corero

[NETWORK SECURITY]

2025 THREAT INTELLIGENCE REPORT

Foreword from the CTO

Ashley Stephenson
Chief Technology and Product Officer
Corero Network Security

Each year, the data tells a story. Not just about what attackers are doing, but about what they're willing to bet on. In 2024, they bet on speed, automation, and access. And why wouldn't they? The tools are inexpensive. The infrastructure is everywhere. The barriers are low. What used to require sophisticated coordination can now be increasingly accomplished with a few dollars, a rented botnet, and some recycled or AI-replicated malware code.

We at Corero have been tracking DDoS trends for years. And while some of the trends feel familiar—fast, short attacks still dominate—there's nuance that demands attention. The frequency is up. The volume is climbing again. The middle of the attack spectrum is thinning out. What's left is a blend of opportunistic pressure and strategic brute force, fueled by automation and constant adaptation.

And just as attackers are evolving, so is the architecture they target. With the rise of hybrid-cloud environments and a shift toward repatriating critical workloads to on-prem infrastructure, the complexity of defense is growing. Traffic paths are less predictable. Enforcement points are more distributed. And for many organizations, that means more blind spots or effectively "open" doors.

This year's report reflects not just what we see in the data, but what we're preparing for. Threat actors are no longer limited by bandwidth or geography. They're building smarter infrastructure, continuously repurposing compromised devices, and increasingly targeting the application layer. As defenders, we need to match that adaptability with visibility, automation, and speed.

This complexity is showing up as new challenges to defender response. According to a study from Merrill Research, many teams report difficulty coordinating across environments, keeping pace with threats, and executing rapid mitigations. The challenge isn't just the volume of attacks—it's the operational friction that slows defense.

Our mission at Corero is to give organizations the power to see, stop, and evolve faster than the threats they face. That mission has never been more urgent.

Thank you for reading, and for being part of the community that defends what matters.

Executive Summary

In 2024, DDoS attackers didn't reinvent their playbook—they perfected it. The data tells a story of relentless, high-frequency attacks carried out with startling efficiency and scale. Fast, short, sub-10Gbps attacks continued to dominate, as they have for years, underscoring a persistent and evolving threat model where disruption is cheap, accessible, and alarmingly effective.

Our analysis of customer traffic patterns shows that organizations we monitored faced an average of 11 DDoS attacks per day in 2024—a 5% increase from the previous year. The majority of these attacks were under 1Gbps in size, capable of slipping under traditional volumetric thresholds while still disrupting availability and performance. These findings reinforce a trend we've observed year over year: frequency is the attacker's weapon of choice.

While small attacks dominate, larger-scale assaults are surging. Attacks exceeding 10Gbps rose to 2.9% of all observed events—the highest since 2018. We believe this reflects an increase in botnet capacity and automation, driven by exploitation of vulnerable devices such as MikroTik routers and derivatives of the Mirai malware running on IoT types of devices.

At the same time, mid-sized attacks—between 5Gbps to 10Gbps—continue to decline, dropping from 19% in 2019 to just 12.4% in 2024. The "middle tier" of DDoS is fading as attackers polarize: many use ubiquitous, low-volume probing to test defenses, while others unleash strategic high-volume campaigns to overwhelm specifically targeted infrastructure.

Quarterly analysis reveals consistent seasonality. Q3 and Q4 remain peak periods for attack activity, aligning with high-traffic business seasons and potentially overloaded staffing windows. Interestingly, Q2 2024 saw fewer attacks overall, but a higher proportion of large attacks—a possible signal of reconnaissance or staged testing ahead of larger campaigns.

Application-layer (Layer 7) attacks are also rising across the industry. HTTP floods, API targeting, and platform-specific DDoS campaigns are becoming more common as attackers seek disruption beyond simple bandwidth saturation. As application defenses become the next front line, organizations must be prepared to defend not just the network, but the business logic itself.

The takeaway is clear:

DDoS is now becoming a state of constant background pressure. Attackers rely on automation, affordability, and infrastructure-scale distribution to keep victims in a reactive “whack-a-mole” posture. What has always worked still works. Until defenders catch up in speed, visibility, and automation, DDoS will remain one of the most effective and persistent tools in the attacker's arsenal.

DDoS is easy. DDoS defense still isn't.

Reading Between the Packets

Each attack leaves a trace. In 2024, our global telemetry captured hundreds of thousands of these traces—patterns in frequency, volume, timing, and tactics—captured from real attacks targeting live production networks.

This section isn't just a record of what happened. We've looked not only at 2024, but at multiple years of historical data to surface patterns, shifts, and persistent strategies that shape the threat landscape. It's an interpretation of what those patterns mean for defenders. Because behind every data point is a decision: by an attacker, by a defender, or by a system forced to choose what to block and what to allow.

