1) Rapper Bot (big botnet / DDoS-for-hire)

Target: Lots of different websites worldwide — government pages, tech companies, social media and many smaller sites.
Technology used: A botnet made from hacked IoT devices (like routers and CCTV/DVRs). The attackers used those devices to flood targets with massive amounts of traffic.
Attacker's motive: Money — the botnet was rented out as a DDoS-for-hire service, so people could pay to attack other sites.
Impact: Hundreds of thousands of attacks over months and many victims; some attacks were massive (terabits per second), causing downtime and big recovery costs for victims

How it could've been stopped/lessened: Use CDNs and scrubbing services that absorb bad traffic, make ISPs help filter attack traffic, and fix insecure IoT devices (change default passwords, update firmware).

2) Pro-Russia hacktivist DDoS attacks on Italy

Target: Official Italian sites — foreign ministry, airports, transport authorities, and some banks.
Technology used: Distributed DDoS tools and botnets that sent lots of requests to overload web servers (both network-level and application-level floods).
Attacker's motive: Political — the group claims support for Russia and attacked Italy in protest of its policies. It's basically hacktivism.
Impact: Websites went offline or were slow for short periods; airport operations were not seriously disrupted, but public-facing sites were knocked down and had to be fixed.

How it could've been stopped/lessened: Use Anycast/CDN protection, rate limiting, WAFs for app traffic, and quick coordination with national CERTs and hosting providers.

3) Major DDoS spike against banks (October 2024 banking campaign)

Target: Multiple banks and financial services across regions.
Technology used: Multi-vector DDoS — attackers used volumetric floods, DNS floods, and attacks that targeted APIs and customer channels. They mixed techniques to get around simple filters.
Attacker's motive: Mixed — sometimes financial extortion, sometimes to cause disruption and shake customer trust. Attackers or DDoS-for-hire services were likely behind it.
Impact: Some banks had outages that lasted hours or even days, hurting customers and costing money to fix. Financial services are high-value targets because downtime affects many people.
How it could've been stopped/lessened: Use scrubbing providers (Akamai, Cloudflare, etc.), keep multiple DNS providers, add API rate limits and anomaly detection, and share intel with FS-ISAC/peers.

4) Large persistent campaign that drove Cloudflare's Q1 2025 numbers

Target: Many Cloudflare customers and infrastructure (the campaign flooded sites Cloudflare protects).
Technology used: Massive, sustained multi-vector attacks over many days that generated millions of attack requests; attackers moved between different attack types.

Attacker's motive: Not always clear — could be testing, disruption, or trying to overwhelm a major provider. Sometimes attacks like this are used as a cover for other crimes.
Impact: Cloudflare recorded a huge spike in blocked attacks for Q1 2025 (an 18-day campaign contributed a big share). The event showed how persistent attackers can be and why big providers need huge capacity.
How it could've been stopped/lessened: Massive Anycast networks, automatic rules to drop malicious packets, and close cooperation between CDNs and ISPs. Also, quick sharing of attack signatures helps everyone block similar traffic

5) DDoS attacks on Gujarat government websites

Target: Gujarat state government websites and critical local web services.
Technology used: DDoS tools combined with anonymization (VPNs, encrypted platforms); local investigators said the attacker used advanced tools and then publicized the attacks on Telegram.
Attacker's motive: Reported as political/retaliation motives — the accused allegedly carried out attacks as a reaction to a government operation and posted propaganda online.
Impact: Intermittent downtime for government websites, an official investigation, and legal charges including cyber-terrorism sections. This case shows how local actors can cause major national security concern.
How it could've been stopped/lessened: Use CDN fronting, upstream ISP filtering, geo-rate limits, good logging for quick attribution, and fast coordination with national CERT / law enforcement.

Investigative brief: Rapper Bot

Rapper Bot — DDoS-for-hire botnet takedown (2025)

Rapper Bot was a Mirai-style IoT botnet rented out to customers that launched hundreds of thousands of DDoS attacks worldwide; US authorities seized its infrastructure and charged a suspected operator in August 2025.

1. Target:
Rapper Bot didn't only target one organization — it was used against many victims including government sites, tech companies, social platforms, and smaller businesses across many countries. Attackers and paying customers could pick victims at will.

2. Technology used:
The botnet was built from insecure IoT devices (routers, DVRs, cameras) infected by Mirai-like malware. These devices were commanded to send huge volumes of traffic (UDP, TCP floods, and other flood types) to victims to overwhelm their networks and servers. The botnet had a control panel for customers to start attacks.

3. Attacker's motive:
The main motive was financial — the botnet operator rented out attack time to customers (DDoS-for-hire). That meant many different people could pay to launch attacks. Some attacks may also have been for revenge or political reasons when customers requested them.

4. Overall impact:

- The botnet was credited with hundreds of thousands of attacks and thousands of victims.

- Individual attacks reached terabit levels, causing outages and big cleanup costs for victims.
- Law enforcement seized key infrastructure and charged a suspect, which stopped this particular service for now.

5. Defensive strategies that could have mitigated the attack:

- **Use CDN/scrubbing services:** Route traffic through providers that can absorb huge floods. This is the fastest way to survive big volumetric attacks.
- **Work with ISPs for upstream filtering:** Ask transit providers to filter or null-route obvious attack prefixes to prevent backbone saturation.
- **Harden IoT devices:** Change default passwords, update firmware, disable unused services, and segment IoT on separate networks — this reduces the size of botnets.
- **DNS and app resilience:** Use multiple DNS providers and a WAF with rate limiting and challenge mechanisms for suspicious application traffic.
- **Share intelligence and coordinate:** Tell FS-ISAC / national CERTs and share indicators so providers and law enforcement can act quickly.

Conclusion

DDoS attacks are getting bigger and cheaper to run because so many devices are insecure and the internet has lots of bandwidth. Some attackers do it for money, some for politics, and some just to show off. To stay safe, companies should use big scrubbing providers, fix insecure devices, and work closely with ISPs and national cyber teams. The Rapper Bot case shows that when companies, researchers and police work together, big botnets can be shut down — but the root causes (bad IoT security and DDoS-for-hire markets) still need fixing.