ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Perfect Cyber Entrap: Fast Automatic Detection & Quarantining of Internet Scanning Worms, Topological Worms, Web Worms, Botnet on the Internet Networks

Miss.Gaikwad Kiran Dhondiram[1],Miss.Mairan Swati Balasaheb[2],Prof.ChouguleMeghraj Balasaheb[3]

Student, Master of Computer Application, Terna College of Engineering, Osmanabad, India [1,2]

Lecturer, Master of Computer Application, Terna College of Engineering, Osmanabad, India [3]

Abstract: Now a day's internet is the most fundamental thing in the computerized world but because of Internet & various infected devices, the system performance degrades and system becomes slower than its capacity due to that our result, output is not going to maintain certainty and surety. The safety and reliability of current Internet and various System networks have been constantly challenged by the increased frequency and virulence of worm outbreaks. Worms are on the top of malware threats attacking computer system although of the evolution of worms detection techniques. Main reason behind that our Internet is important facility but it has some problems due to scanning worms, topological worms, web worms & botnet.This paper produce a method for detecting unknown worms uses Artificial Neural Network (ANN) for classifying worm/ nonworm traffic and predicting the percentage of infection in the infected network. In this paper we are organizing structure of Perfect Cyber Entrap system that will fastly detect and quarantining all such worms and vulnerable situations and quarantining such worms due to that our system gives perfect security mechanism from all such worms and makes system more accurate and fast.

Keywords*:* Perfect Cyber Entrap, Botnet, Internet, Scanning worms, Artificial Neural Network (AAN).

I. INTRODUCTION

The safety and reliability of current Internet and various enterprise networks have been constantly challenged by the increased frequency and virulence of worm outbreaks. Unfortunately, the situation is getting worse by the following observations: An Internet worm is type of malicious software ((malware) that self replicate and distributes copies if itself to its network.

A scanning worm locates vulnerable hosts by generating a list of addresses to probe and then contacting them. This address list may be generated sequentially or pseudo-randomly. Local addresses are often preferentially selected as communication between neighboring hosts will likely encounter Fewer defenses. Internet worms can be included in any type of virus, scripts or program. These worms typically infect system by exploiting bugs or vulnerabilities that can often be found in legitimate software.

Many applications contain information about other hosts providing vulnerable services. Topological worm searches for local information to find new victims by trying to discover the local communication topology the original "Morris" worm used topological techniques including network yellow pages etc/hosts & other sources to find new victims.

Computer worms are similar to viruses in that they replicate functional copies themselves and can cause the same type of damage.

In contrast to viruses, which requires the spreading of infected host file, worms are stand alone software and do not require a host program or human help to propagate. To Spared worms either exploit vulnerability on the target system or use some kind of social engineering to trick uses in to executing them. A worm enters a computer through vulnerability in the system and takes advantage of file transport or information transport features on the system, allowing to travel unaided.

A network of virus-infected computers is controlled remotely by an attacker without the owners knowledge, e.g. to send spam. Infected private network with malicious software controlled as a group. A botnet is a number of internet computers that, although their owners are unaware of it, have been setup to forward transmissions to other computers on the internet. Worm detection and response systems must act quickly to identify and quarantine scanning worms, as when left unchecked such worms have been able to infect the majority of vulnerable hosts on the Internet in a matter of minutes.

We present a hybrid approach to detecting scanning worms that integrates significant improvements we have made to two existing techniques: sequential hypothesis testing and connection rate limiting. Our results show that this two-pronged approach successfully restricts the number of scans that a worm can complete, is highly effective, and has a low false alarm rate.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

II .PERFECT CYBER ENTRAP APPROACH

Perfect Cyber Entrap is unique in its playground, i.e. artificial intelligence and darknet is able to achieve nearly-zero false positive and low false negatives due to the exploitation of darknet space and the provocation of worm behaviors.

