The Low Orbit Ion Cannon (LOIC) was originally developed by Praetox Technology for network stress-testing but since has become open source. With the LOIC becoming open sourced, this has now led to other third-parties being able to use it for DoS attacks. It is an easy tool to use, it requires a simple download and has an easy to use interface allowing the user to launch an attack. LOIC works by flooding the intending victim server with large amounts of TCP, UDP, or HTTP packets. One attacker is not able to generate enough packets to be able to cause a DoS on the victim server, so the attacker requires a mass amount of users all directing their attacks towards the victim server, this can be accomplished using a botnet. A disadvantage of attacking a victim server using LOIC is that you cannot use a proxy, so the attacker's IP address is visible and can lead to legal action. The Tribal Flood Network (TFN) DoS attack is a distributed denial of service attack. Similar to the LOIC it uses a large amount of systems to flood a victim network to overload it with traffic causing the DoS to occur. The difference is that a TFN attack will target routers and firewalls, intending to infect them with malware which will allow the attack to use them in a botnet attack. Once infected, the attack can launch the TFN attack and use the infected systems for the DoS attack on the victim network. This attack also requires a large botnet to be effective and can also lead to legal action if the attack can be identified. The communication between the attacker and their botnet daemons is encrypted and uses UDP, TCP, or ICMP packets to spoof the source IP address for the attack. BootYou is considered a booter or stresser service that launches a DoS attack against the intended website or victim. The idea of this service was that it would essentially allow the average user to pay for the service to be done for them with very little technical knowledge or needing to have the

resources themselves. The user would just need to pay to use the service, and choose where they wanted the attack to target, and the service would be carried out for the user without the user needing to do anything else. Booter services were a way for individuals to make money by providing an on demand service for DDoS attacks, DDos for hire.

A DoS attack is a cyber-attack that is intended to make the network unavailable to the intended customers or users by flooding the traffic to the network and overwhelming it. The damage or impact of a DoS attack can be the downtime leading to a loss of productivity and revenue for the organization/business that is being affected. If a banking business was affected by a DoS attack and the customers were unable to access their funds this would lead to reputational damage to the company. It can also be a large cost to mitigate the damage caused by a DoS attack and to prevent future attacks. To combat DoS attacks that control of network and traffic filtering is crucial, this can prevent malicious traffic from reaching the intended target and can be accomplished through firewalls and IDS/IPS. If this cannot be accomplished another solution is to limit traffic though the network, this can stop malicious traffic but also can stop legitimate traffic by limiting how much traffic reaches the target. An organization can also pay for DDoS protection services such as Cloudflare which specialize in protecting a network against DoS attacks by filtering traffic and distributing it across multiple servers. After a Dos attack it is also important for the organization to have an emergency response plan for how to handle the aftermath of the attack, this can minimize damages to aspects such as reputation depending on how the attack is handled. If the attacker can be identified, the organization can also choose to pursue legal action since DoS attacks are illegal in most countries.

Works Cited:

What is a ddos booter/IP stresser? | *ddos attack tools* | *cloudflare*. (n.d.). Retrieved February 11, 2023, from https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/

What is the low orbit Ion Cannon (LOIC)? - cloudflare. (n.d.). Retrieved February 11, 2023, from https://www.cloudflare.com/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/

Wikimedia Foundation. (2021, December 22). *Tribe Flood Network*. Wikipedia. Retrieved February 11, 2023, from https://en.wikipedia.org/wiki/Tribe_Flood_Network