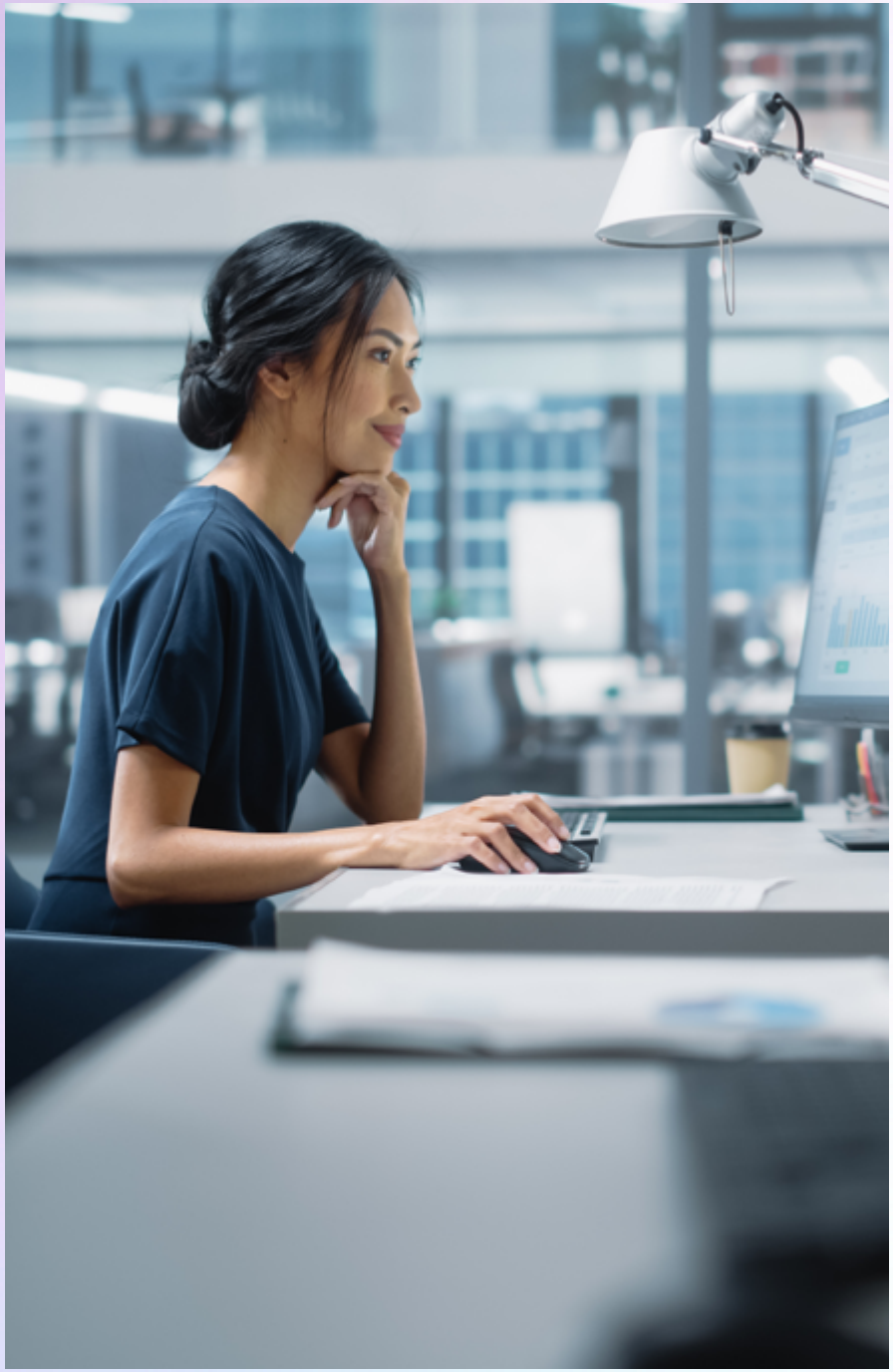
BT Means Business

Protecting your organisation from DDoS attacks

Andy Atkinson
Security Engineering Manager, BT



The growing threat of DDoS attacks

As businesses and organisations seek to become more efficient, there is an increasing reliance on cloud-based services.

Hyper-scalers such as Amazon Web Services, Google, and Microsoft provide computing and storage at enterprise scale – offering organisations flexibility, compliance, and security. Similarly, software-as-a-service (SaaS) providers offer organisations pay-as-you-go access to the applications they need with easy deployment.

Although these services can help organisations take a digital-first approach, they can also create security vulnerabilities. For example, if businesses access cloud-based services through public internet, this can create a weakness that cyber criminals can take advantage of via distributed denial-of-service (DDoS) attacks.

About the author
Andy has been working in IT for over 30 years and in telecoms for the last 17 years in architecture, networking and cyber security roles. He currently leads a team of cyber security pre-sales engineers, who work with corporate and public sector organisations.

What are DDoS attacks?