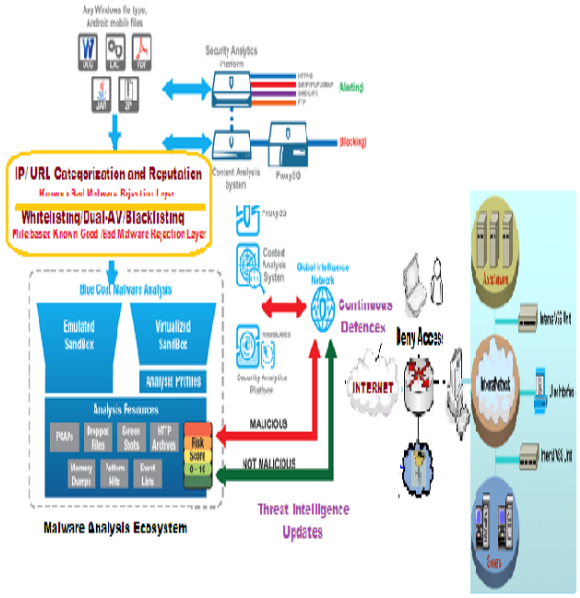

Fig 1.Structure view of Perfect Cyber Entrap

A. Predicting Percentage of Infection

Several approaches are produced attempting to estimate the damage and predict the spread of worms; Kephart and White developed The Epidemiological model, which is a simple model that explains the spread of computer viruses by employing biological epidemiology. The number of infected hosts depends on vulnerability density and scanning rate. The two-factor worm model by Zou et al [24], describes the behavior of worm which based on two factors, the dynamic countermeasure by ISPs and users, and a slowed down worm infection rate. This model explains observed data for Code Red and the decrease in scanning attempts during the last several hours before it ceased propagation. The Analytical Active Worm Propagation (AAWP) model by Chen [2] extends the model of worms that employ random scanning to cover local subnet scanning worms. Parameters in this model include the number of vulnerable machines, size of hit lists, scanning rate, death rate, and patching rate. AAWP better models the behavior of Code Red II than previous models. An approach to minimize the damage due to worm infection in enterprise networks which are produced by Sanguanpong [15] does not require observing variables during attacks. Therefore, it can be used to predict worm damage before the attack occurs. The result produced by Sanguanpong [15] has accuracy ranged from 83.33% to 90.91%, and False-Positive error rate of 0% to 4.16%.

B. Behavioral Detection vs. Signature-Based Detection

Signature-based detection has been the first technique used to fight malware and still remains at the heart of nowadays antivirus software. Jacob [8] describes that these detection techniques search system objects such as files for suspicious byte patterns referenced in a base of signatures. Signatures can precisely identify the threat and name it; signature-based techniques are bound to detect known malware or trivial variants. But signatures are no longer simple byte patterns but complex meta-structures carrying dynamic aspects and a semantic interpretation. On the other hand, behavioral detection is thus more generic and more resilient to modifications than form-based detection.

C. Local Victim Information

Zou, Gao [25], and Staniford, [16] tried to explore global strategies techniques but it require a large monitored network (say, 220 nodes) to distinguish worms from other scanning activities. Some of them look to make nation-wide Internet worm control authority, others proposed to deploy sensors around the Internet. Although there is a need to global co-ordination to protect the Internet from worm intrusions, global detection strategies don't produce complete solution. Dagon and Xinzhou [3] discuss the idea of that since global detection strategies require large amounts of sensor data before detecting worm outbreaks, some local networks might be infected before learning about a worm outbreak. In global detection strategies, in order to gain sufficient worm traffic to become detectable, these strategies have to wait a lot of local networks to fall as victim to the worm. Other Researchers like Guofei [6] uses the idea of using distributed system that detects worm probing traffic through local traffic observations. From local networks point of view, it is more useful to know which machines are infected and how the attack is progressed. Thus worm detection techniques for smaller local networks needs more research.

III. INTELLIGENCE TECHNIQUES USED IN DETECTING NETWORK ATTACKS

A recent survey of intrusion detection [9] suggests using artificial intelligence (AI) techniques to recognize malicious software (malware) in single computers and in computer networks. It describes the research done in developing these AI techniques, and discusses their advantages and limitations. Moskovitch [14] used machine learning techniques in classification of a computer behavior into malicious and benign. He focuses on the feasibility of accurately detecting unknown worm activity in individual computers while minimizing the required set of features collected from the monitored computer. Four feature selection methods were used to reduce the number of features and four learning algorithms were applied on the resulting feature subsets; four commonly used Machine Learning algorithms: Decision Trees, Naive Bayes, Bayesian Networks and Artificial Neural Networks. The evaluation results suggest that by using classification algorithms applied on only 20 features, the mean detection accuracy exceeded 90%, and for specific unknown worms accuracy reached above 99%, while maintaining a low level of false positive rate. Andrzej Bielecki [1] developed a neural approach to worm detection designed as a part of a multi-agent system intended to manage IP networks.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

The efficiency of virus recognition is about 95%. One of the AI techniques mentioned in that survey [9] is ANN.

