securus

detection • connection • protection

Anatomy of a DDOS attack

Anatomy of a DDOS attack

Previously, a denial of service attack would involve a single hacker targeting a single network. These were annoying, but relatively easy to control through firewall policies, assuming that the attack itself didn't prevent access to the devices that could control the attack.

A distributed denial of service attack utilises a number of infected machines, controlled by an attacker, to create a widespread number of hosts with which to attack a destination. Because of the number of machines involved, this is why it is 'distributed'.

An attacker's motivation may be financial, it may be for notoriety, it could be a rival, or even a nation state trying to affect critical infrastructure. Historically, as they were distributed, DDOS attacks were hard to control and isolated source based filtering was impossible to achieve.

The significant growth in threat actors has created a market where a simple DDOS attack is easily purchased on the dark web for small amounts of money, exposing this disruptive technology into the hands of many.

For a few pounds, attacks can be purchased.

The goal of the DDOS attack is to target a network or application and overwhelm it with illegitimate traffic in order to stop it serving its bona fide users. It could be trying to target a network or application resource, which consumes router or server resources, or just flood a network with a volumetric attack to consume all available bandwidth. Attacks can last anywhere from a few minutes to days, but no matter how long, the implication for businesses remains the same: a network or application is cut off from the internet for the duration of the attack – **what would you do in that scenario?**

Anatomy of a DDOS attack

Without a DDOS mitigation system, the only option to stop it was to take a customer or a network segment down until the attack stopped, which has the effect of denying service by other means. DDOS attacks in 2020 may have been 20Gb volumes which would have overwhelmed most systems, but even so a 40Gb – 50Gb attack now is still unable to be mitigated by older DDOS mitigation strategies.

Networks are fundamentally shared resources, so an attack on one server in a customer environment will likely overwhelm other network components. It is the same with service providers with multi 100G and 400G pipes, attacking a single customer could affect other customers.

So, how do we prevent this attack?

Firstly, we cannot stop networks or customers being a target. If people wish to attempt an attack then they can. What we do have is a sophisticated mitigation system that stops a DDOS attack in seconds. Our system establishes a baseline of 'normal' network traffic learnt over a period of time. It then constantly evaluates the live traffic against this baseline to see if it matches or not. It is matches certain parameters, then our routers filter this out in real time.

This approach means that traffic is stopped at the network edge before it can begin to overwhelm service provider or customer equipment. If the attack changes its technique, the system will adapt to this and mitigate it as well. Should a volumetric attack occur greater than the capacity of our system, we can direct traffic to a cloud scrubbing centre to return us clean traffic. With these techniques at our disposal, subscribed customers can ensure that their network is protected with Securus Shield.

Subscribed customers can ensure that their network is protected with **Securus Shield**

Reliable

Specialised

Business-aligned

securus shield

Protect what keeps your business online

contact securus today...

...we maintain complete control over performance and service quality. No third parties, no compromises.

call 03451 283 457

securuscomms.co.uk

detection • connection • protection