Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 2): pp. 2498-2509
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.02.266

Defending Distributed Denial Of Service (Ddos) Attacks: Classification And Art

Abhishek Jain Department of Computer Applications, Graphic Era Hill University, Dehradun, India Doon. abhishek@gmail.com

Anupriya Sharma Ghai Department of Computer Applications, Graphic Era Hill University, Dehradun, India.

Divya Kapil Department of Computer Applications, Graphic Era Hill University, Dehradun, India.

Atika Gupta Department of Computer Applications, Graphic Era Hill University, Dehradun, India.

Bijesh Dhyani Department of Management, Graphic Era Hill University, Dehradun, India.

Aditya Pai H Associate Professor, Graphic Era (Deemed to be university)

Abstract–There are a lot of companies operating its online businesses including e-commerce, e-banking, financial services, and other web-based services using the Internet. With the enormous increase in the number of hosts, it becomes challenging to provide the resources to legitimate users and to protect the resources from attackers. The multiple loopholes of the Internet are being used for Distributed Denial of Service Attacks by the attackers. DDoS prevention measures quickly become obsolete. Attack planners upgrade their tools to circumvent these security systems, and security professionals modify their strategies to handle ever changing new attacks. This paper describes the problem of DDoS attacks, the evolution of DDoS attacks, and what kinds of DDoS attacks may occur in the near future, and what protection mechanisms can be used against these attacks. This will provide a clear understanding of the DDoS attack problem and also valuable guidance for future research.

Keywords- Network, Security, Distributed Denial of Service, DoS, DDoS, Vulnerabilities

1. INTRODUCTION

The Internet is becoming an important component for all types of organizations, don't depend how large or small they may be. All global businesses, other non-profit organizations, government agencies have made huge investments in creating web infrastructure (i.e. hosting web sites, Internet-enabled applications, etc) to have a competitive edge in capturing the market or to help them communicate effectively with their counterparts. The increase in the number of users and reliance upon these web based applications makes them a good and soft target for attackers who wish to harm their business or to leak country secrets intentionally. The relative ease and low costs of launching such attacks have made them one of the most serious threats to the Internet users. By executing a Denial of Service (DoS) attack on an Internet-enabled application, the attackers can force it to freeze and make it unavailable or ineffective.

This paper will describe the history of Denial of Service (DoS) attacks, how Distributed Denial of Service Attacks (DDoS) evolve, the differences in DoS and DDoS attacks and the increasing usage of DDoS attacks to cripple the victim. It will then describe different types of DDoS attacks that occur everyday and some well known tools used to carry out these attacks. It will also brief the issues regarding increase in application layer DDoS attacks. Finally, a review of existing defense mechanisms against DDoS attacks and the scope of future research are discussed.

2. HISTORY OF DENIAL OF SERVICE ATTACKS

Denial of Service (DoS) describes a broad range of attacks where an attacker intentionally disables a computer system, an application, or damage network. Some common methods for causing a DoS attack include flooding the target system with intentional malicious network traffic or crafting some network packets to exploit the vulnerabilities in target operating system or applications (logical attacks). Distributed Denial of Service , or DDoS is an evolved form of DoS that carries out a coordinated Denial of Service attack from a group of agent machines known as Zombies or slaves against a target system. Such attacks usually also cause collateral damage, e.g. causing high packet loss or even virtually detaching certain networks from the Internet.

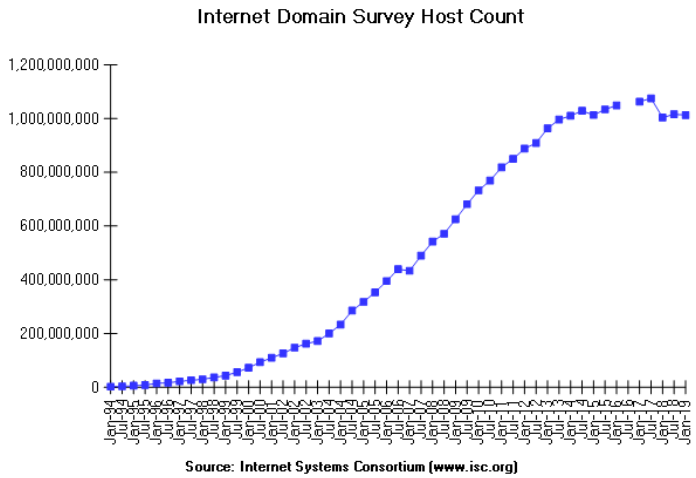

Figure 1. Internet Domain Survey Host Count

The first DoS attacks occurred in the 1990s, when one user would attack another user, usually for revenge or other personal reason [1]. These attacks were usually directed from one single computer at another computer. During this time, software tools were created that enabled users to launch DoS attacks without having to possess in-depth knowledge of how the attacks worked.

