Doelwit van 20,5 miljoen DDoS-aanvallen, een stijging van 358% ten opzichte van vorig jaar: Het 2025 Q1 Threat Report van Cloudflare

blog.cloudflare.com/nl-nl/ddos-threat-report-for-2025-q1

28 april 2025

2025-04-27

Welkom bij de 21e editie van het Cloudflare DDoS Threat Report. Dit rapport wordt elk kwartaal gepubliceerd en biedt een uitgebreide analyse van het veranderende dreigingslandschap van Distributed Denial of Service (DDoS)-aanvallen op basis van de gegevens van het Cloudflare-netwerk. In deze editie richten we ons op het eerste kwartaal (Q1) van 2025. Voor eerdere rapporten ga je naar www.ddosreport.com.

Hoewel dit rapport zich voornamelijk richt op het eerste kwartaal van 2025, bevat het ook recente gegevens van een hypervolumetrische DDoS-campagne die in april 2025 plaatsvond, met enkele van de grootste aanvallen die ooit openbaar zijn gemaakt. In een historische toename van deze activiteiten hebben we de meest intensieve pakketsnelheid-aanval ooit geblokkeerd, met een piek van 4,8 miljard pakketten per seconde (Bpps), 52% groter dan de vorige benchmark. Daarnaast hebben we ons afzonderlijk verdedigd tegen een enorme aanval van 6,5 terabits per seconde (Tbps), wat overeenkomt met de grootste bandbreedte-aanvallen die ooit zijn gemeld.

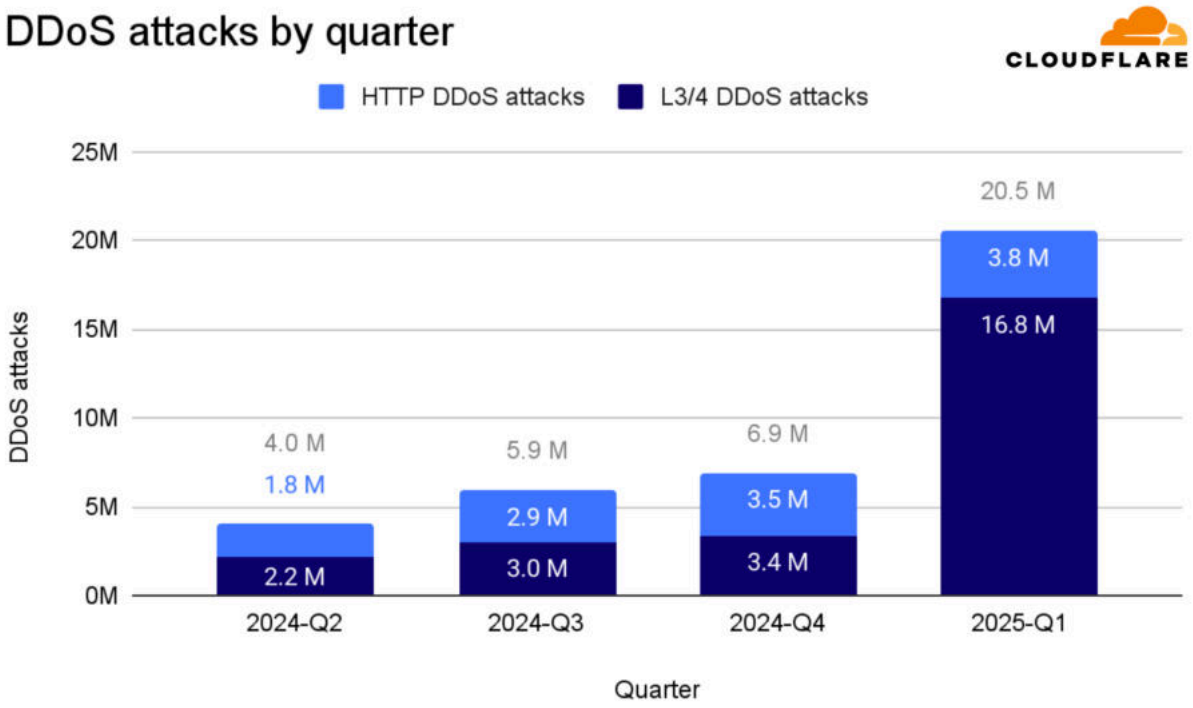
- In het eerste kwartaal van 2025 blokkeerde Cloudflare 20,5 miljoen DDoS-aanvallen. Dat is een stijging van 358% op jaarbasis en een stijging van 198% op kwartaalbasis.
- Ongeveer een derde daarvan, ofwel 6,6 miljoen, was rechtstreeks op de netwerkinfrastructuur van Cloudflare gericht als onderdeel van een 18 dagen durende multi-vectoraanvalscampagne.
- Bovendien blokkeerde Cloudflare in het eerste kwartaal van 2025 ongeveer 700 hypervolumetrische DDoS-aanvallen die de 1 Tbps of 1 Bpps overschreden – gemiddeld zo'n 8 aanvallen per dag.

Alle aanvallen werden door onze autonome verdediging geblokkeerd.

Voor meer informatie over DDoS-aanvallen en andere soorten cyberdreigingen ga je naar ons Learning Center. Ga naar Cloudflare Radar voor de interactieve versie van dit rapport waar je dieper op de materie kunt ingaan. Er is een gratis API voor mensen die geïnteresseerd zijn in het onderzoek naar internettrends. Je kunt ook meer te weten komen over de methodologieën die worden gebruikt om deze rapporten aan te maken.

In het eerste kwartaal van 2025 hebben we 20,5 miljoen DDoS-aanvallen geblokkeerd. Ter vergelijking: in het hele kalenderjaar 2024 hebben we 21,3 miljoen DDoS-aanvallen geblokkeerd. Alleen al het afgelopen kwartaal hebben we dus 96% geblokkeerd van het totaal dat we in 2024 hebben geblokkeerd.

