Distributed Denial of Service (DDoS) Attacks: An Analysis

Divya Aradhya & Glenn M Pinder

Saint Leo University

Authors Note

Contact: divya.aradhya@saintleo.edu & glenn.pinder@email.saintleo.edu

April 5, 2017

Table of Contents

Abstract

Distributed Denial of Service (DDOS) attacks pose a serious problem for organizations, due to the various ways an attacker can launch such an attack. This research paper identifies how Distributed Denial of Service (DDOS) attacks are carried out by attackers, as well as mitigating techniques that organizations can use to reduce the attack surface of associated systems and networks. The paper also touches on the history and timeline of DDoS attacks, as well as causes of increased risk in such an attack. In conclusion, the paper addresses U.S. Legal ramifications, impacts and the future of DoS attacks.

Introduction and Definition

In today's business environment, there is a strong reliance on information. It is the organizations' computer network systems that move data between one system and another. The data is then processed in to information that organizations use to make day-to-day business decisions. Equally or more important is the fact that some of the information traversing a network is personally identifiable information of customers, sensitive corporate information, as well as the information of other business entities. If organizations are separated from their much-needed data, it would bring their day-to-day operations to a grinding halt.

Before an organization's security professional can defend the network against a DoS attack he or she must gain an understanding of what is involved in the attack. There are two instances involved with this type of attack. Two instances involved in a Denial of Service attack. The first involves a Denial of Service (DoS) attack. The definition of a Denial of Service attack is an attack that attempts to prevent a system from answering legitimate requests from users, directly affecting the availability portion of the Confidentiality, Integrity, Availability (C-I-A) triad. Additionally, a DoS attack is launched by a single system (Gibson, 2016). The description of a DoS attack is traffic in and out of a network is blocked when servers are flooded with malformed packets or bits of digital information that contain false Internet Protocol (IP) addresses, other harmful data, or other fake communications. Secondly, there is an attack known as a Distributed Denial of Service (DDoS) attack. A DDoS attack is an attack in which many computers are hijacked and used to flood the target with so many false requests that the server cannot process them all, and normal traffic is blocked (Weaver, Weaver, & Farwood, 2014).

Attackers carry out DDoS attacks using a “botnet” which is a group of computers (called zombies) controlled by an attacker. The term botnet is derived from robot and network. The attacker manages a command and control center, and the computers in the botnet do the bidding of the attacker (Gibson, 2016).

Types and Methods of DDoS Attacks

There are several different methods an attacker uses to perform DoS attacks to restrict or deny access to network data and services.

Methods include-

- Internet Control Message Protocol (ICMP) message abuse,
- Smurf attack,
- SYN Flood, and
- Fraggle attacks

An attacker may use the ICMP by sending a steady stream of ping requests to a target IP address. The **ICMP** sends four packets with each request. The attacker hopes to overwhelm the target system with a continuous stream of ping packets with the goal of disrupting services or crashing it. Mitigating ICMP packet flooding can be accomplished by setting up a filter on the firewall that blocks ICMP requests.

A Transmission Control Protocol (TCP) Flood attack, also known as a **SYN flood**, TCP SYN, or TCP half-open attack is when the attacker exploits the TCP three-way-handshake and tries to confuse the receiving system by sending packets with the SYN flag set, but does not complete the three-way-handshake by withholding the ACK packet. As a result, the receiving system is busy expecting to complete the other portion of the handshake, resulting in the connection being left in a half-open state (Gibson, 2016). Best practices for mitigating SYN flood attacks is to

update and patch firewalls and operating systems so that these types of attacks are blocked (Weaver et al., 2014).

An attacker uses a **Smurf attack** to broadcast ICMP ping packets to multiple computers on a network but spoofs the source IP address using the IP address of the attacked system. By spoofing the source IP address, it causes the ICMP packets to be broadcasted to other computers on its own network. The result of this type of attack causes all systems on the network to respond to the ICMP requests, which tie up network resources or render the network inoperable due to being overwhelmed by looped echo requests and replies. Again, best practices for mitigating this type of attack is to up to date and patch firewalls and operating systems so that these types of attacks are blocked.

