corero [NETWORK SECURITY]

2026 THREAT INTELLIGENCE REPORT

The year every record became the new normal.

A NOTE FROM THE SOC

Teressa Carlin

Threat Research Team (TRT),
Corero Network Security

I've been watching DDoS attack data for a long time and you develop a feel for what is normal and for what is a temporary spike that'll settle back down, but 2025 didn't settle.

By mid-year, the team stopped comparing what we were seeing to prior months and started comparing it to what we thought was possible. Attack sizes that would have triggered all-hands alerts in 2024 were happening with enough regularity that we had to recalibrate what "normal" looked like. That happened more than once. The baseline kept moving.

Two things stood out to me more than anything else. The first is speed. We tracked pulse attacks that hit at terabit scale and were over in six seconds. That's not a window most mitigation architectures were designed for and it forces an uncomfortable conversation about assumptions the industry has been operating on for years. The second is the emerging trend in Botnets such as Aisuru. We've watched botnets come and go, and we've tracked Mirai and its variants for years. Aisuru was a different animal. The growth rate, the vulnerabilities driving it and the ability to run bandwidth and packet-rate attacks simultaneously.

This report is based on the data we collected and analyzed and is a true reflection of what we have lived with for the past year. I hope it's useful to you and your team, and I hope it starts some honest conversations about what's actually required to keep up with where this is heading.

BY THE NUMBERS

Thirty seconds. The headlines.
Everything else is in the pages that follow.

262%
Year-over-year increase in peak attack sizes

2.7 Tbps
Largest observed peak attack volume in 2025

50+
Unique attack vector combinations in a single campaign

12.3 per day
Average DDoS attacks per customer in 2025, the sharpest annual rise in a decade

1.3 BILLION
Packets per second in a single TCP SYN event, February 2026

:06 seconds
Shortest observed attack wave in pulse campaigns

90.9 percent
Attacks now lasting less than 10 minutes, up from 80.7% in 2021

56 percent
Sub-1G attacks under 200 Mbps, small enough to be invisible on most dashboards

30.5 percent
Attacks followed by a repeat within seven days

INSIDE THIS REPORT

01 THE YEAR IN NUMBERS

Attack sizes jumped 262% year over year. Peak volumes hit 2.7 Tbps. A single UDP event threw 1.3 billion packets per second at a target. And all of that happened before 2025 was over.

These aren't projections. They're what our SOC recorded, while Corero solutions were protecting real networks, in real time. The trend line isn't flattening.

This report covers everything our Security Operations Center observed across the full calendar year and into early 2026. The picture is clear: speed, scale, and complexity have all shifted into a new gear. What was a record-breaking event 18 months ago is now a Tuesday. **Three patterns stood out.**

ATTACKS GOT BIGGER

Peak sizes climbed every month through 2025. Q4 produced volumes that would have been unthinkable in Q1. TCP SYN/ACK reflection drove the biggest events, but it wasn't working alone. Multi-vector campaigns combining reflection, UDP floods, and protocol tricks became the norm.

ATTACKS GOT FASTER

Pulse attacks lasting as little as six seconds showed up as a consistent pattern. At terabit volumes, six seconds of unmitigated traffic saturates a 10 Gbps link several times over. The mitigation window has collapsed from minutes to seconds.

ATTACKS GOT SMARTER

Campaigns shift vectors in real time now, adjusting payloads and traffic patterns while the attack is still running. Botnets like Aisuru overtook Mirai-era variants in both scale and capability, and while law enforcement disrupted Aisuru, the compromised devices it exploited are still out there.

AI is accelerating all of it. Attackers use it to find vulnerabilities, automate reconnaissance, adapt to defenses, and erase the forensic breadcrumbs investigators relied on for years.

This report is built on observed data, not vendor positioning. The numbers speak for themselves.

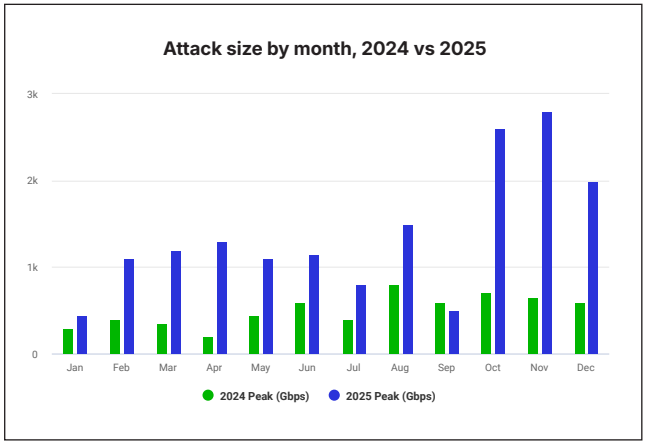
02 THE VOLUME STORY

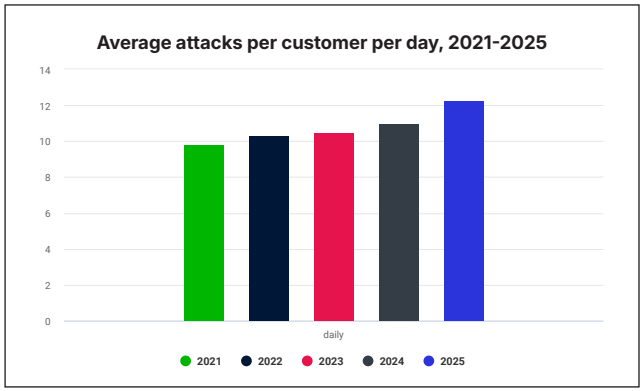
WHAT THE DATA SAYS

262%

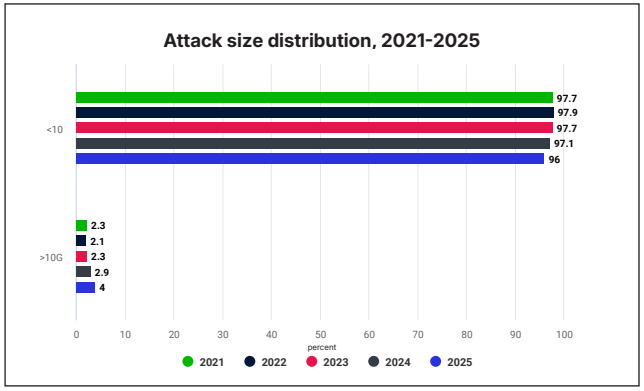
Year-over-year increase in peak attack sizes, 2024 to 2025

Every month in 2025 outpaced its 2024 counterpart and by November, peak sizes hit 2.7 Tbps. That's more than four times the highest monthly peak from the prior year. TCP SYN/ACK reflection drove a significant share of those volumes.



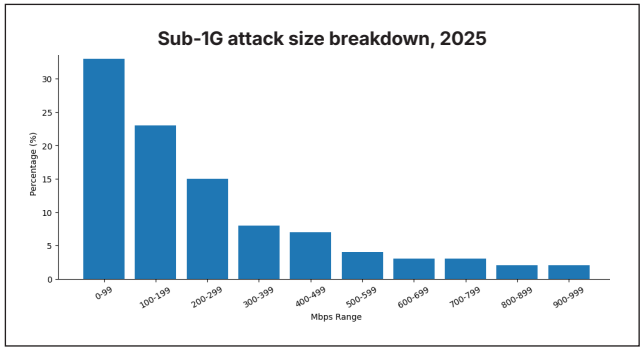


The average number of DDoS attacks per customer per day rose to 12.3 in 2025, up 12% from 11.0 in 2024. That's the sharpest single-year increase we've tracked. Since 2021, when the average sat at 9.8, daily attack frequency has climbed 25%, a sustained and accelerating trend.



The size distribution continues to polarize with over 96% of attacks in 2025 remaining under 10 Gbps. But the share of attacks exceeding 10 Gbps has nearly doubled since 2021, rising from 2.3% to 4.0%. That's a 72% increase in the proportion of large attacks over five years. Small attacks still dominate the count, but the big ones are getting more frequent.

Zooming into the sub-1 Gbps category reveals something worth paying attention to. A third of those attacks, 33%, are under 100 Mbps. Over half are under 200 Mbps. At those volumes, most organizations aren't registering them as attacks at all. They look like normal traffic fluctuation, a brief latency spike, a momentary blip that nobody investigates.



WHERE THE ATTACKS START

A third of all sub-1G attacks are under 100 Mbps which are levels small enough to be invisible on most dashboards. It's also exactly the size range an attacker would use to probe defenses, test response thresholds, and map infrastructure before launching something bigger.

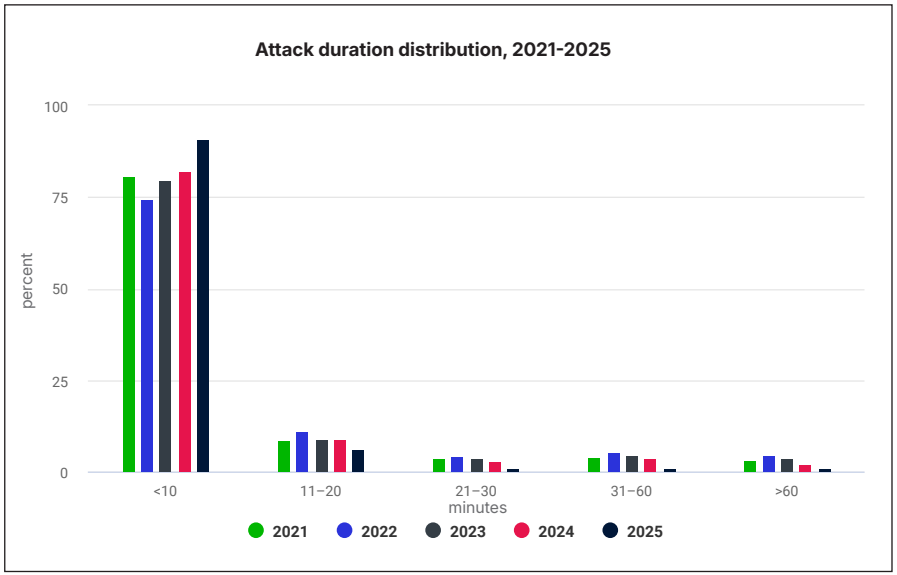
THE BIGGER PICTURE

The volume escalation isn't happening in isolation. Larger botnets, more efficient reflection techniques, and the compounding effect of multi-vector campaigns are all feeding it. The question for any organization isn't whether they'll face volumes at this scale. It's when.

The duration data tells its own story. Over 90.9% of attacks in 2025 lasted less than 10 minutes, up from 80.7% in 2021. Every other duration bracket is shrinking. Attacks lasting 11 to 20 minutes dropped from 8.6% to 5.9%. Attacks over 60 minutes fell from 3.2% to 1.1%. The trend is unmistakable: attacks are getting shorter, faster, and more automated.

WHAT IT MEANS

For capacity planning, if you are using previous methodologies based around the last year or two, you will find you are already behind. Last year we reported the "middle tier" of DDoS was fading as attackers polarized between high-frequency low-volume probing and strategic high-volume campaigns, and that polarization accelerated in 2025. The big attacks got much bigger, the small ones didn't slow down and the middle kept hollowing out. A 262% increase in a single year means the assumptions behind most infrastructure sizing are already outdated.

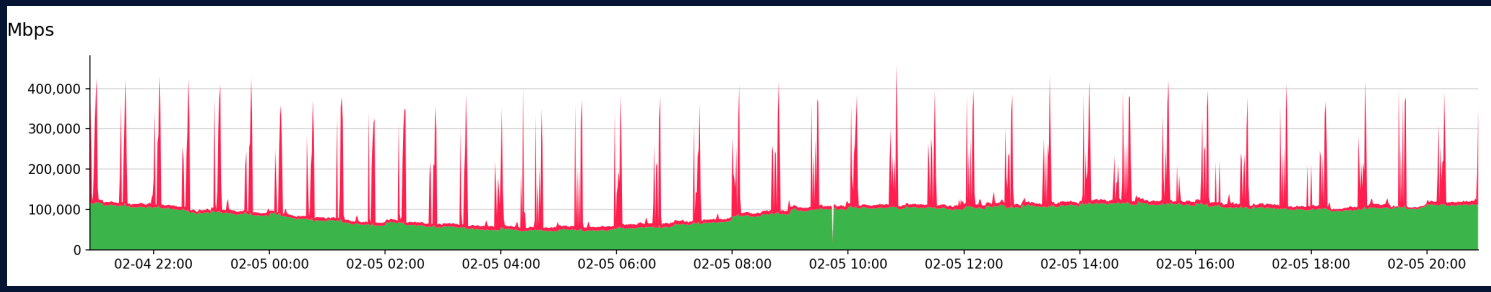


And they come back. Approximately 30.5% of attacks in 2025 were followed by another attack within seven days. Nearly one in three. That's not random. It's a pattern of repeat campaigns, and it means the first attack you see is rarely the last.

03 PULSE ATTACKS:

The Sub-10-Second Problem

WHAT THE DATA SAYS



6 seconds

Shortest observed attack wave in February 2026 pulse campaigns

The TCP SYN incident from early February 2026 tells the story. Each wave lasted between 6 and 38 seconds. Rapid spikes, repeated in succession, with no room for delayed detection, manual intervention, or traffic rerouting. **This isn't a one-off. It's becoming standard.**

WHAT IT MEANS

A 1 Tbps attack runs for 10 seconds. That's 1.25 terabytes of attack traffic. On a 10 Gbps link, this equates to complete saturation, several times over.

Pulse attacks are built around this math. Short, violent bursts designed to cause maximum damage exploiting any gap between detection and mitigation. If mitigation is measured in minutes, it's missing the entire event.

What Happens in 6 Seconds?

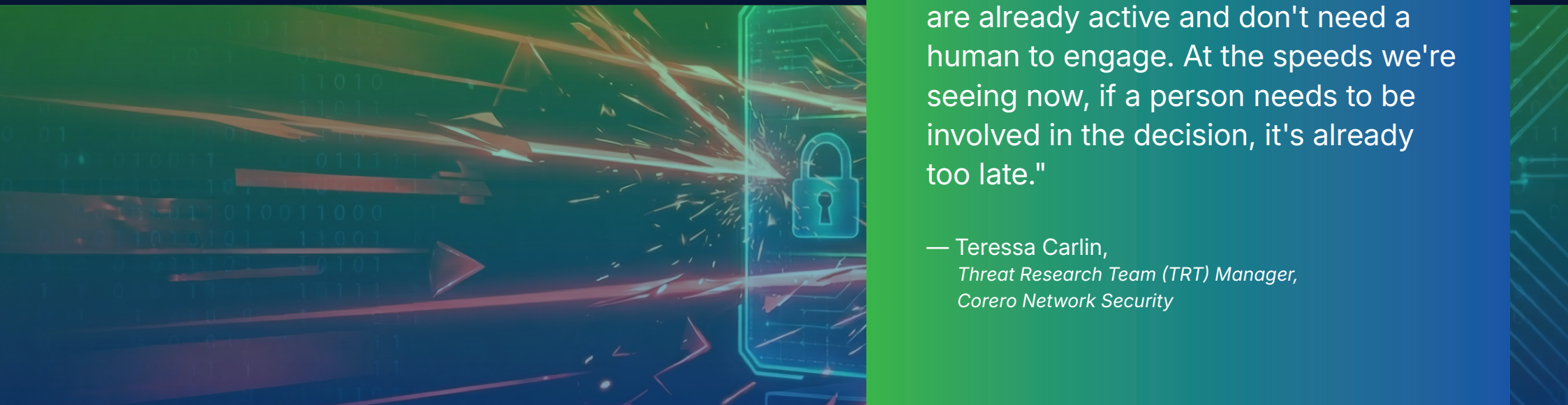
At 1 Tbps: 750 GB of attack traffic hits the network. A 10 Gbps link saturates instantly. Every customer behind that link goes dark. Six seconds. That's the math defenders are being asked to solve.

And it's not just technical. At terabit speeds, brief unmitigated windows translate into dropped transactions, SLA breaches, and customer-facing outages. The business impact is real and measurable.

Put it in SLA terms. A provider delivering 99.999% uptime has 26 seconds of allowable downtime per month. If each pulse attack causes six seconds of unmitigated exposure, just four attacks exhaust the entire monthly budget. FOUR.

THE BIGGER PICTURE

Pulse attacks are challenging a core assumption across much of the industry: that there's time to detect, decide, and respond. Many mitigation architectures were designed around attacks that ramp up, get identified, and get handled. Pulse attacks skip the ramp. They hit full force and they're over before traditional response cycles complete. Solutions that aren't already inline and already active face a fundamental timing problem.



> "You don't fight a 6-second attack. You either had protection in place before it hit, or you didn't. There's no middle ground. What my team focuses on isn't reacting faster. It's making sure our detection and mitigation are already active and don't need a human to engage. At the speeds we're seeing now, if a person needs to be involved in the decision, it's already too late."
>
> — Teressa Carlin,
> *Threat Research Team (TRT) Manager,*
> *Corero Network Security*

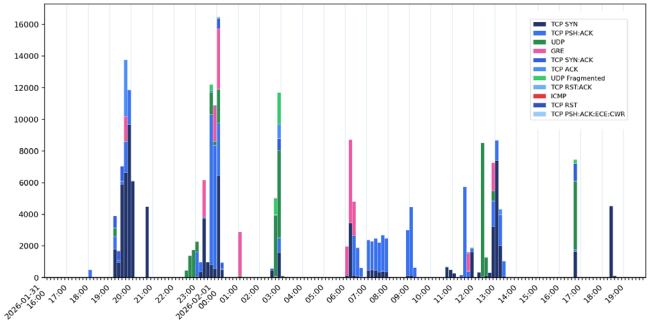
04 MULTI-VECTOR CAMPAIGNS:

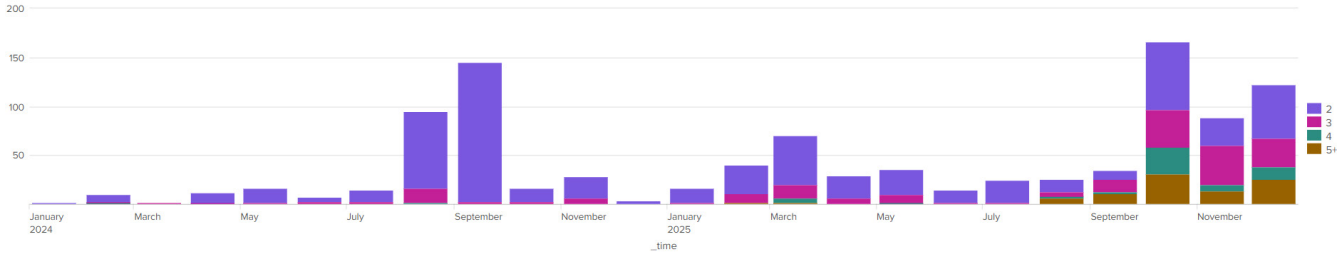
Attacks That Adapt

WHAT THE DATA SAYS

Single-vector DDoS attacks are increasingly rare. What we see now are campaigns that evolve while they're running. Attackers adjust payloads and traffic patterns in direct response to defensive measures, in real time.

This incident from January 2026, tells this story. Multiple vectors ran simultaneously, creating pressure from several directions at once.





WHAT IT MEANS

Last year we introduced the idea of "chained vectors": tightly sequenced attacks shifting between protocols every 30 to 60 seconds. In 2025, that went from an emerging trend to business as usual. Attackers aren't just throwing traffic at networks. They're probing, adapting, and switching tactics faster than most detection systems can reclassify. The reflection data reinforces the point. Individual volumes have increased over two years, and they're now frequently deployed in parallel. The compounding effect is what makes them dangerous. We've been seeing 50+ vectors in single campaigns, with TCP SYN variants, and UDP floods across multiple port combinations, ACK floods, RST floods, FIN floods, and fragmented UDP. All running concurrently in a single attack. Defending against one type at a time doesn't work anymore.

THE BIGGER PICTURE

This exposes a gap in how the industry tests defenses. Most DDoS testing still uses single-vector floods. That tells you how a system handles one scenario but it tells you almost nothing about 50 scenarios running simultaneously while the attacker watches your response and adjusts. The gap between how solutions are typically tested and how attackers actually operate is widening. The sub-1G reconnaissance data connects directly here. When a third of observed attacks are small enough to go unnoticed, and multi-vector campaigns are adapting in real time to defensive responses, the implication is hard to ignore: the small attacks aren't separate from the big ones. They're the scouting runs that inform them.

05 THE ARSENAL

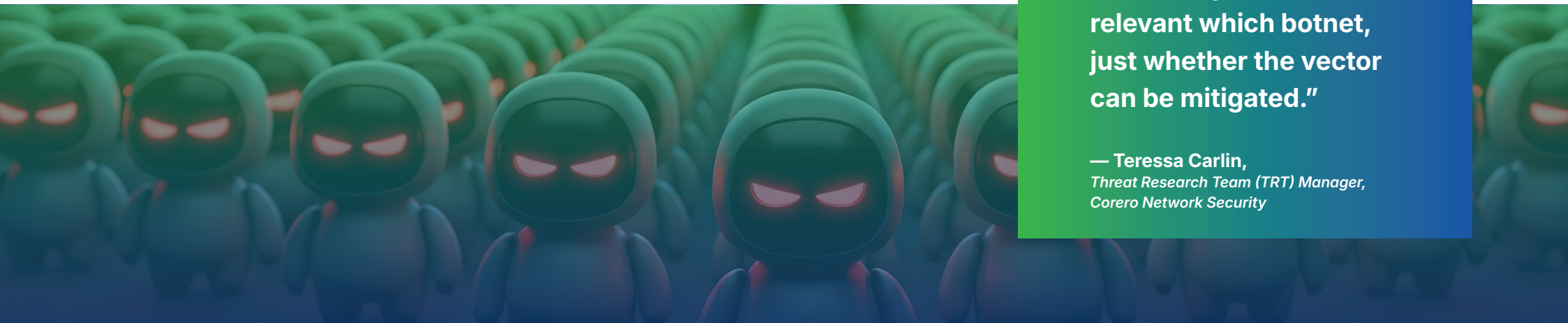
Botnets, reflection, DNS exploitation, & new TCP tricks

AISURU/KIMWOLF: Botnet Domination

By Q4, peak attack sizes ran 40 to 50% above the first-half average for 2025. The Aisuru botnet combining bandwidth-heavy and packet-rate attacks in parallel, TCP and UDP simultaneously. Mirai variants are still active and remain a real threat across the industry. But Aisuru/Kimwolf overtook them in population and observed attack size. It's the difference between a militia and a standing army.

More devices directly equate to higher throughput, better resilience, and sustained high-impact campaigns. And more DDoS vectors have been developed, some of which we've highlighted in this report. Take-down efforts will no doubt temporarily thwart this activity, but there's always a new contender waiting to fill the shoes of the last one, lest we forget that the compromised devices will still be there waiting to be taken advantage of once again.

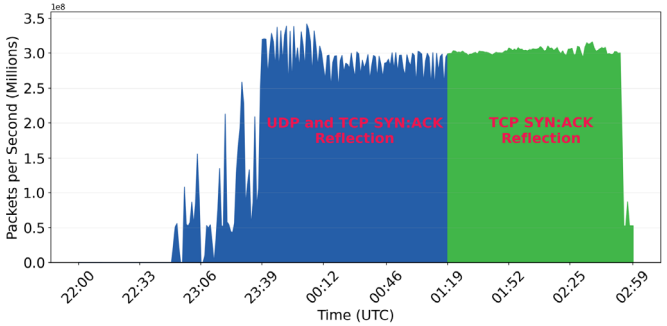
> **"With the naked eye it's almost impossible to tell which botnet is in play. The differences in traffic are subtle, it takes time and expertise to be able to decipher. The same compromised device which once belonged to a Mirai variant can be re-compromised by Aisuru. Essentially, it's not relevant which botnet, just whether the vector can be mitigated."**
>
> **— Teressa Carlin,**
> *Threat Research Team (TRT) Manager, Corero Network Security*



TCP SYN/ACK REFLECTION

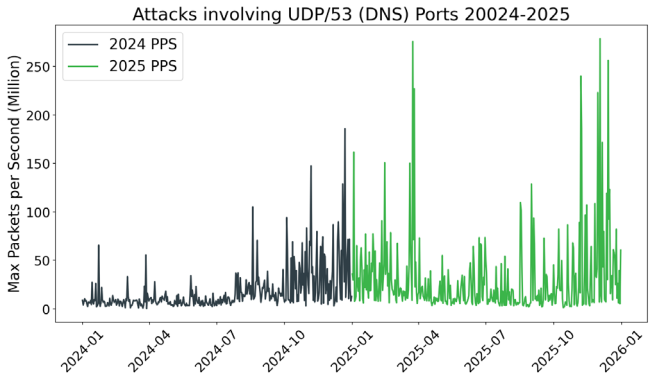
The workhorse vector of 2025. Twenty-four months of upward trajectory, no sign of slowing. High packet rates using small, correctly formed packets distributed across multiple subnets. The goal: overwhelming both bandwidth and CPU at the same time.

LATAM saw a high concentration of these events, ISPs frequently targeted. Especially difficult to mitigate because the attacks used legitimate, well-known sources as reflectors. Blocking those IPs breaks real traffic. Distinguishing malicious traffic inside legitimate flows remains one of the hardest problems in this space.



DNS: Trusted Protocol, Weaponized

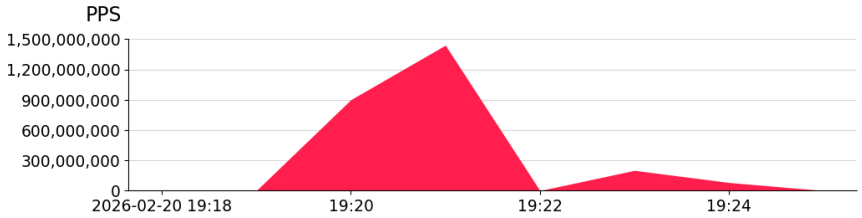
DNS keeps showing up because it keeps working. It's trusted, it's everywhere, and blocking DNS traffic from well-known infrastructure means breaking legitimate services. DNS combined with TCP vectors led with over 102,000 attacks. Some campaigns combined over 60 unique vectors in a single event.



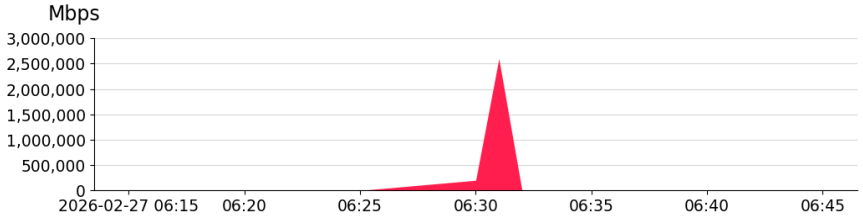
Common Vectors	Number of Attacks	Max unique Vectors seen in one Attack
DNS_TCP	102462	63
HTTP_DNS	98210	31
DNS_HTTP/S	51512	15
DNS_HTTP/S_TCP	1894	51
DNS_SSH	1102	8
DNS_GAMING	1097	13
OTHER	840	77
DNS_GAMING_TCP	418	11
DNS_SSH_TCP	406	19
CLDAP_DNS	167	6
DNS_SNMP	167	7
DNS_NTP	155	10
DNS_NTP_TCP	139	17
DNS_GRE	102	18
DNS_HTTP/SSH_TCP	89	101
DNS_WSDISCOVERY	70	5
DNS_GRE_TCP	65	23
DNS_RDP	61	9
DNS_RDP_TCP	61	12
DNS_SNMP_TCP	57	13
DNS_MYSQL	51	4

UDP: Little and Large

“Little”: floods of small packets with varying lengths, distributed across ports, different payloads starting from just 1 byte. Pattern-based filtering is extremely difficult. Goal: CPU exhaustion.



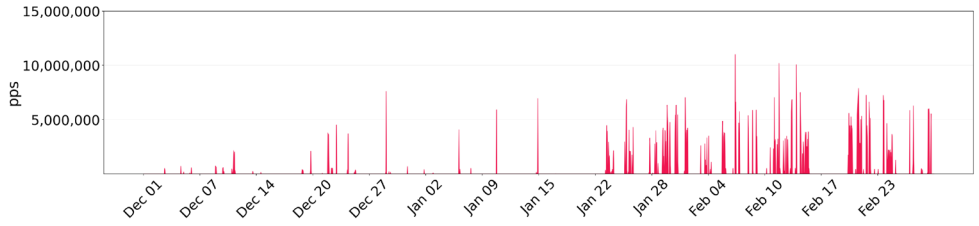
“Large”: oversized UDP packets, set packet length sizes, carpet-bombed across multiple IP subnets with randomized payloads. Signature detection is almost useless.



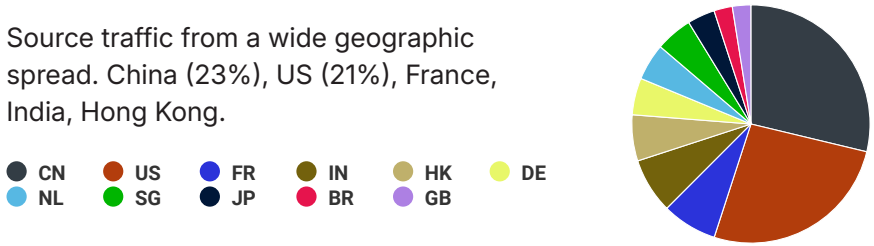
This means defenses need to handle high-packet-rate and high-bandwidth attacks at the same time. Optimizing for one creates a gap.

TCP “Big SYNs”: A New Pattern

TCP SYN packets carrying very large payloads. Under normal conditions, SYNs are small and carry no data. What we’re seeing uses significantly oversized packets, with a Feb 20 event hitting 1.3 billion PPS.



Source traffic from a wide geographic spread. China (23%), US (21%), France, India, Hong Kong.



06 EVOLUTION OR REVOLUTION?

DDoS has been around for 30 years. For most of that time, evolution was gradual. Bigger botnets, larger floods, the occasional protocol exploit. Then the last five or six years happened.

The protocols are largely the same. A lot of the original abuses get recycled. But the tools have changed. AI automation. Massive IoT compromise. Shared botnet infrastructure running like a commercial service. The attacker community has professionalized.

That professionalization doesn't happen in a vacuum. Periods of geopolitical instability have historically accelerated investment in offensive cyber capability, and the tools and techniques developed for state-level operations don't stay contained. They filter into the broader ecosystem. DDoS-as-a-Service platforms now offer capabilities that would have required state resources a decade ago, available to anyone with a few dollars and a target. The line between state-sponsored, ideologically motivated, and commercially operated attacks has blurred to the point where the distinction matters less than the outcome. History shows that conflict accelerates innovation. Recent global conflicts have driven rapid advances in autonomous systems, drone warfare, and cyber operations. Those capabilities don't stay confined to defense communities. They proliferate. And the DDoS ecosystem is a direct beneficiary.

Whether that's evolution or revolution depends on how you define speed. But the pace of the last few years feels more like a break from the past than a continuation of it.

Late 1990s: The First Shots

First attack toolkits (Trinoo, TFN). Basic protocol floods against online casinos and early e-commerce. No purpose-built DDoS defense existed. The only option was calling your ISP.

2000-2010: Scale and Visibility

LOIC, BlackEnergy, early DDoS-for-hire. High-profile hits on Yahoo, Amazon, eBay, CNN. Geopolitical attacks emerge (Estonia 2007). First dedicated security appliances, early scrubbing services (Prolexic, Arbor), and the beginning of cloud-based mitigation.

2010-2019: The Amplification Era

NTP, SSDP, DNS, and Memcached amplification. Mirai and the IoT explosion. MikroTik botnets. Attack tool source code released publicly. DDoS crosses the 1 Tbps barrier in 2018. Corero SmartWall launches real-time inline mitigation.

AI, ATTRIBUTION, AND LETTING GO

Attribution is the holy grail in cybersecurity. Following the trail. Finding the breadcrumbs. Identifying who caused the damage. For DDoS? It's a dead end that keeps getting deader.

DDoS has always made attribution nearly impossible. The data volumes are enormous. Deployments sit at the network edge. Sampling technologies don't capture enough to prove anything.

AI made it worse. Attackers use it to evolve malware, exploit vulnerabilities, launch attacks through DDoS-as-a-Service with hidden origins, and adapt in real time. Whether they're state-sponsored, organized crime, or "APTeens" (Advanced Persistent Teenagers), AI is part of the toolkit now.

It also erases the clues investigators relied on. Language patterns? AI generates clean copy in any language. Coding quirks? Generic code. Infrastructure reuse? Trivial to spin up fresh. The fingerprints are disappearing.

2020-2024: Adaptation & Complexity

Mozi, Meris, Log4Shell. Compromised cloud infrastructure and proxy networks. Carpet-bombing, DNS water torture, pulse attacks emerge. Attackers begin adapting to defenses in real time. Detection-to-block times drop. Surgical filtering replaces blunt-force scrubbing.

2025-2026: The Convergence

Aisuru/Kimwolf reaches millions of devices. Record-breaking terabit-scale attacks. High PPS SYN/ACK reflection and UDP. AI-assisted reconnaissance. Multi-vector adaptive campaigns. Hyper-volumetric attacks. Defense-aware attackers. The line between state-sponsored and commercial attack infrastructure disappears.

The question the defense community needs to ask honestly: is DDoS attribution worth more than understanding what's coming next? The data suggests no.

THE ATTRIBUTION PARADOX

The more resources the industry spends identifying who is behind DDoS attacks, the less it has for stopping the next one. Successful attribution rarely leads to consequences. Attackers know this. They're betting on defenders looking backward while the next campaign is already being assembled.

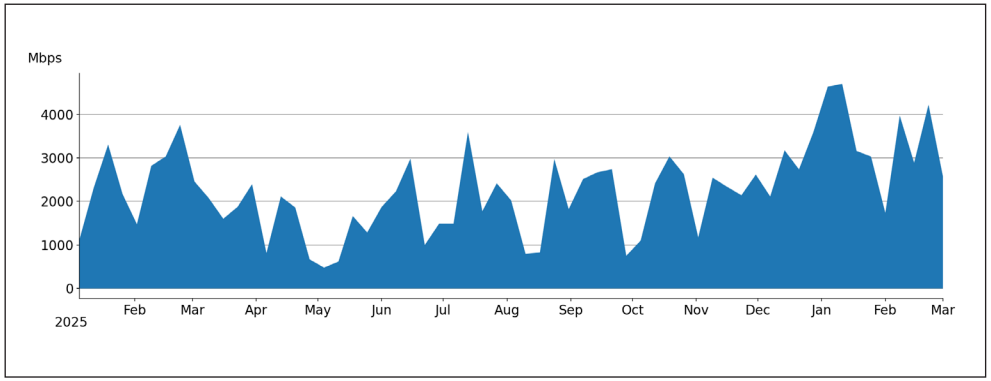
07 THE ARCHITECTURE QUESTION

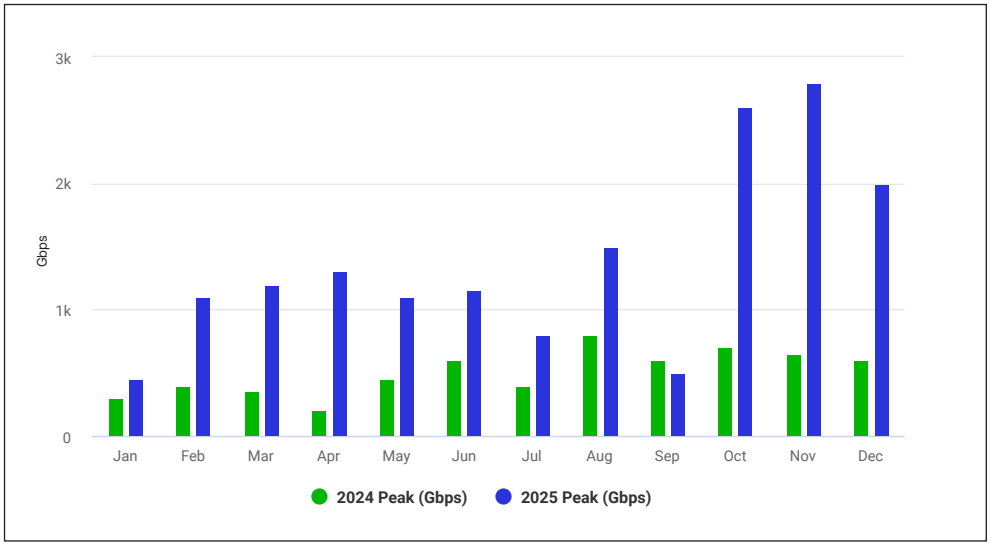
WHAT THE DATA SAYS

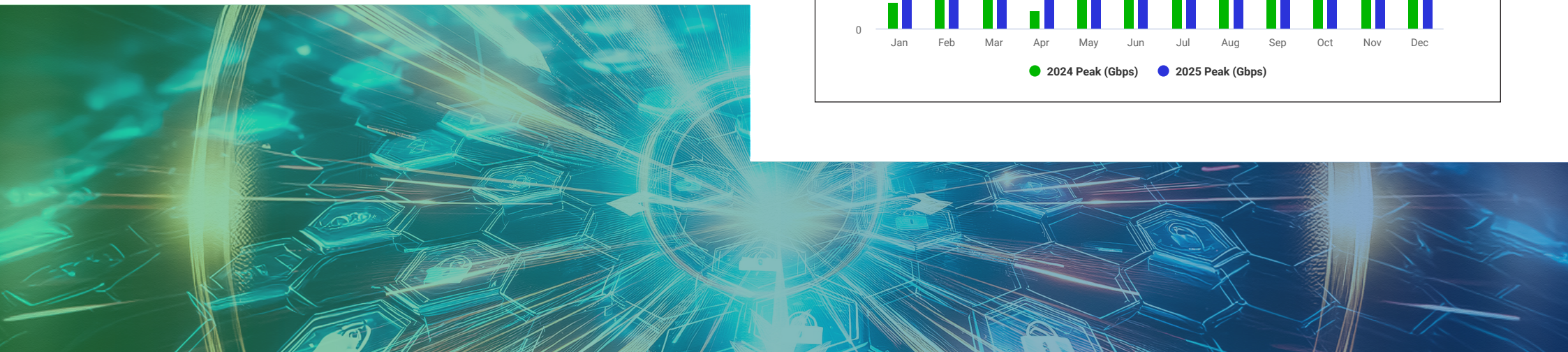
The data in this report puts pressure on every DDoS deployment model. Not one type. All of them.

Pulse attacks challenge any architecture that depends on traffic rerouting. Six-second bursts are over before rerouting completes. Multi-vector campaigns challenge any architecture relying on sequential detection. Fifty simultaneous vectors don't wait for classification. Volumetric peaks at 2.7 Tbps challenge any architecture with fixed local capacity.

Corero protects traffic across GTT's global network, giving us visibility into attack patterns from the cloud side as well. That telemetry tells the same story. The maximum DDoS attack volumes observed on GTT's network rose from a peak of 750 Gbps in 2024 to 2.7 Tbps in 2025. That's a 3.6x year-over-year increase. Q4 was especially stark: October, November, and December all exceeded 2 Tbps, volumes that never appeared once in 2024.







Attack Size (Mbps)	Customer Link BandWidth (Mbps)									
	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000
100,000	99.00%	98.00%	97.00%	96.00%	95.00%	94.00%	93.00%	92.00%	91.00%	90.00%
200,000	99.50%	99.00%	98.50%	98.00%	97.50%	97.00%	96.50%	96.00%	95.50%	95.00%
300,000	99.67%	99.33%	99.00%	98.67%	98.33%	98.00%	97.67%	97.33%	97.00%	96.67%
400,000	99.75%	99.50%	99.25%	99.00%	98.75%	98.50%	98.25%	98.00%	97.75%	97.50%
500,000	99.80%	99.60%	99.40%	99.20%	99.00%	98.80%	98.60%	98.40%	98.20%	98.00%
600,000	99.83%	99.67%	99.50%	99.33%	99.17%	99.00%	98.83%	98.67%	98.50%	98.33%
700,000	99.86%	99.71%	99.57%	99.43%	99.29%	99.14%	99.00%	98.86%	98.71%	98.57%
800,000	99.88%	99.75%	99.63%	99.50%	99.38%	99.25%	99.13%	99.00%	98.88%	98.75%
900,000	99.89%	99.78%	99.67%	99.56%	99.44%	99.33%	99.22%	99.11%	99.00%	98.89%
1,000,000	99.90%	99.80%	99.70%	99.60%	99.50%	99.40%	99.30%	99.20%	99.10%	99.00%
1,100,000	99.91%	99.82%	99.73%	99.64%	99.55%	99.45%	99.36%	99.27%	99.18%	99.09%
1,200,000	99.92%	99.83%	99.75%	99.67%	99.58%	99.50%	99.42%	99.33%	99.25%	99.17%
1,300,000	99.92%	99.85%	99.77%	99.69%	99.62%	99.54%	99.46%	99.38%	99.31%	99.23%
1,400,000	99.93%	99.86%	99.79%	99.71%	99.64%	99.57%	99.50%	99.43%	99.36%	99.29%
1,500,000	99.93%	99.87%	99.80%	99.73%	99.67%	99.60%	99.53%	99.47%	99.40%	99.33%
1,600,000	99.94%	99.88%	99.81%	99.75%	99.69%	99.63%	99.56%	99.50%	99.44%	99.38%
1,700,000	99.94%	99.88%	99.82%	99.76%	99.71%	99.65%	99.59%	99.53%	99.47%	99.41%
1,800,000	99.94%	99.89%	99.83%	99.78%	99.72%	99.67%	99.61%	99.56%	99.50%	99.44%
1,900,000	99.95%	99.89%	99.84%	99.79%	99.74%	99.68%	99.63%	99.58%	99.53%	99.47%
2,000,000	99.95%	99.90%	99.85%	99.80%	99.75%	99.70%	99.65%	99.60%	99.55%	99.50%
2,100,000	99.95%	99.90%	99.86%	99.81%	99.76%	99.71%	99.67%	99.62%	99.57%	99.52%
2,200,000	99.95%	99.91%	99.86%	99.82%	99.77%	99.73%	99.68%	99.64%	99.59%	99.55%
2,300,000	99.96%	99.91%	99.87%	99.83%	99.78%	99.74%	99.70%	99.65%	99.61%	99.57%
2,400,000	99.96%	99.92%	99.88%	99.83%	99.79%	99.75%	99.71%	99.67%	99.63%	99.58%
2,500,000	99.96%	99.92%	99.88%	99.84%	99.80%	99.76%	99.72%	99.68%	99.64%	99.60%

