digicert®
Ultra Products

UltraDDoS Protect

Biannual Distributed Denial-of-Service Analysis

January–June 2025

August 2025

Contents

Introduction

Digicert offers a Distributed Denial-of-Services (DDoS) mitigation service, named UltraDDoS Protect, to its customers. UltraDDoS Protect provides high-performance, flexible, and automated protection across 16 Points of Presence (PoPs) and >15Tbps of DDoS mitigation capacity to enable customer availability and performance under even the largest and most complex DDoS attacks. You can find out more information about UltraDDoS Protect on its product page at https://vercara.digicert.com/ddos-protection. Additionally, Digicert uses UltraDDoS Protect to defend its UltraDNS, UltraDNS², UltraDDR, and UltraWAF platforms against DDoS attacks.

Executive Summary

The first half of 2025 saw a decline in individual DDoS attacks recorded, with 15,260 attacks observed—an 84.37% decrease compared to the same period in 2024. This shift is partially due to extensive tuning of thresholds done by the DigiCert SOC to reduce over-alerting to nuisance traffic, Most of the change reflects changes in attacker behavior, driven in part by global law enforcement operations, including Operation PowerOff, which disrupted DDoS-for-hire platforms and access to large-scale botnets. As a result, many malicious actors appear to be in a rebuilding phase, operating with reduced infrastructure and capability.

A notable trend in 2025 has been the overwhelming dominance of unique-style DDoS attacks, which accounted for over 97% of all activity. Carpet bombing attacks dropped by 94.75% year-over-year, comprising just 12.20% of attacks—based on consistent detection methodology across both years. This suggests a tactical shift toward single-target disruptions rather than distributed, multi-IP attacks.

Most attacks remained low in bandwidth, with nearly 73% falling between 0.0 and 0.5 Gbps. High-bandwidth infrastructure usage dropped sharply, with attacks over 100 Gbps declining by more than 94%. The largest attack observed during this period reached 813.39 Gbps and over 71 million packets per second, underscoring that while rare, large-scale attacks still pose a threat—especially to organizations without dedicated mitigation. Overall, these trends reinforce the assessment that adversaries are currently constrained in their ability to launch volumetric campaigns, likely due to the loss of access to powerful botnets and high-throughput infrastructure.

The Financial Services sector became the top targeted industry, accounting for 47.18% of all attacks, followed by IT/Technical Services and Communication Providers. Geopolitically, regional conflicts continue to influence targeting patterns, with Saudi Arabia, the United States, and Sweden seeing the highest volume of DDoS traffic.

These findings illustrate a transitional period in the DDoS threat landscape, where adversaries are recalibrating tactics in response to infrastructure losses and enforcement pressure. While overall attack volume is down, the continued presence of high-impact events and persistent targeting of critical industries underscores the need for ongoing vigilance. Organizations should remain prepared for short, frequent, and strategically targeted attacks, as threat actors adapt and rebuild their capabilities.

This report is a summary of Distributed Denial-of-Services (DDoS) attacks detected and mitigated by UltraDDoS Protect for January to June 2025. This report is released as TLP:CLEAR except where noted.

Stats at a Glance

Total Number of Attacks:
15,260

Total Number of
Downtime Hours Avoided:
~7,504 Hours

Number of Mega Attacks (100+ Gbps):
40

Largest DDoS Attack (Gbps):
813.39 Gbps

Largest DDoS Attack:
357.08 Mpps
(million packets per second)

Longest DDoS Attack:
11 Days

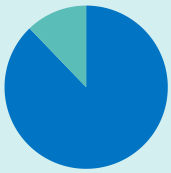
Average DDoS Attack (Gbps):
2.56 Gbps

Median DDoS Attacks (Gbps):
0.11 Gbps

Average DDoS Attack:
473.58 Kpps
(packets per second)

Median DDoS Attack:
37.21 Kpps
(packets per second)

Unique vs
Carpet Bombing



Average Duration: 29.51 minutes

Top Three Industries Targeted

Financial Services
50.87%

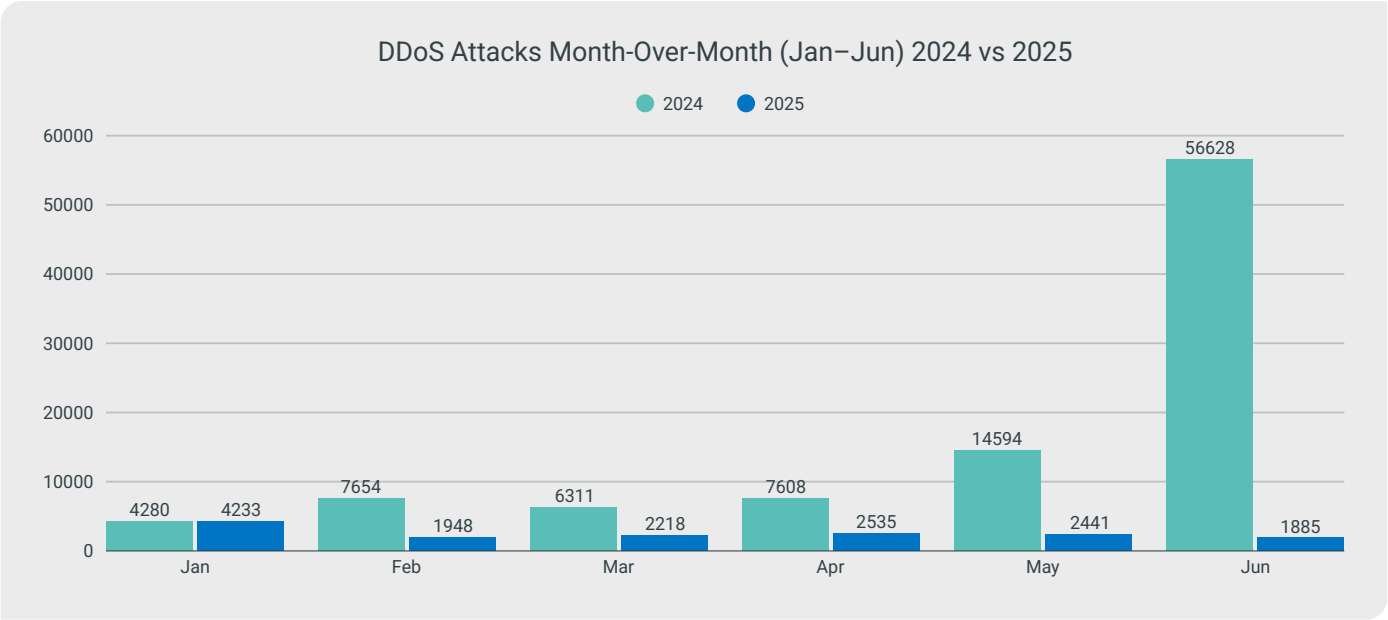
IT/Technical Services
16.61%

Communication Service Providers
16.34%

Attack Statistics and Trends

DDoS attacks are more common than Information Technology and Information Security Teams realize. Most attacks are mitigated quickly. The frequency and number of DDoS attacks vary based on a wide variety of factors such as exploit development, hacktivist campaigns, the number of infected systems used in an attack, and law enforcement takedown operations.

