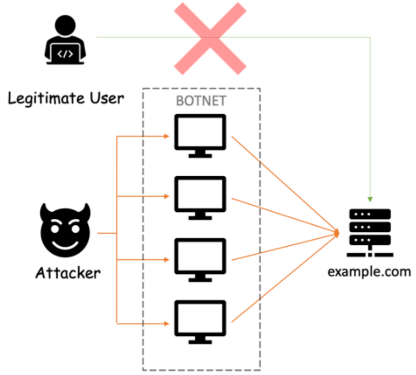
## What is Distributed Denial of Service [DDoS] ?



It is an attack towards the service that is exposed via the Internet to deliberately make it unavailable for legitimate users.

## How DDoS attack is performed?

By overwhelming the target service by sending a larger number of packets from the malware-infected devices.

So that legitimate user is blocked.
[no resources available at the target service to process the request from legitimate users]

## What kind of devices are used as the sources of the attack?

**BOTNET !**

The group of malware-affected devices
is called as
BotNet.

## ! ! ! Quick Mitigation ! ! ! => Scaling up services

One can say that, in the cloud computing world, resources are unlimited. We can keep scale our services horizontally to make it available for legitimate users.

True! => This is one of a mitigation techniques.
**But unlimited resources do not come for free.** More the computing resources we utilize the more we have to pay!
(To be continued…)

## It is that 'easy' to perform DDoS attacks?

Yes!

A person who wants to perform the attack need not be a geek in all technologies that are used in the product, he just needs to have some basic knowledge on ways to perform the attack. If security is not considered as part of our service development, then it is hard to mitigate such attacks.

## Who would be interested in such attacks?

- Criminals 😡who would demand money once they were able to attack successfully. => not to perform attack again/to stop the attack.

[no guarantee that they will not attack again once they are paid, so don't pay instead start gathering information to take legal actions against them]

- Thrill-seekers 😎 who wanted to prove that they have the entire power in the world to stop your business.

- Angry customers [or] ex-employee 😠 of the company who is not in alignment with your business policies.

## !!! Popular Attacks !!!

## "Mirai"

This attack takes a simple route.

#1 With the help of malicious affected devices, it scans for the IP addresses of IoT devices on the Internet.

#2 Try to establish a connection with the default username and password that comes with factory settings of the IoT devices.

#3 Then inject malicious software into the vulnerable IoT devices and turn it into weapons for attacking services.

## How to mitigate attacks like "Mirai"?

First and foremost thing, change the default password to something that is difficult to crack.

🤓

(To be continued...)