Trinoo, a Trojan software application is a attack tool used to start denial of service attacks through multiple sources. Trinoo and others like it would infect computer systems and had the ability to spread automatically in order to enlist an army of machines for the purposes of carrying out DDoS attacks. These trojan programs were often spread through email attachments that an unsuspecting user would run or through vulnerabilities in the operating system.

Once a computer system became infected, it would then communicate back to a central controller and wait for commands that would be issued using Internet Relay Chat (IRC). The collection of compromised systems under the control of a central commander became known as a botnet, named after the term "bot", which is used to describe a program that waits in a chat room and can communicate with users on IRC.

The increasing number of computers infected and participating in various botnets made the way for Distributed Denial of Service attacks. In February of 2000, DDoS attacks became mainstream news when CNN, Yahoo!, E*Trade, and popular ecommerce websites eBay, Amazon, and Buy.com were shut down by DDoS attacks [3].

In 2004, criminal groups began building and using their own botnets for economic gain. Often, these botnets were being offered for hire to attack a company's competitor. Some botnets server a dual-purpose, sending out spam email when they are not being used to commit DDoS attacks. Other criminal groups have used the botnets in an attempt to extort money from online businesses. An example of such an extortion took place in 2005 when an unidentified source demanded money from a UK online gambling website or else they would launch a DDoS attack on them, causing them to lose out on business during an upcoming popular sporting event [5].

In recent years, DDoS attacks have again garnered the attention of the news media, this time for the alleged state-sponsored attacks against another nation's technology infrastructure. In May of 2007, Estonia accused Russia of using DDoS attacks in retaliation to the removal of a Russian Statue from one of the former Soviet Republic's cities [6]. Russia denied any involvement in the attacks, but this attack, lasting several weeks and enlisting a botnet of unprecedented size, illustrated the effectiveness with which an attack could be carried out against a nation for political purposes. In September of 2008, DDoS was again used for political purposes when Myanmar used DDoS attacks to cripple dissident websites, and when Russia allegedly used DDoS attacks against Georgian web sites in coordination with its military action in that country.

These are just some of the high profile attacks that have taken place over the past decade, but there are many more that go unreported. This is especially problematic for financial companies whose customers rely on being able to access their services at any time. The attacks are increasing in volume , frequency, complex day by day.

3. TYPES OF DDOS ATTACKS

The different methods of carrying out a DDoS attack are in abundance each having an edge over other and they continue to evolve as new defensive measures are put in proper shape. In 2004 Mirkovic and Reiher[1] classified the DDOS attacks. They identified an extensive taxonomy based on factors including the degree of automation, how the network agents propagate, what kind of weakness it exploits, whether it spoofs the IP address of the attacking machines, the rate of attack, whether it is filterable or unfilterable based on packet characteristics, and the impact on the victim. For the purposes of this paper, DDoS attacks will simply be categorized by the layer at which they operating in the OSI Network Model. DDoS attacks have exploited the Network layer, Transport layer, and more recently, the Application layer vulnerabilities.

3.1 Network/Transport Layer DDoS Attacks

Network and Transport Layer DDoS Attacks exploit vulnerabilities in network protocols to flood the victim and the victim's network with traffic.

3.1.1 TCP SYN Flood Attack

Discovered early in 1994[8], It is one of the initial instance of a DoS attack. In this attack, the attacker issues a series of TCP SYN packets to the victim with a spoofed source IP Address. With multiple SYN-ACK replies outstanding, eventually the server's resources are consumed and it will be unable to respond to legitimate application requests [9].

One relatively simple solution to minimize the impact of this type of attack is to configure routers to verify the source IP address before forwarding packets in order to prevent IP spoofing. Other solutions involve tuning the TCP/IP stack on the victim's operating system to reduce the amount of time the victim will wait for the ACK, or allowing it to stop waiting for old unanswered ACK replies if the resources become depleted. Yet another solution involves the use of SYN Cookies, which take an entirely different approach that does not keep connections open while waiting for the ACK reply [10].

3.1.2 Smurf IP Attack

In a Smurf IP Attack, named after a tool that can be used to conduct the attack, the attacker sends modified ICMP Echo requests to the broadcast IP address (for example, 10.255.255.255 for a Class A internal network 10.0.0.0) using the intended victim's IP address as the source in the modified request [12]. In this attack, the machines flooding the victim are not under the direct control of the attacker, but are third parties that are simply replying to an ICMP request that happens to have a forged source IP address.

