Internet Worm Detection Using Distributed Blackhole Networks

Kinjal N. Patel

IT Systems & Network Security, GTU

Abstract

In Today's widely interconnected networks, worms and threats against data and infrastructure continuously emerging. Network security always has been interested field for researchers to invent new methods for securing networks. Operational Network Security is probably be traced back to the events when the self propagating code found on the internet. The incident became known as Internet Worm or Great Worm. Many Network security researchers consider this event as "Sputnik moment" that leads researchers and administrators to take action to secure open network. Since last several years there are various methods proposed to secure networks. Here proposed work is composed of various studies and research work on networks monitoring techniques based on Dark-net. Darknet or Blackhole Monitoring is a promising approach to secure network by monitoring unused address space (dark-space) of network. Unused address space contain no legitimate traffic because there is no active host or service running and there is no legitimate reason for packets destined at darknet. This research work describes the system which works on the principle of darknet. Here, proposed design of internet worm monitoring system has four main elements: 1) Blackhole Sensor-which passively collects packets received at dark-space, 2) Low interaction server-extends functionality of Sensor y responding to TCP worm request, 3) Distributed Mechanism-provides high visibility into internet worm by deploying sensors in dispersed networks, 4) Central Monitoring-single point of threat event monitoring across all distributed sensors.

1. Introduction

This research work intends to discuss identification and defense against such threats within context of globally interconnected network –internet. Internet connectivity is the basic need of any organization and hence it is more vulnerable to attack. With the current trend of outsourcing data, cloud computing, and distributed interconnected networks, these processes results in increases exposure of organization and its computation system at risk. Organization all over the world now transacting online and have limited technical support staff, with the lack of full time network operational staff these organizations' are subjected to attacks. With the growing threats to internet, various network security solutions are developed. This research work consists of one of the threat detection system which is globally deployed.

Over the last few years, internet worms are widely emerging problems for network security researchers. Internet worm attacks cause a significant threat to network security and management. Internet users had experienced devastating effects of network worms. Internet worms include SQL Slammer [1], Witty, Blaster [2], Code Red [3] worm that spread at high speed over the internet. These worms spread so rapidly that existing defense system cannot respond until most vulnerable machines have been infected.

Intrusion detection systems, firewalls and other traditional security solutions are used in organizations to defense against external threats but these solutions are costly and difficult to deploy and configure. These security solutions cannot stand with newly emerging threats and worms in internet. Another solutions relating to the use of interactive system including high interaction honey pots and honey-nets, brings their own sets of risk and complications in their operation and deployment within an organization's network. Techniques and tools presented in this work are designed to collect malicious traffic passively and with low interaction.

Darknet/Blackhole monitoring offer unique advantage in observing large scale network events like distributed Denial-of-Service (DDoS) or Internet worms. Darknet is a set of unused IP address space in internet or within specific network. Most of the traffic arriving at dark-net is malicious or unintended because there is no legitimate live host or service on the darknet. This traffic towards Dark-net includes hostile reconnaissance scans, probe activities form infected active worms, DDoS backscatters, and packets from misconfigured hosts.

Darknet monitoring is the effective approach for securing network and defense against new emerging threats in internet and it attracts most researchers' attention to explore new things in the new direction of network security. Several researchers had proposed methods to capture and analyze the traffic directed to the darknet.

2. Related Work

The field of the Darknet monitoring and Blackhole sensor networks is new in the network security with the David Moore's [4] work being one of the earliest mentions of the practical implementation and application of network telescope. Michel Bailey [5] and team present Internet Motion Sensor Project which is the further exploration in the field of darknet & addresses large monitoring surface over glob. The reports on the analysis of the Code Red [3] and Slammer [1] worm were the earliest published information making use of the various projects on darknet. Another darknet project maintained by Team Cymru [6] is the live project and detected worms like Witty. There is still much in the field of darknet. This research aims to clarify some of these aspects.

