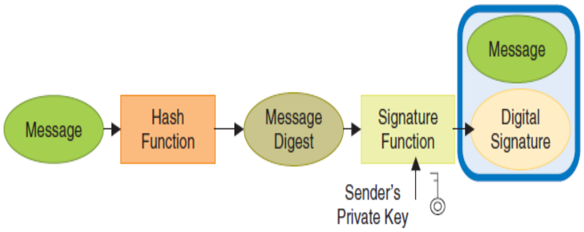


Fig 10: Digital Signature Creation

Our assumption which we used to develop CWD algorithm is that digital signatures will be in encrypted hexadecimal format. Each node in the network has its own signature and they are tamper resistant so that it cannot be duplicated by any other node. Nodes which transmit the packet will attach its digital signature with the transmitted packet. At the receiver, the node uses the public key to decrypt the encrypted signature. This assumption works only if the sender is a normal node. In case of C-Worms, the sender C-Worm node will generate the signature. But at the receiver it cannot be decrypted with the public key. The reason is that C-Worm cannot tamper the digital signature of the legitimate sender node. So the C-Worm node generates digital signature of its own.

Developing a solution for authenticating each node, we introduce our Centralized Worm Detector (CWD) algorithm. In this technique, we maintain a master node which is a centralized node. Master Node is intended to maintain the digital signatures of all the legitimate nodes in the network. Whenever the packet is sent by a sender node, its been stamped with the signature of the sender. The receiver tries to decrypt this signature using the public key in common. If it can decrypt, the receiver node will accept the packet. Else, it will send the digital signature to the master node. The master node will check for the signature. If it is present, then it intimates the node which raised the request to allow the packet in the network. If the signature is not present, then it will block the packet and discard the node from which the packet has been received. Thus by this centralized approach we can recover the network from the propagation of C-Worms and also any type of Worms.

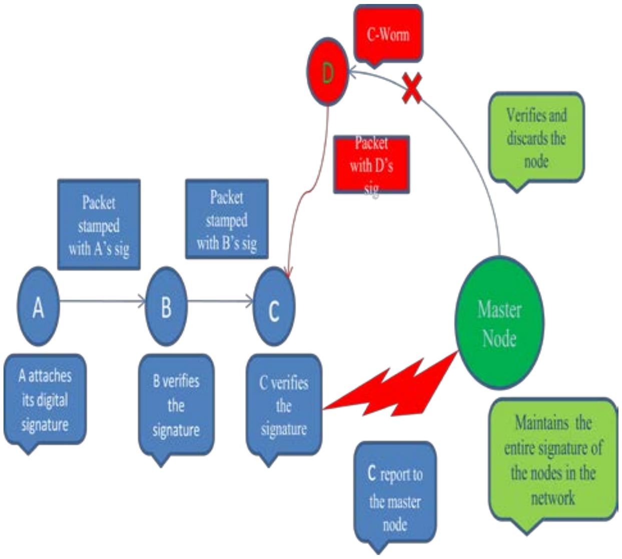

C-Worm
D
Packet with D's sig
Verifies and discards the node
Packet stamped with A's sig
Packet stamped with B's sig
A
B
C
Master Node
A attaches its digital signature
B verifies the signature
C verifies the signature
C report to the master node
Maintains the entire signature of the nodes in the network

Fig 11: Centralized Worm Detector Mechanism

5. CONCLUSION

In this paper, we have developed a new mechanism for detecting the smart natured active worm called C-Worms. C-C-Worms naturally tend to conceal its presence and transmit the packets which will be similar to a normal packet. But the rate at which it transfers the packets differs from the normal packet. By taking this idea as a key factor we developed a mechanism called Controlled Packet Transmission (CPT) technique which effectively detects the propagation of C-Worms by taking three parameters: 1) Constant energy 2) Constant data rate 3) Constant time delay. From the graphs generated from the experimental results differentiates the normal traffic and C-Worm traffic. Also we proposed an algorithm called Centralized Worm Detector (CWD) which gives an efficient way to recover the network from C-Worm as well as from any other worms. Thus through this paper we have given effective methods to detect the C-Worm and recover the network from C-Worm.

