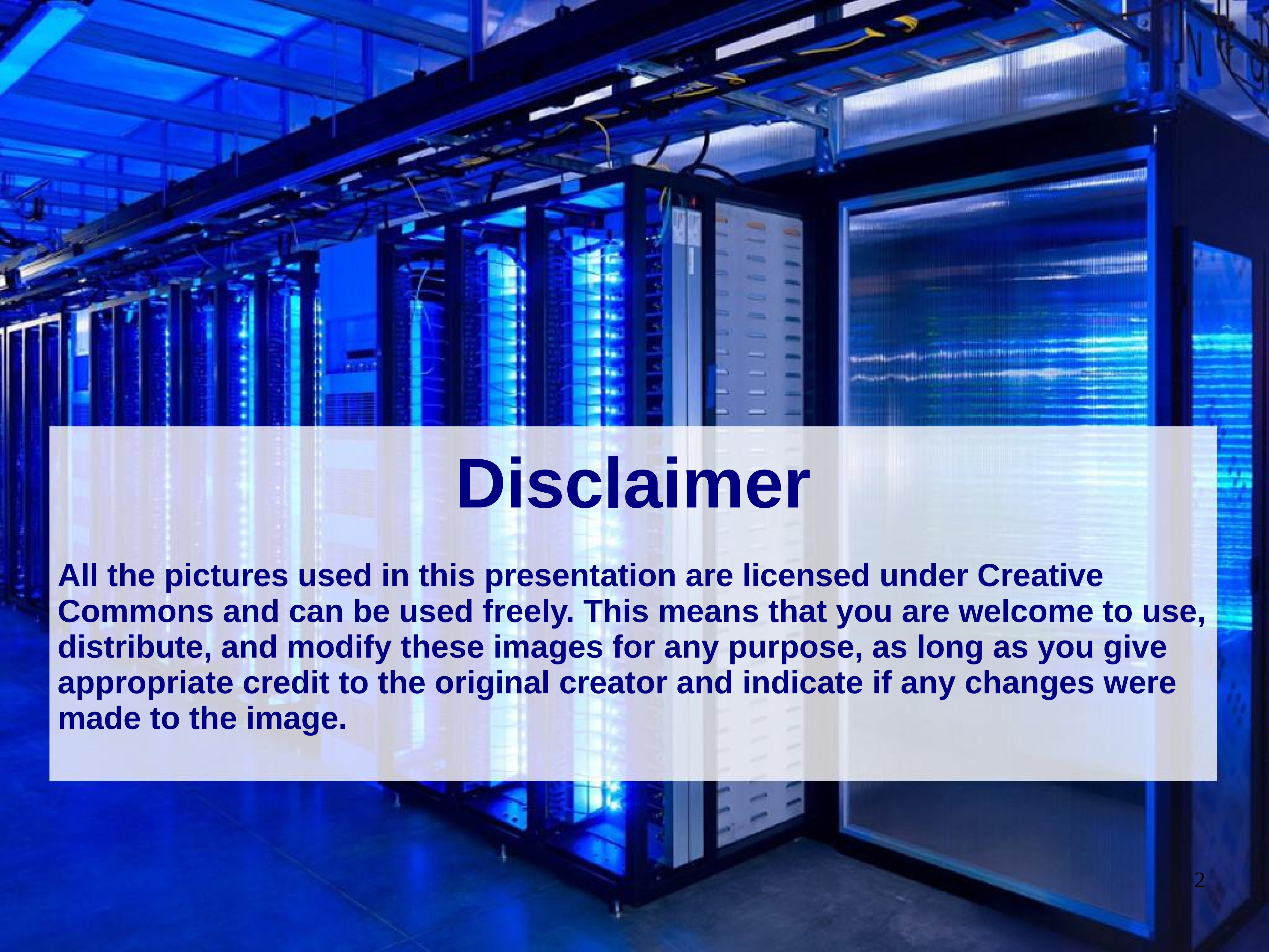
DDoS Attacks

Cryptography 2023

By Stefanos Anastasiades

AEM: 4023



Disclaimer

All the pictures used in this presentation are licensed under Creative Commons and can be used freely. This means that you are welcome to use, distribute, and modify these images for any purpose, as long as you give appropriate credit to the original creator and indicate if any changes were made to the image.

