Trent Giever

Case Project 5-1 DoS Attacks

7/12/18

DoS Attacks

What the average user wants is a website online during their schedule, and that the data given is safe. But both are the targets of threat actors. Threat actors want to disrupt service to a specific site by using a flood of requests that disrupt the server from real users and is called a Denial of Service Attack. The goal of every network admin is to be able to use a filter to help reduce the number of fake requests. A Denial of Service is from a single location, while a Distributed Denial of Service uses a botnet. Denial of Service attacks however are not going anywhere with hackers getting more complex in the attacks.

Since Denial of Service attacks happen all the time it is not hard to find a server affected. The most recent attack on a popular site was against Blizzard Entertainment that created and hosts video games on servers like Overwatch, Heroes of the Storm, Word of Warcraft, and others. The attack started Sunday 7/8/18, and ended Tuesday 7/10/18. The attack caused lag for some players, and others stopped from logging-in. The attack could have been worse if the attack turned off the servers completely and would hurt the trust in Blizzard (DDos Attacks, 2018). Another recent attack on June 27th taught the IT community to not have the CEO insult the hacking group on social media. The hacking group Apophis Squad likely from U.K. attacked Proton Mail in the U.S. with a DDoS attack with a first round knocking out the server system for one minute with a 200 Gbps SSDP flood. After posting of the victory on social media the CEO Bart Butler called them “Clowns” and got 2 days of constant attacks, and the longest down period of 10 minutes. The hackers have claimed 500 Gbps attack, but still needs to be verified (DDoS Attacks, 2018). The best thing might to praise the attackers for finding a vulnerability, then mocking them online.

DoS attacks happen often and is much more severe than I thought it happened from a short down time. Corero Network Security did a survey from network admins and found that a single attack could cost up to $50,000 in “lost business, attack mitigation, and lost productivity”, and 78% said the amount is much greater in the “loss of customer trust and confidence” (DDoS Attacks, 2018). 69% in the survey had between 20 to 50 DDoS attacks per day with the average overall of one attack per day for each server and could be as high as $1.75 million lost profits from the attacks if factoring in 1 per day. The biggest loss is a customer that will go to a different site if the company site is down (DDoS Attacks, 2018). The 1.75 million seems low for some sites like Amazon, and high for a small business that does not sell very many items online and not quite sure how the formula is getting that number.

While looking for a solution for DoS I found a site that had the opposite and had 10 different free program links to attack your enemies (Shankdhar, 2018). It is clear a solution is needed fast. If it is from a single location Denial of Service attack that is not from a botnet then it can be stopped by simply blocking the IP address, but the more modern DDoS attacks from botnets are much harder to stop since it is from many IP addresses, and the only protections make bigger attacks needed to cripple the systems. Cisco Edge and other like items can create SYN cookies that are more efficient at tracking TCP connections and increase the threshold. For HTTP flood by having a network server covering a smaller section to filter through can reduce the impact of one server going down (Weiss, 2012). There is many different programs and hardware that can reduce the impact and can raise the fail threshold, but none is perfect. Modern home routers come with DoS protections but are no means perfect.

The attacks of DoS are not going to end with the current protections on the market. With the rise of ease for anyone to attack an enemy of theirs for free is making it much harder. The current protections are only able to raise up the threshold and force the attackers to pay more for bigger bot nets. Denial of Service is not going to end, and my guess is that the next target will be prime day from all the added users making it easier.

# References

DDoS Attacks. (2018, June 28). *ProtonMail DDoS Attacks Are a Case Study of What Happens When You Mock Attackers.* Retrieved from DDoS: http://ddosattacks.net/protonmail-ddos-attacks-are-a-case-study-of-what-happens-when-you-mock-attackers/

DDos Attacks. (2018, July 10). *That weekend-Long DDoS Attack on Blizzard Is Ovee.* Retrieved from DDoS: http://ddosattacks.net/that-weekend-long-ddos-attack-on-blizzard-is-over/

DDoS Attacks. (2018, July 11). *The cost of DDoS attacks on businesses.* Retrieved from DDoS Attacks: http://ddosattacks.net/the-cost-of-ddos-attacks-on-businesses/

Shankdhar, P. (2018, April 26). *Best DOS Attacks and Free DOS Attacking Tools.* Retrieved from INFOSEC INSTITUTE: https://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/

Weiss, A. (2012, July 2). *How to Prevent DoS Attacks.* Retrieved from eSecurity Planet: https://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html