NETSCOUT

Digital Aftershocks: Damage from DDoS Attacks

DDoS Threat Intelligence Report

Issue 15 – for NTE 23.September 2025

Torkel Anzjøn

Principal Systems Engineer

Agenda

Global DDoS Metrics

Geopolitics & DDoS

Botnets Dominate

Hacktivist Activity

Emerging Threats

How NTE / NETSCOUT Can Help

NETSCOUT SYSTEMS Inc

90%
of the World's
Tier 1 Service Providers

90%
of the US
Fortune 100 Companies

Our Customers Include…

9 in 10
of the Largest Cloud Hosting Providers

3 in 5
of the Largest Social and Online Brands

9 in 10
of the Largest Global Financial Institutions

3,000+
Customers

100+
Countries

$ 850M+
Revenue

Highly profitable
30+ year Track Record

today

NETSCOUT ATLAS – Global Attack Visibility

DDoS Data from 2/3 of routable IP space and ~1/2 of all internet traffic

800+ Tbps Most Tier-1 & 2 ISPs

500+ Service Providers

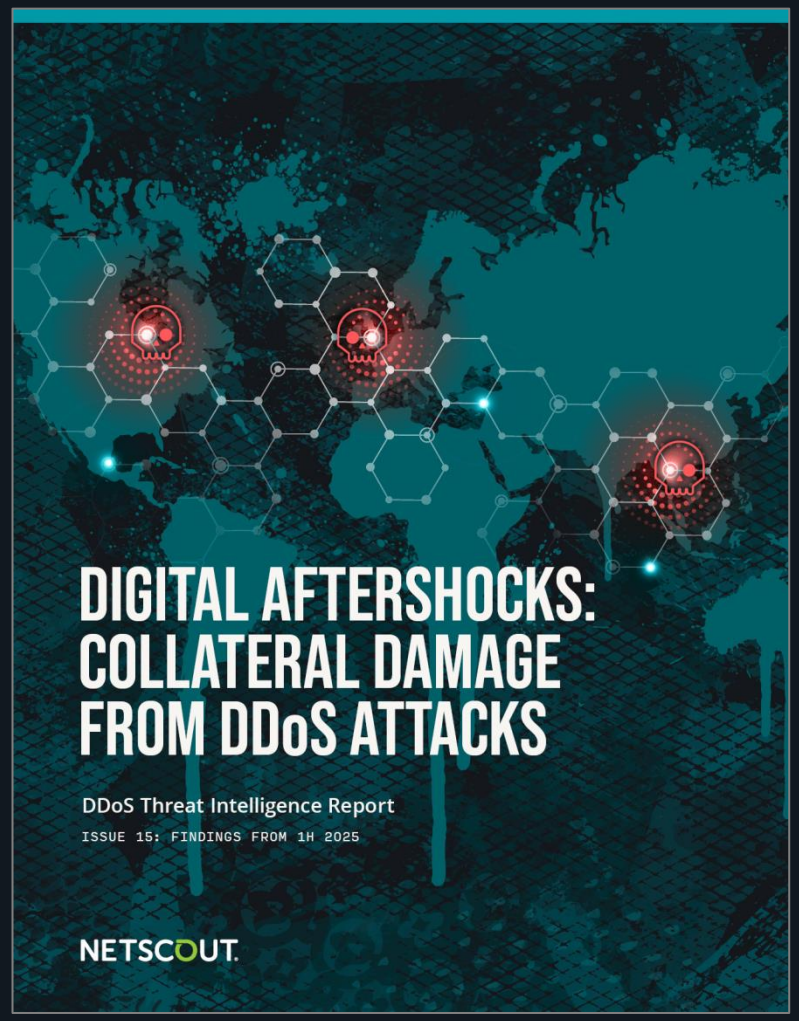
~3,000 Enterprise sites

200+ Countries

netscout.com/horizon

Key Findings

1. 1H2025 DDoS attack frequency is consistent with 1H2024 numbers
2. This period recorded the largest attacks ever seen at 3.12 Tbps & 1.5 & Gpps
3. Geopolitics continues to play a prominent role in hacktivist targeting patterns
4. Global hacktivist takedowns are needed, but insufficient
5. Emerging DDoS hacktivist groups



netscout.com/threatreport

State of DDoS: By the Numbers

Global DDoS Attack Stats 1H 2025

8,062,971 Attacks Observed in 1H 2025

Largest Attack by Bandwidth:

- Max Bandwidth 3.12 Tbps
- Average Packet Size 1,384 Bytes

Largest Attack by Throughput:

- Max Throughput 1.5 Gpps
- Average Packet Size 36 Bytes

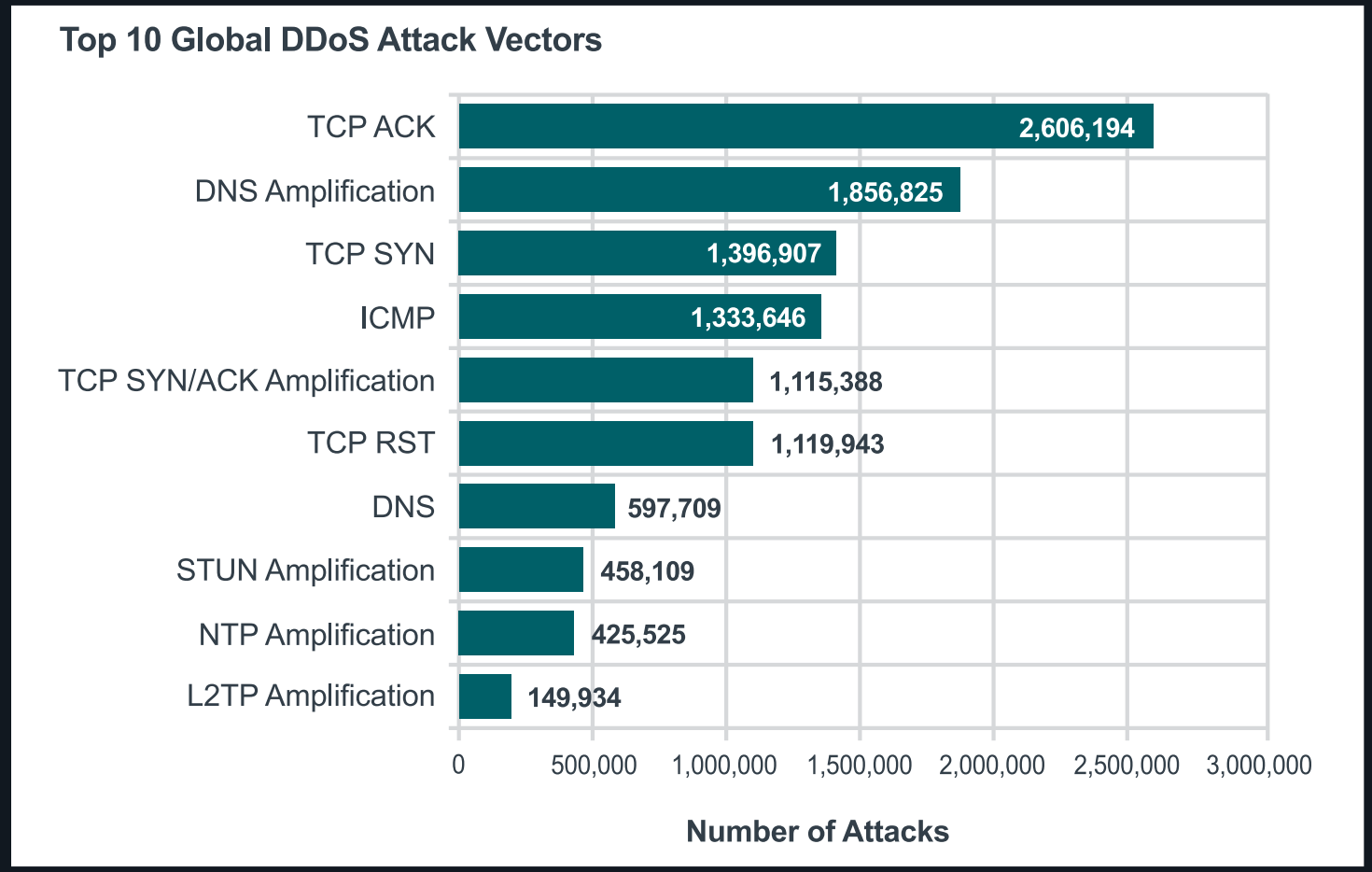
BANDWIDTH BY PERCENTAGE	
<10Mbps	20.33%
10–100Mbps	21.54%
100Mbps–1Gbps	34.45%
1–10Gbps	20.34%
10–100Gbps	3.21%
>100Gbps	0.13%

