Camouflage Worm Detection and Counter-Measures

Edward Danso Ansong, J. B. Hayfron-Acquah, Dominic Damoah, Michael Asante, Brighter Agyeman

Abstract:- This research focuses special attention on a new class of worms called Camouflaging worm (C-Worm). The key difference between C-Worm and traditional worms is that, it displays the ability to intelligently analyse and make changes to its scan traffic volume over time. This new class of active worms is an attack that spread itself on the internet by exploiting vulnerabilities on computer systems.

Keywords:- C-Worm, Camouflaging, traditional, vulnerabilities.

I. INTRODUCTION

This new class of active worms is an attack that spread itself on the internet by exploiting vulnerabilities on computer systems. Many worms are used as bots or zombies which are then networked together to form botnets that can launch DDoS, spamming, etc. As a result of their effects, Worm detection involves control and screening, gleaning data and analyzing scanned traffic for vulnerable avenues for worm attacks. [17], [15] Worms have four main phases of causing infection to user agents. These phases are Worm Target finding scheme, Worm propagation scheme, Worm transmission scheme, Worm payload formats. The commencement of worm's life is to locate vulnerable targets. With blind targeting the attacker does not know them before the attack is done. These blind scanning whether sequential, random, or permutation have rampant downtime connection. This method of scanning have high infection rate because it is very simple to implement. To improve blind scanning scheme, the local subnet is scanned via the present vulnerable target or the entire internet IPV4 addresses. [5]. Another method for target finding the use of hit list. This makes focusing on the target very accurate for the deploying the worm. Hence the worm could be propagated by direct contact or through a third part or as an embedded patch. For example Remote Procedure Call, a service, could be used to silently propagate embedded worms. Worms that are transmittable through TCP are latency limited because TCP are connection oriented and has a 3 way handshake whereas under UDP worms are bandwidth limited because it is connectionless. Worms silently hide in the Payload thereby assuming dynamic and variable size which makes it difficult to detect but it should be noted that the worm's signature stays unchanged. These Payload worms are better described as Monomorphic, Polymorphic and metamorphic. C –Worm has the ability to scan traffic volume intelligently and surreptitiously propagating itself to infest targets.

Manuscript Received on August 2014.

Edward Danso Ansong, Department of Computer Science & Information Technology,Valley View University, Accra-Ghana.

J. B. Hayfron-Acquah, Department of Computer Science, Kwame Nkrumah University of Science & Technology, Kumasi-Ghana.

Dominic Damoah, Department of Computer Science & Information Technology, Valley View University, Accra-Ghana.

Michael Asante, Department of Computer Science, Kwame Nkrumah University of Science & Technology, Kumasi-Ghana.

Brighter Agyeman, Department of Computer Science & Information Technology, Valley View University, Accra-Ghana.

C-Worm is disparate and has the propensity to conceal itself for easily been detected intrusion detection systems and anti-malicious programs very much at variance with the traditional worms. Finally C-Worm demonstrates that it a self- propagating behavior similar to traditional worms.

II. EXISTING DETECTION STRATEGIES

A. Traffic Analysis

Traffic analysis is the act of analyzing the network's communications and the patterns inherent in it. The traffic characteristics are connections ports, efficiency of connection, traffic volume per host over a period, communication peers, and protocols. All these combined gives indication of the presence of worms in the network. [10]

B. Honeypots

Honeypots are used to detect intrusion in a network. As a decoy set up in a network to purposely trap intruders they are used as a monitoring tool. This helps to keep intruders off from accessing vulnerabilities in the network and also to study their behavior. This gives serious indication of possible attacks and inclinations to exploitation. We are able to study the adversaries closely to have insight in their activities and exploitation trends. Suffice to say that this powerful decoy is also useful for in multi-user environments for gathering information to ensure intrusion could be detected and prevented. [10]

C. Signature Based Detection

Signature analysis is the method of analyzing the content of captured data to detect the presence of known strings. These signatures are kept in a database and are derived from the content of known malicious files. These files are typically the executable programs associated with worms. The strength of signature analysis relies on the validity of a basic assumption: that the behavior of one instance of malicious software is representative of all instances. This can also include attacks that occur on a network. For worms, this means that by studying one node of the worm, the behavior of all nodes that are compromised by the worm can be reliably predicted. [10]

