C-Worm Traffic Detection using Power Spectral Density and Spectral Flatness Measure

Sushma Mergu[1], G. Dileep Kumar[2]
Post Graduate Student, Assistant Professor
[1], [2](Department of CSE, SR Engineering College, AP, India)

Abstract: *As Internet and its technologies are improving with rapid pace, there are security threats growing with same pace. The malicious software such as worm is causing such threats to IT systems linked to information super highway. The worms are capable of replicating themselves and infect systems over network. Their traffic propagation can be detected by employing anti worm or virus software. However, there is a new type of worm that can camouflage itself so as to prevent anti worm software from identifying it. The difference between normal worm's traffic and C-worm's traffic can't be found when time domain is considered. However, in terms of frequency definitely it can be differentiated. Based on this hypothesis, this paper presents novel schemes such as PSD and SFM that are capable of differentiating the traffic of C-worm from background traffic. The empirical results revealed that our schemes are effecting in detecting camouflaging worms effectively besides identifying normal worms.*

Keywords *– Traffic propagation, worm, camouflaging worm, time domain, and frequency domain.*

I. Introduction

Worm is a word with broad meaning. It refers to any program which is malicious in nature. Such program could be a VIRUS, worm etc. They have common features which are also there with biological virus. The common features include that they replicate themselves and also propagate from one machine to another machine. The means of propagation is only through infected storage media and also networks of all kinds including those without wire. Active worms continuously strive to propagate themselves to other systems and make them insecure. This is a problem which has been around ever since the world came across malicious programs for the first time. Some worms include Slammer [2], Sasser [3] and Code-Red [1]. Some worms will work together by forming bonnets and cause more damage to IT systems. The attacks made by such worms include DDoS; attack to obtain sensitive information; destroying data [5] and also put forth unwanted materials such as advertisements. Many such worms are commonly known as malware (malicious software). This includes virus as well. The virus could be boot sector virus, file virus, love virus, time bomb virus, Trojan virus and so on. There is enough evidence in the history that some people have made it their business to create malware and also solutions to prevent them. This is major problem in the world of computers. This man made evil will continue posing threats to IT systems and also cause the businesses to loose confidential information and thus loosing confidence and profits in the business [4], [6].

Researchers also predicting the possibility of malicious programs such as bonnets to collaborate and cause more security threats to IT world. Such collaborated bonnets is known as super bots [7]. As there were reports of worms causing major damage to IT systems, the past few years saw significant research in the area of worms. Worm detection and prevention is an essential task required by all systems involved in IT. Thus the presence of anti-worm software is felt and the same is done through research. The process of identifying the worms by observing their scan traffic much anti-worm software succeed in detecting and also preventing any damage to IT systems. The emergence of Internet and also other networking facilities and communication systems paved way for the increase of threats caused by worms. Studying different kinds of worms and their impact on the IT systems and also prevention techniques are to be given paramount importance. When a worm infects a system, it will propagate its traffic in the system to cause damage to its data. It also strives to propagate the traffic to other systems though infected storage media and networks to other systems in the real world. They keep on identifying IP addresses of systems in the world and infect them though the ways known to them. The common way they follow is generating scan traffic in the time domain and frequency domain. Thus they make all the systems attacked by worms vulnerable to security threats. There is a possibility of loosing companies' sensitive information that leads to collapse of business or losing in revenues in large scale. The patterns of the worms [2], [8], [9] are increasing day by day. The more patterns of worm propagation is known, the more possibility to detect and prevent them. The assumption of all software in the world that is sued to combat worms is that the worms generate scan traffic and try to replicate themselves and infect systems in the same network and remote networks. The patterns are generally having same characteristics so as to enable anti-worm to detect them. However, a new class of worm has come into existence. This new worm is capable of hiding its presence.

It is more dangerous than any other worm. Its name is camouflaging worm (C-worm) as the name suggests, it is capable of hiding its scan propagation so as to let the anti worm software believe that there is no worm exists in the system. That is the reason, this special worm is known as Camouflaging Worm (C-worm).

The attackers are constantly increasing their tactics. They are trying to write malicious programs or worms that can hide and defeat the worm detection systems available in the real world. Thus they are making stealth attack successfully as the worm detection systems fail to distinguish the scan traffic of normal's worms and camouflaging worms with respect to time and frequency domains [10], [11]. The C-worm is capable of hiding its traffic or stopping scan traffic when it detects the process of detecting worm in the system. Thus it is hiding itself in such a way that the normal worm detecting systems are not capable of detecting it easily. They can't distinguish the traffic of scan with respect to time and frequency domains. They may be able to detect differences in time domain but fail in detecting in frequency domain. A new scheme is required in order to detect such worms that do not reveal any presence of it to the worm detection systems in general. As it is quite different from other worms, it hides any noticeable traffic that reflects its presence. To achieve this, it manipulate scan traffic in such a way that the traffic can't be detected by the systems where worm detection schemes are running. Therefore, the worm detecting systems are useless in case of C-worms that cause more damage to IT systems when compared with traditional worms [12], [13]. The C-worms are capable of achieving their goal of propagating the systems in the real world and cause damage to the systems without being detected by worm detecting systems.