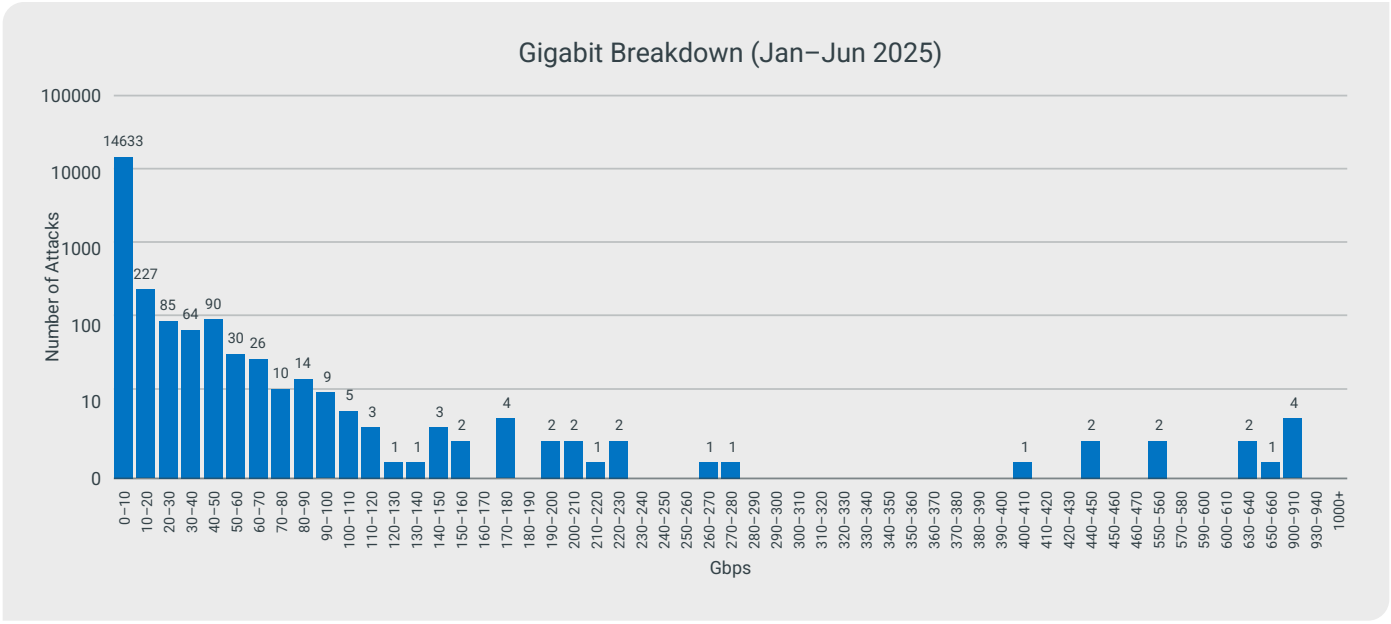
For the first half of 2025 (January through June), **DigiCert UltraDDoS Protect** detected 15,260 DDoS Attacks, a 84.37% decrease compared to the same period in 2024. The significant decrease is assessed to be a broader shift in the DDoS threat landscape with hacktivist groups and other malicious actors deprioritizing large-scale DDoS campaigns in favor of more targeted, strategic attacks. Another key factor behind the decline is the impact of global law enforcement actions such as Operation PowerOff which dismantled major DDoS-for-hire services and disrupted access to critical botnet infrastructure. These takedowns have more than likely forced threat actors into a rebuilding/reconstitution phase, requiring time to reestablish infrastructure and technical expertise.



The largest DDoS attack observed during the first half of 2025 consisted of over 813.39 Gigabits per Second (Gbps) with over 71 million Packets per Second (Mpps). Almost 73% of all observed DDoS attacks were small in nature, consisting of between 0.0 to 0.5 Gbps, which reflects a continued trend of low-volume attacks likely designed for targeted disruption rather than large-scale service outages. Compared to the same period in 2024, every Gbps range experienced a significant decline, with high-bandwidth attacks (100+ Gbps) dropping by over 94%. This widespread reduction is indicative of a constrained threat environment following global enforcement actions and many threat actors appear to be operating at a diminished capacity while they attempt to rebuild their botnets and regain lost capability.

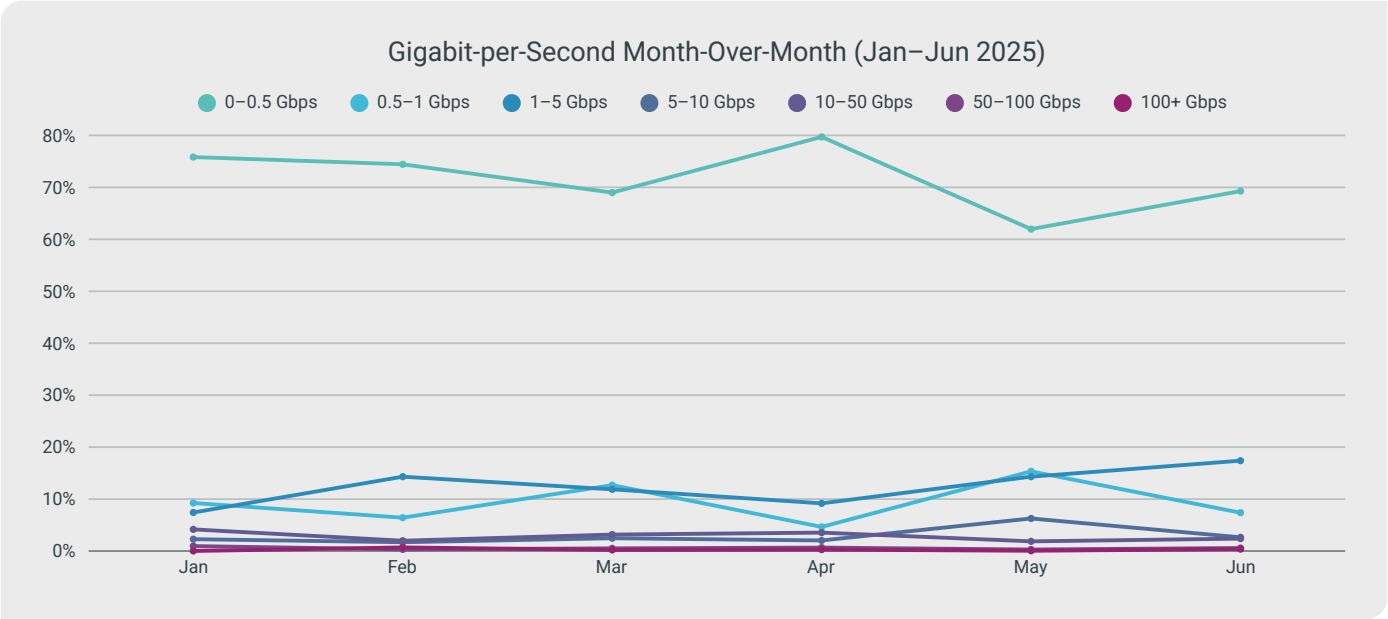
The chart below shows the breakdown in Gbps attacks throughout the first half of 2025.

