NETSCOUT

NEWS RELEASE

NETSCOUT Reveals Qualitative Shifts in DDoS Attack Sophistication, Infrastructure Capacity, and Threat Actor Capabilities

2026-03-04

AI Adoption, coordinated botnets, and persistent hacktivists groups drove millions of attacks

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT® SYSTEMS, INC. (NASDAQ: NTCT), today released its second half of the year 2025 Distributed Denial-of-Service (DDoS) Threat Intelligence Report, revealing sophisticated attacker collaboration, resilient botnets, and compromised IoT infrastructure that drove more than eight million DDoS attacks worldwide – some as large as 30 terabits per second (Tbps) – marking a new era of hyper-scale, coordinated threat activity that continues to outpace global takedown efforts. Meanwhile, the accelerating growth of DDoS-for-hire services is empowering a broader range of threat actors, intensifying operational risk to digitally connected organizations and enterprises.

Implications for security professionals extend far beyond volumetric concerns and include reconnaissance and adaptive evasion which challenge traditional defense paradigms. Organizations must match adversarial innovation with intelligent, autonomous defenses, or risk operational disruption at levels previously considered theoretical.

“Threat actors identify organizations that haven’t invested in the right defenses to stay ahead of sophisticated and coordinated DDoS attacks to take down critical infrastructure,” stated Richard Hummel, director, threat intelligence, NETSCOUT. “Traditional security defenses are no longer working, and with attackers hitting new attack size and complexity ceilings, implementing automated and proactive defenses has become a business-level risk mandate – not just a technical concern for security professionals.”

Key research findings include:

- Massive Attacks on a Global Scale – More than eight million attacks were identified across 203 countries and territories globally.
- Continued Use of Multi-Vector Attacks – approximately 42% of DDoS attacks employed two to five distinct attack vectors, with some adapting dynamically throughout the attack to complicate detection and mitigation.
- Outbound Attacks Impact Broadband and Mobile Services – Extensive direct-path attacks revealed that compromised IoT and customer-premises equipment can generate outbound floods exceeding 1 Tbps, creating liability, service, and reputational risk for broadband and mobile providers.
- Critical Infrastructure Targeted – High-value services such as NTP and DNS continue to face sustained attack pressure, emphasizing the need for resilient, globally distributed architectures to maintain service continuity.
- Threat Actors Scale Up Collaboration – A surge of more than 20,000 botnet-driven attacks in July 2025 exemplified how coordinated threat activity can rapidly overwhelm defenses and disrupt critical government, finance, and transportation services.
- Threat Actor Persistence – Despite international law enforcement dismantling multiple DDoS-for-hire platforms, hacktivist groups and botnets remain resilient, exerting increased pressure.
- AI Integration Accelerates Operations and Collaboration – AI has transitioned to an operational reality, with large language models (LLMs) on the dark web accelerating vulnerability exploitation and botnet expansion, and underground forums documenting a 219% increase in mentions of malicious AI tools. Groups like Keymous+ have demonstrated how partnerships between threat actors amplify attack power, with bandwidth increasing nearly fourfold.

NETSCOUT maps the DDoS landscape through passive, internet vantage points, providing unparalleled visibility into global attack trends. For more than 15 years, NETSCOUT has delivered trusted, consistent DDoS Intelligence based exclusively on directly observed, verifiable attack traffic. NETSCOUT does not aggregate multiple alerts or geographically distributed events into composite peak values, ensuring accuracy, repeatability, and true comparability across reporting periods. Peak metrics reflect single-second maximum bits-per-second (bps) and packets-per-second (pps) rates measured at defined mitigation and monitoring points.

NETSCOUT protects two-thirds of the routed IPv4 space, securing network edges that carried global peak traffic of over 800 Tbps, covering 376 industry verticals and 12,698 Autonomous System Numbers (ASNs) in the second half of 2025. 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.

Resources:

- Download the **NETSCOUT's DDoS Threat Intelligence Report H2 2025**
- See real-time DDoS attack stats and insights by visiting **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