Attack Monitoring and Detection System using Dark IPs

Nikul Jayswal

GTU PG School, Gandhinagar.

Abstract

Information security is a growing concern today for organizations and individuals alike. This has led to growing interest in more aggressive forms of defense to supplement the existing methods. One of these methods involves the use of darknet. A Darknet is a portion of network, a certain routed space of IP Addresses in which there are no active servers o services. I.e., externally no packet should be directed to that address space. Most are the systems are designed for the public internet monitoring. Large or mid-sized organization can also take benefits of the traffic entering on darknets to identify the threats coming on their network. In this paper I have described two major issues in the darknet development and I have proposed method to implement the darknet monitoring system in private network. This is the research work and it is not fully implemented. The implementation of this research work is ongoing.

1. Introduction

With the development of computer network and Internet, network security has become more important issue to the users, private and government organizations, and the defense. As the use of internet is increasing with great ratio, security of the data and information on the network became a major concern. The world is becoming more interconnected by the Internet and as the new networking Technology is introduced. There is a large amount of personal, commercial, military, and government data on networking infrastructures worldwide. The Internet is not free from risks and cybercrime activities in the real world. The valuable information on the internet can be lost, eavesdropped, manipulated or misused and the computer systems can be corrupted.

Today Internet contains so many types of attacks like DDOS (distributed denial of service), viruses, and worms. Viruses and worms are used to infect computers/servers and destroy their data. These threats have many effects on the social and economic activities on the Internet. So we need strong technologies to protecting Internet services from these threats.

In the organizational network environment or the Internet there will be a malicious traffic generated by the malware or the attackers. Network monitoring is one approach to see this type of traffic. If we install a server that collects, analyzes and processes the traffic entering, it would help us to gather more information on the anomalous traffic or malware that may be circulating in the network infrastructure of our organization.

On poplar method for network monitoring is to monitor unused network addresses which can also be called as Dark IPs. Since there is no legitimate host installed in this addresses, traffic sent to such address space is considered to be malicious. Many attackers chose the target randomly. So the infection attempts can be captured by the monitoring the dark ips. Systems that monitors these types of dark address spaces are called darknet sensors, network telescopes or blackholes.

In this paper, I describe the basic issues associated with the darknet. I proposed a method to develop a darknet monitoring system for private networks. The goal of this paper is to provide general information about the darknet monitoring system and idea to develop such system in private organization.

2. Darknet Monitoring

Monitoring packets destined to unused Internet addresses has become an increasingly important measurement technique for detecting and investigating malicious Internet activity. Since there are no legitimate hosts or devices in an unused address block, any observed traffic must be the result of misconfiguration, backscatter from spoofed source addresses, or scanning from worms and other network probing. Systems that monitor unused address space have been called darknets. [1]

In its simplest definition, a darknet is an area of routed IP address space in which no active services reside. [2] While traditionally every client, server, and network device has a unique IP address for each network connection, a darknet is comprised of a range of addresses for which there are no associated valid services or hosts.

What makes a darknet a powerful security tool is that, after initial tuning, any traffic entering it from any source is most likely hostile. In contrast to a traditional network setup, wherein legitimate IP packets are routed to legitimate destination IP addresses and from legitimate source IP addresses, no legitimate packets should be sent to or from a darknet. Although some packets may enter as the result of misconfiguration, the majority are likely sent by malware that scans for vulnerable devices with open ports in order to download, launch, and propagate malicious code.

While darknets are different from traditional IDSs, they use the same type of detection. But with a darknet, we know immediately that any traffic entering is hostile because there are no advertised services in a darknet.
This solves two problems associated with traditional IDSs. [3] First, we don't need to classify the source of data. By design, darknet only monitors traffic and serves no other purpose, so you know any data entering the darknet is hostile. Second, we don't need to inspect the data to know that it's hostile. No one would be probing an empty network space unless he or she was looking for something.

2.1. Basic Problems

Most are the systems are designed for the public internet monitoring. Large or mid-sized organization can also take benefits of the traffic entering on darknets to identify the threats coming on their network. By definition, the dark IPs does not send ant packet or sent any packet. If the dark IP receive any packet than it should not be replied in any way. In the sense, darknet should not send any tcp or udp packets on the network.
After the study of the current darknet scenario we can identify the two major issues related to the darknet: Preparing the IP address spaces for monitoring and Design of algorithm to identify the attack on network.

2.2. Related Work

Michael Bailey et al describe and analyze the important measurement factors associated with the deployment of the darknet. [4] Since a darknet monitor observes traffic to unused addresses, the upstream router must be instructed to forward undeliverable packets to the monitor. They proposed approach to configure the upstream router to statically route an entire address block to the monitor server.

Seiichro Mizoguchi et al presented the result of real operated network monitoring. [5] They setup monitoring servers with several configuration and monitor darknet traffic on production network and analyze the data obtained by each sensor. For the dark IP address space they used the DHCP server installed on real operated network. On the live organizational network, mainly a DHCP service is used to manage IP addresses for production computers. If a computer is connected to the network, DHCP server will automatically assign an IP address to it. Several IP addresses are assigned for the DHCP service. So, there may be many unused addresses which are not assigned, means unused.

