Q3 2025

digicert®

RADAR

Risk Analysis, Detection & Attack Reconnaissance

Introduction

Welcome to RADAR—DigiCert's quarterly threat intelligence brief delivering data-driven insights on emerging cyber threats.

Each edition distills findings from trillions of network events across DigiCert's platform, including UltraDNS, UltraDDoS Protect, and UltraWAF. This breadth of visibility gives RADAR a uniquely authoritative view of attacker behavior and usage trends across infrastructure, applications, and traffic.

Our goal: to turn signal into strategy, helping organizations strengthen resilience, reduce risk, and stay ahead of the next wave of cyber threats.

Executive Summary

Between July and August 2025, DigiCert's UltraDDoS Protect network faced its most intense test yet, absorbing a relentless wave of distributed denial-of-service (DDoS) attacks, many peaking between 600 and 800 gigabits per second (Gbps). The real shock came in two unprecedented events that reached what DigiCert engineers call "internet tsunami" scale: one at 2.4 terabits per second (Tbps), the other at 3.7 Tbps. These attacks underscored the new reality of cyber warfare where the internet itself becomes the weapon and the battlefield.

Cyberattacks in the quarter revealed a threat landscape defined by adaptability and global realignment. Attackers are merging precision with scale while reconfiguring infrastructure to stay resilient.

One example: After law enforcement disrupted major botnets in 2024, many groups rebuilt in regions with weaker regulations and greater geopolitical volatility.

Data from DigiCert's global platform shows DDoS campaigns now alternating between precision strikes and massive subnet floods. Attacks exceeding 1 Tbps have become routine, with multi-terabit, tsunami-scale assaults setting a new benchmark for disruption.

Web exploitation also intensified as attackers automated reconnaissance and exploited legacy code, driving bot traffic to record highs. This industrialization of credential testing has made automated abuse a constant background threat.

Even DNS, the backbone of the internet, showed strain. Query volumes held steady at about 4.2 trillion per month, but malformed traffic spiked 22,000%, revealing how minor misconfigurations and automated probing can ripple across global infrastructure.

Beneath these shifts lies a deeper signal. The same geopolitical and economic forces reshaping global markets are now visible in cyberspace. Much of today's traffic originates in regions where digital infrastructure is growing faster than governance, and where patriotic or opportunistic groups use cyber activity to project influence or disrupt Western systems.

The takeaway is clear. Attackers combine speed, automation, and precision to push global defenses to their limit. DigiCert's visibility across DNS, DDoS, and WAF gives organizations the early detection and coordinated protection needed to stay ahead in a threat environment that never stops adapting.

— Michael Smith, AppSec CTO, DigiCert

Key Insights

Scale meets precision:

Tsunami-class floods and targeted DDoS strikes now occur side by side, showing how attackers blend volume and accuracy to maximize impact.

Global realignment reshapes attack origins:

DDoS and botnet activity are shifting to emerging regions such as Vietnam, Russia, and China as adversaries rebuild and adapt after enforcement actions.

Cyber conflict mirrors global tension:

The United States absorbed most DDoS attacks as regional botnets reemerged across Asia and Eastern Europe.

Digital trust becomes the measure of resilience:

Attackers are no longer only taking systems offline; they're eroding confidence in the reliability and integrity of global connectivity.

Domain NameSystem (DNS)