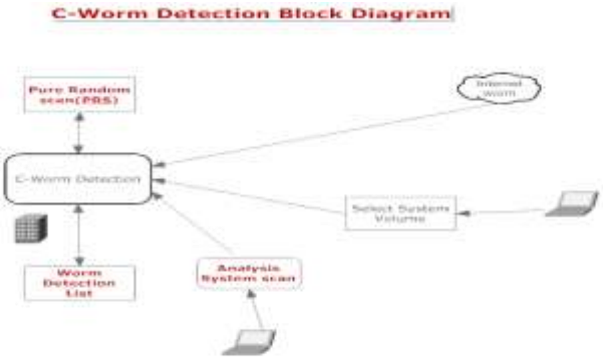

Fig. 1: Block Diagram for C-Worm Detection

We propose new schemes in detecting C-worms in this paper. We achieve this based on the hypotheses that make two points clear. The first point is that C-worms traffic is different form other worms. The second important point is that it is not possible to differential scan traffic of C-worms with traditional worms in time domain. However, they can be distinguished to find differences in terms of frequency domain. These hypotheses make it easy to make experiments and prove the hypotheses with relative ease. This observation makes difference between the detection of worms and also C-worms. In the proposed system we develop two new schemes that make it possible. They are not able to differentiate normal worms and C-worms in terms of time domain while they are capable of detecting such patterns of worms in the frequency domain. PSD and SFM are the two techniques that are used to achieve the worm detection system with a difference. For every PSD the c-worm traffic shows less SFM and this is the evidence that the camouflaging worm hides itself and when reported this is known to others as well. The scan traffic of the C-worm could be based on the port number of IP address. It uses both based on the requirement. The experiments reveal that our schemes are effective when compared with many existing worm detection systems. Moreover, we also used many metrics such as DR (Detection Rate) and DT (Detection Time) and MIR (Maximal Infection Ratio) in order to evaluate the efficiency of the proposed schemes.

II. Related Work

Worms are similar to biological viruses that cause damage to health of human beings and other animals. They have features like self-propagation and replication. These features are with malicious programs that cause problems to computers in the given network. Such malware is known as worms. The worm which is scanning traffic through IP address and also port number of systems and trying to propagate itself to new systems in the networking domain is known as active worm. As the worms are capable of damaging IT systems, the need for research to prevent the same has been felt. In accordance with this, researchers spend considerable time on this topic and still it needs further improvements [9], [16]. Active worms can use many ways in which they can propagate themselves from one system to another system. One such way is Pure Random Scan (PRS). This is a kind of scan in which the worms continuously and randomly find IP addresses an ports of other systems and propagate itself to those systems which IP addresses are known to the worm. Other ways in which worms can propagate include file sharing, email, network port scanning and instant messaging or chatting [17].

When some IP addresses are known to the worms, they try to propagate themselves by maintaining a hit list and following the strategies to propagate themselves into those systems whose IP addresses are scanned by worm. The worms also split IP address space in order to avoid repetition of work and thus they divide and conquer in terms of scanning and propagating themselves into new networks. Some researches also considered developing a new topology that is attack resilient with respect to works [18], [19].

There is a special category of worm that is quite different from the other worms described above. This worm is capable of manipulating its scan traffic and thus making it possible that the traditional worm detecting systems fail to help in this regard. A new comaflagig worm thus created is causing more damage to IT world as it is not detected by conventional anti-worm programs. Essentially the worms that hide their scan traffic are polymorphic in nature [20], [21]. Such worms are known as Camouflaging worms as they are hiding their presence and making the normal worm detection systems vulnerable. With respect to stealthiest, the normal worm and C-worm are having certain similarities. Both are generating same traffic and finding the similarities such as both can detect the difference between the normal traffic and worm's scan traffic. The other main difference between them is that the traditional worm detectors can't find difference while the proposed scheme can distinguish the traffic of the C-worm in the time domain. However, it is challenging to find such result from other schemes. The proposed scheme finds the difference in scan traffic of normal worm and systematic in frequency domain though in time domain it can't differentiate the existing worms and new kind of worm known in frequency domain. The new class of worm is named "C-Worm". Due to self propagation nature of C-worm and its ability to manipulate to hide its presence in the system by camouflaging technique. The actual detection of worms is provided in the next section.

