INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

PREVENTION FROM A DISTRIBUTED DENIEL-OF-SERVICE (DDOS) ATTACK BY USING DNS FEATURES SET.

MOHAMMAD TARIQUE MOHAMMAD SALEEM[1], BRAVIM J. JOREWAR[2]

1. M.E. (Computer Science And Engineering) R.S.C.E., Buldhana.
2. Dept. of computer sci. &engg, Prof. R. S. C. E., Buldhana.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. In a typical DDoS attack, the assailant begins by exploiting a vulnerability in one computer system and making it the DDoS master. The attack master, also known as the botmaster, identifies and identifies and infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified target.

Keywords: DDoS Scrubbing, Zombie, Botnet, FFSN

Corresponding Author: MR. MOHAMMAD TARIQUE MOHAMMAD SALEEM

Access Online On:

www.ijpret.com

How to Cite This Article:

Mohammad Tarique Mohd. Saleem, IJPRET, 2015; Volume 3 (9): 754-759

PAPER-QR CODE

INTRODUCTION

In this work we will study the network security from DDoS as we know that there is a fast flux network that a cybercrime can use to hide their identity by abusing the way domain name system works. So for the same purpose first we have to determine the above mentioned network and after all prevents from such network in this paper we will study the determination of such network which affects the network security. Fast flux DNS takes advantage of the way load balancing is built into the domain name system. DNS allows an administrator to register a number of IP addresses with a single hostname. The alternate addresses are legitimately used to distribute Internet traffic among multiple servers. Typically, the IP addresses associated with a host domain do not change very often, if at all.

The work presented here is related to the prevention of network from various criminals using botnet or DDoS by determining FFSNs, in particular, by jointly building timing, domain name, spatial, network and DNS answer features which are extracted from the first DNS response packet. We consider many rather than a few features and also their combinations which are constructed by surveying the recent literature. The main aim of this survey is to study and analyze the benefits of the features and also, in some cases, the necessity of applying joint feature subsets. We provide an overview of the various feature subsets to be used for classification. We illustrate them by highlighting the efforts done by the authors in developing novel procedures, and analyze them in terms of their discrimination power.

In this paper, the detection of DDoS attack is purely based on the DNS request and the corresponding response packets collected from a recursive DNS server. Unlike recent FFSN detection proposals, our objective is to build a feature pool which may increase the detection of FFSNs. Some of the features require additional operations such as WHOIS messages, IP Coordinate Database, and a list of ground-truth labeled benign domain names. These operations add an additional delay to the detection, however, do not consider consecutive DNS lookups that take TTL value of each domain into account or take several minutes/hours to collect.

Materials and Methods:

DNS security threats:

Foot printing: is the process by which DNS zone data is obtained by an attacker to provide the attacker with the DNS domain names, computer names, and IP addresses for sensitive network resources. An attacker commonly begins an attack by using this DNS data to diagram, or

footprint, a network. DNS domain and computer names usually indicate the function or location of a domain or computer in order to help users remember and identify domains and computers more easily. An attacker takes advantage of the same DNS principle to learn the function or location of domains and computers in the network.

Denial-of-service attack is when an attacker attempts to deny the availability of network services by flooding one or more DNS servers in the network with recursive queries. As a DNS server is flooded with queries, its CPU usage will eventually reach its maximum and the DNS Server service will become unavailable. Without a fully operating DNS server on the network, network services that use DNS will become unavailable to network users.

Data modification is an attempt by an attacker (that has foot printed a network using DNS) to use valid IP addresses in IP packets the attacker has created, thereby giving these packets the appearance of coming from a valid IP address in the network. This is commonly called IP spoofing. With a valid IP address (an IP address within the IP address range of a subnet), the attacker can gain access to the network and destroy data or conduct other attacks.

Redirection is when an attacker is able to redirect queries for DNS names to servers under the control of the attacker. One method of redirection involves the attempt to pollute the DNS cache of a DNS server with erroneous DNS data that may direct future queries to servers under the control of the attacker. For example, if a query were originally made for example.microsoft.com and a referral answer provided a record for a name outside of the microsoft.com domain, such as malicious-user.com, then the DNS server would use the cached data for malicious-user.com to resolve a query for that name. Redirection can be accomplished whenever an attacker has writable access to DNS data, such as with insecure dynamic updates.

RESULT AND DISCUSSION:

With regards to scrubbing-lane approaches, years ago Internet Service Providers (ISP) realized, “Yes DDoS is a problem we will have to deal with now and in the future”. From some reports as early as the year 2000 ISPs began observing DDoS attacks traversing their networks. How did they see the effects of DDoS attacks – way back then?