2.3. Public Projects

One of the easiest ways for organizations to reap the benefits of a darknet is to participate in any one of a number of public darknet projects. There are several projects developed to monitor public dark ips by security organizations and universities.

2.3.1 Internet Motion Sensor: (ims.eecs.umich.edu)

Internet Motion Sensor (IMS) is the globally deployed distributed darknet monitoring system. The servers of the IMS are deployed in various ISP networks, major service providers, large enterprise networks and academic networks. There are total 18 such organizations and 60 darknet blocks which monitors 17 million IP addresses which represents 1.25% of all routed IPv4 address space.

2.3.2The Darknet Mesh Project: (projects.oucs.ox.ac.uk/darknet/)

The Darknet Mesh Project is a collaborative project between the Network Security Team at OUCS (Oxford University Computing Services), and other security teams at UK universities to produce a collaborative means to detect and report on traffic hitting a collection of darknets. Participants within a darknet mesh must register, their address space in CIDR notation, and an alert email address. This data is then fetched by each participant within the mesh to determine what addresses should be monitored by the darknet code. Once installed and configured, the script monitors for traffic from participating

organizations, collects flows flowing to the darknet and emails the appropriate administrator for the network.

2.4. Private Darknet [2]

Mid-sized to large organizations can also benefit from implementing their own private darknet. The greater the number of users is in an enterprise, the more devices administrators have to manage, and the greater the need is for safer, faster, and more reliable network traffic analysis. With a private darknet, organizations can quickly differentiate between legitimate and malicious traffic on their networks.

However, before organizations invest in a private darknet, they must have a proven test environment in place. Once space is allocated in this test environment, the organization can distribute known bad traffic to ensure it reaches the darknet test environment and that security administrators understand what to do with that data.

When the test period is complete, the organization can then identify the unused network space to be allocated to the darknet, monitor it for a period of time to ensure it is not being used, then, if necessary, implement network changes to make sure no legitimate traffic is routed to that space. A collector must also be set up within the darknet that captures any traffic that enter.

3. Monitoring System

Most are the systems are designed for the public internet monitoring. Large or mid-sized organization can also take benefits of the traffic entering on darknets to identify the threats coming on their network. By definition, the dark IPs does not send any packet. If the dark IP receive any packet than it should not be replied in any way. In the sense, darknet should not generate any tcp or udp packets on the network.

In most of the systems which we have studied earlier proposed to prepare the IP address space for monitoring and then monitor the traffic on dark IPs. If we allocate a whole subnet for monitoring [4], we need large IP address space which is not feasible in mid-sized organization and the IP address blacklisting problem may be arise. Attackers may detect the dark IPs based on the no reply strategy. If we use some another system to detect the dark IPs like, using DHCP server [5], the monitoring server should be communicate with the DHCP server, which is against the default definition of the darknet (never generate tcp/udp packets). And also we have to be dependent on the DHCP server.

For the configuration of the monitoring server, most of the proposed system make the decision of the malicious traffic based on the fail connection maid with the darknet. The main goal of the darknet is less false positive and false negative compared to the traditional IDS / IPS.

3.1. Preparing Dark IP for Monitoring

After studying the limitation of existing system, I proposed a totally independent monitoring system which is not rely on any legitimate system on the network.

- Monitoring system itself prepares the dark IPs presented on the network and monitors the traffic entering on the darknet.
- No need to communicate with the other machines on the network, so it will not generate any tcp or udp packets.
- Monitoring server will be placed in the same intranet where all other systems are placed.
- Monitoring server will receive the packets based on the mac address traffic, so it can also monitor the traffic coming from the internet and traffic coming from the internal network also.

Real time identification of the dark IPs can be done based on the arp requests for the particular IP address. If the machine is up, machine will immediately replies for the arp request, if machine is down, that means the dark ip, the reply of arp request never responded.

Whenever packet arrives in the network from internet, or internal network it need mac address to deliver a packet to the system successfully. For that purpose, if the packet is for dark ip, the arp request for that ip never responded. If the machine is live host, that particular machine will respond to the arp request.

After the some number of arp request, if the respond is not sent than we can guess that this is the packet for dark IP and host is not alive, so monitoring server will respond that arp request by configure for itself the ip address for that APR request. If monitoring server itself configure that dark ip address for that request, the traffic for that ip will be directed to the monitoring server. For ARP request, Server should not manually reply that request, just configure the IP address to monitoring server. In all new OS, we can give as much IP addresses as we want (Create allies).

The main advantage of this system is we need not to create any IP address space for monitoring and it is totally independent and does not rely on any legitimate system.

3.2. Monitoring Server Configuration

By definition darknet do not receive any user or legitimate traffic. Robin Berthier and Michel Cukier divided the traffic possibly received by darknet into three categories: [6]

- Misconfiguration traffic: When a source is trying to establish a connection with a destination incorrectly which may be unused IP.
- Backscatter Traffic: When the victim of a Dos attack is trying to reply to a spoofed network address.
- Malicious Traffic: When an attacker is trying attack on the network or particular host.

