ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

Novel Malicious Detection Approach and Emergence of Worm Security

R. Shashi Rekha, K.C Ravi Kumar
SriDevi Women's Engineering College ,Hyderabad

Abstract – Worm spreads over the network are malicious pose major security threats to the ability of anomaly to propagate in automated process which compromise the computer network evolve during their propagation and challenge to detect against the computer. A class of virus are Worm Trojans Malicious and Anomaly, worm is different because to manipulate its scan method over the time, it propagation from existing worm detection system based on analysing the propagation of generated by worms. Our work analysis methods to avoid the active worm and conduct a comprehensive comparison between previous systems, observes the frequency domain due to recurring manipulation nature of the worm. A novel approach presents the spectrum based system to detect the active worm such Camouflaging using the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to a comprehensive set of detection metrics and real-world traces as background traffic, proposed work shows generality of spectrum-based scheme in effectively detecting not only the Malicious, but also traditional active worms as well.

***Index Terms*- Networks, Malicious, Worm Scan Methods, Detection, Security.**

I. INTRODUCTION

Active worm is a software program that propagates itself over a network, reproducing itself as it goes unlike viruses which have to attach themselves to a particular program, like an email client, worms are self-contained. They look for a particular exploit and use that to copy themselves onto vulnerable machines. They may simply try to replicate themselves, or they may do something malicious to the infected computer. Once a worm is downloaded, it will scan the network for other vulnerable machines and send those machines their code. Worms use many scanning methods. Most common methods are random scanning, where an infected machine randomly choose an IP address and tries to infect that address, and subnet scanning, where an infected machines tried IP addresses that are similar to the address of the infected machines. Random scanning is often used because it is faster even if it has a lower chance of hitting real computers [1]. Network service worms spread by exploiting vulnerability in a network service associated with an operating system or an application. Once a worm infects a system, it typically uses that system to scan for other systems running the targeted service and then attempts to infect those systems as well. Because they act completely without human intervention, network service worms can typically [2] propagate more quickly than other forms of malware. The rapid spread of worms and the intensive scanning they often perform to identify new targets often overwhelm networks and security systems (e.g., network intrusion detection sensors), as well as infected systems such as network service worms are [3] Sesser and Witty.

Due to the substantial damage caused by worms in the existing work there have been significant efforts on developing defence mechanisms against worms. Detection of worms is one of the most important tasks in defence against them, which usually is [8] based on the behavioural features of [4] worms. The typical self-propagating behaviour of a traditional worm can be described as follows: After a worm instance identifies and infects a vulnerable host on the Internet, this newly infected host 1 will automatically scan the IP addresses to identify other vulnerable hosts and infects [5] them in a similar manner. Most existing detection schemes are based on a tacit assumption that each worm infected host keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been widely believed that the worm scan traffic volume and the worm infected host number show exponentially increasing patterns [7]. However, worms are evolving and some recently seen smart-worms contradict such assumption by reducing their [6] propagation speed to avoid detection. 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 behaviour similar to traditional worms, i.e., it intends to rapidly infect as many vulnerable hosts as possible. However, the C-Worm is quite different from traditional worms in a way that it camouflages any noticeable trends in the number of infected hosts over time. The camouflage is achieved by manipulating the scan traffic volume of worm infected hosts. 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 worm detection schemes [9].

II. RELATED WORK

A worm is a self-replicating computer program uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. The name worm comes from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Many worms

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

have been created which are only designed to spread, and don't attempt to alter the systems they pass through. However, as the Morris worm and Mydoom showed, the network traffic and other unintended effects can often cause major disruption. A "payload" is code designed to do more than spread the worm - it might delete files on a host system (e.g., the Explore Zip worm), encrypt files in a crypto viral extortion attack, or send documents via e-mail. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" under control of the worm author - So big and Mydoom are examples which created zombies. Networks of such machines are often referred to as botnets and are very commonly used by spam senders for sending junk email or to cloak their website's address. Spammers are therefore thought to be a source of funding for the creation of such worms, and worm writers have been caught selling lists of IP addresses of infected machines. Others try to blackmail companies with threatened DoS attacks. Backdoors can be exploited by other malware, including worms. Examples include Doom juice, which spreads better using the backdoor opened by Mydoom and at least one instance of malware taking advantage of the root kit and backdoor installed by the Sony/BMG DRM software utilized by millions of music CDs prior to late 2005.