Gigabit-per-Second			
Gbps	Total Count	Percentage	% Change from 2024
0.0–0.5	11,011	72.31%	▼ -84.45%
0.5–1	1,424	9.35%	▼ -84.30%
1–5	1,761	11.56%	▼ -81.48%
5–10	437	2.87%	▼ -76.39%
10–50	466	3.06%	▼ -84.48%
50–100	89	0.58%	▼ -90.25%
100+	40	0.26%	▼ -94.53%

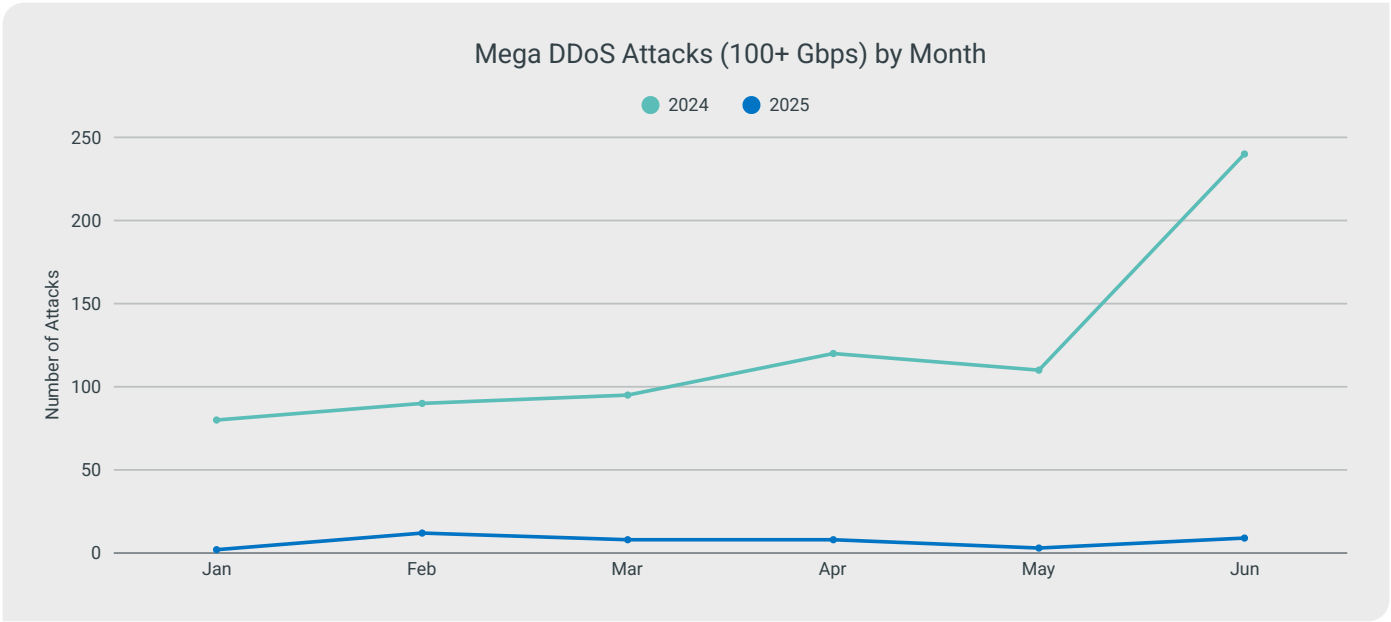


The chart below shows the distribution of DDoS attacks by Gbps range on a monthly basis from January through June 2025. The vast majority of attacks each month fell within the 0.0-0.5 Gbps range, consistently accounting for over 60%, and peaking near 80% in April. High bandwidth attacks (5 Gbps and above) remained relatively infrequent with each category rarely exceeding 5% of the monthly activity. This pattern highlights a continued reliance on low-volume attacks, suggesting that threat actors might be operating with limited infrastructure or capability, or that malicious actors are shifting their tactics away from large-scale volumetric attacks towards smaller, more frequent and purposeful attacks.

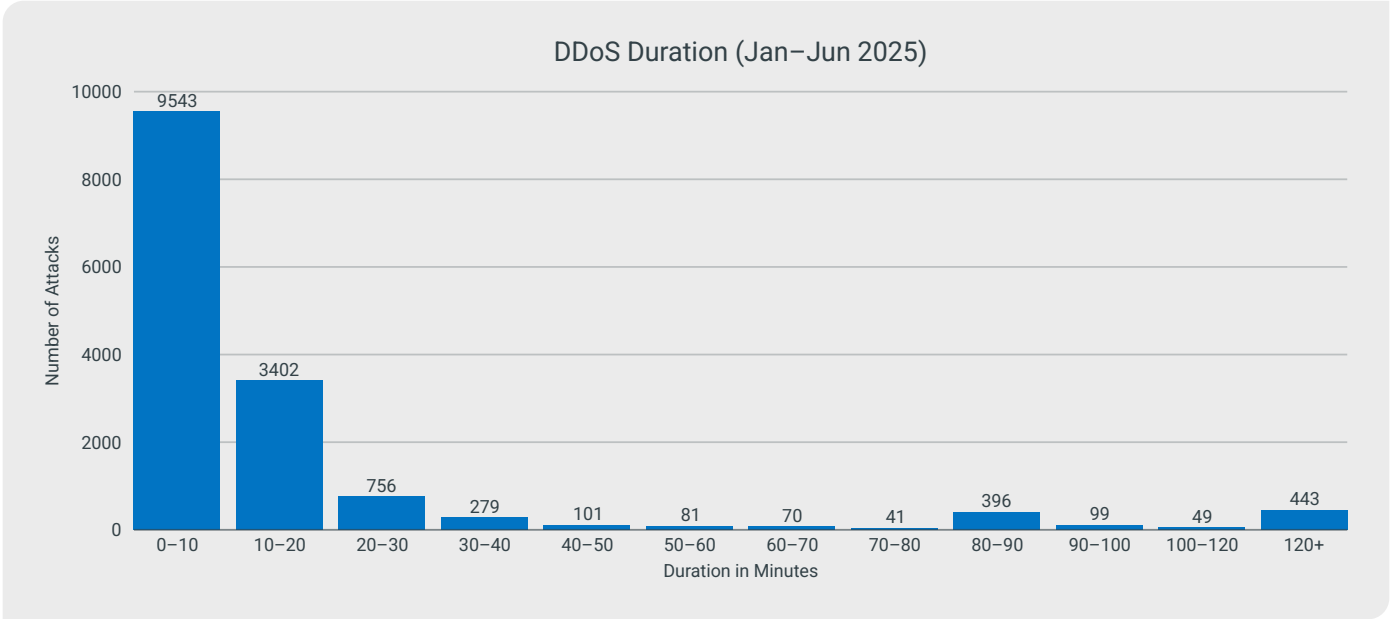
The chart below shows the distribution of DDoS attacks by Gbps range on a monthly basis from January through June 2025. The vast majority of attacks each month fell within the 0.0-0.5 Gbps range, consistently accounting for over 60%, and peaking near 80% in April. High bandwidth attacks (5 Gbps and above) remained relatively infrequent with each category rarely exceeding 5% of the monthly activity. This pattern highlights a continued reliance on low-volume attacks, suggesting that threat actors might be operating with limited infrastructure or capability, or that malicious actors are shifting their tactics away from large-scale volumetric attacks towards smaller, more frequent and purposeful attacks.