Contents

What is a DoS Attack?

- A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to it’s intended users

- DoS Attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash

- They are relatively simple to carry out, even by an unskilled attacker

- They often target web servers of high profile organizations

DoS Attacks

Two main types of DoS Attacks:

- *Overwhelming quantity of traffic* (flooding)
  Buffer overflow attacks such as ICMP Flood (also known as smurf attack or ping of death) and SYN Flood
- *Maliciously formatted packets* (crashing)
  Attacks that exploit vulnerabilities or bugs that cause the target system to crash

- A DoS Attack is carried out from a single source thus making it easier to pinpoint and defend against it for modern security technologies

What is a DDoS Attack?

A **Distributed-Denial-of-Service (DDoS) attack** occurs when multiple systems orchestrate a synchronized DoS attack to a single target

- The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once

- Modern security technologies have mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it’s still regarded as an elevated threat and is of high concern to organizations

DDoS Attacks

How do they work:

1. An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems

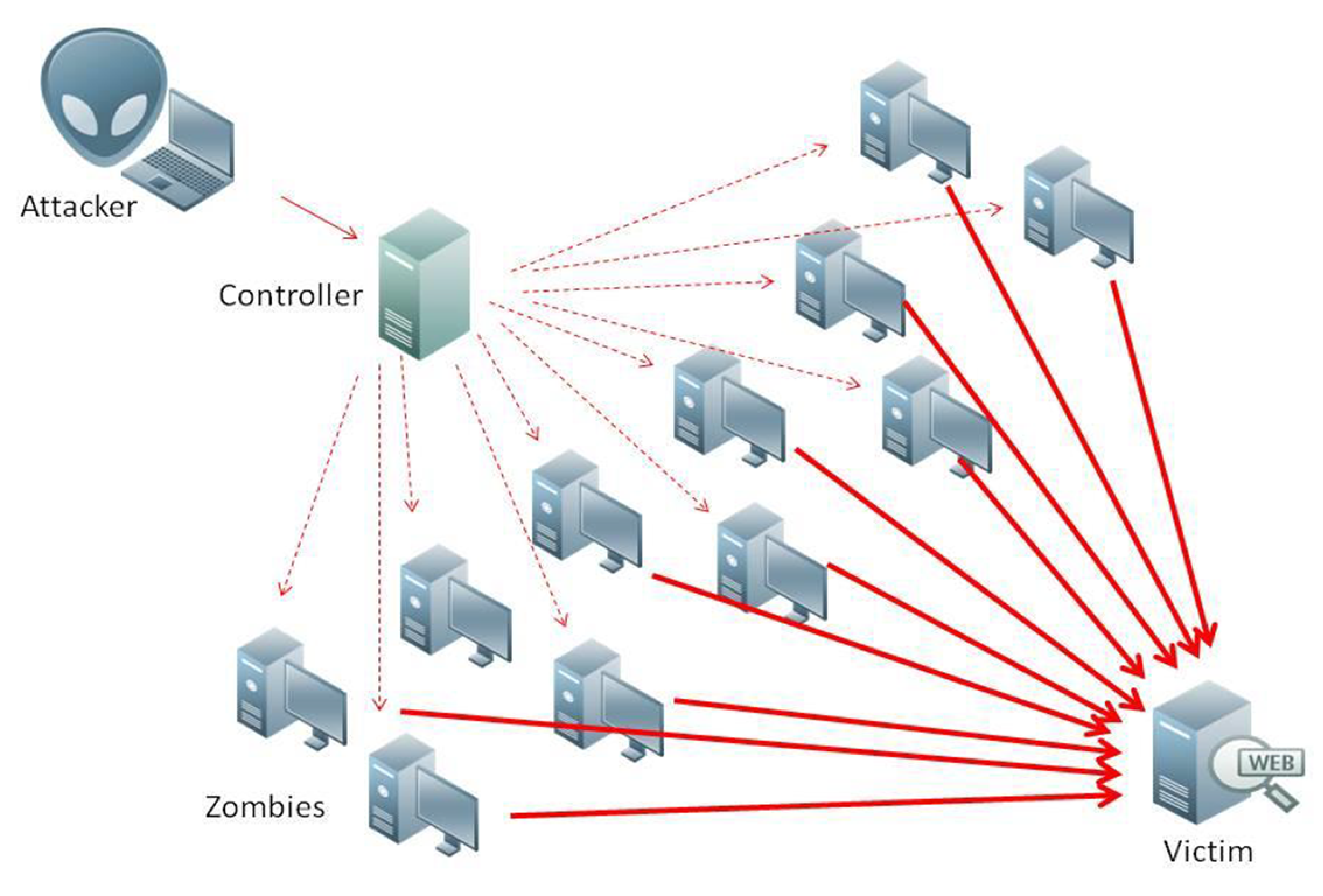
2. The zombie computers will constantly scan and infect more hosts, creating more and more zombies