3. Research Outline

All This research has been conducted with the following objectives in mind:

- To provide network security solution having advantages over traditional security solutions.
- The use of dark-net monitoring technique for collecting and monitoring traffic forwarded to unused IP (dark-space) address space of network.
- Using the passive packet collector server (Blackhole sensor) and low interactive server for better identification of threats and newly emerging worms.
- The assessment of distributed monitoring system as a means of early detection and most importantly to identify the spreading of worms or the events like DDoS attacks over large scale, further whether malicious traffic is widespread or has targeted to specific organizational network.
- The study of suitable tools and methods for the designing the distributed architecture for the proposed system and analysis of packets collected at analysis server.
- The final objective is to design a system/ framework based on above goals which allows more easier and structured application of Darknet as a part of organization's security strategy as well as collected information for operational and research purpose is also considered.

4. Darknet Traffic Monitoring

4.1 Darknet Taxonomy

While the concept of darknet has been discussed since 2002, there are lots of varying definitions as to what each concept means. Dark-net, Telescope, Sink and Blackhole, these terms are used to describe system with no live host and which acts as a complete passive packet collector. This type of system is defined as "Blackhole" by Michel Bailey & Cooke [7]. This research further defines the design of distributed Blackhole sensors in dispersed networks. The term "Darknet" is used in open and general communication. It is dark because network block does not have any live system. Sink and Telescope refer to the type of system which capture all traffic destined to unused space.

The term darknet is also used in different sense which refers to hidden distributed private networks on internet. This is mainly used for distributing illicit content. This widespread acceptance of private darknet is followed by publication of "The darknet & Future of content Distribution" [8].

4.2 Incoming Traffic at Darknet

Primary advantage of using Blackhole networks to detect worms and threats over standard methods is that, due to no active host or service running over dark space, traffic monitored by Blackhole sensor is malicious or unintended. Hence there is no requirement of separating legitimate traffic from malicious traffic. Traffic originating from internet hosts and arrived at Blackhole networks can be classified as one of the following categories:

1) Backscatters: Traffic resulting from the monitored address space being maliciously used for spoofing elsewhere mostly DDoS attacks or misconfigured attacks. This also includes probing activities from worm infected hosts.

2) Misconfigured: Traffic is the result of misconfigured host on the network which sends unwanted packets in network.

3) Aggressive/Hostile: The bulk of observed traffic seen on sensor node can be classified as likely to attack or hostile. This includes various network scans.

4.3 Classification of Traffic

Classification of dark-net traffic is important if the data collected by monitoring node is used for automated countermeasures or security management

system. Traffic received at Blackhole sensor can be further classified into two broad categories:

4.3.1 Passive Traffic: Traffic which requires no legitimate response from system's TCP/TP networking stack when it is received at monitoring node. Traffic observed at Blackhole sensor considered as passive may be result of scanning activity by worm infected host, denial of service or ping floods, misconfigurations or the traffic generated by software or hardware error of host. IP payloads such as TCP RST or ICMP unreachable datagram can be classified as passive traffic.

4.3.2 Active Traffic: Traffic which requires response from System's TCP/IP stack when processed. The TCP scanning techniques attempt to elicit either a RST packet in response from ports not listening, or a response as a part of TCP 3-way handshake in case of SYN scanning on ports that are not listening.TCP null scan, URG scan, SYN scan and FIN scan are the example of active scanning by network scanning tools like nmap.

4.4 Monitoring Schemes

4.4.1 Passive Monitoring: Most organization use IDS or Firewall as their security solutions, which makes system complex and hard to manage. Two main problems with traditional security solution are differentiation of malicious traffic and legitimate traffic and dealing with increasing traffic in network. Blackhole monitoring node scan mitigate above growing challenges by only monitoring the traffic which is intended to unused IP space of network. Traffic is malicious hence there is no active host. The Blackhole sensor in this research does not respond to any packets arrived at sensor, hence no one can sense about the packet capturing.

