A Brief Report on Recent DDoS Attacks

By: Linto Baby

A Distributed Denial-of-Service (DDoS) attack is when hackers flood a website or online service with so much traffic that it crashes and becomes unavailable for legitimate users. These attacks have become a common weapon for everyone from online activists to governments.

This report will give a quick summary of five recent DDoS incidents and then take a closer look at one of the largest attacks ever seen.

Five Recent DDoS Incidents at a Glance

Here are five examples that show the different reasons and ways DDoS attacks are used today:

1. **The 7.3 Tbps Mega Attack (May 2025):** This was a massive, but very short, attack aimed at an internet hosting provider. The goal wasn't to ask for money, but likely to show off the attacker's power or test the defenses of a major internet security company.[1]
2. **The 18-Day Campaign (Early 2025):** Instead of one big attack, this was a long, drawn-out campaign against the internet infrastructure company Cloudflare. For 18 days, attackers relentlessly hit the company with millions of small attacks, likely trying to wear down their systems and find a weak spot.[4]
3. **Attack on a News Outlet (June 2025):** An independent news site in Eastern Europe was hit with a DDoS attack right after it published a story about a local Pride parade. This is a clear example of an attack motivated by ideology, meant to silence a specific viewpoint.[4]
4. **Pressure on Taiwan Before Elections (January 2025):** In the weeks before Taiwan's general elections, government and telecom websites were flooded with millions of daily cyberattack attempts. The goal was likely political: to disrupt services and create doubt about the election process.[1]
5. **Hacktivists vs. Italy (January 2025):** A pro-Russian hacking group called NoName057(16) targeted Italian government websites. This was a politically motivated attack, done to show support for Russia by disrupting a NATO country that supports Ukraine.[6]

A Closer Look: The Record-Breaking 7.3 Tbps Attack

Let's dive into the details of the biggest attack from the list, which set a new record for its sheer size.

- **The Target:** The attack was aimed at a hosting provider—a company that runs the servers for many other businesses' websites and online services. Attacking a hosting provider is a strategic move because it can cause problems for thousands of their customers all at once.[2]
- **The Technology Used:** The attack was a massive flood of data, hitting a peak of 7.3 terabits per second (Tbps). To put that in perspective, it was like trying to force the data of thousands of HD movies through a garden hose in less than a minute. The hackers used a huge network of over 122,000 computers from 161 different countries to launch the attack.[2] They mostly used a simple method called a **UDP flood**, which just involves sending a firehose of data at the target. They also mixed in some cleverer techniques that tricked old, forgotten internet services into sending junk traffic to the victim, making the attack even bigger.[2]
- **The Attacker's Motive:** Since no ransom was demanded, the motive was likely to show off. The attackers were probably demonstrating the power of their botnet (the network of hacked computers) to impress other criminals or to test the limits of the world's best cyber defenses.[4]
- **The Overall Impact:** The attack was incredibly powerful but lasted only 45 seconds.[2] Because the target was using a modern DDoS protection service, the attack was blocked automatically and had minimal real-world impact. However, it served as a major wake-up call, showing just how powerful these attacks have become.
- **Defensive Strategies:** The attack was stopped successfully because the defense was spread out all over the world. Instead of all 7.3 Tbps of traffic hitting one location, it was distributed across hundreds of data centers globally.[2] The system automatically detected the attack in seconds and filtered out the bad traffic before it could do any damage. This shows that the only effective way to defend against such massive attacks is to use a large, cloud-based security service that can absorb the traffic far away from the actual target. Relying on a firewall at your own office or data center wouldn't stand a chance.

Works cited

1. DDoS Attack Statistics: 20.5M Attacks Blocked in Q1 2025 - DeepStrike, accessed October 2, 2025, https://deepstrike.io/blog/ddos-attack-statistics
2. Defending the Internet: how Cloudflare blocked a monumental 7.3 ..., accessed October 2, 2025, https://blog.cloudflare.com/defending-the-internet-how-cloudflare-blocked-a-m

onumental-7-3-tbps-ddos/
3. Internet Under Fire: Analysis of the record-breaking 7.3 Tbps DDoS attack - FastNetMon, accessed October 2, 2025, https://fastnetmon.com/2025/06/23/internet-under-fire-analysis-of-the-record-breaking-7-3-tbps-ddos-attack/
4. Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report, accessed October 2, 2025, https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/
5. 2025 DDoS Trends Report - MazeBolt, accessed October 2, 2025, https://mazebolt.com/resources/2025-ddos-trends-report
6. Significant Cyber Incidents | Strategic Technologies Program - CSIS, accessed October 2, 2025, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
7. Hacktivist group responsible for cyberattacks on critical infrastructure in Europe taken down | Eurojust | European Union Agency for Criminal Justice Cooperation, accessed October 2, 2025, https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down
8. Noname057(16) - Wikipedia, accessed October 2, 2025, https://en.wikipedia.org/wiki/Noname057(16)