A **Fraggle attack** is like a Smurf attack in that it tries to overwhelm a system with packets. The difference between a fraggle attack and smurf attack is a fraggle uses User Datagram Protocol (UDP) packets to carry out the attack. UDP port 7 or 9 is targeted with echo requests or character generation. Disabling the port is a best practice for mitigating this type of attack (Gibson, 2016).

The DDoS attacks that were discussed in the before-mentioned paragraphs are the common types that attackers use, so the attacks are always at the forefront of security websites, magazines and educational texts. Internet Control Message Protocol (ICMP) message abuse, Smurf attack, SYN Flood, and Fraggle attacks impact the networks at Layers 3 and 4 of the OSI Model. There is a DDoS attack that happens at Layer 7 of the OSI Model that does not get a lot attention in the security reporting and awareness arena. One of the reasons it does not receive the same press as the Layer 3 and 4 DDoS attacks is because of the ingenuity that goes into setting up the attack. The fact that it is complex in nature makes difficult to defend against. The attack is carried out with the help of “HTTP GET”. Since HTTP GET is an Application Layer protocol, which means

that the three-way-handshake has already occurred and the perpetrator is already in the network. After meeting the criteria for a connection, the attacker is passed on to the Application Layer where the HTTP protocol lies. This is where the attacker performs actions that will degrade or impair an organizations resources. The fact that the attacker can make legitimate requests for web pages, files and objects is alarming, because an overwhelming number of requests causes the web services to focus a lot of its resources to the requests. The action could cause a denial of services to other resources legitimate users may need (MacVittie, 2008).

A denial of service in this type of attack is alarming, but what is even more alarming is that the attacker uses malicious code, such as malware and Trojans to deliver the bots to client and server systems, which are controlled by the attacker from a remote location to launch additional application layer HTTP GET requests. The result could potentially end up being a full blown distributed denial of service attack. The attack does not always have to be against the platforms that the attacker has infiltrated, instead it may be an attack on the website that is trying to respond to all the "Get" requests from different IP addresses (MacVittie, 2008).

Mitigation Techniques and Tools

Mitigating this type of attack can be a nightmare for a security professional, because of the legitimacy portion of the attack. A "deny all" for a specific IP address in a firewall access list may not be the best option because there are valid requests inter-mingled with the attacker's requests. In retrospect modifying the firewall to deny all would accomplish exactly what the attacker wants which is to deny or disrupt services. One method of mitigating this type of attack would be implement a form of traffic shaping that restricts the amount of HTTP GET requests users can make in a prescribed amount of time (MacVittie, 2008).

Per a white paper published on Cisco.com entitled “Defeating DDoS Attacks” suggests that mitigating the DDoS threat is built around four elements. First, mitigate the threat, not just detect it. Secondly, accurately distinguish good traffic from bad traffic to preserve business continuity, not just detect the overall presence of an attack. Thirdly, include performance and architecture to deploy upstream to protect all points of vulnerability. Finally, maintain reliable and cost-efficient scalability. The adoption of the four elements will enable a more defined response to DDoS attacks through an integrated approach that encompasses detection and blocking, provide better confirmation of attacks than firewall filtering or intrusion detection prevention systems (IDPS). Additionally, the use of behavior based anomaly recognition to differentiate legitimate traffic from that with malicious intent ("Defeating DDoS Attacks," 2014).

As DDoS threats continue to increase in frequency as well as sophistication, it is important for security professionals to adopt and implement a defense-in-depth strategy for dealing with this type of attack. It starts by changing our thought processes with regards to these types of attacks. Looking at the DoS threat from both inside and outside of the network is a good place to start. Attackers can launch malicious threats from different locations, which means that security professionals must think outside of the box in establishing countermeasures to protect the organization. The impact of DDoS attacks on organizations frequently appear in the headlines, but mitigation techniques still have a way to go.

