Analysis of Five Recent DDoS Attacks (2023-2025)

Distributed Denial of Service (DDoS) attacks remain a major threat to online infrastructure, with recent incidents showing increased scale and sophistication. Below are summaries of five notable DDoS attacks from 2023-2025, each detailing the target, technology used, attacker's motive, overall impact, and defensive strategies.

HTTP/2 Rapid Reset DDoS Attack (October 2023)
Target:
Major cloud providers (AWS, Google Cloud, Cloudflare) and their customers. Technology Used: Exploited HTTP/2 protocol's Rapid Reset feature, sending rapid RST_STREAM frames to overwhelm servers with minimal botnet resources. Attacker's Motive: Likely to demonstrate capability or disrupt for hire, part of DDoS-for-hire trends. Overall Impact: Peaked at 398 million requests per second, causing temporary service disruptions; exposed HTTP/2 vulnerabilities. Defensive Strategies: Use protocol-specific rate limiting, patch HTTP/2 to limit streams, deploy advanced DDoS mitigation services like Cloudflare.
Carpet-Bombing DDoS Attack (2024)
Target:
Large Eastern European service provider and its network. Technology Used: Distributed low-volume traffic across thousands of IPs via botnet hierarchy (execution bots, proxies, command-and-control), evading detection. Attacker's Motive: Likely extortion or competitive disruption. Overall Impact: Caused network congestion, prolonged downtime, and higher costs; contributed to doubled DDoS incidents in 2024. Defensive Strategies: Deploy intelligent DDoS protection with behavioral analysis, implement zero-trust segmentation, scan and patch devices to prevent botnet recruitment.

Aisuru Botnet DDoS on KrebsOnSecurity (May 2025)
Target: KrebsOnSecurity.com, a cybersecurity news site. Technology Used: IoT-based Aisuru/Airashi botnet with ~300,000 devices, sending UDP floods via zero-day exploits in devices like Cambium cnPilot routers. Attacker's Motive: Likely a test to showcase botnet power for DDoS-for-hire services via Telegram. Overall Impact: Reached 6.3 Tbps briefly but caused no downtime due to protections; showed IoT botnet escalation. Defensive Strategies: Use free mitigation like Google’s Project Shield, disclose botnet exploits publicly, harden devices with firmware updates and IoT isolation.

Hyper-Volumetric DDoS Attacks (Q2 2025)
Target: Hosting providers and cloud services, including Cloudflare-protected entities. Technology Used: Multi-vector floods with UDP, NTP reflection, and Mirai botnet, delivering massive data in short bursts. Attacker's Motive: Disruption for downtime or extortion, often AI-amplified or geopolitically driven. Overall Impact: Peaked at 7.3 Tbps, with 7.3 million attacks mitigated in Q2 2025; overwhelmed smaller networks, raised cyber costs. Defensive Strategies: Use automated cloud scrubbing, full packet inspection for Layer 7 threats, adopt machine-learning-based adaptive defenses.

Aisuru Botnet DDoS on US ISPs and Gaming Servers (October 2025)
Target: US ISPs (AT&T, Comcast, Verizon) and gaming platforms like Minecraft servers with TCPShield. Technology Used: Expanded Aisuru botnet with 300,000+ devices, using leaked Mirai code for UDP floods and proxy networks via zero-day exploits. Attacker's Motive: DDoS-for-hire and proxy rental for profit; targeted gaming to push protection services. Overall Impact: Record 29.6 Tbps test attack, sustained 15-22 Tbps causing outages and ISP congestion; $1M+ monthly mitigation costs. Defensive Strategies: Implement ISP-level traffic suppression, segregate IoT devices, pursue collaborative botnet takedowns, use specialized protections like Global Secure Layer.