DIGITAL AFTERSHOCKS: COLLATERAL DAMAGE FROM DDoS ATTACKS

DDoS Threat Intelligence Report

ISSUE 15: FINDINGS FROM 1H 2025

NETSCOUT®

CONTENTS

INTRODUCTION

The NETSCOUT® 1H2025 report is a concise, research-based analysis of the evolving distributed-denial-of-service (DDoS) attack and defense landscape. Designed to quickly equip readers with actionable intelligence, it delivers insights critical for ongoing network operations and strategic planning.

The digital battlefield of 2025 is defined by an unprecedented escalation in DDoS warfare, with more than 8 million attacks recorded in the first half alone. These attacks have evolved beyond simple disruption tools into precision-guided weapons of geopolitical influence, capable of destabilizing critical infrastructure at the most crucial moments. High-profile events have become focal points for this digital warfare. During the World Economic Forum in January, for example, Switzerland saw attack volumes double to over 1,400 incidents compared to similar time periods in December. This occurred alongside relentless campaigns from hacktivist groups like NoName057(16), who orchestrated hundreds of coordinated strikes monthly. Arms-length nation-state actors have weaponized DDoS to target communications, transportation, energy, and defense sectors, often operated by private industry, creating cascading effects across interconnected networks.

Driving this surge is the democratization of attack tools. Readily available DDoS-for-hire services have erased the barrier to entry, enabling even novice actors to launch sophisticated campaigns. This accessibility is amplified by new technologies: Artificial Intelligence (AI)-enhanced automation, multi-vector attacks, and carpet-bombing techniques now overwhelm traditional defenses with ease. Vast botnets compromising of tens of thousands of compromised Internet of Things (IoT) devices, servers, and routers deliver sustained attacks averaging 18 minutes, more than enough time to inflict significant operational disruption. The recent Iran-Israel cyber conflict, which generated more than 15,000 attacks, shows how quickly regional tensions rapidly escalate into global digital warfare.

This evolving threat landscape demands immediate action. Organizations can no longer rely on reactive defenses against attackers that adapt faster than security teams can respond. The integration of AI, the persistence of botnets that swiftly regroup after takedowns, and the exploitation of known vulnerabilities create a perfect storm of cyber risk. Without comprehensive visibility into attack patterns, real-time threat intelligence, and proactive mitigation strategies, organizations remain vulnerable to attacks that not only target them directly but also create collateral damage across entire service provider networks. The urgency for adaptive, intelligence-driven DDoS protection has never been greater.

KEY FINDINGS

Global DDoS Attack Volume Remains Massive, with Regional Variations:

The first half of 2025 recorded 8,062,971 attacks globally, with EMEA bearing the heaviest burden at 3.2 million attacks. Peak attacks reached devastating speeds of 3.12 Tbps and 1.5 Gpps, demonstrating sustained intensity despite volume fluctuations.

Geopolitical Events Trigger Unprecedented DDoS Campaigns:

Major political events catalyzed massive attack spikes, during the World Economic Forum Switzerland saw more than 1,400 attacks (double normal rates when compared to similar time periods in December), Italy faced sustained targeting during political discussions, and the India-Pakistan conflict saw hacktivist groups such as SYLHET GANG-SG and Keymous+ target Indian government and financial sectors, while the Iran-Israel conflict generated more than 15,000 attacks against Iran versus 279 against Israel.

Botnet-Driven Attacks Dominate with Increased Sophistication:

March 2025 averaged 880 bot-driven DDoS attacks daily, peaking at 1,600 incidents. Attack durations increased to an average of 18 minutes and 24 seconds, with threat actors employing complex multi-vector combinations and exploiting known vulnerabilities in IoT devices, servers, and routers.

NoName057(16) Maintains Dominance Among Familiar Threat Actors:

The hacktivist group claimed more than 475 attacks in March alone, 337% more than the next most active group, targeting government websites in Spain, Taiwan, and Ukraine with TCP ACK floods, TCP SYN floods, and HTTP/2 POST requests.

New Threat Actors Emerge with DDoS-as-a-Service Capabilities:

DieNet orchestrated over 60 attacks since March 2025, while Keymous+ confirmed 73 attacks across 28 industry sectors in 23 countries. Both groups leverage shared DDoS-for-hire infrastructure, lowering barriers to entry and expanding the threat landscape.

SECTION 01

BY THE NUMBERS

STATE OF DDoS

Global Highlights

Attack Count

8,062,971

To understand the gravity of today's DDoS threat landscape, we must first examine raw data revealing attack patterns across global regions. The following analysis breaks down attack volumes, vectors, and intensities that shaped the first half of 2025, providing critical context for the geopolitical and tactical trends that follow.

