Why Would Anyone Bomb Me?

In this lesson, we'll explore the reasons why someone would want to take a website down.

Why would anyone want a website taken down?

There are a number of reasons someone would want to take a website down: maybe they're a competitor with bad ethics, or simply a malicious person looking for a quick buck in the form of ransom. DDoS can be used to shut down political websites that might not be in line with a government's view, or even against sites of dubious morals.

> ## **i** Defending dubious morals
>
> Cloudflare was at the epicenter of a widely publicized story around their protection of a site known as "The Daily Stormer", which promoted repugnant and disgusting content I won't discuss further in this course.
>
> While many have applauded Cloudflare for taking action, I want to highlight their response to this entire incident in which they argued it should not be their job to regulate what content is available online. It sheds some light on a very important topic and I would recommend everyone read through their reasoning and some of the reactions they've received:
>
> - cloudflare.com/cloudflare-criticism/
> - blog.cloudflare.com/why-we-terminated-daily-stormer/

DDoS attacks are cheap and easy to execute

Unfortunately, the cost of a DDoS attack is painfully low as computing power has gotten cheaper and cheaper over time. One could order a DDoS attack with a bandwidth of 125 Gbps for around five minutes for around $5, all available on the black market.

In "The Cost of Launching a DDoS Attack", Kaspersky highlights how attacks have gotten extremely easy to order online, with a very low entry price and the potential to cause huge losses for the target. It is estimated that the cost of DDoS attacks for SMEs is around $120.000 per attack, reaching up to $2 million for large enterprises.

In the next lesson, we'll look at a few notable DDoS attacks.