3. When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack

DDoS Attacks

Attacker’s Advantages:

- He can leverage the greater volume of machine to execute a seriously disruptive attack
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)
- It’s more difficult to shut down multiple machines than one
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems


Attacker
Controller
Zombies
WEB
Victim

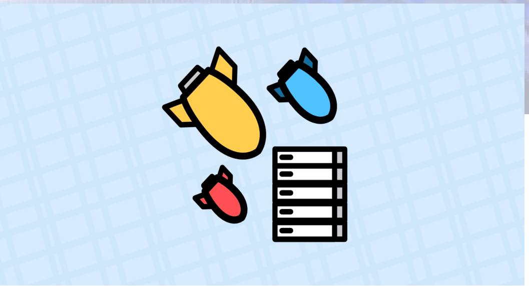
1. Use of Bots

- A DDoS botnet uses bots as part of a DDoS attack, overwhelming a target server or network with traffic from a large number of bots

- In such attacks, the bots themselves are not the target of the attack. Instead, the bots are used to flood some other remote target with traffic

- The attacker leverages the massive scale of the botnet to generate traffic that overwhelms the network and server resources of the target

2. Bruteforce Attack



- Unlike other types of cyberattacks, a DDoS attack does not typically employ a prolonged, stealthy approach

- Instead, a DDoS attack often takes the form of a highly visible bruteforce attack

- It is intended to rapidly cause damage to the victim’s network and systems infrastructure and to their business and reputation

3. Target

- DDoS attacks often target specific organizations for personal or political reasons, or to extort a ransom payment in exchange for stopping the attack

Aim of DDoS Attack:

1. Competitive advantage against rival business
2. Ransom demands for stopping the attack
3. Hacktivist behavior for protests and upstaging
4. For fun

4. Dual Risk

DDoS botnets represent a dual risk for organizations:

- The organization itself can be the target of a DDoS attack

- And even if the organization isn't the ultimate target, any infected endpoints participating in the attack will consume valuable network resources and facilitate a criminal act, albeit unwittingly

5. Targeted Strategy

- A DDoS attack can also be used as part of a targeted strategy for a later attack

- While the victim organization is busy defending against the DDoS attack and restoring the network and systems, the attacker can deliver an exploit to the victim network that will enable a malware infection and establish a foothold in the network

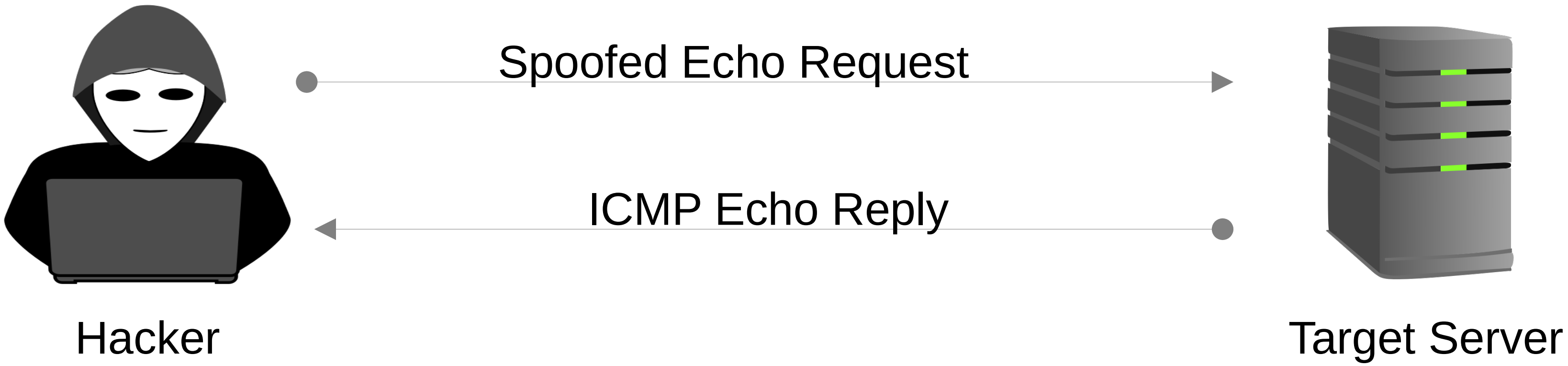
- The attacker can then return later to expand the (stealthy) attack and extract stolen data