2.1 Worm Detection

The detecting of worms is the research that has been around for the past many years. The reason for this kind of research is to protect IT systems by preventing malicious code from entering into our network. The detection systems of worm are of two types. They are known as host – based detection and the second one is network-based detection. Host based detection systems are to analyze the scan traffic in the hosts they are available. They identify and prevent worms whose main purpose is propagating from one system to another system and spoil the whole communication system. [23], [24]. The network based systems for detecting worms use different approach. They use IP addresses of the scanned systems and then try to propagate themselves. Many researchers worked on these kind of systems [12], [13]. The worms that spread to other machine can be prevented by employing effective worm detection systems. However, the existing worm detection systems are not adequate special type of worms such as C-worm can't be detected by them. A network based systems are widely used and the wide spreading of worms is a proven fact, it is evident that new schemes are essential to combat such special kind of worms both in terms of both time domain and also frequency domain. As traffic is not confined to a particular system and it is related to networks, it is essential that the proposed scheme must be of type network-based worm detection system. In the Internet there must be a provision to detect worms such as Cyber center [8], network telescope [25] and SANSISC [15]. The detections systems can be spread across WWW in order to successfully detect the presence of worms successfully. Each monitor passively monitor sings either IP address or using port numbering through the network based detection systems. Such network based detection systems are capable of analyzing the scan traffic so worms and recognizing them. Many proposed systems in the literature [13], [14] are able to provide statistics and analyze patterns generated by worms. These schemes are based on the global scan traffic monitoring and detection of anomalous traffic [21], [2]. A state-space feedback control model is presented by [26] in order to detect and control spread of worms and viruses. This is done by measuring the velocity of the new connections made by an infected computer. However, the approaches that analyze scan traffic of worms are mainly used in developing detection systems.

III. Modeling Of The C-Worm

The C-Worm modeling is based on our observations that have been made after some research. The C-worm block diagram is shown in fig. 1. The initial research revealed that the C-Worm is not same as other worms though it has similarities with normal worms. The normal worms perform scan traffic in order to replicate themselves and also propagate from one system to another system in a network environment. The same is followed by C-Worms also. However, there are two observations made clearly. The first observation is that, the C-Worm scan traffic involves IP addresses and port numbers and scan traffic is different from normal worms. The second observation is that the detection systems can't find the difference between scan traffic of C-worms and normal worms in terms of frequency domain. In time domain they appear to be same. The second observation also reveals that it is essential to differentiate the C-Worm traffic from other worm's traffic only in frequency domain. Based on these observations, our experiments are made. Our experiments focused on the traffic analysis and frequency domain and the results revealed that our scheme is capable of detecting C-Worms. When our scheme launches, it analyzes the dynamics of C-Worm traffic in Internet. It follows a theory known as control system theory [27]. In order to demonstrate effectiveness of the proposed scheme, the overall traffic flow of C-Worm should be slow so as to show the detection process effectively. Control parameters are introduced to this effect such as attack probability on each infected computer. This indicates the probability in which C-Worm participates in the propagation of the worm. The control parameter in our model is generic in nature and its value is 1 indicating traditional worms and other value for C-Worms. In the process of modeling camouflaging worm, the following characteristics are followed.

- The traffic of C-worm is similar to non-worm traffic in terms of time domain. This means that over a period of time the scan traffic of the normal worm and C-worm is same.
- C-Worm does not show any trends while its propagation so as to hide its presence effectively.
- The average traffic of Worm is sufficient to model the C-Worm propagation model faster in order to cause rapid damage on the Internet.

We assume that the worm attacker manipulates scan traffic and the scan traffic of C-Worm follows different random distribution means.

3.1 Propagation Model of C-Worm

Epidemic dynamic model is used to work with the propagation model of C-Worm [2], [9]. This model assumes any given computer should be in one of the following states. The states are vulnerable, immune and infected. Immune state computer can't be infected. The vulnerable computer is the one that can be infected by C-Worm. The infected state does mean that the system is already infected. The epidemic model for the traditional PRS is represented as:

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

The epidemic model for the C-Worm propagation is represented as:

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

IV. Performance Evaluation

Performance of the proposed scheme is evaluated using some evaluation metrics known as IR, DT, and MIR. The detection time is the time taken to detect C-Worm. MIR provides ratio of number of infected computers and total number of vulnerable computers. The higher the values of these metrics, the more effective the attacks are. The lower these values are, the lower the effectiveness of attacks.

