digicert®

UltraDDoS Protect

Annual Distributed Denial-of-Service Analysis

January – December 2025

REPORT

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 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.

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

Executive Summary

The 2025 DDoS landscape, as observed by DigiCert, reflected a continued shift toward fewer but more consequential disruption attempts. While overall event volume declined compared to the prior year, the attacks that did occur were, on average, more intense and more persistent, with higher throughput, higher packet rates, and longer runtimes. The reduction in total attacks is likely attributable to a combination of external disruption and internal refinement: global law enforcement operations, including initiatives publicly associated with takedowns of DDoS for hire services, constrained access to botnet and stressor infrastructure, while DigiCert's Security Operations Center also executed a customer satisfaction effort to reassess thresholds and tune alerting to account for normal traffic growth and flash crowd conditions, reducing non actionable detections.

A defining development in 2025 was the emergence and rapid normalization of tsunami-class DDoS attacks, with multiple events exceeding the one terabit per second threshold and one establishing a new peak record for DigiCert (3.7 Tbps). These attacks represent a step change in scale and indicate that a smaller subset of malicious actors, including those associated with or leveraging botnet ecosystems such as Aisuru botnet and Kimwolf botnet, retains access to mature, high-capacity infrastructure that can be deployed when disruptive impact, coercion, or strategic signaling is prioritized.

Most activity, however, remained smaller in bandwidth and shorter in duration, reinforcing that the broader botnet ecosystem is still optimized for repeatable, low overhead disruption rather than sustained maximum output. Operationally, the majority of events also remained comparatively simple, with attacks most often relying on a single vector rather than complex multi-vector execution. This indicates that routine disruption is still driven by scalable, low complexity flooding, while more sophisticated multi-vector behavior is likely reserved for higher intent campaigns. Carpet bombing activity remained a minority of events but continues to pose risk because it distributes pressure across many targets or endpoints, increasing response complexity and expanding the operational blast radius. Direct path attacks also continued to dominate, with amplification and reflection serving as a supporting capability used selectively rather than as a constant operating model.

In conclusion, 2025 demonstrated a dual reality: a persistent baseline of routine, smaller scale attacks alongside a growing capacity for rare but exceptionally high impact events. Industry targeting further underscores this intent-driven model, as malicious actors concentrated effort on sectors such as Financial Services and IT/Technical Services where downtime creates immediate leverage, reputational pressure, and potential downstream disruption across dependent customers. Malicious actors appear to reserve top tier bandwidth campaigns for decisive moments, while relying on simpler methods for day-to-day pressure and disruption. Maintaining resilience requires strong baseline controls for common attack patterns, and the ability to rapidly absorb and mitigate sudden escalation to tsunami-level throughput.

Stats at a Glance

Total Number of Attacks: **29,998**

Total number of hours of downtime avoided: **~14,333 Hours**

Number of Mega Attacks (100+ Gbps): **99**

Largest DDoS Attack (Gbps): **3.7 Tbps** (164.29% increase compared to 2024)

Median DDoS Attacks (Gbps): **0.24 Gbps** (60% increase compared to 2024)

Average DDoS Attack (Gbps): **2.69 Gbps** (21.72% increase compared to 2024)

Largest DDoS Attack (million packets-per-second): **425.61 Mpps**

Median DDoS Attacks (packet-per-second): **41.32 Kpps** (9a1.30% increase compared to 2024)

Average DDoS Attack (packets-per-second): **544.84 Kpps** (83.58% increase compared to 2024)

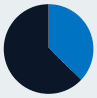
Longest DDoS Attack: **11.00 Days** (237.61% increase compared to November 2025)

Average Duration: **28.67 Minutes** (6.11% increase compared to 2024)

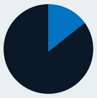
Median Duration: **7.58 Minutes** (9.86% increase compared to 2024)

Unique vs Carpet Bombing: **82.61%** Unique **17.39%** Carpet Bombing

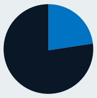
Top Three Industries Targeted:



Financial Services (37.23%)



IT/Technical Services (15.04%)



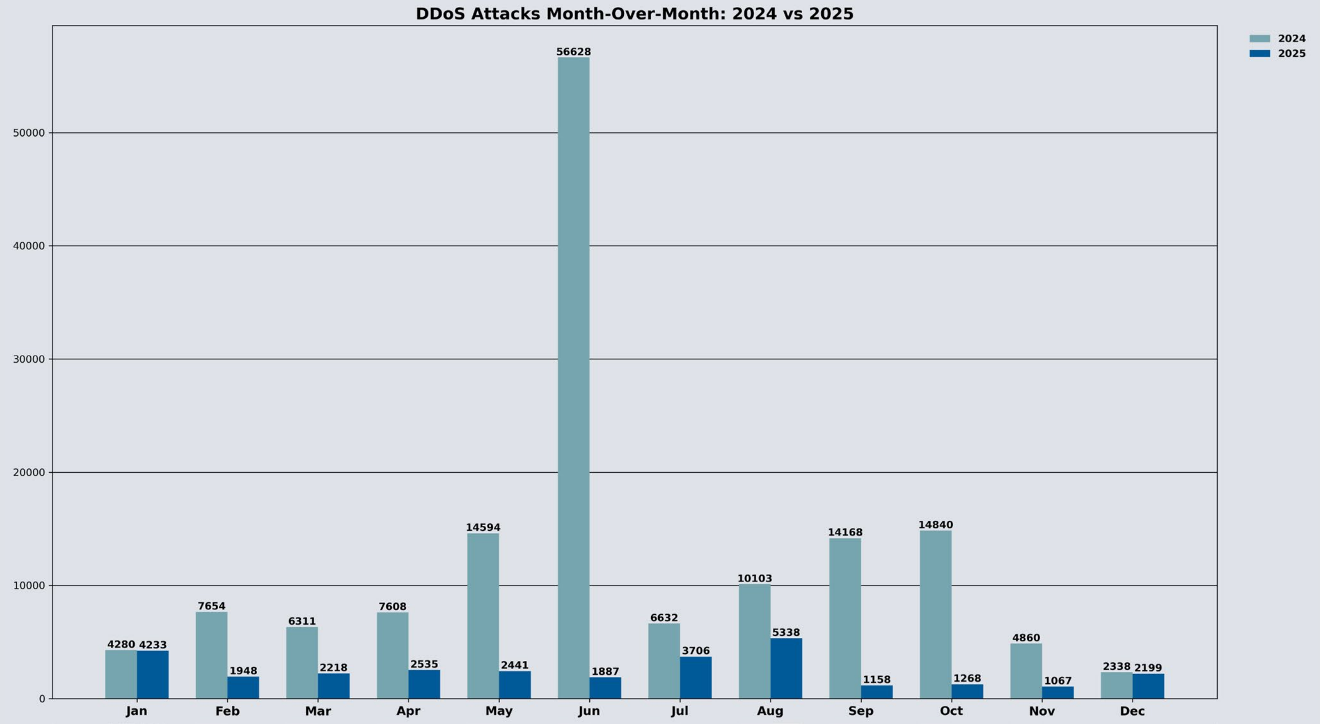
Software/Web Services (22.98%)

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.

During 2025, DigiCert UltraDDoS Protect detected 29,998 DDoS Attacks, an 88.91% decrease compared to 2024. The significant decrease in the overall number of DDoS attacks is more than likely linked to two key factors. The first key factor was global law enforcement actions such as Operation PowerOff and Operation Eastwood which dismantled major DDoS-for-hire services and disrupted access to critical botnet infrastructure. The second key factor was a customer satisfaction program run by the DigiCert Security Operations Center to conduct threshold analysis and fine-tuning of alerts to adjust for phenomena such as traffic growth and flash crowds.

During 2025, DigiCert saw a monthly average of approximately 2,499 DDoS attacks and a median of 2,208 while 2024 had an average of 12,501 DDoS attacks and a median of 7,631 which was a decrease of 80% in terms of the average and a 71.06% decrease in terms of the median.