Percentage of traffic that must be blocked to prevent link saturation: Requires >99.9% Requires >99.5% Requires ≤99.5%

And here's where the math gets uncomfortable for anyone relying on cloud-only scrubbing. As attacks scale into the terabit range while customer access links remain in the 1 to 10 Gbps range, mitigation has to be nearly perfect. Even 0.5% of residual traffic from a large attack can completely saturate a customer's connection. A 1 Tbps attack against a customer on a 1 Gbps link requires 99.9% mitigation effectiveness just to keep the link clear. At 2.5 Tbps, that number climbs to 99.96%. The bigger the attacks get, the closer to 100% mitigation has to be. The margin for error is shrinking toward zero.

The 0.5% Problem At terabit scale, "almost perfect" mitigation isn't good enough. Half a percent of a 2 Tbps attack is 10 Gbps of leaked traffic. That's a complete outage for any customer on a standard access link. The math doesn't leave room for "good enough."

Making it harder: cloud traffic volatility has been climbing steadily, with year-over-year swings rising from 129% in 2021 to 161% in 2025. More volatile baseline traffic makes it harder to distinguish legitimate surges from attack spikes, which means the filtering that needs to be near-perfect is also working against an increasingly unpredictable backdrop.

WHAT IT MEANS

The industry has treated this as a binary choice: cloud scrubbing or on-premise appliances. Scalability or granularity. Remote capacity or local speed. The attacks in this report don't respect those categories.

A pulse attack doesn't care whether an architecture is cloud-native or on-premise. It cares whether mitigation is faster than six seconds. A multi-vector campaign doesn't care about deployment models. It cares whether detection handles 50 vectors at once.

The Question Worth Asking

The old question was "where do we send traffic to be cleaned?" The better one: "can our architecture handle attacks that are simultaneously fast, large, and complex?" Most organizations haven't tested that scenario. Attackers have.

THE BIGGER PICTURE

The vendor community, ourselves included, needs to be honest about what single-layer architectures can and can't do. No single deployment model handles everything in this report. Integration, intelligence sharing, and interoperability between defensive layers will define the next chapter of DDoS defense more than any individual product.

This is why the industry is moving toward integrated partnerships between edge protection providers and cloud-scale networks. Corero's alliances with Akamai and GTT are one example of this shift, combining edge-level and cloud-scale protection in a single integrated model. It's a pattern emerging across the industry, and the data in this report explains why.

08 WHAT'S NEXT

Where the data says this is heading

The volume ceiling hasn't been found

The 262% year-over-year increase followed a steady monthly escalation through 2025. Nothing in the data suggests a plateau. Botnet proliferation, expanding DDoS-as-a-Service infrastructure, and AI-assisted tooling all point in one direction. Expect 2026 peaks to exceed 2025.

Pulse attacks will force an industry reckoning

The sub-10-second pattern isn't a novelty. It's a stress test of the entire defense ecosystem. Architectures designed around time to detect, reroute, and scrub are being challenged at a foundational level. Expect this pattern to become more common. The industry will have to confront whether current response time benchmarks are still relevant.

Aisuru/Kimwolf hasn't peaked

Aisuru saw twelve to 18% monthly growth in the months before its disruption by law enforcement, this is concerning. Undisclosed zero-days driving that growth make these botnets a genuine wildcard. Until those exploits are identified and patched at scale, these botnets will keep expanding. More devices, higher throughput, more sustained campaigns.

AI keeps eroding attribution and accelerating adaptation

Every forensic shortcut is being smoothed out. Language analysis, code patterns, infrastructure tracking. AI also accelerates how fast attacks adapt to defenses. The gap between attacker adaptation and defender response is growing.

Geopolitical instability will keep fueling the attack ecosystem

Global conflict doesn't just produce headlines. It produces infrastructure. State investment in offensive cyber capabilities creates tools, techniques, and trained operators that eventually move into the broader ecosystem. Hacktivism, retaliatory campaigns, and ideologically motivated attacks all spike during periods of instability. The regional concentrations we observed in 2025, including elevated activity across LATAM and traffic sourced heavily from a handful of nations, are consistent with this pattern. As long as geopolitical tensions persist, the DDoS ecosystem has a steady supply of motivation, funding, and talent feeding it.

Multi-vector complexity is climbing

Fifty-plus simultaneous vectors isn't the ceiling. It's the new floor. As infrastructure grows and tooling automates, the vector count will keep climbing. Testing methodologies and benchmarks need to catch up.

The convergence is the real story

Bigger, faster, smarter. Any one alone is manageable. All three compounding each other is a qualitatively different problem. A 2.7 Tbps attack arriving in a 6-second burst while cycling through 50 vectors isn't just more of the same. It's a new category of threat. **That convergence is what makes 2025 a turning point.**

DDoS is easy. DDoS defense still isn't. The data doesn't lie, and it doesn't have an agenda. Use this report to have honest conversations about where things stand. Share it with your team, your leadership, your partners. The signal is there for anyone willing to look at it clearly.

corero [NETWORK SECURITY]

ABOUT CORERO NETWORK SECURITY

Corero Network Security is a global provider of automated network security and integrated business continuity solutions, trusted by enterprises in more than 50 countries. Built on a platform that unifies SmartWall ONE™ DDoS protection with CORE intelligence, Corero delivers real-time protection, traffic intelligence, and access control across financial services, healthcare, SaaS, telecommunications, and government sectors. Headquartered in London with operational centers in Marlborough, Massachusetts, and Edinburgh, UK.

For more information, visit corero.com.

This report is based on data collected by Corero Network Security's Security Operations Center throughout 2025 and into early 2026. All attack data reflects real-world observations from protected networks. No customer names or identifying information are included.