UNMASKING THE SWARM: THE EVOLVING TACTICS OF BOTNET-DRIVEN DDoS ATTACKS

DDoS Threat Intelligence Report

ISSUE 16: FINDINGS FROM 2H 2025

NETSCOUT

CONTENTS

INTRODUCTION

The second half of 2025 marked a transformative period in the distributed denial-of-service (DDoS) threat landscape. Organizations worldwide faced an unprecedented convergence of challenges: the maturation of artificial intelligence (AI) as an offensive weapon, the emergence of high-capacity botnet infrastructure capable of multiterabit attacks, and the persistent evolution of DDoS-for-hire services that continue democratizing sophisticated cyberattacks despite sustained law enforcement pressure.

This report synthesizes data from NETSCOUT's ATLAS® global threat intelligence platform, which monitored more than 8 million DDoS attacks across 203 countries and territories during this period. ATLAS provides unparalleled internet visibility, collecting, analyzing, prioritizing, and disseminating data on DDoS attacks.

The findings reveal a threat environment where traditional barriers between intent and capability have effectively collapsed, where attacks up to 30 terabits per second represent the new ceiling of demonstrated capacity, and where conversational AI interfaces now guide even nontechnical adversaries through complex attack orchestration.

VISIBILITY AT A GLOBAL SCALE

800 Tbps

two-thirds of the routed IPv4 space protected

203

countries and territories impacted

376

industry verticals

12,698

autonomous system numbers (ASNs)

EXECUTIVE SUMMARY

Between July and December 2025, NETSCOUT® ATLAS telemetry recorded more than 8 million DDoS attacks globally, representing a relatively stable attack count compared to the first half of the year. However, this statistical stability masks profound qualitative shifts in attack sophistication, infrastructure capacity, and threat actor capabilities.

Massive attack capacity: The period witnessed demonstration attacks up to 30 terabits per second and 4 gigapackets per second, primarily launched via Internet of Things (IoT) botnets such as Aisuru and related TurboMirai variants.

AI integration accelerates: The integration of AI, including the use of dark-web large language models (LLMs) for DDoS attack operations transitioned from emerging trend to operational reality.

Persistent threat actor activity: Despite coordinated international law enforcement operations including Operation Eastwood targeting NoName057(16) and the dismantling of multiple DDoS-for-hire platforms, hacktivist groups and commodity botnets maintained elevated pressure throughout the period. NoName057(16) alone claimed more than 200 attacks in July, demonstrating operational resilience despite infrastructure seizures.

Infrastructure under sustained pressure: Critical internet infrastructure faced continuous assault, with DNS root servers experiencing varied attack patterns across different instances and Network Time Protocol (NTP) services generating more than 45,000 attack alerts. The attacks demonstrated both the resilience of well-architected systems and the persistent nature of modern threats.

Geographic and sectoral targeting: Government agencies, financial services, telecommunications, transportation, and hospitality sectors experienced the highest concentration of attacks. Regional analysis revealed EMEA leading with 3.3 million attacks, followed by APAC with 1.9 million, North America with 1.27 million, and Latin America with 1.01 million events.

The second half of 2025 represents not merely an evolutionary step in DDoS threats, but a fundamental shift in who can launch sophisticated attacks, how quickly they can adapt to defenses, and the maximum demonstrated impact achievable.

KEY FINDINGS

Global Scale

- The global DDoS attack landscape continues to expand, with more than 8 million attacks across 203 countries, underscoring the increasing operational risk to digitally connected enterprises.

IoT Botnets and Outbound Risk

- Massive direct-path attack demonstrations in 2025 revealed that compromised customer-premises equipment can generate outbound floods exceeding 1Tbps, creating significant liability, reputation, and service-availability risk for broadband providers.
- Eleven11 (RapperBot) was associated with more than 3,600 DDoS events between 2021 and mid-2025, frequently generating high-volume attacks, reinforcing the need for continual threat monitoring and rapid coordinated takedown strategies.

AI-Enhanced DDoS-for-Hire

- DDoS-for-hire platforms are using dark-web LLMs and conversational AI to lower barriers to attack, enabling even unskilled threat actors to launch complex, multivector campaigns with simple natural-language prompts—heightening risk for all industries.

Threat Actors Collaborate and Scale Up

- July 2025 saw a surge of more than 20,000 botnet-driven attacks, showing how coordinated threat activity can rapidly overwhelm defenses and disrupt essential government, finance, and transportation services.
- Groups such as Keymous demonstrate how partnerships between threat actors amplify attack power, with bandwidth increasing nearly 4x—a reminder that adversaries innovate and scale just like legitimate businesses.

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.
- DNS root servers maintained high availability despite continuous attack pressure.
- Broadband networks are increasingly exposed to 1+Tbps internal attacks from compromised devices, reinforcing the importance of embedded security and provider-level mitigation.
- Successful anycast-based defenses confirm that strategic traffic distribution reduces risk and strengthens uptime for critical systems.

