International Journal of Computer Science and Engineering Communications
Vol.3, Issue 3, 2015, Page.1171-1176
ISSN: 2347–8586
www.scientistlink.org

Host Based Determination of Camouflaging Worm

Deva Kumar.R[1], Kishore Kumar.G.S[2], Vignesh.S[3] , Venkatakrishnan B[4], S.Sindhu[5], A. Saranya[6]
[1,2,3,4]UG Scholar, [5,6]Assistant Professor
Department of Computer Science and Engineering
Rajalakshmi Institute of *Technology* ,Chennai, India
[1]*devakumar.r.2011.cse@ritchennai.edu.in,*
[2]*kishorekumar.g.s.2011.cse@rithennai.edu.in,*[3]*vignesh.s.2011.cse@ritchnnai.edu.in,* [5]*sindhu.s@ritchennai.edu.in*

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. Here we analyze hidden type active worms, referred to as Camouflaging Worm. This Worm is different from basic worms because of its ability to intelligent manipulate its scan traffic volume over time. This worm Camouflages its propagation from existing worm detection systems based on analyzing the propagation traffic generated by worms. We analyze characteristics of the Camouflages worm and conduct a comprehensive comparison between its traffic and non-worm traffic (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.

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: (a) launch massive Distributed Denial-of-Service (DDoS) attacks that disrupt the Internet utilities, (b) access confidential information that can be misused through large scale traffic sniffing, key logging, identity theft etc, (c) destroy data that has a high monetary value, and (d) 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 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.
In this system, the detection is commonly based on the self propagating behavior of worms that can be described as follows: after a worm-infected computer identifies and infects a vulnerable computer on the Internet, this newly infected computer1 will automatically and continuously scan several IP addresses to identify and infect other vulnerable computers. As such, numerous existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns. Nevertheless, the attackers are crafting attack strategies that intend to defeat existing worm detection systems. In particular, 'stealth' is one attack strategy used by a recently-discovered active worm called "Attack" worm and the "self-stopping" worm circumvent detection by hibernating (i.e., stop propagating) with a pre-determined period.

Worm might also use the evasive scan and traffic morphing technique to hide the detection 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. 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: (a) still achieve its ultimate goal of infecting as many computers as possible before being detected, and (b) position itself to launch subsequent attacks

SYSTEM ANALYSIS

PROBLEM DEFINITION

Security vulnerabilities must be prevented to begin with, a problem which must addressed by the programming language community. However, while vulnerabilities exist and pose threats of large-scale damage, it is critical to also focus on network-based detection, as this paper does, to detect wide spreading worms.

EXISTING SYSTEM

Existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed.

It has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns. The attackers are crafting attack strategies that intend to defeat existing worm detection systems. In particular, 'stealth' is one attack strategy used by a recently-discovered active worm called "Attack". Worm might also use the evasive scan and traffic morphing technique to hide the detection.

LIMITATIONS OF EXISTING SYSTEM

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.

PROPOSED SYSTEM

Proposed Worm detection schemes that are based on the global scan traffic monitor by detecting traffic anomalous behavior, there are other worm detection and defense schemes such as sequential hypothesis testing for detecting worm-infected computers, payload-based worm signature detection. In presented both theoretical modeling and experimental results on a collaborative worm signature generation system that employs distributed fingerprint filtering and aggregation and multiple edge networks behavior continues to be a useful weapon against worms, and that in practice multifaceted defense has advantages. 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 Camouflaging Worm, but usual intrusions as well.

ADVANTAGES OF PROPOSED SYSTEM

Here, as we are detecting c-worms thereby this algorithm also detects other normal worms too. Even new upcoming worms can also be detected without any antivirus software and internet update. Worm traffic and background traffic can be differentiated.

SYSTEM ARCHITECTURE:

In this project, files are being scanned and finds which are modified, anomaly in behavior and worm infected files through the status of the detector algorithm.

