fasthosts ProActive

Digital defence

DDoS attacks

Welcome to the 'Digital defence' series, where we cover cybersecurity threats and how to protect your business. In this first part, we're focusing on DDoS attacks – one of the most common threats that can disrupt online services by overwhelming them with traffic.

What is a DDoS attack?

A Distributed Denial of Service (DDoS) attack is a cyberattack that crashes a website or service by flooding it with huge amounts of fake traffic. This traffic comes from many sources, often compromised devices in a botnet, a network of computers or devices controlled remotely by cybercriminals to carry out malicious activities.

The result is that the target system becomes so overwhelmed by requests that it can't serve real users, causing slowdowns or complete outages. Additionally, if auto-scaling is enabled during a DDoS attack, it can lead to higher costs due to the increased resource usage needed to handle the flood of malicious traffic.

Common types of DDoS attacks

- Volumetric attacks – These are designed to flood the target with so much data that it runs out of bandwidth. Think of it as trying to force a river through a straw.
- Protocol attacks – These attacks target server weaknesses by overwhelming resources like firewalls or load balancers. For example, a SYN flood overloads servers with more connection requests than they can handle.
- Application layer attacks – These are more sophisticated, targeting specific applications, like a login page, with the intent of overwhelming just that service.

The impact

- Downtime – Long service outages result in lost revenue, especially for businesses that rely on online transactions.
- Reputation damage – Frequent downtime can damage customer trust and result in lost business.
- Recovery costs – The aftermath of a DDoS attack can be expensive. This includes restoring systems, improving defences, and compensating affected customers.

Defending against DDoS attacks

- DDoS mitigation tools – Services like Fasthosts ProActive offer real-time monitoring and traffic filtering, identifying and blocking malicious traffic before it reaches your site.

- Scalable infrastructure – Hosting your website on cloud platforms with elastic bandwidth allows you to automatically adjust resources to handle sudden traffic spikes without crashing. However, it's important that this is carefully monitored to reduce the risk of unexpected high costs.
- Rate limiting – This tactic limits how many requests an individual user or IP can make in a short period, reducing the chance of a DDoS attack overloading your servers.
- Traffic monitoring – Regular monitoring for unusual traffic patterns can help identify an attack early, giving you time to respond.
- Redundancy plans – Putting backup servers and failover strategies in place ensures your services stay online, even if one part of your system is attacked.

DDoS attacks are a growing threat, but with a proactive approach, you can reduce their impact. Understanding how DDoS attacks work and putting the right defences in place is critical to maintaining uptime and protecting your business.

At Fasthosts ProActive, we offer advanced solutions to help safeguard your digital assets against these types of threats.

If you have any questions or want to find out how we can help your business, give us a call on 0333 111 2000 or book a meeting at a time that suits you.