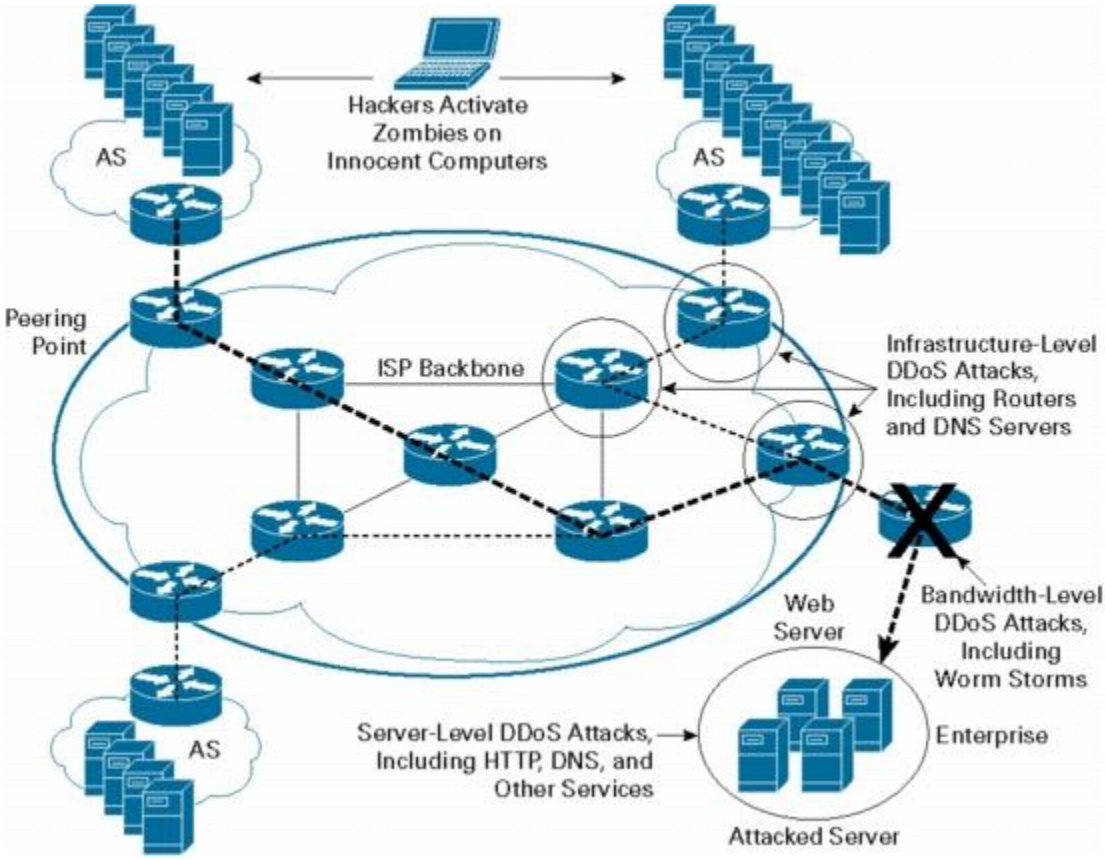

Figure 1- Examples of Distributed Denial of Service Attacks

("Defeating DDoS Attacks," 2014)

History of DDoS Attacks – a Timeline of the Biggest Attacks

Below is a timeline tracing DDoS attacks which caused enough damage to hit the headlines-

2000: Attacks on Amazon, eBay, Dell, Yahoo!, and CNN

A 15-year-old hacker, "MafiaBoy", brought down Amazon, eBay, Dell, CNN, and Yahoo! portals. The financial damaged was estimated at 1.2 billion dollars.

2001: Code Red

Code Red attacked computers running unpatched Microsoft's IIS web server. The White House portal, https://www/whitehouse.gov, was one of its victims and it left messages saying 'Hacked by Chinese'.

2003: SQL Slammer

This tiny "376 byte" worm managed to replicate itself with such effectiveness that it brought down the Internet and mobile telecom networks for several hours in South Korea.

2006: Estonia

This is possible the first time "criminal spammer botnets threatened the national security of a country"[5] The Internet was completely shut down and banks, media stations, newspapers, government sites – all came to a standstill on the day that Estonia was moving a politically charged statue from one location to another.