GLOBAL AND REGIONAL ATTACKS

2H 2025

Global Attack Count

8,088,463

NAMER Attack Count

1,272,625

EMEA Attack Count

3,331,570

LATAM Attack Count

1,014,148

APAC Attack Count

1,904,602

EXPLORE IN-DEPTH ANALYSIS

VECTOR AND COMPLEXITY TRENDS

Across regions, more than half of all attacks were multivector, with 42.06 percent using 2 to 5 vectors and only about 1.12 percent using more than 10, confirming that moderate multivector complexity is now standard practice.

Frequently observed methods included DNS and DNS amplification, SSDP, SNMP, mDNS, memcached, CLDAP, NetBIOS, and mixed TCP floods (ACK, SYN, RST, SYN-ACK amplification), often blended to stress bandwidth and state simultaneously.

Attacks targeting critical infrastructure such as DNS root servers and NTP continued throughout 2025; at least 38 significant DNS root events were recorded, including a 21Gbps flood against the A root server. Meanwhile, more than 45,000 alerts with NTP components demonstrated that reflection from misconfigured NTP systems remains a widely exploited vector despite gradual remediation.

Carpet-bombing attacks steadily trended up in the last six months of 2025, beginning the period with an average of about 750 attacks per day and ending in approximately 830 per day on average.

EXPLORE IN-DEPTH ANALYSIS

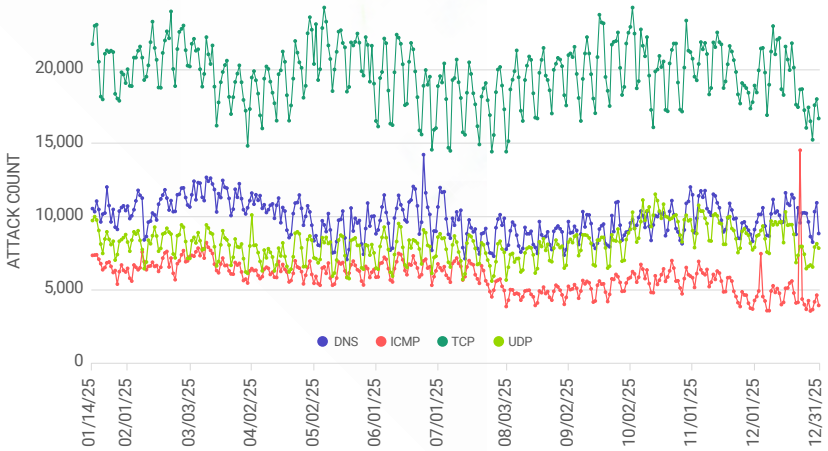


Figure 1: Global Attack Vector Type

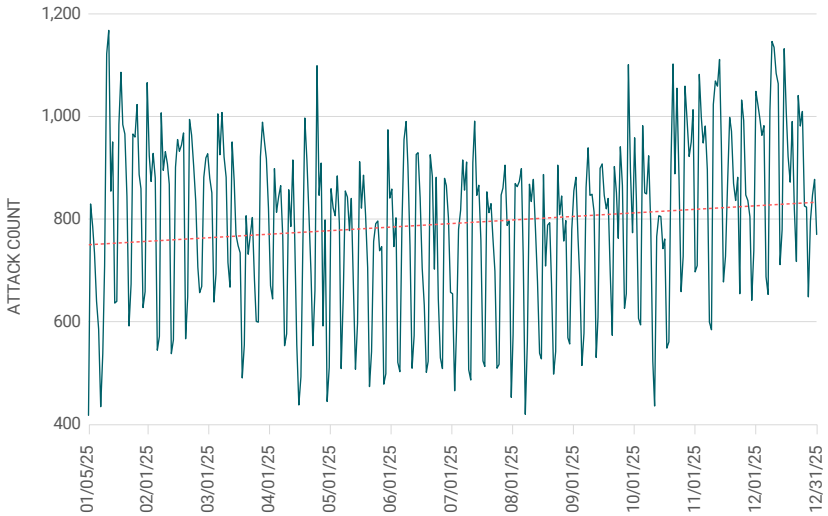
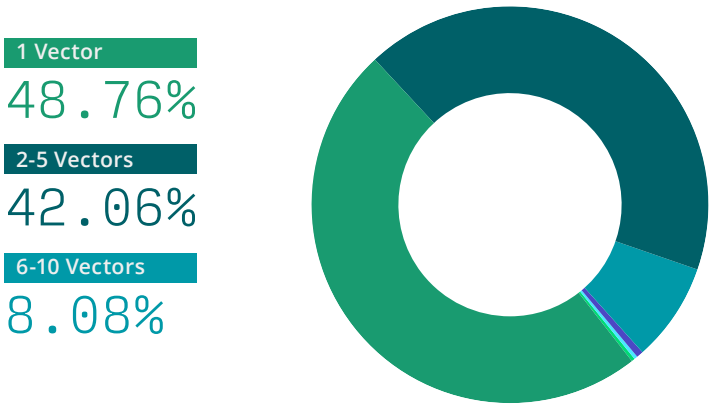