Beginning with the very first research into worms at Xerox PARC there have been attempts to create useful worms. The Nachi family of worms, for example, tried to download and install patches from Microsoft's website to fix vulnerabilities in the host system — by exploiting those same vulnerabilities. In practice, although this may have made these systems more secure, it generated considerable network traffic, rebooted the machine in the course of patching it, and did its work without the consent of the computer's owner or user. Other worms, such as XSS worms have been written for research to determine the factors of how worms spread, such as social activity and change in user behavior. Still more worms do very little, or are pranks, such as one that sends the popular picture of the lolowl with the phrase "ORLY?" to a print queue in the infected computer. Most security experts regard all worms as malware, whatever their payload or their writers' intentions. Protecting against dangerous computer worms spread by exploiting vulnerabilities in operating systems, **a**ll vendors supply regular security updates (see "Patch Tuesday"), and if these are installed to a machine then the majority of worms are unable to spread to it. If a vendor acknowledges vulnerability but has yet to release a security update to patch it, a zero day exploit is possible. However, these are relatively rare. Users need to be wary of opening unexpected email, and should not run attached files or programs, or visit web sites that are linked to such emails. Anti-virus and anti-spy ware software are helpful, but must be kept up-to-date with new pattern files at least every few days. The use of a firewall is also recommended, computer worms malicious, self-propagating programs represent a substantial threat to large networks. Since these threats can propagate more rapidly than human response automated defenses are critical for detecting and responding to infections. One of the key defenses against scanning worms which spread throughout an enterprise is containment. Worm containment, also known as virus throttling, works by detecting that a worm is operating in the network and then blocking the infected machines from contacting further hosts. Currently, such containment mechanisms only work against scanning worms because they leverage the anomaly of a local host attempting to connect to multiple other hosts as the means of detecting an infect, within an enterprise, containment operates by breaking the network into many small pieces, or cells. Within each cell (which might encompass just a single machine), a worm can spread unimpeded. But between cells, containment attempts to limit further infections by blocking outgoing connections from infected cells. A key problem in containment of scanning worms is efficiently detecting and suppressing the scanning. Since containment blocks suspicious machines, it is critical that the false positive rate be very low. Additionally, since a successful infection could potentially subvert any software protections put on the host machine, containment is best effected inside the network rather than on the end-hosts. Trace-based analysis shows that the algorithms are both highly effective and sensitive when monitoring scanning on an Internet access link, able to detect low-rate TCP and UDP scanners which probe our enterprise. One deficiency of our work, however, is that we were unable to obtain internal enterprise traces. These can be very difficult to acquire, but we are currently pursuing doing so. Until we can, the efficacy of our algorithm when deployed internal to an enterprise can only be partly inferred from its robust access-link performance.

III. MALWARE

Viruses worms are all part of a class of software called malware or malicious software specifically designed to damage disrupt, steal general inflict some other bad or illegitimate on data hosts or networks. There are many different classes of malware infecting systems and propagating themselves. Malware can infect systems by being bundled with other programs or attached as macros to files. Others are installed by exploiting a known vulnerability in an operating systems network device or other software such a whole in browser that only requires users to visit a website to infect their computers. Malware cannot damage the physical hardware of systems and network equipment but it can damage the data and software residing on the equipment malware should also not be confused with defective software which is intended for legitimate purposes but has errors or bugs.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

A. Types of Malware

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program spreads from one computer to another leaving infection as it travels. Viruses can range in severity from causing mildly effects to damaging data or software and causing denial-of-service conditions. All viruses are attached to an executable file which means the virus may exist on a system but will not be active or able to spread until a user runs or open the malicious host file or program when the host code is executed the viral code is executed. Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage, in contrast to viruses which require the spreading of an infected host file worms are standalone software and do not require a host program or user help to propagate. To spread worms either a vulnerability on the target system or uses some kind of social engineering to trick users into executing them.

Trojan is other type of malware harmful piece of software that looks legitimate users are typically tricked into loading and executing it on their systems. After it is activated can achieve any number of attacks on the host from irritating the user to damaging the host.

B. Technique to Protect From Worms

Worms perform to find vulnerable hosts depending on how worms choose their perfect destinations from source to destination space using the scan method.

1. Selective Random Method:

Instead of scanning the whole IP address space at random set of addresses that may belong to existing machines can be selected as the target address space. Address list can be either obtained from the global or the local routing this care takes so that unallocated or reserved address blocks in the IP address space are not selected for scanning. Worms can avoid addresses within these address blocks for example A list contains around 32 address blocks should never appear in the public network. An IPv4 address allocation map is a similar list that shows the 8 address blocks which have been allocated, slapper worm made use of these lists in order to spread rapidly. Using the selective random scan need to carry information about the selected target addresses. Selective random scan the databases carrying the information can be hundreds of bytes therefore additional database will not affect the already slow spreading of worms.

