Dyn

/delivers/

WHITEPAPER

Everything You Need To Know About 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 inexpensive 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

For ecommerce giants, just a second of downtime could mean thousands in lost revenue. Even if your company isn't as large as Amazon or eBay, any amount of profit loss due to downtime should be cause for concern. 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.

2012: TOP ECOMMERCE SITES GET HIT HARD BY DOWNTIME

1,102,919
total minutes
of downtime

3,421
average minutes
per company

$866,038,469
in total
lost revenue

$1,890,913
average lost
per company[3]

Brand Damage
If potential customers are trying to reach your website and are greeted with an error message, they probably won't immediately assume that the site is under a DDoS attack. They will most likely assume that there is something wrong with the development of the website itself and may feel that it is unreliable, making them less likely to return. 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 company (think web hosts) and if your servers go down due to an attack, all of your customers' websites go down as well. It can take only a few moments of downtime a year to provoke a customer to move to another service provider.

Personnel Cost
The time spent by your personnel to investigate and mitigate an attack can be costly. Time spent by your operations team dealing with an attack only takes away from their normal work. Similarly, your help desk will also see an influx of calls and tickets due to questions surrounding access during downtime. All of these extra hours can massively add up over the duration of an attack.

How Can I Reduce The Threat Of An Attack?

Don't make yourself a target Keep your network clean of spammers and other miscreants that make trouble. You're less likely to get wrapped up in their shenanigans.

Awareness
Know your network's normal behavior, so you can know when you come under a DDoS. There are many tools that can help you do this: InternetSeer, NetFlow, sFlow, Splunk, Nagios, Cacti, Smokeping, Munin, DSC, and others.

Capacity
If possible, build the biggest network you can with effective elements for installing wire speed access control lists at the edge of your network for mitigation. Create a deep packet inspection/caching/scrubbing layer in the core

of the network for advanced mitigation. Finally, make sure you provision enough server capacity and tune for best performance under high load.

Practice Your Defense Plans

Knowing how to use your defensive strategy is just as important as buying and installing it. If you don't know how to use it effectively, why even have it? Practice the drills over and over to get this committed to your staff's minds. There's too much at stake to not go through the process.

How Do I Know If I'm Being Attacked?

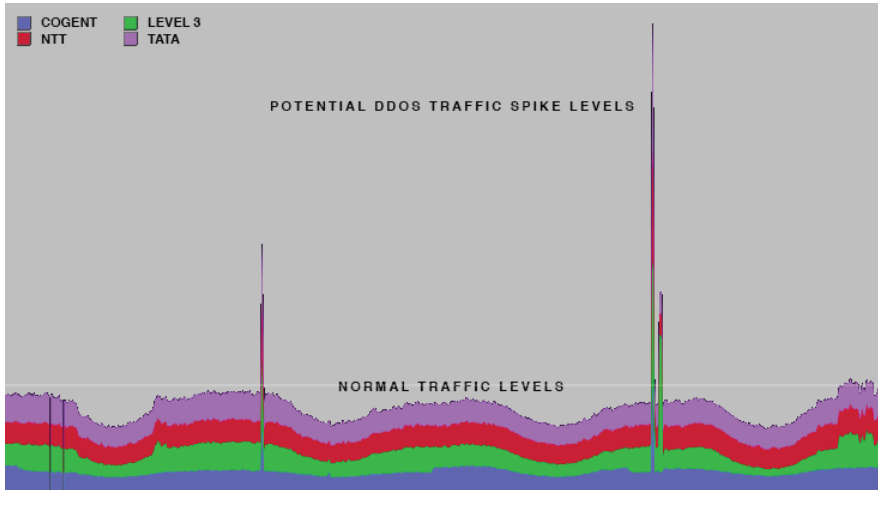
Sometimes it may be difficult to distinguish legitimate traffic from a DDoS attack. If your website gets mentioned on the most popular TV show in America,there's a good chance you will receive a large boost in overall traffic. If you're not prepared for spikes of such magnitude, your website might react in a way similar to if it was undergoing a DDoS attack.

So how can you tell the difference? If slowed or denied service continues for a period of time that seems too long to be simply caused by heavy traffic (a few days rather than a spike during a campaign), it is time for you to start to look 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.

Network monitoring graph with normal & DDoS traffic shown



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 complicated, 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 necessary 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.

BONUS BLOG CONTENT

How BCP38 Can Help

And why you shouldn't blame open recursives for DDoS attacks

dyn.com/bcpblog

Want a drastic increase in your website's performance? Contact us to get started.

dyn.com sales@dyn.com +1 888 840 3258 150 Dow Street, Manchester, NH 03101 USA