MAZEBOLT

7 DDoS Trends to Watch in 2026

Based on MazeBolt's internal data and market research, we can expect to see the following DDoS attack trends in the year ahead:

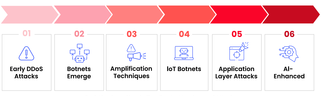
1

Botnets Will Grow Fast and Get Smarter

DDoS attacks will continue to involve botnet operations, allowing attackers to:

- Automate target selection
- Optimize vector orchestration
- Adapt to defenses in real time

The use of botnets is part of the evolution of DDoS attacks, which have developed over time:



Evolution from Simple Flooding to AI-enhanced Attacks

2

Attacks Will Be Smaller and Smarter

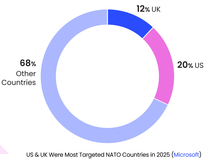
Attackers will continue using AI-enhanced techniques for:

- Smarter Targeting and Timing
- Self-Learning Automation
- Multi-Vector Coordination
- Lowered Barrier to Entry
- Traffic Camouflage
- Evading Traditional Defenses

3

DDoS Will Continue to Be Used as a Geopolitical Weapon

DDoS attacks will continue to be used as precision instruments that target critical infrastructure at the most damaging times.

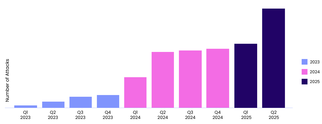


US & UK Were Most Targeted NATO Countries in 2025 (Microsoft)

4

Application-layer and API Attacks are Expected to Rise

The number of DDoS attacks targeting ISO Layer 7 will continue to grow.



The Surge in Web DDoS Attack Activity (Source: Radware)

5

Multicloud Environments Will Create Increased DDoS Risk

As enterprises adopt cloud, edge, and hybrid environments, these decentralized architectures introduce complexity - making it significantly harder to monitor, secure, and patch every exposed point.

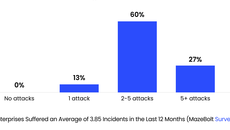
Attack Surface	=	IP/FQDN	x	Service	x	Attack Vector
		188.114.97.12		HTTP		Slowloris
		www.mazebolt.com		HTTPS		SYN Flood
		kb.mazebolt.com		IPSec		IP Fragmented
		blog.mazebolt.com		DNS		DNS Request Flood

More Complex Attack Surfaces Mean Greater Risk of DDoS Downtime

6

Under-tested DDoS Protections Will Be Increasingly Vulnerable

According to MazeBolt research, enterprises that run point-in-time pentests typically cover less than 1 percent of the total attack surface. This leads to a proliferation of hidden DDoS misconfigurations and vulnerabilities.



Enterprises Suffered an Average of 3.85 Incidents in the Last 12 Months (MazeBolt Survey)

7

DDoS Attacks Will Involve Multiple Vectors & Layers

Continuous DDoS testing will be even more critical in the coming year, as DDoS attacks increasingly blend multiple layers and vectors into coordinated assaults. That's because these complex DDoS attacks are harder to block. Note that:

- They're harder to detect and mitigate
- The trend is accelerating
- Attackers are moving from brute force to precision
- The outcome is operational unpredictability

To learn more about 2026 DDoS attack trends in the AI era, download the full report.