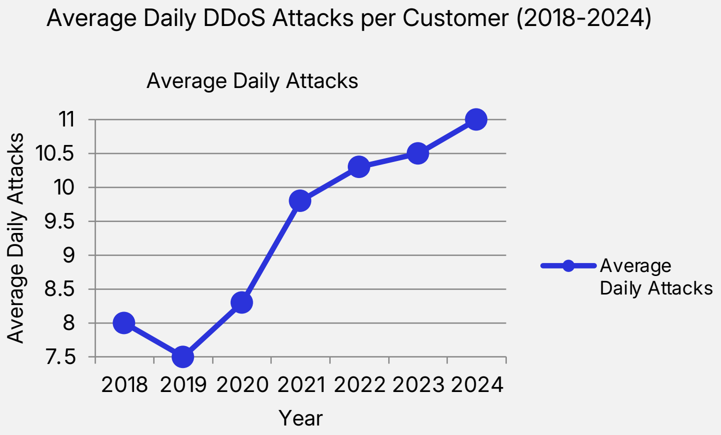
In the pages that follow, we break down the trends that we believe defined 2024: what the data says, why it matters, and what defenders can do in response. This is where the numbers meet the real world—and where real strategy begins.

Let's look at what the attackers left behind.

The Pulse of Pressure:
Daily DDoS Attack Frequency

WHAT THE DATA SAYS

In 2024, Corero customers experienced an average of 11 DDoS attacks per day, up from 10.48 in 2023. That's a 5% increase year over year, and part of a broader multi-year trend. Since 2018, the daily average has climbed steadily from around 8 to typically 11 attacks per customer per day—a 37.5% increase over six years.



WHAT IT MEANS

This isn't a spike—it's a strategy. The frequency of attacks is not random; it's deliberate. As the number of attackers increase, so does the continuous background pressure, using automation and lower-cost infrastructure weaponization to keep defenses active, overwhelmed, or desensitized.

Many of these high-frequency attacks are short-lived and sub-saturating, making them easy to dismiss as background noise. But they serve key purposes:

- Probing for weaknesses
- Measuring mitigation thresholds
- Timing response delays
- Distracting security teams from more targeted activities

Put simply:

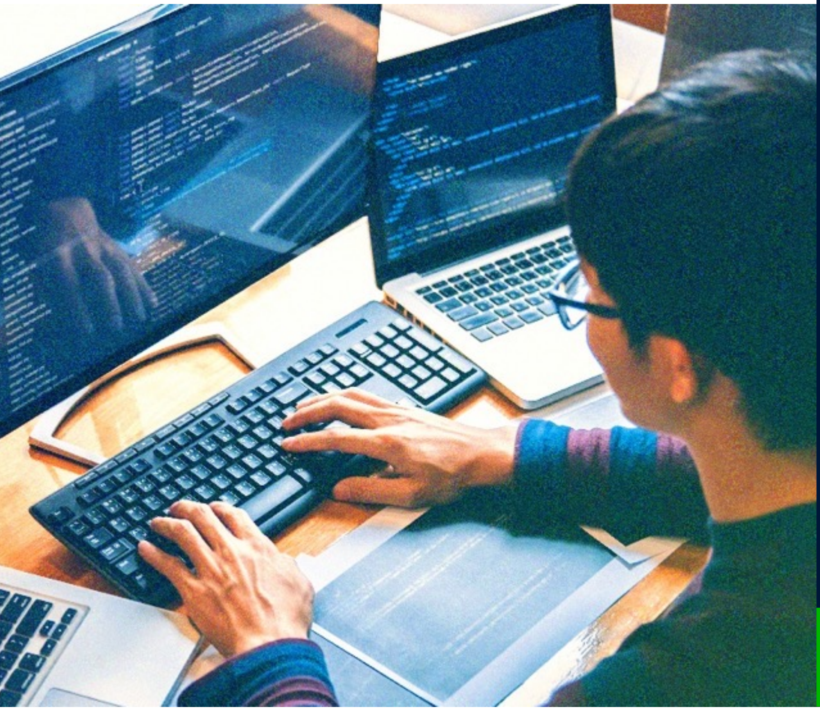
If you're defending 11 attacks per day, you're not responding to an anomaly—you're operating in a live-fire environment.

The Pulse of Pressure

WHAT YOU CAN DO

Organizations must treat frequent attacks as a default condition, not an exception. Key actions include:

- Automate response workflows to detect and mitigate without human intervention.
- Improve detection sensitivity to identify short-duration, sub-threshold anomalies.
- Establish a better understanding of normal traffic behavior, so you can identify deviations more accurately.
- Harden edge infrastructure to absorb or deflect high-frequency, low-volume attacks without consuming valuable internal resources.



Is it a Blip or a DDoS Attack?

How do you know you're under attack when the indicators look like noise?

That’s exactly the problem. Most of the attacks we observe—especially those under 1Gbps—don’t necessarily cause obvious outages. They do create latency, packet loss, or transient disruptions that look like any number of common network issues. Many organizations write them off as ISP glitches or normal internet weather.

But here’s what distinguishes these events as attacks:

1. They follow patterns: perhaps time of day, similar protocol characteristics, same source regions.
2. They coincide with broader scanning, probing, or increasing credential stuffing campaigns.
3. They disappear or move on quickly when defenses engage—anomalous behavior for real outages.
4. They return again and again, often with a different signature.