A. Using Artificial Neural Network in Worm Detection

Stopel et-al [17] produced an approach for detecting the presence of computer worms based on ANN using the computer's behavioral measures. Stopel et-al [17] compared three different feature selection techniques for the dimensionality reduction and identification of the most prominent features to capture efficiently the computer behavior in the context of worm activity. In order to evaluate the different techniques, several computers were infected with five different worms and 323 different.

B. Trapping Worms using Darknets

Worms replicate themselves without human interactions by remotely exploiting known vulnerabilities in operating systems or application services. If we break down the actions of these worms [4] [5] [6], the following common behaviors or stages will be exposed: Target Selection, Exploitation, and Replication [19].

IV. QUARANTINING WORMS THROUGH BLACKLISTING AND FILTERING

Address blacklisting and packet filtering are two major approaches to quarantine worm propagation. Address blacklisting excludes traffic from identified worm sources, while packet filtering could drop traffic according to specified rules. The rule can be a traffic flow specification or a typical payload content, which is identified as a particular worm signature. Strictly speaking, address blacklisting is a special form of packet filtering. The access control entry (FW1) in Figure 2 is an example of address blacklisting. Perfect Cyber Entrap is designed to support both methods to mitigate spreading worms and its ultimate goal is to realize complete automation for worm quarantine:

-Firstly, traffic communicating with administrated darknet spaces is automatically classified according to intended services;

-Secondly, those worm traffic related to one service type is grouped and leveraged to automatically extract worm signatures5;

-Thirdly, those worm signatures are automatically uploaded to reconfigure firewalling or routing devices to drop relevant worm traffic. Recent research efforts like Autograph [21] and EarlyBird [25] are exploring automatic ways to extract worm signatures. This paper examines the approach of address blacklisting. However, it can be easily extended to accommodate signature-based content filtering.

In the following sections, we study the formal analysis of Perfect Cyber Entrap and examine its effectiveness and responsiveness.

V. RELATED WORK

Modeling, detecting, and quarantining worms have drawn significant attention due to observed outrages of various worms [4, 5, 9, 8]. In the following, we examine related work in these areas:

A. Worm Modeling- Accurate models could give insights into mitigating worm spreadings by examining various factors which influence their spread. Kephart and White *et al.* [20] proposed a classic epidemiological model to measure computer virus prevalence. Zou *et al.* [38] analyzed the propagation of the Code Red worm and presented *two factor model* by taking into account network congestions and human counter-measures for worm propagation. Chen *et al.* [13] further considered parameters such as the worm scan rate, the vulnerability patching rate, and the victim death rate and proposed a concise discrete-time worm model, i.e., *AAWP* model. However, they did not consider each individual peering AS in current Internet and have not analyzed defense mechanisms in great depth.

B. Early Detection- Timely detection of worms at early stage is critical in mitigating malicious spreadings. Virulent worms could cause certain traffic characteristics like abnormalities in overall traffic and similarities within worm traffic. These traffic characteristics could be leveraged for detecting the existence of worms. EarlyBird[25] examines *heavy hitter* and *many flows* in Internet traffic to infer the existence of worms. Based on highly repetitive content in worm traffic, EarlyBird further extracts worm signatures automatically. However, polymorphic or metamorphic worms impose a significant challenge by obfuscating worm payloads. Packet Matching [12] detects worm probing traffic by matching destination port numbers between incoming and outgoing connections and blocks those traffic once identified accordingly. Different from Packet Matching, Perfect Cyber Entrap takes advantage of darknet space to detect the existence of worm and thus is able to achieve nearly zero false-positive (correctly identify a worm node once detected) and very low false-negative (false to detect the existence of worm nodes).