Mega-Attacks (attacks consisting of 100+ Gbps) remained rare in 2025, making up only a small portion of overall DDoS activity each month. The volume of mega attacks in 2025 stayed consistently low, with no significant spikes throughout the first half of the year. This marks a notable shift from the previous year, when June saw a dramatic surge in such high-volume events. While still capable of overwhelming unprotected networks, the reduced frequency of mega attacks in 2025 suggests that threat actors are becoming more economical and targeted in their attacks. This usually signals an increase in attack sophistication as smaller attacks are better able to evade defenses.



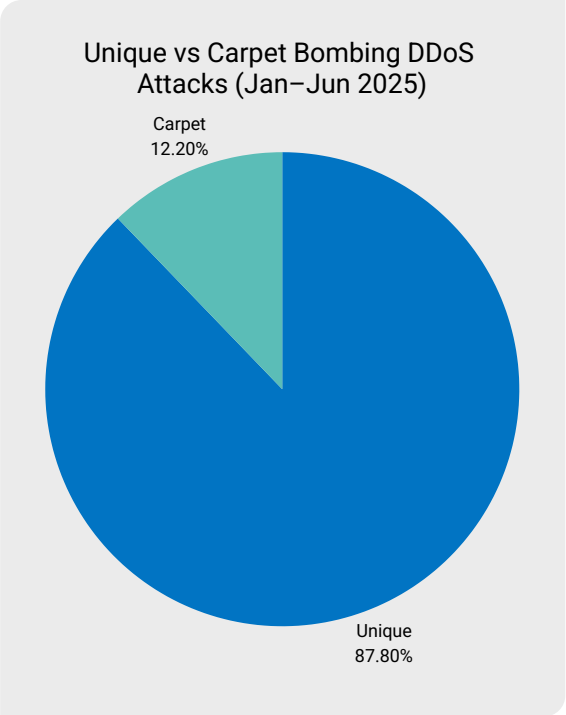
The chart below shows the breakdown of DDoS attack duration observed from January through June 2025. A clear majority of attacks, nearly 10,000, lasted less than 10 minutes, reinforcing a trend towards short-duration, high frequency events likely aimed at quick disruption or testing network response while evading detection and mitigation. As duration time increases, the number of attacks drops sharply, with long-lasting attacks (over 120 minutes) making up a very small portion of the total activity. This distribution may indicate a strategic shift by malicious actors towards low-cost, low-risk attacks that still achieve visibility or impact, while avoiding the sustained resource demands.



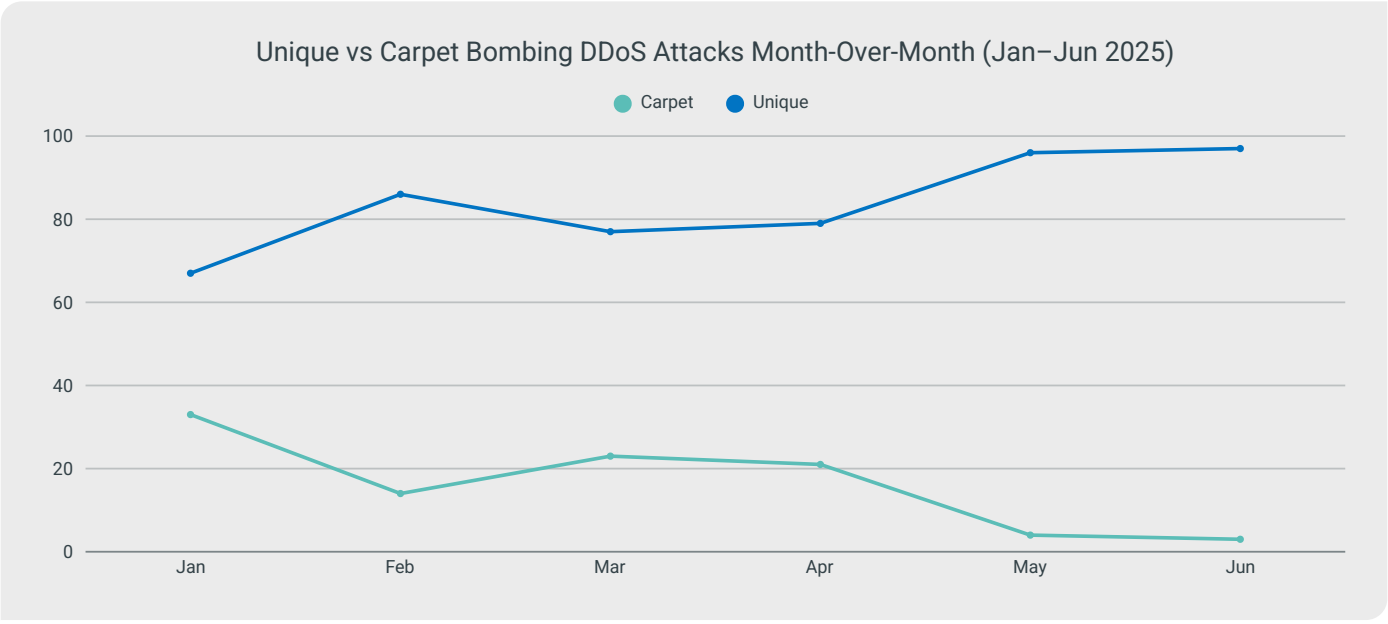
Unique vs Carpet Bombing DDoS Attacks

Carpet bombing DDoS attacks target all the IP addresses in a network block or multiple contiguous blocks over a brief period to evade detection and blocking but also to overload some types of mitigation gear with clean traffic by forcing the target organization to onboard all their network blocks.