DURATION BY PERCENTAGE	
< 5 min	17.95%
5–15 min	52.51%
15–30 min	12.65%
30–60 min	6.64%
60+ min	10.25%

Multi-vector DDoS Attacks are Common

Over half of all attacks include more than one vector

VECTORS BY PERCENTAGE	
1 Vector	48.28%
2–5 Vectors	42.42%
6–10 Vectors	7.8%
11–15 Vectors	0.99%
16–20 Vectors	0.42%
21+ Vectors	0.14%



Global Attack Distribution

Regional Breakdown

NAMER

Attack Count
1,306,278

Largest Attack by Throughput	Largest Attack by Bandwidth
Date 3/30/25	**Date** 6/13/25
Max Throughput 612.90 Mpps	**Max Bandwidth** 1.48 Tbps
Average Packet Size 200 Bytes	**Average Packet Size** 1,390 Bytes
Target  United States	**Target**  United States
Vectors TCP ACK	**Vectors** CLDAP Amplification, UDP Flood

EMEA

Attack Count
3,268,863

Largest Attack by Throughput	Largest Attack by Bandwidth
Date 4/25/25	**Date** 2/24/25
Max Throughput 1.50 Gpps	**Max Bandwidth** 3.12 Tbps
Average Packet Size 36 Bytes	**Average Packet Size** 1,384 Bytes
Target  Germany	**Target**  Netherlands
Vectors CLDAP Amplification, DNS, L2TP Amplification, MS SQL RS Amplification, NTP Amplification, NetBIOS	**Vectors** DNS, DNS Amplification, ICMP, L2TP Amplification, MS SQL RS Amplification, NetBIOS

LATAM

Attack Count
1,070,492

Largest Attack by Throughput	Largest Attack by Bandwidth
Date 2/3/25	**Date** 1/23/2025
Max Throughput 290.38 Mpps	**Max Bandwidth** 477.53 Gbps
Average Packet Size 51 Bytes	**Average Packet Size** 1,312 Bytes
Target  Brazil	**Target**  Puerto Rico
Vectors DNS, DNS Amplification, ICMP, NTP Amplification, TCP ACK, TCP RST, TCP SYN, TCP SYN/ACK Amplification	**Vectors** DNS, DNS Amplification, ICMP, TCP ACK, TCP RST, TCP SYN/ACK Amplification

APAC

Attack Count
1,846,922

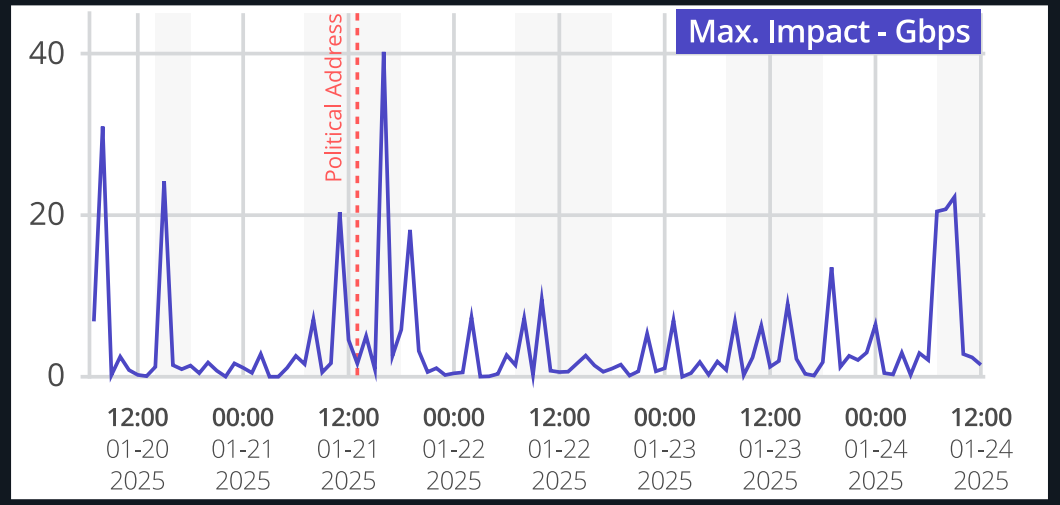
Largest Attack by Throughput	Largest Attack by Bandwidth
Date 2/20/2025	**Date** 3/2/2025
Max Throughput 741.80 Mpps	**Max Bandwidth** 1.43 Tbps
Average Packet Size 61 Bytes	**Average Packet Size** 540 Bytes
Target  Indonesia	**Target**  Australia
Vectors DNS, ICMP, TCP SYN	**Vectors** CLDAP Amplification, L2TP Amplification, NTP Amplification,