As mentioned before, darknet has advantages over normal networks in its ability collecting highly concentrated malicious traffic. With the same observation, Network Telescope [22], Internet Motion Sensor [2], and i Sink[36] explore one or a set of dedicated darknet spaces for inferring certain remote network events, sensing Internet motions, and understanding network abuse. However, these approaches (1) are either passively monitoring these background radiation traffic or interacting with them in a limited fashion; and (2) did not further propose counter-measures to mitigate worm propagation. Instead, Perfect Cyber Entrap enables full-interaction with dynamically instantiated virtual machines and takes a further step in attempting to reactively quarantine detected worm nodes. Also with deployment within each peering enterprise networks Perfect Cyber Entrap has the authoritative to block worm nodes or filter relevant traffic at the source.

C. Dynamic Quarantine- Accurate worm modeling and early detection need to be followed by dynamic quarantine mechanisms in order to successfully curtail worm

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

outrages. Williamson *et al.* [29] proposed the idea of host-based rate limiting by restricting the number of new outgoing connections connections.

Chen *et al.*[11] designed a temporal rate-limit algorithm and a spatial rate-limit algorithm to make the speed of worm propagation configurable by the parameters of their defense system, i.e., *DAW*. Zou *et al.* [39] suggested quarantining a host whenever its behavior looks suspicious by blocking traffic on its anomaly port. Then the quarantine is released after a short time, even if the host has not been inspected by security staffs yet. Weaver [31] suggested breaking the network into many small *cells* and limited a worm's spread by isolating it in the cell.

Wong *et al.* [34] examined the placement of rate-limiting filter and found that (1) backbone routers could be effective in limiting randomly-scanning worms and (2) a reasonable rate limits for an enterprise network would severely restrict the spread of a worm with negligible impact on almost all legitimate traffic. More generally, Moore *et al.* [23] examined the design space for worm containment systems and studied the efficacy of address blacklisting and content filtering. Perfect Cyber Entrap complements these approaches and further takes feasibility of counter-measures into consideration: actively quarantines nodes within its authoritative domain while blacklisting those nodes infecting from outside. Additionally, Perfect Cyber Entrap further enables the cooperation among different domains which could further slow-down worm spreadings.

VI. CONCLUSION

Increased frequency and virulence or automatic replication of worm outbreaks significantly challenge the safety and reliability of any Enterprise network and current shared Internet infrastructure. This paper proposes a systematic fast automatic detection & quarantining by Perfect Cyber Entrap to detect and quarantine worm spreadings. Perfect Cyber Entrap leverages available darknet space for worm capture, utilizes virtual machines for triggering infection, and actively quarantines active worms by traffic filtering.

Malicious activity detector using Artificial Intelligent System is responsible to analyze the traffics carefully and try to detect malicious activities that internal host may perform and separate those hosts and send to next stage.

Traffic monitoring is responsible to detect the group of hosts that have similar behavior and communication pattern by inspecting network traffics. So Perfect Cyber Entrap simply evaluate fast and automatic detection and quarantining of Internet scanning worms, Topological worms, web worms and botnet on the enterprise network which connected to the Internet.

