DDoS Attacks

-Abhinav V R

Overview of Five Recent DDoS Attacks

Attack	Target	Peak Size	Technology Used	Motive
1. Aisuru Botnet Attack	European network infrastructure company	22.2 Tbps	IoT botnet (404,000+ IPs), non-spoofed traffic	Bragging rights, botnet-for-hire
2. India-Pakistan Hacktivist Campaign	Indian government and financial sectors	Thousands of attacks	DDoS-for-hire, AI-enhanced scheduling	Geopolitical disruption
3. Japan's New Year Carpet-Bomb Attack	Airlines, banks, telecoms	Unspecified, but widespread	Multi-server "carpet-bomb" DDoS	Destabilize infrastructure during holidays
4. French Retailer HTTP/2 Attack	Home supply e-commerce site	6 million RPS	HTTP/2 Rapid Reset + botnet	Disrupt shopping experience

5. 1.33 Million-Device Botnet Attack	Online betting platform	Tens of millions of RPS	Massive botnet (mostly Brazil-based)	Financial disruption, testing defenses

Selected Incident: Aisuru Botnet Attack (22.2 Tbps)

-> Target

A European network infrastructure company was the primary target, though the attack could have impacted broader internet services if not mitigated.

-> Technology Used

- **Botnet Composition:** Over 404,000 infected devices, mainly IoT routers.
- **Attack Type:** Hyper-volumetric DDoS, peaking at 22.2 Tbps.
- **Infection Vector:** Malware distributed via a compromised update server of Totolink routers.
- **Traffic Characteristics:** Non-spoofed IPs, indicating real compromised devices.

-> Attacker’s Motive

- **Primary Motive:** Demonstration of power and bragging rights.
- **Secondary Motive:** Commercial — selling botnet access and DDoS capabilities on Telegram.

- **Group Identity:** Aisuru, known for flamboyant and destructive attacks on ISPs.

-> Overall Impact

- **Immediate Impact:** Cloudflare successfully mitigated the attack, preventing downtime.
- **Potential Impact:** Without robust defenses, such an attack could cripple ISPs, disrupt services, and cause cascading failures across dependent networks.
- **Industry Alarm:** Set a new record for DDoS intensity, doubling the previous peak.

-> Defensive Strategies

- **Autonomous Mitigation:** Cloudflare used real-time detection and automated blocking.
- **Botnet Disruption:** Security researchers traced and sinkholed infected devices.
- **Recommended Measures:**
    - Deploy AI-enhanced DDoS protection.
    - Patch and secure IoT devices, especially routers.
    - Monitor for unusual traffic spikes and use geo-distributed filtering.
    - Educate users and vendors on secure firmware update practices.