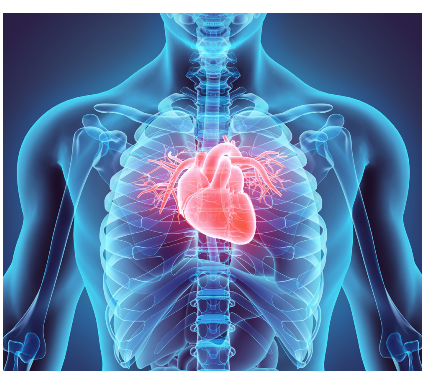
The Anatomy of a DDoS Attack

March 16, 2017
by SentinelOne

Distributed denial of service or DDoS attacks are a big deal in today's cybersecurity world. Time and time again, you'll hear about a DDoS attack that took down a website or part of a company or government system.

So what do these attacks do? What is a DDoS Attack?



Behind the fancy name of "distributed denial of service attack," the idea of these attacks is pretty simple. Essentially, a large volume of users or user activity hits a system at a particular time. Because there are so many demands on the system, it shuts down.

On the web, it works this way: attackers either enlist a large number of people to interact with the website at once, or they figure out some high-tech way to manufacture a large amount of network traffic simultaneously, as if hundreds of people were interacting with the system at the same time.

Most web systems are only designed for a certain maximum amount of traffic – and above that threshold, they become unable to deal with the incoming requests. In this way, hackers use DDoS attacks to crash businesses and personal websites.

So how do companies defend against DDoS attacks?

In some ways, new cloud services can help companies and other parties defend their systems against DDoS attacks.

One method is scaling.

In this way, an unusually high volume of traffic isn't an attack, it's just part of what happens from day-to-day. For example, if you're running a 9 to 5 business with hundreds of employees, when they all go online around 9am and the system experiences peak time traffic, perhaps it will crash.

What cloud systems offer is a more elastic and on-demand service – in some cases, that makes it possible for a business to order more accommodation for traffic volumes at a certain period of time. In older and less scalable systems, this kind of peak time handling was usually not feasible. Now, expanding the system's temporary capacity can help handle peak traffic, and it can also help defend against the consequences of DDoS attacks. If an attacker is able to leverage a greater volume of users, say several hundred, an ironclad cloud contract can help the site or system to withstand the demand and serve all of the incoming queries successfully.

Another method is network enhancement.

Much of the effective protection against DDoS attacks consist of 'reading' or observing network activity in a more capable way. This happens on a deeper level than scaling.

Tools like firewalls and network analysis resources can help build a better picture of what's happening inside a given system.

When the system knows more about the identity of each end user, it can assess whether high volumes of user behavior are legitimate, like that 9 to 5 clocking in, or more likely to be presenting a malicious attack. When the system knows more about where the requests are coming from, it can use machine learning or heuristic principles to determine whether an attack is likely to be taking place.

For more information on protecting your business from DDoS attacks, please download the Next Generation Endpoint Protection Buyer's Guide.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Understanding How .LINK Files Work
- Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool
- Threat Actor UAC-0056 Targeting Ukraine with Fake Translation Software
- Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
- From the Front Lines | Hive Ransomware Deploys Novel IPfuscation Technique To Avoid Detection
- From the Front Lines | Peering into A PYSA Ransomware Attack