One solution to the Smurf IP Attack is to configure routers to block IP broadcasts, since usually they do not need to be routed [11]. As is the case with many DDoS attacks, it is difficult for the victim alone to take protective steps. It requires the cooperative securing of multiple systems and network equipment.

3.1.3 Echo/Chargen UDP Flood Attack

The Echo/Chargen UDP Flood attack "connects" network services from two victim machines, one that produces output (such as the chargen service, RFC864) with another that consumes the output and responds (such as the echo service).

Preventing an Echo/Chargen or other similar UDP Flood attack can be done by disabling the echo and chargen services and filtering echo and chargen UDP traffic within the network [12]. Because this type of attack is not limited to just the echo or chargen services, it is a good idea to disable and filter any unused UDP service.

3.1.4 Ping of Death Attack

In this attack, the attacker build a ping request with a size bigger than what is permissible by the design [13]. If the victim's system does not protect against this, it could result in a buffer overflow, eventually overwriting memory used by the operating system or other applications and causing the system to crash

The Ping of Death and other similar attacks occur in the network and transport layers, but exploit vulnerabilities in the software implementation instead of in the protocols themselves. The vulnerabilities that allow these attacks have been fixed in more recent versions of operating systems, but it is an example of how poorly designed or developed software can expose vulnerabilities that allow an attacker to take an entire system down.

3.1.5: Teardrop Attack

It take advantage of the shortcomings in the reassembling of network data packets. It involves sending useless or empty IP fragments with oversized, payloads to the target system which causes the fragmentation to be indecently handled and forces it to collide, suspend, or reboot. Most up to date releases of operating systems include fixes for the Teardrop denial of service attack and its variants.

3.2 Application Layer DDoS Attacks

As security software and hardware vendors have become more adept at preventing traditional DDoS attacks, attackers have devised more complex and harder to protect against methods to disabling remote systems. Here are some types of Common DDoS Attacks at Application Layer [16]

3.2.1 Repeated One-Shot Attacks

3.2.2 Asymmetric Attacks

3.2.3 Application-Exploit Attacks

3.2.4 Request-Flooding Attacks

An example of an application layer attack is one that overloads a website by simulating actual usage of the website. For example, consider an e-commerce website that offers its clients a searchable product catalog. An attacker might examine the HTML of the website to determine how to directly query the product catalog search web page and when use a program to repeatedly issue random product search requests. If the attacker uses a botnet to enlist the help of many infected agent machines, this attack can be devastating to the victim's website, causing it to run very slow or even become completely unavailable. For a large e-commerce website, this could result in millions of dollars in lost sales.

4. DDOS ATTACK TOOLS

In order to carry out DDoS attacks on a large scale, software tools have been created to make it simple for the attacker to control the infected botnets. There are four popular tools that have been widely used: Stacheldraht , Trinoo, TFN2K, and Tribe Flood Network (TFN). Other DDoS applications may also be in use but not widely available or discovered yet. The following subsections describe the operation and capabilities of the four main DDoS applications.

4.1 Trinoo

Trinoo, also known as Trin00, is a DDoS attack tool that was released in 1999 and can run on Windows or UNIX platforms [4]. It uses a combination of TCP and UDP packets for communication. It only supports carrying out UDP Flood attacks.

4.2 Tribe Flood Network (TFN)

TFN, is a tool used to start on synchronized denial of service attacks from a lot of sources against one or more targets. There are also more types of attacks available in TFN than in Trinoo, with the attacker being able to choose from TCP SYN, UDP Flood, Ping of Death, or Smurf IP attacks.

4.3 TFN2K

TFN2K is a new version of the original TFN attack tool [17]. It adds the ability to communicate using TCP, UDP, or ICMP ECHOREPLY, and even the ability to randomly switch between the three methods in order to evade filtering mechanisms. It also allows the attacker to kick off multiple types of DDoS attacks together. These changes represent another evolutionary step in DDoS attack tools to make them more potent and more difficult to detect or prevent.

4.4 Stacheldraht

Stacheldraht is yet another DDoS attack tool that is based on the source code of the original TFN tool and combines features of Trinoo and TFN [18]. Like the others, it also has a client and daemon component design that relies on infected machines to carry out the attacks. Stacheldraht, however, uses an encrypted “telnet-like” interface for the attacker to control the client application, making it more difficult for network administrators to detect or monitor.