The emergence of Tsunami Attacks

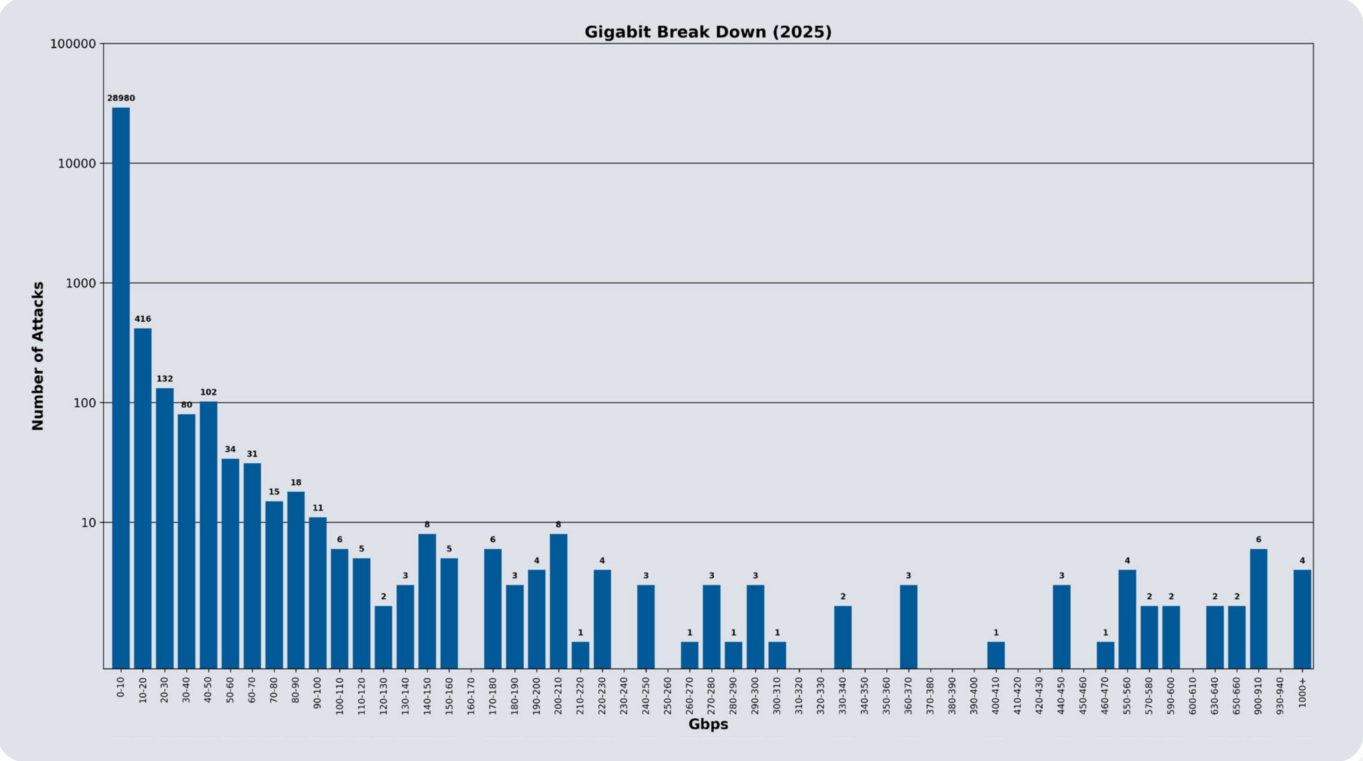
2025 saw the emergence of a new category of DDoS attacks, which quickly became prominent: the Tsunami DDoS attack. These types of DDoS attacks are classified as sophisticated, high-volume attacks over 1 Tbps, designed to overload traditional defenses and cause widespread damage.

During 2025, DigiCert mitigated four Tsunami DDoS attacks, with the largest consisting of more than 3.7 Tbps and 336 million Packets per Second (Mpps), a new DDoS record. The other Tsunami DDoS attacks observed during 2025 were a 2.4 Tbps attack with over 553 Mpps, a 2.0 Tbps attack with over 178 Mpps and a 1.1 Tbps with over 99 Mpps. Collectively, these incidents demonstrate both scale and operational maturity, and they align with a broader shift in which malicious actors appear to have rebuilt and expanded DDoS infrastructure following multiple law enforcement takedown actions in late 2024 and early 2025.

Although DigiCert observed several large-scale volumetric DDoS attacks in 2025, the majority of activity remained concentrated in the lower bandwidth range. Attacks measuring between 0.0 and 0.5 Gbps accounted for nearly 65% of all observed events, reinforcing that day-to-day disruption, reconnaissance, and pressure tactics continue to be driven by high volume, low intensity campaigns, rather than peak throughput. This pattern indicates malicious actors still prioritize smaller scale attacks for routine operations, while reserving extreme bandwidth events for more decisive, higher impact campaigns. It also suggests that most botnets remain constrained by limited capacity and reliably generate only lower scale traffic, with tsunami-level capability concentrated among a narrower set of mature infrastructures.

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

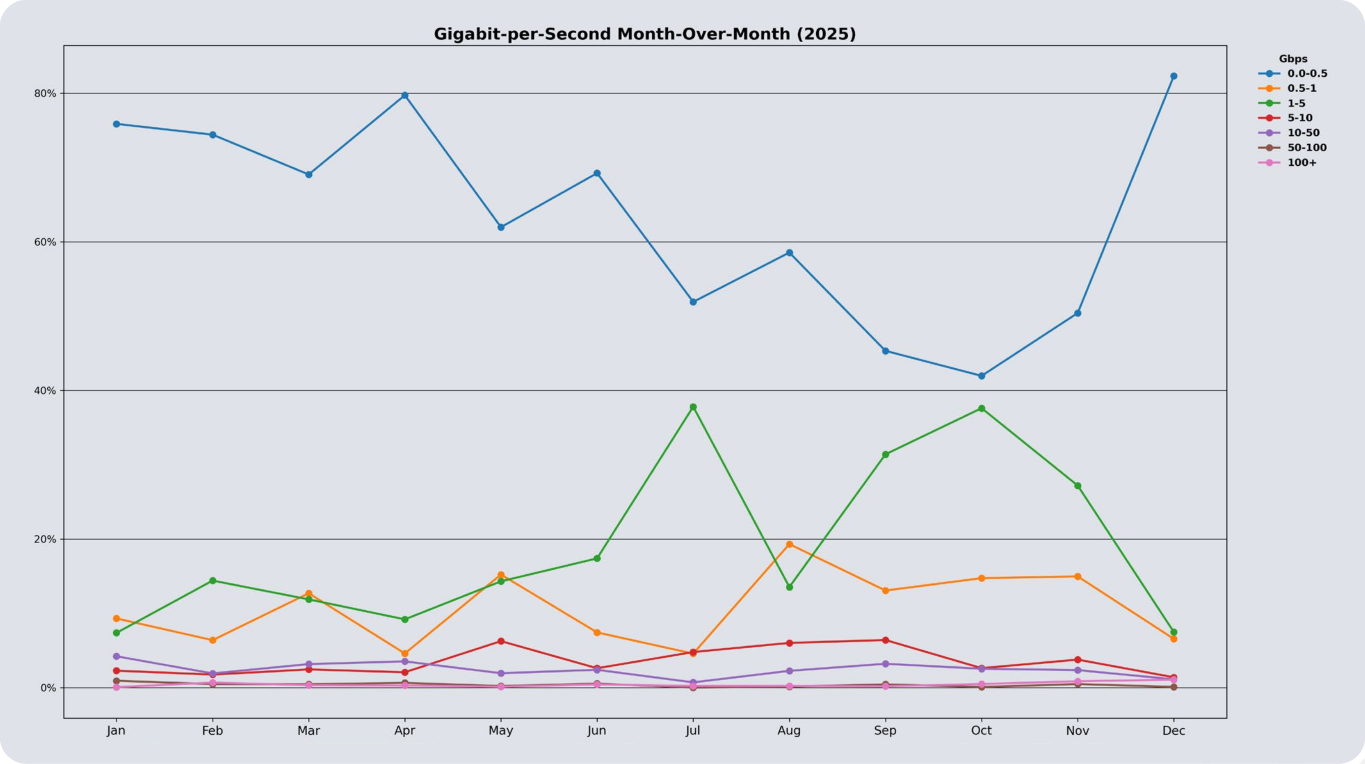
Gigabit per Second			
Gbps	Total Count	Percentage	% Yearly Change
0 - 0.5	19, 434	64.96%	↓ -82.05%
0.5 - 1	3, 262	10.90%	↓ -79.51%
1 - 5	5, 172	17.29%	↓ -64.11%
5 - 10	1, 112	3.72%	↓ -61.89%
10 - 50	730	2.44%	↓ -84.80%
50 - 100	109	0.36%	↓ -91.67%
100+	99	0.33%	↓ -90.81%



Activity across bandwidth

The 2025 month-over-month Gbps distribution shows that sub-0.5 Gbps activity consistently dominated the threat landscape, with notable periods where mid-tier bandwidth became more prevalent. From January through April, 0.0 to 0.5 Gbps attacks accounted for roughly 70% to 80% of events, indicating a steady baseline of low bandwidth disruption and probing. That share declined through mid-year, reaching its lowest levels in September and October, where the data shows a temporary rebalancing toward higher throughput, particularly in the 0.5 to 1 Gbps range, with surges in July and again across September and October. The 1 to 5 Gbps range peaked in August and remained elevated into November.