4.1 Simulation Setup

The experiments are made both for normal and C-Worm traffic. The total number of vulnerable computers is assumed to be around 30000. By varying parameters C-Worm attacks are simulated. The detection involved port scan traffic and also non worm traffic. Logs and traffic traces are used to observe the behavior of worms. The detection results of C-Worm are provided in Table1.

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

Table 1: Detection results for C-Worm

Table 1 shows the results of detection with various parameters and also with various evaluation schemes such as DR (Detection Rate), MIR (Maximal Infection Ratio) besides providing the detection time in minutes.

4.2 Detection Performance for Traditional PRS Worms

The detection performance of traditional PRS worms is presented in fig. 3 and 4. The results use evaluation metrics such as MIR and DR respectively.

Maximal Infection Ratio of PRS Worm

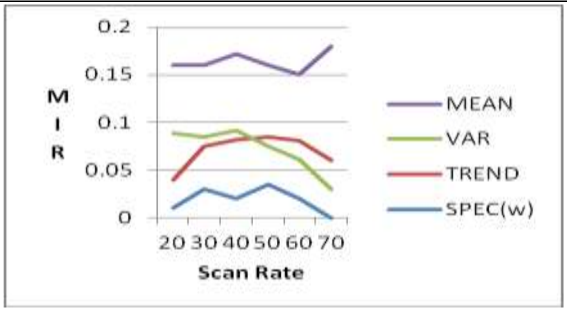

Fig. 2: Maximal Infection Ratio of PRS Worm

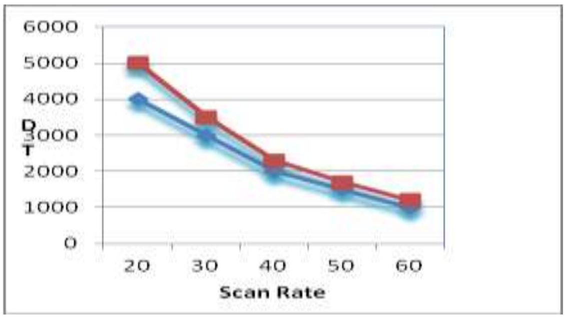

Fig. 3: Detection Time of PRS Worm

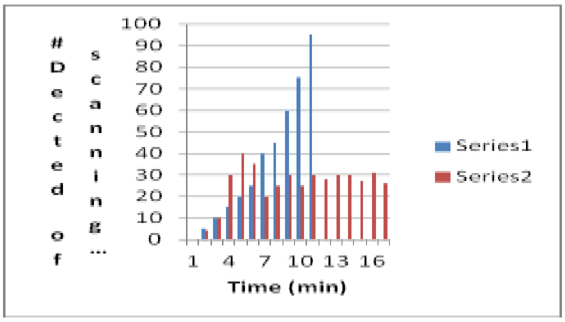

Fig. 4: Number of Detected Scanning Hosts on Camouflaging Worm

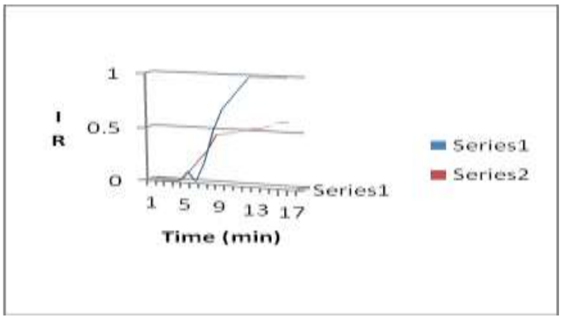

Fig. 5: Infected Ratio for the C-Worm and PRS Worm

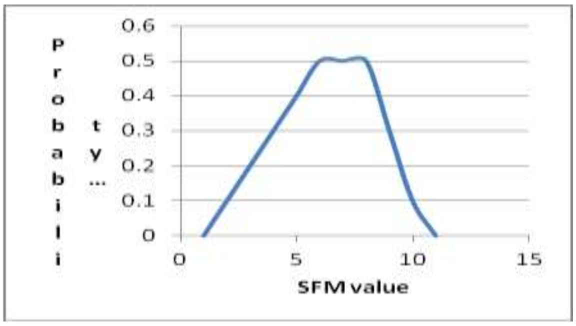

Fig. 6: PDF of SFM on normal non-worm traffic

V. Conclusion

A new type of malware or worm is studied in this paper. The worm known as Camouflaging Worm, as the name implies, can hide its propagation and scan information from the worm detection systems and cause damage to IT systems. As the conventional detection systems can't identify the presence of such worm, we developed a scheme that can identify the C-Worm in terms of frequency domain. The modeling and detection of this worm is based on the observations we made. The observation include, the C-Worm also propagates by scanning IP addresses of the systems in the network. The second observation is that in the frequency of the scanning the C-Worm is different from other worms. These two observations are used as hypotheses in this paper and the research is made based on these hypotheses. The practical work and the results reveal that the hypotheses are fully supported or proved to be correct.