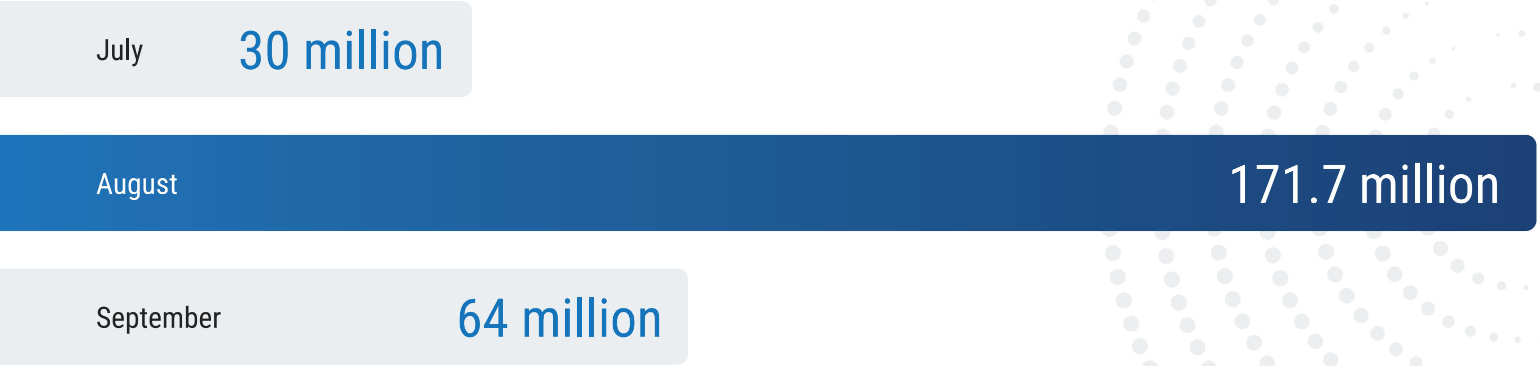
DNS remained the backbone of digital trust in the third quarter of 2025, handling about 4.2 trillion authoritative queries per month across DigiCert's global infrastructure. Activity followed predictable business and academic cycles, with the August uptick aligning with back-to-school demand and early Q4 retail/eCommerce activity, a reminder that DNS mirrors the rhythms of a connected global economy.

Within this stability, regional growth and seasonal changes reflected legitimate internet activity: China's query share climbed to 7.1%, and Japan entered the top 10 queries by volume for the first time, signaling continued expansion of resolver infrastructure across Asia. IPv6 accounted for roughly one quarter of total DNS traffic, marking steady adoption of next-generation connectivity.

While most DNS activity remains healthy, operational anomalies surfaced at scale. These anomalies—typically caused by misconfigured resolvers or automated scanning but sometimes a symptom of scanning or an attack—highlight how small inefficiencies can ripple globally through interconnected systems.

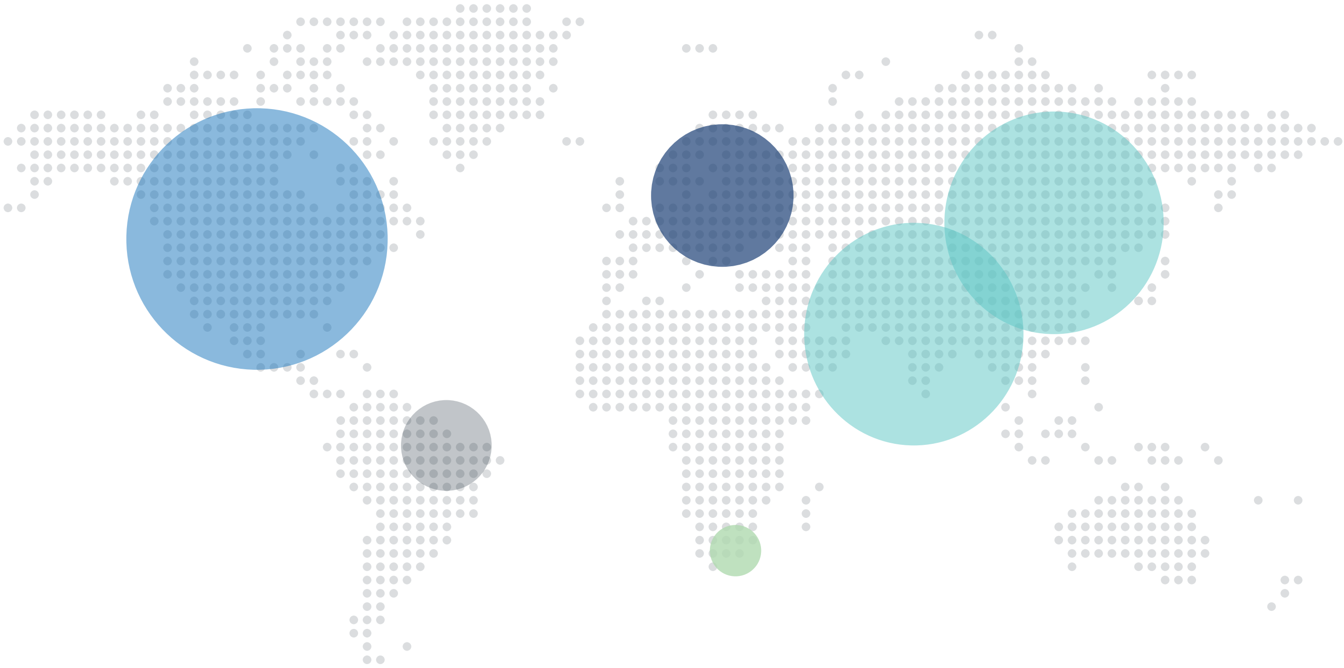
UltraDNS processed more than 12.5 trillion queries, providing dependable DNS resolution throughout periods of elevated anomaly activity.