4.4.2 Distributed Monitoring*:* The principle of darknet monitoring can be extended by implementing distributed architecture for monitoring threats over large surface. In this distributed mechanism multiple Blackhole sensor nodes are deployed in dispersed networks like organization network, university campus or any internet service provider network.

5. Methodology of Distributed Blackhole Networks

5.1 Passive Monitoring with Blackhole Sensor

Blackhole sensor is not a sensor in the sense of wireless sensors but it is the system to monitor portions of unused IP address space. Specifically a Blackhole Sensor makes use of unallocated IP addresses which are not being used for running services. The Blackhole Sensors passively collect all UDP and ICMP traffic and get information in one packet (Witty and Slammer [1] worms were based on UDP in which the entire worm payload was transmitted in the first packet).

5.1.1 Identifying Unused and Unallocated Address Space: The first issue with the dark space monitoring is to find out and filter the unused and unallocated address spaces within organization networks. Depending on their policies, different organization use different methods to allocate IPs to the live systems. There are mainly two approaches to assign IPs to every system in network:

Statically assigned IP addresses in Network- If the network uses this method to assign IPs than Blackhole Sensor is pre configured to monitor the network block of IP addresses which are not used and unallocated.

Used DHCP server to assign IP addresses- DHCP server maintains the list of all assigned IPs and corresponding host in the "dhcp-lease" file. From that file we can filter the list of unassigned IP addresses.

5.1.2 Location of Blackhole Sensor: Another important consideration of Blackhole monitoring is placement of Blackhole Sensors in network. Important darknet placement consideration is the location within a network. If a darknet monitor is placed behind a firewall or other infrastructure protection or filtering device, it will likely not observe all externally sourced threats, as some packets are already filtered by firewall. On the other hand, Blackhole sensor within the network can also provide important visibility into locally-scoped threats within a network. The most frequently occurred threats are executed from entity within security parameter. Ideally, a Blackhole sensor deployment that includes monitors deployed both inside and outside network perimeters should have the greatest potential visibility.

5.1.3 Sample Network Block with Blackhole Sensor:

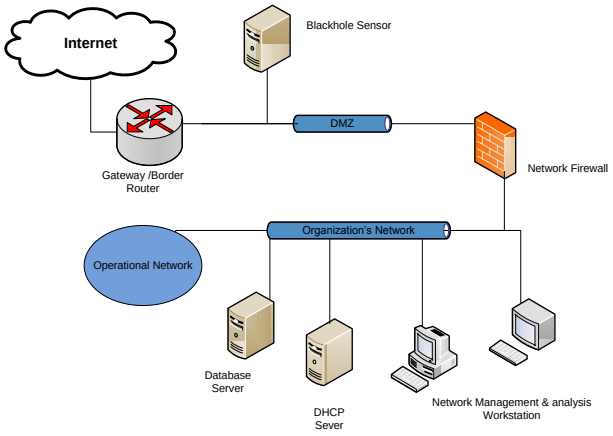

Figure 1 Sample Network Block with Blackhole Sensor

Fig. 1 is the sample network diagram with Blackhole sensor represent passive monitoring scheme with one Blackhole sensor within network. In this scheme Blackhole sensor deployed after border router of organization and before the main firewall. This allows the Blackhole sensor to capture all types of packets without any further filtration done by any security device. Sensor monitors the unused IP address block of the network. The sensor was either comprised of independently routed /24 (class c addresses) sized net-block or run the script to fetch list of IPs to monitor. In above diagram we allocated specific predefined net-block to sensor for monitoring.
The monitored net-block is the component of the net-block which is allocated to the organization's network, from which internet connectivity is obtained. Packets were logged to disk on the sensor systems using libpcap with appropriate filters, to only log traffic destined to a specific net-block. The sensor's host firewall is configured to prevent any response to incoming traffic being generated, so as to avoid potentially disclosing their presence and passively capturing packets.

