Understanding the Behavior of a Denial of Service Attack for a Better Defense

Alexander Cannell

Southern Utah University

October 2016

**Abstract**

We just witnessed on Friday October 21st 2016 one of the biggest distributed denial of service (DDoS) attacks it brought down a lot of sites. My coworker stated, “This attack is the worst DDoS attack I have seen.” Events like these show proof that DDoS attacks are evolving into scarier creatures. As Jose Nazario stated, “DDoS attacks are constantly evolving as the nature of technology used and motivations of the attackers are changing… A DDoS attack is designed to overwhelm victims with traffic and prevent their network resources from working correctly for their legitimate clients.” (Network Security, 2008) DDoS is a very powerful attack tool and can cause significant damages. The purpose of this Literature review is to do research on the following questions; what are the motivations behind these attacks? What is a DDoS attack? Also, how do I detect and protect against DDoS attacks?

**Reviewing of Literature**

*Understanding the Motivations behind a DDoS Attack:*

I just had a party the other day, a bunch of my friends who didn't know each other with the only thing in common is knowing me. I noticed the whole night the topic centered on getting to understand someone else's motivation. What I mean by motivation is what makes them the person that they are, or why they do what they do. With questions like what do you do for work? What do you do for school? What do you do for fun? etc… How did you get into that? When someone understood someone else's motivation they could relate and become better friends. Now in the world of Information Security we aren't necessarily looking for friends but once we understand someone's motivation helps us better defend against attacks from that someone. As Sun Tzu once stated, “If you know the enemy and know yourself you need not fear the result of a hundred battles.”

There are several motivations of a Denial of Service Attack they are Hacktivism, Business Crime, Cyber Warfare, and Other. Hacktivism is the combination of two words hack and activism, meaning hacking for a cause such as social or political. An example of hacktivism is the very popular hacker group Anonymous who typically wear Guy Fawkes masks. We are seeing an increase in Hacktivism throughout the years, and we are only going to see more instances of hacktivism. Honestly I’m kind of on the fence about hacktivist and their hacktivism activities. Svetlana Nikitina stated it perfectly, “It is difficult to determine whether rogue programs are a transient problem which will go away as hackers develop a different ethical standard; whether they are a drop in the bucket of problems which may arise as the criminally motivated become more computer literate; or whether they are like the common cold afflictions which come with the use of computers with which we must learn to live.” (Hacker Culture, 2012) Business Crime is a broad definition that encompasses Disgruntled Employees who want revenge, Competitors who want to get an edge in tough markets, and even unintentional acts of harm. Each of these Business crimes are either revenge, or money motivated hacking. Cyber warfare is any virtual conflict initiated as a politically motivated attack on an enemy fought on the virtual battlefield. A great example of this is the malware Stuxnet, which is a zero day vulnerability that is designed to attack a specific target specifically the nuclear facilities the first cyber warfare weapon. (Stuxnet, 2011) It is my belief that our wars in the near future (some could argue in the present) will be fought not on a battlefield with boots on the ground but in cyberspace. DDoS can be a powerful weapon to be used in war. (Cyberwar, 2015) Other is a generalized term that encompasses any criminal act or unintentional criminal act done on a computer or the internet. I’m using this term to describe everything else. Some examples of this could also be Terrorists, Nation States, thieves, Amateurs/Script Kiddies/Noobs, Grey Hat Hackers, Black Hat Hackers, etc... Once we understand what the different categories of cyber attackers it gives us the first step of understanding their motivations. (Motivates, 2014)

How we analyze someone's motivations after an incident? Looking at Figure 1 below we can see that we can group these categories of hackers/attackers into two sections by asking where is the attack coming from inside or outside? Once we have determined where the attack is coming from we can then move on to determining the type or category of attack then the motivation behind the attack. Now the majority of the time DDoS attacks will be coming from outside rather than inside. (Hackers Motivation, 2003)