Monthly Volume of FormErr Anomalies in Q3 2025



DNS traffic also mirrored predictable global patterns tied to business and academic cycles. The September uptick corresponded with back-to-school activity and early Q4 retail preparation, illustrating how DNS quietly reflects the rhythms of a connected global economy.

Where DNS Queries Came From in Q3 2025



38% North America

● United States

28% Asia-Pacific

● China and India

20% Europe

● Germany

8% Latin America

● Brazil

6% Middle East and Africa

● South Africa

Protecting Your Organization

View DNS as Critical Infrastructure

Treat DNS as a control plane for service management and a core enabler of performance and scale, not just an attack surface.

Watch for Anomalies

Use UltraDNS analytics to identify FormErr or NXDOMAIN surges that can signal misconfigurations or scanning activity.

Optimize Configuration Hygiene

Regularly audit DNS settings and query traffic to reduce noise from nonexistent domain lookups, dangling zone delegations, and malformed queries.

Leverage Resilience Features

Use UltraDNS^2 alongside UltraDNS for network diversity and fault isolation, ensuring stability even under anomalous load.

Distributed Denial-of-Service (DDoS)

As adversaries rebuilt botnets disrupted by the dismantling major criminal networks in late 2024, both attack frequency and scale increased. While last year's takedowns temporarily reduced global DDoS volume, many operators had rebuilt their infrastructure and regained the capacity to launch large-scale attacks by mid-2025.

At their height, carpet-bombing campaigns against enterprises accounted for 65% of all incidents observed by DigiCert in September. These subnet floods targeted entire ranges instead of single endpoints, increasing collateral risk across networks. Unique precision attacks represented 91% of events, showing how adversaries now toggle between scale and accuracy to test global defenses.

DigiCert mitigated two tsunami-class events that peaked at 2.4 Tbps and 3.7 Tbps, preventing more than 3,000 hours of potential downtime for our customers.

Attack origins reflected broader geopolitical and economic forces. The United States remained the largest launch point, showing the density of compromised assets in mature digital economies. Vietnam, Russia, and China expanded their share of global traffic, signaling the return of botnets in less-regulated regions. Latin America and Southeast Asia continued to serve as low-cost hosting and reflection zones, with economic opportunity and political tension in these regions shaping cyber risk dynamics.