D. Power Spectral Density (PSD) Method

[10] Power Spectral Density (PSD) method is a detection method for determining distinct pattern of C worms in the frequency domain. C worms propagate furtively using the Power Spectral Density (PSD) and Spectral Flatness Measure (SFM) of the scan traffic. As proposed by [16], spectrum-based detection scheme can be used for detecting C-Worm effectively. This scheme captures the distinct pattern of the C-Worm in the frequency domain, and thereby has the potential of effectively detecting the C-Worm propagation. A source count is used as the basis of the worm detection. The source count is the number of the unique sources that launch scans during worm propagation. Source

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

count data is obtained because a worm detection system collects logs from distributed monitors across the Internet. The source count is obtained by counting the number of unique source IP addresses in received logs. The metrics that were used in evaluating this approach were the Detection Time (DT) and the Maximal Infection Ratio (MIR). DT is defined as the time taken to successfully detect a wide-spreading worm from the moment the worm spreading starts. It quantifies the detection speed of a detection scheme. MIR defines the ratio of infected host number over the total number of vulnerable hosts up to the moment when the worm spreading is detected. Analysis and evaluation showed that, although the C-Worm successfully camouflages its propagation in the time domain, its camouflaging nature inevitably manifests as a distinct pattern in the frequency domain. The evaluation data showed that this scheme achieved superior detection performance against the C-Worm in comparison with existing worm detection schemes. [16]. Also, as illustrated by [4], the application of the spectrum based detection scheme again proved efficient in detecting C-Worms. This scheme makes use of Power Spectral Density (PSD) and Spectral Flatness Measure (SFM). In order to identify the C-Worm propagation in the frequency domain, we use the distribution of Power Spectral Density (PSD) and its corresponding Spectral Flatness Measure (SFM) of the scan traffic. Particularly, PSD describes how the power of a time series is distributed in the frequency domain. Mathematically, it is defined as the Fourier transform of the auto-correlation of a time series. The SFM of PSD is defined as the ratio of geometric mean to arithmetic mean of the coefficients of PSD. The range of SFM values is between 0 and 1 and a larger SFM value implies flatter PSD distribution and vice versa.

III. RELATED WORKS

A. Detection Based on Various Scan Techniques

[13] Analyses various scan techniques and proposed a generic worm detection architecture that monitors malicious activities. They evaluated an algorithm to detect the spread of worms using real time traces and simulations. They presented an analysis on potential scan techniques that worms can employ to scan vulnerable machines. In particular, they found that worms can choose targets more carefully than the random scan. A worm that scans only IP addresses announced in the global routing table can spread faster than a worm that employs random scan. They analyzed a family of scan methods and compared them to the random scan. Second, they proposed worm detection architecture and algorithms for prompt detection of worm activities. Their detection architecture takes advantage of the fact that a worm typically scans some unassigned IP addresses or an inactive port of assigned IP addresses. By monitoring unassigned IP addresses or inactive ports, one can collect statistics on scan traffic. These statistics include the number of source/destination addresses and volume of the scan traffic. They proposed a detection algorithm called victim number based algorithm, which relies solely on the increase of source addresses of scan traffic and evaluated its effectiveness. Drawback: Their solution can detect worm activities when only 4% of the vulnerable machines are infected. The number of false alarms increases in the case of a DDoS attack or in the case of a hot website visit or in the case of a hot website visit.

B. Super Spreaders Detection

[6] Considered how to detect super spreaders. They proposed an algorithm with guaranteed accuracy and memory management. The algorithm was experimented on network and distributed environments with traces of Super Spreader. The results show great efficiency than earlier algorithms. The algorithm has been extended with proposition to two efficient algorithms to find super spreaders. The first one is algorithm that is able to filter sample from a set of distinct source destinations. The second one a sophisticated algorithm which is memory efficient and has two level filtering schemes. The only drawback is that it require a minimum sampling rate.

C. Varying Scan Rate Worm Detection

[17] The new worms, VSR worm is the polymorphic type that spreads easily and avoids detection. Furthermore, an effective analysis of the VSR worm shows it is able to avoid detection by existing and recent worm detection algorithms. Hence novel schemes have been developed to detect VSR and traditions worms alike. One such schemes is the Distribution Entropy-Based Dynamic (DED) detection which is able to detect VSR worms with different scan rates. This scheme launches distributed attacks by scanning targets for basic detection of prominent attributes carefully designed for the propagation of the worms. .Performance evaluation demonstrated that DED detection scheme is fast and accurate in detecting both VSR and traditional worms.