NAMER Highlights

Attack Count

1,306,278

Largest Attack by Throughput

Date
3/30/25

Max Throughput
612.90 Mpps

Average Packet Size
200 Bytes

Target
United States

Vectors
TCP ACK

Largest Attack by Bandwidth

Date
6/13/25

Max Bandwidth
1.48 Tbps

Average Packet Size
1,390 Bytes

Target
United States

Vectors
CLDAP Amplification, UDP Flood

LATAM Highlights

Attack Count

1,070,492

Largest Attack by Throughput

Date
2/3/25

Max Throughput
290.38 Mpps

Average Packet Size
51 Bytes

Target
Brazil

Vectors
DNS, DNS Amplification, ICMP, NTP Amplification, TCP ACK, TCP RST, TCP SYN, TCP SYN/ACK Amplification

Largest Attack by Bandwidth

Date
1/23/2025

Max Bandwidth
477.53 Gbps

Average Packet Size
1,312 Bytes

Target
Puerto Rico

Vectors
DNS, DNS Amplification, ICMP, TCP ACK, TCP RST, TCP SYN/ACK Amplification

EMEA Highlights

Attack Count

3,268,863

Largest Attack by Throughput

Date

4/25/25

Max Throughput

1.50 Gpps

Average Packet Size

36 Bytes

Target

Germany

Vectors

CLDAP Amplification, DNS, L2TP Amplification, MS SQL RS Amplification, NTP Amplification, NetBIOS Amplification, RIPv1

Largest Attack by Bandwidth

Date

2/24/25

Max Bandwidth

3.12 Tbps

Average Packet Size

1,384 Bytes

Target

Netherlands

Vectors

DNS, DNS Amplification, ICMP, L2TP Amplification, MS SQL RS Amplification, NetBIOS Amplification, RIPv1 Amplification, SNMP

APAC Highlights

Attack Count

1,846,922

Largest Attack by Throughput

Date

2/20/2025

Max Throughput

741.80 Mpps

Average Packet Size

61 Bytes

Target

Indonesia

Vectors

DNS, ICMP, TCP SYN

Largest Attack by Bandwidth

Date

3/2/2025

Max Bandwidth

1.43 Tbps

Average Packet Size

540 Bytes

Target

Australia

Vectors

CLDAP Amplification, L2TP Amplification, NTP Amplification, NetBIOS Amplification, SNMP Amplification, SSDP Amplification, TCP SYN, Chargen Amplification, mDNS Amplification

Note: The sum of regional attack counts differs from the global attack count due to differences in GeoIP enrichment availability.

TARGETED NATIONS + POLITICAL DISRUPTIONS

Global DDoS Trends Mirror Geopolitical Unrest

Although these statistics paint a sobering picture of DDoS prevalence, the numbers alone don't reveal the calculated timing and political motivations driving many attacks. The following section explores how major geopolitical events served as catalysts for coordinated DDoS campaigns, transforming digital attacks into instruments of political influence and disruption.

Switzerland

JANUARY 20-24

DDoS Attacks at the World Economic Forum

During the annual World Economic Forum (WEF) held in Davos-Klosters, Switzerland, from January 20th to 24th, several notable events garnered significant media attention. Notably, prominent political figures delivered several special addresses that drew substantial public interest. NETSCOUT's ASERT team observed a notable surge in DDoS attacks shortly preceding and during at least one of these addresses.

During the event's commencement and conclusion, ASERT detected more than 1,400 DDoS attacks of diverse magnitudes and attack vectors. Notably, the observed attack frequency during and immediately preceding the WEF was approximately double that of comparable time periods in December. The subsequent graphs illustrate the observed DDoS attack events on a daily basis. An overview is presented in Figure 1, where the gray-highlighted vertical bars signify the WEF's schedule.