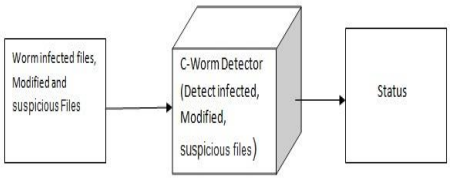

Fig.1. System Architecture

WORKFLOW DIAGRAM

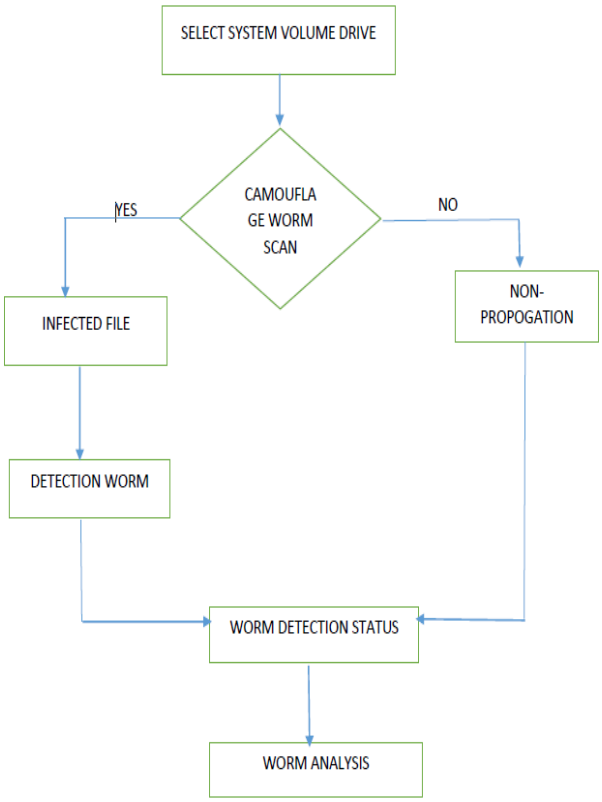

Fig.2. Workflow Diagram

LITERATURE SURVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

ACTIVE WORMS

Active worms are similar to biological viruses in terms of their infectious and self-propagating nature. They identify vulnerable computers, infect them and the worm-infected computers propagate the infection further to other vulnerable computers. In order to understand worm behavior, we first need to model it. With this understanding, effective detection and defense schemes could be developed to mitigate the impact of the worms. For this reason, tremendous research effort has focused on this area,

Active worms use various scan mechanisms to propagate themselves efficiently. The basic form of active worms can be categorized as having the Pure Random Scan (PRS) nature. In the PRS form, a worm-infected computer continuously scans a set of random Internet IP addresses to find new vulnerable computers. Other worms propagate themselves more effectively than PRS worms using various methods, e.g., network port scanning, email, file sharing, Peer-to-Peer (P2P) networks, and Instant Messaging (IM. In addition, worms use different scan strategies during different stages of propagation. In order to increase propagation efficiency, they use a local network or hit list to infect previously identified vulnerable computers at the initial stage of propagation. They may also use DNS, network topology and routing information to identify active computers instead of randomly scanning IP addresses. They split the target IP address space during propagation in order to avoid duplicate scans. Studied a divide-conquer scanning technique that could potentially spread faster and stealthier than a traditional random-scanning worm. Ha formulated the problem of finding a fast and resilient propagation topology and propagation schedule for Flash worms. Studied the worm propagation over the sensor networks

Worm (C-Worm) studied in this paper aims to elude the detection by the worm defense system during worm propagation. Closely related, but orthogonal to our work, are the evolved active worms that are polymorphic in nature. Polymorphic worms are able to change their binary representation or signature as part of their propagation process. This can be achieved with self-encryption mechanisms or semantics preserving code manipulation techniques. The C-Worm also shares some similarity with stealthy port-scan attacks. Such attacks try to find out available services in a target system, while avoiding detection. It is accomplished by decreasing the port scan rate, hiding the origin of attackers, etc. Due to the nature of self-propagation, the C-Worm must use more complex mechanisms to manipulate the scan traffic volume over time in order to avoid detection.

MODULES:

- Random Scan Module.
- Worms are Malicious Detection Module or Anomaly detection.
- C-worm detection module.

MODULES DESCRIPTION:

1. Random Scanning Module

C-Worm can be extended to defeat other newly developed detection schemes, such as destination distribution-based detection. In the following, Recall that the attack target distribution based schemes analyze the distribution of attack targets (destination IP addresses, USB port, external devices etc) as basic detection data to capture the fundamental features of worm propagation, i.e., they continuously scan different targets. We scan the all drives first it will randomly scan the files. Then after that we have a chance to scan each drive separately.

2. Worms are Malicious Detection Module or Anomaly detection

Worms are malicious programs that execute on these computers, analyzing the behavior of worm executables plays an important role in host based detection systems. Many detection schemes fall under this category. In contrast, network-based detection systems detect worms primarily by monitoring, collecting, and analyzing the scan traffic (messages to identify vulnerable computers) generated by worm attacks. Ideally, security vulnerabilities must be prevented to begin with, a problem which must addressed by the programming language community.However, while vulnerabilities exist and pose threats of large-scale damage, it is critical to also focus on network-based detection, as this paper does, to detect wide spreading worms.