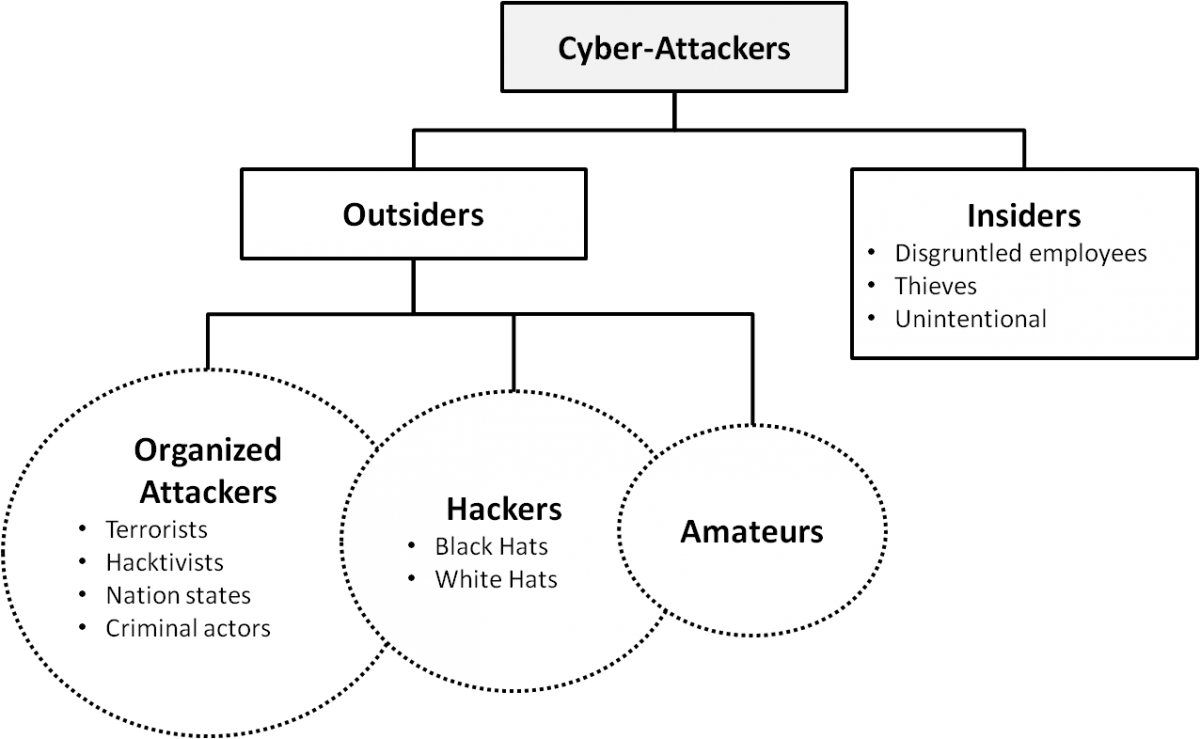


Figure 1: <http://timreview.ca/sites/default/files/TIMReview_October2014_HanDongre1.png>

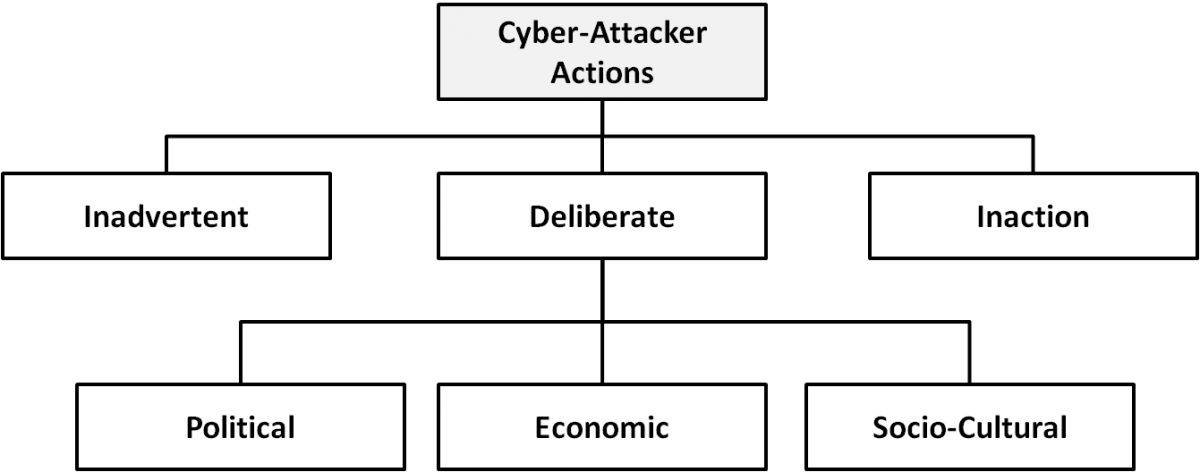


Figure 2: <http://timreview.ca/sites/default/files/TIMReview_October2014_HanDongre2.png>

*Understanding What a DDoS Attack Is:*

We are seeing an increase in cyber attacks, and that is a problem for all of us. Now that everyone is connected in some way to cyberspace through our phones, our laptops, and other personal devices. Compromised computers can be used as stepping stones for the next attack or become a part of a BotNet to be used in a Denial of Service attack. What is a DoS Attack? (Cyberwar, 2015)