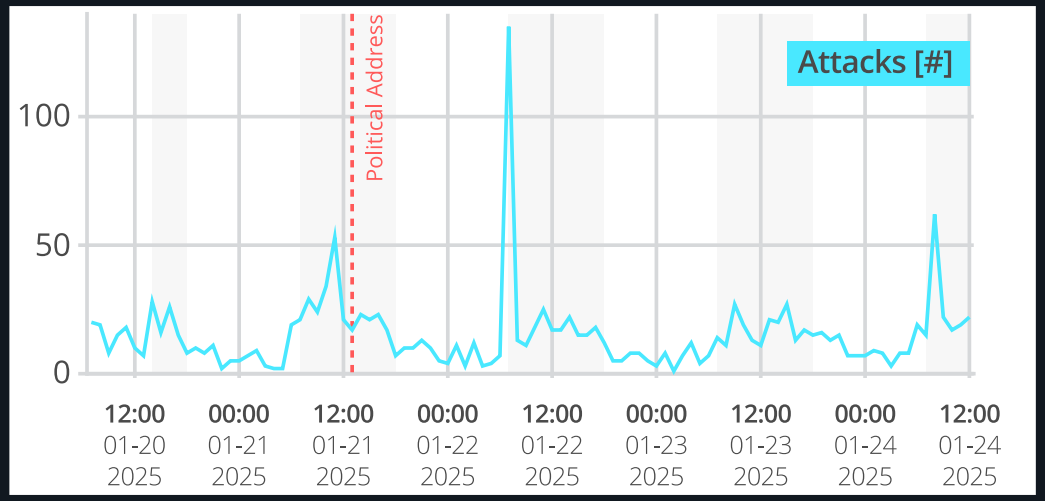
Geopolitical Events Drive DDoS Trends

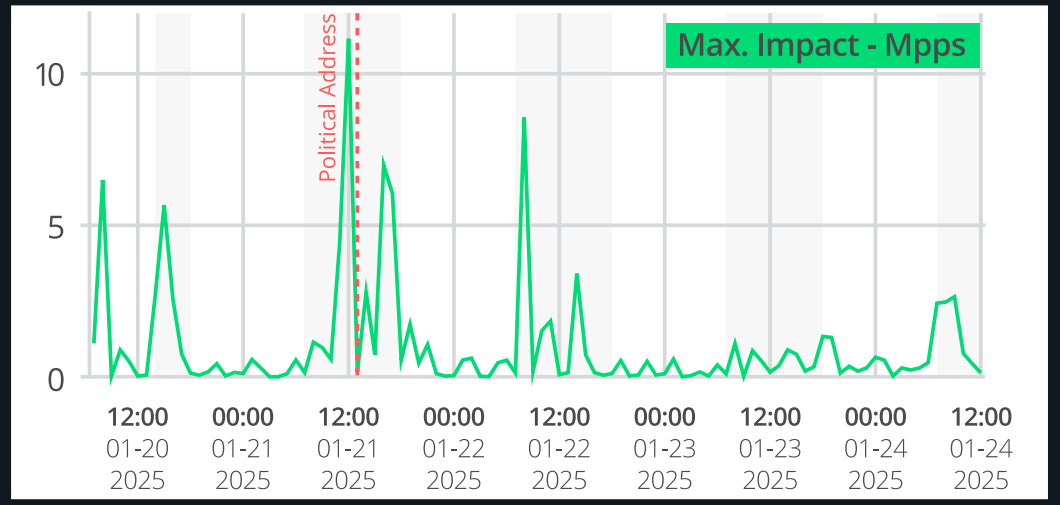
Case Study – World Economic Forum - Switzerland

Geopolitical Event Analysis

- Timeline: January 20 – 24, 2025
- Attack Volume: 1,400 attacks (200% increase over December)
- Timing: Coincided with political speeches