2. Routable Technique:

The reduced scanning address space if a worm also know which of the addresses are routable or are in use then it can spread faster and more effectively can avoid detection this type of scan technique where unassigned IP addresses which are not routable on the internet are removed from the worms databases is known as routable technique using this type of method is that the code size of the worm has to be increased as it needs to carry a routable IP addresses database. The database cannot be to large as it leads to along infection time resulting in s slowdown of the worm propagation.

3. Divide-Conquer Scan:

Instead of scanning the complete database the host infected divides its address database among its victims such as after machine A infects machine B, machine A will divide its routable addresses into halves and transmit one half to machine B. Machine B can then scan the other half using divide –conquer method the code sixe of the worm can be further reduced because each victim will scan a different and also a less address space. One weak point of Divide-Conquer scan is single point of failure during worm propagation if one infected machine is turned off or gets crashed the database passed to it will be lost. Possible solution generates a hitlist where a worm infects a large number of hosts before passing on the database and other solution generates counter each time the worm program is transferred to a new victim a counter is incremented.

4. Hybrid Technique:

Technique targets by a specific address database might miss many vulnerable hosts that are not globally reachable to avoid this attacker can combine routable method with random scan at the next stage of the propagation to infect more machines. Advantage of this technique is that even though the propagation has been detected the hybrid method can be used to infect more number of machines as it is already to late for effective defence. The fact that a large number of machines use private IP addresses and hidden and protected by gateway machines from the internet better performs can be achieved if those addresses can be scanned with more power.

IV. PROBLEM DEFINITION

An attack spreads over the complete work environment becomes a worm which pose the security threats to the network due to this worm to propagate in an automated fashion need to compromise computers. To avoid this type of active worms refers Camouflaging worm manipulates its scan traffic over time.

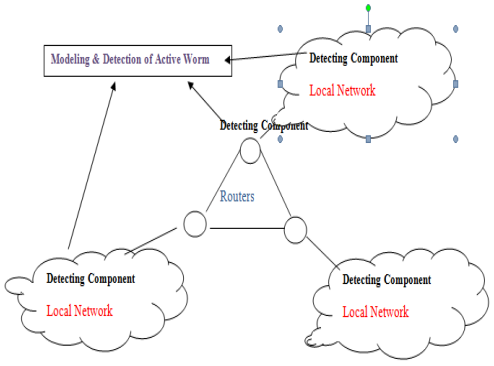

Fig 1 Proposed Architecture

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

A Detection Technique

Novel based detection method recalls that the worm goes undetected by detection method that tries to determine the worm propagation only in the time domain. To identify the worm propagation in the frequency domain we use the power of a time series is in the frequency domain mathematically is defined as the Fourier transforms of the autocorrelation of the time series and corresponds to the changes in the number of worm instances that actively conduct scans over time. The SFM is defined as the ratio of geometric mean to arithmetic mean of the coefficients of power of time series.

Using Power Spectral Density method to obtain the distribution for worm detection data, need to transform data from the time domain into the frequency domain to do this process we use a random process to model the worm detection data. PSD captures recurring pattern in the frequency domain shows a comparatively even distribution across a wide spectrum range for the normal non-worm. The PSD corresponding Spectral Flatness Measure captures anomaly behaviour in certain range of frequencies defined as the ratio of the geometric mean to the arithmetic mean of the PSD coefficients. SFM is a existing measure for discriminating frequencies in various applications such as frame detection in speech recognition. The method of applying an appropriate detection rule to detect worm propagation, SFM value can be used to sensitively distinguish the worm and normal non-worm scan traffic, the worm detection is performed by comparing the SFM with a predefined threshold Tr. If the SFM value is smaller than a predefined threshold Tr, then a worm propagation alert is generated, value of the threshold Tr used by the C-Worm detection can be fittingly set based on the knowledge of statistical distribution (e.g., PDF) of SFM values that correspond to the non-worm scan traffic.

B. Comparative Study

In the previous worm detection schemes will not be able to detect such scan traffic patterns, important to understand such smart-worms and develop new countermeasures to defend against them. Previous analysis of 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, 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 compare to existing worm detection our analysis shows worm detection schemes that are based on the global scan traffic monitor by detecting traffic anomalous behaviour, there are other worm detection and defence schemes such as sequential hypothesis testing for detecting worm-infected computers, payload-based worm signature detection. A state-space feedback control model that detects the spread of these viruses or worms by measuring the velocity of the number of new connections an infected computer makes. Despite the different approaches describes to detecting widely scanning anomaly behaviour continues to be a useful weapon against worms, and that in practice multifaceted defence has advantages.

C. Analysis of Proposed Worm Detection Scheme

Analysis of below description explains how to implement the proposed worm detection.

