The Terabit Era of Distributed Denial of Service (DDoS) Attacks

DDoS attacks have become much larger, more frequent, sophisticated, and diverse. As the DDoS threats grow, so does the impact of the DDoS attacks: they take down network infrastructure and services and leave many users without access to cloud-based content or critical communications.

They also bring significant financial impact – either direct (in the form of lost revenues or penalties) or indirect – in the loss of customer loyalty and churn.

Here's a timeline of the most impactful DDoS attacks as we enter the DDoS terabit era.

More information:

Learn more about the DDoS threats and how Nokia can help you to strengthen your network defenses by clicking here.

2013 | Spamhaus

300 Gbps

In at no. 10 is the 2013 attack against Spamhaus, which was overloaded with 300 gigabits of traffic per second, knocking its website and part of its email services offline. As an anti-spam organization, the company is targeted frequently.

2014 | Occupy Central

500 Gbps

The Hong-Kong Occupy campaign was hit by a massive 500 Gbps attack after its launch in 2014. The attackers targeted not only Occupy Central's web hosting services, but two other associated sites too.

2016 | Krebs on Security

620 Gbps

American journalist and reporter Brian Krebs' website suffered an attack almost twice the size of anything it had previously experienced in September 2016. Luckily, attempts to knock KrebsonSecurity.com offline did not succeed.

2016 | OVH

1 Tbps

At no.4 is the barrage that targeted cloud hosting company OVH in September 2016. Significantly more powerful than the Imperva attack, it was the largest seen at the time, comprising more than 150,000 IoT devices.

2018 | GitHub

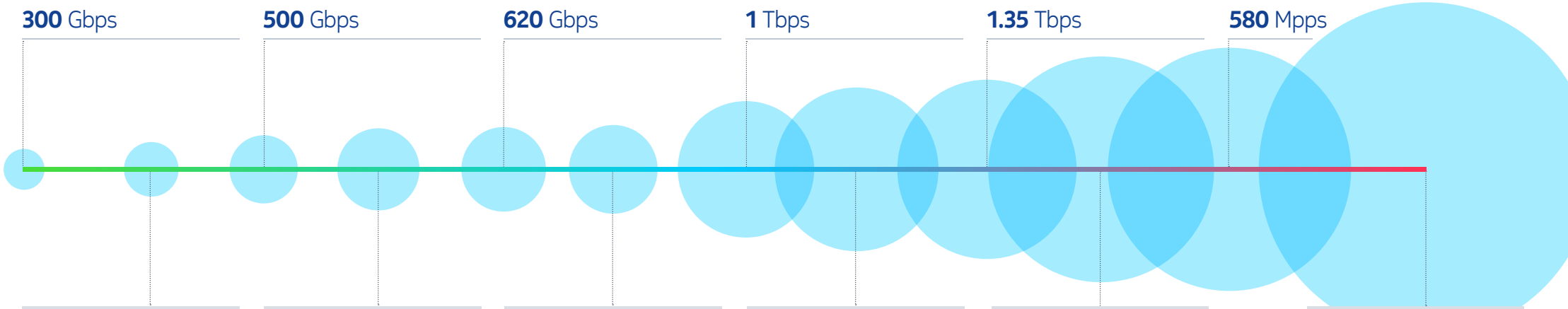
1.35 Tbps

GitHub was hit by a record-breaking attack in February 2018, with an onslaught of traffic at 1.35 terabits per second. This time attackers used Memcached servers to amplify the attack using a spoofed IP address.

2019 | GitHub

580 Mpps

In January, Imperva reported a DDoS attack of over 500 million packets per second (Mpps); one of their clients was under a TCP SYN flood attack which used a range of randomized and spoofed IP packets of 800 to 900 bytes in size. In April, they reported a 580 Mpps attack.



2014 | Cloudflare

400 Gbps

The 9th most harmful attack was directed at the security provider Cloudflare in 2014. The powerful NTP amplification attack was originally aimed at a customer, but managed to take down Cloudflare's whole network using a mirroring technique.

2016 | BBC

602 Gbps

On New Year's Eve, 2016, the BBC's websites were swamped and taken down for several hours. The attackers, New World Hacking, claimed to be testing their server power.

2016 | Imperva

650 Gbps

This 2016 Leet botnet attack was the first of its kind, attacking the cybersecurity software company Imperva with a whopping 650 Gbps. A second attempt only lasted 17 minutes but was able to flood more than 150 million packets per second.

2016 | DYN DNS

1.2 Tbps

DNS provider DYN was hit by a huge cyberattack in 2016, taking down major websites like Twitter, Amazon and The Guardian with it. The attack was reportedly commanded by the malware code Mirai, with the affected website Mashable warning, "this is just the beginning for these types of attacks." (Source)

2018 | Tier-1 US provider

1.7 Tbps

Just five days later, GitHub's unwanted record was broken. An unnamed US service provider suffered a 1.7Tbps attack. Its defenses fortunately proved strong enough to prevent any outages, but not everybody is so well prepared.

2020 | Amazon, Akamai

2.3 Tbps **809** Mpps

In May 2020, Amazon reported the mitigation of 2.3 Tbps flooding attack using their AWS Shield. On June 21, Akamai reported an attack at 809 Mpps (418 Gbps) aimed at a bank, which lasted less than 10 minutes, and used a large number of (new) IP addresses.

NOKIA

Having robust network protection against the ever-growing size, sophistication, and frequency of DDoS attacks is more important than ever. At Nokia, we are experts in providing our customers with advanced security solutions that can protect your networks and customers against harmful DDoS attacks. Our big data-driven security analytics, combined with our auto-mitigation and router-based protection allows you to implement a full, 360-degree insight-driven network security framework – to protect you from all kinds of DDoS attacks (inbound, outbound, data center-based, etc.) Our approach can improve the overall efficiency of DDoS protection while reducing the costs by as much as 85% - when compared to legacy, scrubbing center-based approach.