2010: Wikileaks

This is an early case of "hactivism". PayPal had suspended services to Wikileaks, and Wikileaks supporters retaliated by launching a successful DDoS attack on PayPal.

2011: Sony,

A DDoS attack on Sony was purportedly used to block detection of a data breach.

2012: DOJ

Hacktivist group "Anonymous" attacks the websites of the Department of Justice, CIA, and MI6.

2013: Spamhaus

The attack on the Dutch anti-spam site was the largest one, as of 2013.

2014: Attack on Hong Kong

Independent news site in Hong Kong: "AppleDaily" and "PopVote" were brought down by a massive attack launched for political reasons.

2015: GitHub

GitHub experienced outages across its network and China was suspected to be behind the attacks. [6]

2015: BBC

On New Year's Eve of 2015, the BBC was hit with the biggest DDoS attack till that date. A group called the “New World Hackers” [6] claimed they did it as a "test of power."

2016: Krebs on Security

The blog of security expert Brian Krebs was the victim of an IoT (Internet of Things) DDoS attack – the largest till date.

DDoS and Risk

The following are the reasons for increasing risk levels of a DDoS attack[7].

Attack Motivation

The timeline of DDoS attacks clearly shows the change in motivation. While the early attacks were launched by school kids and teenagers wanting “bragging rights”, the attacks quickly moved to “hactivism”, and is now an organized cybercrime by professional criminals, oftentimes State-sponsored.

Growth of Attack Size

The Mirai botnet was a 1.1 Tbps[8], and it launched the largest DDoS attack ever. The sizes of the attacks have been growing drastically over the last few years with the increase in cellular devices, and now, the “smart appliances” of the IoT world.

Increasing Complexity of Attacks

56% of attacks “multi-vector attacks that targeted infrastructure, applications and services simultaneously, up from 42% last year. 93% reported application-layer DDOS attacks.” [7] The most common service targeted by application-layer attacks is now DNS (rather than HTTP).

Targeting the Cloud

There is a sharp increase in data centers seeing outbound attacks from servers within their networks, and with increase in cloud services, the Cloud DDoS attack have grown.

Firewalls unable to withstand attacks

Studies show that "more than half of enterprise respondents reported a firewall failure as a result of a DDOS attack" [7]. Firewalls add to the attack surface, and in the first line of fire, and more of than now are unable to track an onslaught of connections and end up being the first victims of DDoS attacks. And as they are inline, they can also add network latency.

Impact of DDoS attacks

Analyzing a 2014 survey done by Incapsula Inc. on top US-based businesses which were victims of DDoS attacks, brings to lights important statistics and helps to quantify the risk, threats, and impact of DDoS attacks. [9]