For the first half of 2025, carpet bombing style DDoS attacks made up only 12.20% of all observed attacks, marking a sharp 94.75% decrease from the same period in 2024. This drop is based on consistent methodology across both years, confirming a genuine shift in how these attacks are being deployed. Carpet bombing attacks, which target multiple IPs simultaneously to increase disruption and evade detection, appear to have been used far less frequently in 2025. This may indicate a pivot by malicious actors toward more direct, single-target attacks, or a reduced capability to launch the broader, more complex campaigns typically associated with carpet bombing.



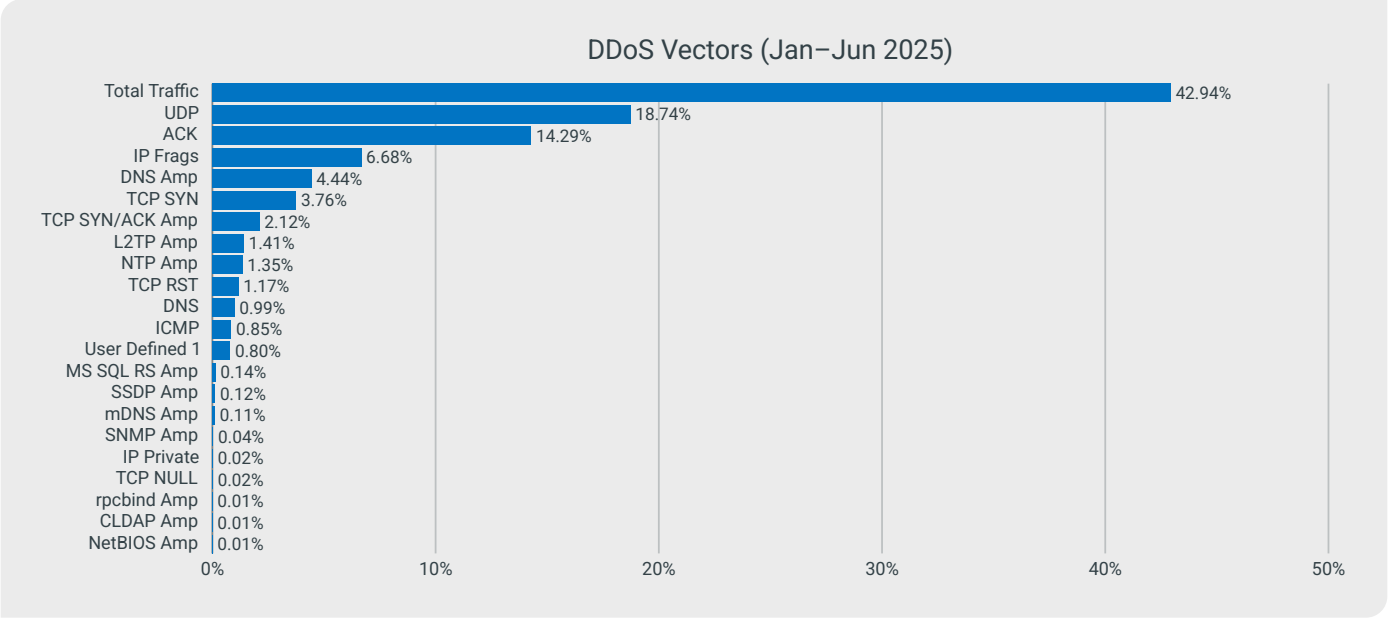
When looking at the month-over-month trend for the first half of 2025, unique style DDoS attacks consistently dominated, comprising over 75% of all attacks each month and reaching over 95% by June. In contrast, carpet bombing attacks steadily declined, dropping from 33% in January to just over 3% by June. This pattern reflects a sustained shift away from the widespread use of carpet bombing observed in 2024. The sharp divergence highlights a clear change in attacker behavior, with a notable reduction in the deployment of broad, distributed targeting techniques throughout the first half of 2025.