Figure 2: Daily Carpet-Bombing Attacks

Vectors by Percentage



DDoS-CAPABLE BOTNETS

TURBOMIRAI-CLASS IOT BOTNETS

A new generation of Mirai-derived IoT botnets, collectively referred to as TurboMirai, represents one of the most important developments in DDoS infrastructure during 2025. These botnets, including Aisuru and Eleven11, are characterized by high per-node output, multi-Tbps and multi-Gpps attack capability, and a focus on direct-path packet floods rather than spoofed reflection, often relying on compromised broadband customer-premises equipment (CPE), cameras, and routers.

Aisuru

- Aisuru launched direct-path attacks up to 30Tbps and 4Gpps, primarily targeting online gaming organizations, and generated outbound attack traffic above 1Tbps from compromised customer-premises devices in several broadband networks.
- The botnet retained classical Mirai capabilities (UDP/TCP/GRE floods, DNS query flooding) and added carpet-bombing, pseudo-randomized source/destination ports and TCP flag combinations, and an onboard residential proxy service to reflect HTTPS application-layer DDoS.

Eleven11 (RapperBot)

- Eleven11 was associated with more than 3,600 DDoS events between 2021 and mid-2025 and could generate hundreds of Gbps per attack before authorities disrupted its infrastructure following mid-2025 arrests.
- Operators relied on alternative DNS roots such as OpenNIC (.libre domains) and later ICANN gTLDs (.live, .info), storing C2 IPs in TXT records (plaintext or encrypted) to enable flexible, stealthy reconfiguration.

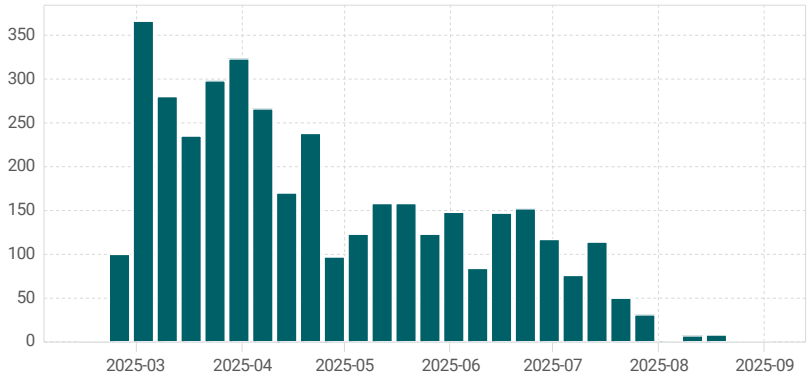


Figure 3: ML-identified Eleven11 Alerts

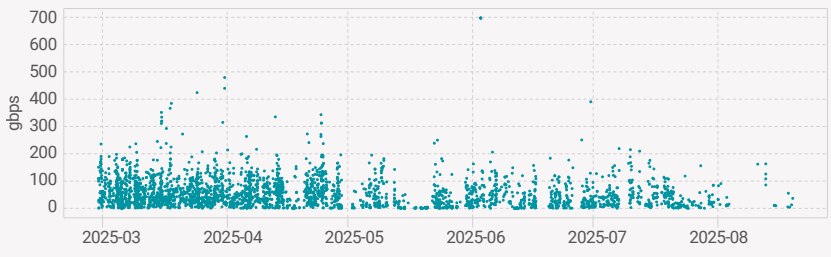


Figure 4: Eleven11 Alert Impact

Because TurboMirai-class bots run without privileged access, they cannot spoof IP addresses, making attack traffic traceable to actual on-net devices—an important advantage for defenders with sufficient visibility and remediation processes.

EXPLORE IN-DEPTH ANALYSIS

VULNERABILITIES AND PROPAGATION

DDoS botnets continued to exploit long-standing vulnerabilities in routers, cameras, and other embedded systems, with most observed exploitation attempts closely linked to TurboMirai and related legacy variants, often combined with brute-force attacks on Telnet and other remote-access services. Observed exploitation included CVE-2015-2051 (D-Link routers), CVE-2017-17215 (Huawei HG532 routers), and a variety of more recent remote-execution and configuration-abuse flaws in service-provider and CPE equipment.

Campaigns frequently focused on specific device ecosystems—for example, VStarcam cameras or Actiontec C1000A routers—to ensure scalable, repeatable enrollment into botnets. Many compromised devices remained active in attacks over multiple days due to poor patching practices, default credentials, and limited operator visibility.