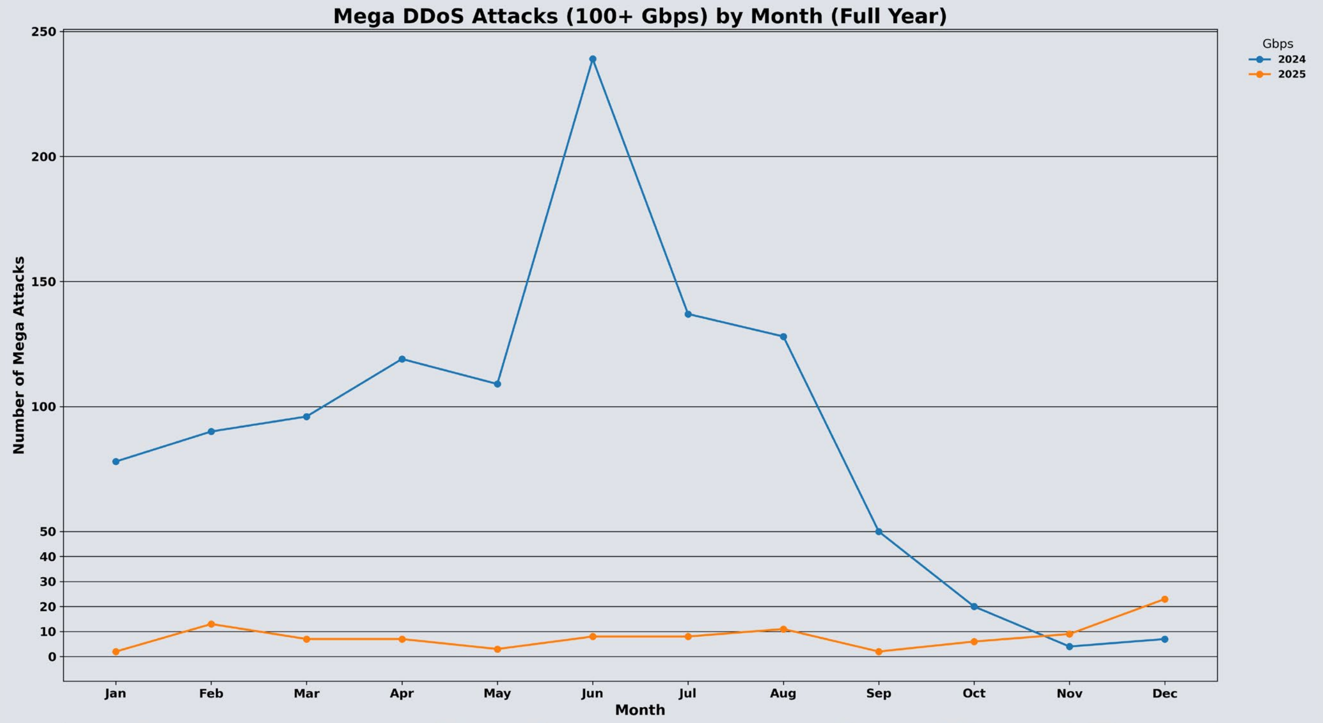
Despite these shifts, the higher bandwidth categories, including 5 to 10 Gbps and above, remained comparatively flat and consistently low throughout the year, suggesting that large scale capability was present but not broadly exercised across routine operations. By December, the distribution sharply reverted back toward 0.0 to 0.5 Gbps attacks, reinforcing that most observed activity still clusters in smaller bandwidth events, with episodic mid-tier increases that are likely tied to specific campaigns rather than a sustained new baseline.



Instances of Mega Activity

In 2025, mega DDoS attacks (attacks consisting of 100+ Gbps) remained comparatively limited and uneven when measured against 2024. While 2024 sustained a high tempo of mega activity from January through August and culminated in a dramatic June surge before sharply tapering in the final quarter, 2025 maintained a much lower baseline for most of the year. After a brief elevation in February 2025 generally held to single digit to low teen monthly totals through the spring and summer, dipped again in September, and then gradually increased through October and November before a clearer rise in December.

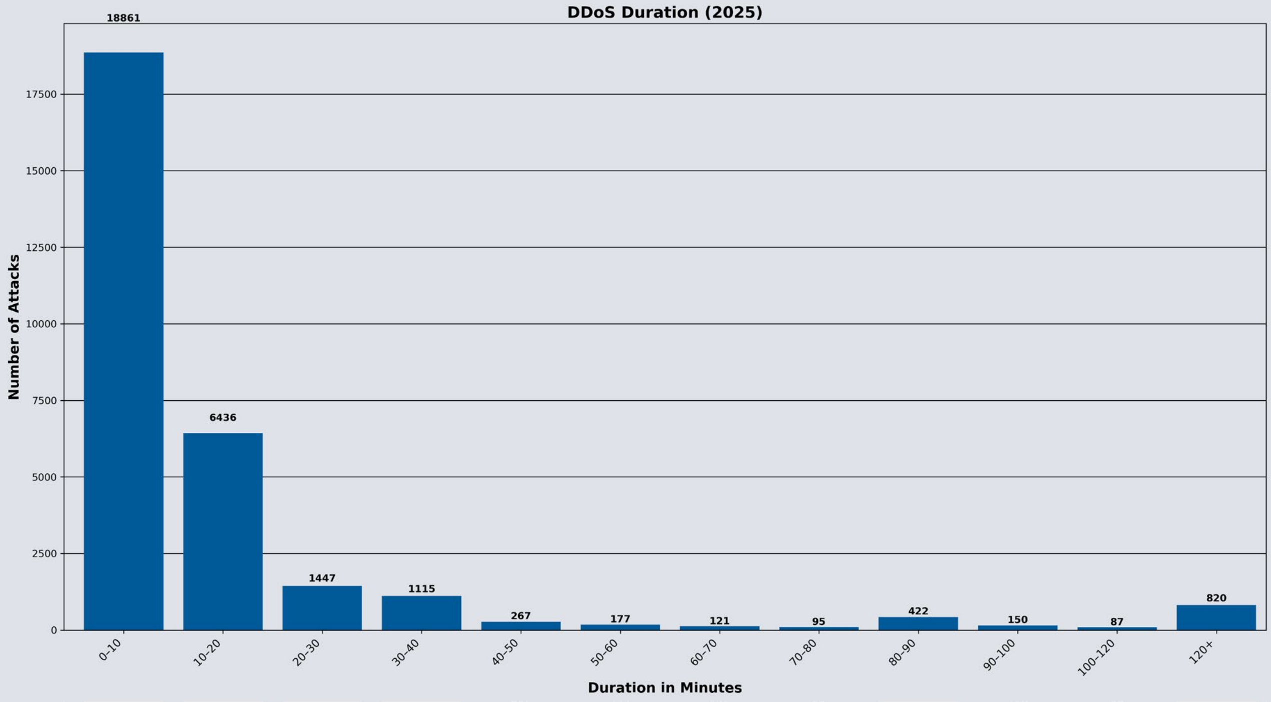
This side-by-side pattern indicates that, relative to 2024, malicious actors in 2025 either exercised greater restraint with high throughput campaigns, faced reduced access to large scale infrastructure, or shifted toward smaller, more repeatable operations. Even with tsunami-level events present during 2025, the overall cadence of mega attacks suggests that extreme capability was used selectively rather than as a persistent operating model, and that most botnet ecosystems continued to support smaller scale attacks with large scale events reserved for higher impact campaigns.



Duration

The 2025 duration profile is heavily skewed toward short lived activity, indicating that most DDoS operations were executed as brief bursts rather than sustained campaigns. Attacks lasting 0 to 10 minutes represented 18,861 events (approximately 63% of total activity), while 10 to 20 minutes added 6,436 events (approximately 21%), meaning roughly 84% of attacks concluded within the first 20 minutes. After that point, volumes drop sharply across the 20 to 40 minute ranges and remain comparatively low through 40 to 80 minutes, reflecting a steep attrition curve, where fewer campaigns maintain pressure once initial disruption attempts fail.

Longer duration events were present but uncommon, with 120+ minute attacks totaling 820 events, (approximately 3%), suggesting that sustained operations were reserved for specific objectives such as prolonged disruption, coercion, or high value targeting. One notable deviation is the increase in the 80 to 90 minute bin, relative to adjacent ranges, which may indicate a subset of campaigns designed to persist beyond common mitigation and monitoring windows. Overall, the distribution aligns with a threat environment where malicious actors favor quick, repeatable attacks to test response and create localized disruption, while only a smaller portion of activity reflects the intent, coordination, and resources required to sustain longer operations.