5.2 Low Interaction Sensor Node

5.2.1 Drawbacks of Only Passive Blackhole Monitoring Technique: Blackhole Sensor passively collects all UDP and ICMP traffic and gets information in one packet. There is one problem remaining with TCP based threats. UDP is a connectionless protocol so application level data is sent without the receiver ever responding. For example, the Witty worms were based on UDP in which the entire worm payload was transmitted in the first packet so analysis server will encounter the malicious payload. On the other hand, TCP is a connection oriented protocol, no application data is sent until after connection establishment. This has two major repercussions for any TCP based threats; threats to the same port cannot be distinguished from each other, and threats will not send the exploit payload if a connection cannot be established.

5.2.2 Advantages Along with Low Interaction Sensor: To improve the threat detection functionality Blackhole sensor is deployed with the low interaction server component. Low interaction functionality responds to the specific packet request to elicit payload data and the information about the source. In past worms like Blaster worm which first opens a TCP connection to port 135 and sends an RPC bind request. RPC request message is sent containing buffer overflow and code to open backdoor port on TCP port 4444. Then this infected host sends message via backdoor to download the worm payload. This transactions of the Blaster worm is captured by IMS . Low interaction functionality can be provided by changing the firewall rules of the Blackhole sensors to responds to the specific packets requests. We can control level of interactivity by assigning the rules as per requirement.
Advantages:

- Passive Blackhole sensor records all the packets sent to the monitoring block and low interaction component respond to specific TCP request to obtain more information about the source data.
- Blackhole sensor along with low interaction server elicit initial packet from each TCP connection.
- Provides controlled level of interactivity so traffic to the same service can be identified.
- This approach provides the maximum service coverage without the need for maintaining heavy service emulation.
- Gives much probability to identify worm payloads.

5.3 Distributed Mechanism

The Internet worm detection system consists of a set of distributed Blackhole sensors, each monitoring a dedicated range of unused IP address space. Sensors are globally located at different university and corporation or providers. Even if the small address block is monitored by each sensor it has higher probability of observing large scale of malicious events in advance.

6. Proposed Design of Distributed Blackhole Networks

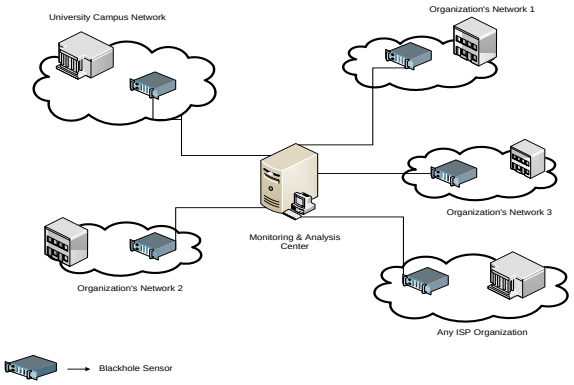

Figure 2 System Architecture for Distributed Blackhole Networks

Fig. 2 shows the sample architecture of proposed design of distributed Blackhole networks to detect worm and other threats beyond the geographical boundary. The main components of the architecture are:

1) Indentified Unused Address Space within Network: Specific predefined net-block is allocated to monitoring server or Blackhole server will fetch list of unused IPs to monitor from the network's DHCP server. Another is statically defined list of the unused IP addresses to Blackhole sensor.

2) Blackhole Sensor [Passive Packet Capture Server]: Blackhole Sensor capture all the traffic received at unused space without responding to any request. It can be placed before the firewall if firewall filtering traffic or it can be placed within the network to enable capturing of inbound traffic destined to unused address space.

3) Blackhole Sensor with Extended Feature of Low interaction Capability: Low interaction provides improved functionality in worm payload capturing with traditional passive capturing. Low interaction Blackhole sensor will elicit malicious payload information by responding to the TCP connection request of worms.