Types of DDoS Attacks

1. Volumetric/Network Based Attack

These attacks focus on consuming all the bandwidth allocated to a server. A huge volume of requests are sent to the server which warrant a reply from the server and block all the bandwidth for regular users

Examples: UDP Floods, ICMP Echo Requests

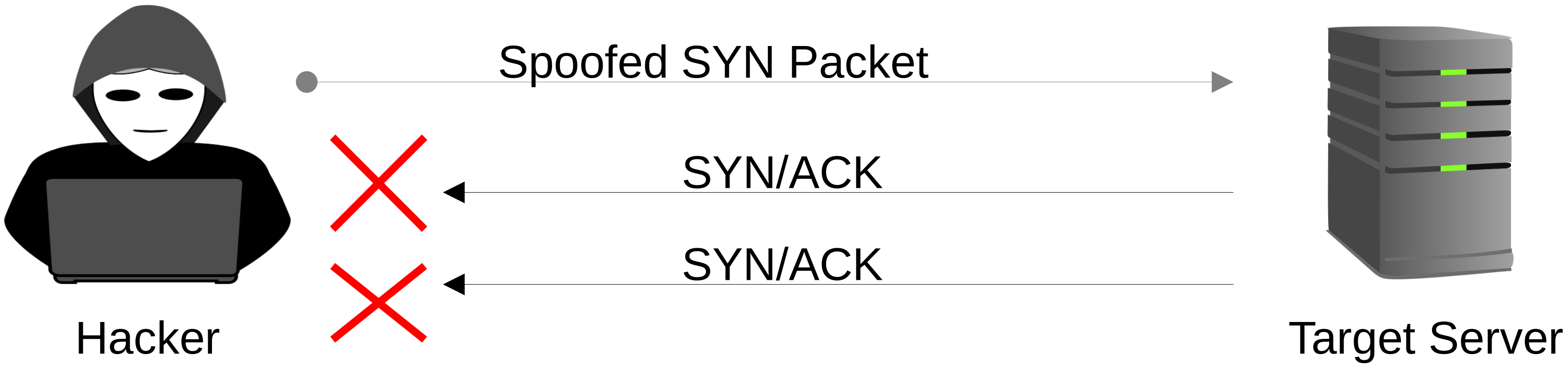


Types of DDoS Attacks

2. Protocol Based Attack

These consume the actual resources of a target by exhausting the firewalls and load balancers kept in place. Layers three and four of the OSI model are compromised.