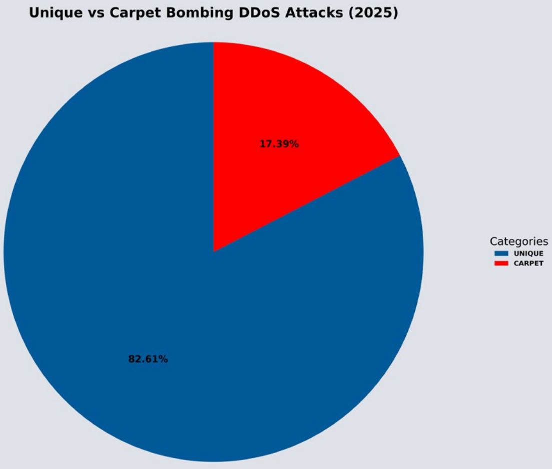


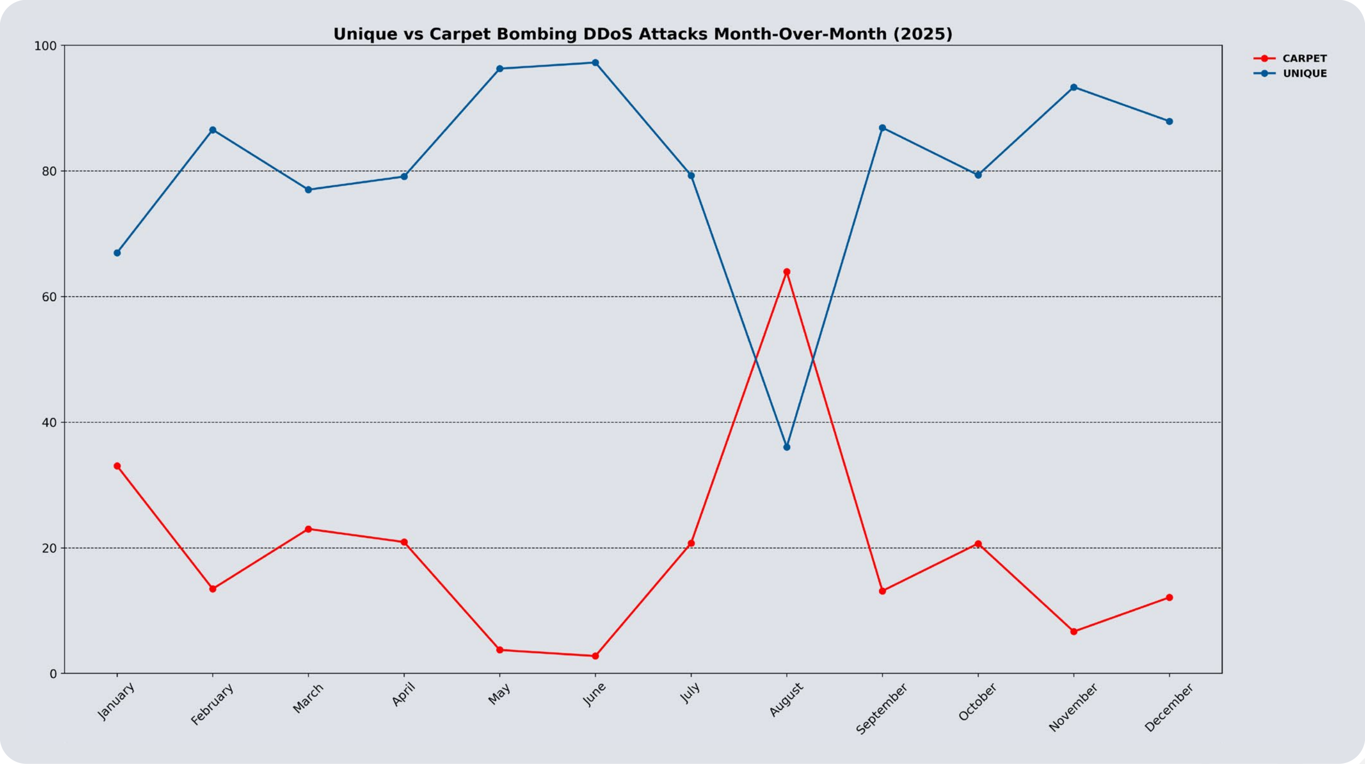
Unique vs Carpet Bombing DDoS Attacks

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.

In 2025, the majority of observed DDoS activity was classified as unique attacks, accounting for 82.61% of events, while carpet bombing attacks represented 17.39%. This split indicates that most campaigns continued to rely on discrete, single target operations rather than distributed, multi-target flooding intended to create broader disruption across many endpoints. It is also important to note that the carpet-bombing analysis methodology was updated in May 2025 to improve accuracy, which contributed to a notable reduction in the number of attacks categorized as carpet bombing for the remainder of the year. The revised approach incorporates additional data elements and applies stricter identification criteria to ensure that only larger and more operationally impactful carpet-bombing activity is counted, improving confidence that reported events reflect deliberate, high scale campaigns rather than smaller, ambiguous patterns that can resemble carpet bombing behavior.

When looking at the month-over-month trend for 2025, unique attacks remained the dominant pattern across the year, generally comprising the majority of monthly events and indicating that most malicious actors continued to favor discrete, single-target operations. Carpet bombing activity was comparatively lower and more episodic, declining to minimal levels in late spring and early summer. These attacks rose sharply in August, where they briefly became the predominant type, coinciding with a pronounced drop in unique attacks. This spike is consistent with a concentrated campaign period in which malicious actors shifted toward broad, multi-target disruption tactics. After August, carpet bombing levels fell back toward baseline and unique attacks again dominated through the remainder of the year, reinforcing that carpet bombing was used selectively and in bursts rather than as a steady operating model.





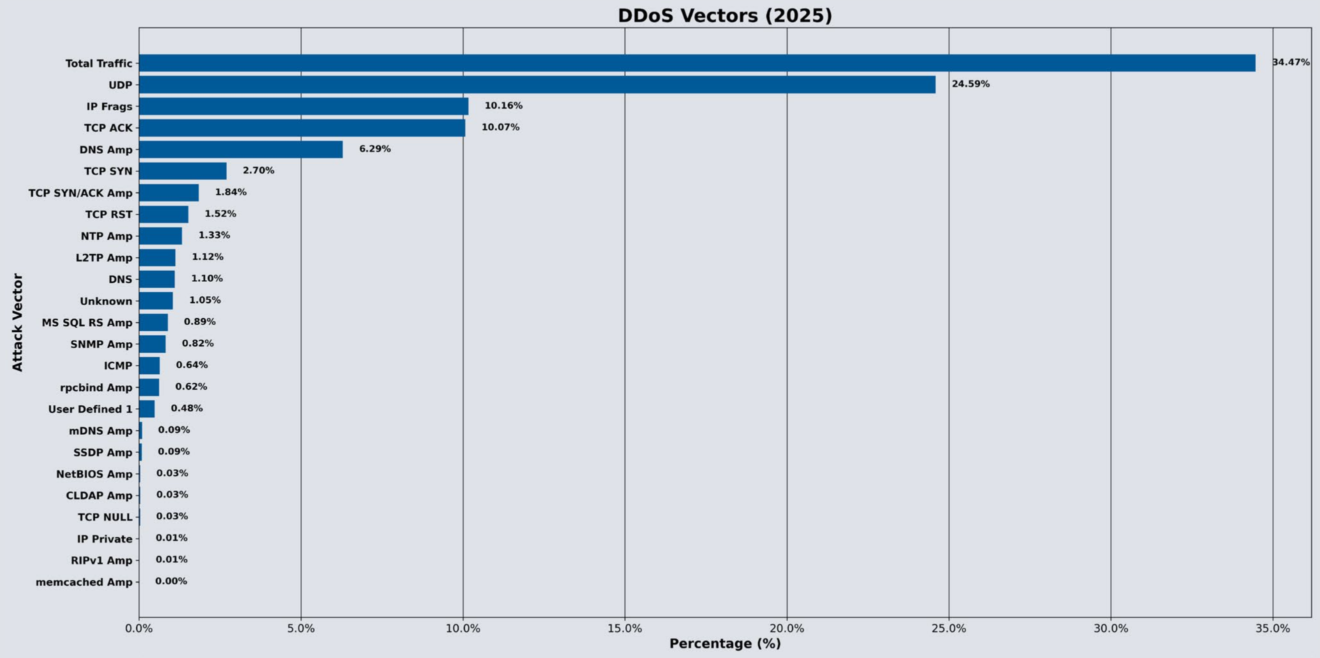
Attack Vectors

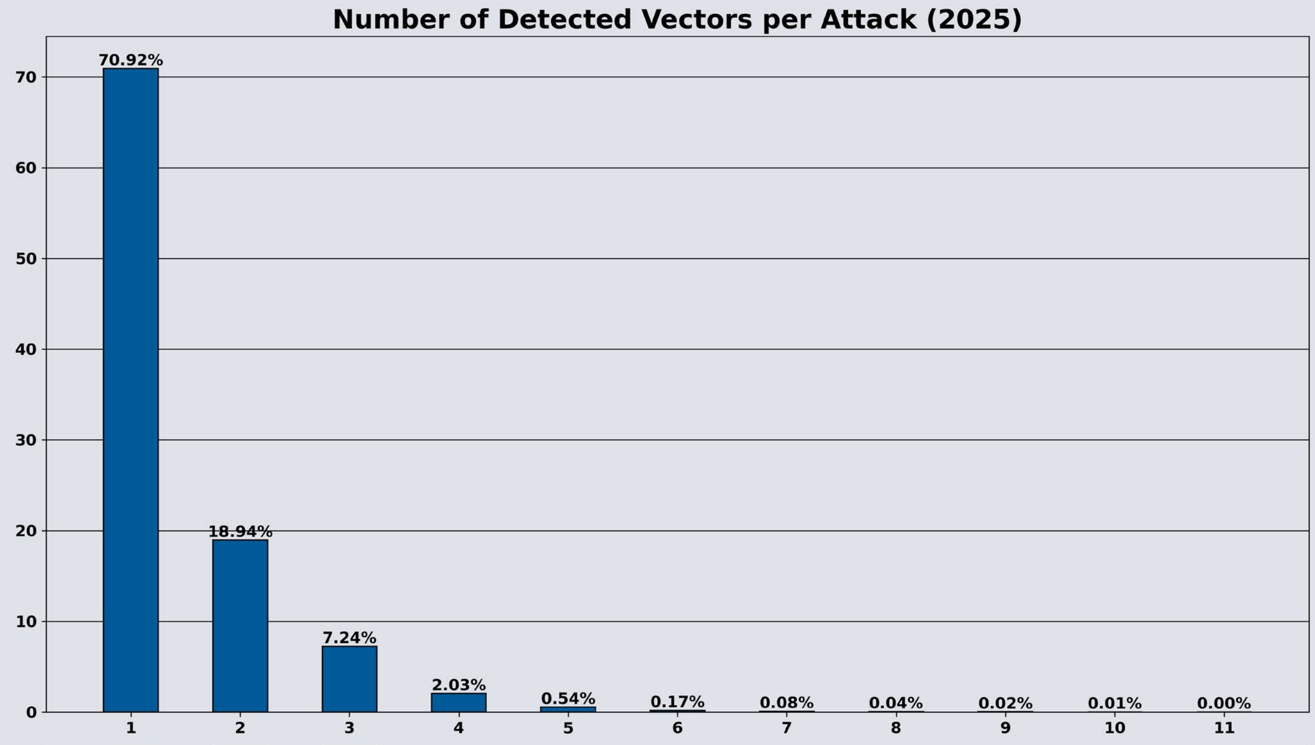
An attack vector is a mechanism, usually an abused network protocol or a variety of packets inside of a protocol, that a DDoS attack uses to generate high volumes of traffic. Attack vectors also serve as signatures to detect DDoS traffic outside Gbps and PPS. Attack vector statistics change in popularity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

