Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.568 – 573

RESEARCH ARTICLE

A Novel Approach of Detecting the Camouflaging Worm

HEMALATHA R[1], S. PRATHIBA[2]
[1]Department of Information Technology, Bharath University, India
[2]Department of Information Technology, Bharath University, India

Abstract— Active worms 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. In this paper, we investigate 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 analysing the propagation traffic generated by worms. We analyse characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and nonworm traffic (background traffic). We observe that these two types of traffic are barely distinguishable in the time domain. However, their distinction is clear in the frequency domain, due to the recurring manipulative nature of the C-Worm. Motivated by our observations, the design a novel spectrum-based scheme to detect the C-Worm. Our scheme uses the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to distinguish the C-Worm traffic from background traffic. Using a comprehensive set of detection metrics and real-world traces as background traffic, we conduct extensive performance evaluations on our proposed spectrum-based detection scheme. The performance data clearly demonstrates that our scheme can effectively detect the C-Worm propagation. Furthermore, we show the generality of our spectrum-based scheme in effectively detecting not only the C-Worm, but traditional worms as well.
In the existing system, traditional worms are more threats to the internet and also would produce lot of overall network traffic. It is very easy to identify the worm using traditional worm detection as the overall network traffic is increased. In the proposed model, camouflage worm is modelled and detection using spectrum based approach. Worm targets only vulnerable node so that overall traffic level is not increased. Spectrum based approach which is used to kill the C-worm. Modifications are mode in designing a worm which is used to increase the CPU load in the system, and also compared with traffic level of an application initiation and the C-worm. This process makes very clear process of execution.

Key Terms: - Worm; Camouflaging Worm; Power Spectral Density; Spectral Flatness Measure

I. INTRODUCTION

AN active worm refers to a malicious software program that propagates itself on the Internet to infect other computers. The propagation of the worm is based on exploiting vulnerabilities of computers on the Internet. 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. These botnets can be used to:

1. Launch massive Distributed Denial-of-Service (DDoS) attacks that disrupt the Internet utilities

2. Access confidential information that can be misused through large-scale traffic sniffing, key logging, identity theft, etc.,

3. Destroy data that has a high monetary value

4. Distribute large-scale unsolicited advertisement emails (as spam) or software (as malware).

There is evidence showing that infected computers are being rented out as "Botnets" for creating an entire black-market industry for renting, trading, and managing "owned" computers, leading to economic incentives for attackers. Researchers also showed possibility of "super botnets," networks of independent botnets that can be coordinated for attacks of unprecedented scale. For an adversary, super botnets would also be extremely versatile and resistant to countermeasures. Due to the substantial damage caused by worms in the past years, there have been significant efforts on developing detection and defense mechanisms against worms. A network-based worm detection system plays a major role by monitoring, collecting, and analyzing the scan traffic (messages to identify vulnerable computers) generated during worm attacks.

The influence of the network characteristics on the virus spread is analyzed in a new the intertwined Marko chain model, whose only approximation lies in the application of mean field theory. The mean field approximation is quantized in detail. The intertwined model has been compared with the exact 2-state Markov model and with previously proposed "homogeneous" or "local" models. The sharp epidemic threshold, which is a consequence of mean field theory, is rigorously shown to be equal to1, where max is the largest eigenvalue the spectral radius—of the adjacency matrix. A continued fraction expansion of the steady-state infection probability at node is presented as well as several upper bound The model belongs to the class of susceptible infected susceptible (SIS) models that, together with the susceptible infected removed (SIR) models, are the standard models for computer virus infections. Each node in the network is either infected or healthy. An infected node can infect its neighbors with an infection rate, but it is cured with curing rate. However, once cured and healthy, the node is again prone to the virus. Both infection and curing processes are independent. Refinements like the existence of an incubation period, an infection rate that depends on the number of neighbours, a curing process. That takes a certain amount of time, and other sophistications are not considered.

