IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 8, August 2014 ISSN 2321-5992

A COMPARITIVE STUDY ON VARIOUS INTERNET WORM DETECTION TECHNIQUES

Nithya.K[1], Dr.A.Malathi[2]

[1]M.Phil Scholar, Government Arts College, Coimbatore.

[2]Assistant Professor of Computer Science

Government Arts College, Coimbatore.

ABSTRACT

Computer worms are behavior of self-propagation over the host machines and have been terrorizing the internet for last several years. The malicious codes knows as internet worm and increasing complexity of network applications, the threats of internet worm against network security are more and more serious. This paper presents a depth survey on various internet worm detection techniques such as host based, Honeypot based, content based and behavior based detection technique. And the comparative study on various internet worm detection techniques.

Key Words: internet worm; host based; honeypot based content based; behavior based.

1. INTRODUCTION

Internet worm is self-propagating program the program worm running on host will actively scan the network that host is connected to additional victims to infect. Internet worm is a program that propagating across a network exploiting security or policy flaws in widely used services. Network worm is malware that compromise integrity and availability of internet. Internet worm against computer system and network security are increasingly serious .internet worm mainly focus on function structure, execution mechanism, scanning strategies, propagation model, countermeasure technology. Morris worm community for first time in 1988 that a worm brings the internet down in hours, new worm outbreak occurred periodically. The host are vulnerable to worm typically account for small portion of IP address space. Worms rely on high volume random scan to find victims. Intrusion detection system and anti-virus software maybe upgraded to detect and remove a worm, routers and firewalls maybe configured to block the packets, worm signature. The preceding tools limit ability of worm to infect host, but work by anatos et al.[1]also possible to reduce the worm find host to infect. Infected host also be quarantined to limit the ability to infect additional targets [2] ,[3], infect host can be restore ad patched to prevent reinfection.

2. RELATED WORK

Much recent research on internet worm is propagation modeling. A classic epidemiological model of computer virus proposed by kephart and white [16].this model is later used to analyze the propagation behavior of code red like worms by Staiford et al[17] and Moore et al [18].chen et al proposed sophisticated worm propagation model[19] based on discrete times in this same work the model is applied to monitor ,detect and defend against the spread of worm under rather simplified addresses are monitored and connection made those address triggers a worm alert. The distributed warring system by zou et al[20] monitored unused address for trend of illegitimate scan traffic an internet. Two problem using this approach first one is attackers easily overwhelm system with false positive by sending packets addresses some normal program scan the internet for research or other purposes and hit the monitored addresses. Second one is good response time. Honeypot [21] gained lot of attention recently. The goal is attract and trap and attack traffic on the internet. Provos[22] designed virtual honeypot framework to exhibit the TCP/IP stack of different operating system. Kreibich and crow croft honeycomb to identify the worm signature using longest common substrings. Dagon et al honey stat detect worm behavioral small network.

3. TYPES OF INTERNET WORMS

The first internet worm is Morris worm. The recent internet worms is Morris, code red, slammer and witty.

MORRIS WORM

The Morris worm is launched in November 1988 by Robert Tappan Morris. This worm not intended to any harm, but designed to discover number of host on the internet. The worm is supposed to run a process each infected host to respond to query .

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 8, August 2014 ISSN 2321-5992

CODE RED WORM

Code Red was July 2001 affecting computer running Microsoft's internet information server (IIS) web service. The code red I use a blind scan scheme that scans port 80 on random IP addresses to find other vulnerable machines then launches a denial of services attack targeting a set of IP address.

SLAMMER WORM

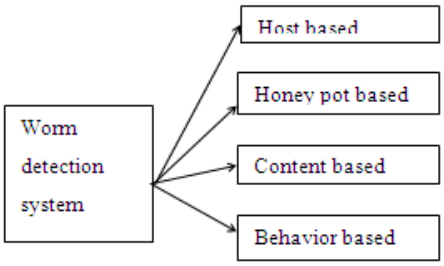
Slammer is sapphire one of the smallest worm. This worm found in January 2003 targeting Microsoft SQL server 2000 or MS 2000.slammer uses UDP port1434 to exploit a buffer overflow in MS SQL server. The code size is 376 byte.

WITTY WORM

The witty worm is released in March 2004 targeting buffer overflow vulnerability in several internet security systems. This worm includes real secure server sensor, real secure desktop and Black ICE.

4. WORM DETECTION TECHNIQUES

The worm detection techniques individually applied in various detection systems. Each technique briefly analyzed strength and weakness of worm detection. The detection system a relatively completed structure for detecting one or more research publication .detection techniques specified low-level of detecting one aspect of worm. This worm detection technique using four categories such as host based, honeypot based, content based and behavior based detection techniques. The four categories of worm detection techniques are as follows



Worm Detection Techniques

HOST-BASED DETECTION

Host-based detection is characterized the information only available at the end-host. Modification may require to operating system or software that runs to give the detection software access to internets of execution environment. Host-based techniques are includes buffer overflow detection, correlating network data to memory errors and looking for patterns in system calls.