They further divide the last category into:

- Random Attack: When an attacker tries to discover the vulnerable host on the network by using scanning techniques.
- Targeted Attack: When an attacker has knowledge of the location of a specific network resource to compromise. In this situation the attacker does not usually need to scan multiple network addresses to find it.

3.2.1 Random Attack

In Random attack, the attacker perform the activity on set of destination ip addresses. It will communicate with several machines in the network in particular time period. Attacker usually perform scanning to identify the vulnerable hosts in the network.

Robin Berthier et al. [6] proposed a method to divide the darknet traffic for random attack:

- Misconfiguration Traffic: Packets with SYN flag on with less than N destination address per hour.
- Malicious Traffic: Packets with SYN flag on with more than N destination address per hour.
- Backscatter: Packets with Other flag combination with more than N destination address per hour.

3.2.2 Targeted Attack

In targeted attack, the attacker perform activity on particular machine or address. He or she will try to communicate with the particular machine and sends number of packets on particular machine. I proposed a method which will help to divide the darknet traffic. Usually attacker has a knowledge of the existing system and does not perform scanning.

- Misconfiguration: Packets with SYN flag on and less than M packets per minute.
- Malicious Traffic: Packets with SYN flag on and more than M packets per minute.
- Backscatter Traffic: Packets with other flag combination and more than M packets per minute.

3.2.2 Combined Method

To divide the darknet traffic for both random attack and targeted attack, we can combine both the above filter. Now the combined filter will be:

- Misconfiguration: Packets with SYN flag with less than N destination per source per hour and less than M packets per destination per minute.
- Malicious Traffic: Packets with SYN flag with more than N destination per hour and more than M packets per destination per minute.
- Backscatter: Packets with other flag combination with more than N destination per hour and more than M packets per destination per minute.

Apart from filtering the packets, we can add IDS/IPS on dark IPs which will take care of known signatures and attack patterns to identify attacks and threats.

4. Some Good Practices

For efficient result if it is possible than don't assign first and last ips from network range to any legitimate machines. Attacker mostly scans whole network like 192.168.100.0/24. If the first ips will be dark than the monitor server detect the attack first and prevent the scanning. Moreover, in most IT environment, the servers and gateways have last ips from the range. If we do not use last ips than the monitoring server may prevent the network from the targeted attack.

5. Conclusion

The information produced by a darknet can be used with existing network security technologies to provide more intelligence in security, and protecting clients inside a network. This paper describes the method which can be used to develop a darknet monitoring system to monitor the attacks on the private organization. The proposed system is totally independent and can be used to detect the external threats as well as internal threats. It does not required new configuration, it can work effectively in existing setup.

6. References

[1] The Darknet Project- Team Cymru: www.teamcymru.org/Services/darknets.html

[2] Michael Smith – Symantech Global Services : " Darknet : Security's Bright Future." www.infosectoday.com/Articles/Darknets.html

[3] Jonathan Yarden: "Learn how darknets can serve as an early warning detection system for network threats." on November 18, 2005. www.techrepublic.com/Articles

[4] Michael Bailey, Evan Cooke, Farnam Jahanian, Andrew Myrick, Sushant Sinha: "Practical Darknet Measurement". *In 2006 40th Annual conference on Information Science and Systems. IEEE Published Year 2006s, Pages: 1496-1501*

[5] Seiichro Mizoguchi, Yoshiro Fukushima, Yoshiaki Kasahara, Yoshiaki Hori, Kouicjhi Sakurai : "Darknet Monitoring on Real Operated Networks." *In 2010 International Conference on Broadband, Wireless Computing, Communication and Application. IEEE Published Year: 2012, Pages: 278-285*

[6] Robin Berthier and Michel Cukier: "The Deployment of a darknet on an organization wide network: An Empirical Analysis." *In 2008 11th IEEE High Assurance Systems Engineering Symposium. IEEE Published Year:2008, Pages : 59-68*

[7] Masashi Eto, Daisuke Inoue, Mio Suzuki and Koji Nakao: "Multipurpose Network Monitoring Platform using Dynamic Address Assignment." In 2012 Seventh Asia Joint Conference on Information Security. IEEE Published Year: 2012, Pages: 79-84

[8] David Moore, Colleen Shannon, Geoffrey M. Voelker, and Stefan Savage. "Network telescopes: Technical report." Department of Computer Science and Engineering, University of California, San Diego, 2004.

[9] Akihiro Shimoda, Shigeke Goto. "Virtual Dark IP for Internet Threat Detection." In APAN Network Research Workshop 2007. Pages: 44-51

[10] [9] Claude Fackkha, Elias Bou-Harb, Amine Boukhtouta, Son Dinh, Farkhund Iqbal, Mourad Debbabi. "Investigating the Dark Cyberspace: Profiling, Threat based Analysis and Correlation." In 2012 7th International Conference on Risks and Security of Internet and Systems. IEEE Published Year: 2012, Pages: 1-8

[11] Barry Irwin: "A Baseline study of potentially malicious activities across five network telescopes." In 2013 5th International conference on cyber conflicts. IEEE Published Year: 2013, Pages: 1-17