When I think about Denial of Service Attacks I have to think about it in terms of real life examples this helps me remember. DDoS is like playing catch with someone. You (Website/Targeted servers) are there with your friend (legitimate traffic) playing catch back and forth. Then all of the sudden the local gang (BotNet) with the leader (Master controller) come by and see you are playing catch. The leader (Master Controller) gives the local gang (BotNet) a command to attack or to throw baseballs at you (Targeted Servers). You see said baseballs flying at your head so you duck to protect yourself, but you also are not available to receive your friends traffic either. So in simplest terms a DDoS Attack is an attack in which multiple attackers overload computing/network resources with a large amount of traffic causing legitimate users access to those resources. (Symantec, 2016)

I have mentioned BotNets. BotNets are very important inguard to DDoS Attacks, they are the devices that send out the large amounts of traffic. Botnets are a network of infected computers, devices, or nodes that can be controlled via malicious software to do the controllers bidding. Large Botnets consist of the attacker’s controller machine, a series of handlers which relay commands and prevents direct contact with the compromised devices, and then the compromised or infected devices themselves. Other uses for Botnets are sending Email Spammers, Peer to Peer, Spyware, Bitcoin Mining, Click Fraud, and of course DDoS attacks. If you ever have a desire to use a botnet but don't want to spend the time or don't have the skill to create one you can hire your own personal Botnet. (SANS, 2003)

There are several different types of DDoS Attacks these are Flood/Volumetric, Connection State, and Application-Layer Attacks. Flood/Volumetric attacks seek to take up all the available bandwidth; causing legitimate user to no longer be able to connect to an application or server. Some examples of Flood/Volumetric attacks are User Datagram Protocol (UDP) Floods, Internet Control Message Protocol (ICMP) Floods, and Domain Name System (DNS) Reflection. This week on Friday October 21st 2016 there was a massive DDoS DNS Reflection attack on the web services company Dyn that brought down their DNS servers causing a major outage across the United States. Major Websites went down including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud, and The New York Times. No one has taken credit for the attack, and we still don't know what the motivation behind the attack was. I was talking to my co-worker about it and he quoted Batman, “Some people just want to watch the world burn.” But I think it was more of a curiosity or Grey Hat motivation.(NYTimes, 2016) Connection State Attacks fill up connection tables on network devices with active connections; some examples of these devices are firewalls, webservers, and application servers to prevent legitimate connections onto that device. Application Layer Attacks are attacks on application server with the purpose of overloading the server with a large amount of requests for application resources, this eats up all available resources causing crashes. (Symantec, 2016) DDoS is a powerful tool which has and will continue to wreak havoc on private organizations, people, and governments.

*Understanding Different Preventive Measures:*

The company I work for is a major target for attack. We handle a lot of people’s personal data, and client data too. If we were to lose that or the confidence of our customers we would lose money. Also if our site goes down, is slow, or unusable we lose customers due to the quality of the site, which means we lose customers. That is why it is so important for not only the company I work for but others like it to have a way of defending against DDoS attacks.

The best way to defend against a DDoS attack is a process called mitigation. DDoS Mitigation means to make the impact of the increased traffic less severe and less likely to cause problems. With the rapid and extraordinary changes with DDoS techniques and common protections are not always going to be able to prevent real damages. I.e. Bandwidth provisioning, firewall, intrusion prevention systems, intrusion detection systems, etc... One way is to pay your ISP to detect and mitigate DDoS attacks. Another is and probably the best way is to hire a third party mitigation service company to mitigate your traffic. They mitigate traffic by examining all the incoming traffic and scrubbing out the bad traffic. A successful mitigation has to include 24/7 monitoring for detection, adequate detection/monitoring software, best practices for mitigation services, and an incident handling procedure for your company. What I mean by best practices is centralized data gathering/analysis for your organization you have to know what is going on), layered defense approach to allow only legit traffic and discard unwanted, scalable infrastructure to better handle demand of system functions during an attack, and understand your system this practice helps you better detect DDoS attacks especially application layer attacks which are tricky to detect. (SANS Mitigation, 2003)

*Incident Handling Procedure:*

I have noticed from an assignment in my Network Security Class when we were doing research on Incident Handling Procedures that most Information Security Incident Handling Procedures follow the same major stages Preparation, Identification, Containment, Corrective, Recovery, and Post Mortem. An Incident Handling Procedure helps an incident response team to properly act to prevent and mitigate the damages caused by an potentially damaging event. The procedure is the same with a Distributed Denial of Service Attack Incident Handling Procedure. These essential stages help us defend during a DDoS attack. (CERT-EU, 2014)

