MAZEBOLT

Damaging DDoS Downtime: Who Is at Risk?

Attacks Have Become More Common

Hacktivist groups motivated by political and ideological agendas are driving the current increase in DDoS attacks:



DDoS attacks surged 30% in the first half of 2024, compared to the first half of 2023.

DDoS attacks on critical infrastructure increased by 55% YoY since 2020.

Top DDoS Targets by Industry

Industries that demand business continuity are at higher risk of DDoS attacks:

Finance

Disrupted online services and availability, causing financial and reputational damages

Healthcare

Targeted the patient management systems and telemedicine platforms used by healthcare providers

Government

Often coincided with political events; aimed to erode public trust and disrupt administrative functions

Transportation

Disrupted airlines and railway booking systems; exposed or blocked access to sensitive data; and impacted supply chains

The Costs of a DDoS Attack

Damaging downtime is just one aspect of the total cost of a DDoS attack:

Lost Business	Downtime of Services or Websites	Damage to Professional Reputation	Increased Churn as Customers Lose Trust
Legal Costs	Time Invested in Response & Recovery	Compliance & Regulatory Fines	Reputation Management (PR/Media)

Rising Cost of Regulation

New and more stringent regulations frequently mean that organizations must make adjustments to their operations in order to be compliant:

Regulatory Framework	Date for Compliance	Where it Applies
SEC Cyber Risk Management	December 18, 2023	US
NIS 2 Directive	October 17, 2024	EU
Digital Operational Resilience Act (DORA)	January 17, 2025	EU

Most Prevalent DDoS Attack Types

While the frequency of DDoS attacks continues to rise, the attacks are also evolving in complexity and scale. Common types of DDoS attacks include:

Volumetric Attack

A botnet attack floods the network with traffic that appears legitimate but soon overwhelms the network.

Targeted Application Layer Attack

Requires fewer resources, and targets vulnerabilities within applications by mimicking legitimate user behavior.

Multi-Vector Assault

Sophisticated attack that combines multiple attack techniques or vectors.

Mitigate the Risk with Continuous DDoS Testing

Continuous DDoS testing is an ongoing process that requires you to:

01 Continuously test all layers of DDoS protection solutions

02 Uncover DDoS vulnerabilities



03 Create prioritized remediation recommendations

04 Ensure vulnerabilities are patched and do not return

Learn More about Eliminating the Risk of DDoS Attacks

GET THE REPORT

MAZEBOLT