OUTBOUND AND CROSSBOUND DDoS

Outbound and crossbound DDoS traffic emerged as a critical operational challenge, especially for broadband and mobile operators whose networks hosted significant botnet populations. Providers reported incidents where outbound Aisuru traffic beyond 1Tbps or 1Gpps disrupted access and aggregation infrastructure, causing line-card failures and impacting unrelated subscribers.

In mobile and fixed wireless environments, carpet-bombing and botnet propagation traffic stressed stateful packet core components, NAT resources, and radio spectrum.

THREAT ACTORS AND CAMPAIGNS

NoName057(16) and July 2025 Botnet Pulse

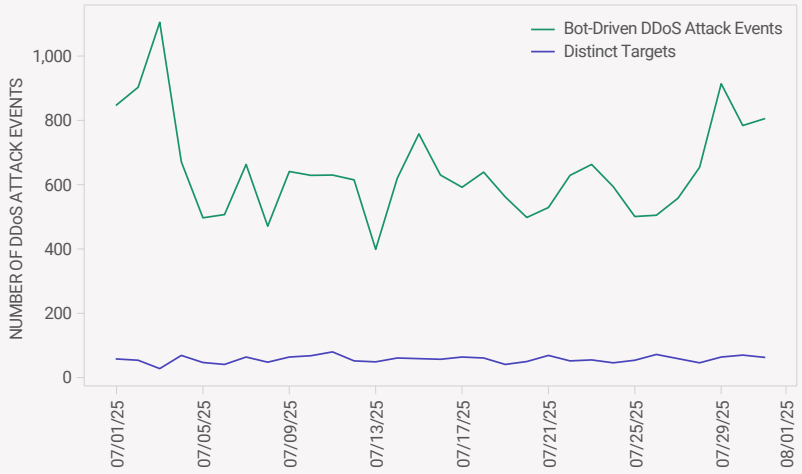


Figure 5: Daily Bot-Driven Attack Events | July 2025

July 2025 illustrated the sustained pressure on service-provider backbones and transit networks, with more than 20,000 DDoS events recorded and more than 600 attacks per day on average. Activity peaked at 1,105 events on July 3, coinciding with U.S. holiday traffic and new botnet deployments, including Go-based flooders such as hpingbot.

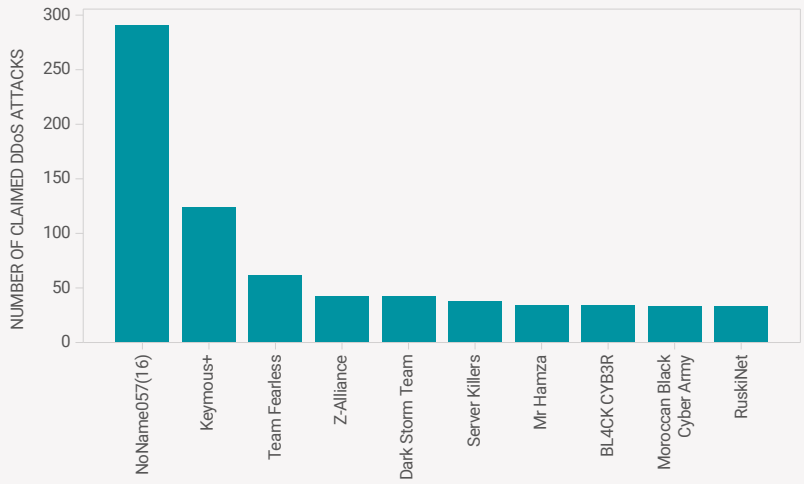


Figure 6: Claimed DDoS Attacks by Threat Actor | July 2025

Hacktivist collective NoName057(16) accounted for more than 200 of roughly 700 claimed attacks and showed strong alignment between public announcements and observed traffic. Typical campaigns used multivector strategies including HTTP/2 POST floods and TCP ACK/SYN blends, targeting government, transportation, and financial services, often using CDNs and cloud providers as traffic sources or relays to complicate mitigation.

Keymous and DDoS54

Figure 7: Keymous+ DDoS Attack Campaigns

Between February and September 2025, Keymous conducted 249 DDoS attacks across 60 organizations in 21 industries and 15 countries, with peak individual bandwidth at 11.8Gbps and collaborative events reaching 44Gbps. Top targeted industries included government, hospitality, transportation, financial services, and telecommunications, with geographic concentration in Morocco, Saudi Arabia, Sudan, India, and France.