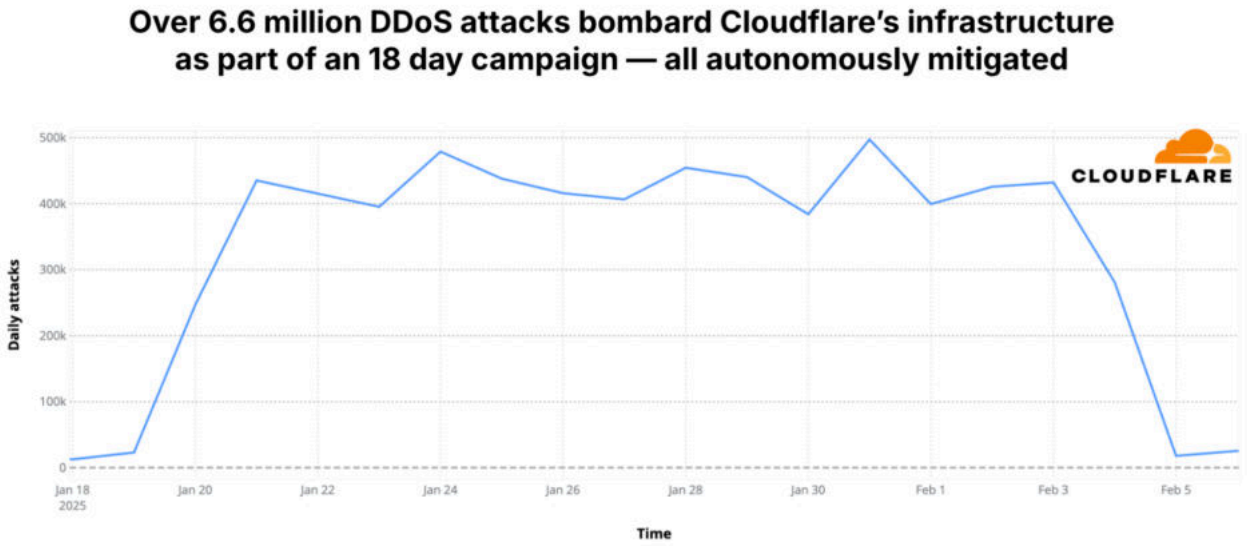
De grootste toename vond plaats bij DDoS-aanvallen op netwerkniveau. In het eerste kwartaal van 2025 hebben we 16,8 miljoen DDoS-aanvallen op netwerkniveau geblokkeerd. Dat is een toename van 397% op kwartaalbasis en een stijging van 509% op jaarbasis. Het aantal HTTP DDoS-aanvallen is ook toegenomen: met 7% op kwartaalbasis en met 118% op jaarbasis.



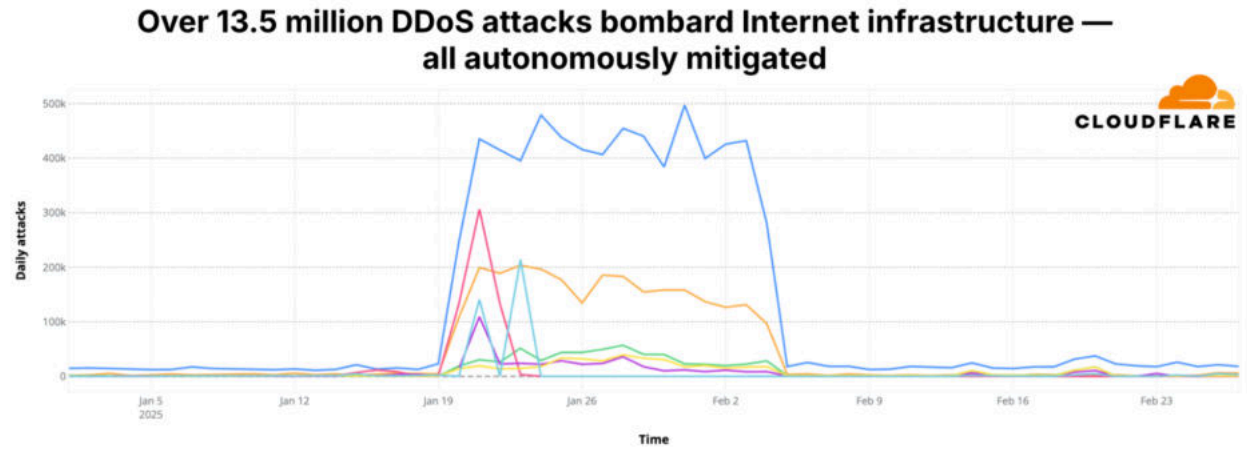
Wij tellen DDoS-aanvallen op basis van unieke realtime vingerafdrukken die door onze systemen worden gegenereerd. Soms kan één aanval of campagne meerdere vingerafdrukken genereren, vooral wanneer verschillende mitigatiestrategieën worden toegepast. Hoewel dit soms tot hogere aantallen kan leiden, krijgen we wel een goed algemeen beeld van de aanvalsactiviteit gedurende een bepaalde periode.

Van de 20,5 miljoen DDoS-aanvallen die in het eerste kwartaal werden geblokkeerd, waren 16,8 miljoen gericht op de netwerklaag. Daarvan waren 6,6 miljoen rechtstreeks gericht op de netwerkinfrastructuur van Cloudflare. Nog eens 6,9 miljoen hosting- en serviceproviders die het doelwit waren van een aanval worden door Cloudflare beschermd.

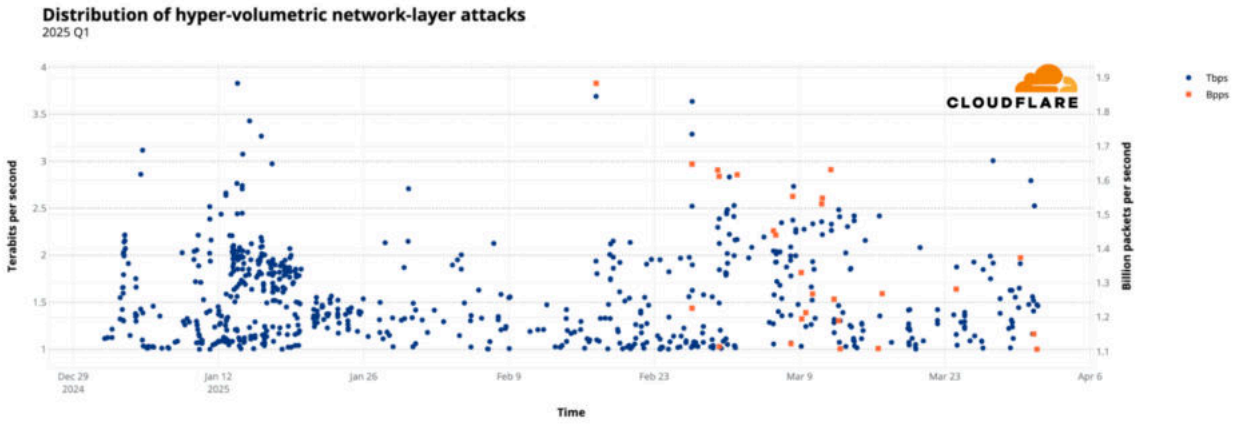
Deze aanvallen maakten deel uit van een 18 dagen durende multi-vector DDoS-campagne die onder andere bestond uit SYN flood attacks, door Mirai gegenereerde DDoS-aanvallen en SSDP amplification attacks. Deze aanvallen werden, net als alle 20,5 miljoen aanvallen, autonoom door onze DDoS-verdediging gedetecteerd en geblokkeerd.



In de onderstaande grafiek worden de dagelijkse aggregaten van aanvallen op Cloudflare met de blauwe lijn weergegeven. De andere kleuren vertegenwoordigen de verschillende hosting- en internetproviders die de Magic Transit-service van Cloudflare gebruiken en die tegelijkertijd werden aangevallen.

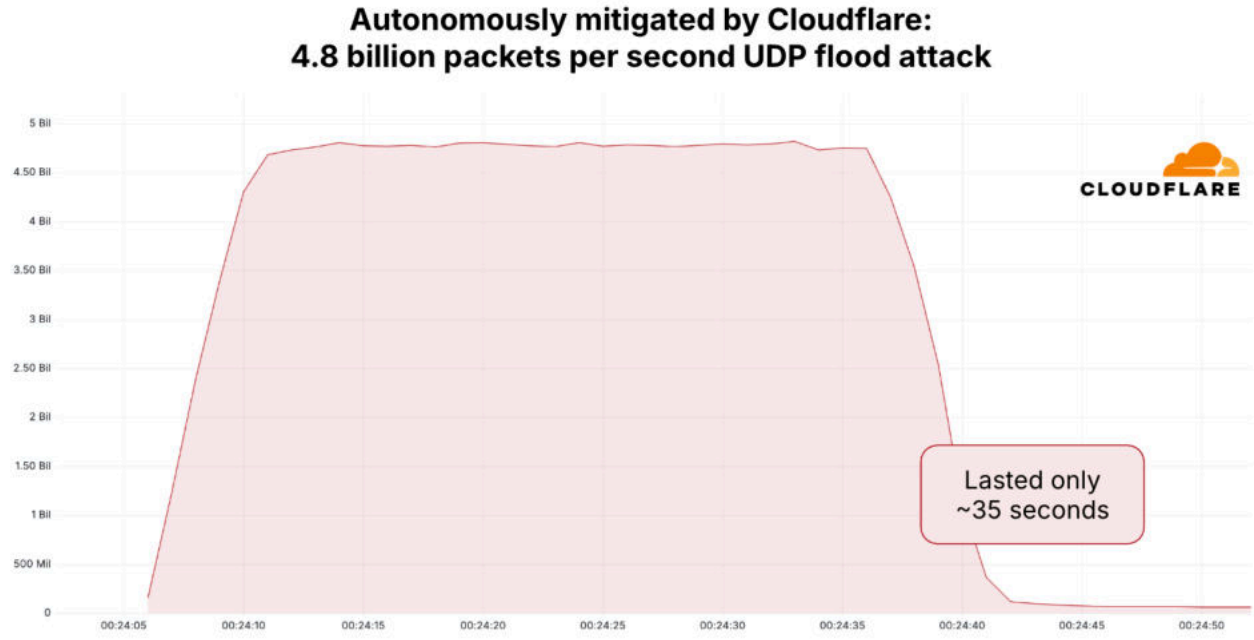


Hypervolumetrische DDoS-aanvallen zijn aanvallen die sneller zijn dan 1-2 Tbps of 1 Bpps. In Q1 2025 hebben we meer dan 700 van deze aanvallen geblokkeerd. Ongeveer 4 op de 100.000 DDoS-aanvallen op netwerkniveau waren hypervolumetrisch. Hypervolumetrische DDoS-aanvallen vinden meestal plaats via UDP.

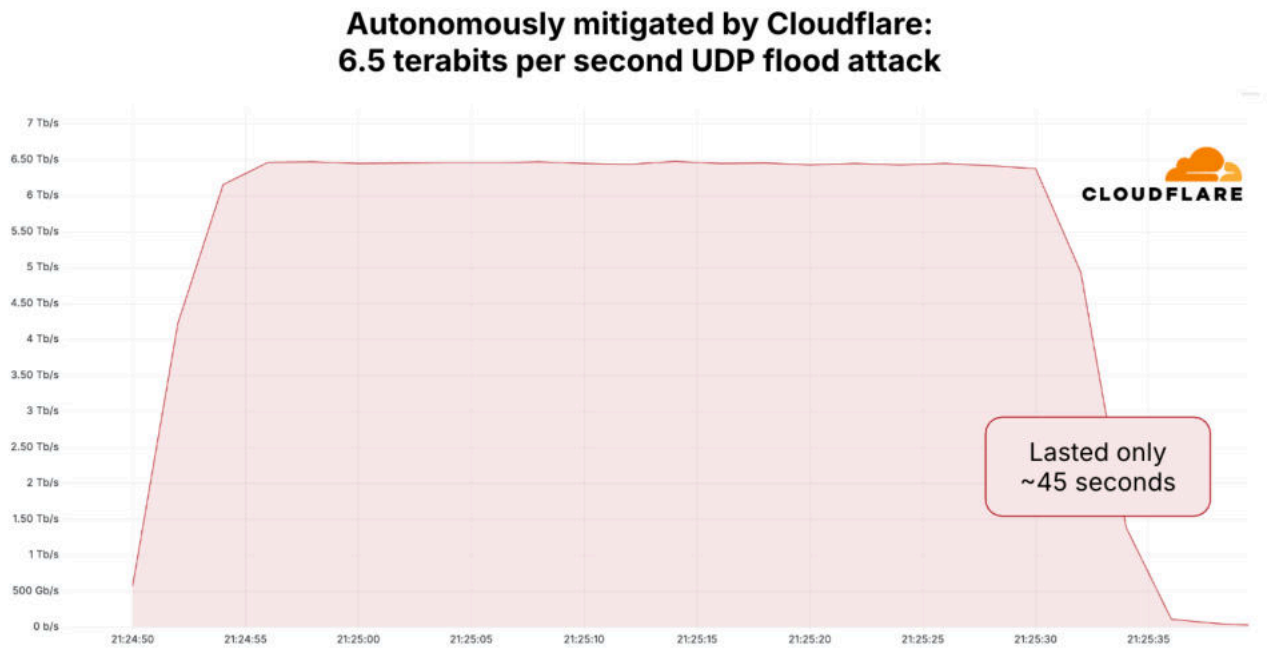


Hoewel dit rapport zich voornamelijk richt op het eerste kwartaal van 2025, vinden wij het belangrijk om ook de enorme, recordbrekende hypervolumetrische DDoS-aanvallen te noemen die zijn doorgegaan tot in Q2. Daarom hebben we de eerste inzichten uit die campagne in dit rapport opgenomen.

In de tweede helft van april 2025 detecteerden en blokkeerden de systemen van Cloudflare automatisch tientallen hypervolumetrische DDoS-aanvallen als onderdeel van een intensieve campagne. De grootste aanvallen bereikten pieken van 4,8 Bpps en 6,5 Tbps. Deze enorme pieken duurden meestal 35 tot 45 seconden. Met een snelheid van 6,5 Tbps is deze aanval even snel als de grootste openbaar bekendgemaakte DDoS-aanval tot nu toe. De aanval van 4,8 Bpps is de grootste die ooit is bekendgemaakt vanuit het perspectief van de pakketintensiteit, ongeveer 52% groter dan het vorige record van 3,15 Bpps.



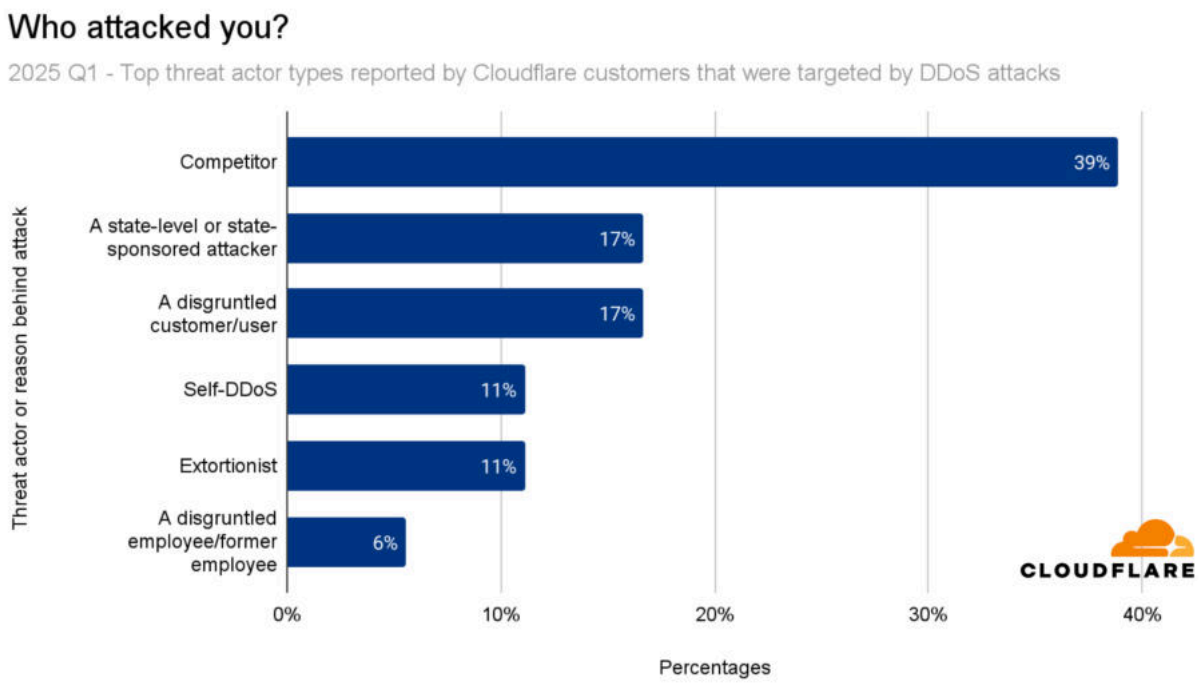
De aanvallen waren afkomstig uit 147 landen en waren gericht op meerdere IP-adressen en poorten van een hostingprovider die door Cloudflare Magic Transit wordt beschermd. Alle aanvallen werden met succes door het netwerk van Cloudflare geblokkeerd.



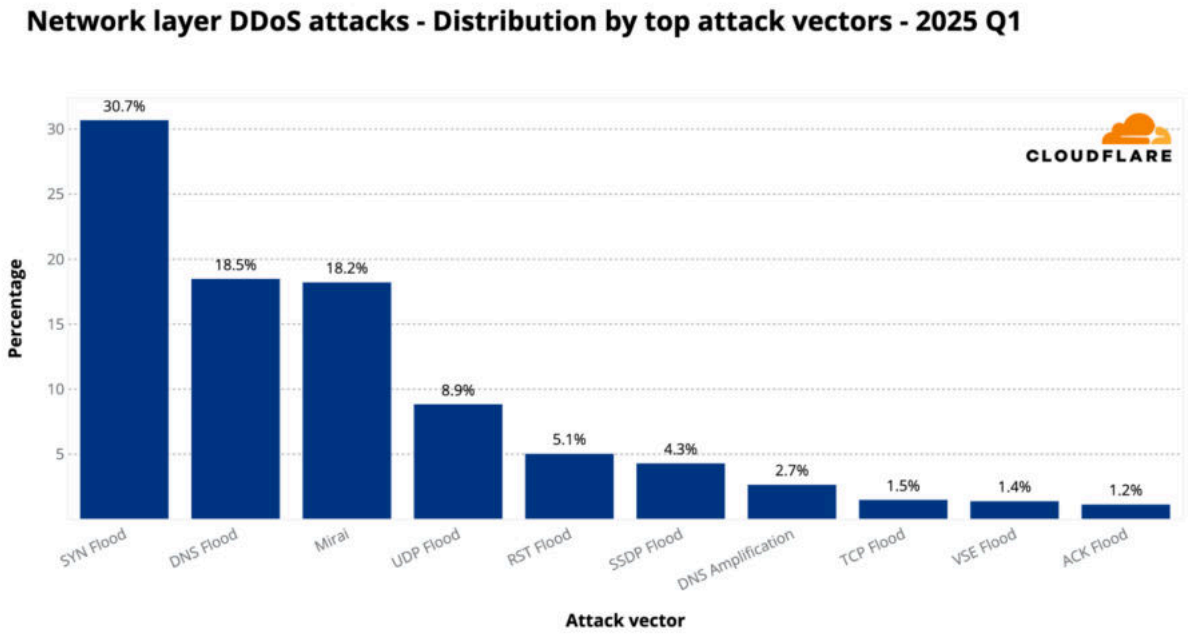
In een enquête onder Cloudflare-klanten die het doelwit waren van DDoS-aanvallen, gaf de meerderheid aan dat ze niet wisten wie de aanvaller was. Degenen die het wel wisten, gaven aan dat hun concurrenten deze meeste van deze aanvallen hadden uitgevoerd (39%). Dat is vergelijkbaar met het vorige kwartaal. Dit komt veel in de gaming- en gokindustrie voor.

Nog eens 17% meldde dat een staat of een door een staat gesponsorde actor achter de aanval zat, en een vergelijkbaar percentage meldde dat een ontevreden gebruiker of klant de aanval had uitgevoerd.

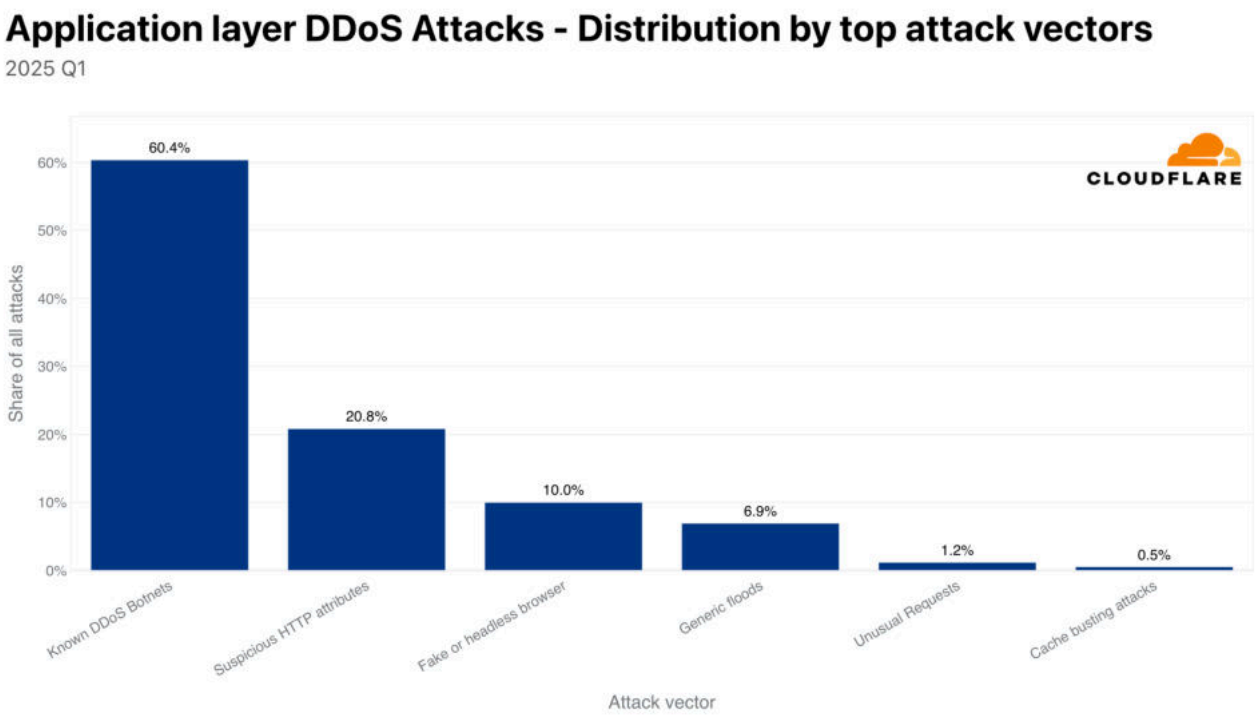
Nog eens 11% gaf aan dat ze de DDoS-aanval per ongeluk tegen zichzelf hadden gericht (self-DDoS) en een vergelijkbaar percentage zei dat een afperser achter de aanvallen zat. 6% gaf aan dat de aanvallen werden uitgevoerd door ontevreden of voormalige werknemers.



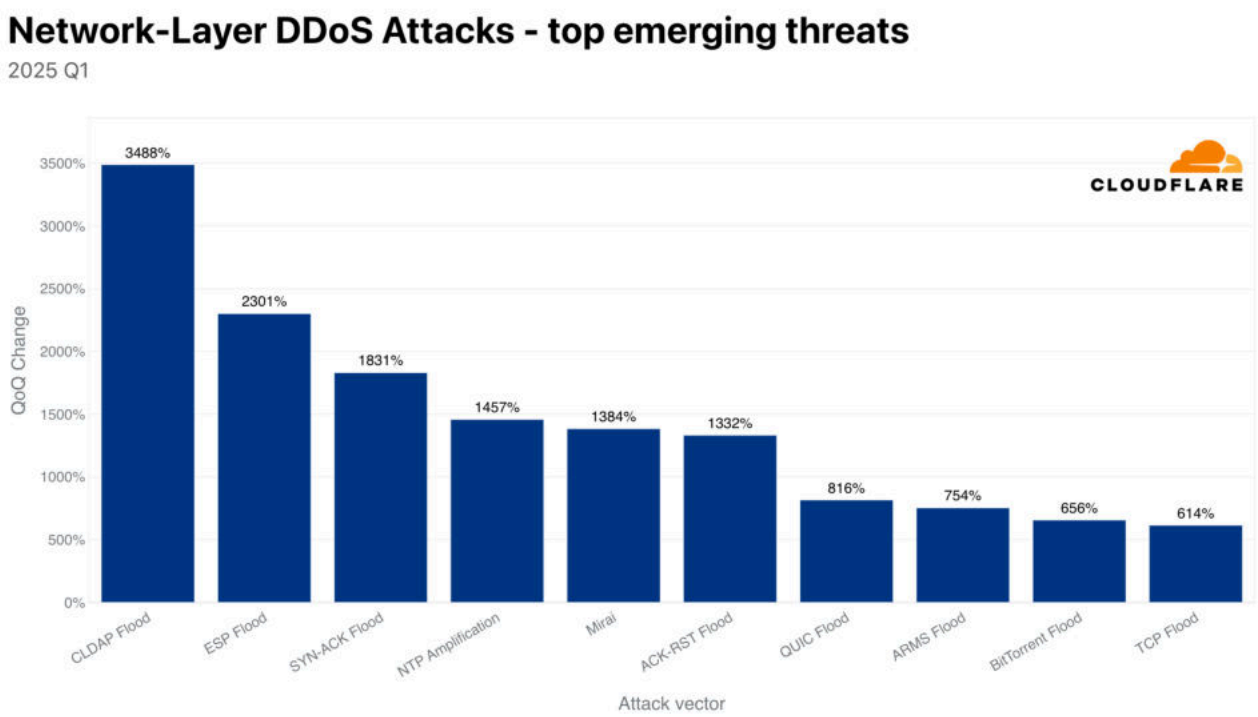
Op de netwerklaag is SYN flood nog steeds de meestvoorkomende Layer 3/4 DDoS-aanvalsvector, gevolgd door DNS flood-aanvallen. Door Mirai gelanceerde DDoS-aanvallen staan nu op de derde plaats en vervangen daarmee UDP flood-aanvallen.



Wat HTTP betreft werd meer dan 60% van de aanvallen geïdentificeerd en geblokkeerd als bekende botnets. 21% bestond uit aanvallen met verdachte HTTP-attributen, nog eens 10% werd gelanceerd door botnets die zich voordeden als browsers en de resterende 8% bestond uit generieke floods, aanvallen met ongebruikelijke verzoekpatronen en cache busting-aanvallen.



In Q1 2025 zagen we een stijging van 3488% op kwartaalbasis van het aantal CLDAP-reflection/amplification attacks. CLDAP (Connectionless Lightweight Directory Access Protocol) is een variant van LDAP (Lightweight Directory Access Protocol) en wordt gebruikt voor het opvragen en wijzigen van directoryservices die via IP-netwerken worden uitgevoerd. CLDAP is verbindingsloos en gebruikt UDP in plaats van TCP. Hierdoor is het sneller maar minder betrouwbaar. Aangezien UDP wordt gebruikt, is er geen handshake-vereiste. Hierdoor kunnen aanvallers het bron IP-adres vervalsen en dit vervolgens als een reflectievector misbruiken. Bij deze aanvallen worden kleine zoekopdrachten verzonden met een vervalst bron-IP-adres (het IP-adres van het slachtoffer). Hierdoor sturen servers grote antwoorden naar het slachtoffer, waardoor het slachtoffer overbelast raakt. De mitigatie bestaat uit het filteren en bewaken van ongebruikelijk CLDAP-verkeer.

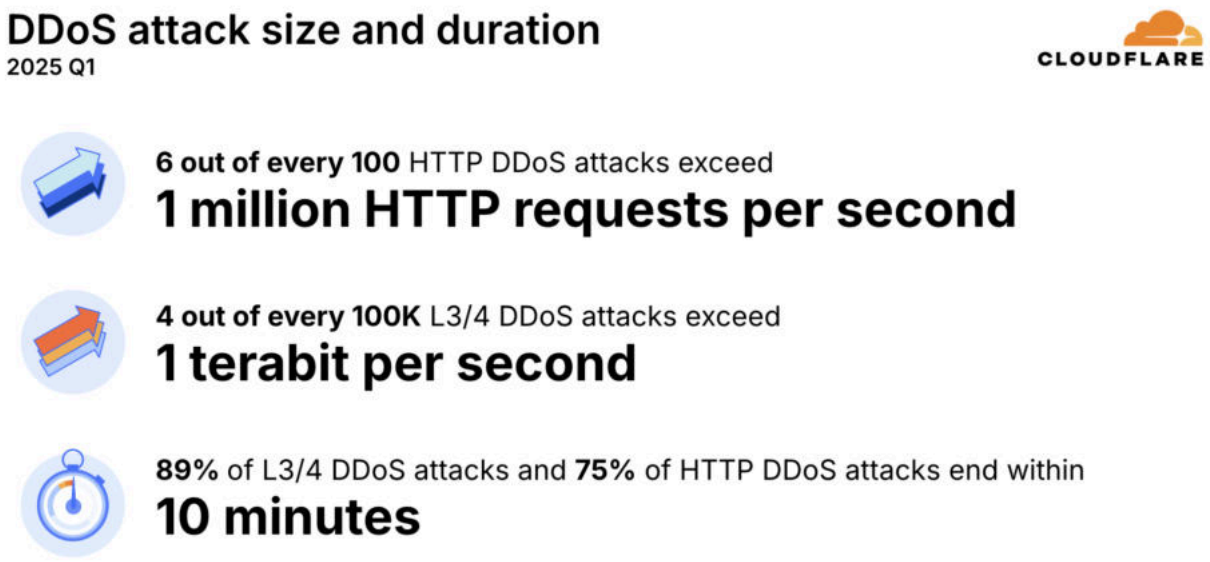


We zagen ook een toename van 2301% op kwartaalbasis van het aantal ESP-reflection/amplification attacks. Het ESP-protocol (Encapsulating Security Payload) is onderdeel van IPsec en levert vertrouwelijkheid, authenticatie en integriteit voor netwerkcommunicatie. Er kan echter misbruik van worden gemaakt voor DDoS-aanvallen, als kwaadwillenden misbruik maken van verkeerd geconfigureerde of kwetsbare systemen om het verkeer naar een bepaald doelwit te versterken of te spiegelen, wat leidt tot verstoring van de dienstverlening. Net als bij andere protocollen is het beveiligen en correct configureren van de systemen die ESP gebruiken van essentieel belang om de risico's van DDoS-aanvallen te blokkeren.

Ondanks de toename van de hypervolumetrische aanvallen, zijn de meeste DDoS-aanvallen klein. In Q1 2025 hadden 99% van de Layer 3/4 DDoS-aanvallen een snelheid van minder dan 1 Gbps en 1 Mpps. Evenzo bestond 94% van de HTTP DDoS-aanvallen uit 1 miljoen verzoeken per seconde (rps). Maar 'klein' is een relatief begrip. De meeste Internet property's zijn niet bestand tegen zelfs dergelijke kleine aanvallen. Ze kunnen onbeschermde internetlinks gemakkelijk verzadigen en onbeschermde servers laten crashen.

Bovendien duren de meeste aanvallen maar heel kort. 89% van de Layer 3/4 DDoS-aanvallen en 75% van de HTTP DDoS-aanvallen eindigen binnen 10 minuten. Zelfs de grootste, recordbrekende, hypervolumetrische DDoS-aanvallen kunnen van heel korte duur zijn, zoals de 35 seconden durende aanval in de bovenstaande voorbeelden. 35 seconden of zelfs 10 minuten is onvoldoende tijd voor handmatige mitigatie of het activeren van een on-demand oplossing: tegen de tijd dat een beveiligingsanalist de waarschuwing ontvangt en de aanval analyseert, is de aanval al voorbij. En ook al duren de aanvallen maar kort, het druppeleffect van de aanval kan tot netwerk- en

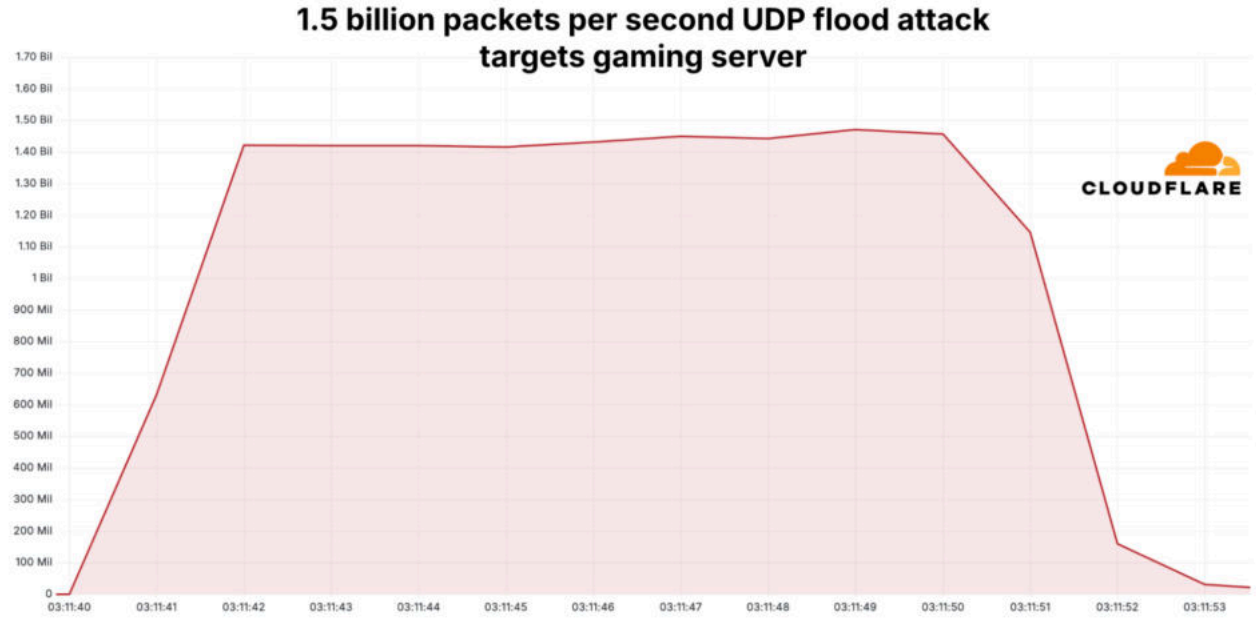
applicatiestoringen veroorzaken. Het herstel kan dagen duren, terwijl de services uit de lucht zijn of minder goed functioneren. Het huidige dreigingslandschap maakt menselijk ingrijpen onmogelijk. Detectie en mitigatie moeten altijd actief, geïntegreerd en geautomatiseerd zijn, met voldoende capaciteit en wereldwijde dekking om zowel het aanvalsverkeer als het legitieme piekverkeer te kunnen verwerken.



Anderzijds is het aantal hypervolumetrische HTTP DDoS-aanvallen van meer dan 1 Mrps verdubbeld. In Q1 2025 waren 6 van de 100 HTTP DDoS-aanvallen sneller dan 1 Mrps. Op netwerkniveau was 1 op de 100.000 aanvallen sneller dan 1 Tbps of 1 Bpps.

Een van dit soort aanvallen was gericht op een Cloudflare Magic Transit-klant. De klant zelf is een Amerikaanse hostingprovider die onder andere webservers, Voice over IP (VOIP)-servers en gameservers levert. Deze specifieke aanval was gericht op poort 27015. Deze port wordt meestal geassocieerd met multiplayer-gamingservers, vooral games die gebruikmaken van Valve's source engine, zoals Counter-Strike: Global Offensive (CS:GO), Team Fortress 2, Garry's Mod, Left 4 Dead en Half-Life 2: Deathmatch.

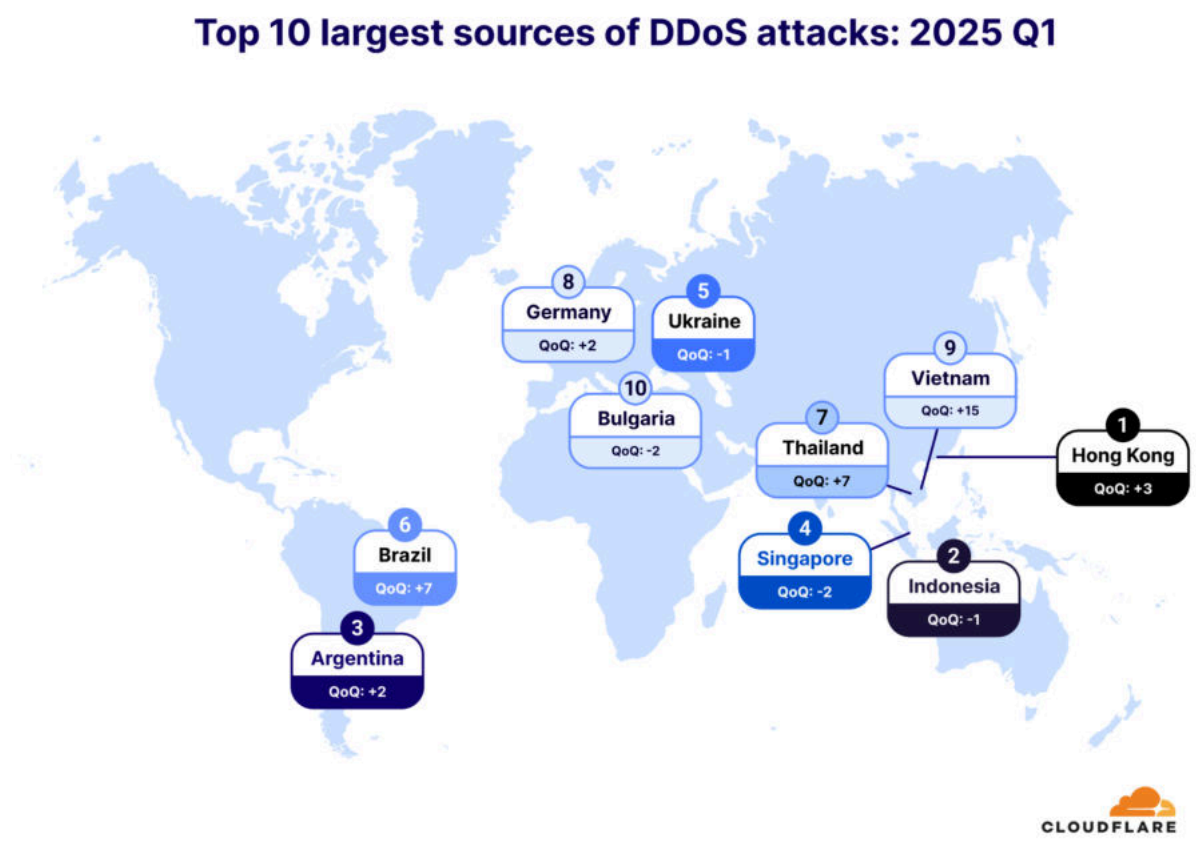
De poort wordt gebruikt voor de verbinding met de gameserver, zodat clients verbinding kunnen maken met de server om online te spelen. Vaak is deze poort open voor zowel UDP als TCP, afhankelijk van de game en het soort communicatie dat plaatsvindt. Deze klant werd het doelwit van meerdere hypervolumetrische aanvallen die autonoom door Cloudflare werden geblokkeerd.



Tijdens het eerste kwartaal van 2025 vond er een aanzienlijke verschuiving plaats in de top 10 van de meest aangevallen landen overal ter wereld. Duitsland maakte een opmerkelijke sprong en steeg vier plaatsen. Daarmee is dat nu het meest aangevallen land. Op de tweede plaats staat Turkije dat nu ook ineens 11 plaatsen hoger staat. Op de derde plaats staat China. Dit land zakte twee plaatsen ten opzichte van het voorgaande kwartaal, terwijl Hongkong onveranderd bleef. India staat nu vier plaatsen hoger, terwijl Brazilië gelijk bleef. Taiwan daalde vier plaatsen. De Filipijnen ondergingen de grootste daling met 6 plaatsen. Zuid-Korea en Indonesië stegen echter allebei met twee plaatsen.

De top 10 van meest aangevallen sectoren tijdens Q1 2025 vertoonde een aantal opvallende veranderingen. De gok- en casinobranche steeg vier plaatsen op de ranglijst van meest aangevallen sectoren, terwijl de telecommunicatie-, serviceprovider- en carriersector één plaats zakte. De informatietechnologie en -dienstensector en de internetsector vertoonden kleine schommelingen, met respectievelijk een stijging en een daling van twee plaatsen. De gamingsector en de sector voor bank- en financiële dienstverlening zijn allebei één plaats gestegen, terwijl de cyberbeveiligingsector een enorme sprong van 37 plaatsen maakte ten opzichte van het voorgaande kwartaal. De detailhandel daalde één plaats, terwijl de productiee, machine-, technologie- en engineeringsector nu 28 plaatsen hoger staat. De luchtvaart- en ruimtevaartsector maakte de grootste sprong van allemaal. Deze sector steeg met 40 plaatsen en was daarmee de tiende meest aangevallen sector.