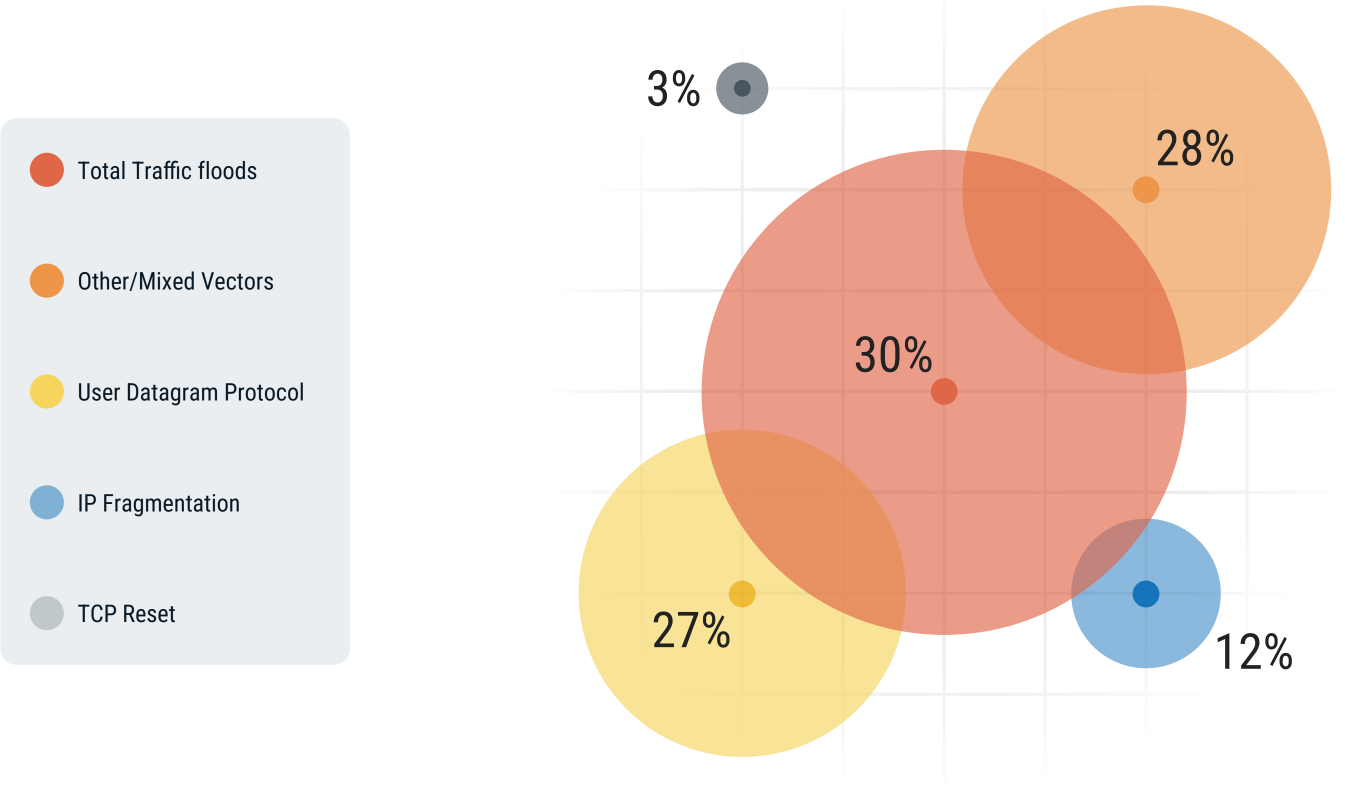
Industry targeting followed predictable patterns, but higher education saw a notable surge. While financial and web services remained prime targets, September saw a sharp rise in attacks on universities and academic networks during peak enrollment periods. Adversaries exploited open campus infrastructures and seasonal online activity, making education one of the fastest-growing targets for large-scale DDoS campaigns.

Top Targets of DDoS Attacks in Q3 2025

The United States absorbed over half of all attacks around the world

58%	United States
11%	Saudi Arabia
11%	United Kingdom
7%	Switzerland, Gibraltar, Austria
7%	Sri Lanka, Indonesia
6%	Australia, India, Vietnam, Germany, France, Spain

How Cybercriminals Attacked in Q3 2025



Protecting Your Organization

Prepare for Subnet-wide Floods

Carpet-bombing expands the attack surface to entire IP ranges. Organizations should confirm that their mitigation strategies extend beyond single hosts.

DigiCert's UltraDDoS Protect includes subnet-aware filtering to counter this tactic.

Treat Tsunami-class Events as Standard Risk

Build continuity and incident response assumptions on this baseline.

DigiCert provides >15 Tbps of global mitigation capacity across 16 PoPs to absorb record floods.

Expect Blended Vectors

UDP floods are increasingly combined with DNS amplification and fragmentation.

Customers should enable DigiCert's advanced telemetry, automated alerting, and trained SOC operators to catch these hybrid campaigns early.

Web Application Firewall (WAF)

The web threat landscape in the third quarter of 2025 was defined by precision, automation, and persistence. Total web requests declined from about 1.1 trillion in July to 980 million by September, yet malicious activity grew sharply over the same period—from 51 percent to 73 percent—showing that attackers are focusing on high-value targets rather than broad, opportunistic campaigns.

Automated traffic continued to rise, with total bot violations reaching 32 million in September—the highest of the quarter. This shows a growing reliance on automation for reconnaissance, credential testing, and exploit delivery, confirming that bots now underpin most large-scale attacks.

