What is a (D)DoS

2026-06-20

Non-technical (D)DoS overview: how denial-of-service attacks operate at the Business, Social, and Informational level, and what protection looks like at each.

(D)DoS attacks are not just a technical problem — they operate at the Business, Social, and Informational level as well. This post covers the non-technical dimensions; the technical follow-up covers Layer 3/4 network floods, BGP hijacking, TLS handshake attacks, Layer 7 application DDoS, and operational resilience.

Originally published at opensourcerers.org; updated with current examples and expanded framing.

Series navigation: - **Part 1 — Non-technical: Business, Social, Informational (this post)** - Part 2 — Technical: Network floods, BGP hijacking, Layer 7, Resilience - Part 3 — Application Security

> **i Scope note**
>
> This article uses the term "Denial of Service" in a broader sense than the usual network-security definition. It covers Business, Social, and Informational disruption — not just the network-layer attacks most readers associate with DDoS.

Introduction

The topic "Denial of Service" (DoS) and "Distributed Denial of Service" (DDoS) is always a hot topic because it could happen at any time for any Service at any Level. To understand what a (D)DoS is, let us explain what a "Service" is, what possible attacks are available and why such a denial of service attack could happen at any time for any Service.

Let us try to bring several perspectives to that topic because a Service has several levels by default.

- **Business Level**. This is the cash point, why any service is offered to people.
- **Informational**. News and other information services to distribute information.
- **Social**. These are the People behind the other levels. They provide and ensure the service.
- **Technical Level**. The technical implementation and the workhorse where the attacks most of the time happen. We will dive into this topic in a dedicated Blog post.

Scenario

The goal of a (D)DoS is to deny the delivery of the service to the end user.

This can happen in many different ways as we will see in this article when I explain it with the different levels. But an easy example would be to just shut down the HTTP Endpoint which is serving the website. So the end user can't reach the service.

An easy example for a DDoS would be (if we assume a service which can take n Requests per second) to create n requests per second from different devices.

Key difference between DoS and DDoS: DDoS has a lot of distributed infrastructure on the attacker side and it always has a “bruteforce” aspect in overloading the service.

The picture tries to highlight the different aspects of a (D)DoS attack. You can see here the target which should come down, the different devices and controller, IT, human, and some involved technologies.

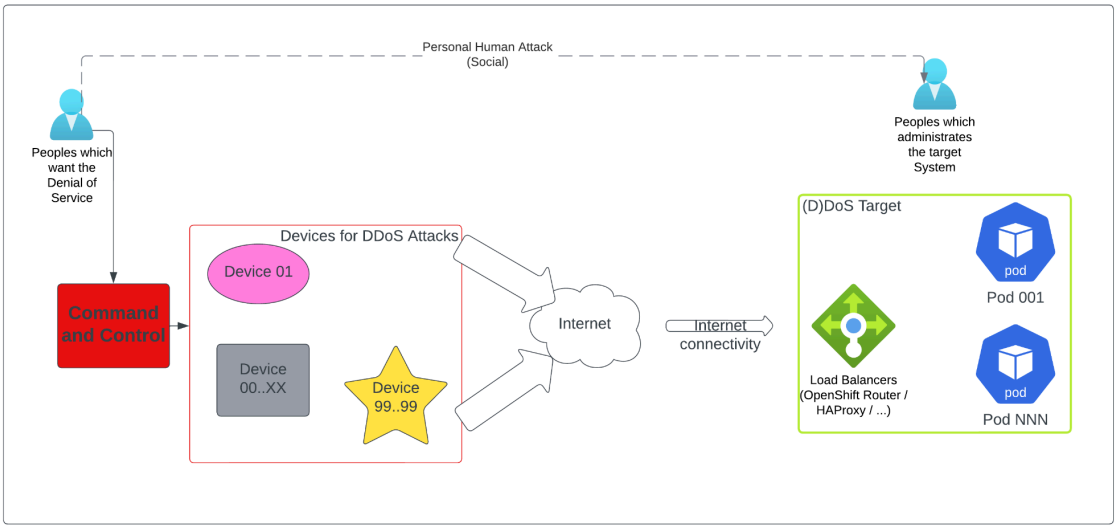

Figure 1: DDoS attack overview: target, devices, command and control structure

In the picture you can see on the left hand side the people who want the service to not be working, which is the main goal for a (D)DoS. The people manage the “Command and Control” part which controls the different devices in the “Devices for DDoS Attacks” Box. All devices are mostly connected via the internet to attack the target service. The attacked service could implement different defense strategies which will be shown in the next article covering the (D)DoS topic.