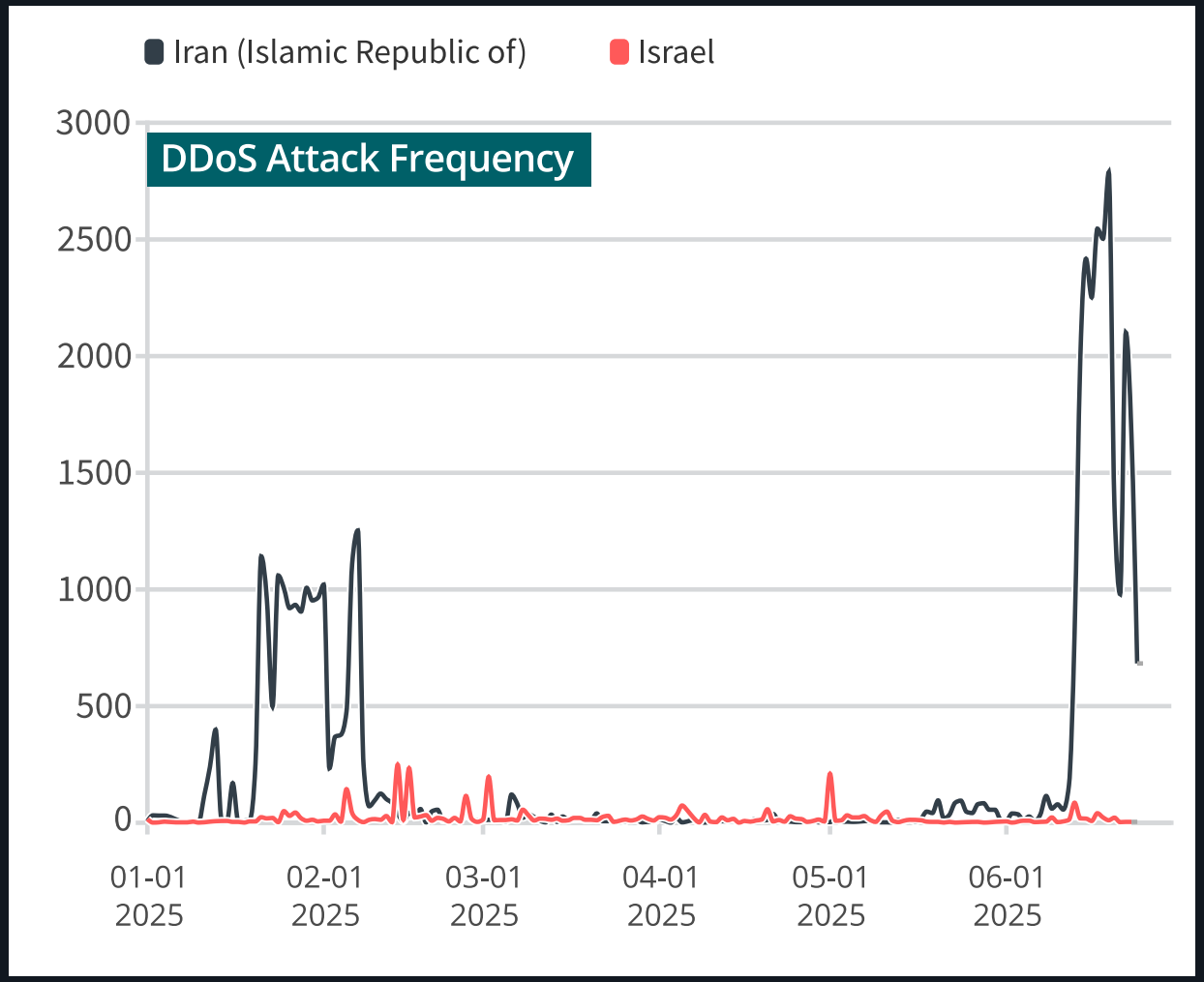




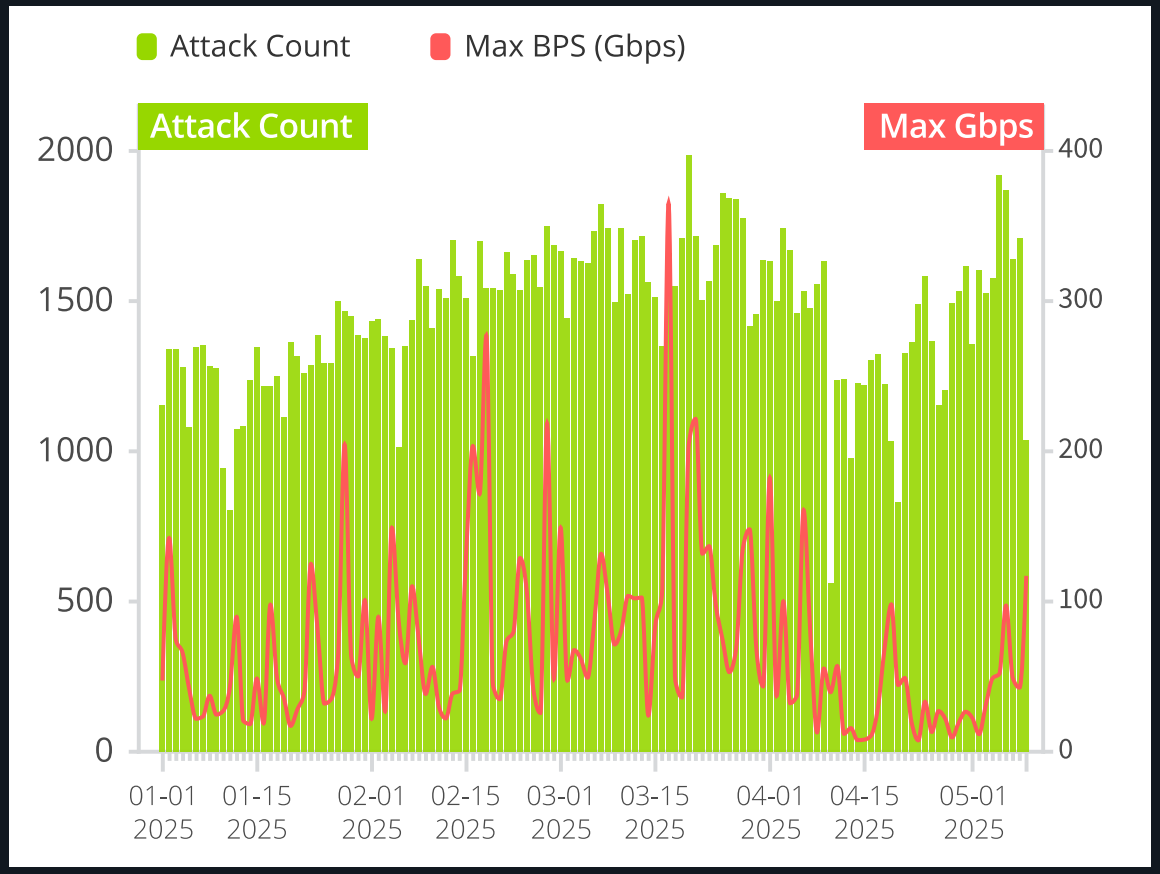


Case Study: Iran-Israel Cyber Escalation

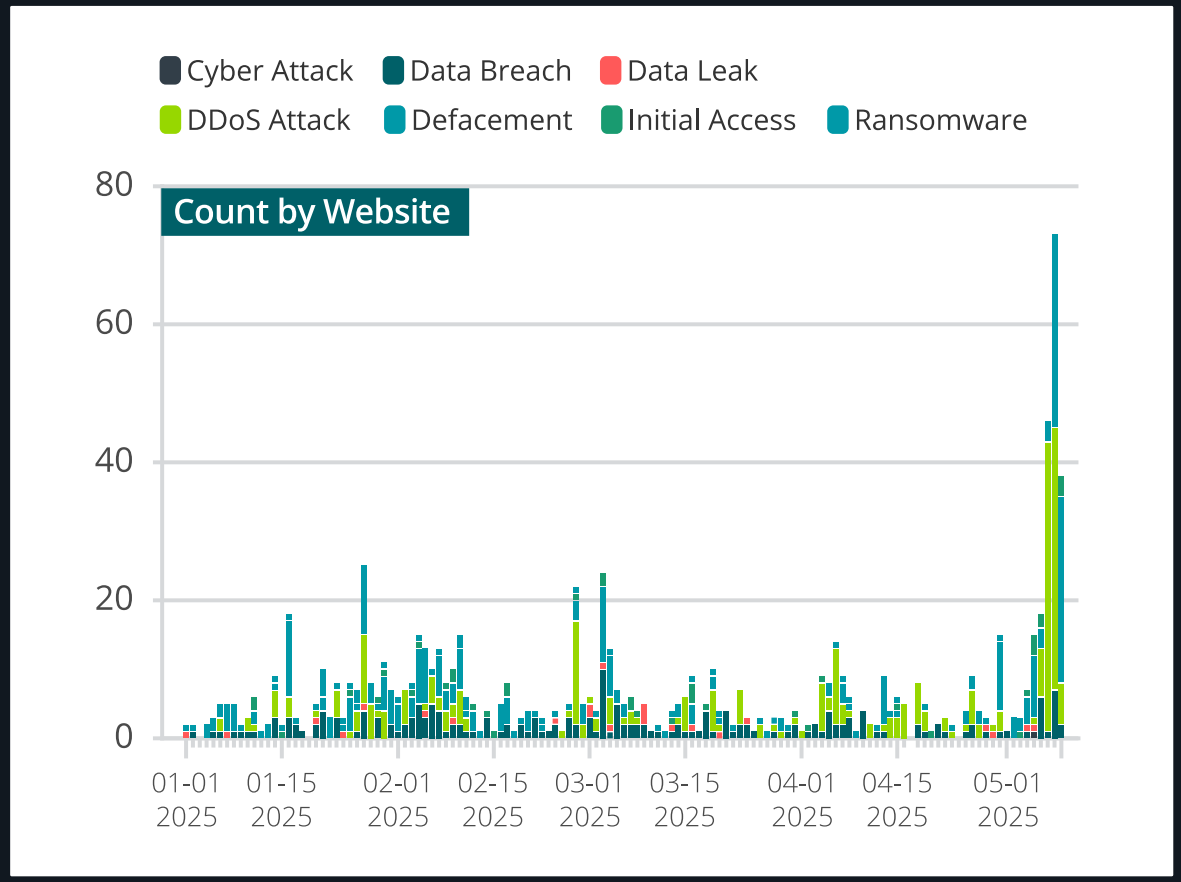
- Attack Asymmetry: 15,000+ against Iran vs 279+ against Israel
- Peak Activity: 2,800 attacks in a single day
- Attack Metrics: Iran faced large, volumetric attacks while Israel faced a variety of lower impact attacks.