Examples: SYN Flooding, Ping of Death

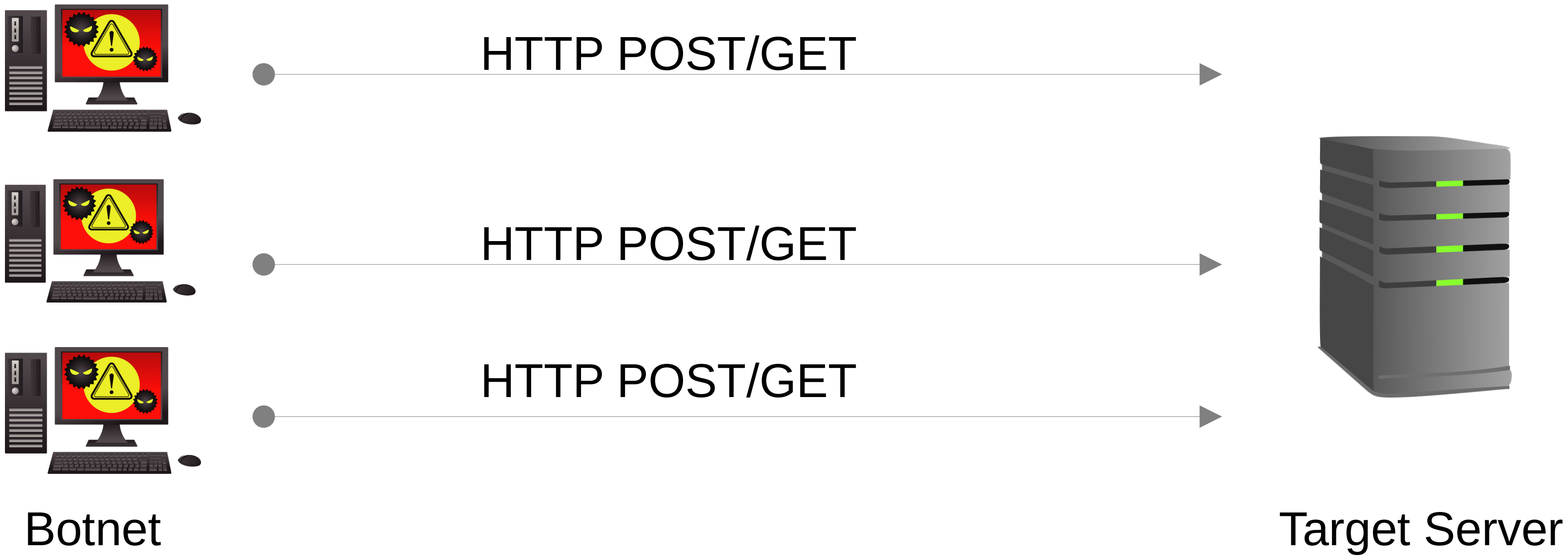


Types of DDoS Attacks

3. Application Based Attack

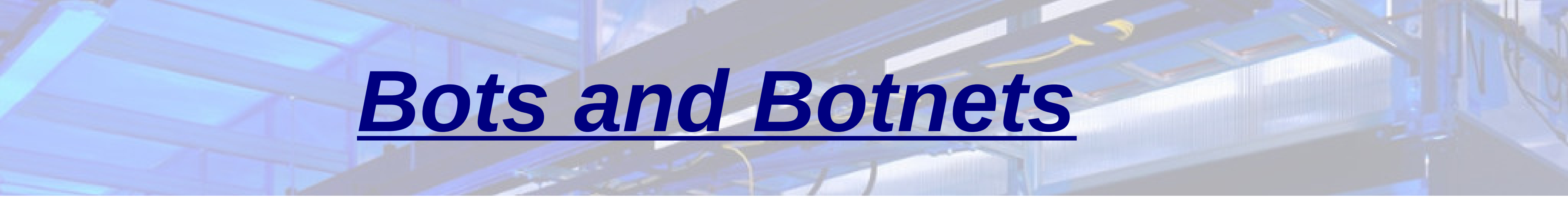
Sophisticated attacks that crash the entire server by targeting application and OS level vulnerabilities. It can stop specific applications from delivering necessary information.

Examples: HTTP Flooding, BGP Hijacking



Most Famous DDoS Attacks

- The **AWS** attack of February 2020 – 2.3 Tbps
  By using compromised CLDAP web servers
- The **GitHub** attack of February 2018 – 1.3 Tbps
  Lasted 20 minutes – Memcached DDoS attack
- The **Dyn** attack of October 2016
  Lasted 1 day – Mirai Botnet
- The **GitHub** attack of 2015
  Lasted several days – Originated from China
- The **Spamhaus** attack of 2013 – 300 Gbps
- The **Mafiaboy** attack of 2000 – 15 yo boy took down CNN, Dell, E-Trade, eBay and Yahoo
- The **Estonia** attack of 2007 – From Russia



Bots and Botnets

Bots

- Bots (or zombies) are individual endpoints that are infected with advanced malware (by visiting an unsafe website or opening an infected email attachment or infected media file) that enables an attacker to take control of the compromised endpoint