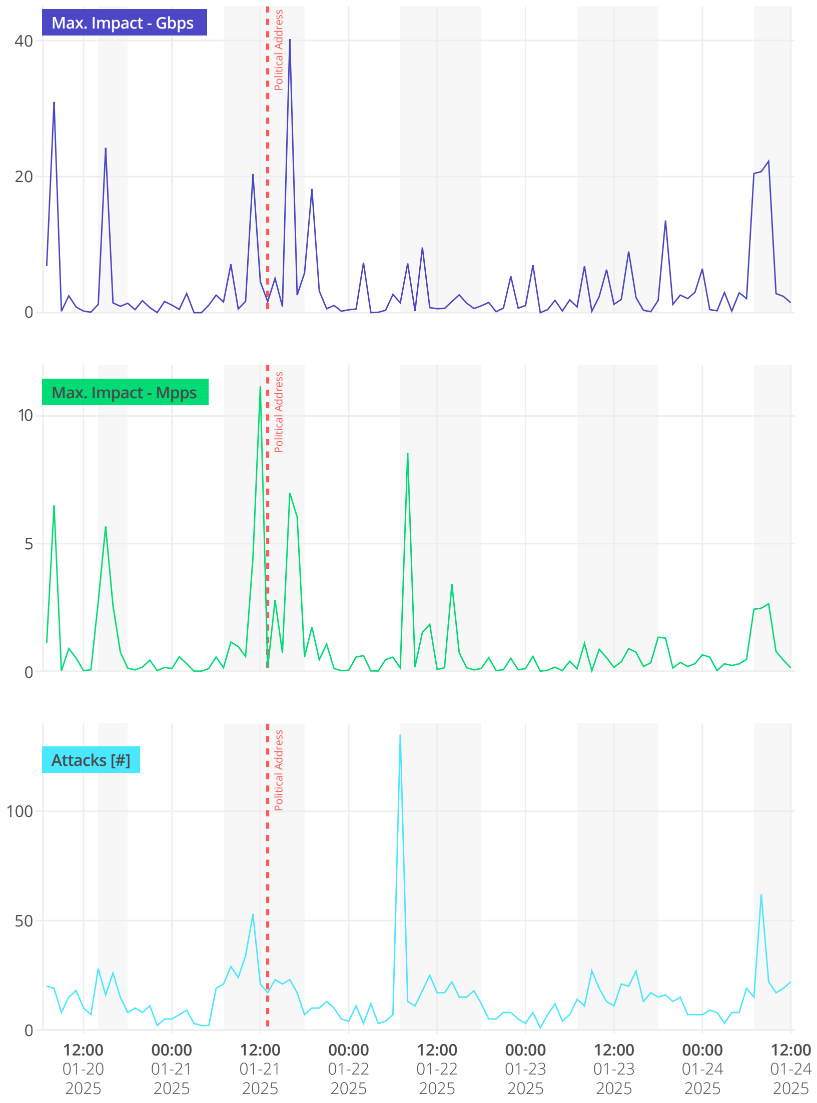


Figure 1: Three DDoS attack metrics as observed by ASERT. The grey regions mark the official schedule of the event.

Italy

FEBRUARY 16 – MARCH 03

Italy in the Crosshairs

During the period of February to March 2025, a series of political discussions appear to have attracted the attention of several threat actors, including NoName057(16). The targeted industries exhibit similar patterns observed in previous incidents. However, it is noteworthy that some additional targeting may not have been intentional.

Although ASERT primarily concentrates on DDoS research, we monitor a broad spectrum of cyber incidents by monitoring publicly reported attacks. As depicted in Figure 2, reports of cyberattacks against Italian entities experienced a surge on February 16th, persisting for two weeks before declining significantly by March 3rd.

The incidents attributed to threat actors encompass a spectrum of activities, including website defacements, network intrusions, and ransomware attacks. Notably, the most prevalent claim against Italian organizations observed was directed towards DDoS attacks. ASERT identified a substantial proportion of publicly reported DDoS attacks occurring between February 16 and March 03, which were specifically targeted at public sector entities within regional and local Italian jurisdictions.

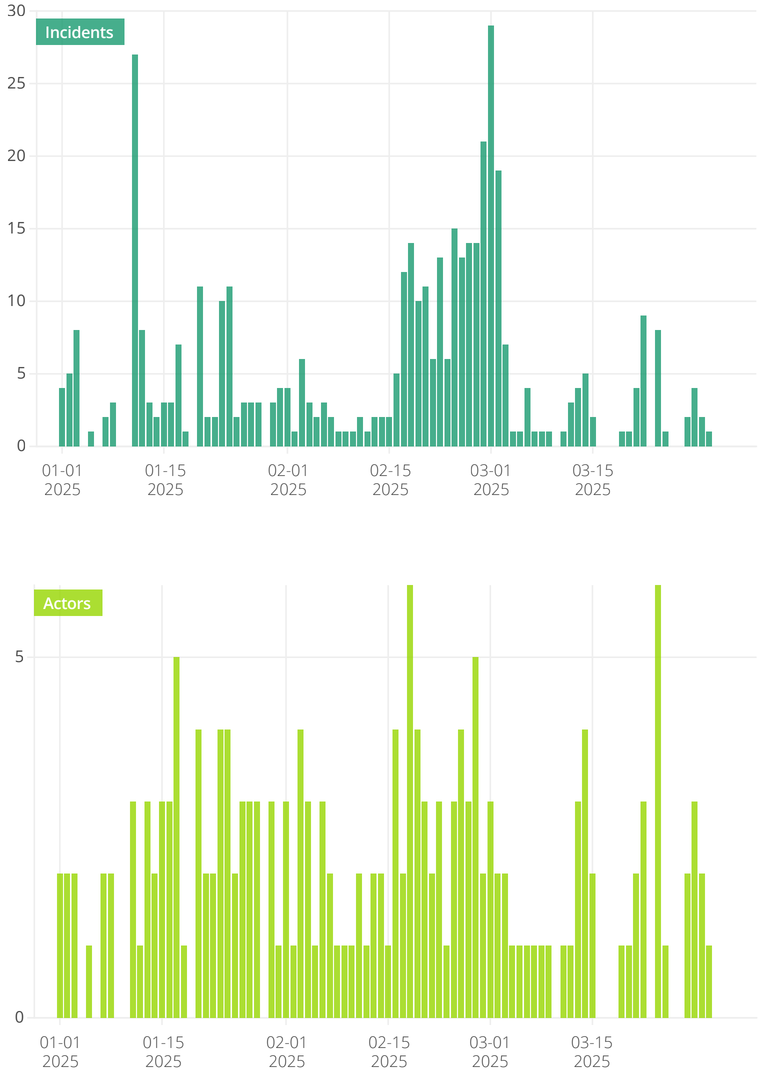


Figure 2: Overview of three months of cyber incidents publicly claimed by threat actors against Italian organizations.