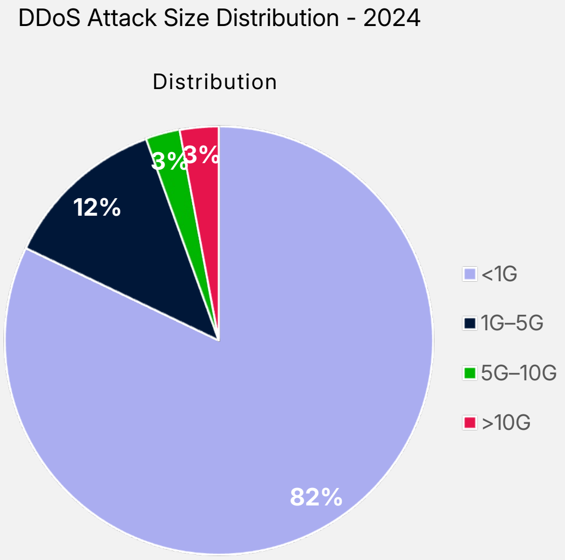
If you see a pattern of short-duration, seemingly minor disruptions, you might not be dealing with unreliable infrastructure.

You might be dealing with an attacker testing your limits.

Under the Radar, Over the Line:
The Persistence of Sub-10Gbps Attacks

WHAT THE DATA SAYS

More than 82% of all DDoS attacks observed in 2024 were under just 1Gbps in size. These small-scale attacks are by far the most common type seen in the wild. Often dismissed as background noise, they persist because they're easier to launch, harder to detect, and effective at degrading overall service quality or testing the limits of a defense.


DDoS Attack Size Distribution - 2024

WHAT IT MEANS

Small attacks don't mean small impact. These sub-10Gbps campaigns can still knock over fragile application services, exhaust firewalls, or trigger unnecessary and costly scaling operations in cloud environments. They're efficient—and in many cases, ominous precursors to larger campaigns. It's also important to note that these numbers do not necessarily represent discrete attacks and there are, assuredly, instances where an attacker may have launched several small attacks that aggregate to a larger total attack.

Defenders often miss these attacks not because they are inherently stealthy, but because they operate in a poorly policed detection gray zone. They would trip broad volumetric alarms or cause immediately identifiable outages. Instead, they tread lightly, producing faint footprints: delayed page loads, intermittent 5xx errors, or momentary DNS hiccups or failures. These effects are easily missed as random internet noise—but taken in context, they often indicate coordinated probing or deliberate degradation.

The implication for defenders is clear: these are not background artifacts—there are valid signals of potentially more disruptive attacks. And the best way to surface them is through behavioral monitoring and correlation across time and systems. This is where operational visibility, not just raw bandwidth defense, becomes critical.

Under the Radar, Over the Line

WHAT YOU CAN DO

- Look for performance anomalies—like latency spikes or unexplained service flaps—as early indicators.
- Correlate events across your environment to spot multi-pronged, low-volume campaigns.
- Tune alert thresholds to better capture small, persistent disruptions that evade volumetric triggers.

Test or Target?

Small attacks aren't necessarily failed big ones. Many are probes. Some are designed to test detection thresholds. Others target specific applications with just enough pressure to cause instability. Knowing the difference—test vs. target—requires context. And context comes from visibility, telemetry, and investigation.

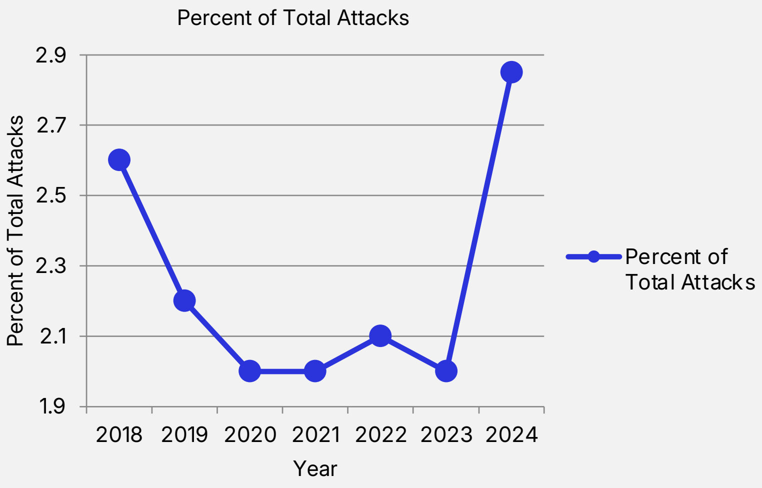
The Return of More Powerful Botnets:
Rise in >10Gbps Attacks

WHAT THE DATA SAYS

In 2024, 2.9% of all observed DDoS attacks exceeded 10Gbps in size. This is the highest share of large-scale attacks since 2018, following several years of relatively flat trends in these activities.

While these events remain rare compared to the dominant sub-1Gbps category, their potential for disruption is outsized, often targeting infrastructure chokepoints, downstream capacity limits, or service-level agreements.

Growth of >10Gbps DDoS Attacks (2018-2024)



WHAT IT MEANS

This growth signals that botnet firepower is increasing again—and that attackers are either gaining access to more devices or better orchestrating the ones they already control.