In 2025, DDoS activity was concentrated in a small number of high frequency vectors, indicating that most malicious actors continued to favor reliable, repeatable techniques over complex traffic orchestration. The largest category, Total Traffic (34.47%) reflects attacks that exceeded established volumetric thresholds or exhibited characteristics consistent with potential carpet-bombing activity, rather than a single protocol specific vector. Its prominence suggests a meaningful share of events either generated sufficient volume to trigger threshold-based detection or relied on distributed targeting patterns that elevate overall traffic across many endpoints. UDP (24.59%) remained the most common discrete vector, reinforcing that generic UDP flooding continues to be an effective method for rapidly generating bandwidth pressure. IP Frags (10.16%) and TCP ACK (10.07%) further indicate sustained use of fragmentation and state pressure behavior that can increase processing overhead and complicate filtering.

Amplification and reflection remained present but comparatively less dominant, with DNS amplification leading at 6.29%, followed by smaller contributions from TCP SYN ACK amplification (1.84%) and NTP amplification (1.33%). Other amplification vectors, including MS SQL RS, SNMP, and rpcbind, appeared at low but persistent levels, suggesting opportunistic use of exposed third-party services rather than reliance on a single dominant reflector beyond DNS.

Vectors-per-attack distribution shows that most operations were intentionally simple. Approximately 70.92% of attacks used a single detected vector and 18.94% used two vectors, while only 7.24% used three vectors and 2.03% used four vectors, with higher counts rare. Overall, the data indicates that routine disruption is largely driven by single vector flooding and threshold triggering activity, while multi vector execution appears reserved for more deliberate campaigns where resilience against mitigation and sustained pressure are higher priorities.


DDoS Vectors (2025)
Attack Vector
Total Traffic 34.47%
UDP 24.59%
IP Frags 10.16%
TCP ACK 10.07%
DNS Amp 6.29%
TCP SYN 2.70%
TCP SYN/ACK Amp 1.84%
TCP RST 1.52%
NTP Amp 1.33%
L2TP Amp 1.12%
DNS 1.10%
Unknown 1.05%
MS SQL RS Amp 0.89%
SNMP Amp 0.82%
ICMP 0.64%
rpcbind Amp 0.62%
User Defined 1 0.48%
mDNS Amp 0.09%
SSDP Amp 0.09%
NetBIOS Amp 0.03%
CLDAP Amp 0.03%
TCP NULL 0.03%
IP Private 0.01%
RIPv1 Amp 0.01%
memcached Amp 0.00%
0.0%
5.0%
10.0%
15.0%
20.0%
25.0%
30.0%
35.0%
Percentage (%)


Number of Detected Vectors per Attack (2025)
70
60
50
40
30
20
10
0
70.92%
18.94%
7.24%
2.03%
0.54%
0.17%
0.08%
0.04%
0.02%
0.01%
0.00%
1
2
3
4
5
6
7
8
9
10
11

Vector distribution through the year

The 2025 month-over-month vector distribution shows a dynamic mix of baseline activity and short, campaign driven spikes across several techniques.

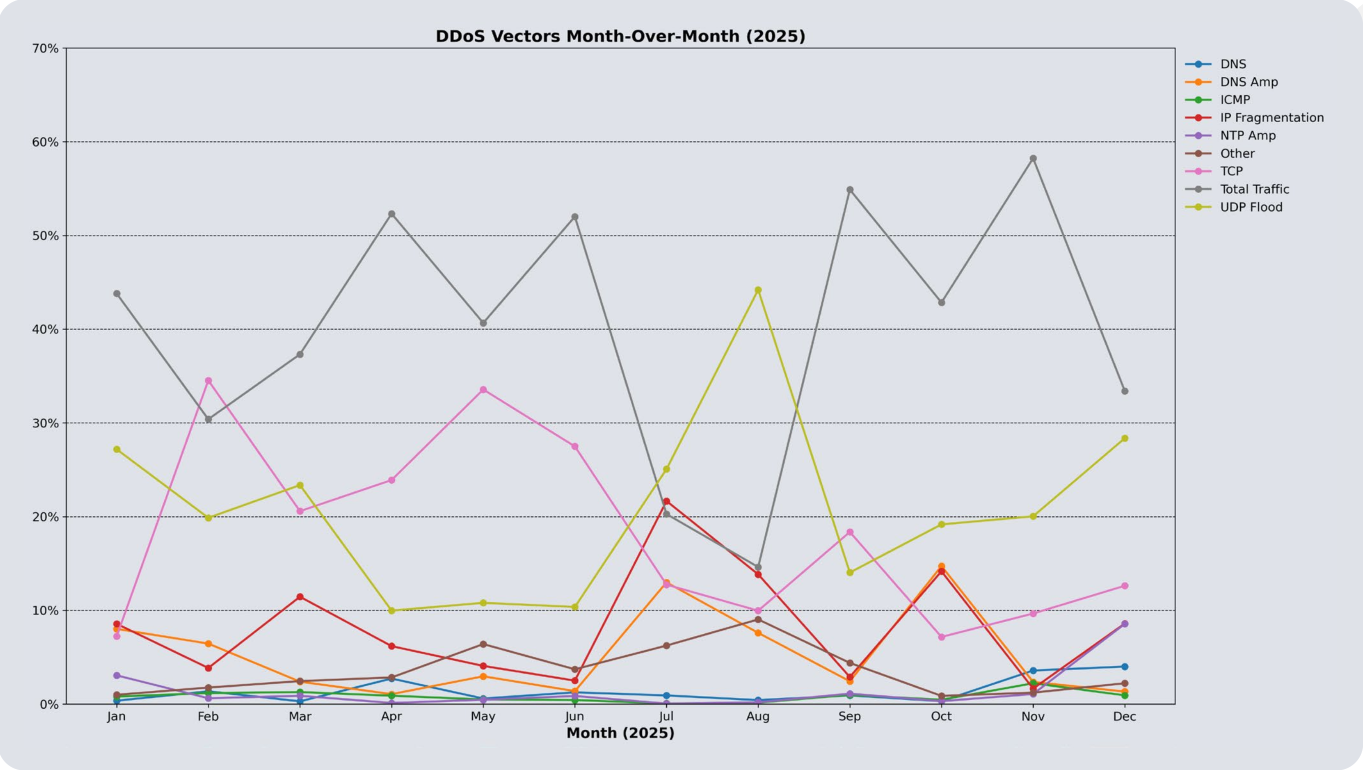
The Total Traffic category consistently accounts for the largest share in most months, remaining elevated through the first half of the year and then surging again in September and November, before easing in December. This pattern aligns with periodic increases in threshold triggering activity and potential carpet-bombing style behavior rather than a single protocol specific vector.

UDP Flood remains a persistent driver throughout the year, starting relatively high in January, dipping through spring, then rising sharply to its annual peak in August, and finishing the year elevated in December, which is consistent with broad, repeatable volumetric flooding used as a dependable pressure mechanism.

TCP activity is more volatile, spiking early in the year with pronounced peaks in February and May, then declining in mid-year before stabilizing and recovering modestly toward the end of the year.

Several secondary vectors show concentrated bursts that likely reflect discrete campaigns or technique shifts, including IP fragmentation, which spikes sharply in July and remains elevated in August, and DNS amplification, which increases in July and reappears as a notable contributor in October. NTP amplification remains low for most of the year but rises in December, suggesting limited but recurring access to reflector capacity.

Overall, the data indicates malicious actors rotated between a few dependable vectors while selectively introducing amplification and fragmentation during specific periods to increase impact or complicate mitigation.