De rangschikking van de 10 grootste bronnen van DDoS-aanvallen in Q1 2025 is ook aanzienlijk veranderd. Hongkong schoot naar de eerste plaats en steeg drie plaatsen ten opzichte van het voorgaande kwartaal. Indonesië zakte naar de tweede plaats, terwijl Argentinië twee plaatsen naar de derde plaats steeg. Singapore zakte twee plaatsen naar de vierde plaats en Oekraïne zakte één plaats naar de vijfde plaats. Brazilië maakte een opvallende sprong en steeg zeven plaatsen naar de zesde plaats, op de voet gevolgd door Thailand, dat ook zeven plaatsen naar de zevende plaats steeg. Ook Duitsland is gestegen en staat nu op de achtste plaats. Vietnam maakte de meest dramatische stijging door: dit land steeg 15 plaatsen en staat nu op de negende plaats. Tot slot zakte Bulgarije twee plaatsen naar de tiende plaats.

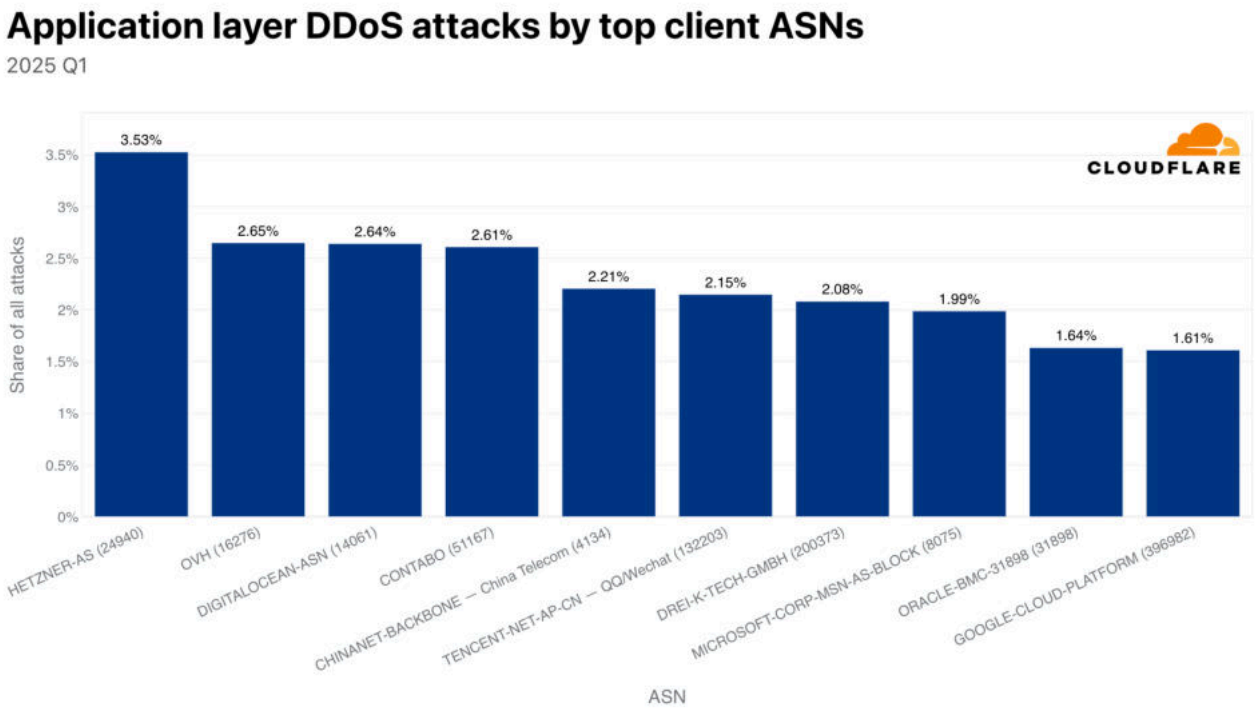


Een ASN (autonoom systeemnummer) is een uniek nummer dat wordt toegewezen aan een netwerk of een groep IP-netwerken die volgens één routingbeleid op internet actief zijn. Een ASN wordt gebruikt om routinginformatie tussen systemen uit te wisselen met behulp van protocollen zoals BGP (Border Gateway Protocol).

Wanneer gekeken wordt naar de oorsprong van DDoS-aanvallen, specifiek HTTP DDoS-aanvallen, vallen een aantal autonome systemen op. In Q1 2025 was het Duitse bedrijf Hetzner (AS24940) nog steeds grootste bron van HTTP DDoS-aanvallen. Het werd gevolgd door het Franse OVH (AS16276) op de tweede plaats, het Amerikaanse DigitalOcean (AS14061) op de derde plaats en een andere Duitse provider, Contabo (AS51167), op de vierde plaats.

Andere grote bronnen waren het in China gevestigde ChinaNet Backbone (AS4134) en Tencent (AS132203), het in Oostenrijk gevestigde Drei (AS200373) en drie in de VS gevestigde providers die de top 10 compleet maken: Microsoft (AS8075), Oracle (AS31898) en Google Cloud Platform (AS396982). De meeste netwerken op deze ranglijst zijn bekende cloudcomputing- of hostingproviders. Dit onderstreept hoe vaak cloudinfrastructuur wordt misbruikt – opzettelijk of door uitbuiting – om DDoS-aanvallen uit te voeren.

Om hostingproviders, cloudcomputing-providers en alle internetproviders te helpen bij het identificeren en verwijderen van de accounts die dergelijke aanvallen uitvoeren, maken we gebruik van Cloudflare's unieke positie om een gratis DDoS-botnetdreigingsfeed voor serviceproviders te leveren. Wereldwijd hebben meer dan 600 organisaties zich al voor deze feed aangemeld. Het geeft serviceproviders een lijst met IP-adressen binnen hun Autonoom Systeemnummer (ASN) die HTTP DDoS-aanvallen uitvoeren. De feed is helemaal gratis. Het enige wat je moet doen is een gratis Cloudflare-account openen, het ASN verifiëren via PeeringDB en vervolgens de dreigingsinformatie ophalen via API.



Bij Cloudflare is het onze missie om een beter internet te bouwen. Een belangrijk onderdeel van deze inzet is het aanbieden van gratis bescherming tegen DDoS-aanvallen. Ook ondersteunen we de bredere internetgemeenschap door gratis tools beschikbaar te stellen waarmee andere netwerken botnets kunnen detecteren en ontmantelen die binnen hun infrastructuur actief zijn.

Naarmate het dreigingslandschap zich verder ontwikkelt, zien we dat veel organisaties DDoS-bescherming pas implementeren nadat ze zijn aangevallen, of dat ze nog steeds op verouderde, on-demand-oplossingen vertrouwen. Uit onze gegevens blijkt dat mensen met proactieve beveiligingsstrategieën daarentegen veel veerkrachtiger zijn. Daarom richten wij ons op automatisering en een uitgebreide, altijd actieve, inline beveiligingsaanpak om zowel bestaande als nieuwe dreigingen voor te blijven.

Dankzij ons wereldwijde netwerk met een capaciteit van 348 Tbps in 335 steden blijven we ons inzetten om onbeperkte DDoS-bescherming te bieden, ongeacht de omvang, duur of frequentie van de aanvallen.