NETSCOUT

NEWS RELEASE

New NETSCOUT Research Confirms DDoS Continues to Dominate the Digital Battlefield, Destabilizing Critical Infrastructure

2025-08-27

AI integration, persistent hacktivist campaigns, and nation-state actors weaponize DDoS attacks, creating unprecedented risks for organizations globally

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT® SYSTEMS, INC. (NASDAQ: NTCT), today released its **latest research** detailing the evolving Distributed Denial-of-Service (DDoS) attack landscape. NETSCOUT monitored more than 8 million DDoS attacks globally in the first half of 2025, including more than 3.2 million in EMEA. DDoS attacks have evolved into precision-guided weapons of geopolitical influence capable of destabilizing critical infrastructure.

Hacktivist groups like NoName057(16) orchestrated hundreds of coordinated strikes each month, targeting the communications, transportation, energy, and defense sectors. DDoS-for-hire services have democratized attack tools, enabling novice actors to execute sophisticated attack campaigns. AI-enhanced automation, multi-vector attacks, and carpet bombing techniques challenge traditional defenses. Botnets compromised tens of thousands of IoT devices, servers, and routers, delivering sustained attacks and causing significant disruption. While each of these elements is dangerous on its own, in aggregate, they have formed the perfect storm, creating unprecedented cyber risk for organizations and service provider networks around the world.

Key research findings include:

- Massive Global Attack Volume – NETSCOUT observed more than 50 attacks greater than a terabit-per-second (Tbps) and multiple gigapacket-per-second (Gpps) attacks in the first half of 2025, including a 3.12 Tbps attack in the Netherlands and a 1.5 Gpps attack in the United States.
- Geopolitical Events Triggered Unprecedented DDoS Attacks – The India-Pakistan conflict saw hacktivist groups

target the Indian government and financial sectors in May, while the Iran-Israel conflict generated more than 15,000 attacks against Iran and 279 against Israel in June.

- Botnet-Driven Attacks Gained Sophistication – More than 880 bot-driven DDoS attacks occurred daily in March, peaking at 1,600 incidents, with attack durations increasing to an average of 18 minutes.
- New Threat Actors Emerged – Leveraging DDoS-for-hire infrastructure, DieNet orchestrated over 60 attacks since March, while Keymous+ launched 73 attacks across 28 industry sectors in 23 countries.
- NoName057(16) Maintained Dominance – Claiming more than 475 attacks in March alone, 337% more than the next most active group, the hacktivist group targeted government websites in Spain, Taiwan, and Ukraine.

“As hacktivist groups leverage more automation, shared infrastructure, and evolving tactics, organizations must recognize that traditional defenses are no longer sufficient,” stated Richard Hummel, director, threat intelligence, NETSCOUT. “The **integration of AI assistants** and the use of large language models (LLMs), such as WormGPT and FraudGPT, escalates that concern. And, while the recent **takedown of NoName057(16)** was successful in temporarily reducing the group’s DDoS botnet activities, preventing a future return to the top DDoS hacktivist threat is not guaranteed. Organizations need intelligence-driven, proven DDoS defenses that can deal with the sophisticated attacks we see today.”

NETSCOUT maps the DDoS landscape through passive, active, and reactive vantage points, providing unparalleled visibility into global attack trends. NETSCOUT protects two-thirds of the routed IPv4 space, securing network edges that carried global peak traffic of over 800 Tbps in 1H2025. It monitors tens of thousands of daily DDoS attacks by tracking multiple botnets and DDoS-for-hire services that leverage millions of abused or compromised devices.

Visit our **website** to learn more about NETSCOUT's DDoS Threat Intelligence Report. For real-time DDoS attack stats and insights, visit **NETSCOUT Cyber Threat Horizon**.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance and availability disruptions through its unique visibility platform and solutions powered by its pioneering deep packet inspection at scale technology. NETSCOUT serves the world’s largest enterprises, service providers, and public sector organizations. Learn more at **www.netscout.com** or follow @NETSCOUT on **LinkedIn**, **X**, or **Facebook**.

Editorial Contacts:

Chris Lucas
NETSCOUT Systems, Inc.

+1 978 614 4124
chris.lucas@netscout.com

Chris Shattuck
Finn Partners for NETSCOUT
+1 404 502 6755
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC