What is a DDoS Attack?

A DDoS (Distributed Denial of Service) is a kind of Denial of Service (DoS) attack. As the name implies, a DoS simply tries to prevent a service from working. In a DDoS, the attacker uses a large number of machines from all over the Internet to send enormous amounts of traffic towards the target. Usually, the source of the traffic is a network of compromised “zombie” computers (also known as a botnet) that send the traffic.

There are different techniques attackers can use to take down different parts of their target’s system. Some attacks focus mainly on overwhelming the server and slowing response times while others target specific applications. DNS attacks can be particularly harmful because without DNS, your website, applications, email, etc. are rendered useless.

Why Should I Be Aware Of DDoS Attacks?

Hacker forums, blogs, and even YouTube share easily accessible information on how to set up a DDoS attack, making it so that practically anyone with an Internet connection can launch their own attack. Attackers can rent botnets or purchase relatively cheap tools to launch their attack.

Due to the growing ease of launching DDoS attacks, the number of attacks is also on the rise. In 2012, there was a 53% increase in the total number of DDoS attacks over 2011 with a 1.9% increase in total DNS attacks.

DDoS attacks are not only obnoxious to deal with, but they can be a great detriment to your company. Companies that have undergone DDoS attacks have experienced the following:

**Loss of Income** [see sidebar]

For ecommerce giants, just a second of downtime could mean thousands in lost revenue. Even if your company isn’t an Amazon or eBay, profit loss due to downtime is nothing to scoff at. Not only do you miss a potential sale in real time, that customer is less likely to come back and try to purchase from you again in the future.

**Brand Damage**

If people are trying to reach your website and they are greeted with an error message, they probably won’t immediately think, “No problem. They must be under a DDoS attack.” They may simply feel that your site is unreliable and might just avoid ever visiting it again. Press surrounding DDoS attacks can also paint a bad picture for your brand. If the driving force behind the attack was based on political or moral agendas, your brand could acquire a negative image because it was one of the attacker’s targets.

**Loss of Customer Confidence**

Just as your brand image may deteriorate in the public eye, your customers may also lose confidence in your company. If you have a web service-based

---

**In 2010, 412 of the top ecommerce websites experienced:**

- **840 minutes** was the median downtime
- **3,291 minutes** was the average downtime
- **1,343,643** total minutes of downtime
- **$800,099** average revenue lost during downtime
- **$329,640,928** total revenue lost due to website downtime
P3: What is a DDoS Attack?

into what is happening, and it is reasonable to expect an attack is the cause.
Additionally, if the same source address is querying for the same data long
before the Time to Live (TTL) has passed, it could be a sign that they are not a
“normal” full-service resolver and are up to no good.
Unfortunately, you cannot simply check to see if all of the traffic is coming
from one IP, as this is the exact purpose of a DDoS: to have traffic coming from
multiple sources.

How Can I Survive A DDoS Attack?

There are a few different routes you can take in order to mitigate an attack with
some more effective than others.

Your ISP will most likely offer DDoS mitigation but if your traffic grows too
large and starts affecting their other customers, or if the attack is too compli-
cated, they may just turn you off.

If you would rather handle the mitigation in-house, you can buy your own
hardware, which can be very expensive. Also, a specialized team is also neces-

sary to successfully mitigate the attack and a great deal of available bandwidth
is required to make the attack go unnoticed by your end users.

Your best bet in mitigating an attack is to outsource to a service provider. A
managed DNS provider can redirect site visitors to hosts that aren’t down with
advanced features like load balancing and performance monitoring. Also, most
managed DNS providers are able to integrate with cloud providers, allowing
you to use additional resources to handle the load from the attack.

Key Takeaways

The best way to avoid any disruption from a DDoS attack is to be prepared for
it. Talk to your DNS provider and ask about their mitigation techniques, and
if you currently are doing everything in-house or are relying on your ISP or a
firewall, evaluate your situation. Do you feel confident that what you have in
place can successfully mitigate an attack?

If you are having a hard time deciding whether or not you actually need to
invest in a stronger mitigation technique (e.g. you believe your industry or
business is at a low risk of an attack), figure out the impact it would have on
your company financially if it were to happen. Although it may not be an
apparent risk, the cost associated with being attacked is usually much higher
than the cost to take safeguards.