5. DEFENDING AGAINST DDOS ATTACKS

Defending against DDoS attacks is challenging because it requires the cooperation of many different parties. Businesses, end users, operating system developers, network equipment manufacturers, internet service providers, law enforcement, and government officials must work in conjunction to deal effectively with the danger of DDoS attacks. Same is the case of infected agent machines that carry out DDoS attacks as members of a botnet. The individual owners of these machines may not experience any noticeable l effect from their machines participating in carrying out a DDoS attack,

but they certainly could have taken measures that would have prevented their participation.

5.1 Business Organizations

Businesses may be the victims of DDoS attacks, so they have a high incentive to protect themselves from attacks. Businesses should make sure that firewalls and routers are configured to filter out unnecessary traffic and prevent the forwarding of broadcast packets or packets with spoofed IP addresses. System administrators should also work to turn off any unused services and features on servers and apply the latest security patches from operating system and network equipment vendors. Business application developers who are developing programs that will run on a web server should be careful not to expose performance-costly operations to external users who have not logged into the system.

Businesses that have critical network applications should also implement redundant network configurations and keep a "Stand by" that can be switched over to in case of a DDoS attack. By having a contingency plan in place before an attack occurs. It can help to minimize the downtime and cost of a DDoS attack.

Because businesses have a large number of computers and always-on high speed connections to the Internet, their systems can also be participating in carrying out DDoS attacks if they are infected with DDoS malicious scripts. It is important for businesses to protect themselves by making sure that antivirus software is installed on all systems, the most recent security patches have been applied, spam filtering is performed on the mail server, and users are educated about the dangers of opening suspicious looking email attachments.

5.2 Operating System and Application Developers

Vulnerabilities in operating systems often enable attackers to control or carry out DDoS attacks. Therefore Operating System Developers have the ability to improve the overall protection from DDoS attacks by securing the operating system software. Open software operating systems, such as Linux, benefit from having a community of users examining the code for vulnerabilities and quickly fixing security holes. Others, such as Microsoft, who does not make their source code publicly available, chose to tackle security by instituting corporate initiatives such as the Trustworthy Computing Initiative and Security Development Lifecycle [19]. These initiatives have worked to address concerns that their customers had with the high number of successful attacks that occurred against their operating system. They strongly advocated building security into the operating system and other applications during the design phase and making it easier for the customer to choose a more secure configuration by default instead of having an insecure configuration as the default after installing it.

Application developers who write software that is connected to the Internet also should take measures to avoid vulnerabilities. Many Denial of Service attacks take advantage of a flaw in how an application was designed or developed, so it is important to include DoS security early on in the design of an application, and throughout the lifecycle through code reviews and testing [20].

5.3 Network Equipment Manufacturers

Firewall and router equipment manufacturers have taken steps to allow their equipment to better prevent DDoS attacks. Since these pieces of hardware sit at the nodes between networks, they are an ideal place to filter out DDoS traffic. Features on routers, such as the unicast reverse path verification feature, prevent the forwarding of packets that have a spoofed source address, which are used to carry out some forms of DDoS attacks [21]. Other features such as limiting the rate of TCP SYN packets and limiting the rate of ICMP packets can reduce the potential of a network or transport later DDoS attacks. However, because networking equipment does not have specific knowledge of the applications running behind it, it cannot effectively prevent application layer DDoS attacks.

Besides adding DDoS defense features into routers and firewalls, many networking equipment vendors offer dedicated DDoS protection devices that can be added to a network to detect and defend against DDoS attacks. These devices work by analyzing network traffic under normal conditions so they can detect when an attack has occurred, and if detected, diverting traffic for inspection in order to filter out the attacker traffic from legitimate traffic [22].

5.4 End Users

End users are far less likely to be the target of a DDoS attack, but like businesses, they face the possibility of their PC becoming infected by a botnet application. It is important for end users to make sure they have antivirus software installed, that they apply the latest operating system updates, and do not open suspicious looking attachments. There is no known defense against a DOS attack other than having the router auto ignore requests from certain IP ranges, which of course the router would have to process by checking incoming requests against that list, which would eat some of it's processor, which a sufficient attacking force can cause lag through which makes the DOS attack successful in the end anyway.

5.5 Law Enforcement Agencies and Government Support

The investigation of computer crimes is still a relatively new area of concern for law enforcement officials. Improving the ability to find and prosecute criminals who carry out DDoS attacks may help reduce the number of attacks that occur. In recent years, law enforcement agencies have created specialized task forces such as the FBI's cyber division which was formed to investigate computer related crimes, including DDoS attacks. The amendments in law should be done to set the punishments for the guilty depending on the degree of the offence. Government officials must continue to enact new legislation and adapt current legislation to protect businesses and people from computer-related crimes.