India

MAY 03-09

DDoS Attacks in India Amid India-Pakistan Conflict

Escalating geopolitical tensions between India and Pakistan have extended into the realm of cyberspace, resulting in a notable surge in claims of DDoS attacks directed at Indian organizations. Hacktivist groups have seized public social media platforms to publicly display their online operations against critical Indian infrastructure. These groups include SYLHET GANG-SG, Keymous+, AnonSec, and others, which have asserted attacks on government, defense, and financial sectors. This summary analyzes these social media claims, examining the nature of the boasted attacks as reported on public platforms and contrasting them with actual impact data from NETSCOUT's ATLAS® telemetry to provide a comprehensive perspective on the situation.

In contrast to the social media claims, NETSCOUT's ATLAS telemetry offers a more comprehensive analysis of the actual impact of Distributed Denial of Service (DDoS) attacks targeting India from May 3 to May 9, 2025. The telemetry data meticulously tracks attack counts, average and maximum bandwidth in Gbps, as illustrated in Figure 4.

Indian network operators successfully mitigated these threats, preventing widespread disruptions. As the ongoing cyber conflict persists, organizations must maintain heightened vigilance, employing advanced DDoS protection and real-time threat operational intelligence to effectively counter hacktivist attack campaigns.

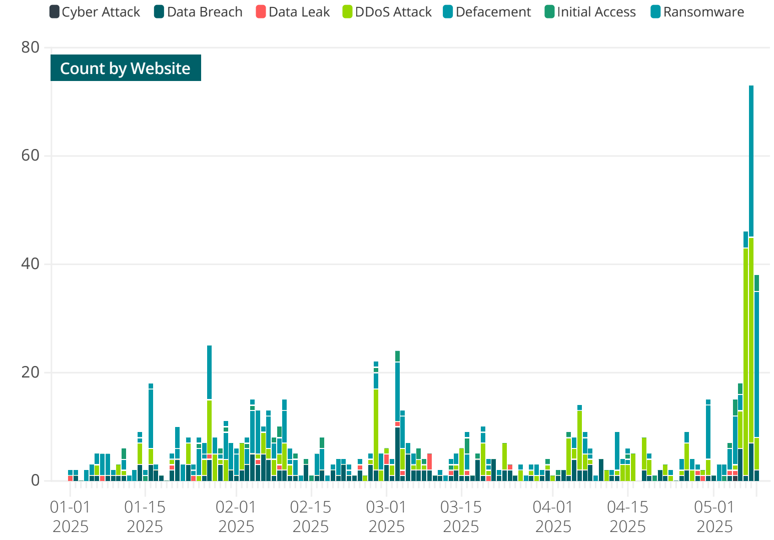


Figure 3: Adversary Attack Claims (count by website).

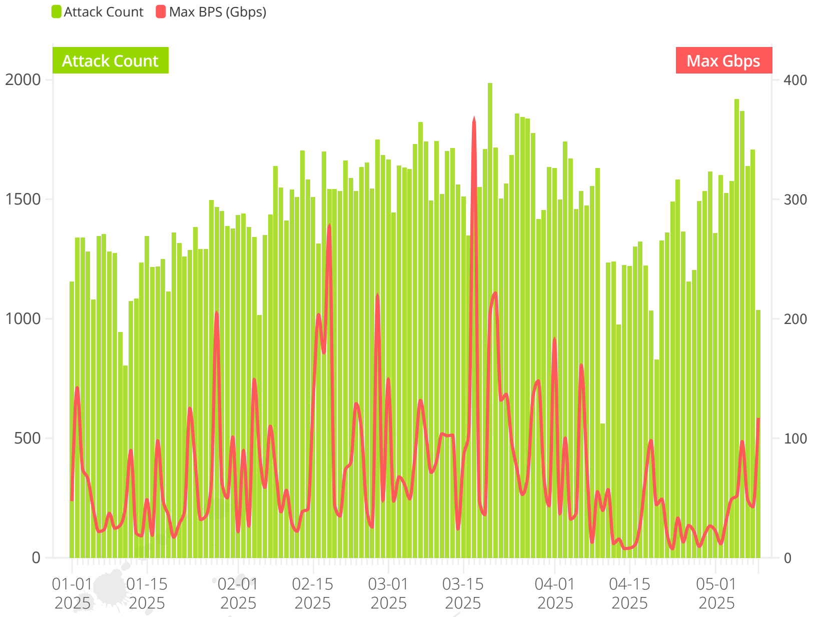


Figure 4: Daily Attack Count + Maximum Bits-Per-Second.