Contributing factors likely include:

- Exploitation of vulnerable routers and IoT devices, such as MikroTik hardware
- Continued evolution and resurgence of Mirai-based malware
- Growing use of DDoS-for-hire services with multi-vector attack capabilities

These larger attacks are often:

- Used as smokescreens for data exfiltration or lateral movement
- Timed to maximize operational disruption (e.g., peak hours or during incidents)
- Paired with ransom demands, threatening repeat or sustained attacks

The Return of More Powerful Botnets

WHAT YOU CAN DO

- Know your capacity limits. What your ISP can absorb ≠ what your infrastructure can tolerate.
- Work with upstream providers to understand attack redirection, scrubbing, and failover options.
- Test your mitigation response to simulated larger-scale events (not just volumetric, but multi-vector).
- Don't assume rarity equals safety. These attacks may be fewer, but their impact—on revenue, operations, and reputation—can be severe.

Why Bigger Isn't Always Louder

Large-scale attacks make headlines, but they're not always designed to break the internet. Some are used as smokescreens, masking more subtle intrusions. Others are timed to cause maximum operational stress—at shift changes, during peak hours, or in tandem with ransomware demands.

What makes these attacks dangerous isn't just their bandwidth. It's their pattern of targeting, timing, and the disruption they create beyond the network—from alert fatigue to executive panic.

Don't mistake rarity for irrelevance. Large attacks are strategic weapons, and they're back in the arsenal.

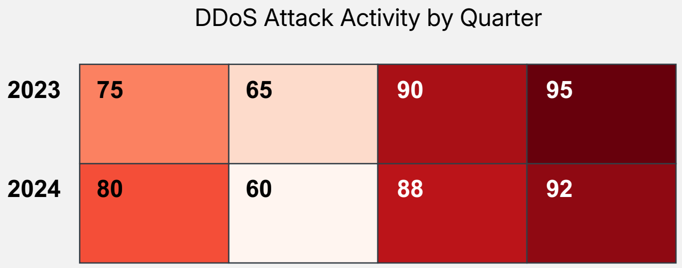
When the Storms Come:
DDoS Seasonality and Strategic Timing

WHAT THE DATA SAYS

Across 2023 and 2024, Corero observed recurring spikes in attack volume during Q3 and Q4. In both years:

- Q3 saw a rise in total attack frequency, particularly sub-1Gbps bursts.
- Q4 followed with a broader mix of attack sizes, including a higher concentration of >1Gbps events.

By contrast, Q2 2024 saw a dip in frequency but a higher share of large-scale attacks, including >10Gbps events.



WHAT IT MEANS

Attackers don't operate in a vacuum—they respond to business rhythms, calendar events, and operational pressure points.

Key seasonal patterns may include:

Q3 Back-to-school and pre-holiday ramp-ups (targeting gaming, retail, education)

Q4 Holiday season and IT change freezes, which often coincide with reduced staffing and delayed response windows

These trends suggests that attack timing is becoming more strategic, aligning with moments when disruption hurts most.

When the Storms Come

WHAT YOU CAN DO

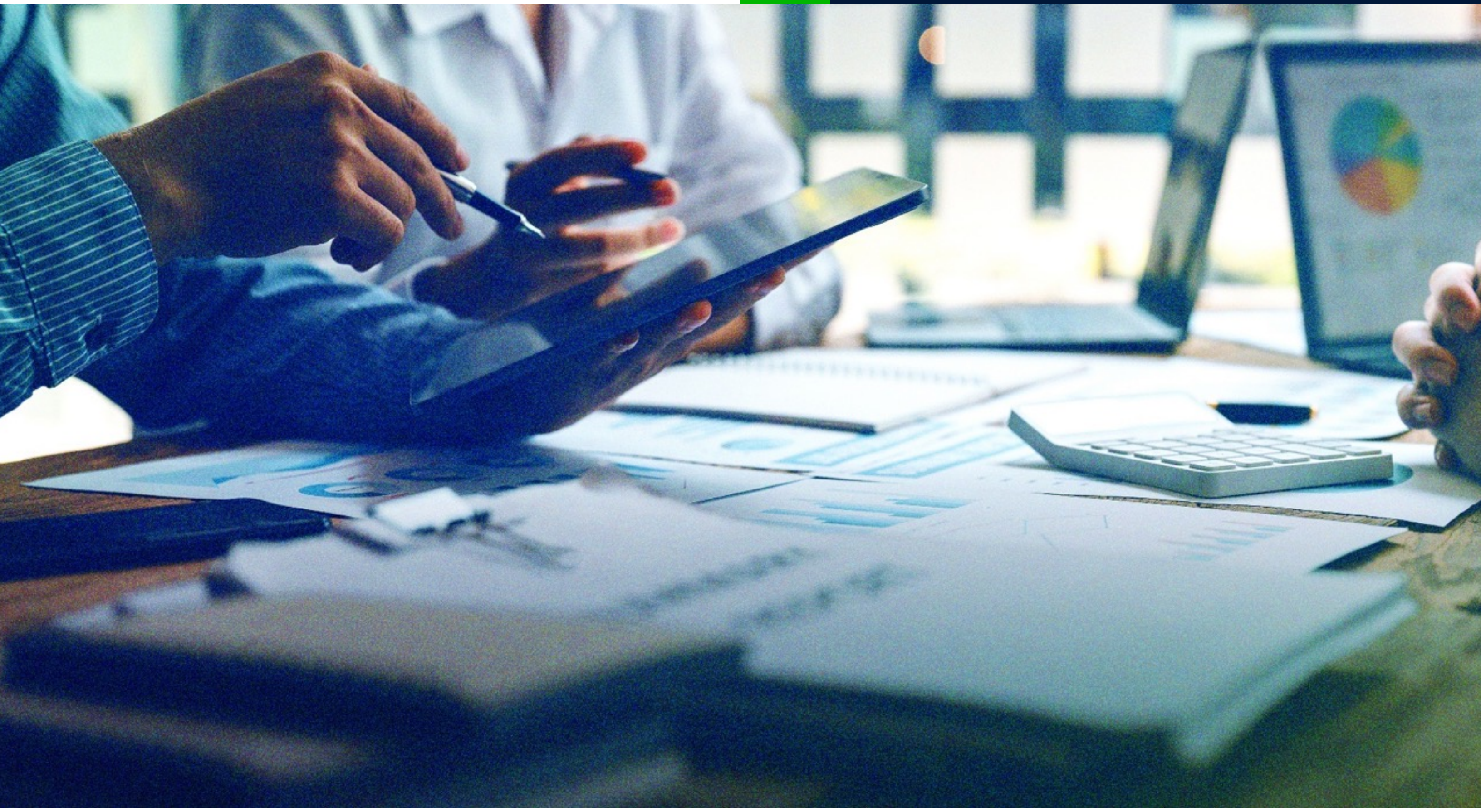
- Staff your defenses with seasonality in mind. Plan for increased activity during late Q3 and Q4.
- Use low-volume periods like Q1 and Q2 to harden your infrastructure and test mitigation workflows.
- Align red team/blue team exercises with known DDoS peaks to ensure coverage and confidence.
- Don’t rely on average trends alone—look at historical seasonality to forecast pressure windows.