Size of the Companies

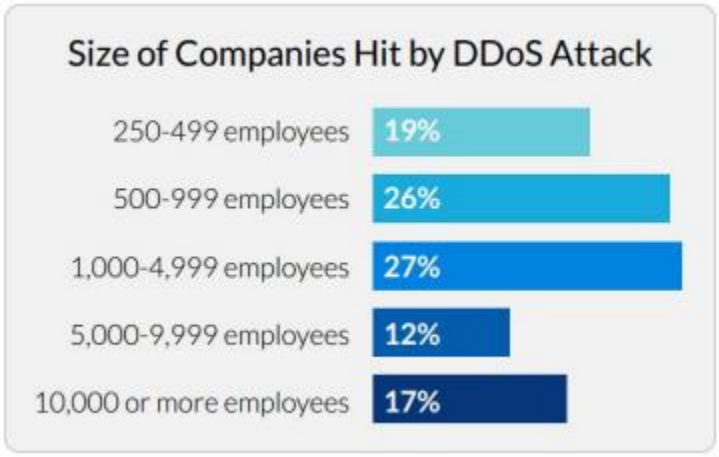

Figure 2 - Chart depicting the sizes of companies hit by DDoS Attacks

Duration of Attack

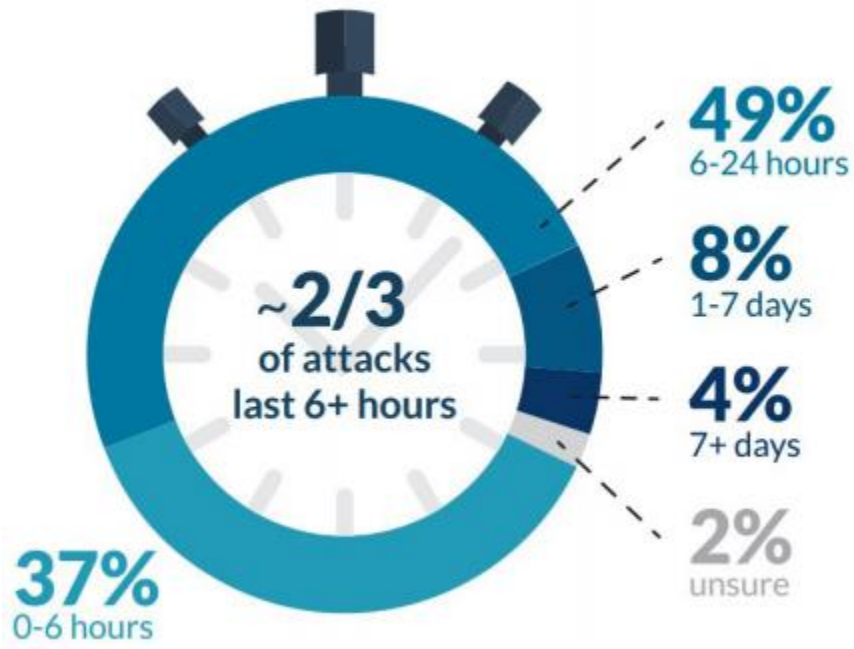

Figure 3- Chart depicting the duration of DDoS attacks

Intent of Attack

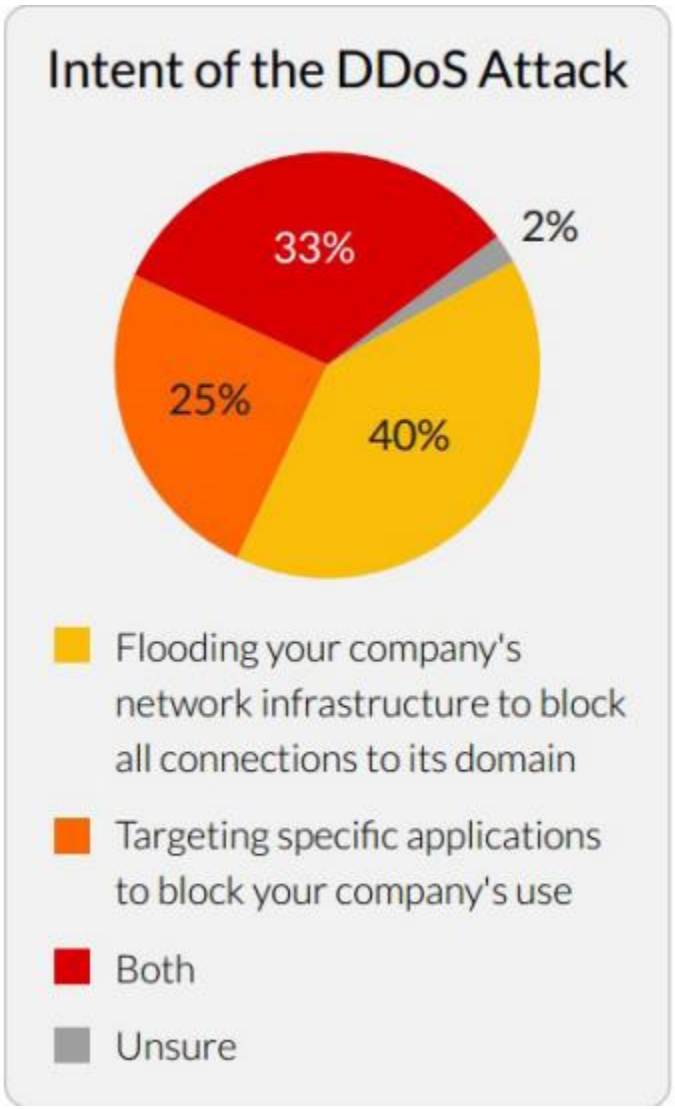

Figure 4 - Chart depicting the intent of the DDoS attacks

Cost and Losses

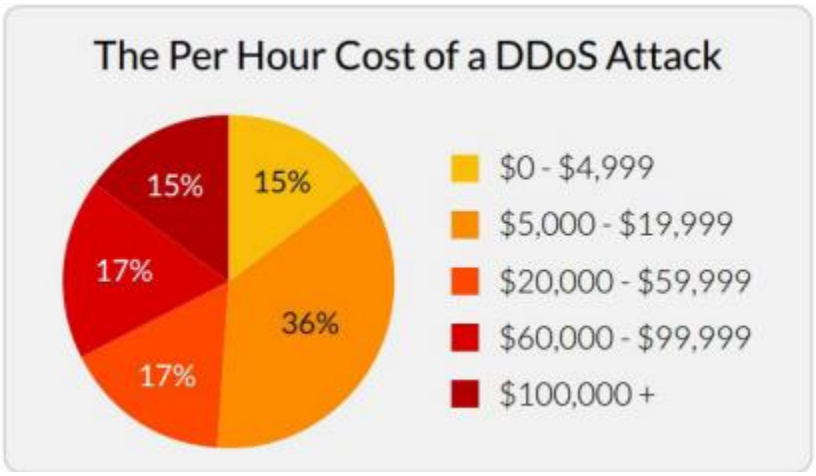