Iran Israel

JUNE 13

Iran-Israel Cyberwarfare Escalates

Upon the commencement of Operation Rising Lion on June 13, 2025, the Iran-Israel cyber conflict intensified, characterized by substantial DDoS attacks.

Iran endured more than 15,000 cyberattacks in comparison to Israel's 279 since June 13, 2025, with a peak of nearly 2,800 attacks occurring within a single day. This suggests Iran is a primary target, facing significantly higher pressure.

Hacktivists repeatedly targeted Elbit Systems, a prominent Israeli defense company, asserting responsibility for several disruptions. This concentration on critical infrastructure suggests potential broader risks to defense operations.

Iran's efforts to restrict internet access to mitigate cyberattacks and control communications have resulted in a decrease in online traffic, but they have not succeeded in halting attacks. These attacks persist at a high frequency. Notably, nearly all 15,000 attacks on Iran were observed from networks outside Iran. This is consistent with the nature of all DDoS attacks, where untargeted networks bear the burden of carrying DDoS attack traffic regardless of the target's status.

Hacktivist groups attacking both nations claim far more attacks than verified data shows (e.g., 900 claims versus 86 actual attacks in Israel on June 13). These inflated reports, often spread on social media, may be propaganda to amplify perceived impact, or the attacks were too small to register on DDoS detection platforms rendering them ineffective.

Israel encountered relatively simpler and lower-volume attacks employing fundamental techniques, whereas Iran encountered more intense and high-bandwidth attacks. This distinction underscores the existence of diverse threats necessitating customized defenses.

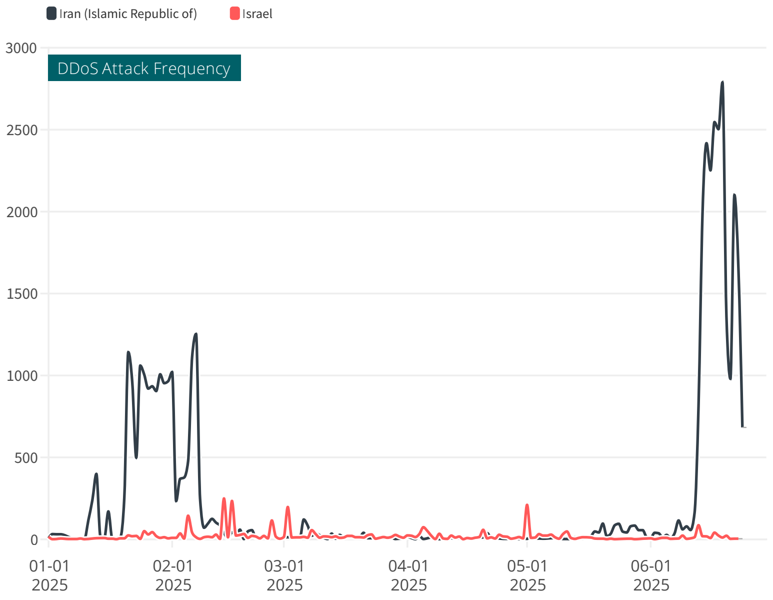


Figure 5: Daily DDoS attack frequency through June 25, 2025.

SECTION 03

Botnets and Familiar Foes Drive DDoS Attack Activity

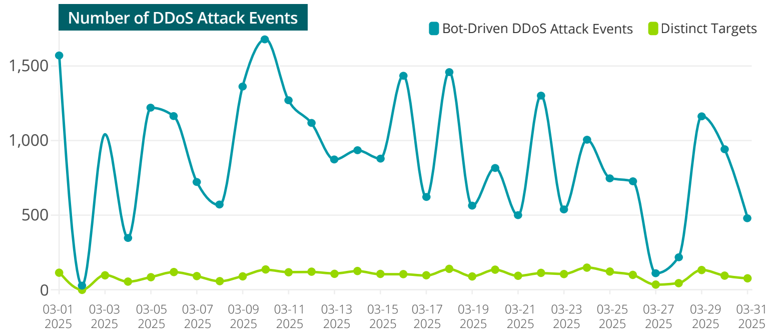
Behind these politically motivated campaigns lies a robust infrastructure of botnets and experienced threat actors who have perfected their craft. The persistence and sophistication of these groups, combined with their ability to rapidly mobilize massive bot armies, represents the operational backbone of modern DDoS warfare examined in detail below.

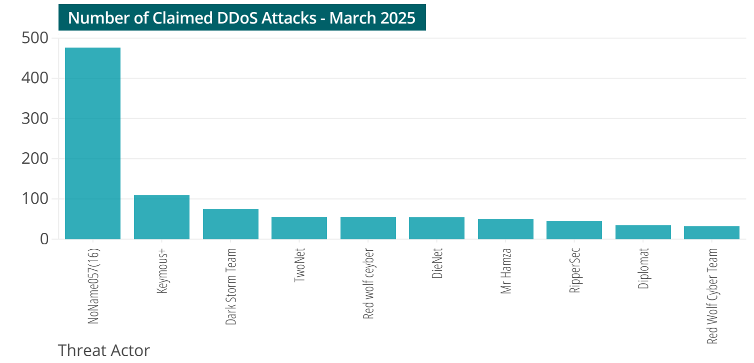
Attackers didn't need new exploits to drive more than 27,000 botnet-driven DDoS attacks in March 2025. Instead, they exploited previously known vulnerabilities to execute more sophisticated and enduring campaigns that targeted service providers with an average of one attack every two minutes. The tactics we observed align with the ongoing evolution of botnet-driven threats and the persistent strain on backbone infrastructure.