Botnets

- A botnet is a network of bots (often tens of thousands or more) working together under the control of attackers using numerous servers

Botnets

- In a botnet, advanced malware works together towards a common objective, with each bot growing the power and destructiveness of it

- The botnet can evolve to pursue new goals or adapt as different security countermeasures are deployed

- Communication between the individual bots and the larger botnet through C2 (Command and Control) servers provides resiliency

Botnets

- Given their flexibility and ability to evade defenses, botnets present a significant threat to organizations

- The ultimate impact of a botnet is largely left up to the attacker, from sending spam one day to stealing credit card data the next

- Because many cyberattacks go undetected for months or even years, botnets can cause a great deal of damage

Botnets

- Botnets are dubious sources of income for cybercriminals
- They are created by them to harvest computing resources (bots)
- Control of botnets (through C2 servers) can then be sold or rented out to other cybercriminals

Example: Rustock Botnet

- The Rustock botnet is an example of a spamming botnet. It could send up to to 25,000 spam email messages per hour from an individual bot. At it’s peak, it sent an average of 192 spam emails per minute per bot. Rustock is estimated to have infected more than 2.4 million computers worldwide. In March 2011, the FBI working with Microsoft and others, was able to take down the Rustock botnet. By then, the botnet had operated for more than five years. At the time, it was responsible for sending up to 60 percent of the world’s spam

Biggest Botnets of all time

- ***ZeuS*** (2007-present) – Banking Trojan
  Over 13 million bots in 196 countries
- ***Storm*** (2007-2008) – email worm (spam/DDoS)
  About 2 million bots
- ***Mariposa*** (2009-2011) – Trojan/worm
  12m + 11m bots (2 outbreaks) in 190 countries
- **ZeroAccess** (2011-2013) – Trojan downloader, spamming malware, coin miner – 9 million bots
- ***Dridex*** (2011-present) – Banking Trojan
  Unknown number of bots
- ***Emotet*** (2014-present) – Banking Trojan, Malware loader
  Unknown number of bots
- ***3ve*** (2013-2018) – Click fraud botnet
  About 2 million bots
- ***Mirai*** (2016-present) – DDoS botnet
  At least 560,000 bots

Disabling a Botnet

- The key to “taking down” or “decapitating” a botnet is to separate the bots (hosts) from their brains (C2 servers)

- If the bots cannot get to their servers, they cannot get new instructions, upload stolen data, or do anything that makes botnets so unique and dangerous

- Disabling a botnet presents many challenges and almost always requires enormous amount of investigation, expertise and coordination between numerous industry, security and law enforcement organizations worldwide

How to prevent DDoS Attacks

At individual level:

1. Protect your devices with the latest security software
2. Watch out for phishing scams – even ones seemingly from friends or family
3. Be mindful of the websites you visit and always verify links before you click

→While your own personal experience in a DDoS attack is nothing more than the inconvenience of a downed website, there is always a risk your device could be one of the many that's used as part of a bot army. Antivirus software will help not only to keep your devices safe from malware, but to prevent future DDoS attacks

How to prevent DDoS Attacks

At organizational level:

1. Employ load balancers and firewalls
2. Detect an attack early and mitigate the damage beyond that point
3. Switch to cloud service providers like AWS and Azure
4. Allocate more bandwidth to prevent clogging of data
5. Using Content Delivery Networks (CDNs) that have redundant servers

Sources

Introduction to Cybersecurity Course by Palo Alto Networks at https://beacon.paloaltonetworks.com/
Introduction to Cybersecurity Course by Cisco at https://skillsforall.com/
https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
https://cybernews.com/security/the-8-biggest-botnets-of-all-time/
https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/top-5-most-famous-ddos-attacks
https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

Video Sources

https://youtu.be/ilhGh9CEIwM
https://youtu.be/JZY6_Ws6sKE

Image Sources

https://openverse.org/search/?q=ddos%20attack&license_type=commercial,modification
https://freesvg.org/computer-server-vector-image
https://freesvg.org/anonymous-hacker-vector-image
https://creazilla.com/nodes/36230-computer-virus-pc-clipart
https://commons.wikimedia.org/wiki/File:How-to-stop-a-ddos-attack.png