MAZEBOLT

BATTLING DDoS IN THE GAMING WORLD

TAKING IT DAY BY DAY

23,000
Approximately **23,000 DDoS attacks** are happening every 24 hours.

10 Million
In 2022, almost **10 million DDoS** attacks were launched.

YEARLY AVERAGES

$30,000	A company loses **$30,000 USD per hour** after a DDoS attack.
$120,000	Getting back online and remediating the damage caused by a successful DDoS attack can cost **up to $120,000 USD.**
$417,000	Large firms lose around **$417,000 USD** due to DDoS attacks, per year.
50 hours	A successful DDoS attack lasts **50 hours.**

1 week of gaming time is equal to a **50 hour DDoS attack**

6.68 days
18–25 year old gamers

6.66 days
26–35 year old gamers

Many gaming companies do not share hard actual data about DDoS attacks in an effort to avoid reputational damage. But from the rising number of reports and documentations (many coming from actual gamers), it's clear that from the total number of DDoS attacks in 2022, many were aimed at gaming companies.

MOST COMMON DDoS ATTACK VECTORS ON GAMING COMPANIES

HTTP Flood

UDP Flood

Empty Connection Flood

Layer 7 Reflection DDoS attacks

82%	Layer 7 Reflection DDoS attacks **increased by 82%** in 2022.
60%	**60%** of DDoS attacks are network attacks.

Most cloud services and applications are not DDoS resilient against HTTP floods, browser simulation attacks and more.

GAMING ATTACKERS

Why do attackers launch DDoS attacks against gaming companies?

- Overload servers and disrupt business activity.
- Ransom from major companies in tournaments or official game launches.
- Competitive advantage over opponents by compromising their network connection – both on players and companies.

DDoS ATTACK DESTINATIONS

*Number of Active Gamers



BEFORE & AFTER

Gaming Companies Before Implementing RADAR™

- Average Vulnerability of DDoS Attack Surface – **47%**
- Existing Mitigation Layers: CDN, CPE, WAF
- Average number of vulnerable targets: **2000**

Gaming Companies After 2 Testing Cycles with RADAR™

- Average Vulnerability of DDoS attack Surface – **3%**
- Existing Mitigation Layers: Scrubbing Center, CDN, CPE, WAF
- Average number of vulnerable targets: **120**

ACHIEVING DDoS RESILIENCE WITH MAZEBOLT RADAR™

- RADAR identifies all DDoS attacks that bypass existing mitigation systems.
- RADAR brings visibility into Dynamic DDoS attack surface vulnerabilities through continuous and non-disruptive testing.
- RADAR closes the DDoS remediation loop from insight to action by working with the mitigation vendors, providing visibility into misconfigurations, prioritizing a remediation plan and validation efforts.
- RADAR maximizes ROI on existing mitigation by fulfilling its full potential and making sure it actually mitigates DDoS attacks on previously unknown vulnerabilities.
- RADAR is adaptive, ensuring that mitigation systems are updated on all DDoS vulnerabilities, automatically testing DDoS attacks on live environments with zero operational downtime.

MAZEBOLT

Mazebolt is pioneering a new standard in achieving true DDoS resilience by identifying and eliminating vulnerabilities.

VISIT MAZEBOLT.COM