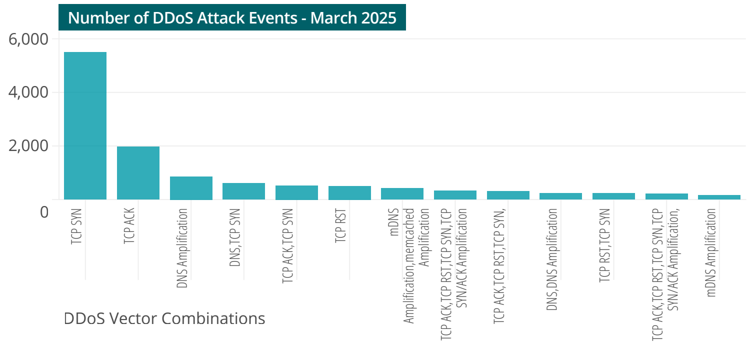
NETSCOUT detected persistent bot-driven DDoS activity directed at the service provider sector throughout March 2025. On average, approximately 880 confirmed DDoS attack events per day were recorded, with a peak on March 10 when more than 1,600 incidents were observed. These attacks were fueled by substantial, distributed botnets constructed via the exploitation of predominantly known vulnerabilities in web servers, routers, and IoT devices.

NETSCOUT's ASERT team monitors tens of thousands of distinct bots engaged in attacks each month. Although the daily volume experienced a slight decline from February's levels, attackers compensated for this by employing more intricate vector combinations, expanding their port targeting, and extending the duration of their attacks. Botnet-driven DDoS attack events persisted, with average durations exhibiting a cumulative increase compared with preceding months.

The hacktivist group NoName057 (16) maintained its dominance in both claimed operations and actual attack activity. The group frequently employed various techniques, including TCP ACK floods, TCP SYN floods, and even HTTP/2 POST requests, against predominantly government websites located in Spain, Taiwan, and Ukraine. This suggests a persistent pattern of politically motivated campaigns.







SECTION 04

A New Hacktivist Threat, Profiling DieNet

Understanding the mechanics of botnet operations provides essential context for examining the specific groups orchestrating these attacks. The following profiles reveal how both established and emerging threat actors leverage shared infrastructure and evolving tactics to achieve their ideological and destructive goals.

In the spring of 2025, DieNet, a newly formed hacktivist group, orchestrated more than 60 DDoS attacks, targeting critical infrastructure from United States transit systems to Iraqi government websites. The group made its public debut on March 7, 2025, through a now-disabled Telegram channel. ASERT has identified that DieNet utilizes DDoS-as-a-service infrastructure, shared with other groups such as OverFlame and DenBots Proof, to execute ideologically motivated attacks against the United States, Iraq, Israel, Sweden, and Egypt. DieNet's targets encompass transportation, energy, medical systems, and digital commerce. Although the group asserts some level of success, it frequently presents challenges, if not outright impossibilities, in validating the extent of its impact on the targeted entities. Nevertheless, the scale and frequency of its actions reveal the ease with which new actors can exploit rented infrastructure to launch their own DDoS campaigns.

These detailed threat actor profiles underscore a fundamental truth: the DDoS landscape has evolved into a complex ecosystem where arms-length state actors, hacktivists, and cybercriminals converge. As we look toward the future, organizations must recognize that traditional defenses are no longer sufficient against this multifaceted threat.

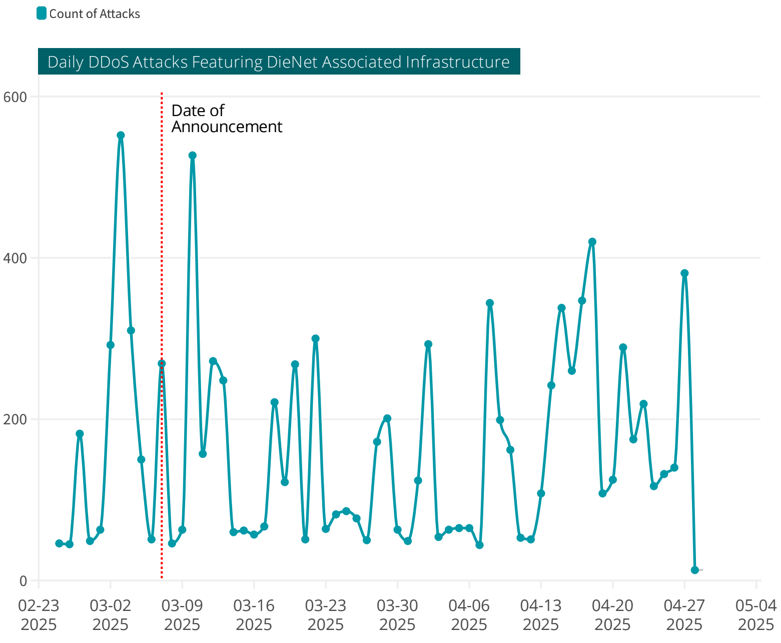


Figure 6: Daily attack count prior to and following DieNet's launch.