1. Detection of Worm Scheme

Worm the Worm has a self-propagating behaviour similar to traditional worms, i.e., it intends to rapidly infect as many vulnerable computers as possible. However, the 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

2. Malicious Worm

Worms are malicious programs that execute on these computers, analysing the behaviour of worm executable 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 analysing the scan traffic (messages to identify vulnerable computers) generated by worm attacks. Many detection schemes fall under this category. 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**.**

3. Apply Random Method to Avoid Worm

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 (the scanned destination IP addresses) as basic detection data to capture the fundamental features of worm propagation, i.e., they continuously scan different targets.

4. Propagate the Worm

Worm scan traffic volume in the open-loop control system will expose a much higher probability to show an increasing trend with the progress of worm propagation.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

As more and more computers get infected, they, in turn, take part in scanning other computers. Hence, we consider the Cworm as a worst case attacking scenario that uses a closed loop control for regulating the propagation speed based on the feedback propagation status.

V. CONCLUSION

In this paper a general worm detection scheme uses to detect the malicious worms in computer networks, internet. Scanning method is first applied to routing components. The system built on each network data to identify the malicious anomaly classifies into normal or anomaly, the system compares with previous work disadvantages shows the better performance.

Our future work is to designed and implemented a novel explanation mechanism for the problem to identify high false attacks can also be resolved high rate of accuracy in the case of any business method with human-understandable can also improve the efficiency.

REFERENCES

[1] The Jargon file lexicon." http://www.catb.org/~esr/jargon.

[2] National Institute of Standards and Technology Special Publication 800-83 Natl. Inst. Stand. Technol. Spec.Publ. 800-83, 101 pages (November 2005).

[3] IEEE Transactions On Dependable And Secure Computing, Vol. 8, No.3, May June 2011.

[4] C. C. Zou, W. Gong, and D. Towsley, "Code-red worm propagation modelling and analysis," in Proceedings of the 9-th ACM Conference on Computer and Communication Security (CCS), Washington DC, November 2002.

[5] S. Staniford, V. Paxson, and N. Weaver, "How to own the internet in your spare time," in Proceedings of the 11-th USENIX Security Symposium, San Francisco, CA, August 2002.

[6] Z. S. Chen, L.X. Gao, and K. Kwiat, "Modeling the spread of active worms," in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.

[7] M. Garetto, W. B. Gong, and D. Towsley, "Modeling malware spreading dynamics," in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.

[8] C. Zou, W. B. Gong, D. Towsley, and L. X. Gao, "Monitoring and early detection for internet worms," in Proceedings of the 10-th ACM Conference on Computer and Communication Security (CCS), Washington DC, October 2003.

[9] S. Venkataraman, D. Song, P. Gibbons, and A. Blum, "New streaming algorithms for super spreader detection," in Proceedings of the 12-th IEEE Network and Distributed Systems Security Symposium (NDSS), San Diego, CA, February 2005.

[10] J. Wu, S. Vangala, and L. X. Gao, "An effective architecture and algorithm for detecting worms with various scan techniques," in Proceedings of the 11-th IEEE Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2004.

[11] H. Kim and B. Karp, "Autograph: Toward Automated, Distributed Worm Signature Detection," Proc. 13th USENIX Security Symp. (SECURITY), Aug. 2004.

[12] M. Cai, K. Hwang, J. Pan, and C. Papadopoulos, "Worm shield: Fast Worm Signature Generation with Distributed Fingerprint Aggregation," IEEE Trans. Dependable and Secure Computing, vol. 4,no. 2, pp. 88-104, Apr.-June 2007.

[13] 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.

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

[15] J.B. Grizzard, V. Sharma, C. Nunnery, B.B. Kang, and D. Dagon, "Peer-to-Peer Botnets: Overview and Case Study," Proc. USENIX Workshop Hot Topics in Understanding Botnets (HotBots), Apr. 2007.

[16] P. Wang, S. SParka, and C. Zou, "An Advanced Hybrid Peer-to- Peer Botnet," Proc. USENIX Workshop Hot Topics in Understanding Botnets (HotBots), Apr. 2007.

AUTHOR BIOGRAPHY

R. Shashi Rekha pursuing M.Tech CSE from SriDevi Women's Engineering College B.Tech CSE from Nishitha College of Engineering & Technology. Her research areas include Software Engineering Unified Modelling Language Information Security.

K.C Ravi Kumar M.Tech CSE from JNTU Hderabad currently he is the head of department for M.Tech CSE programme in SriDevi Women's Engineering College having 17 years of Academic Experience. He is life member of IEEE & IST areas of research include Data Mining & Data Warehousing Information Retrival Systems Information Security.