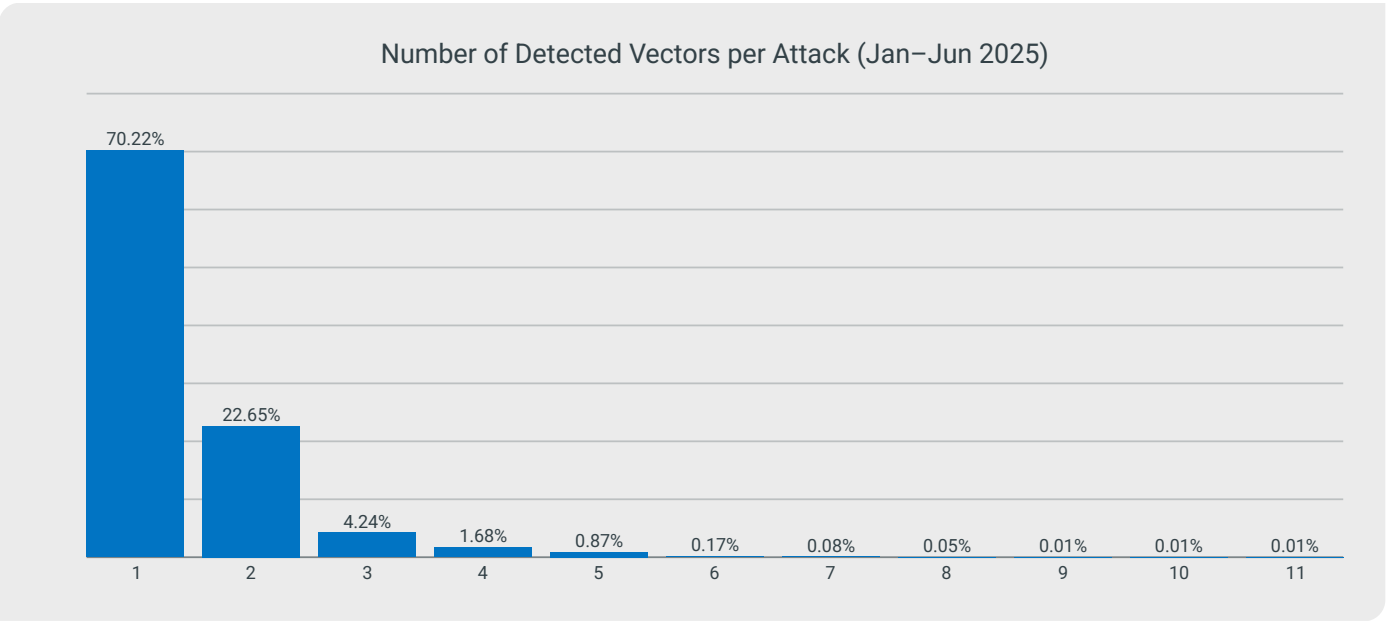


Attack Vectors

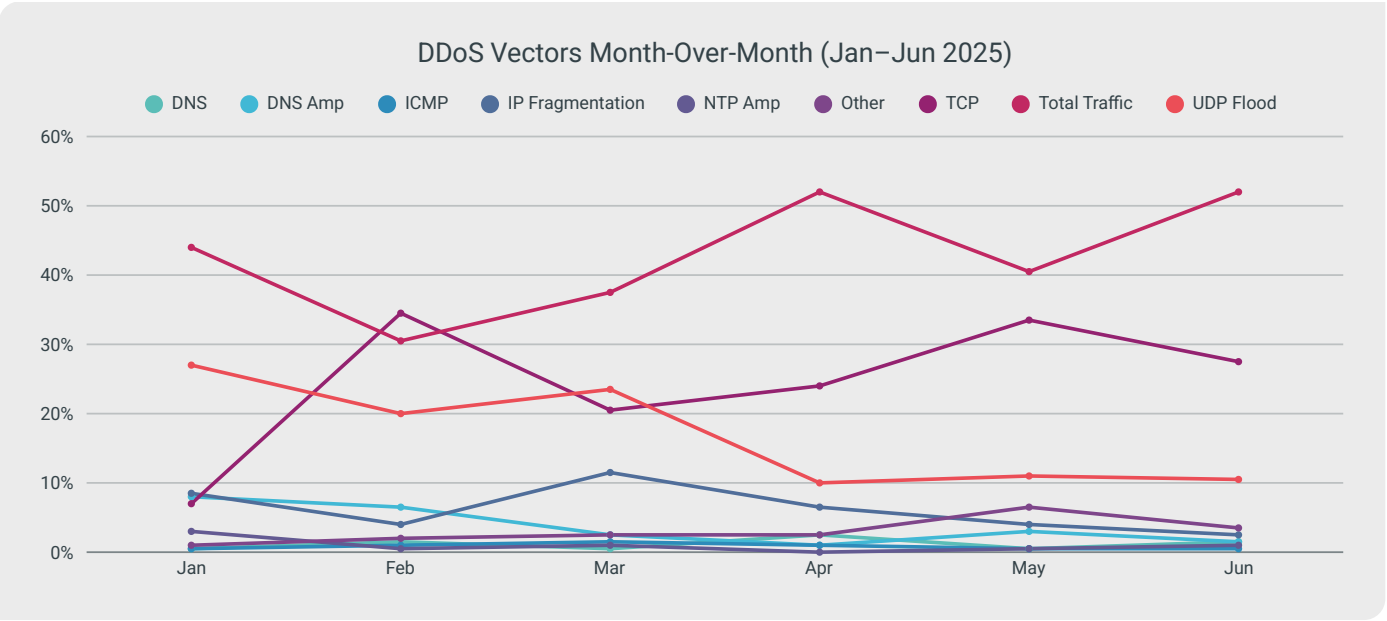
An attack vector is a mechanism, usually an abused network protocol or a variety of packets inside of a protocol, that a DDoS attack uses to generate high volumes of traffic. Attack vectors also serve as signatures to detect DDoS traffic outside of looking solely at Gbps and PPS. Attack vector statistics change in popularity from month to month based on attack platform tooling, numbers of vulnerable endpoints that are accessible across the internet, and newly discovered vulnerabilities.

For the first half of 2025, the most commonly observed DDoS vector was the Total Traffic vector, accounting for 42.94% of all activity. this vector captures any kind of flood attack aimed at a particular victim host. This was followed by UDP at 18.74% and TCP ACK at 14.29%, while DNS Amplification dropped to just 4.44%, a notable decline from its leading position in 2024. This shift aligns with the broader reduction in complex, distributed attack types. Additionally, 70.22% of all DDoS attacks utilized a single vector, while 29.78% involved two or more vectors. Although multi-vector attacks remain in use, the data shows a clear preference for simpler, single-vector campaigns during the first half of 2025.





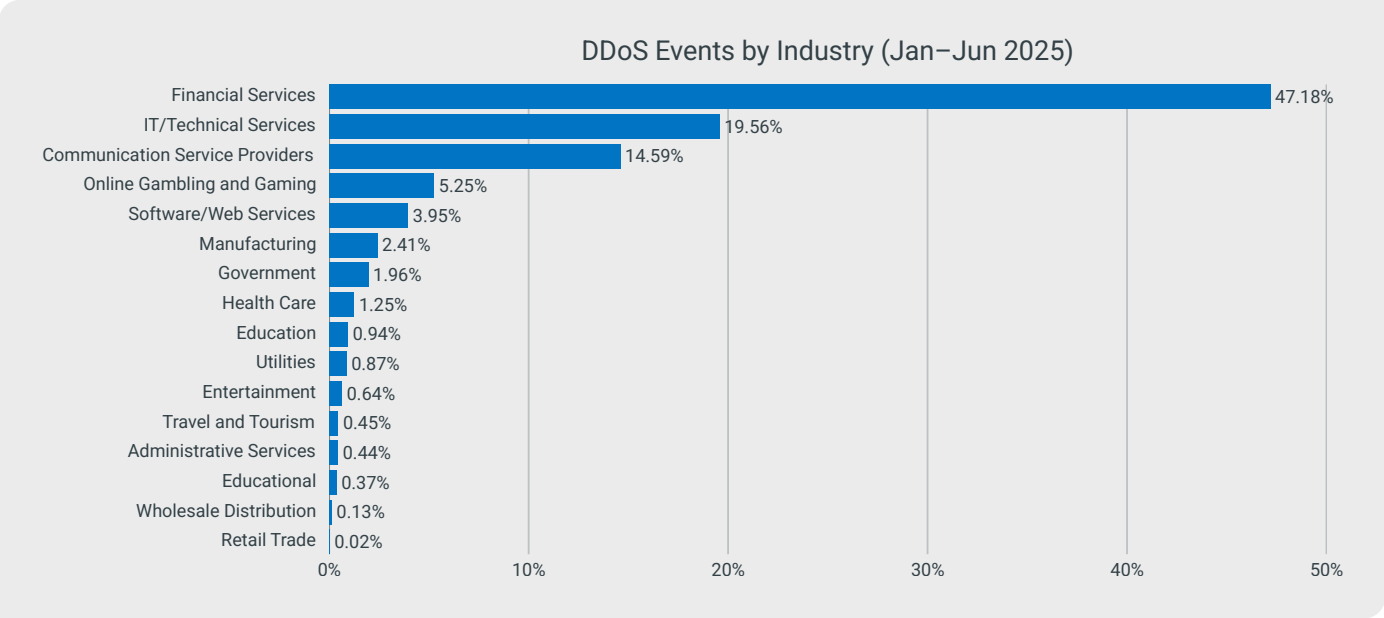
Looking at DDoS vectors month-over-month for January through June 2025, the Total Traffic vector remained dominant throughout the period, peaking above 50% in both April and June. TCP-based vectors rose steadily from January, peaking in May before slightly declining in June, reflecting increased reliance on TCP mechanisms for disruption. The UDP Flood vector showed a downward trend from January to April, with a slight recovery in May and June. IP Fragmentation peaked in March but declined in the following months, while DNS Amplification and NTP Amplification both saw modest but steady decreases over time. These trends suggest that while high-volume vectors like Total Traffic remain the primary method, there is dynamic month-to-month variation in how other vectors are deployed, likely reflecting shifts in attack objectives or available infrastructure.