* Preparation:
  + Contacts
  + Procedures
  + ISP, third party mitigation services, and specialized support
  + Network and Infrastructure setups
* Identification:
  + Detection and Alerting
  + Attack Analysis.
  + Motivation identification (Check above). Making a list of potential DDoS attack initiators, and investigate possible motives.
  + Mitigation acquirement/refinement.
* Containment:
  + Network modifications
  + Content Delivery Control
  + Traffic control
* Corrective:
  + Bandwidth Prioritization and blocking
  + Traffic scrubbing
  + Sinkholing
* Recovery:
  + Normal State Verification
* Post Mortem:
  + Incident Review
  + Investigation
  + Information Disclosure
  + If needed inform Law Enforcement
  + Post Mortem Report after investigation

**Method**

If I were to conduct a study on what can be done to detect and protect against DDoS? If I had access to a different companies DDoS data I would change my question to what is the value of a DDoS mitigation service during an attack for a bigger company as opposed to a smaller company? I think that is a more specific question that I would find interesting to find out the answer too. I think the best way to do so would be by the Sampling Design Method. Grabbing appropriate data from big/small companies and third party migration services. I would compare all three to the SANS standard for DDoS prevention. If I didn't have access to the data I would look at news reports of DDoS attacks and compare them to the SANS Standard to determine if we are getting better at handling DDoS attacks. It would be interesting to see if the rate of successful DDoS Attacks have significantly decreased since the implementation of DDoS Mitigation. I find the concept and simplicity of DDoS Attacks so intriguing.

**Resources**

* Perlroth. (2016, October). Hackers Used New Weapons to Disrupt Major Websites Across ... Retrieved October 23, 2016, from http://mediaentertainmentnews.typepad.com/blog/2016/10/hackers-used-new-weapons-to-disrupt-major-websites-across-us-the-new-york-times.html
* SANS. (2003, August). SANS Institute InfoSec Reading Room. Retrieved October 23, 2016, from https://www.sans.org/reading-room/whitepapers/intrusion/summary-dos-ddos-prevention-monitoring-mitigation-techniques-service-provider-enviro-1212
* SANS. (2003, August). SANS Institute InfoSec Reading Room. Retrieved October 23, 2016, from https://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299
* NIKITINA, S. (2012). Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture. *Journal Of Popular Culture*,*45*(1), 133-152.
* Elazari, K. (2015). HOW TO SURVIVE CYBERWAR. *Scientific American*, *312*(4), 66-69
* Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-Based Model of Computer Hackers' Motivation. *Cyberpsychology & Behavior*, *6*(2), 171-180.
* Jung, J. (2002, May). Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites. Retrieved October 22, 2016, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.682&rep=rep1&type=pdf
* Akamai Inc. (2015, March). How to Evaluate DDoS Mitigation Providers - Akamai. Retrieved October 23, 2016, from https://www.akamai.com/jp/ja/multimedia/documents/content/how-to-evaluate-ddos-mitigation-providers-four-critical-criterial-white-paper.pdf
* CERT EU. (2014, July). DDoS Overview and Incident Response Guide July 2014. Retrieved October 23, 2016, from http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP\_14\_09\_DDoS\_final.pdf
* Floyd, K. (2007, September). The Autotelic Propensity of Types of Hackers. Retrieved October 22, 2016, from http://delivery.acm.org.proxy.li.suu.edu:2048/10.1145/1410000/1409926/a16-floyd.pdf?ip=134.250.60.5&id=1409926&acc=ACTIVE SERVICE&key=B63ACEF81C6334F5.A640D303AF84EDEF.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=684590593&CFTOKEN=55996768&\_\_acm\_\_=1477201669\_2480ed793243bc67ab9eac69ca01919e
* Han, C. (2014, October). Q&A. What Motivates Cyber-Attackers? | TIM Review. Retrieved October 23, 2016, from http://timreview.ca/article/838
* Nazario, J. (2008, July). DDoS attack evolution - ScienceDirect.com. Retrieved October 23, 2016, from http://www.sciencedirect.com/science/article/pii/S1353485808700862
* Incapsula Inc. (2016, January). Global DDoS Threat Landscape | Q1 2016 | Incapsula. Retrieved October 23, 2016, from https://www.incapsula.com/ddos-report/ddos-report-q1-2016.html
* Sager, C. (2014, June). Why Do People Perform DDoS Attacks? | BrainStuff. Retrieved October 23, 2016, from http://www.brainstuffshow.com/blogs/why-do-people-perform-ddos-attacks.htm
* Symantec. (2016, April). Symantec’s 2016 Internet Security Threat Report. Retrieved October 23, 2016, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf