Ryan Angelo
December 4th, 2009

The Anatomy of a Distributed Denial of Service Attack (DDoS)

How Zombies Can Take Down Giants

On October 23rd, 2002, people all around the world were opening up their browsers, only to find their favorite websites unavailable. Some people were trying to connect to their multimillion-dollar online businesses, while others were trying to go online to collect information for an upcoming presentation they would be delivering or to see when their flight would be leaving. What these people, who were growing frustrated at their lack of connection didn't know is, the internet was under attack. The 13 servers that are at the top of the internet's domain name system hierarchy were under attack by a distributed denial of service attack, and a large portion of the internet was unavailable to users across the globe.

A distributed denial of service attack happens when a group of systems attack targeted web servers, overloading their bandwidth and/or resources, thereby rendering them useless. Imagine being the last person left on your dodgeball team in high school. The other team has a dozen people left, and you are alone. You already have one ball in your hand as the other team all winds their arms back and throws a dozen balls at you simultaneously. There is nothing you can do. You might be able to handle a few of them coming at you, but you are inevitably going to be brought down. Distributed denial of service attacks have the power to bring the largest, fastest and most complex networks to their knees.

Building a Distributed Denial of Service Attack

One may wonder how a distributed denial of service attack is formulated. Where do all of the machines doing the attacking come from? The answer is zombies. Zombies are computers which have been compromised, generally through becoming infected by malware, generally Trojans. Once compromised, these systems can be given commands by attackers. The zombies can check in with the hacker through IRC channels, where the hacker can give new commands to be carried out. IRC channels provide anonymity by obscuring the names and IP addresses of the users and additionally offer the benefit of not having to scan for active bots because they all check in to the hidden, private IRC channel. Furthermore, attackers utilize tools such as Stacheldraht to connect to handlers. Handlers are systems which have been compromised, and these Handlers are the systems which give the commands to the zombie systems (also referred to as zombie agents). This means that the attacker is covering his tracks to an extent because he isn't giving the commands directly to the zombie agents but rather to a specific few compromised handlers, who in turn give out the commands. Additionally, this distributes tasks, making the group of compromised systems, referred to as a botnet, similar to an army. Each handler machine, which can be thought of like a lieutenant, is able to give commands to 1,000 zombies. This means that an attacker could control 5 handlers and ultimately have control of 5,000 zombie machines. To offer an idea of how large a normal botnet is, studies predict the the median size is around 45,000. That is 45,000 compromised machines in a single botnet. The botnet has the remarkable power of 45,000 machines that are all being given a single task, to bring down the targeted site. Interestingly, botnets have become so prevalent that they are incredibly cheap to purchase, with one bot averaging $0.50. This means that competing companies, crime rings, and individuals can have access to a botnet for malicious, corrupt purposes at a low cost.

Another way to carry out a distributed denial of service attack, which is slightly different is a trojan such as “MyDoom”. Trojans such as MyDoom have the address for which they are going to flood hardwired into the code, rather than making the system a zombie that takes orders. When a system is infected with a variant of MyDoom, they are told to attack specific sites because it is hardwired into their code. With hundreds of thousands, and at times, millions of infections, the flood of compromised systems hitting these specific sites is devastating. In 2004 Microsoft offered a $250,000 reward for information leading to the arrest of the author of MyDoom, after finding out that the worm was going to be targeting Microsoft’s website. MyDoom, a trojan whose abilities extend farther than just DDoS attacks, was the fastest spreading virus in history. MyDoom wreaked havoc around the world for 5 years, and as of September 2009, is still in the wild and a major issue in the United States. The author, thought to be in Russia, has never been caught.

The Attack

There are several types of attacks which can be carried out, all of which constitute a denial of service attack. Such attacks include SMURF attacks, which would send spoofed ping messages to a targeted network, and at the time, the systems on the targeted network would respond. When an attacker used a large pool of spoofed IPs to send these pings to a target network, the bandwidth would overwhelm the targeted network as each system on the network would reply to each request packet sent, making it unusable. Fortunately, modern network configurations generally can ignore ping requests, which protects the internal network but the traffic is already coming through the connection so traffic from the WAN (outside network) can still be slowed down or denied service.