The theory of the spreads of epidemics through a network can be applied to the spread of e-mail worms and other computer viruses, the propagation of faults or failures, and, more generally, the spread of information (e.g., news, rumours, brand awareness, and marketing of new products) and epidemic dissemination or/and routing in ad hoc and peer-to-peer networks.

II. RELATED WORK

A. In the context of the Internet, net-work fragmentation is well known and occurs in many situations, including an increasing preponderance of network address translation, firewalls, and virtual private networks. Recently, however, new threats to Internet consistency have received media attention.

The issues fall into two categories: Conflict concerning naming and the use of geo location to restrict access to resources. First, a number of nations have raised formal objections to the oversight of ICANN by the United States, and a number of private organizations such as Unified Root have emerged to offer alternative name spaces. Global agreement on Internet governance is becoming increasingly difficult, which means the potential for inconsistency in naming resulting from multiple Domain Name Service (DNS) roots or addresses that are not globally unique will only increase. To a significant extent, the Internet depends upon everyone having access to the same set of names. The threats, therefore, are a) the same name does not exist in both of two locations (lack of global consistency), and b) the same name refers to different resources in different locations (lack of global uniqueness).Second, a perceived increase in online criminal activity has created viable business models for businesses that provide geo location services marketed for about how a user is connected to the Internet (such as IP address and Internet service provider (ISP) data) to determine whether the user is likely to be fraudulent. This has caused a number of legitimate online transactions to be denied when users are not connected at their usual point of attachment. Finally, various governments and service providers around the world have deployed network technology that (accidentally or intentionally) restricts access to certain Internet content.

B. These services are sometimes referred to as session oriented services because they operate on traffic flowing between pairs of source and destination nodes. In the case of a stub autonomous system (AS), some of these source and destination nodes are likely to be edge routers connected to the hosts, whereas in the case of a large transit AS, these nodes are two border routers in the ingress and egress of the AS. The serviced traffic traverses the shortest path from the source to the service gateway and then the shortest path from the gateway to the destination. Traditionally, such service gateways have been placed on the boundary of an AS since all inter domain traffic passes. However, there is a growing trend to place network services inside the AS. It was first shown by that FTP traffic can be significantly reduced by placing caches in strategic locations inside the AS backbone. Since then, there has been a large volume of work that demonstrates the benefits of well-planned placement strategies in a variety of service contexts. Such strategies take into account the distribution of traffic as well as the topology of the AS. Research on service placement has concentrated mainly on placing the service gateways in a way that minimizes the average length of the traversed routes.

Therefore, each flow always selects the service gateway that imposes the shortest possible route. However, this approach does not take into account the reciprocal effect of individual flows, the load imposed on the network links, and the possible existence of hotspots (congested areas) in the network.

C. In this paper we present a scalable routing protocol for ad hoc networks. The protocol is based on geographic location management strategy that keeps the overhead of routing packets relatively small. Nodes are assigned home regions and all nodes within a home region know the approximate location of the registered nodes. As nodes travel, they send location update messages to their home regions and this information is used to route data packets. In this paper, we derive theoretical performance results for the protocol and prove that the control overhead scales linearly with node speed and as N3=2 with increasing number of nodes. These results indicate that our protocol is well suited to relatively large ad hoc networks where nodes travel at high speed. In this paper we present a new routing protocol and derive a theoretical bound that characterizes its scalability. Our routing protocol relies on a location update mechanism that maintains approximate location information for all nodes in a distributed fashion. As nodes move, this approximate location information is constantly updated. To maintain the location information in a decentralized way, we map node IDs to a geographic sub-region of the network.

In this paper we presented a new routing protocol for large networks and developed a theoretical model for predicting its scalability with respect to increased node speeds as well as increasing network sizes. One disadvantage of this protocol is, it does not determining a lower bound for routing overhead.