REFERENCES

[1]. Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao “Modeling and detection of camouflaging worm”, IEEE transactions on dependable and secure computing, vol. 8, no. 3, may/june 2011.

[2]. Zesheng Chen, Lixin Gao, and Chuanyi Ji “On Effectiveness of Defense Systems against Active Worms”, Dissertation Abstracts International, 2007 - csa.com.

[3]. Senthilkumar G. Cheetancheri, John Mark Agosta, Denver H. Dash "A Distributed Host based Worm Detection System", Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, ISBN:1-59593-571-1.

[4]. Wei Yu, Xun Wang, Dong Xuan and David Lee "Effective Detection of Active Worms with Varying Scan Rate", Securecomm and Workshops, 2006 , IEEE Digital library.

[5]. Guofei Gu, Monirul Sharif, Xinzhou Qin, David Dagon, Wenke Lee and George Riley "Worm Detection, EarlyWarning and Response Based on Local Victim Information", Computer Security Applications Conference, 2004.

[6]. Frank Akujobi, Ioannis Lambadaris, Evangelos Kranakis "Modeling host-based detection and active worm containment", Proceedings of the 11th communications and networking simulation symposium, 2008

[7]. Sumeet Singh, Cristian Estan, George Varghese, Stefan Savage "The EarlyBird System for Real-time Detection of Unknown Worms", Technical Report CS2003-0761, University of California, San Diego,. August 2003.

[8]. Pele li, Mehdi salour, and Xiao su, San jose state university "Asurvey of internet worm detection and containment", surveys IEEE Communications, electronic magazine of Original peer-reviewed survey article, 1st quarter 2008, volume 10, no. 1.

[9]. Jun Li, Paul Knickerbocker "Functional similarities between computer worms and biological pathogens", Elsevier computers & security 26 (2007) 338 – 347.

[10]. 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.

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

[12]. Z.S. Chen, L.X. Gao, and K. Kwiat, "Modeling the Spread of Active Worms," Proc. IEEE INFOCOM, Mar. 2003.

[13]. 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.

[14]. 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 (SECURECOMM), Sept. 2007.

[15]. X. Wang, W. Yu, X. Fu, D. Xuan, and W. Zhao, "iloc: An Invisible Localization Attack to Internet Threat Monitoring Systems," Proc. 27th IEEE INFOCOM, Apr. 2008.

[16]. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "The spread of the sapphire/slammer worm," Tech. Rep., Jan. 2003, http://www.caida.org/outreach/papers/2003/ sapphire/ sapphire.html.

[17]. C. C. Zou, L. Gao, W. Gong, and D. Towsley, "Monitoring and early warning for internet worms," Department of Computer Science, Univ. of Massachusetts, Amherst, Tech. Rep. TR-CSE-03-01, 2003.

[18]. D. T. C. Zou, W. Gong, and S. Cai, "Routing Worm: A Fast, Selective Attack Worm Based on IP Address Information," *Proc. 19th ACM/IEEE/SCS Wksp. Principles of Advanced and Distrib. Simulation*, 2005.

[19]. D. G. Glazer, "Computer Worms," May 2005, http://www.research.umbc.edu/~dgorin1/is432/worms.htm.

[20]. B. M. J. Lockwood, "Design of a System for Real-Time Worm Detection," *Proc. 12th IEEE Annual Symp. High Perf. Interconnects*, 2004.

[21]. B. K. H. Kim, "Autograph: Toward Automated, Distributed Worm Signature Detection," *Proc. 13th USENIX Sec. Symp.*, 2004.

[22]. M. E. D. Kienzle, "Recent Worms: A Survey and Trends," *Proc. ACM WORM '03*, 2003.

[23]. P. A. S. Antonatos, E. P. Markatos, K. G. Anagnostakis, "Defending Against Hitlist Worms Using Network Address Space Randomization," *Proc. ACM WORM '05*, 2005.

[24]. C. W. C. Wong *et al.*, "Dynamic Quarantine of Internet Worms," *Proc. Int'l Conf. Dependable Sys. and Networks*, 2004.

[25]. L.-H. L. David Brumley, Pongsin Poosankam, and Dawn Song, "Design Space and Analysis of Worm Defense Strategies," *Proc. ACM Symp. Info., Comp. and Commun. Sec.*, 2006.