D. Distributed Host Based Worm Detection System

[1] Presents a method for detecting large-scale worm attacks using only end-host detectors. These detectors propagate and aggregate alerts to cooperating partners to detect large scale distributed attacks in progress. The properties of the host-based detectors may in fact be relatively poor in isolation but when taken collectively result in a high-quality distributed worm detector. A cooperative alert sharing protocol coupled with distributed sequential hypothesis testing to generate global alarms about distributed attacks. They evaluated the system's response in the presence of a variety of false alarm conditions and in the presence of an Internet worm attack. Their evaluation is conducted with agents on the Emu lab and DETERS emulated test beds using real operating systems and computing platforms.

Disadvantages: They have not taken into consideration the effect of the worm traffic from outside their network of interest. They have also not considered the effects of malicious nodes in the federation in their experiments.

E. Mining Dynamic Program Execution

[12] Proposed a new worm detection approach based on mining dynamic program executions. This approach captures dynamic program behaviour to provide accurate and efficient detection against both seen and unseen worms. In particular, they executed a large number of real world worms and benign programs (executables), and trace their system calls. They applied two classifier-learning algorithms (Naïve Bayes and Support Vector Machine) to obtain classifiers from a large number of features extracted from the system call traces. The learned classifiers are further used to carry out rapid worm detection with low overhead on the end-host. Their experimental results clearly

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

demonstrate the effectiveness of their approach to detect new worms in terms of a very high detection rate and a low false positive rate.

Disadvantages: This method is the study of host-based detection and they did not consider information about the traffic generated by the executables during the worm detection. Since these worm behaviours are exposed from different perspectives, consideration of multiple behaviours could provide more accurate worm detection.

F. Local Worm Victim Detection Algorithm

Local worm victim detection algorithm [3] has a focus on Destination Source Correlation (DSC) and Scanning pattern. They are able to detect zero-day scanning worms. DSC is designed to reveal scans and fast attacking worms. Slow spreading worms are usually brought under control since they are less destructive in the network. For example SQL slammer and Code Red are so fast that human intervention is practically impossible as the case may be in slow spreading worms, email worms. DSC is replete with mechanism to detect infection and check scan rate for malicious and then quarantine the infected outgoing traffic at the port. The downside is that the DSC may not effectively detect email worms.

A. Real-Time Worm Detection

[6] Present the design and implementation of a system that automatically detects new worms in real time by monitoring all traffic on a network. In this paper, they presented the design and implementation of a system that automatically detects new worms in real-time by monitoring traffic on a network. The system uses Field Programmable Gate Arrays (FPGAs) to scan packets for patterns of similar content. Given that a new worm hits the network and the rate of infection is high, the system is automatically able to detect an outbreak. Frequently occurring strings in packet payloads are instantly reported as likely worm signatures.

Disadvantages: The system is quite effective at detecting smaller worms at an early stage. But detecting larger worms becomes a much harder task.

Other related works

A. Different Host Based Defense Systems

[2] Focuses on the detection of active worms which are automated malicious code, posing a major threat to internet security. In this paper, they have investigated the modelling and analysis of these security threats. As a result two groups of defense systems are identified. The first group is the scanning rate and the second group exploits vulnerable machines. This work provides insight into the essence of different host based defense systems and their combination quantitatively.

B. WAtCoS

[8] In this research they have made a comparison on visualization, simulation and games and stated that how useful they in malware studies. WAtCos [8] demonstrates the potentials of using visualization, simulation and games. For example it can be used in a multicast environments to evaluated spread of such worms as Ramen and SQL Slammer.

C. Digital Signatures

[14] Describes the working and the use of digital signatures in protecting our confidential information flowing through a network. This paper briefs about the conventional and digital signature characteristics followed by explaining the procedure to create and verify the digital signature and digital envelope. Its applications in real time are also discussed over here. This work is motivated by the fact that most organizations nowadays do electronic transactions which is why they protection. It is highly expected that the emerging technology will grow exponentially in the near future.