Another type of attack, which focuses on using all of the targets system resources is a SYN flood attack. A SYN flood attack is when the distributed systems under the control of the attacker, send TCP connection requests faster than the target machine can process them. The attacker creates a random source address (where it is coming from) for each packet that is going to be sent. The SYN flag in each packet is set to request a connection to be opened with the targeted server, with the IP address of the attacker, which is spoofed. The victim server(s) responds to the connection request and waits for confirmation from the spoofed IP address. This confirmation from the spoofed IP address will never actually come. The victim’s table of connections that are being made to the server fill up with connections that are waiting for a reply, and as this table fills up, new connections are ignored, including the connection of authentic users. Modern servers have operating systems which can generally handle extremely large connection tables, making SYN flood attacks more difficult, however they are still a widely used and effective method of bringing down a server.

Modern DDoS attacks are far more difficult to prevent because of how genuine the traffic heading into the server looks and how massive the traffic can be. The bots send ping requests or connection requests at a massive volume from all different locations and converge on one location. The amount of traffic focusing on one point causes the bandwidth to become overloaded, disabling genuine traffic from accessing the given server(s). Valid users use TCP packets to connect to server(s). Because of this, modern attacks often utilize the SYN floods to bring down a server. The server needs to accept the TCP packets because that is how legitimate users request a connection, so unlike pings which can be blocked, TCP packets cannot be blocked. It therefore becomes hard to decipher what is genuine traffic and what is traffic coming from a botnet. The TCP packets, as mentioned previously have source IPs which are spoofed, so the servers see the the source IP as unique, so genuine traffic is hard to separate from fraudulent traffic. It is effective because of the underlying design of how the internet works. Furthermore, it should be noted that a ping request attack is also still a viable method of attack because, although the ping can be ignored by the router, the routers decision to actively deny the ping request still causes any upstream traffic to be slowed down. That is to say, the router is protecting what is inside the network, but any traffic that is coming from outside the router is still effected because of the amount of traffic that the router is receiving and making decisions about.

The Solution

Preventing a DDoS attack is nearly impossible because of the fact that authentic traffic and fraudulent traffic cannot be separated, and because regardless of whether the fraudulent traffic can be spotted, by the time the router for the server recognizes the traffic, the fraudulent traffic has already come down the router's pipe and is already doing what it was designed to do. One possible way of circumventing an attack is by changing the IP address of your server. Unfortunately, having your IP changed when you are on a cable modem or DSL connection is not simple. You can change your MAC address which tells the Internet Service Provider to change your IP, because generally your IP is tied to your MAC address. However, some ISPs tie your subscription to your MAC address, so you would need to spoof your MAC address. Furthermore, the downside of simply changing your IP would mean that, although you no longer are the target of the attack, someone else will obtain your old IP and become the victim of the DDoS attack. This is because your hardware is not the actual target, but rather your IP address. Proxy servers are one way of putting something between you and your IP which would direct traffic from another source, however this is not convenient for many people. DDoS attacks exploit what is a structural flaw that currently has no solution.

"Lawful" DDoS Attacks

There is such a large quantity of people online now that many websites have millions of users each day visiting their site. An interesting and new situation is when a large number of people converge on a site, for example, digg.com. Digg.com is a social news website where users can vote on stories and the more votes a story has, the closer to the front page it is. All of these stories have links to other websites. Digg.com is designed to maintain a quality connection for hundreds of thousands of users at one time, however, when those hundreds of thousands of users all click on some of the links that are near the front page, a huge number of people hit the site at the same time. This is, by definition, a DDoS attack. Although not malicious in intent, the users of such websites as digg.com bring down websites because of their enormous volume of traffic in a small period of time, focused on one website. Such an occurrence has been labeled “the digg effect.” A number of other websites, such as Slashdot, another news website which was one of the original websites to start causing these lawful DDoS attacks. A website would be featured on Slashdot and would subsequently be “Slashdotted.” It would seem that the only way to solve this problem would be for more websites to have more capable equipment that could handle the sudden load. It presents an interesting situation for the future of the internet. As more people get online, and as more content moves online, large, focused access to specific sites is going to become more prevalent.