References

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

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

[3] CERT,CERT/CCAdvisories, http://www.cert.org/advisories/,2010.12 IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 3, MAY/JUNE 2011

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

[5] R. Naraine, Botnet Hunters Search for Command and Control Servers,http://www.eweek.com/article2/0,1759,1829347,00.asp, 2010.

[6] R. Vogt, J. Aycock, and M. Jacobson, "Quorum Sensing and Self-Stopping Worms," Proc. Fifth ACM Workshop Recurring Malcode (WORM), Oct. 2007.

[7] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time," Proc. 11th SENIX Security Symp. (SECURITY),Aug. 2002.

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

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

[10] C. Wright, S. Coull, and F. Monrose, "Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis," Proc. 15th IEEE Network and Distributed System Security Symp. (NDSS), Feb. 2008.

[11] 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.

[12] S. Venkataraman, D. Song, P. Gibbons, and A. Blum, "New Streaming Algorithms for SuperSpreader Detection," Proc. 12th IEEE Network and Distributed Systems Security Symp. (NDSS), Feb.2005.

[13] J. Wu, S. Vangala, and L.X. Gao, "An Effective Architecture and Algorithm for Detecting Worms with Various Scan Techniques,"Proc. 11th IEEE Network and Distributed System Security Symp.(NDSS), Feb. 2004.

[14] SANS, Internet Storm Center, http://isc.sans.org/, 2010.

[15] C.C. Zou, W. Gong, and D. Towsley, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense,"Proc. First ACM CCS Workshop Rapid Malcode (WORM), Oct. 2003.

[16] C. Zou, D. Towsley, and W. Gong, "Email Worm Modeling and Defense," Proc. 13th Int'l Conf. omputer Comm. and Networks (ICCCN), Oct. 2004.

[17] Y. Li, Z. Chen, and C. Chen, "Understanding Divide-Conquer-Scanning Worms," Proc. Int'l Performance Computing and Comm.Conf. (IPCCC), Dec. 2008.

[18] D. Ha and H. Ngo, "On the Trade-Off between Speed and Resiliency of Flash Worms and Similar Malcodes," Proc. Fifth ACM Workshop Recurring Malcode (WORM), Oct. 2007.

[19] L. Martignoni, D. Bruschi, and M. Monga, Detecting Self-Mutating Malware Using Control Flow Graph Matching," Proc.Conf. Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), July 2006.

[20] R. Perdisci, O. Kolesnikov, P. Fogla, M. Sharif, and W. Lee,"Polymorphic Blending Attacks," Proc. 15th USENIX Security Symp. (SECURITY), Aug. 2006.

[21] Linux.com,UnderstandingStealthScans:orewarnedis Forearmed,http://security.itworld.com/4363/LWD010321vcontrol3/page1.html, 2010.

[22] J.Z. Kolter and M.A. Maloof, "Learning to Detect Malicious Executables in the Wild," Proc. 10th ACM SIGKDD, Aug. 2004.

[23] 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.

[24] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The Internet Motion Sensor: A Distributed Blackhole Monitoring System," Proc. 12th IEEE Network and Distributed Systems Security Symp. (NDSS), Feb. 2005.

[25] R. Dantu, J.W. Cangussu, and S. Patwardhan, "Fast Worm Containment Using Feedback Control," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 119-136, Apr.-June 2007.

[26] K. Ogata, Modern Control Engineering. Pearson Prentice Hall, 2002.

About The Authors

	Sushma Mergu received the B.Tech Degree in Computer Science and Engineering from Kamala Institute of Technology and Science, Karimnagar, A.P, India. Currently doing M.tech in Computer Science and Engineering at SR Engineering College, Warangal, India. Her research interests include Networking and Security.
	G.Dileep Kumar received the B.Tech degree in Computer Science & Engineering from JSN College of Engineering & Technology, Kaghaz nagar, India and M.Tech degree in Software Engineering from Ramappa Engineering College, Warangal, India. Currently he is an Assistant Professor in the department Computer Science & Engineering, SR Engineering College, Warangal, India. His research interests include Data Mining, Network Security and Mobile Adhoc Networks.