Direct path versus amplification

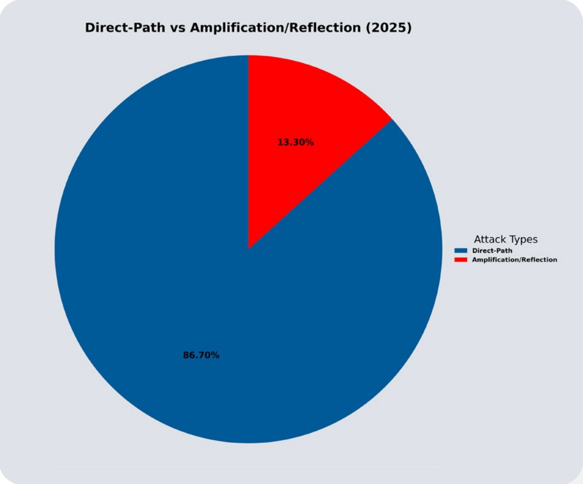
Across 2025, direct path activity clearly dominated the observed DDoS landscape, accounting for 86.70% of attacks, while amplification and reflection techniques represented 13.30%. This split indicates that most malicious actors relied on traffic generated directly from botnet infrastructure, rather than depending on third party reflectors to multiply throughput. When comparing month over month behavior, 2025 shows a more distributed pattern than 2024, with pronounced mid-year clustering.

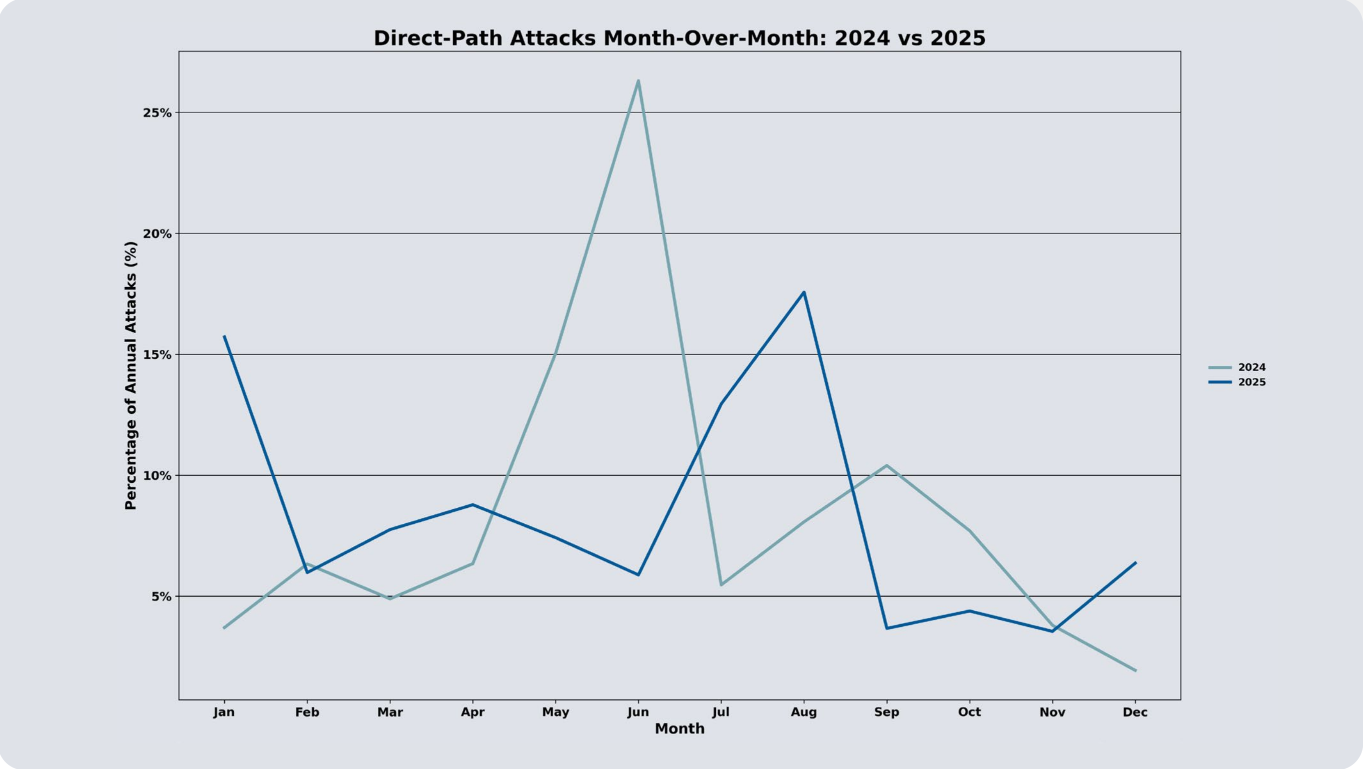
In 2025, direct path attacks were elevated early in January, then remained moderate through the spring before rising sharply in July and August, suggesting a period where botnet-driven flooding became the primary operational focus.

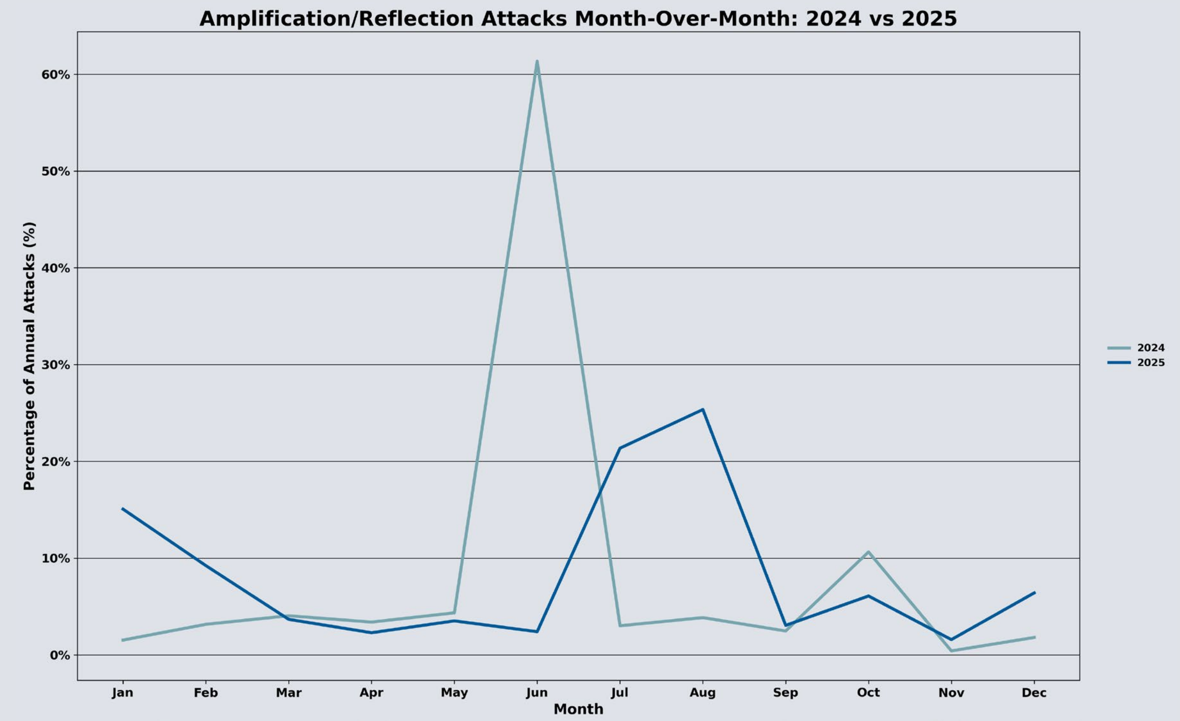
Amplification and reflection activity in 2025 followed a similar cadence, declining across the first half of the year and then increasing noticeably in July and August, which is consistent with malicious actors briefly expanding into reflector enabled capacity during a concentrated campaign window, before returning to lower levels in September and then gradually rebuilding into December.

By contrast, 2024 exhibits a much more extreme June concentration, with amplification and reflection peaking dramatically during that month and direct path also reaching its highest share, followed by a rapid normalization afterward.

Overall, the 2025 profile suggests amplification and reflection remained a supporting capability that was activated selectively, while direct path techniques remained the dependable baseline across the year, reinforcing that sustained botnet capacity continues to be more consistently available than large scale reflector driven infrastructure.







Events By Targeted Industry

Examining attacks by industry allows extrapolation into other organizations inside the same 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.

Highest targeted industries

In 2025, DDoS targeting was heavily concentrated in sectors where availability is tightly linked to revenue, customer trust, and downstream operational dependency.