> With 32 million bot violations in September alone, Q3 confirmed what many suspected—automation now powers the majority of large-scale cyberattacks.

Live traffic to customer websites and our honeypot network revealed a large amount of vulnerability scanning from cloud provider infrastructure. Attackers used FreeMarker template injection, Log4Shell-style JNDI exploits, and webshell installation attempts, demonstrating a sustained focus on persistence and lateral movement rather than single-point disruption.

Throughout the quarter, travel and hospitality remained the most targeted sector at 81% by September, followed by financial services at 12% and retail at 6%. These industries' dependence on uptime and customer data keeps them among the most lucrative for attackers, with seasonal patterns aligning closely to global travel and consumer activity.

Protecting Your Organization

Use Sector-specific Protection

Enable and regularly review UltraWAF's advanced, CVE-specific protection profiles to ensure detection logic is aligned with your application stack and traffic behavior.

Block Bad Automation

Turn on bot-mitigation controls, such as IP reputation and bot signatures, to stop credentials and scanning bots early.

Patch Legacy Paths Fast

Use UltraWAF's virtual patching to block these vulnerabilities in real time while permanent code or configuration fixes are implemented.

Watch for Anomalies

Set alerts for spikes in HTTP requests to detect attacks early, enabling faster incident response and limiting attacker dwell time.

Conclusion

The third quarter of 2025 marked a turning point in how attackers operate.

Threats are evolving faster than the defenses meant to stop them, combining automation, precision, and scale to exploit weaknesses across every layer of digital infrastructure.

The result: a threat landscape where volume matters less than adaptability and coordination.

Across DigiCert's platform, this pattern was easy to see. DDoS campaigns blended precision strikes with large-scale floods. Web exploitation became more automated and persistent, driven by legacy vulnerabilities and credential abuse. DNS remained stable but showed how small anomalies can ripple globally through interconnected systems.

For security leaders, the lesson is clear:
Attacks no longer happen in isolation. They move across infrastructure, application, and service layers, testing the seams that connect to modern ecosystems. Defending against them requires coordinated visibility, decisive response, and scalable resilience.

Key Recommendations:

Unify Defenses Across Layers
Build shared visibility between network, application, and DNS teams to close detection gaps and speed up response.

Use Data for Faster Decisions
Integrate telemetry from security controls into a single view, so analysts can act on anomalies in minutes, not hours.

Plan for Scale and Persistence
Assume 1-terabit-plus DDoS floods and continuous automation are the norm; validate mitigation capacity and incident playbooks regularly.

Digital trust has become the benchmark of resilience. As the threat landscape continues to evolve, security leaders must act now to strengthen visibility, build integrated defenses, and partner with providers that can deliver the scale and intelligence needed to stay ahead.

FAQ

What is carpet bombing?

A carpet-bombing attack floods entire network subnets instead of targeting one server or IP address. By distributing attack traffic across many hosts, adversaries make it harder for defenses to onboard target IP addresses, sample traffic, and mitigate the attack, causing widespread service disruption.

What is an ‘internet tsunami’?

An internet tsunami is a massive DDoS attack exceeding 1 Tbps—a rare, fast-moving event that can overwhelm both the targeted organization and service provider networks. Like a real tsunami, it hits with minimal warning and demands specialized, high-capacity defenses to stay online.

What is a FormErr anomaly?

Short for “format error,” FormErr refers to a specific DNS error that occurs when a DNS server receives a malformed or invalid DNS query message. It’s a response returned by a DNS server when the query it received does not conform to proper DNS protocol, indicating a misconfiguration, software bug, malicious activity, or probing.

What is NXDOMAIN traffic?

NXDOMAIN traffic comes from DNS lookups for domains that don’t exist. While often caused by typos or misconfigurations, spikes in NXDOMAIN queries can also indicate DNS water torture DDoS attacks, automated scanning, or enumeration by attackers probing for hostnames.

What does “total bot violations” mean?

A bot violation occurs when the Web Application Firewall (WAF) detects and blocks automated, non-human traffic that violates access rules, such as vulnerability scanning, credential stuffing, content theft, scraping, spam posting, or API abuse. It essentially measures malicious, or unwanted, automation rather than human-driven attacks

About DigiCert

DigiCert is the world’s leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit digicert.com or follow @digicert.