6. AREAS FOR FURTHER RESEARCH

The evolution of DDoS attacks has been from lower layers of the OSI Network Model to the upper layer, the Application Layer. Researchers and security professionals have been working to come up with ways to understand the context of the network traffic in order to determine whether it is a DDoS attack or legitimate and block or allow it accordingly. The increased use of web services, web based applications and Service Oriented Architecture (SOA) [23] designs present yet another potential vulnerability that needs to be exploited**.** Still more potential exists to disrupt applications such as Voice over Internet Protocol (VoIP), streaming media via DDoS attacks.

7. CONCLUSION

Distributed Denial of Service attacks are increasingly becoming a powerful weapon to disrupt the commercial activities and communications of people, businesses, and governments. The IT Security Industry has been in a race to keep up with the evolution of DDoS attacks, and there are steps that all of the involved parties must take in order to protect each other from the effects of these attacks. In the end, the following of secure practices in all phases of Development from the software developers and hardware designers to the system administrators and end users, will be what protects the Internet from the threat of Distributed Denial of Service attacks.

8. REFERENCES

[1] Mirkovic, J. and Reiher, P. 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. SIGCOMM Comput. Commun. Rev. 34, 2 (Apr. 2004), 39-53. DOI= http://doi.acm.org/10.1145/997150.997156

[2] Internet Denial of Service: Attack and Defense mechanisms By Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reiher
denialofservice.uw.hu/ch03lev1sec3.html

[3] Gary C. Kessler Defenses Against Distributed Denial of Service Attacks November 2000 www.garykessler.net/library/ddos.html
[4] Paul Wagenseil http://www.foxnews.com/story/0,2933,188102,00.html
[5] Andy McCue. June 11, 2004. "Bookie reveals $100,000 cost of denial-of-service extortion attacks". Silicon.com.
http://software.silicon.com/security/0,39024655,39121278,00.htm

[6] Mark Lander, John Markoff. May 29, 2007. "Digital Fears Emerge After Data Siege in Estonia". New York Times.
http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&oref=slogin

[7] Kevin Mandia .Oct 2002 Incident Response - Investigating Computer Crime. by Aleksandar Stancin - Monday, 28 October 2002.

[7.1] http://www.foxholetechnology.com/pdf/FoxholeTechnologyRioREY.pdf

[8] B. Ziegler. Hacker Tangles Panix Web Site, Wall StreetJournal, September 12, 1996.
[9] CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks. November 29, 2000. http://www.cert.org/advisories/CA-1996-21.html

[10] RFC 4987 – TCP SYN Flooding Attacks and Common Mitigations. August 2007.
http://tools.ietf.org/html/rfc4987

[11] CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. January 5, 1998.
http://www.cert.org/advisories/CA-1998-01.html

[12] CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack. September 24, 1997.
http://www.cert.org/advisories/CA-1996-01.html

[13] "Ping of Death." 1996. Insecure.org.
http://insecure.org/sploits/ping-o-death.html

[14]Donald E. Eastlake, 3rdUpdates RFC 1035 CyberCash June 1998
[15]DNS Protection: DNS Amplification: Mitigation
http://www.a10networks.com/resources/files/SS-FSS_DNS.pdf
[16] White Paper of Arbor Networks : The Growing Threat of Application-Layer DDoS Attacks February 28 2011

[17] Jason Barlow and Woody Thrower. February 10, 2000. "TFN2K – An Analysis." AXENT Security Team.
http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt

[18] David Dittrich. December 31, 1999. "The 'stacheldraht' distributed denial of service attack tool." University of Washington.
http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

[19] Steve Lipner and Michael Howard. March 2005. "The Trustworthy Computing Security Development Lifecycle." Microsoft Corporation.
http://msdn.microsoft.com/en-us/library/ms995349.aspx

[20] Michael Howard and David LeBlanc. (2003). Writing Secure Code (Second Edition). Chapter 17 – Protecting Against Denial of Service Attacks.

[21] "Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks." Cisco Systems, Inc. Document ID: 13634. April 22, 2008.
http://www.cisco.com/application/pdf/paws/13634/newsflash.pdf

[22] "Cisco Traffic Anomaly Detection and Mitigation Solutions. Product Bulletin." Cisco.
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5887/prod_bulletin0900aecd800fd124_ps5888_Products_Bulletin.html

[23]Nishchal Bhalla and Sahba Kazirooni February 15 2007 "Web Service Vulnerabilities"