D. Networks while focusing only on one aspect of the configuration the one related to the configuration of the Border Gateway Protocol (BGP). BGP is the most commonly deployed inter-domain routing protocol. It allows networks to connect to each other. measured BGP configuration errors that were visible from routing updates at the Oregon Route Views servers over the course of 21 days, and found that misconfigurations were pervasive. About 75% of all new advertised routes were erroneously announced during that time, which was a conservative estimate according to the authors. In addition to their prevalence, network resulted in the propagation of routes, leading to“ misdirected/lost traffic for tens of thousands of networks” .Several solutions have been proposed to deal with the router misconfiguration problem. All but one of them compare configurations with a list of constraints or common best practices that a network ought to follow to function correctly. This approach makes the assumption that rules violations are misconfigurations, and is very effective in detecting certain types of clear-cut problems, such as checking that internal BGP speakers form a full mesh, verifying that all IP addresses within a network are unique, and determining whether referenced routing policies are actually defined. However, the identification and definition of the constraint scan be a challenging task. What constitutes an error sometimes depends on the network what is an error for one network can be common practice for another. This relativism of error definition is echoed by others studied configuration files from networks.

III. ALGORITHM EXPLANATION

Spectrum Based Analysis

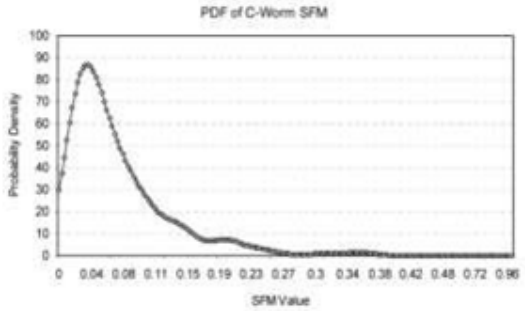
1. **PowerSpectral Density**
2. **Spectral Flatness Measure**

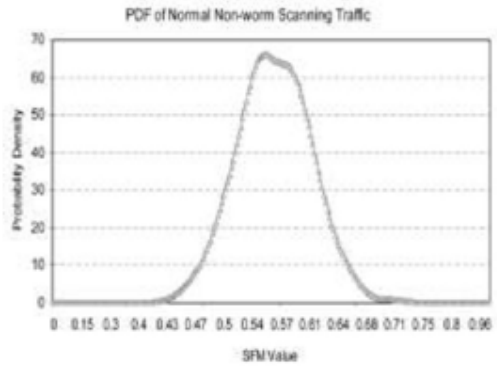
PowerSpectral Density

Transfer data from time domain Scan Traffic determined the discrete fourier transform. Compare c-worm traffic and normal worm trafficTransform data from time domain into frequency domain Random process x(t),t∈[0,n], X(t)-source count in time periodPSD SCAN traffic data is determined using Discrete fourier transformΦ(Rx[L],k)=Є(Rx[L].e^-j2Πkn/NCompare non-worm traffic and c-worm traffic.

Spectral flatness measure

Distinguish the scan traffic of c-worm and normal non-worm traffics spectral flatness measure concentration of data at narrow frequency range Higher concentration at small Spectrum comparatively.





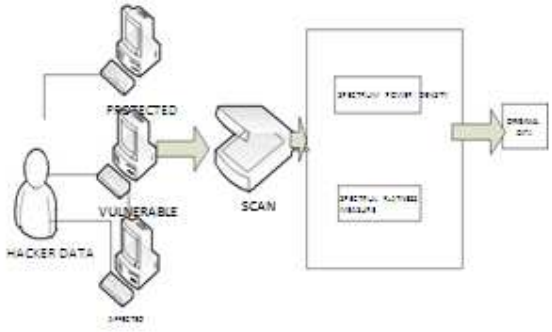
Compare c-worm traffic and non worm traffic.