Figure 5 - Chart depicting the cost of a DDoS attack

Company Profile – Sector

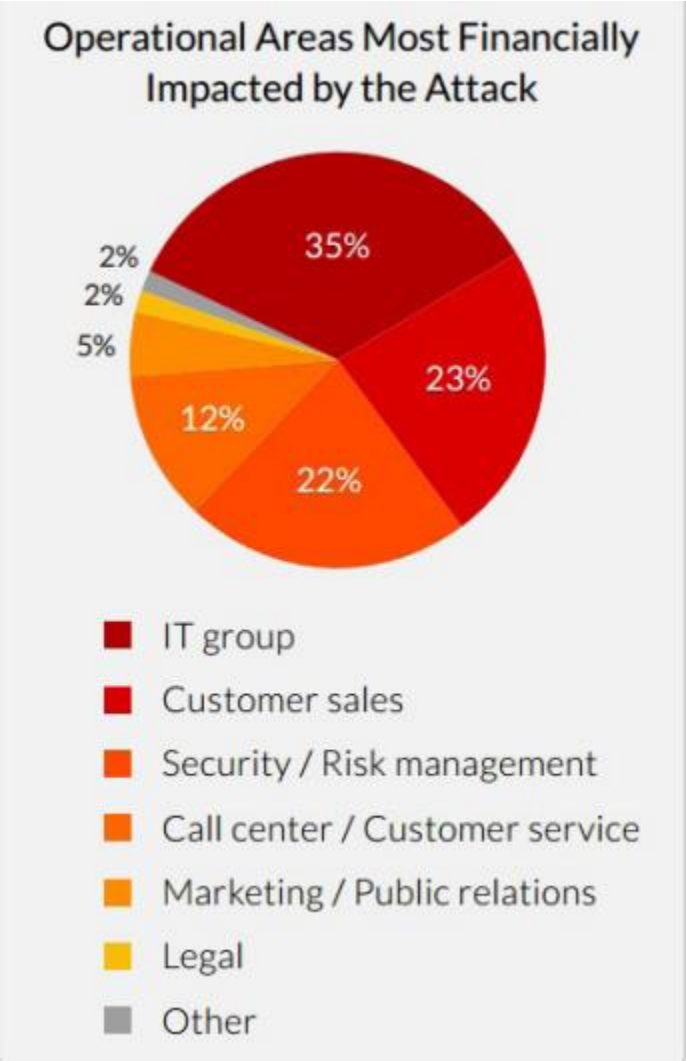

Figure 6 - Chart depicting the operation areas most financially impacted by the attack

The survey clearly shows that no company is safe from DDoS attacks and the costs and losses of their impact can be devastating – at an average of $40,000 per hour, and about $500,000 for the entire duration on one attack.