Case Study: India-Pakistan Conflict

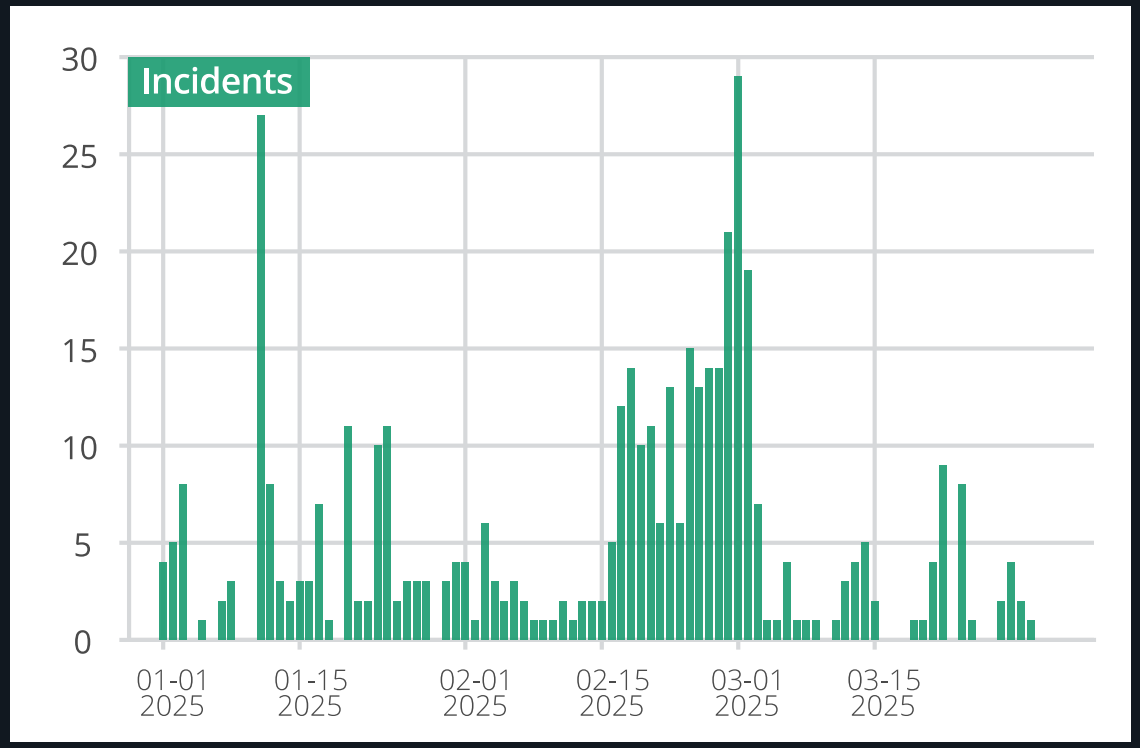


DDoS attacks escalated while impact decreased

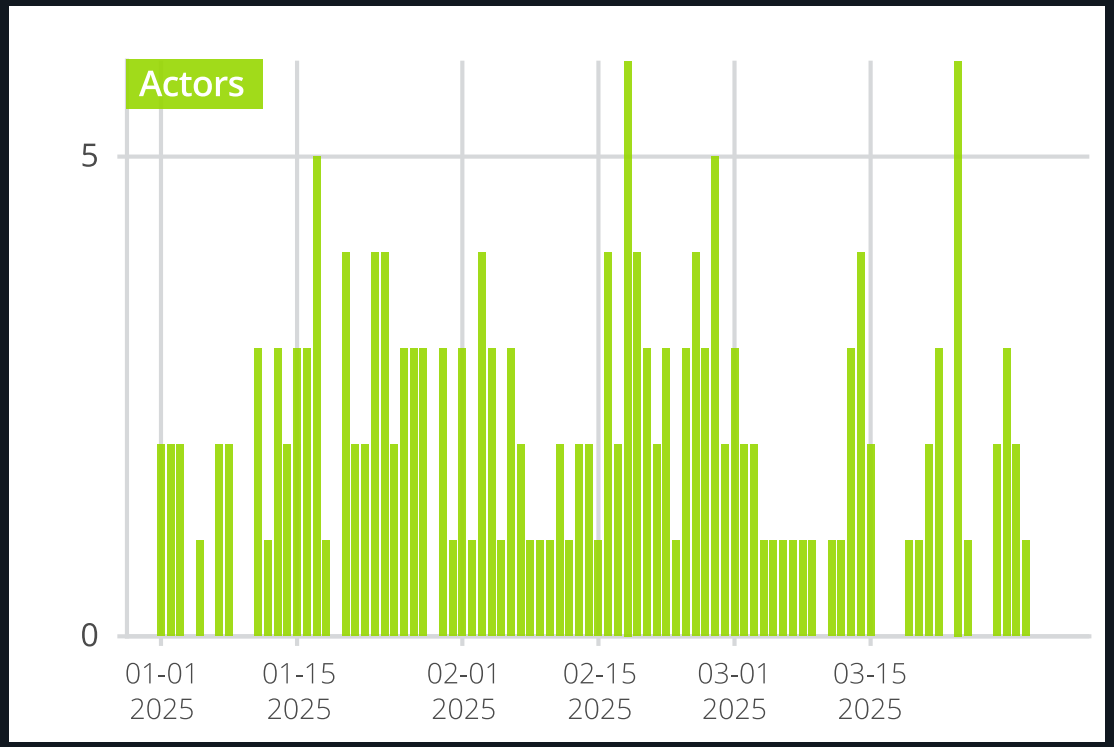


Cyber attacks significantly increased as a whole

Case Study: Italy in the Crosshairs



DDoS attacks peaked during major political discourse



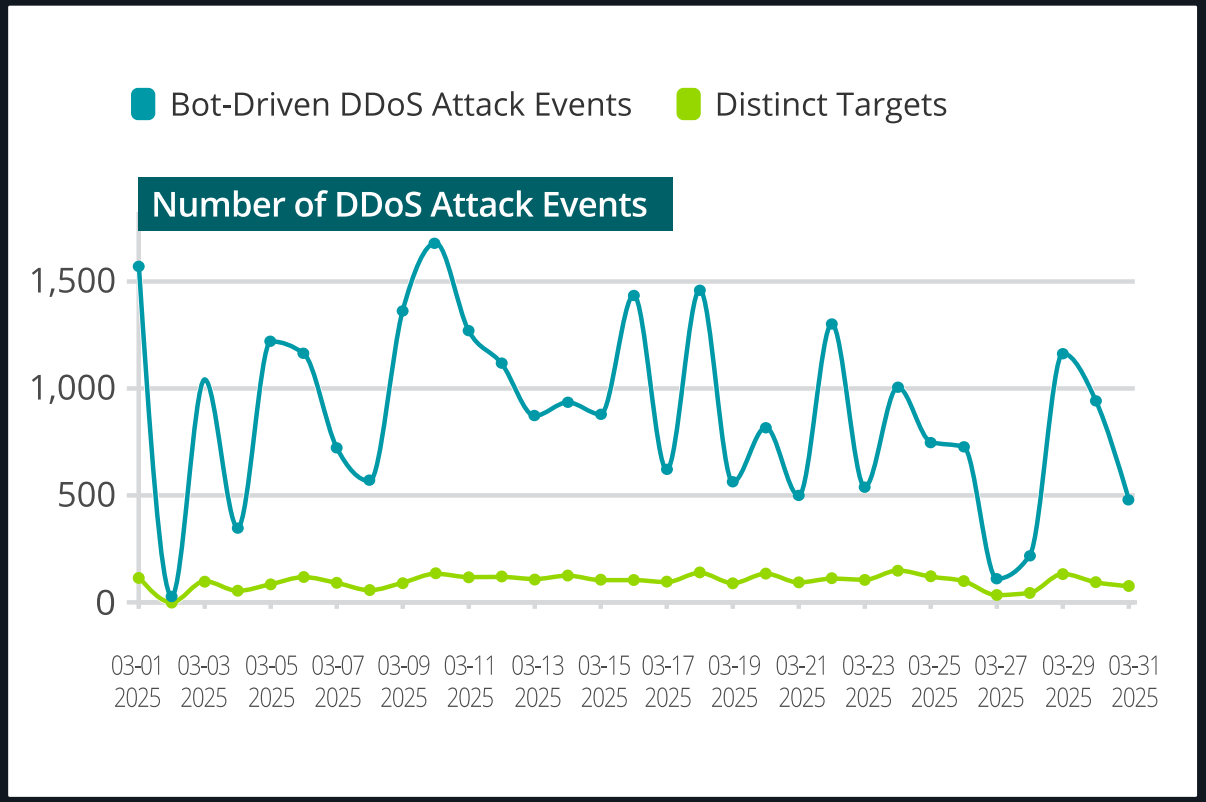
Public claims by DDoS hacktivists, predominantly NoName057(16) during the heightened attack periods