IV. PROPOSED SYSTEM ARCHITECTURE

In the Proposed System, We are modeling the Camouflaging Worm (C-Worm), in which the Behavior is hidden and its action is implicitly kept secret. So this Process of Detecting the C-Worm is not possible using the usual Traditional Worm Detection Techniques as well as IP Trace Back Systems. 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 Detection method is Spectrum method based Process to continuously monitor the

Traffic Process. Even though smaller amount of Traffic is only going to generate the Spectrum based process will identify the C-Worm based on the Behavior.



System Overall Architecture

There are three types of system 1.affected system 2.protected system 3.vulnerable system

Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM).It detect and delete the c-worm.

V. CONCLUSION

C-Worm could use based on the limited network and computing resources available during its propagation. Incorporating the Peer-to-Peer techniques to disseminate information through secured channels Actually a worm could take advantage of the knowledge that an infection attempt was a new hit reaching a previously uninfected vulnerable computer and duplicate hit reaching a previously infected vulnerable computer. The approach used by the "self-stopping" worms that do not require a global overlay control network for Realizing their behavior in practice. We call our approach to estimate the Distributed Co-ordination method. In this method, there is no centralized co-ordination between the C-Worm instances to obtain feedback information about the value. The distributed co-ordination requires each C-Worm infected computer to be marked with a watermark indicating that the C-Worm infection code has already been installed on the scanned host as with "Code-Red" worms. Thus, when an already infected computer .A scans another infected computer then computer A will detect the water mark and know that computer B has already been infected. By scanning vulnerable computers and obtaining the water-marks information during the scanning.

REFERENCES

[1] W. Gong, and D. Towsley C.C. Zou, , Nov. 2010 "Code-Red Worm Propagation Modeling and Analysis," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS).
[2] Cert, cert/cc advisories, may/june 2010 388 iesee transactions on dependable and secure computing, vol. 8, no. 3
[3] S. Coull, and F. Monrose C. Wright,), Feb. 2009 , "Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis," Proc. 15th IEEE Network and Distributed System Security Symp. (NDSS).
[4] J. Brown D. Moore, C. Shannon, and, "Code-Red), Nov. 2010: A Case Study on the Spread and Victims of an Internet Worm," Proc. Second Internet Measurement Workshop (IMW).
[5] W.B. Gong, and L.X. Gao Towsley, C. Zou, D. Oct. 2010, "Monitoring and Early Detection for Internet Worms," Proc. 10th ACM Conf. Computer and Comm. Security (CCS),.
[6] D. Moore, V. Paxson, and S. Savage, , July 2010 "Inside the Slammer Worm," Proc. IEEE Magazine of Security and Privacy.
[7] J. Ma, and S. Savage, , G.M. Voelker Nov. 2010 "Self-Stopping Worms," Proc. ACM Workshop Rapid Malcode (WORM),
[8] M. Garetto, W.B. Gong, and D. Towsley, , Mar. 2010 "Modeling Malware Spreading Dynamics," Proc. IEEE INFOCOM
[9] J. Caballero, M.G. Kang and D. Song,), July 8, 2011 "Distributed Evasive Scan Techniques and Countermeasures," Proc. Int'l Conf. Detection of Intrusions and MalwareandVulnerability Assessment (DIMVA.
[10] P.R. Roberts, Zotob.asp, 2010 Arrest Breaks Credit Card Fraud Ring, http:// www.eweek.com/article2/0,1895,1854162,00.

[11] R. Naraine, asp, 2010 Botnet Hunters Search for Command and Control Servers, http://www.eweek.com/article2/0,1759,1829347,00.
[12] R. Vogt, J. Aycock, and M. Jacobson, , Oct. 2009 "Quorum Sensing and Self-Stopping Worms," Proc. Fifth ACM Workshop Recurring Malcode (WORM).
[13] V. Paxson S. Staniford, and N. Weaver, Aug 2009 "How to Own the Internet in Your Spare Time," Proc. 11th USENIX Security Symp. (SECURITY).

