SURVEY OF ABSTRACT METHODS FOR HOW TO SAFEGUARD AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACKS

Tiruveedula GopiKrishna¹, DavuluriNageswara Rao², Mohamed A.Abdelhadi³

¹Research Scholar, Computer Department, Faculty of Arts & Science, Al-Jufra, Sirt University, Hoon, Al-Jufra, Libya.
²Lecturer, Computer Department, Faculty Science, Sirt University, Sirt, Libya.
³Lecturer, Department of Computer Science, Faculty of Arts & Science, Hoon, Aljufra, Sirt University, Libya.

ABSTRACT

In this article, we have tried to demonstrate that any business, large or small, that is dependent on Internet traffic to generate sales, service its customers, or maintain confidentiality is a candidate for stepped up protection against Denial of Service and Distributed Denial of Service attacks for their network systems. No business or industry should consider itself completely safe from such attacks, as a failure to maintain defensive measures can result in severe financial and reputational consequences. And we discussed some existing ways you can help safeguard your internetworking environment or a company. We also describe existing methods and techniques used in denial of service attacks, and we list possible defenses.

Keywords: DDoS, Strategies, Prevention, Detection, Tools, Attacks.

I. INTRODUCTION

A DDOS attack (better known as a Distributed Denial of Service attack) is a type of web attack that seeks to disrupt the normal function of the targeted computer network. This is any type of attack that attempts to make this computer resource unavailable to its users. While this type of attack typically follows the same sorts of patterns, the definition of the term Distributed Denial of Service does not make any specific indications of how this type of attack is to be pulled off. What makes this type of attack "distributed" is the concerted efforts between a large number of disruptors all for the common goal of preventing web servers (and therefore websites) from functioning effectively at all. These users may be willing participants, or in some cases be tricked into downloading software that
will use their terminal to aid in the offensive. All in all, regardless of the means, a DDOS attack is simply a combined effort to prevent computer systems from working as well as they should, typically from a remote location over the internet [1, 2, and 3].

The most common method of attack is to send a mass saturation of incessant requests for external communication to the target. These systems are flooded with requests for information from non-users, and often non-visitor to the website. The goal of this attack is to create a large enough presence of false traffic such that legitimate web traffic intended for actual web users is slowed down and delayed. If this type of service becomes too slow, time sensitive information such as live video footage may be rendered entirely useless to legitimate end users [1].

For a DDOS to work effectively, the process has to be heavily automated on the attacker's end. Customized software is designed to flood these services with false traffic, and is run on as many computers as possible. There are a few instances in which this type of software was set up like a virus, infecting computers and taking control of their communication functions. These users unwillingly are aiding in a DDOS attack, sometimes without being the slightest bit aware of it. If there seems to be large delays in normal internet service, there may be outbound requests being made consuming your internet connections given throughput, and can sometimes be an indication of foul play. Users seeking to limit this risk should keep anti-virus software up to date, and scan frequently for these types of programs [2].

While there are few court cases on the books of Distributed Denial of Service perpetrators being held accountable for their actions, as well as the potential lost income for commercial websites, this type of activity almost always violates the terms of service and acceptable use policies of internet service providers, as well as often violating individual communication law within the nation. These types of attacks have become more and more prevalent as time goes on, and in many nation legislation is in the works, with hopes of criminal penalties for those involved with this sort of attack.

All in all, a DDOS attack is a very real threat to businesses and organizations across the world, and it's important that they be prepared in case some group of people decides to cause trouble for your organization. Being prepared to identify these types of threats is an important part of proper internet use, and should be a part of your daily life online.

II. CATEGORIES DOS ATTACKS

2.1 Operating system attacks--Defined as attacks directed against a certain facet of the computer's operating system. The objective of these attacks is to cause the system to freeze or completely restart. As operating system attacks are very explicit in nature, applying software updates or patches that are released by software manufacturers or independent developers can easily prevent them [4].

2.2 Networking attacks--The more common type of DoS attack, which attempts to take advantage of built-in aspects of the networking functions of a system. Though various methods are used in these attacks, the most common type is that which directs so much data at the network interfaces of a system, that it closes down completely, or resets the network interface being targeted. It was a variation of this type of attack that caused the attacks earlier this year [4].