G= (V, E, F, δ)

V- Set of vertices. Each representing system calls s Є ∑

E-Set of edge E=C V* V

F-Set of function U f: $X_1, X_2, \ldots, X_n$ - > y

Where each x_i is output argument, o_j of system call s Є ∑

δ - Assign function ∫ i to each system call argument a_i. Behavior graph encodes relationship between system calls. Host based worm detection is based on modifying the software running on particular host to allow the internal state. The worm is interacting with operating system or deployed software. The Covers [4], sweeper [5], and Honey stat [6] all use of buffer over flow detection from system such as stack guard [7], trigger the worm detection. Malan and smith [8] compare the pattern of system calls on one machine with patterns exhibited by peers.

HONEYPOT-BASED DETECTION

Honey pot-based system is vulnerable host on network that provides no real services. Any traffic to honey pot can immediately considered suspicious. Honey pot based worm detection is closely related to host based detection but differ in host based detection deployed honey pot by design no function beyond worm detection. The basic form of the model expresses a binary expecting of the honey pot state.

$E(Y) = 1/1+e^{-z}$

Where

$Z=\beta_0 + Є + \sum^{k}_{j=1} \sum^{nj}_{i=1} (\beta_{i,j} X_{i,j})$

J is counter for each individual honey pot event I is counter for each individual port traffic observation for specific honey pot. Each $\beta_{i,j}$ regression coefficient corresponding to the $X_{i,j}$variable. All host based worm detection methods deployed the software running on honey pot .Honeycomb [9] among the first honey pot system automatically generate signature from traffic directed. Tand et al.determined the assumption of honey pots is malicious a deliberate attack is [10] two detection models to more accurately determine the connection activity represents an actual attack. The Honey

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 8, August 2014 ISSN 2321-5992

stat work by Dagon et al.[6] slightly different approach. Buffer overflow detector like stack guard [7] to detect malicious activity and network monitoring

CONTENT-BASED DETECTION

The content of network traffic looking for byte patterns that match signature of a worm. The signature is generated the fly the worm detector developed manually from deconstruction of worm instance. This system included static signature, dynamic signature and advanced signature.

Let G=(V,E) be a direct graph and set of vertices is V and set of Edges is E. vertex $v_i \in V$, let $In(v_i)$ set of vertices that point to it. Out (v_i) set of vertices that v_i points.

$$NM(v_i) = (1-d)\, e_i + d \sum_{j \in In(v_i)} 1/out(v_i)\, NM(v_i)$$

Where d ϵ [0,1] is the damaging factor represent the probability of random surfer to jump randomly to the page not pointed by current one.

Content-based worm detection is based on idea that a worm exploits vulnerability. Traffic containing signature is almost certainly generated worm and signature is established worm detection becomes straight forward. Content based system possesses the many desired attributes. The large information gain identifying individual connection carrying worm infection. The biggest limitation on content based system not provides coverage for polymorphic worms that change the appearance the payload for each connection. Snort [11] and Bro are two most popular and established open source system .the design to deployed network gateway to monitor inbound and outbound network traffic. Thenet bait [12] system extended the collection of snort based detector.

BEHAVIOR-BASED DETECTION

Behavior based system work the network behavior of end hosts and identifying patterns that are indicative of worm. The system is including the connection failures, network telescopes, pattern of destination addresses and causation. Berk et al.employ this technique for ICMP undeliverable packets indicating connection failures[13],and Worm Early Warning(WEW) system by chen and ranka use the reset messages much the same .Zou et al.among the idea of worm detection , the monitors that capture the scanning behavior host once it was deemed to infected. The noise and quantization or acquisition error, it suffices to replace each equation $a^k x = b_k$, where a^k is the k^{th} row of A and b_k is the k^{th} component of b,

$$a_k \cdot x \leq b_k + \epsilon$$
$$a_k \cdot x \geq b_k - \epsilon$$

This present a general behavioral characterization of proximity malware, capture the anomaly and abnormal behavior and functional differences .this also identifies the imperfect order to detect proximity malware. The proposed system introduces backtracking method which is used to track the previous behaviors analysis. The combinatorial optimization algorithm is a method that consists of finding optimal evidence and object from finite set of object and evidences.

The stack guard [14] compiler modification protects program against buffer overflow in majority of cases with only small performance. A more advanced version CCurad[15], protects all memory access.

5. DISCUSSION ON WORMDETECTION TECHNIQUES

Table 1. Discussion on worm detection techniques

TECHNIQUES	ADVANTAGE	DISADVANTAGE
Host Based	Robust against Polymorphism	1.Per-machine deployment 2.Buffer overflow attacks Only
Content Based	1.Deployable at gateway 2.Fast vs. non-polymorphic Worms	Vulnerable to Polymorphism
Behavior Based	1.Deployable at gateway 2.Robust against Polymorphism	No signature generation

6. CONCLUSION

The security is the primary concern in every field of computer network from the worm detection. This paper provides a depth survey on various types of worm detection techniques. The four major categories in detection technique such as host based, honeypot based, content based and behavior based. In this survey the behavior based detection is best of other worm detection techniques.