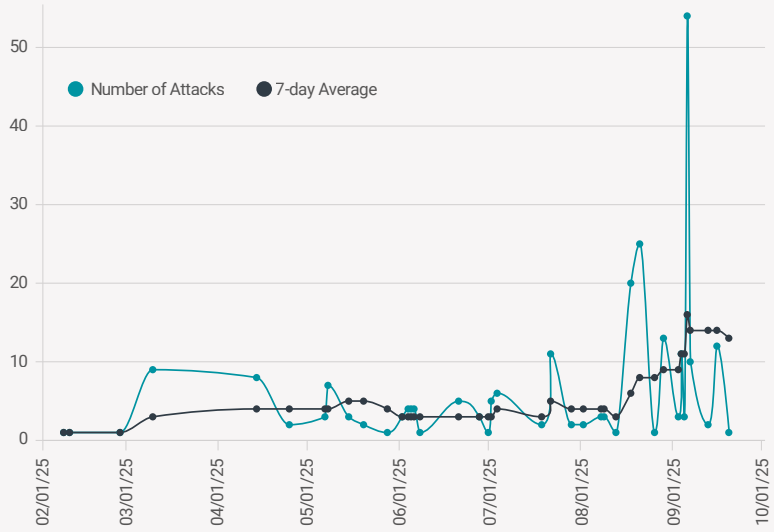


Figure 8: Daily Attack Frequency - Keymous+

Keymous attacks were notable for:

- Human-directed timing, with more than 30 percent of attacks occurring around 06:00 UTC to coincide with morning operational peaks in North Africa and the Middle East.
- Diverse infrastructure spanning Tor, public cloud instances, compromised IoT and consumer devices, and commercial VPN/proxy services, yielding tens to hundreds of thousands of unique source IPs per campaign.

A confirmed partnership with DDoS54 announced April 12, 2025, resulted in a 44Gbps multivector CLDAP and DNS amplification campaign with 4.23Mpps and 1,312-byte packets, illustrating the impact of threat-actor collaboration on attack scale.

CRITICAL INFRASTRUCTURE UNDER PRESSURE

Analysis of DDoS activity against DNS root servers identified at least 38 significant attacks in 2025, including a 21Gbps flood targeting the A root server on August 17. Although the root system's anycast design and capacity mitigated user-visible impact, the attacks underscore adversary interest in testing the resilience of key internet infrastructure.

NTP-based DDoS remained prevalent; more than 45,000 DDoS alerts included NTP traffic components, spanning both classic reflection/amplification and misconfiguration-driven time-synchronization floods. These events reinforced the need for consistent hardening of time services and monitoring for anomalous timing traffic patterns.

DNS Root Server Resilience

Despite continuous attack pressure throughout the period, the DNS root server system maintained high availability, validating the effectiveness of anycast deployment, operational diversity, and comprehensive capacity provisioning. Analysis revealed striking disparities in attack volume across different root instances:

A root

Received most frequent attacks, possibly due to alphabetical position prompting attacker selection

M root

Faced numerous diverse attack vectors

D and H–L roots

Primarily experienced ICMP probing rather than sustained flooding

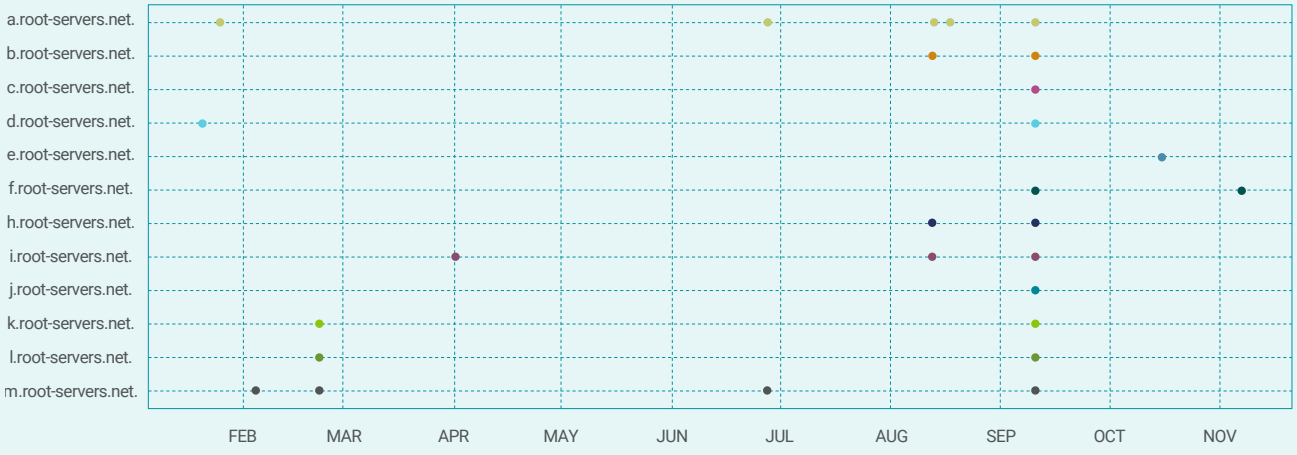


Figure 9: Chronological Overview

The strongest volumetric attack reached 21Gbps targeting the A root server on August 17, 2025. While significant for individual operators, this attack volume remained well below root system capacity thresholds, demonstrating the value of distributed infrastructure resilience.