Botnets and Familiar Foes Drive DDoS Activity

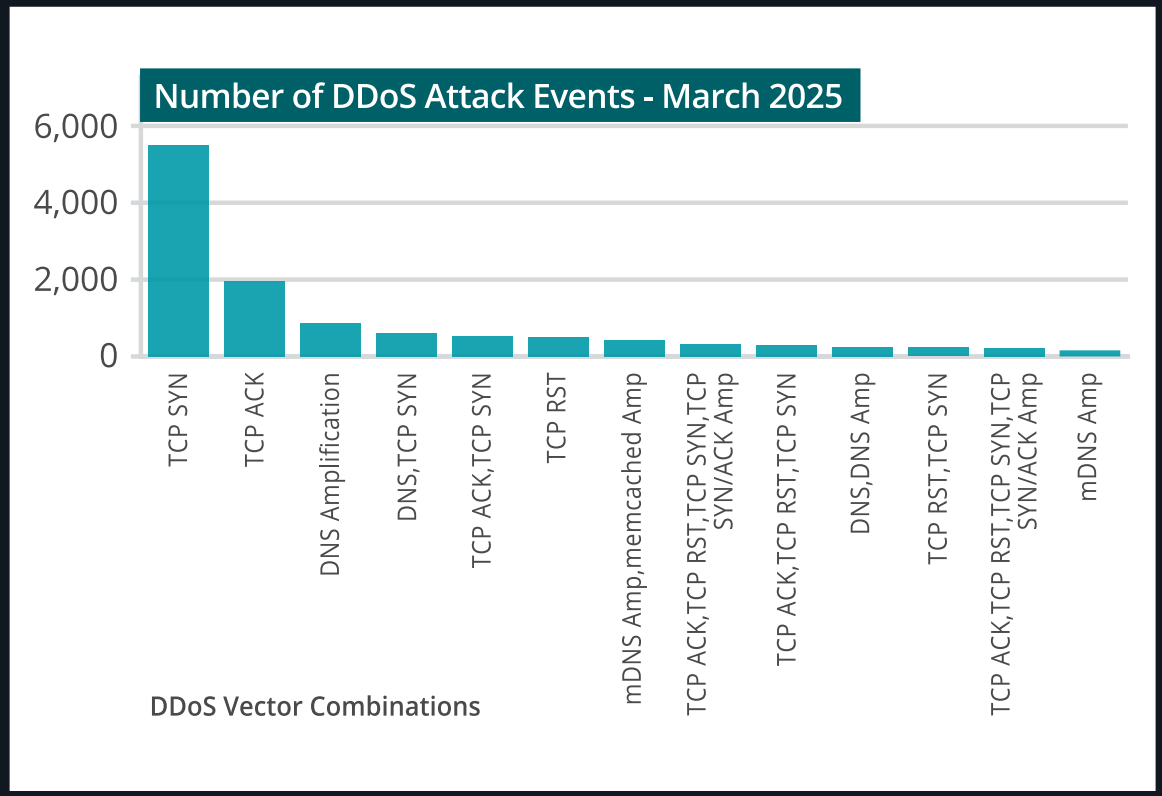
Botnet Activity

Botnet-Driven Attacks Dominate with Increased Sophistication

March 2025



March 2025

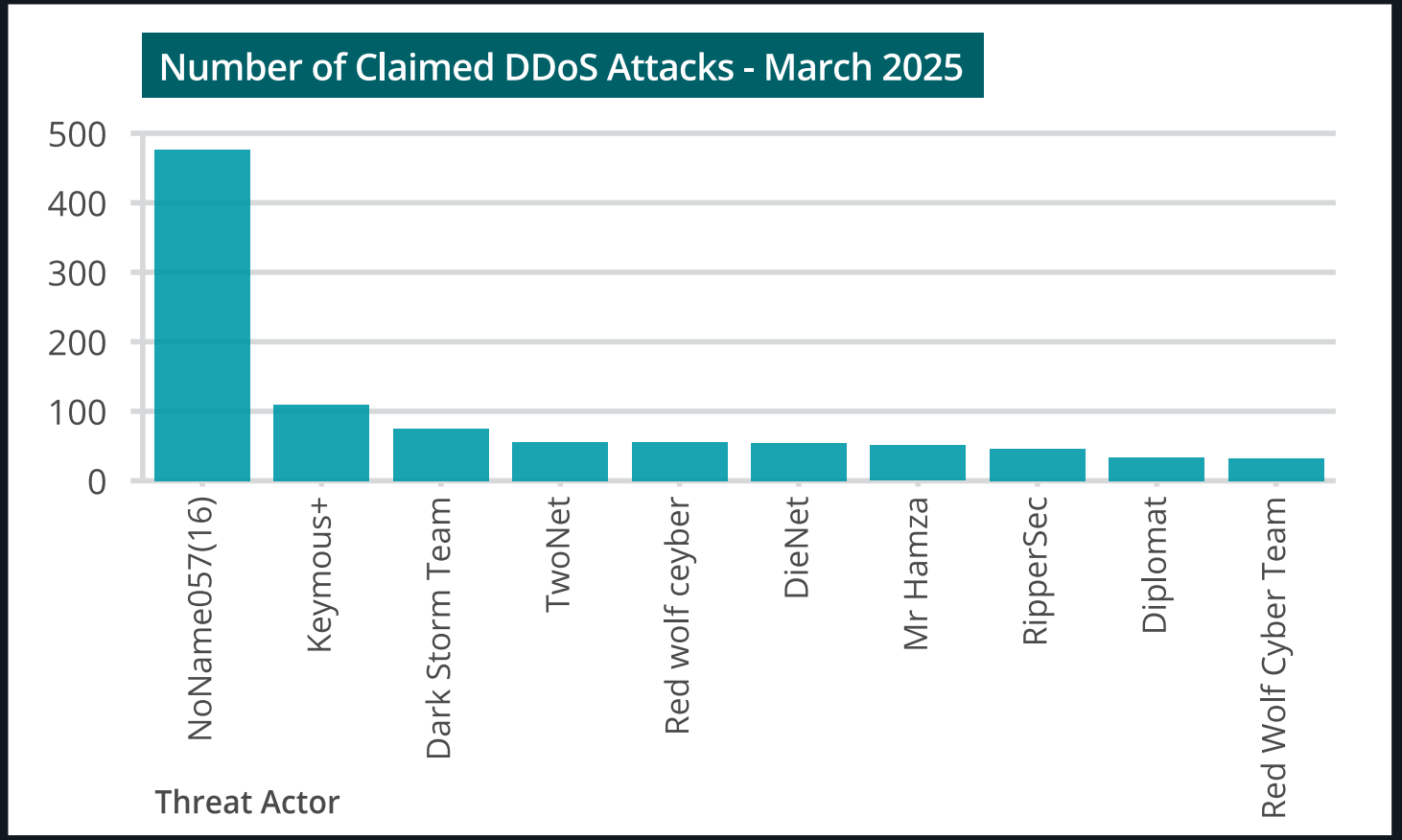


Threat Actor Profiles

NoName057(16)

Dominant Threat Actor

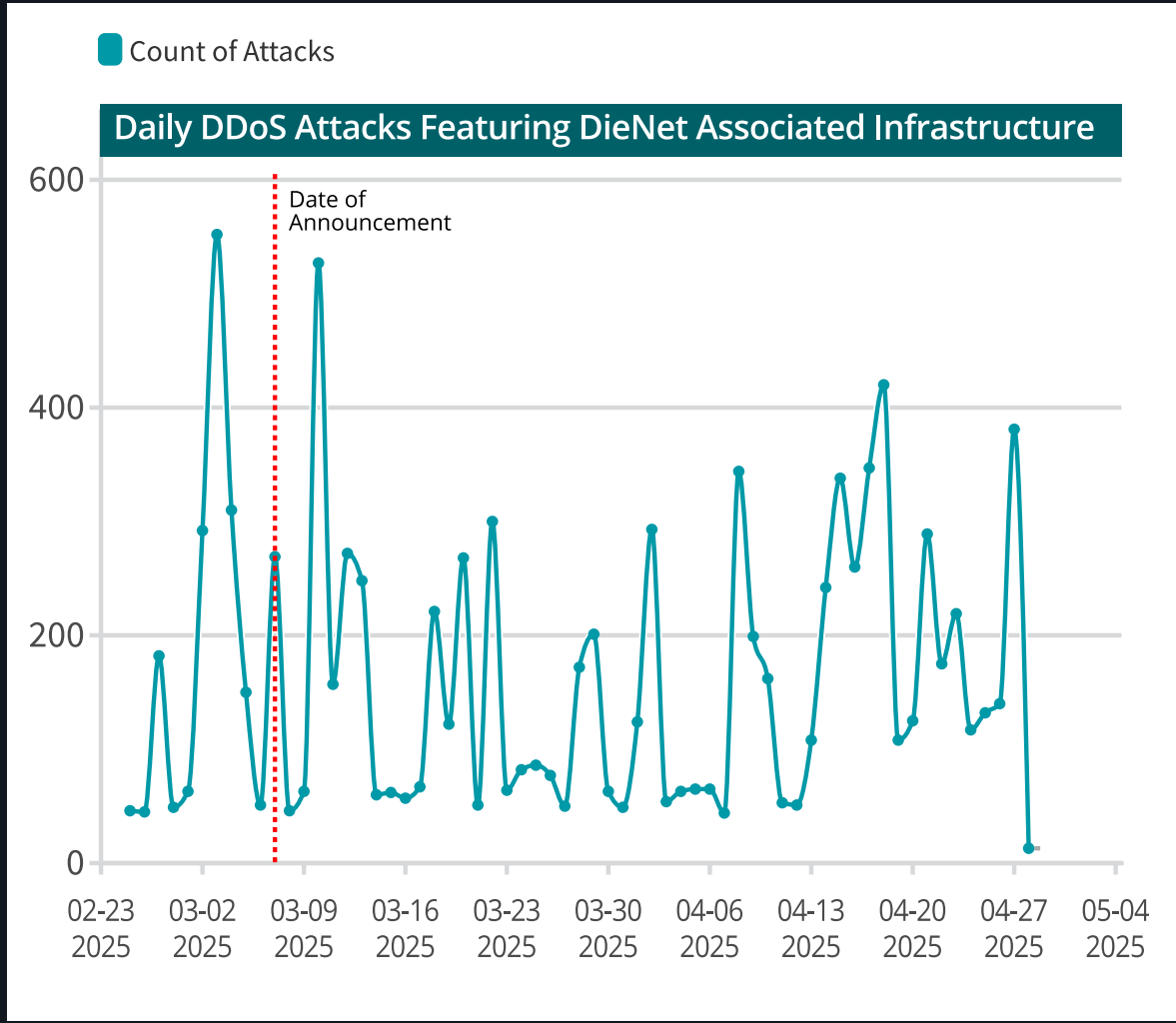
- Activity Level: 475+ attacks in March 2025 (337% more than next most active group)
- Targeting Pattern: Western countries and governments politically aligned with Ukraine or against Russia and their allies.
- Post Operation Eastwood: Continued activity and targeting within 2 days, though apparent diminished impact (bps/pps).