4) Distributed Blackhole Sensor within Different Networks: Distributed Blackhole Sensors in different geographically dispersed networks provides the better visibility into wide spread worms and threats in internet. Large organization having distributed offices in wide area gain useful knowledge about the attacks specifically destined to their organization.

5) Central Monitoring & Analysis Center: The packets captured by the each distributed sensor are stored in log file and these log files are securely forwarded to one central monitoring server. This central Monitoring server will collect all log files and analyze the traffic at each sensor and characterize the result. This functionality provides the single point of interface for monitoring and analysis.

7. Conclusion

The Distributed Blackhole architecture for detecting fast spreading internet worm mainly reflects on capturing, collecting, monitoring and analyzing of traffic destined to dark space. This threat detection technique offers unique advantage in observing large scale events like distributed denial of service (DDoS) or internet worms over traditional security solutions. Central logging facility in proposed system provides single point of interface in monitoring the large scale events. Blackhole Sensors with additional low interactivity functionality with incoming packets is useful for identifying signature of TCP based worm payload. This solution includes further study to identify nature of threats and worms.

8. References

[1] D., Paxson, V., Savage, S., Shannon, C., Staniford, S., andWeaver, N. Moore, "Inside the Slammer worm," *Security & Privacy, IEEE*, vol. 1, no. 4, pp. 33-39, July-August 2003.

[2] (2005, July/August) www.nsrg.eecs.umich.edu. [Online]. http://nsrg.eecs.umich.edu/publications/IEEE_Security_Privacy_Blaster_Final.pdf

[3] D. Moore, and J. Brown C. Shannon, "Code-Red: A Case Study on the Spread and Victims of an Internet," in *Proc. Internet Measurement Workshop (IMW), ACM Press*, 2002, pp. 273–284.

[4] David Moore. (2002) caida.org. [Online]. http://www.caida.org/publications/presentations/2002/usenix_sec/usenix_sec_2002_files/frame.html

[5] Even Cooke, Farnam Jahanian, Joes Nazario, and David Watson Michael Bailey, "The Internet Motion Sensor: A distributed Blackhole Monitoring System," in *Proceedings of Network and Distributed System Security Symposium (NDSS '05)*, San Diego, CA, February 2005.

[6] Team Cymru. (2004) team-cymru.org [online]. http://www.team-cymru.org/Services/darknets.html

[7] M. Bailey, Z. M. Mao, D.Watson, and F. Jahanian E. Cooke, "Toward understanding distributed blackhole placement," in *In Proc of ACM CCS Workshop on Rapid Malcode, ACM Press*, October 2004.

[8] Peter, England, Paul, Peinado, Marcus, and Willman, Bryan Biddle, "The Darknet and the Future Content Distribution ," in *ACM Workshop on Digital Rights Management*, Washington D.C., November 2002.

[9] Yoshiro Fukushima, Yoshiaki Kasahara, Yoshiaki Hori, Kouichi Sakurai Seiichiro Mizoguchi, "Darknet Monitoring on Real-Operated Networks," in *International conference on Broadband, Wireless Computing, Communication and Applications*, 2010.

[10] E. Cooke, F. Jahanian, A. Myrick, and S. Sinha M. Bailey, "Practical Darkent measurement," in *In 40th annual Connference on Information Science and system (CISS)*, Princeton, NJ, 2006, pp. 1496-1501.

[11] Robin Berthier and Michel Cukier, "The Deployment of a Darknet on an Organization-Wide Network: An Empirical Analysis," in *11th IEEE High Assurance Systems Engineering Symposium*, 2008, pp. 59-68.

[12] Elias Bou-Harb, Amine Boukhtouta, Son Dinh, Farkhund Iqbal, Mourad Debbabi Claude Fachkha, "Investigating the Dark Cyberspace: Profiling, Threat-Based Analysis and Correlation," in *7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2012, pp. 1-8.

.