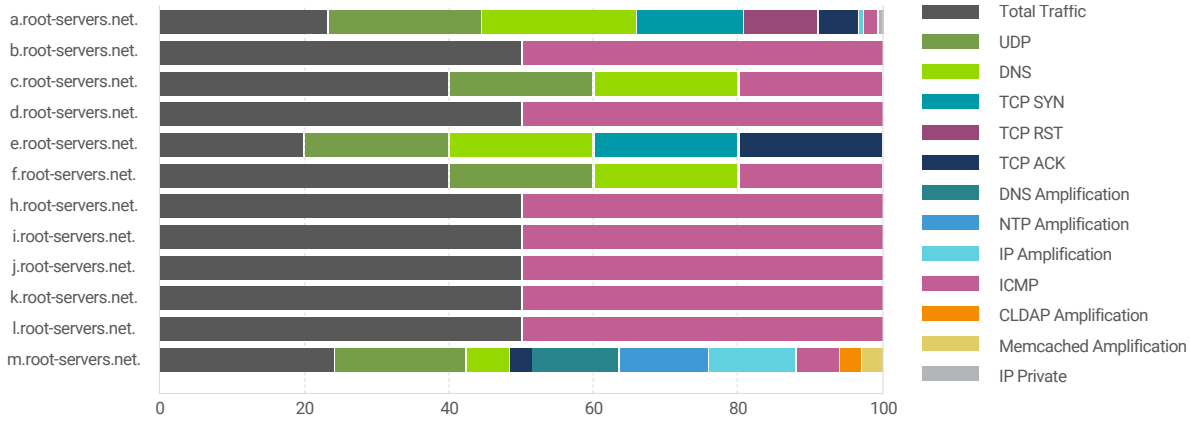


Figure 10: DDoS Attack Events Chronogical View

Geographic and topological factors contributed to varying exposure: Instances with more anycast deployments or strategic positioning attracted more legitimate traffic and consequently more attack traffic. However, the isolation provided by anycast simultaneously prevented localized attacks from affecting global root system availability.

NTP Service Exploitation

Network Time Protocol (NTP) services generated more than 45,000 DDoS alerts during the period, with approximately one-fourth (12,000 alerts) triggered by NTP-specific detection logic. While this represents a relatively small proportion compared with total attack volume, NTP's ubiquity and critical role in authentication, logging, and system synchronization makes any exploitation concerning.

Analysis of NTP activity across honeypots, vulnerability scanning, and attack telemetry revealed three key findings:

Scanner activity remains elevated:

Unsolicited NTP traffic predominantly consists of mode 7 (private/management) messages probing for monlist functionality, mode 3 (client synchronization) messages from research projects, and mode 6 (control) messages from unknown sources.

Vulnerable population declining but persistent:

Although historically measured in hundreds of thousands, abuseable NTP systems now number in the low thousands. However, these remaining systems continue generating reflection/amplification attacks due to delayed patching or abandonment.

Traffic predictability enables defense:

Legitimate NTP traffic exhibits highly consistent patterns (predominantly mode 3, fixed 48-byte UDP payload). This predictability enables precise filtering during attacks, allowing defenders to drop anomalous NTP traffic while maintaining time synchronization.

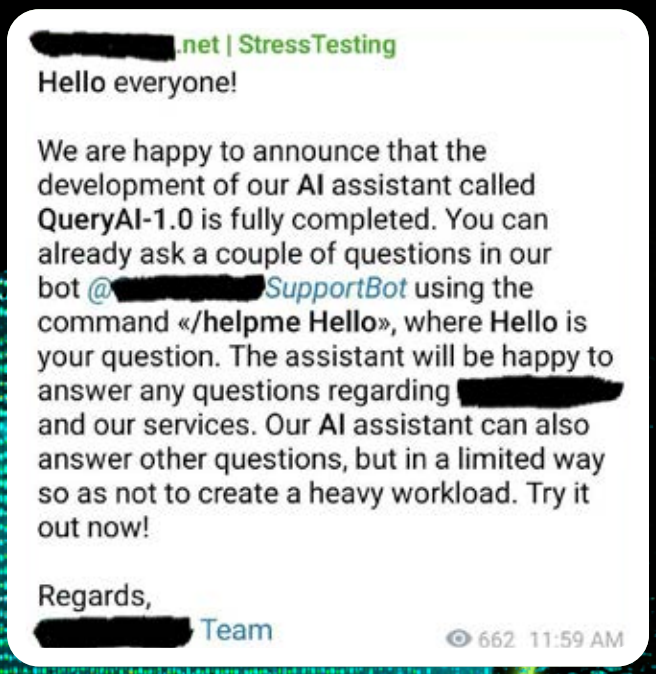
The concentration of vulnerable NTP systems across diverse hosting providers prevents simple network-level blocking but enables targeted threat intelligence sharing to inform protective measures.