When Defenders Blink

Q4 is a favorite season for attackers—not because it’s cold, but because security teams are stretched thin. Budgets are frozen. Staff are out on holiday PTO. And change windows are limited by business risk tolerance.

Attackers know this. They exploit timing as much as tools, launching DDoS campaigns when response time is slowest and tolerance for disruption is lowest.

If your defenses depend on people being present, rested, and ready, then seasonality isn’t just a pattern—it’s an opportunity for the adversary.



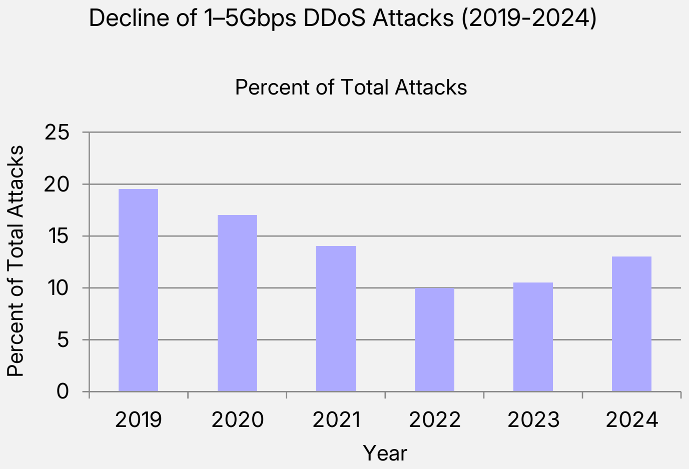
The Mysterious Middle:
The Decline of 1–5Gbps Attacks

WHAT THE DATA SAYS

In 2019, attacks in the 1–5Gbps range made up nearly 19.4% of all observed DDoS events. By 2024, that number had dropped to just 12.4%—a 34% reduction in share over five years.

While there have been some year-to-year fluctuations, the longer-term trend for this tier has been downward—declining from 19.4% in 2019 to 12.8% in 2024.

Perhaps it is just being outstripped by the growth in flanking attacks.



WHAT IT MEANS

This trend signals a strategic polarization in attacker behavior, but why still remains speculative. Here's our take:

Many attackers are opting for low-volume, high-frequency attacks that avoid detection and test response.

Others may be investing in large-scale, high-impact floods enabled by botnets and pay-to-play infrastructure.

Is the middle tier becoming obsolete because it's ineffective or no longer efficient?

The 1–5Gbps range:

- Is too small to crash modern infrastructure outright
- But too large to go unnoticed
- And less cost-effective than the alternatives

The shift away from the middle may reflect how defenders have evolved. Our view is that the 1–5Gbps range used to be a blind spot for many providers—big enough to hurt, small enough to sneak through. But as DDoS protection matured, that window narrowed. Attackers noticed. Today, they're not wasting bandwidth where it's likely to get flagged and filtered. They go big to overwhelm—or small to slip under the radar.

For defenders, the net is recalibrating expectations. If your detection and response posture is still weighted toward catching mid-tier floods, you may be over-resourced for what's no longer common—and under-prepared for where the edge cases live.

The Mysterious Middle

WHAT YOU CAN DO

Watch the edges, not just the middle. Detection logic should focus on burst patterns and anomalies, not just fixed thresholds.

Evaluate your defensive posture at both ends of the spectrum—can you handle thousands of small bursts? Can you absorb a 20Gbps hit?

Test mitigation tuning to avoid overspending resources on attacks that are no longer prevalent—but don't remove coverage entirely.

The DDoS Middle Tier is Disappearing

The DDoS "middle tier" is shrinking as a percentage of all attacks. These attacks once represented a strategic balance—big enough to impact performance, small enough to avoid immediate detection.

We believe attackers are optimizing for ROI. Sub-1Gbps attacks are cheaper and more surgical. >10Gbps floods are more dramatic and disruptive. The 1–5Gbps range? It's increasingly left behind.

This could be a sign of how attacker efficiency shapes the entire threat landscape.

Attacks Are Evolving:
Smarter, More Adaptive DDoS Campaigns

WHAT THE DATA SAYS

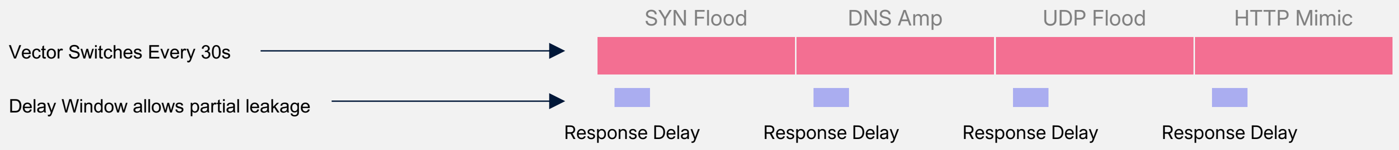
We observed a growing pattern of multi-vector, sequential, and evasive DDoS campaigns throughout 2024. While volume alone is no longer the defining factor, attacker behavior is becoming more sophisticated. In many cases, attackers launched coordinated attacks targeting different subnets either simultaneously or in rapid succession, often combining multiple vectors in short bursts. These campaigns are not only harder to detect but also aim to exploit delay gaps in detection and mitigation systems.

This behavior includes:

- Rapid vector switching (e.g., alternating between SYN floods, DNS amplification, and HTTP mimics)
- Testing defenses by probing for weak points, then modifying tactics
- Launching high-volume attacks with microbursts to circumvent static thresholds

In several observed campaigns, attackers employed what we describe here as “chained vectors”: tightly sequenced attacks that rapidly shift between protocols every 30–60 seconds. While each vector on its own may be manageable, the timing and coordination are designed to exploit even brief lags in detection or mitigation—keeping defenses reactive rather than responsive.

Chained Vector Timing and Response Gaps



WHAT IT MEANS

This evolution indicates that attackers are no longer just aiming for disruption; they’re trying to outmaneuver automation. The shift from brute force to strategic adaptability challenges even the most responsive mitigation frameworks.

Traditional defenses are often built to detect volume, not velocity. Each time an attacker switches tactics—say from opening fake TCP connections to triggering DNS amplification or launching UDP floods—the defense has to pause, reassess, and reclassify. That cycle, however short, creates repeated blind spots.

We have observed campaigns in the wild that rotate vectors just as mitigation activates, creating a churn effect that leaves SOC teams chasing the tail of the attack. This isn’t noise. It’s design.

The ability to detect intent—not just packets—is becoming essential.

Attacks Are Evolving

WHAT YOU CAN DO

Hunt for short-term patterns: Use your telemetry to identify rapid shifts in protocol type, port targeting, or packet size. These changes—especially if occurring every 30–60 seconds—can indicate chained vector behavior.

Tag and flag anomalies in real time: Develop lightweight rules or scripts that tag new traffic profiles as they emerge. This helps create fast feedback loops for your SOC, even before full detection cycles complete.

Build SOC playbooks around attacker behavior: Use known chaining patterns to inform your escalation workflows. Set expectations internally around what 'normal' response cadence looks like—and what might signal something more coordinated.

Why Vector Switching Works

In today's mitigation environments, time is everything. Most DDoS defenses rely on detection signatures, rate thresholds, and pattern recognition that take time to activate. Even advanced platforms may take 10–30 seconds, or longer, to analyze traffic and begin mitigation.

Attackers exploit this. By switching vectors every 30–60 seconds, they:

- Evade persistent filtering
- Confuse analytics tools tuned to specific attack types
- Force defenses to restart mitigation cycles

The result: leakage, resource exhaustion, and SOC fatigue.

It's not about overwhelming defenses—it's about staying one step ahead.

Application-Layer Attacks: DDoS is Rising

WHAT THE DATA SAYS

Our observations consistently indicate a rise in application-layer (Layer 7) attacks. These attacks are typically:

- Smaller in bandwidth
- Harder to detect due to encryption
- Targeting APIs, login portals, shopping carts, search functions, and other resource-intensive endpoints

We've seen signs—both internally and across the industry—that application disruptions are increasingly being traced back to lower-volume attacks not visible in traditional volumetric data. Attackers are also using L3/L4 probes as reconnaissance for follow-up L7 attacks, further blurring the line between network and application threat surfaces.

Comparing L3/L4 vs. L7 DDoS Attacks

	Target	Attack Type	Detection Challenge	Impact Focus
L3/L4 DDoS	Network Infrastructure	Volumetric Floods	Packet rate & Volume	Bandwidth Saturation
L7 DDoS	Application & APIs	Mimic Legitimate Users	Behavioral/ **Pattern-Based**	Service Degradation

WHAT IT MEANS

Application-layer DDoS isn't about flooding the pipe—it's about breaking the app.