REFFERENCE

[1] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, \Defending against hit list worms using network address space randomization," in Proceedings of the Workshop on Rapid Malcode. New York, NY: ACM Press, 2005.

[2] N. Weaver, S. Staniford, and V. Paxson, \Very fast containment of scanning worms," in Proceedings of the USENIX Security Symposium. Berkeley, CA: USENIX, 2004.

[3] A. J. Ganesh, D. Gunawardena, P. Key, L. Massouli, and J. Scott, \E_cient quarantining of scanning worms: Optimal detection and coordination," in Proceedings of IEEE INFOCOM. Washington, DC: IEEE Computer Society, 2006.

[4] Z. Liang and R. Sekar, \Fast and automated generation of attack signatures: Abasis for building self-protecting servers," in Proceedings of the Conference on Computer and Communications Security. New York, NY: ACM Press, 2005.

[5] J. Tucek, J. Newsome, S. Lu, C. Huang, S. Xanthos, D. Brumley, Y. Zhou, and D. Song, \Sweeper: A lightweight end-to-end system for defending against fast worms," in Proceedings of the EuroSys Conference, 2007.

[6] D. Dagon, X. Qin, G. GU, W. Lee, J. Grizzard, J. Levin, and H. Owen, \Honeystat: Local worm detection using honeypots," in Proceedings of the Symposium on Recent Advances in Intrusion Detection, ser. Lecture Notes in Computer Science, vol. 3224. Berlin, Heidelberg: Springer-Verlag, September 2004.

[7] C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, and H. Hinton, \Stackguard: Automatic adaptive detection and prevention of bu_er-overow attacks," in Proceedings of the USENIX Security Symposium. Berkeley, CA: USENIX, January 1998.

[8] D. J. Malan and M. D. Smith, \Host-based detection of worms through peer-to-peer cooperation," in Proceedings of the Workshop on Rapid Malcode. New York, NY: ACM Press, 2005.

[9] C. Kreibich and J. Crowcroft, \Honeycomb: Creating intrusion detection signatures using honeypots," in Proceedings of the Workshop on Hot Topics in Networks. Berkeley, CA: USENIX, 2003.

[10] Y. Tang, H. Hu, X. Lu, and J. Wang, \Honids: Enhancing honeypot system with intrusion detection models," in Proceedings of the IEEE International Information Assurance Workshop. Washington, DC: IEEE Computer Society, 2006.

[11] M. Roesch, \Snort - lightweight intrusion detection for networks," in Proceedings of the Conference on Systems Administration. Berkeley, CA: USENIX, November 1999.

[12] B. N. Chun, J. Lee, and H. Weather spoon, \Net bait: A distributed worm detection service," Intel Research Berkeley, Tech. Rep. IRB-TR-03-033, 2003.

[13] V. Berk, G. Bakos, and R. Morris, \Designing a framework for active worm detection on global networks," in Proceedings of the IEEE International Information Assurance Workshop. Washington, DC: IEEE Computer Society, 2003.

[14] C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, and H. Hinton, \Stack guard: Automatic adaptive detection and prevention of bu_er-overow attacks," in Proceedings of the USENIX Security Symposium. Berkeley, CA: USENIX, January 1998.

[15] J. Condit, M. Harren, S. McPeak, G. C. Necula, and W. Weimer, \CCured in the real world," in Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation. New York, NY: ACM Press, 2003.

[16] J. O. Kephart and S. R. White, \Directed-Graph Epidemiological Models of Computer Viruses," in Proceedings of the 1991 IEEE Symposium on Securityand Privacy, Oakland, California, USA, May 1991.

[17] S. Staniford, V. Paxson, and N. Weaver, \How to 0wn the Internet in Your Spare Time," in Proceedings of the 11th USENIX Security Symposium (Security '2002), San Francisco, California, USA, Aug. 2002.

[18] D. Moore, C. Shannon, and K. Cla®y, \Code-Red: A Case Study on the Spread and Victims of an Internet Worm," in Proceedings of the 2nd InternetMeasurement Workshop (IMW '2002), Marseille, France, Nov. 2002.

[19] Z. Chen, L. Gao, and K. Kwiat, \Modeling the Spread of Active Worms," in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer andCommunications Societies (INFOCOM' 2003), San Francisco, California, USA, Mar. 2003.

[20] C. C. Zou, L. Gao, W. Gong, and D. Towsley, \Monitoring and Early Warning for Internet Worms," in Proceedings of the 10th ACM Conference on Computerand Communication Security (CCS '2003). Washington D.C., USA: ACM Press, Oct. 2003.

[21] L. Spitzner, Honeypots: Tracking Hackers. Reading, Massachusetts, USA: Addison-Wesley, 2002.

[22] N. Provos, \A virtual Honeypot Framework," in Proceedings of the 13th USENIX Security Symposium (Security '2004), San Diego, California, USA, Aug. 2004.