AI-ENHANCED DDoS AND CHATBOT-DRIVEN COORDINATION

FROM AUTOMATED TO INTELLIGENT DDoS-FOR-HIRE

The DDoS-for-hire ecosystem entered a new phase in 2025 as conversational AI assistants began integrating directly into stresser platforms, with QueryAI-1.0 on <stresserName>.net serving as a concrete example.

Historically, these services evolved from manual tools to automated portals offering attack scheduling, APIs, reconnaissance, and adaptive logic; conversational AI now builds on this by allowing operators to define objectives in plain language while the system manages all technical details.



In an AI-integrated DDoS-for-hire platform, the assistant can:

- Perform target reconnaissance and basic vulnerability assessment to identify optimal attack surfaces
- Select attack vectors, parameters, and timing based on desired outcomes (for example, outages during specific events) without the user needing protocol knowledge

DEMOCRATIZATION ACCELERATOR

Conversational AI interfaces amplify an already democratized threat landscape where booter services and malicious LLMs have long lowered technical barriers. Dark-web models such as WormGPT and FraudGPT, priced around $60–$200 per month, show how nontechnical users can already generate malware and phishing content, while inexpensive voice-cloning tools allow realistic social engineering at scale.

Embedding similar AI capabilities in DDoS-for-hire services eliminates nearly all remaining friction:

Users can request outcomes ("disrupt this site during business hours in Europe") instead of configuring ports, protocols, or packet sizes.

The AI agent can suggest refinements based on failed attempts ("try targeting their API endpoints instead" or "shift focus to regional data centers"), turning DDoS into a conversational, iterative process.

Threat-intelligence monitoring across thousands of underground channels has documented a 219 percent increase in mentions of malicious AI tools and a 52 percent increase in jailbreak-related discussions, alongside concrete cases where exploit scanners such as KuroCracks leveraged ChatGPT to optimize code for vulnerability CVE-2024-10914. These developments drastically shorten the time from disclosure to weaponization and expand the pool of capable threat actors.

CONCLUSION

The DDoS landscape in the second half of 2025 combined sustained global attack volume, increasingly capable IoT botnets, sophisticated threat-actor campaigns, and a decisive shift toward AI-enhanced DDoS-for-hire operations. While volumetric and high-pps peaks remain relatively rare, they continue to shape defensive requirements, and the average attack is now short, intense, and often multivector, targeting a broad range of industries and geographies.

CONTRIBUTORS

Chris Conrad, Writer/Editor
Richard Hummel, Writer/Editor
Roland Dobbins, Writer
John Kristoff, Writer
Max Resing, Writer

METHODOLOGY

The data in this report is derived from NETSCOUT's ATLAS Threat Intelligence, which provides unparalleled internet visibility at a global scale, collecting, analyzing, prioritizing, and disseminating data on DDoS attacks from 203 countries and territories, 376 industry verticals, and 12,698 autonomous system numbers (ASNs).

NETSCOUT maps the DDoS landscape via passive, active, and reactive vantage points, providing unique visibility into global attack trends. We protect two-thirds of the routed IPv4 space, securing network edges that faced global peak traffic of over 800Tbps in 2H 2025. By tracking multiple botnets and DDoS-for-hire services that leverage millions of abused or compromised devices, we monitor tens of thousands of daily DDoS attacks. Our global intelligence spans attack signatures for more than 100 threat actors, ensuring proactive defense against evolving threats.

ABOUT ASERT

ASERT is NETSCOUT's elite group of engineers and researchers specializing in information security. Their breadth and depth of knowledge and real-world experience combined with NETSCOUT's unique, unrivaled visibility into global internet traffic and the threat landscape, enables them to provide insights and mediation for customers to manage active threats and their long-term security profile.

The ASERT team shares insights via threat blogs, customer advisories, and DDoS Threat Intelligence reports to increase knowledge and preparation for all global organizations dealing with evolving threats.

