This is a true story about fighting against a large-scale DDoS attack.  
.  
.  
Written by [Sahn Lam](https://www.linkedin.com/in/ACoAAAMfZ70B-6p6akpK0O36okeb8JYUJjRC7HA)  
  
One memorable challenge at Zynga Poker back in the day was the battles against distributed denial-of-service (DDoS) attacks. Why would anyone DDoS a poker game, you might ask?   
  
Here is one of the many reasons: When the stake is high, an attacker would perform DDoS a table to block anyone from sending in continuation bets, which resulted in an automatic forfeit after the timer runs out.  
  
How does a DDoS attack work? The malicious goal of a DDoS attack is to disrupt the normal flow of traffic to a service. This is done by sending a large volume of attack traffic to the victim using a large group of compromised network-connected devices. These compromised devices are called a botnet. They are computers and IoT devices infected by malware which allows them to be controlled by an attacker.  
  
How does a service know it is under a DDoS attack? It is not easy to tell. DDoS traffic comes in many forms. A sophisticated DDoS attack employs several of them simultaneously to try to blend in with the normal traffic, making it difficult for an operator to mitigate without harming real users.  
  
What are some of the common attacks?  
  
- A HTTP flood attacks the application layer by sending the victim a large number of HTTP requests from the botnet.  
  
- A SYN flood exploits a weakness of the TCP layer by sending a large number of TCP SYN packets with spoofed source IP addresses. When the victim responds to each request, the response never returns, exhausting the precious resources.  
  
- A DNS amplification attack sends a large volume of DNS requests to open DNS servers from the botnet but with the return address pointed at the victim. The large volume of DNS responses clogs up the victim’s network.  
  
While there are many ways to mitigate an attack, the most effective strategy is to have a huge network capacity to absorb the attack. One approach that has been effectively deployed at services like Cloudflare is to use an Anycast network to scatter the attack traffic across a huge network of distributed servers. This technique spreads the impact of attack traffic across many servers, rendering it ineffective.  
  
Had Cloudflare existed back in the days the battle with Zynga Poker hackers would have been a bit easier.  
  
Image source: <https://lnkd.in/eAysfnav>  
  
—  
Subscribe to our weekly system design newsletter (10-min read): <https://bit.ly/3FEGliw>  
   
[#systemdesign](https://www.linkedin.com/feed/hashtag/?keywords=systemdesign&highlightedUpdateUrns=urn%3Ali%3Aactivity%3A6942140124247822336) [#coding](https://www.linkedin.com/feed/hashtag/?keywords=coding&highlightedUpdateUrns=urn%3Ali%3Aactivity%3A6942140124247822336) [#interviewtips](https://www.linkedin.com/feed/hashtag/?keywords=interviewtips&highlightedUpdateUrns=urn%3Ali%3Aactivity%3A6942140124247822336)  
.