DieNet – Emerging Threat Actor

Debut: March 7, 2025

- Attack Activity: 60+ attacks between debut and June 30, 2025
- Infrastructure: Shared with OverFlame, DenBots, and potentially other DDoS-as-a-Service platforms.
- Targeting Pattern: US Transit, Iraq, Israel, Sweden, and Egypt



Conclusion

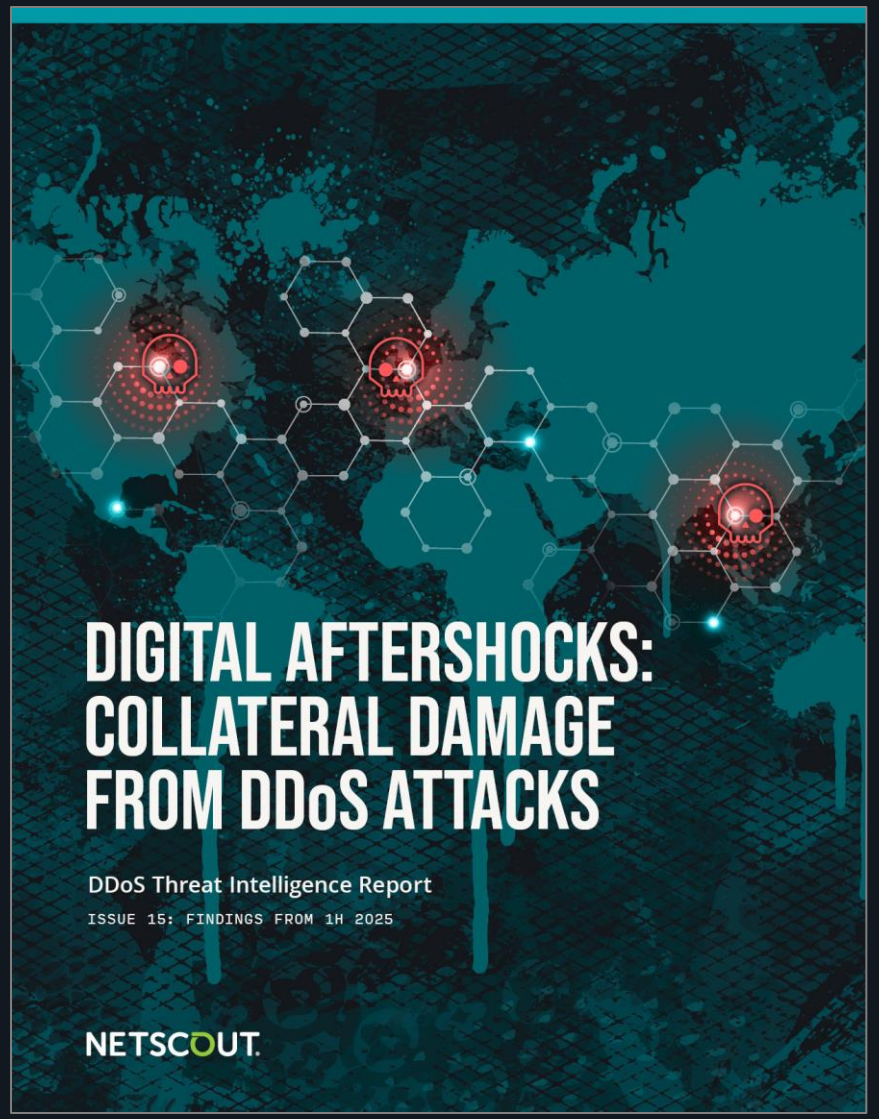
Threat Evolution: Botnets continue to increase in power and attack frequency on Enterprises and Service Providers alike

Geopolitical Integration: Cyber attacks increasingly synchronized with political events and conflicts

Technology Arms Race: AI-enhanced attacks necessitate AI-powered defense mechanisms

Infrastructure Vulnerability: Collateral damage across service provider networks also impacts enterprises

Call to Action: Organizations must embrace proactive strategies that outpace attackers through proven intelligence-driven solutions



How NETSCOUT Can Help

AI/ML-powered on-prem and cloud DDoS protection

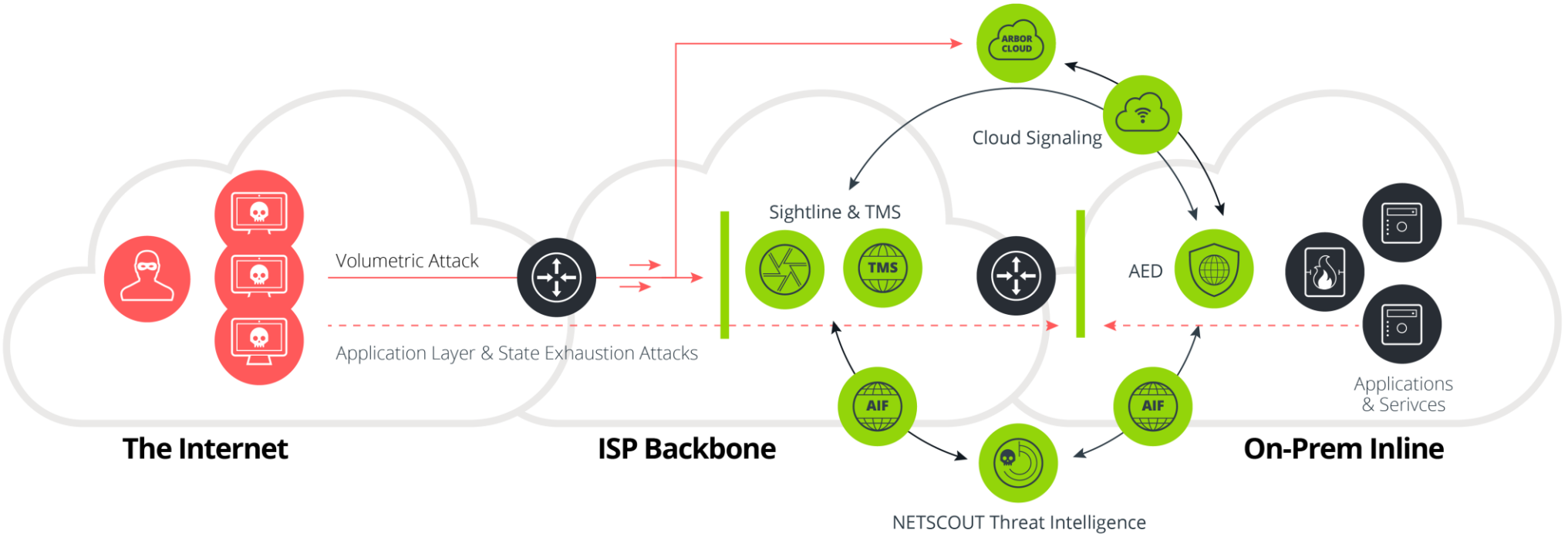
Arbor Cloud

In-cloud DDoS attack protection.

16 scrubbing centers, and over 15Tbps of capacity.

Cloud Signaling

Provides communication between NETSCOUT Arbor Mitigation solutions.



Sightline & TMS

Automated detection, out-of-band surgical mitigation (up to 400G per device); can be100% 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 protection (up to 200G per device); from inbound and outbound threats (i.e., DDoS attacks and IoCs).

Cloud signaling upstream for large attacks.

NETSCOUT Industry Leading Technology

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

How NETSCOUT Can Help

Geopolitical Unrest

- 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.

How NETSCOUT Can Help

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

Thank you.

netscout.com