Looking For a Solution

If DDoS attacks are impossible to combat directly, and it is the structure of how the internet operates that causes DDoS attacks to be successful, one must consider how DDoS occurrences can be minimized as the internet grows. Large companies that rely on their website and other networks to make money, should invest in equipment that can provide a large amount of bandwidth when necessary. Additionally, certain DDoS attacks can be minimized by correct hardware configuration, specifically in the router. Proposing that the structure of the internet changes, where a handshake between the server and client are not carried out in such a way that it can be detrimental to the performance of other users is a difficult proposition. To change the structure of a system that already has itself implemented deeply into billions of systems would be a challenge, a challenge that only massive ISP’s would be able to even think about carrying out. One might propose that ISPs take more responsibility for the traffic that comes into their networks, however, then there is always the argument that ISPs are invading the privacy of their customers by doing deep packet analysis. Time and the continual improvement of hardware may be the only answer. It is possible that the only way to prevent a DDoS attack is by creating a network infrastructure which can accept and deal with the attack.

If Interested, additional readings:
The Strange Tale of Denial of Service Attacks Against GRC by Steve Gibson, Gibson Research Corporation.
www.crime-research.org/library/grcdos.pdf

Works Cited

Dittrich, David. " The "stacheldraht" distributed denial of service attack tool." 31 Dec 1999. University of Washington, Web. 3 Dec 2009. <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt>.

"Feds investigating ‘largest ever’ Internet attack Attack of the Drones." *The Register*. 23 Oct 2002. ComputerWire, Web. 3 Dec 2009. <http://www.theregister.co.uk/2002/10/23/feds_investigating_largest_ever_internet/>.

Gibson, Steve. "The Attacks on GRC.com." *Gibson Research Corporation*. 02, Jun, 2001. Gibson Research Corporation, Web. 3 Dec 2009. <http://www.grc.com/intro.htm>.

Hurley, Edward. "Countdown begins for Mydoom DDoS attacks." *SearchSecurity.com*. 30 Jan, 2004. Information Security Magazine, Web. 3 Dec 2009. <http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci947185,00.html>.

Legon, Jeordan. "Security firm: MyDoom worm fastest yet." *CNN.com International*. 28 Jan, 2004. CNN.com International, Web. 3 Dec 2009. <http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/>.

McDowell , Mindi. "National Cyber Alert System Cyber Security Tip ST04-015." *Understanding Denial-of-Service Attacks* November 4, 2009: n. pag. Web. 3 Dec 2009. <http://www.us-cert.gov/cas/tips/ST04-015.html>.

"Preventing Smurf Attacks." *NORDUNet*. Web. 3 Dec 2009. <http://www.nordu.net/articles/smurf.html>.

"Security Now - Episode 8." *Security Now*. Podcast. 3 Dec 2009. <http://www.grc.com/securitynow.htm>.

"SYN Floods." *Internet Security Systems*. Internet Security Systems, Web. 3 Dec 2009. <http://www.iss.net/security_center/advice/Exploits/TCP/SYN_flood/default.htm>.

"The Botnet Trackers." *The Washington Post*. 16 Feb 2006. The Washington Post, Web. 3 Dec 2009. <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/16/AR2006021601388.html>.

"Types of DDoS Attacks." *Advanced Networking Management Lab (ANML) Distributed Denial of Service Attacks(DDoS) Resources*. Pervasive Technology Labs at Indiana University, Web. 3 Dec 2009. <http://anml.iu.edu/ddos/types.html>.