Business

The Business Service is the main point for a company to gain money to be able to pay the people who work for the company and all other expenses which a business oriented company has.
A denial of service from a business point of view could be to offer the people who work for the company a much better service (higher salary, social service, family offering, ...) so that they leave the company and much less people have to do the job for more people or attack any other business relevant part which is important for the business. This aspect is not very often shown in the context of a (D)DoS attack but that’s, from my point of view, the most threatening point of a (D)DoS attack at every level. The reason for that is that the recovery time from such an attack is quite high because the lack of people who know the setup, the tools and all parts of the service to keep the service up and working could be gone.

I'd call this an **organizational denial of service** — or **service disruption through organizational means** — to make it explicit that this is an intentional extension of the DDoS threat model. The mechanism is real, but the attack surface is human and organizational rather than technical.

Another aspect for this attack requires a very good knowledge of the field of the business in which the company works which leads to a relatively high amount of work for the attacks and in some cases a high investment of money. These facts lead to the conclusion that such an attack requires some preparation time in the real world compared to the technical attack which could be mostly done in the digital world.

The Business kind of attack is a disaster because it could bring the company down as there could be no income when a service isn't reachable or usable for paying customers.

Possible Protection

Well, the protection against such an attack is quite difficult as the attacking party is not always known. My experience is to handle people with respect and honor their work as you never know when you meet the people again or what upset humans to think or in the worst case start such an attack.

Social

Even though that's not a commonly agreed DoS attack, let me bring this on the table as still most of the administration personnel are humans, nowadays. There is a long history of social hacking just because the attack uses humans' deeply integrated emotions. We would also like to show that such an attack is a valid point of view and could have a deep impact on the company's business and existence.

The scenario is that an attack group or person recognizes who the administration person of a service is and manipulates the administrative person in that kind to impact the service in a bad manner. That this is not just a hypothetical scenario can be proved with your favorite search engine.

AI-assisted social engineering is already being used at scale in phishing and targeted manipulation campaigns, although fully autonomous attacks remain limited. AI systems themselves have also become an attack surface: prompt injection and model manipulation are emerging vectors worth keeping in mind.

Possible Protection

The protection against such an attack is somehow possible **if** the attacking party is known. Some people have a gut feeling that something is wrong, and if trust levels within the company are high enough, they will communicate with colleagues and supervisors to get help against such an attack. Here is also my experience: people who feel respected and valued are far less likely to become a threat — the same principle that applies at the Business level.

As you have read this several times in this post and you might think "I do this already in my company or community" be brave and make a real anonymous survey how satisfied and happy the people are in the company or community

Informational

The last kind of (D)DoS in this article is the Information Level. There is something called Information Warfare which could be seen as (D)DoS from my point of view as when information is spread that a company's business is in a "bad" state, customers end their relationship with the company, which results in less income and leads directly to possible company closure.

Possible Protection

The protection against such an attack is very hard nowadays. Fast Information updates are only possible where the attacked company or community have access to the Information platform. The current social media platforms are widely used but clarifications from the attacked side could be overlooked.

Conclusion

As you have seen in this blog post the topic (D)DoS is not only a technical topic but also a business and social one. That's one of the reasons why I think that security is not only a topic for some people of a company or community, it's the topic for all people from top to down, down to top, left to right and right to left.

Even though these posts originate from 2023/2024, the topic remains highly relevant. AI crawlers in particular have become a new variant of this problem: aggressive indexing bots generate high request volumes from distributed infrastructure, hitting smaller sites in a way that is functionally indistinguishable from a classic volumetric DDoS — the same mitigation techniques (rate limiting, WAF, connection throttling) apply.

In the next blog post you will see the technical part and some ways to protect yourself against a technical (D)DoS attack.