Simple, they had already begun to deploy vast amounts of network infrastructure that supported NetFlow. From their infrastructure NetFlow records were obtained and forwarded to NetFlow Collectors. Running an analysis application using the NetFlow records, network engineers and technicians could view, monitor, report, trend, and alert based upon statistics that were collected from their infrastructures. They would detect points of congestion in their

networks and make tertiary changes to the backbone to reduce and eliminate bottlenecks. They still use the same techniques today.

Searching for a Solution

As traffic fluctuations related to ongoing DDoS attacks became more commonplace; ISPs began searching for a solution to remove DDoS traffic from their networks. However, the options were limited and did not completely eliminate the problem. Instead of enabling the removal of DDoS traffic at the boarders (peer points) of their networks, the concept of "scrubbing" the DDoS traffic within their networks with the sole intention of eliminating the attack from affecting their downstream customers and their SLAs was born.

In other words ISPs accept the DDoS traffic from their peers and forward the DDoS traffic through their networks. Then, using BGP they would reroute all the traffic destined to the attack victim, through what is called a "scrubbing-lane". The scrubbing-lane was intended to filter the DDoS traffic out from the traffic flow while allowing good traffic to be forwarded to its destination.

Ongoing challenge:

This approach requires the usage of BGP route injection techniques and the GRE Tunnel approach; which is viewed as cumbersome and somewhat inefficient, requiring human intervention for BGP route injections and often blocks as much good user traffic as bad, DDoS traffic. If the deployed technology used to scrub traffic worked somewhat well in a scrubbing-lane approach, why wasn't the technology deployed at ISP peer points or other strategic points in the network subsequently blocking the attack before they get in?

Simple – deploying a scrubbing-lane approach at the peer points will block just as much good traffic as bad; downstream customers would lose their legitimate user traffic in the process. ISPs that have commonly deployed the NetFlow/scrubbing-lane approach are still struggling with its inefficiencies and coming to realize that the scrubbing-lane approach doesn't necessarily scale economically when we're talking about scrubbing 40Gbps, 100Gbps or more of DDoS attack traffic.

Re-thinking DDoS protection in the ISP environment:

Traditional on-demand and scrubbing-lane approaches can be replaced with real-time, inline defenses that eliminate the DDoS threat for providers and their customers. Corero First Line of

Defense solutions provide always on DDoS protection, event reporting and analytics for Service providers that are looking for alternatives in defeating the DDoS challenge.

Corero SmartWall® Threat Defense System transparently blocks DDoS attack traffic before it enters-or-traverses the ISPs network. ISPs are taking advantage of the SmartWall® Threat Defense System and are now enabled to defeat DDoS attacks in real-time; before their customers are even aware an attack has taken place—allowing the good user traffic to flow unimpeded to its destination. This purpose built DDoS defense technology provides carrier class protection, and unlimited scalability for even the most robust provider networks. The secret: No false positives. The SmartWall 'Do No Harm' architecture, scales to virtually any bandwidth in increments of 10Gbps, removes all unwanted DDoS attack traffic, all without dropping legitimate traffic. Of course, for those ISPs that are still committed to using scrubbing lanes, SmartWall provides an excellent solution here as well.

CONCLUSION:

Security is a very difficult topic. Everyone has a different idea of what ``security'' is, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your organization. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

Many people pay great amounts of lip service to security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know why what's been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

REFERENCES:

1. B. Daya, "Network Security: History, Importance, and Future", University of Florida Department of Electrical and Computer Engineering, 2013.

2. Li CHEN, Web Security: Theory and Applications, School of Software, Sun Yat-sen University, China.

3. J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.

4. A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.

5. S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009.

6. M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.

7. R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.

8. Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.

9. M. A. Shibli, "MagicNET: Human Immune System & Network Security," IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No.1, January2009.

10. M. Silva, "Virtual Forensics: Social Network Security Solutions," Proceedings of Student Research Day, CSIS, Pace University, 2009.

11. R. K. Khalil, "A Study of Network Security Systems," IJCSNS International Journal of Computer Science and Network Security, 2010.

12. S. Alabady, "Design and Implementation of a Network Security," Technology,Vol. 1, p. 11, 2009.

13. B. Preneel, "Cryptography for Network Security," Katholieke Universiteit Leuven and IBBT, 2009.

14. M. Kassim, "An Analysis on Bandwidth Utilization and Traffic Pattern," IACSIT Press, 2011.

15. M. Eian, "Fragility of the Robust Security Network: 80211," Norwegian University of Science and Technology 2011.