DDoS attacks flood your network with traffic, rendering your internet service unusable. As DDoS attacks can lead to serious operational, financial, and reputational consequences, it is essential you protect your organisation against them.

Criminals sometimes use DDoS attacks as a means of extortion or as a distraction tactic while they carry out other cyber attacks aimed at infiltrating your defences with a view to obtaining access to sensitive data. DDoS attacks are also used on ransomware victims to ratchet up the pressure to pay.

There are many complex reasons for the rise in DDoS attacks, including cheap and easy access to DDoS-as-a-service platforms and the proliferation of insecure web-facing servers and Internet of Things (IoT) devices. These devices can easily be compromised and used to create large-scale botnets – armies of devices infected with malicious software that can be controlled as a group without the owner's knowledge.

19 DDoS attacks are launched every minute

Fact: in the third quarter of 2022 alone, there was a **90% increase** in DDoS attacks around the globe, compared to the same period the previous year.

Multi-vector attacks

These botnets can be commanded to transmit large amounts of data at targets across the globe, overwhelming the capacity of the networks and devices and ultimately leading to loss of service.

But it is not just the volume of attacks that is concerning. Attacks are becoming larger, longer in duration, and more sophisticated.

So-called multi-vector attacks use various denial-of-service techniques at the same time: volumetric attacks (overloading your available bandwidth), state exhaustion attacks (attempting to cause your perimeter firewalls to fail), and application layer attacks (taking advantage of specific vulnerabilities in the application layer).

30 billion IoT devices by 2025

Fact: These devices tend to have security vulnerabilities making them easy to compromise and use to unleash DDoS attacks

Response

What should I consider to combat DDoS attacks effectively?

Considering the damage that DDoS attacks can cause, every organisation needs a robust cyber security posture. When assessing your current set-up, it's important to ask yourself the following questions:

1. Are you monitoring your internet traffic? Could you identify a DDoS attack?

Monitoring your network for deviations can help you spot potential attacks, but it's important to understand your baseline first. DDoS attacks can be mistaken for normal IT problems – often manifesting as slow network performance, unavailability of a particular website, an inability to access any website, and internet disconnection.

2. Are you working with your Internet Service Provider (ISP) or Cloud Service Provider (CSP) to prevent DDoS attacks?

Firewalls can't prevent volumetric DDoS attacks. Instead, they need to be mitigated in the cloud – bad traffic should be removed before it hits your perimeter security, but legitimate traffic should still be allowed to reach its destination. Remember: the bandwidth on your critical internet circuits can easily be consumed by a DDoS attack – rendering your internet circuit unusable.

3. Do you have a solution to protect against other denial-of-service attacks?

State exhaustion attacks and application layer attacks cannot be prevented in the cloud. To defend against them, you need a specialised security appliance in front of your critical assets. These devices continuously update themselves with DDoS-specific threat intelligence and monitor all traffic coming in and out of your network to identify and mitigate against sophisticated denial-of-service attempts.

4. Do you have a response plan in place specifically for DDoS attacks?

What would happen if your organisation was left without internet access for a few hours or several weeks? What would the impact be to your users, customers, and citizens? How would you ensure business continuity? How would you ensure you maintain administrative access? What would your response be to a ransom demand? It is better to establish a response plan before an attack, rather than trying to establish one once an attack is underway.

Strategy

Strategy is half the battle

Wherever you are running critical services over the internet you should consider protection from DDoS attacks as part of your organisation's cyber security strategy.

After all, having the right tools in place and a detailed response plan can be the difference between an attack being a minor inconvenience and a lethal threat.

Make sure you understand what your critical applications are and where they reside. Who would be impacted by them not being available and how? What is your tolerance for downtime for those applications? What would the impact be on your organisation? For example, you might experience loss of revenue, loss of customers/ partners, loss of services to citizens, or reputational damage.

Use this information to help build a business case for protection. With the right tools, the right strategy, and the right cyber security partner by your side, it is possible to neutralise these attacks before they affect your critical services.

We can help you protect your organisation

The BT Security team was born out of the necessity to protect our own organisation

Our customer facing websites and our streaming services are critical assets that we protect 24/7 using our world-class DDoS mitigation platform.

The good news is that the very same platform that we use to protect ourselves is available to protect our customers. BT is now a Leader in the IDC MarketScape for European Managed Security Services and has a team of 3000+ cyber security experts. Every day, we're trusted by businesses, the government, and the emergency services to keep them safe by reducing their exposure to cyber threats, and DDoS protection is just one of the services BT Security can provide.

A proactive approach to reduce your risk

Whatever your organisation does, if you rely on the internet to deliver your services then you could be vulnerable.

But even though your organisation is at risk of DDoS attacks, the consequences are not inevitable. With the right proactive approach, you can protect against DDoS attacks, reduce their impact, and keep your organisation running.

Looking for an experienced cyber security partner?

Contact us for more support on protecting your organisation against DDoS attacks.

Offices Worldwide

June 2023