↗ **Learn more at netscout.com/asert**

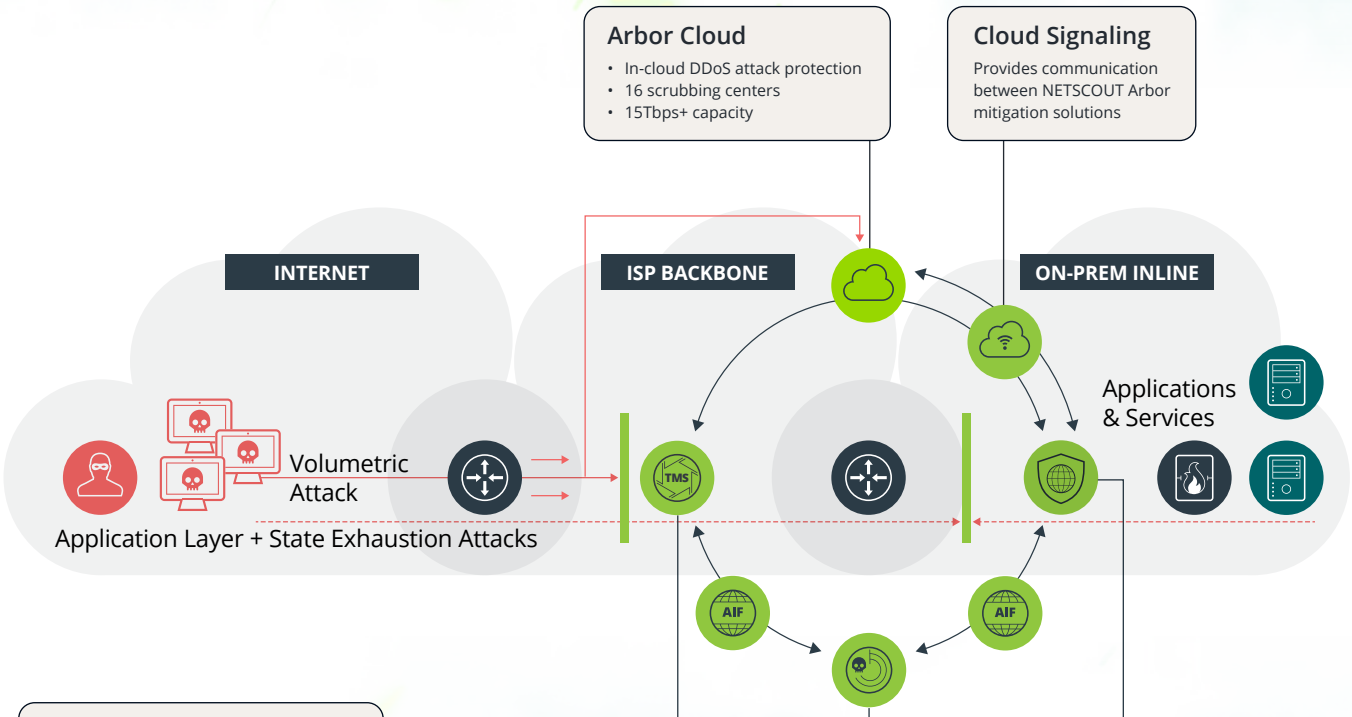
ABOUT NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) is a leading provider of observability, AIOps, cybersecurity, and DDoS attack protection solutions. NETSCOUT 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.

ATLAS Intelligence Feed (AIF) is AI-powered automated threat intelligence that continuously delivers relevant, actionable DDoS threat intelligence that is used proactively to defend against DDoS attacks and other cyberthreats. The world's most demanding government, enterprise, and service provider organizations rely on NETSCOUT's industry-leading Arbor Adaptive DDoS Protection solutions to protect the digital services that advance our connected world.

↗ **Visit netscout.com**

NETSCOUT DDoS PROTECTION SOLUTIONS



To defend against the evolving threats documented in this report, NETSCOUT offers comprehensive DDoS protection backed by the world's best AI-powered threat intelligence and more than 25 years of DDoS experience. NETSCOUT's Arbor Adaptive DDoS Protection is a purpose-built solution designed to protect the availability of your mission-critical services. Our best-in-class portfolio of products includes:

Arbor Sightline

Real-time visibility and anomaly detection using flow telemetry across service provider and enterprise networks. Provides early warning of developing attacks and enables rapid response coordination.

Arbor Edge Defense (AED)

Inline, always-on protection blocking both inbound DDoS attacks and outbound threat communications. Prevents compromised devices from participating in attacks while protecting against inbound floods.

Arbor Threat Mitigation System (TMS)

High-throughput scrubbing removing malicious traffic before reaching business-critical services. Scales to multiterabit attack volumes while maintaining legitimate traffic flow.

ATLAS Intelligence Feed (AIF)

Live global, AI-powered and human-curated threat intelligence tailored to Arbor solutions, updating blocklists and detection logic in near real-time based on observations from NETSCOUT's worldwide visibility platform.

Arbor Sightline Mobile

Specialized visibility for mobile packet core environments, providing international mobile subscriber identity (IMSI) attribution and detection of carpet-bombing attacks affecting wireless networks.

These solutions work in concert to provide defense-in-depth against the full spectrum of threats documented in this report, from AI-enhanced adaptive attacks to multiterabit IoT botnet floods to sophisticated hacktivist campaigns.

NETSCOUT.COM

Follow @NETSCOUT

NETSCOUT

©2026 NETSCOUT SYSTEMS, INC. All rights reserved.
NETSCOUT, and the NETSCOUT logo are registered trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. All other brands and product names and registered and unregistered trademarks are the sole property of their respective owners.

SECR_001_EN-2503 2H 2025 02/2026