D. Survey of Internet Worm Detection and Containment

[7] This paper focus on the internet worm attacks, and schemes specifically designed for detection and containment. Attention is also devoted to identification of worms by their characteristics and behavior for classification purposes. Algorithms for detection and containment are also visited with the view to exploring current methodologies for slowing down spread of worms or stopping them entirely. Finally this paper throws open the scope of where to locate and implement detection and containment as well as the challenges of detecting worms that go undetected for further research.

IV. CONCLUSION

DDOS attacks, particularly TCP SYN Flood attack results in slow network performance, unavailability of a particular web site, inability to access any web site and dramatic increase in the amount of spam you receive in your account.

An active worm such as Camouflaging worms infects as many computers before being detected. As more and more computers get infected, they, in turn, take part in scanning other computers. Hence, it is considered the C-worm as a worst case attacking scenario that uses a closed-loop control for regulating the propagation speed based on the feedback propagation status.

REFERENCES

[1] Cheetancheri, S. G., Agosta, J. M., Dash, D. H., Levitt, K. N., Rowe, J., & Schooler, E. M. (2006). A distributed host-based worm detection system. LSAD '06 Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense (pp. 107-113). ACM.

[2] Chen, Z., Gao, L., & Ji, C. (2003). On Effectiveness of defense systems against active worms.

[3] Gu, G., Sharif, M., Qin, X., Dagon, D., Lee, W., & Riley, G. (2004). Worm detection, early warning and response based on local victim information. 20 th Annual Computer Security Applications Conference.

[4] M.A.BASEER, M., NARAYANA, M. P., & LAHANE, M. S. (2013). Modeling and Detection of Camouflaging Worm. INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGIES, VOL. 01, ISSUE 02, 99-104. Retrieved 12 2013

[5] M.K, P. C., & P.V, M. (2012). Modelling and Detection of Camouflaging Worms. International Journal of Emerging Technology and Advanced Engineering, 2-3. Retrieved 12 2013

[6] Madhusudan, B., & Lockwood, J. (2004). Design of a System for Real-Time Worm Detection. HOTI 12.

[7] Pele Li Mehdi Salour, X. S. (2008). Survey of Internet Worm Detection and Containment. IEEE Communications Surveys.

[8] Saudi, M. M., Seman, K., Tamil, E. M., Yamani, M., Idris, I., & Visualization, A. (2008). Worm Analysis through Computer Simulation (WAtCoS). Proceedings of the World Congress in Engineering 2008, 1.

[9] Singh, S., Estan, C., Varghese, G., & Savage, S. (2003). The EarlyBird System for Real-time Detection of Unknown Worms. Technical Report CS2003-0761. University of California, San Diego.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

[10] Talli, P., & Krishna, M. V. (2012). Detection of Active Internet Worm: Camouflaging Worm. nternational Journal of Electronics Communication and Computer Engineering, 3(5), 1172-1175. Retrieved 12 2013

[11] Venkataraman, S., Song, D., Gibbons, P. B., & Blum, A. (2004). New Streaming Algorithms for Fast Detection of Superspreaders. Intel Corporation. Retrieved 1 2014

[12] Wang, X., Yu, W., Champion, A., Fu, X., & Xuan, D. (2007). Detecting Worms via Mining Dynamic Program Execution. Third International Conference on Security and Privacy in Communication Networks and the Workshops, SecureComm 2007, (pp. 412-421). Nice,France.

[13] Wu, J., Vangala, S., Gao, L., & Kwiat, K. (2004). An Effective Architecture and Algorithm for Detecting Worms with Various Scan Techniques. 11th Annual Network and Distributed System Security Symposium (NDSS '04).

[14] Yi, B. k. (2006). Digital Signatures.

[15] Yu, W., Wang, X., Calyam, P., Xuan, D., & Zhao, W. (2011). Modeling and Detection of Camouflaging Worm. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL., 1-3. Retrieved 12 29, 2013

[16] Yu, W., Wang, X., PrasadCalyam, Xuan, D., & Zhao, W. (n.d.). On Detecting Camouflaging Worm.

[17] Yu, W., Wang, X., Xuan, D., & Lee, D. (2006). Effective Detection of Active Worms with Varying Scan Rate. IEEE International Conference on Security and Privacy in Communication Networks (SecureComm).

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.