III. TYPES OF DDOS ATTACKS

3.1 Application-layer DDOS attack

Application layer DDOS attack: Application-layer DDOS attacks are attacks that target Windows, Apache, OpenBSD, or other software vulnerabilities to perform the attack and crash the server [6].
3.2 **Protocol DOS attack**

Protocol DDOS attack: A protocol DDOS attacks is a DOS attack on the protocol level. This category includes Synflood, Ping of Death, and more [6].

3.3 **Volume-based DDOS attack**

Volume-based DDOS attack: This type of attack includes ICMP floods, UDP floods, and other kinds of floods performed via spoofed packets.

3.4 **Reflected Attack**

A reflected attack is where an attacker creates forged packets that will be sent out to as many computers as possible. When these computers receive the packets they will reply, but the reply will be a spoofed address that actually routes to the target. All of the computers will attempt to communicate at once and this will cause the site to be bogged down with requests until the server resources are exhausted[6].

3.5 **Peer-to-Peer Attacks**

Peer-to-Peer servers present an opportunity for attackers. What happens is instead of using a botnet to siphon traffic towards the target, a peer-to-peer server is exploited to route traffic to the target website. When done successfully, people using the file-sharing hub are instead sent to the target website until the website is overwhelmed and sent offline[6].

3.6 **Nuke**

Corrupt and fragmented packets are sent via a modified ping utility to keep the malicious packets to be delivered to the target. Eventually, the target machine goes offline. This attack focuses on comprising computer networks and is an old distributed denial of service attack [6].

3.7 **Slowloris**

Slowloris is a tool that allows an attacker to use fewer resources during an attack. During the attack connections to the target machine will be opened with partial requests and allowed to stay open for the maximum time possible. It will also send HTTP headers at certain intervals. This adds to the requests, but never completes them – keeping more connections open longer until the target website is no longer able to stay online[8].

3.8 **Degradation of Service Attacks**

The purpose of this attack is to slow server response times. A DDoS attack seeks to take a website or server offline. That is not the case in a degradation of service attack. The goal here is to slow response time to a level that essentially makes the website unusable for most people. Zombie computers are leveraged to flood a target machine with malicious traffic that will cause performance and page-loading issues. These types of attacks can be difficult to detect because the goal is not to take the website offline, but to degrade performance. They are often confused with simply an increase in website traffic [8].

3.9 **Unintentional DDoS**

Unintentional DDoS happens when a spike in web traffic causes a server to not be able to handle all of the incoming requests. The traffic that occurs, the more resources are used. This causes pages to timeout when loading and eventually the server will fail to respond and go offline [6].
3.10 Application Level Attacks

Application level attacks target areas that have more vulnerabilities. Rather than attempt to overwhelm the entire server, an attacker will focus their attack on one – or a few – applications. Web-based email apps, WordPress, Joomla, and forum software are good examples of application specific targets [6].

3.11 Multi-Vector Attacks

Multi-vector attacks are the most complex forms of distributed denial of service (DDoS) attack. Instead of utilizing a single method, a combination of tools and strategies are used to overwhelm the target and take it offline. Often times, multi-vector attacks will target specific applications on the target server, as well as, flood the target with a large volume of malicious traffic. These types of DDoS attacks are the most difficult to mitigate because the attack come in different forms and target different resources simultaneously [6].

IV. TRADITIONAL METHODS

It used to be that a denial of service was the simplest type of attack out there. Someone would start the ping command on their computer, aim it at their target address, and let it run full speed, trying to literally flood the other side with Echo Requests, or ping packets. Of course, this quickly changed, because in this case, the attacker would need a connection with more bandwidth than the target site. First, they moved on to larger hosts, like compromising a server at a university or research center -- somewhere with a lot of bandwidth -- and sent their attacks from there. But now, botnets are used in almost all cases, because it's simpler for them, and is less apparent, making the attack completely distributed. In fact, malware authors have made a big business of running a botnet. They actually rent their compromised zombie computers, by the hour. If someone wants to bring down a website, all they have to do is pay the botnet owner a certain amount of money, and those thousands of compromised systems are aimed at the target. While a single computer would have no chance of bringing a site down, if 10,000 computers or more all send a request at once, it would bring down any unprotected server [9].