International Journal of Computer Science and Engineering Communications
Vol.3, Issue 3, 2015, Page.1171-1176
ISSN: 2347–8586
www.scientistlink.org

3. C-worm Detection Module

Camouflaging Worm(C-Worm). 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. 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. We analyze the actual behavior of the each file with compare with our malware data sets. The datasets are defined actual behavior of the file. Each scanning files compare with our datasets if detect any anomaly behavior of file and to detect the c-worm.

EXPERIMENTAL SECTION:

The front end is done using java and this project consists of three modules- (i).Random Scanning Module, (ii).Worms is Malicious Detection Module or Anomaly detection, (iii). C-worm Detection Module.

The user selects a particular drive or scans all the drive together in order to find out the infected files and obtains the status report and list of affected files.

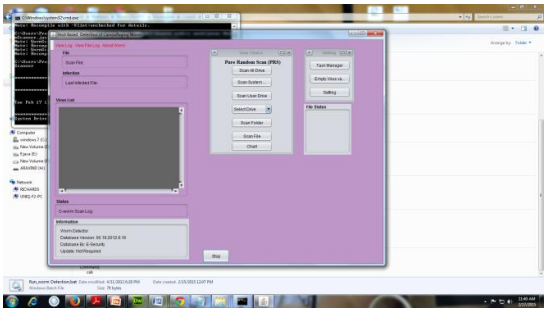

Fig. 3. Interface

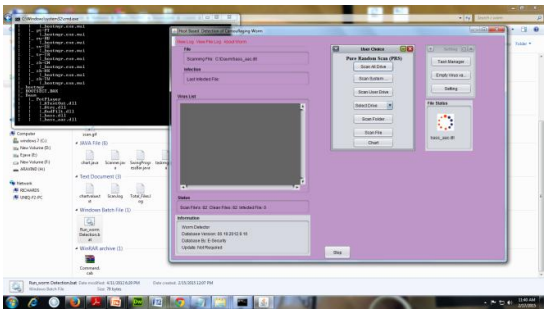

Fig. 4. Random Scanning Module

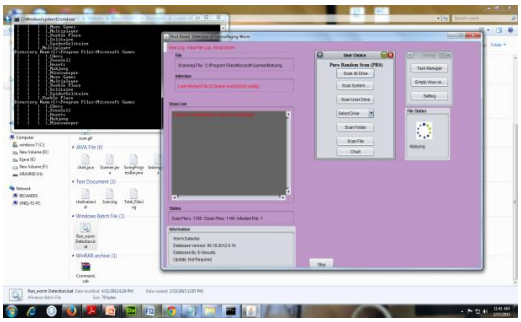

Fig. 5. C Worm Detection

CONCLUSION

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, this project is developed on a spectrum-based detection scheme to detect the C-Worm. Our evaluation data showed that our scheme achieved superior detection performance against the C-Worm in comparison with existing representative detection schemes. This paper lays the foundation for ongoing studies of "smart" worms that intelligently adapt their propagation patterns to reduce the effectiveness of countermeasures.

REFERENCES

[1] D. Moore, C. Shannon et al., "Code-red: a case study on the spread and victims of an internet worm," in Proc. 2nd ACM SIGCOMM Workshop on Internet measurement. ACM, 2002, pp. 273–284 [Online].Available: http://dl.acm.org/citation.cfm?id=637244.
[2] H. Berghel, "The code red worm," Commun. of the ACM, vol. 44, no. 12, pp. 15–19, 2001.
[3] H. V. Poor, "An introduction to signal detection and estimation," New York, Springer-Verlag, 1988, 559 p., vol. 1, 1988.
[4] A. L. Foster, "Colleges brace for the next worm," The Chronicle of Higher Education, vol. 50, no. 28, p. A29, 2004.
[5] V.Weafer.(2010) Downadup/conficker and april fools day: One year later. [Online]. Available: http://www.symantec.com/connect/blogs/downadupconficker-andapril- fool-s-day-one-year-later
[6] Symantec.(2008) W32.downadup (win32/conficker). [Online]. Available: http://www.symantec.com/security response/writeup.jsp? docid=2008-112203-2408-99
[7] M. Fossi, G. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J. Blackbird, M. K. Low, D. Mazurek, D. McKinney et al., "Symantec internet security threat report trends for 2010," Volume, vol. 16, p. 20, 2011.