CONCLUSION

The relentless evolution of DDoS threats demands equally sophisticated defenses. NETSCOUT's comprehensive protection ecosystem, including Arbor Edge Defense® for perimeter security, Arbor Sightline for network-wide visibility and detection, and the Arbor Threat Mitigation System™ for surgical attack response, provides the multi-layered defense required in today's threat landscape. NETSCOUT's Arbor DDoS Protection leverages AI to counter AI-enhanced attacks, while the AI-powered ATLAS Intelligence Feed® delivers real-time threat data from defending two-thirds of global IPv4 space. As DDoS solidifies its role as a primary cyberweapon, organizations must embrace proactive, intelligence-driven strategies powered by proven solutions that outpace attackers at every turn.

CONTRIBUTORS

Chris Conrad, Writer/Editor
Richard Hummel, Writer/Editor
Gary Sockrider, Writer/Editor
Filippo Vitale, Writer
Marcin Nawrocki, Writer
Max Resing, Writer

METHODOLOGY

NETSCOUT maps the DDoS landscape via passive, active, and reactive vantage points, providing unparalleled 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 1H 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, including groups such as NoName057(16), 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 freely shares insights for global good via threat blogs, customer advisories, and the biannual DDoS Threat Intelligence Report, to increase knowledge and preparation for 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.

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 205 countries and territories, 398 industry verticals, and 15,612 autonomous system numbers (ASNs).

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.

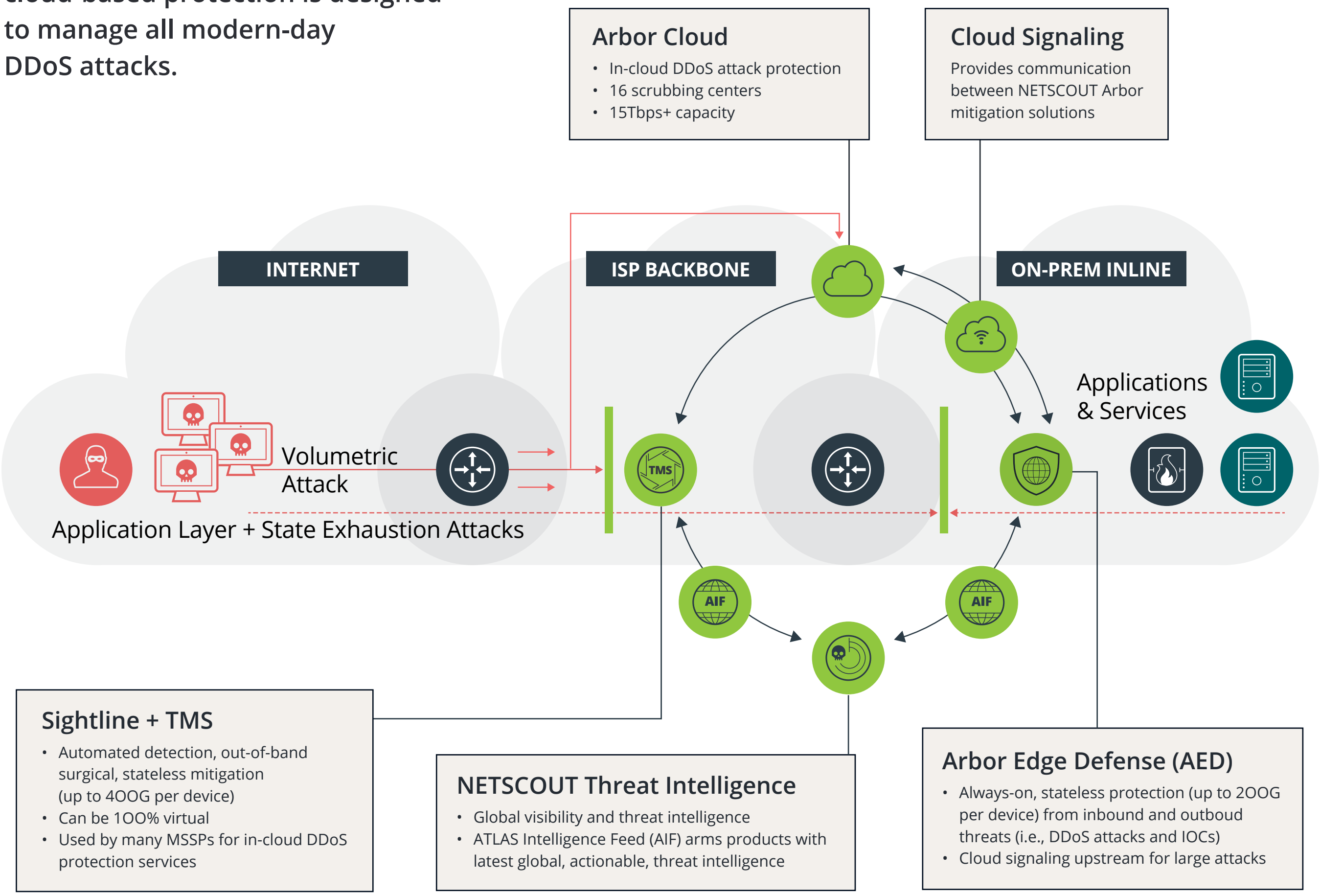
The world's most demanding government, enterprise, and service provider organizations rely on NETSCOUT's industry-leading Arbor Adaptive DDoS Protection solutions to protect the digital services that advance our connected world.