The type of attack evolved as well. ICMP, what's used by the ping command, is easily blocked. Now, there are various ways that a DDoS attack can be done. First there's what's called a Syn attack, which simply means that the attacker opens a TCP connection, the way you would normally connect to a website, but never finishes the initial handshake. It basically leaves the server hanging. Another clever way is to use DNS. There are a lot of network providers who have their DNS servers configured to allow anyone to launch queries, even people that aren't customers of theirs. Also, because DNS uses UDP, which is a stateless protocol, these two facts make this a potent way to create a denial of service. All the attacker has to do is find open DNS resolvers, craft a fake UDP packet that has a spoofed address, the one of the target site, and send it to the DNS server. While the request comes from the attacker and his botnet, the server thinks that request came from the server instead, and will send the reply to that location. So instead of having the actual botnet conduct the attack, the only thing the target site will see is a bunch of DNS replies coming from many open resolvers, all around the Internet. Also, it's a very scalable type of attack, because you can send a single UDP packet to a DNS server asking for a full dump of a certain domain, and receive a very large reply [9].

Here, we describe the distributed denial of service methods employed by an attacker. These techniques help an attacker coordinate and execute the attack. These types of attacks plagued the Internet in February 2000. However, these distributed attack techniques still rely on the previously described attack methods to carry out the attacks. The techniques are listed in chronological order. It can be observed that as time has passed, the distributed techniques (Trinoo, TFN, Stacheldraht,
Shaft, and TFN2K have become technically more advanced and, hence, more difficult to detect. Trinoo uses TCP to communicate between the attacker and the control master program. The master program communicates with the attack daemons using UDP packets.

(a) Trinoo’s attack daemons implement UDP Flood attacks against the target victim [10]. Tribe Flood Network (TFN) uses a command line interface to communicate between the attacker and the control master program. Communication between the control master and attack daemons is done via ICMP echo reply packets. TFN’s attack daemons implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks [10].

(b) Stacheldraht (German term for “barbed wire”) is based on the TFN attack. However, unlike TFN, Stacheldraht uses an encrypted TCP connection for communication between the attacker and master control program. Communication between the master control program and attack daemons is conducted using TCP and ICMP, and involves an automatic update technique for the attack daemons. The attack daemons for Stacheldraht implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks [10].

(c) Shaft is modeled after Trinoo. Communication between the control master program and attack daemons is achieved using UDP packets. The control master program and the attacker communicate via a simple TCP telnet connection. A distinctive feature of Shaft is the ability to switch control master servers and ports in real time, hence making detection by intrusion detection tools difficult [11].

(d) TFN2K uses TCP, UDP, ICMP, or all three to communicate between the control master program and the attack daemons. Communication between the real attacker and control master is encrypted using a key-based CAST-256 algorithm [1]. In addition, TFN2K conducts covert exercises to hide itself from intrusion detection systems. TFN2K attack daemons implement Smurf, SYN, UDP, and ICMP Flood attacks [2].

V. HOWTO PROTECT YOUR NETWORK

So as you can see, a DDoS can take multiple forms, and when building a defense against them, it's important to consider these variants. The easiest, although a costly way to defend yourself, is to buy more bandwidth. A denial of service is a game of capacity. If you have 10,000 systems sending 1 Mbps your way that means you're getting 10 Gb of data hitting your server every second. That's a lot of traffic. In this case, the same rules apply as for normal redundancy. You want more servers, spread around various datacenters, and you want to use good load balancing. Having that traffic spread out to multiple servers will help the load, and hopefully your pipes will be large enough to handle all that traffic. But modern DDoS attacks are getting insanely large, and quite often can be much bigger than what your finances will allow in terms of bandwidth. Plus, sometimes it's not your website that will be targeted, a fact that many administrators tend to forget[9].