REFERENCES

[1] Dynamic Firewall Tools - dynfw. http://www.gentoo.org/pro j /en/dynfw.xml.
[2] Internet Motion Sensor. http://ims.eecs.umich.edu/.
[3] The Honeynet Project. http://www.honeynet.org.
[4] Code Red Worms. CAIDA Analysis of Code-Red Wormshttp://www.caida.org/analysis/security/code- red/, 2001.
[5] MSBlaster Worms. CERT Advisory CA-2003-20 W32/Blaster Worms http://www.cert.org/advisories/CA-2003-20.html, Aug. 2003.
[6] SQL/Slammer Worms. CERT Advisory CA-2003- 04 MS-SQL Server Worms http://www.cert.org/advisories/CA-2003-04.html, Jan. 2003.
[7] CERT/CC Statistics. CERT Coordination Centre, http://www.cert.org/stats/cert stats.html, 2004.
[8] Sasser Worms. http://www.microsoft.com /security/incident/sasser.asp, May 2004.
[9] Witty Worms. http://securityresponse.symantec.com/ avcenter/venc/data/w32.witty.worm.html, Mar. 2004.
[10] S. Chen and S. Ranka. An Internet-Worm Early Warning System. Proceedings of the IEEE Globecom 2004 – Security and Network Management, Dallas Texas, USA, Nov. 2004.
[11] S. Chen and Y. Tang. Slowing Down Internet Worms. Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'04), Tokyo, Japan, Mar. 2004.
[12] X. Chen and J. Heidemann. Detecting Early Worm Propagation through Packet Matching. Technical Report ISI-TR- 2004-585, USC/Information Sciences Institute, Feb. 2004.
[13] Z. Chen, L. Gao, and K. Kwiat. Modeling the Spread of Active Worms. INFOCOM 2003, San Francisco, CA, Mar. 2003.
[14] D. Dagon, X. Qin, G. Gu, W. Lee, J. Grizzard, J. Levine, and H. Owen. HoneyStat: Local Worm Detection Using Honeypots. Proceedings of the 7th International Symposium on Recent Advances In Intrusion Detection (RAID 2004), Sophia Antipolis,French Riviera, France, Sept. 2004.
[15] R. Dantu, J. Cangussu, and A. Yelimeli. Dynamic Control of Worm Propagation. Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 1, Apr. 2004.
[16] H. W. Hethcote. The Mathematics of Infectious Diseases. SIAM Review, vol. 42, no. 4, pp. 599- 653, 2000.
[17] X. Jiang and D. Xu. BAIT-TRAP: a Catering Honeypot Framework. Aug. 2004.
[18] X. Jiang and D. Xu. Collapsar: A VM-Based Architecture for Network Attack Detention Center. Proceedings of the USENIX 13th Security Symposium, San Diego, USA, Aug. 2004.
[19] X. Jiang and D. Xu. Worm Meets Beehive. Department of Computer Sciences Technical Report CSD TR 04-027, Purdue University, May 2004.
[20] J. O. Kephart and S. R. White. Measuring and Modeling Computer Virus Prevalence. Proc. of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy, 2-15, May 1993.
[21] H. A. Kim and B. Karp. Autograph: Toward Automated, Distributed Worm Signature Detection. Proceedings of the 13th Usenix Security Symposium (Security 2004), San Diego, CA, Aug. 2004.
[22] D. Moore. Network Telescopes: Observing Small or Distant Security Events. Proc. of the 11th USENIX Security Symposium (Security '02), San Francisco, CA, Aug. 2002.
[23] D. Moore, C. Shannon, G. M. Voelker, and S. Savage. Internet Quarantine: Requirements for Containing Self- Propagating Code. Proceedings of the IEEE Infocom Conference, San Francisco, CA, Apr. 2003.
[24] S. E. Schechter, J. Jung, and A. W. Berger. Fast Detection of Scanning Worm Infections. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID), Sophia Antipolis, French Riviera, France, Sept. 2004.
[25] S. Singh, C. Estan, G. Varghese, and S. Savage. Automated Worm Fingerprinting. Proceedings of the ACM/USENIX Symposium on Operating System Design and Implementation, San Francisco, CA, Dec. 2004.
[26] E. Spafford. The Internet Worm Program: an Analysis. Purdue CS Technical Report TR-CSD-823, 1988.
[27] S. Staniford, G. Grim, and R. Jonkman. Flash Worms: Thirty Seconds to Infect the Internet. http://www.silicondefense.com/flash, Aug. 2001.
[28] S. Staniford, V. Paxson, and N. Weaver. How to 0wn the Internet in Your Spare Time. Proceedings of the USENIX 11th Security Symposium, San Francisco, USA, Aug. 2002.
[29] J. Twycross and M. M. Williamson. Implementing and Testing a Virus Throttle. Proceedings of the USENIX 12t Security Symposium, Washington DC, USA, Aug. 2003.
[30] H. J. Wang, C. Guo, D. R. Simon, and A. Zugenmaier. Shield: Vulnerability-Driven Network Filters for Preventing Known Vulnerability Exploits. SIGCOMM 2004, Sept. 2004.
[31] N. Weaver, S. Staniford, and V. Paxson. Very Fast Containment of Scanning Worms. Proceedings of the USENIX 13th Security Symposium, San Diego, USA, Aug. 2004.
[32] E. W. Weisstein. Logistic Equation. http://mathworld.wolfram. Com/LogisticEquation.html.
[33] P. J. Welcher and G. Moerschel. Cisco PIX Firewall Basics. http://www.netcraftsmen.net/welcher/papers/pix01.html.