Top tier industries

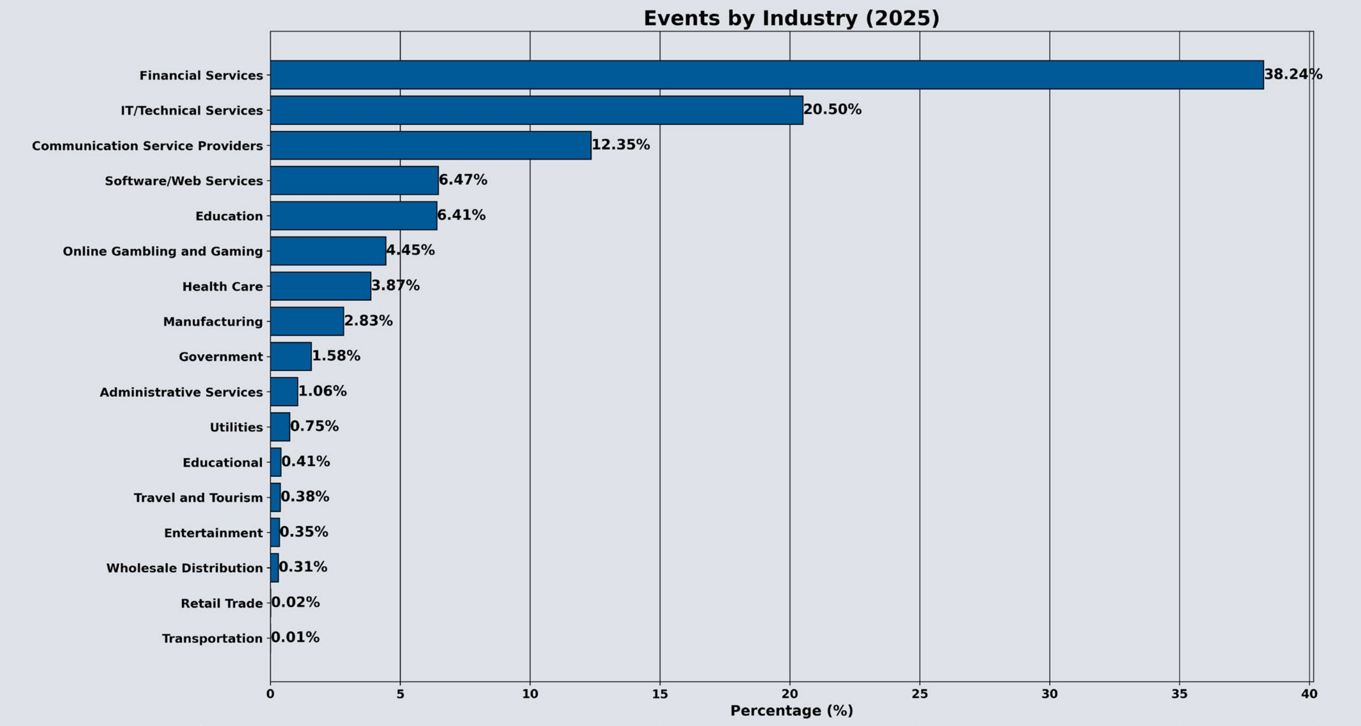
Financial Services accounted for 38.24% of observed events, making it the primary target, which is consistent with the sector's low tolerance for disruption and the high leverage malicious actors gain by interrupting payment flows, online banking, trading platforms, and authentication services. Financial organizations also present strong extortion value, since even short outages can create immediate customer impact and reputational pressure.

IT and Technical Services represented 20.50% of attacks, reflecting the role of managed service providers, cloud hosting, and technology platforms as aggregation points. Disrupting these providers can create cascading effects across multiple customer environments, making them attractive targets for malicious actors seeking broad impact with a single campaign.

Communication Service Providers comprised 12.35%, which aligns with the strategic value of degrading connectivity and core internet services, alongside the fact that telecommunications infrastructure can amplify business disruption across a wide range of dependent industries.

Second tier industries

A second tier of targeting included Software and Web Services at 6.47% and Education at 6.41%, where highly visible online services, seasonal traffic patterns, and comparatively uneven security maturity can increase susceptibility. Online Gambling and Gaming accounted for 4.45%, a sector frequently targeted due to real-time service requirements, high sensitivity to latency and downtime, and competitive or coercive motives that can translate into immediate financial losses. Lower shares across Health Care, Manufacturing, and Government still reflect meaningful risk, but the overall distribution indicates malicious actors prioritized industries where disruption is most measurable, response windows are short, and the opportunity for extortion, retaliation, or strategic signaling is highest.



Opportunistic attack patterns

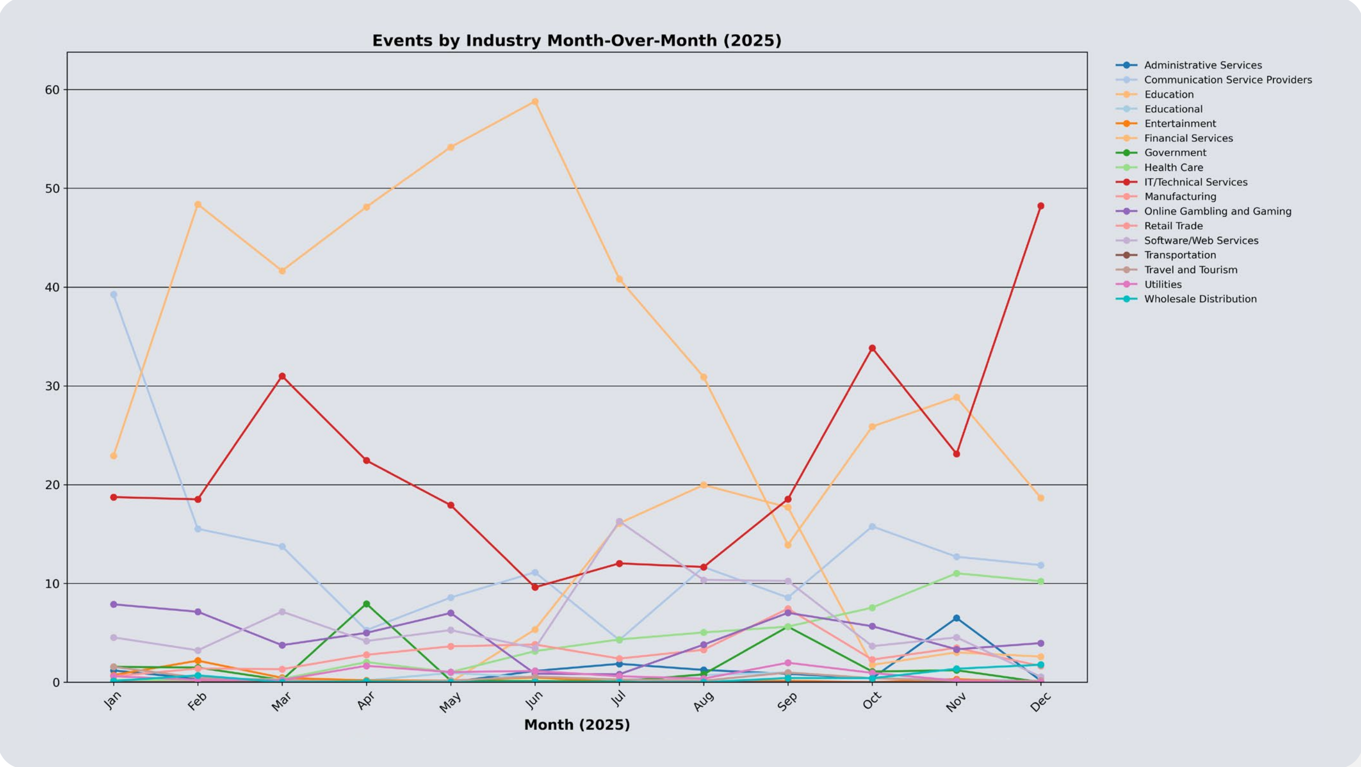
Industry targeting in 2025 shows clear seasonality and episodic surges that suggest campaign level focus rather than a uniform distribution across the year.

The most pronounced early year concentration appears in Financial Services, where activity rises sharply beginning in February, remains elevated through the spring, and peaks around late spring to early summer before steadily declining, a pattern that may align with tax season driven fraud pressure, increased log in activity, and higher sensitivity to availability for payment, banking, and customer authentication workflows.

IT and Technical Services displays a different profile, with intermittent spikes in the first half of the year, a renewed rise in the fall, and a pronounced surge in December, consistent with technology and managed service environments being targeted when malicious actors aim to create downstream impact across multiple customers, or when major vulnerability disclosures and patch cycles can drive scanning and exploitation related traffic that escalates into denial of service.

Communication Service Providers and several mid-tier sectors show localized increases during the summer and early fall, which may reflect attempts to degrade connectivity and amplify disruption during concentrated campaign windows.

In contrast, most remaining industries stay comparatively low and stable, indicating they were not primary targets for sustained activity, even if they still experienced periodic events. Overall, the distribution supports that malicious actors concentrated effort where downtime creates immediate leverage, and shifted targeting in response to seasonal demand, major public events, and tactical opportunities created by infrastructure dependencies.



Attacks By Country

The 2025 distribution of attacked countries indicates that DDoS activity remained concentrated in markets with large digital footprints, high value services, and strong downstream dependency on availability.