One of the most critical pieces of your network is your DNS server. It's a bad idea to leave it as an open resolver, and it should be locked down in order to save you from being used as part of an attack. But in a similar way, what if those servers came under attack? Even if your website is up, if no one can connect to your DNS servers and resolve your domain name, that's just as bad. Most domain registrations are done with two DNS servers, but quite often that may not be enough. Make sure your DNS is protected behind the same type of load balancing that your web and other resources are. There are also companies out there that provide redundant DNS that you can use. For example, many people use content delivery networks to serve files to customers in a distributed way, which is
a great way to also protect them against DDoS attacks, but many of those companies also offer enhanced DNS protection as well, which is something you may want to look at. For example, it's quite obvious that your website is never going to be asking random DNS servers for queries, so there's no reason to allow UDP port 53 packets heading for your servers. Block everything you can at your network border, where you have the largest pipe, or better yet, get your upstream provider to block them for you. Many Internet providers offer this type of service to businesses, where you can be in touch with their network operating centers and make sure they block any unwanted traffic, and also help you out in the event that you're getting attacked. In a similar way, there are many ways to protect your network from Syn attacks, by increasing your TCP backlog, reducing the Syn-Received timer, or using Syn caches.[9]

Finally, you should also think about ways to mitigate any attack that does reach your site. For example, most modern websites use a lot of dynamic resources. While the actual bandwidth from an attack may be manageable, often what ends up failing is the database, or the custom scripts you may be running. Think about using caching servers to provide as much static content as possible. Have a plan in place to quickly replace dynamic resources with static ones, in the event that you're getting attacked. And make sure to have detection systems in place. The worst thing for any business is for the network or site to go down, so you want to be alerted as soon as an attack starts, and be ready to deal with it. Because of the way it's done, halting a DDoS attack at the source is incredibly difficult. But setting up an infrastructure that is distributed, hardened, and secure is possible, and that's something you should think about when setting up your network. Distributed denial of service (DDoS) attacks is a growing concern with far-reaching effects for businesses and organizations of all sizes. DDoS attacks are used by criminal enterprises, politically-motivated cyber terrorists, and hackers hoping to bring websites down for fun or profit. Now, more than ever, it is crucial for organizations and online retailers to measure their risk of attack and create a DDoS attack protection plan in advance in order to mitigate risk and enable a fast recovery[10,11].

Many observers have stated that there are currently no successful defenses against a fully distributed denial of service attack. This may be true. Nevertheless, there are numerous safety measures that a host or network can perform to make the network and neighboring networks more secure. These measures include:

1) **Filtering Routers:** Filtering all packets entering and leaving the network protects the network from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker [12]. This measure requires installing ingress and egress packet filters on all routers.

2) **Disabling IP Broadcasts:** By disabling IP broadcasts, host computers can no longer be used as amplifiers in ICMPFlood and Smurf attacks. However, to defend against this attack, all neighboring networks need to disable IP broadcasts.

3) **Applying Security Patches:** To guard against denial of service attacks, host computers must be updated with the latest security patches and techniques. For example, in the case of the SYN Flood attack [8], there are three steps that the host computers can take to guard themselves from attacks: increase the size of the connection queue, decrease the time-out waiting for the three-way handshake, and employ vendor software patches to detect and circumvent the problem.

4) **Disabling Unused Services:** If UDP echo or charge services are not required, disabling them will help to defend against the attack. In general, if network services are unneeded or unused, the services should be disabled to prevent tampering and attacks.
Performing Intrusion Detection: By performing intrusion detection, a host computer and network are guarded against being a source for an attack, as while as being a victim of an attack. Network monitoring is a very good pre-emptive way of guarding against denial of service attacks. By monitoring traffic patterns, a network can determine when it is under attack, and can take the required steps to defend itself. By inspecting host systems, a host can also prevent it from hosting an attack on another network [13].

VI. CONCLUSION

In this paper, we discussed distributed denial of service attacks on the Internet. We described how distributed attacks are conducted; we reviewed some distributed denial of service techniques, and discuss various defense mechanisms that could be employed by networks and hosts. So, every company should take care of it and set up good level of protection to defend DDOS attack. Further work is though needed that combines well known security drawbacks of wireless protocols with defense techniques that are already mature in a wireless environment.

VII. ACKNOWLEDGEMENTS

We would like to thank to all our faculty members who contributed their valuable information to prepare this paper.

VIII. REFERENCES