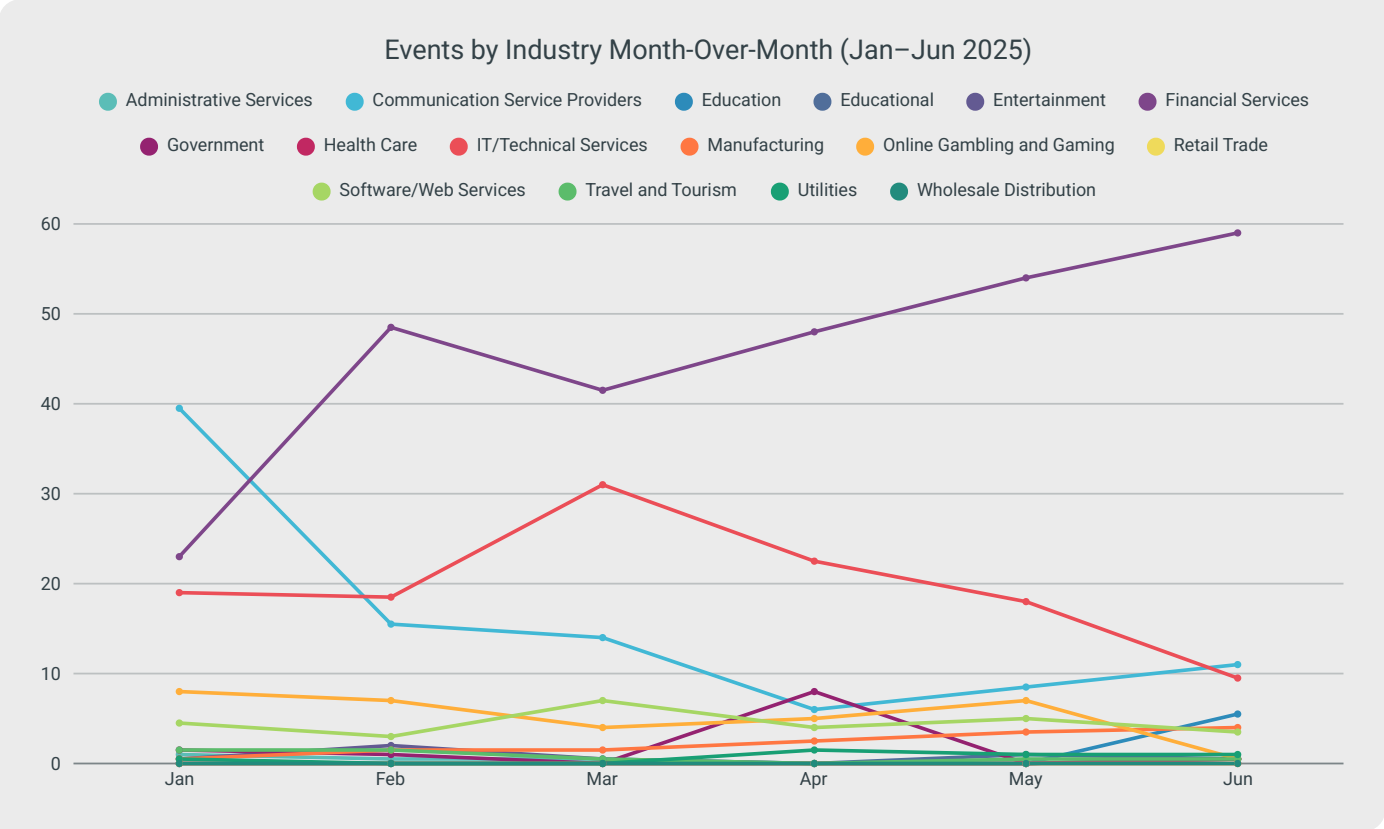
Events by Targeted Industry

The industry targeted in an attack is of interest because it can be extrapolated into other organizations inside of that industry as a "peer benchmark." Industry statistics also provide insight into DDoS attack campaigns. For instance, attacks against eCommerce companies are usually related to protection rackets and DDoS ransom activity, while attacks against the government are usually geopolitical or hacktivism.

For the first half of 2025, the Financial Services industry emerged as the most targeted sector, accounting for 47.18% of all observed DDoS attacks. This was followed by IT/Technical Services at 19.56%, and Communication Service Providers at 14.59%. These three industries combined made up over 80% of total DDoS activity, indicating a strong focus by malicious actors on disrupting critical digital infrastructure and financially driven services. Other sectors, including Online Gambling and Gaming, Software/Web Services, and Manufacturing, saw comparatively lower, but still notable, levels of targeting.