↗ **Visit netscout.com**

RELATED NETSCOUT PRODUCTS

NETSCOUT ARBOR DDoS ATTACK PROTECTION SOLUTIONS

The intelligent combination of AI/ML-powered on-premises and cloud-based protection is designed to manage all modern-day DDoS attacks.



Arbor Cloud

- In-cloud DDoS attack protection
- 16 scrubbing centers
- 15Tbps+ capacity

Cloud Signaling

Provides communication between NETSCOUT Arbor mitigation solutions

Sightline + TMS

- Automated detection, out-of-band surgical, stateless mitigation (up to 400G per device)
- Can be 100% virtual
- Used by many MSSPs for in-cloud DDoS protection services

NETSCOUT Threat Intelligence

- Global visibility and threat intelligence
- ATLAS Intelligence Feed (AIF) arms products with latest global, actionable, threat intelligence

Arbor Edge Defense (AED)

- Always-on, stateless protection (up to 200G per device) from inbound and outboud threats (i.e., DDoS attacks and IOCs)
- Cloud signaling upstream for large attacks

NETSCOUT Industry Leading Technology

NETSCOUT AI/ML technologies in the ATLAS Intelligence Feed (AIF) and Adaptive DDoS Protection, deliver proactive, dependable cybersecurity solutions that safeguard networks against evolving threats without compromising performance or accessibility.

NETSCOUT SOLUTIONS

ATLAS Intelligence Feed (AIF)

AI/ML-powered analysis continuously updates DDoS products and services.

Adaptive DDoS Protection

- Neutralizes attacks against enterprises and service providers
- Leverages AIF to automatically and accurately blocks malicious traffic
- Provides predictable, reliable behavior that ensures operational continuity for customers

BEST PRACTICES FOR

DDoS Defense

- Hybrid on-premises or inline plus cloud-based solutions
- Intelligent and automated integration
- Dynamic, adaptable AI/ML-powered DDoS protection
- Robust defenses against all types of DDoS attacks

DDoS PROTECTION FOR

Enterprise

Blending the power of AI/ML-fueled NETSCOUT Arbor Edge Defense (AED) and the massive upstream DDoS scrubbing capacity of NETSCOUT Arbor Cloud

Service Providers

AI- and ML-powered DDoS attack mitigation of NETSCOUT Arbor Sightline and NETSCOUT Arbor Threat Mitigation System (TMS) to protect complex large-scale networks

HOW NETSCOUT CAN HELP

Geopolitical Events

Geopolitical unrest serves as a driving force behind DDoS attacks. During electoral cycles, protests, and significant policy transformations, adversaries exploit vulnerable moments of national security to overwhelm critical infrastructure. Consequently, any entity can become a potential target of DDoS attacks triggered by geopolitical events. These attacks traverse service provider networks across regions, necessitating automated detection and substantial mitigation capabilities, which are provided by Arbor Sightline and TMS.

Botnet-Driven Attacks with Increased Sophistication

Botnets are becoming increasingly sophisticated, with threat actors employing intricate multi-vector combinations and exploiting known vulnerabilities in IoT devices, servers, and routers. Arbor DDoS protection offers a hybrid combination of on-premises and cloud-based mitigation, providing the most comprehensive protection against all types of DDoS attacks.

Threat Actors with DDoS-as-a-Service Capabilities

Both novel and seasoned threat actors exploit shared DDoS-for-hire infrastructure, diminishing entry barriers and expanding the threat spectrum. Advancements in DDoS-for-hire services now incorporate AI-enhanced attacks, scalability through automation, and substantially enhanced attack efficacy. Consequently, combating AI attacks necessitates employing AI defense mechanisms, as human capabilities are insufficient to keep pace. Given the automation employed in attacks, countering this necessitates employing automated adaptive DDoS defense. Arbor Edge Defense, Sightline, Threat Mitigation System and the ATLAS Intelligence Feed can effectively thwart these sophisticated attacks.

NETSCOUT.COM

Follow @NETSCOUT

NETSCOUT

SECR_001_EN-2501 1H 2025 08/2025