NETSCOUT

DDoS THREAT INTELLIGENCE REPORT: UNMASKING THE SWARM

Issue 16: 2nd Half 2025

AI-enabled attacks, massive botnets, and unprecedented scale redefine the DDoS threat landscape.

GLOBAL DDoS ACTIVITY AT A GLANCE (2H 2025)

8,088,463
DDoS attacks observed globally

203
countries and territories impacted

376
industry verticals by throughput

12,698
autonomous system numbers (ASNs)

MORE THAN HALF OF ALL ATTACKS ARE MULTIVECTOR

A Fundamental Shift in the Threat Landscape

DDoS attacks are no longer simply defined by volume, frequency and complexity. In the second half of 2025, attackers increasingly leveraged artificial intelligence to plan, launch, and adapt attacks in real time.

Sophisticated attacks **NO LONGER REQUIRE** deep technical expertise

AI IS EMBEDDED across the DDoS attack lifecycle

The gap between attacker intent and execution has **NARROWED DRAMATICALLY**

THE DRIVERS AND THE RISK

A New Generation of Mirai-Derived IoT Botnets is Reshaping DDoS Infrastructure.

BOTNETS REDEFINED

- Direct-path floods instead of reflection-only attacks
- Compromised routers, cameras, and customer-premises equipment
- Outbound attack traffic exceeding 1Tbps from provider networks
- Botnets such as Aisuru demonstrating multi-terabit capability

AI-DRIVEN DDoS OPERATIONS

Conversational AI is now integrated into DDoS-for-hire platforms, allowing attackers to define objectives in plain language while the system handles execution.

- Reconnaissance and vector selection
- Timing and scale optimization
- Dynamic adaptation to defensive measures

GROWTH OF THE MALICIOUS AI ECOSYSTEM

219% INCREASE in AI jailbreak discussions

52% INCREASE in underground mentions of malicious AI tools

PRESSURE ON CRITICAL INTERNET INFRASTRUCTURE

38+ SIGNIFICANT attacks against DNS root servers

45,000+ ATTACKS involving NTP services

IMPLICATIONS FOR DEFENDERS

Legacy defenses struggle against AI-enhanced DDoS campaigns. Static signatures, manual response, and limited visibility are no longer sufficient. Effective defense requires intelligence-driven, automated, and adaptive protection.

Key Takeaway

AI-enhanced DDoS attacks are an operational reality. Organizations that delay modernization face increased operational, financial, and reputational risk.

READ THE FULL DDOS THREAT INTELLIGENCE REPORT – ISSUE 16

Explore detailed regional analysis, botnet and threat-actor insights, and AI-driven attack techniques.

WWW.NETSCOUT.COM/THREATREPORT

NETSCOUT

SECG_035_EN-2601 02/2026