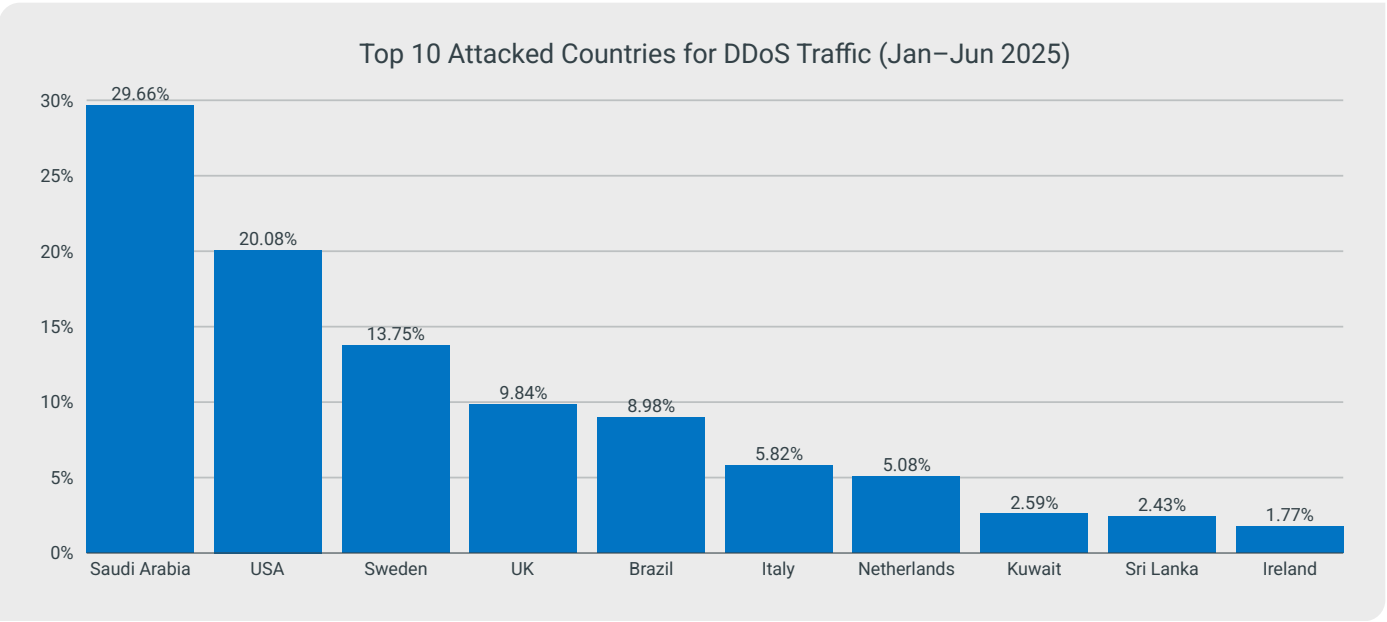


Since the start of 2025, the Financial Services industry has experienced a consistent month-over-month increase in DDoS activity, becoming the most targeted sector by February and continuing to rise through June. In contrast, Communication Service Providers, which began the year as the top target, saw a steady decline in attack volume over the same period. The IT/Technical Services sector also saw elevated activity early in the year, peaking in March before trending downward. Meanwhile, industries such as Software/Web Services and Online Gambling and Gaming experienced modest fluctuations but remained secondary targets in terms of overall volume.



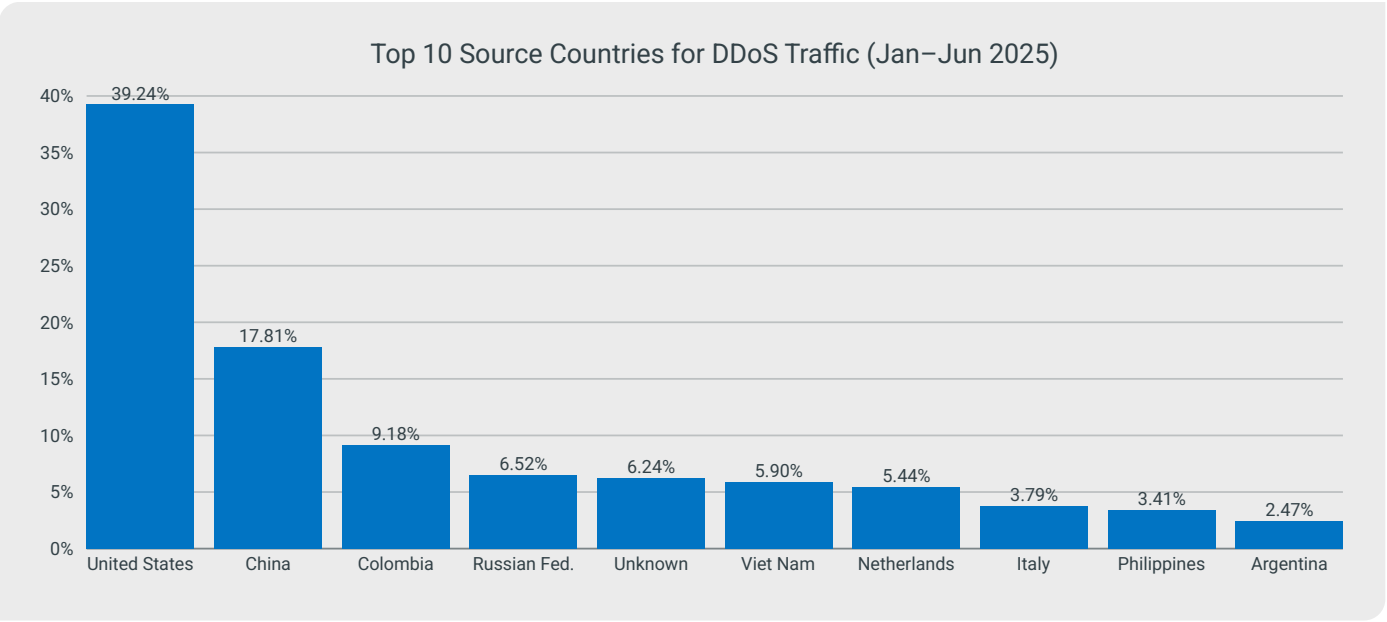
Attacks by Country

From January to June 2025, Saudi Arabia was the most targeted country for DDoS traffic, accounting for 29.66% of observed activity, followed by the United States (20.08%) and Sweden (13.75%). The high volume of attacks on Saudi Arabia and other countries in the Middle East may be linked to regional conflict and instability, where cyber activity, including DDoS attacks, is increasingly used as a tool for geopolitical messaging and disruption by various threat actors and sympathizers. Similarly, heightened DDoS activity targeting Western nations—particularly the U.S., U.K., and Sweden—can be tied to continued pro-Russian hacktivist operations related to the Russia-Ukraine war, as these groups often target countries perceived to support Ukraine militarily or politically. The inclusion of smaller nations like Kuwait, Sri Lanka, and Ireland underscores the global reach of these campaigns and the opportunistic nature of threat actors seeking to exploit vulnerable or symbolic targets amid international conflict.



Attacks by Source Country

For the first half of 2025, the United States once again generated the most observed DDoS traffic, accounting for 39.24% of total volume. This is likely driven by malicious actors leveraging U.S.-based botnets and abusing Virtual Private Servers (VPS) hosted on domestic cloud infrastructure to mask their true origin. These platforms offer high-bandwidth connectivity and are often populated with compromised IoT devices, making them attractive for launching large-scale attacks. China ranked second at 17.81%, followed by Colombia at 9.18%, with Russia and Vietnam rounding out the top five. It is important to note that DDoS source IPs can be spoofed depending on the vector and tooling used, meaning the observed country of origin may not reflect the attacker's true location. The distribution is further influenced by concentrations of spoofable IP space, widespread IoT vulnerabilities, and readily available cloud resources across these regions.



digicert®
Ultra Products

About DigiCert Ultra Security

The world's top brands depend on DigiCert to safeguard their digital infrastructure and online presence. DigiCert offers a suite of cloud delivered services that are always secure, reliable, and available and enable global businesses to thrive online. The company's ultra secure suite of solutions protects organizations' networks and applications against risks and downtime, ensuring that businesses and their customers enjoy exceptional, and uninterrupted, interactions all day, every day. Delivering the industry's best performance and always-on service, DigiCert's mission- critical security portfolio provides best-in-class DNS, application, and network security including DDoS protection, WAF, and Bot management services to its global 5000 customers and beyond.

To learn more about DigiCert solutions, please visit our **website** or **contact us.**

Call USA +1 (844) 929-0808
Call EMEA +44 808 175 1189
vercara.digicert.com

This report is a summary of Distributed Denial-of-Services (DDoS) attacks detected and mitigated by UltraDDoS Protect for January to June 2025. This report is released as TLP:CLEAR except where noted.