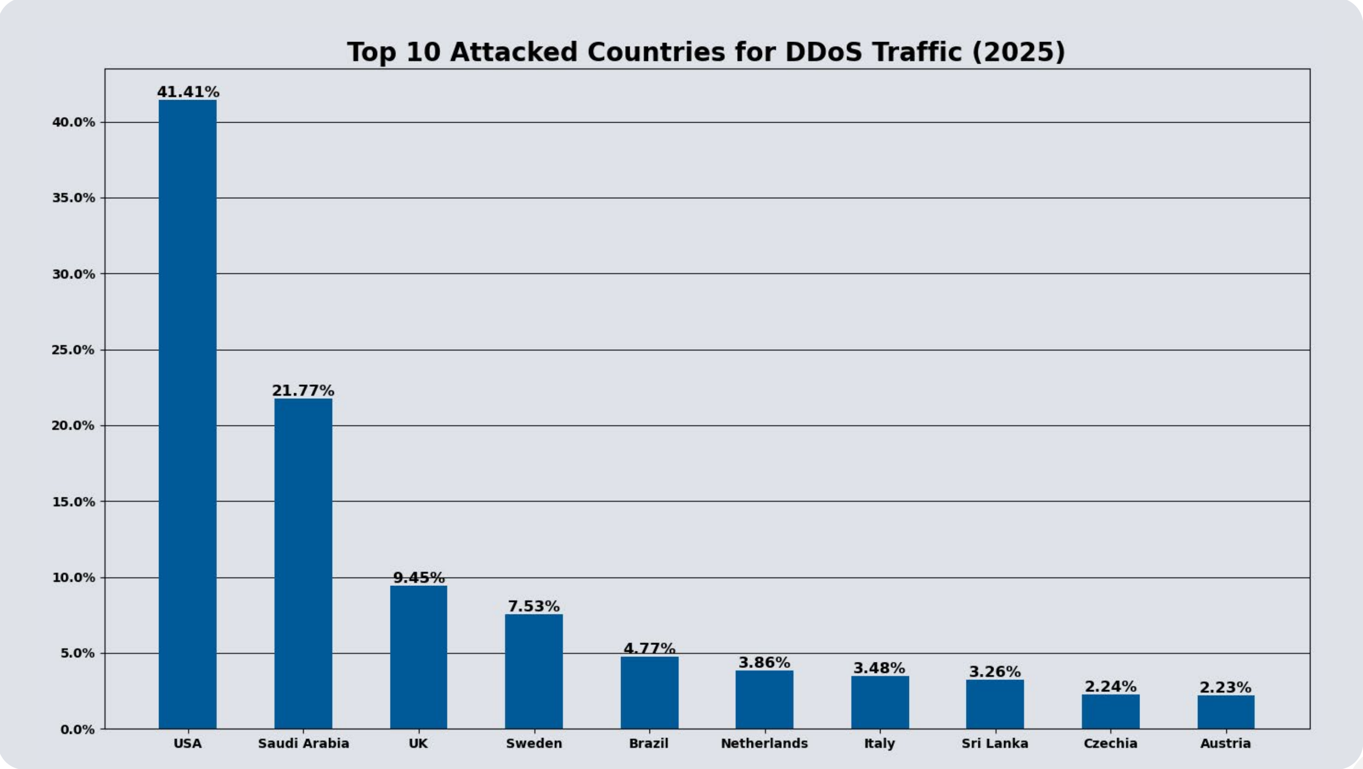
The United States represented 41.41% of observed attacks, which is consistent with the scale of its online economy and the density of high impact targets such as financial services, cloud and managed service providers, and public sector organizations, all of which can produce outsized operational and reputational effects when disrupted.

Saudi Arabia accounted for 21.77%, a level that may reflect a combination of strategic targeting considerations, including the prominence of energy and government-aligned services, heightened regional geopolitical sensitivity, and the visibility of national initiatives and events that can increase both traffic volume and attacker incentive.

The United Kingdom (9.45%) and Sweden (7.53%) further reinforce that European targets remained a sustained focus, potentially driven by a mix of geopolitical tension spillover, high reliance on online public services, and the concentration of enterprises that are frequently targeted for disruption and extortion.

Several countries in the list, including the Netherlands (3.86%), also represent significant internet infrastructure and hosting ecosystems, where targeting can be motivated by the opportunity to impact collocated services or high value platforms. Brazil (4.77%) aligns with large scale consumer internet usage and a mature financial sector that is frequently targeted for disruption. Italy, Austria, and Czechia collectively suggest persistent pressure across the broader European environment, while Sri Lanka's presence may reflect targeting tied to localized political sensitivity, economic conditions, or regional instability.

Overall, the pattern is consistent with malicious actors prioritizing countries where disruption is most likely to create immediate leverage, attract attention, or amplify broader geopolitical and operational objectives.



Attacks By Source Country

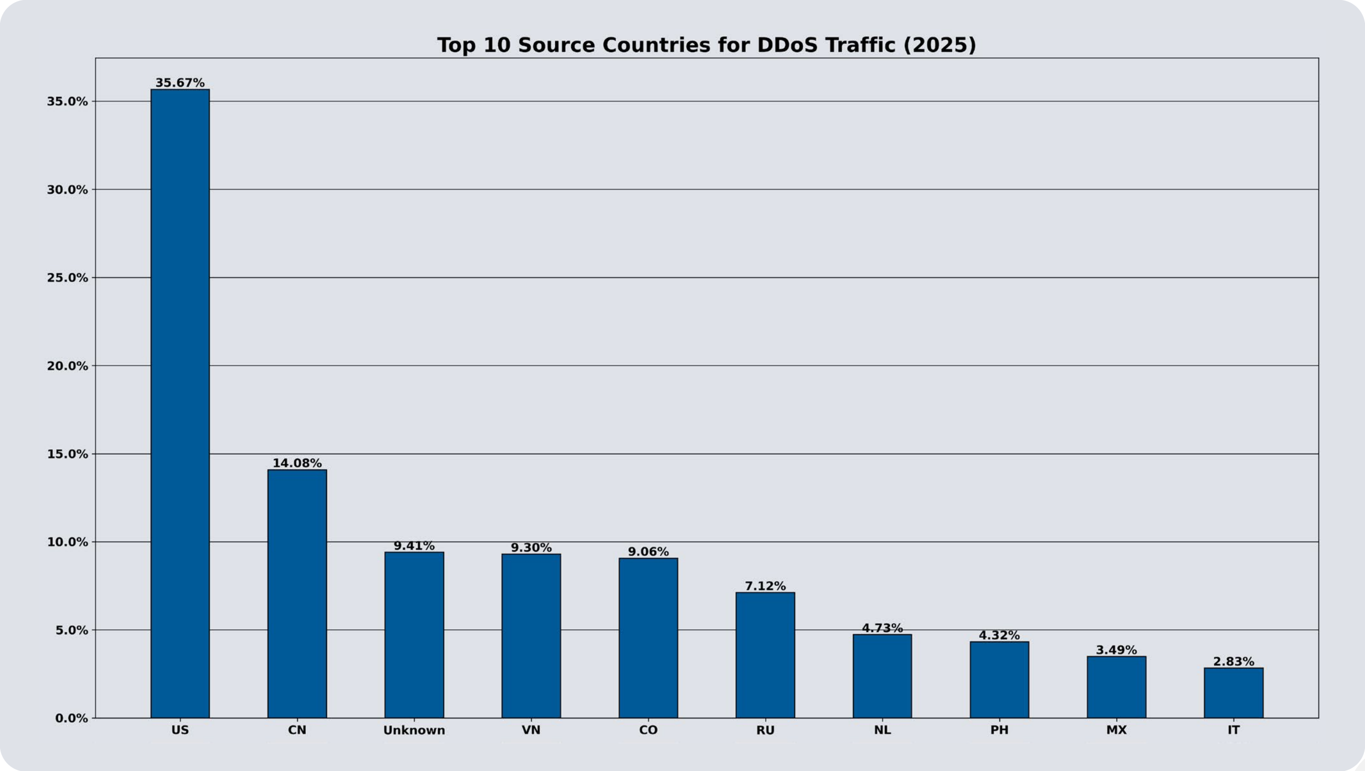
The top five source countries for observed DDoS traffic in 2025 were the United States (35.67%), China (14.08%), an Unknown category (9.41%), Vietnam (9.30%), and Colombia (9.06%).

The United States leading as a source is consistent with the global concentration of cloud infrastructure, data centers, and consumer broadband, where compromised servers, misconfigured services, and infected endpoints can be leveraged into botnet capacity, even when the controlling malicious actors are located elsewhere. China's share similarly aligns with the scale of its internet population and device ecosystem, which can provide significant botnet recruitment potential through vulnerable IoT, residential devices, and exposed services.

The Unknown category is likely influenced by visibility limits in attribution and telemetry, including traffic that cannot be confidently geolocated due to factors such as anonymization infrastructure, NAT, routing complexity, or incomplete IP to geography resolution.

Vietnam and Colombia round out the top five, likely reflecting persistent botnet recruitment in regions where large volumes of consumer devices and hosting resources coexist with uneven patching and security hygiene, creating durable pools of compromised endpoints that can be repurposed for high volume flooding.

Overall, the distribution is more indicative of where attack infrastructure is sourced or where compromised devices reside, rather than a direct indicator of malicious actor origin or intent. 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.



About DigiCert Ultra DDoS Protect

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 DDoS solutions, please visit our website or contact us.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.