DDoS and the US Law

DDoS attacks may be subject to "civil and criminal liability, including fine and imprisonment, under state and federal law." [10]

Federal Law

The Computer Fraud and Abuse Act (CFAA) is a federal criminal law (18 U.S.C. § 1030) that makes unlawful certain computer-related activities involving the unauthorized access of: [11]

- Any computer to obtain certain types of prohibited information
- A protected computer, defined by the statute to include a computer used by or for the federal government or a financial institution, or in interstate or foreign commerce or communication.

State Law

The following 25 US states have laws that directly address denial of service attacks: [12] Alabama, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Mississippi, Missouri, Nevada, New Hampshire, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Tennessee, Virginia, Washington, West Virginia, and Wyoming

The Florida State Law[13] addresses this is in **Fla. Stat. § 815.06** which particularly refers to *"815.06 Offenses against users of computers, computer systems, computer networks, and electronic devices 2(b) Disrupts or denies or causes the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;"*

Future of DDoS Attacks

DDoS attacks target the "Availability" factor of the Information Security C-I-A triad. It is arguably "the easiest way to cause havoc and attack an organization"[14]. Underground networks and the dark web now offer "DDoS as a Service" and people without technical skills, can hire a

group of “expert hackers” to launch DDoS attacks. They can also lease out tools which will do the work for them.

The source code of the Mirai botnet which launched the biggest DDoS attack till date, was released on the Internet by the hackers. Within a couple of months, the IoT-targeting code was adapted to attack Windows systems and this code was released in the wild, as well.

DDoS attacks are here to stay and are growing in strength and size with each passing day. Companies should invest in resources, technical expertise, and infrastructure and guard themselves as the stakes are high, the costs due to losses higher, and it’s only a matter of time before they are targeted.

References

1. Defeating DDoS Attacks. (2014). Retrieved from http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html
2. Gibson, D. (2016). *Systems Security Certified Practitioner: All in One Exam Guide* (2nd ed.). NY: McGraw Hill Education.
3. MacVittie, L. (2008). Layer 4 vs Layer 7 DoS Attack. Retrieved from https://devcentral.f5.com/articles/layer-4-vs-layer-7-dos-attack
4. Weaver, R., Weaver, D., & Farwood, D. (2014). *Guide to Network Defense and Countermeasures* (3 ed.). Boston, MA: Course Technology, Cengage Learning.
5. Kaspersky, E. (2016, December 16). A Brief History of DDoS Attacks. Retrieved from https://eugene.kaspersky.com/2016/12/06/a-brief-history-of-ddos-attacks/
6. Knecht, T. (2016, August 29). 5 Biggest DDoS Attacks of The Past Decade. Retrieved from https://www.abusix.com/blog/5-biggest-ddos-attacks-of-the-past-decade
7. Arbor Networks Johannesburg, 23 May 2016. (2016, May 23). Understanding the risk and cost of a DDOS attack. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=152783
8. Mapping Mirai: A Botnet Case Study. (2016, October 05). Retrieved from https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html
9. © Incapsula, Inc. 2014 All Rights Reserv. (n.d.). What DDoS Attacks Really Cost Businesses. Retrieved from https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

10. Distributed Denial-of-Service (DDoS) Attack. (n.d.). Retrieved from http://us.practicallaw.com/7-516-9293
11. Computer Fraud and Abuse Act (CFAA). (n.d.). Retrieved from http://us.practicallaw.com/2-508-3428
12. (n.d.). Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#DDOS
13. Statutes & Constitution: View Statutes: Online Sunshine. (2017, March 19). Retrieved from http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899%2F0815%2F0815.html
14. Cooper, P. (2014, February 04). The future of DDoS, and how to stay ahead of attacks. Retrieved from http://www.itproportal.com/2014/02/04/the-future-of-ddos-and-how-to-stay-ahead-of-attacks/