These attacks often:

Mimic legitimate user traffic (e.g., HTTPS GET/POST requests)

Exploit resource exhaustion (CPU/memory/money) rather than bandwidth

Operate under the radar of traditional volumetric detection tools

The move toward L7 reflects a broader evolution: DDoS isn't just infrastructure-centric anymore. It's business-centric. Application attackers are aiming to surgically take down what matters most—customer experience, transaction flow, or authentication.

This trend also underscores the rise of platform-aware adversaries, who know how to exploit victim specific architectures, cloud workloads, or web app logic.

Application-Layer Attacks

WHAT YOU CAN DO

Start monitoring application-layer health alongside network traffic. Unusual load times, 5xx errors, or login failures could signal DDoS.

Integrate L7 defense capabilities into your broader DDoS mitigation stack—even if they're still in early phases.

Collaborate with app dev and platform teams, not just network ops, to develop coordinated response strategies.

Consider user-behavior modeling and rate-limiting strategies to detect high-rate, lower-volume signature abuse.

When 'Normal' Traffic Becomes an Attack

Application-layer DDoS is difficult to spot because it often mimics real users. A login flood may look like a busy Monday. A shopping cart attack may look like Black Friday traffic.

The difference is in intent—and pattern. L7 attacks are typically:

- Highly repetitive
- Spread across rotating IPs
- Designed to waste application rather than network resources

Defending against this requires behavioral analysis and application awareness—not just packet filtering.

Defenders Are Still Playing Catch-Up

WHAT THE DATA SAYS

Defenders face mounting challenges in catching up as DDoS attack patterns have grown more automated, adaptive, and evasive. According to research commissioned by Corero and conducted by Merrill Research, a significant share of organizations report:

- Difficulty coordinating across security, network, and platform teams
- Inability to maintain clear visibility into all traffic paths (especially in hybrid and multi-cloud environments)
- Delays in detection-to-mitigation workflows
- Shortage of skilled personnel to manage and tune security defenses

This mirrors what we see in the field: defenders are not failing because of tools—they're struggling because of diversity, complexity, and the pace of change.

WHAT IT MEANS

Defensive posture is increasingly distributed. Cloud adoption has outpaced visibility. The line between application, infrastructure, and security teams has blurred. And traditional playbooks assume a level of control that most organizations no longer have.

Even the best mitigation systems are only as good as:

The signals they receive

The automation they can execute

The clarity of ownership behind them

This isn't just a tech gap. It's an operational gap.

Defenders Are Still Playing Catch-Up

WHAT YOU CAN DO

- Conduct a DDoS readiness audit—across people, process, and tooling
- Clarify ownership of response: who triages, who acts, who tunes?
- Build playbooks that reflect your actual infrastructure—including hybrid, CDN, and cloud layers
- Invest in automation, but don't assume it's plug-and-play—it needs visibility and tuning
- Make DDoS tabletop exercises a regular event across security and ops

DDoS Response is a Team Sport

DDoS response doesn't live in one team anymore. It touches network ops, app teams, cloud architects, and SOC analysts. Yet many organizations still treat it like a siloed discipline.

To be effective, mitigation must be:

- Cross-functional
- Pre-authorized
- Continuously exercised

Your best defense may not be the fanciest tool—it's the people who know when and how to use it.

It’s Not the Platform. It’s the Pressure.

So far, we’ve focused on attacker behavior and technical trends. But at the center of every one of these insights is a team—a human team—tasked with defending against them.

That’s why we commissioned Merrill Research to go deeper. We wanted to understand not just the threats, but how they’re experienced by practitioners: the security and network professionals who live the response, the stress, and the reality of defending under pressure.

These findings reflect input from both Corero customers and non-customers alike. The goal was simple: understand what’s working, what’s not, and what defenders actually need.

DDoS defense isn’t a question of whether technology works. It’s a question of whether teams can work with it—across functions, in real time, and under pressure.

Merrill Research surfaced a consistent pattern: the challenges defenders face aren’t about capability, they’re about coordination. Even with solid tools in place, many teams still struggle to align across platforms, roles, and workflows.

Key themes that emerged:

- Difficulty demonstrating the value of DDoS protection to business stakeholders
- Limited coordination among cloud, network, and application teams
- Gaps in tuning, playbooks, and integrated response strategies
- Uncertainty around ownership and communication during active threats

The “so what” is this: resilience doesn’t come from tools alone. It comes from alignment.

When teams can see clearly, act decisively, and communicate confidently, they don’t just react faster—they recover stronger.

Vendors have a responsibility to reduce the operational burden they place on their customers—with products that integrate easily into existing architectures, workflows, and tooling ecosystems, and that can themselves be integrated into. Good tech should adapt to the way teams already operate—not the other way around.

What Defenders Told Us

68%

say demonstrating the ROI of DDoS protection to leadership is a challenge.

51%

cite lack of cross-team coordination as a key vulnerability.

47%

report difficulty adapting existing tools to hybrid environments.

And more than half say they aren’t confident in their ability to mitigate advanced attacks without vendor guidance.

Conclusion: Seeing the Signal in the Noise

The DDoS threat landscape in 2024 wasn’t marked by chaos. It was marked by clarity—for those who knew where to look.

Short, sub-saturating attacks continued to dominate the landscape, more frequent than ever and tactically efficient. At the other end of the spectrum, large-scale attacks gained new momentum, aided by modern botnets and commodity toolkits. And in between, a noticeable decline in mid-sized attacks told us something else: attackers are optimizing.

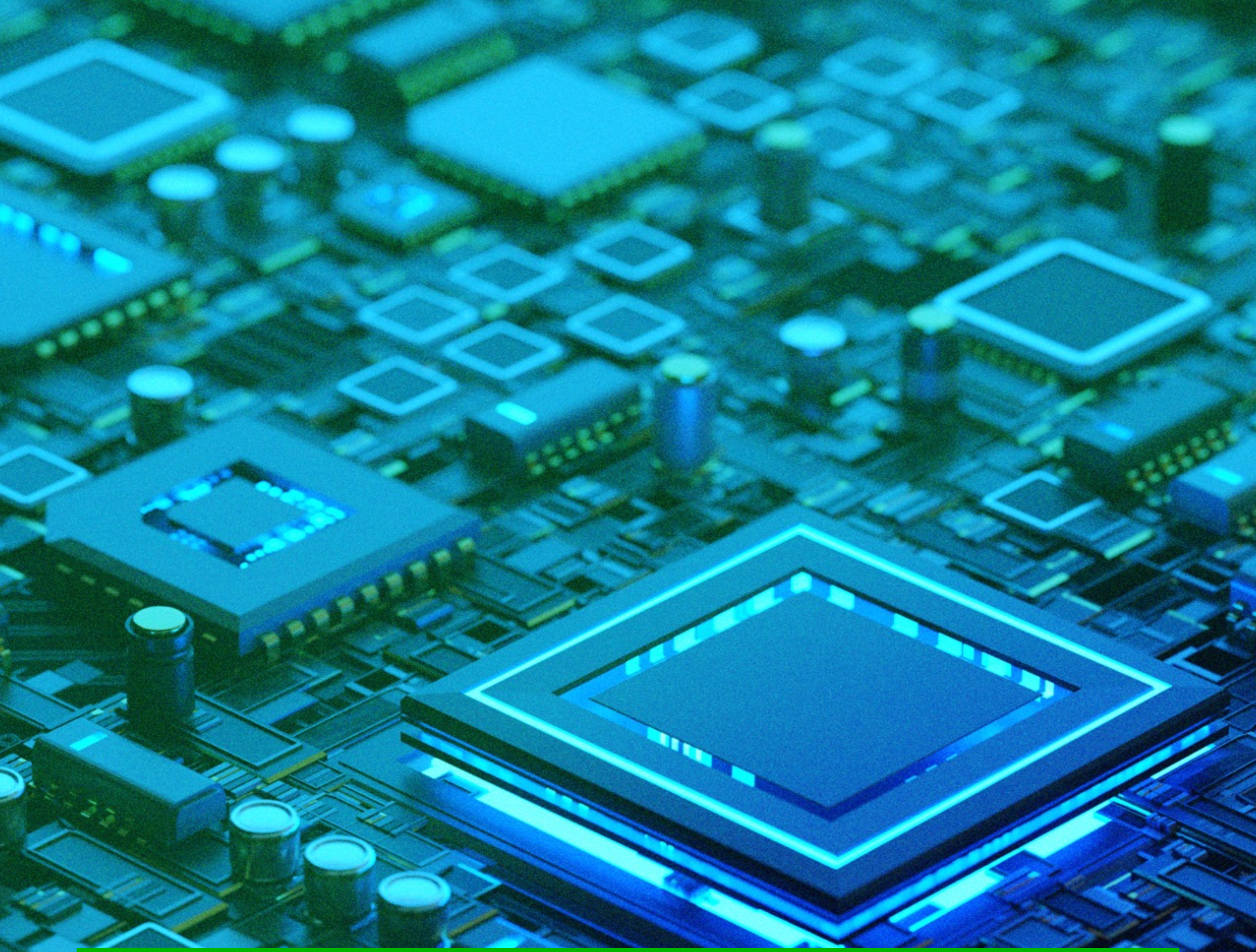
They’re choosing their moments. Their methods. Their targets.

But the technical trends only tell part of the story. As the data evolved, so did the experience of defending against it. Merrill Research surfaced what many already feel: the challenge isn’t always about capability. It’s about alignment. Visibility. Confidence. And being ready when the attack is real, but not yet obvious.

Defending against modern DDoS campaigns requires more than faster mitigation or smarter filters. It requires integration—of tools, of people, of strategies. The strongest posture isn’t built from a single platform. It’s built from coordination, clarity, and support that matches the speed of the threat.

DDoS is easy. Defense still isn’t. But when defenders are aligned, informed, and empowered—that’s when the advantage starts to shift.

The signal is there. **And so is the solution.**



corero
[NETWORK SECURITY]

ABOUT CORERO NETWORK SECURITY

Corero Network Security is a leading provider of distributed denial of service (DDoS) protection solutions. We are specialists in automatic detection and protection solutions, that include network visibility, analytics, and reporting tools. Corero's technology provides scalable protection capabilities against both external DDoS attackers and internal DDoS threats, in even the most complex edge and subscriber environments, ensuring internet service availability and uptime. Corero's key operational centers are in Marlborough, Massachusetts, USA, and Edinburgh, UK, with the Company's headquarters in London, UK. The Company is listed on the London Stock Exchange's AIM market under the ticker CNS.

For more information, visit www.corero.com, and follow us on LinkedIn and Twitter.