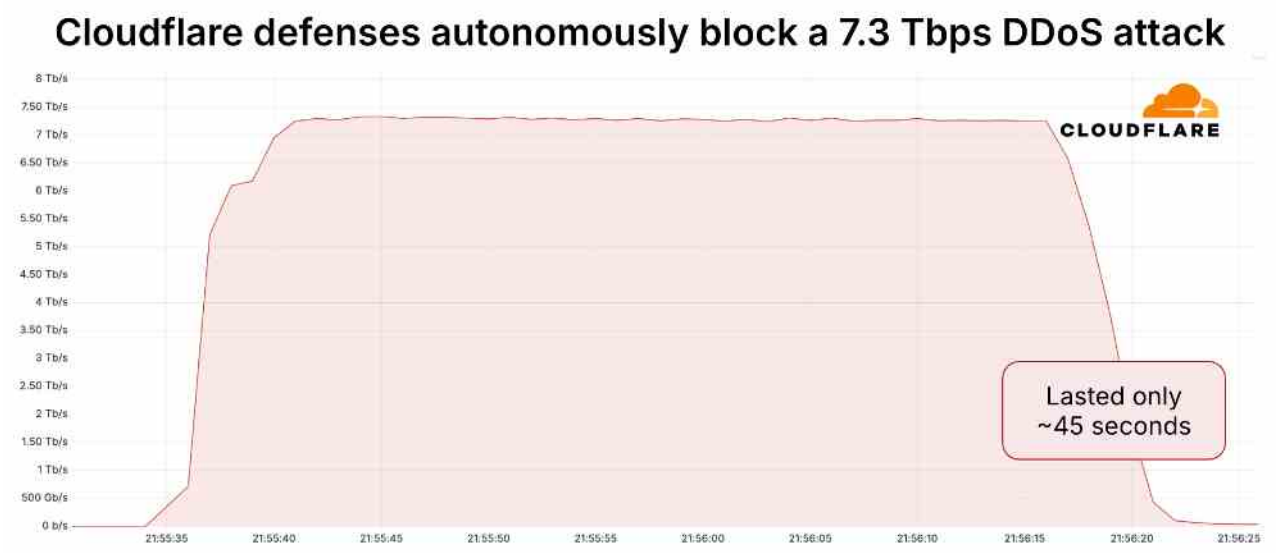
Het internet verdedigen: hoe Cloudflare een monumentale DDoS-aanval van 7,3 Tbps blokkeerde

blog.cloudflare.com/nl-nl/defending-the-internet-how-cloudflare-blocked-a-monumental-7-3-tbps-ddos

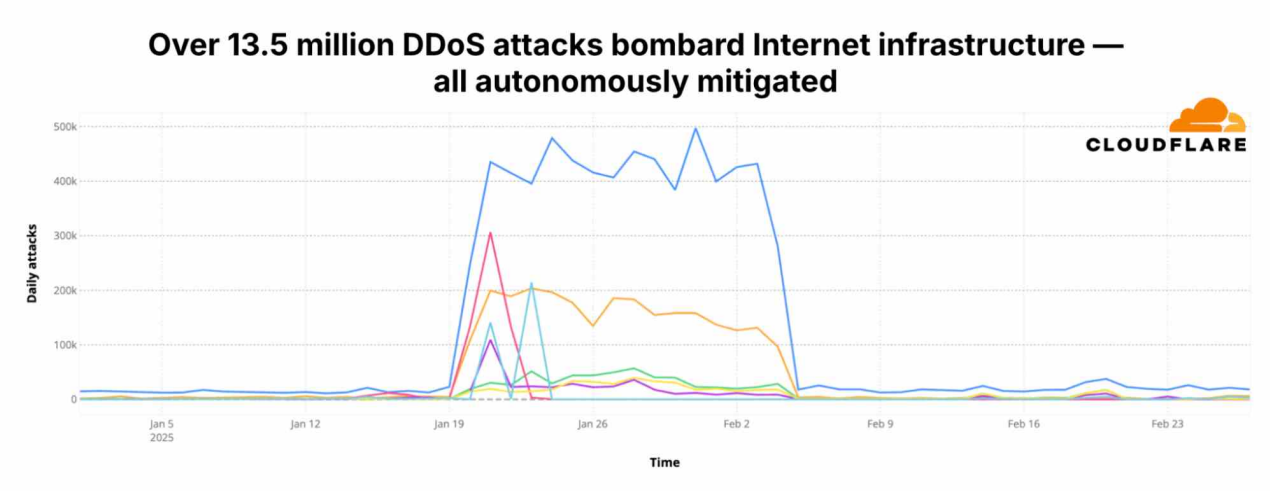
19 juni 2025

Medio mei 2025 blokkeerde Cloudflare de grootste DDoS-aanval ooit gemeten: een verbluffende 7,3 terabit per seconde (Tbps). Dit volgt kort op de publicatie van ons DDoS-bedreigingsrapport voor het eerste kwartaal van 2025, op 27 april 2025. Daarin noemden we aanvallen met een snelheid van 6,5 Tbps en 4,8 miljard pakketten per seconde (pps). De 7,3 Tbps-aanval is 12% groter dan ons vorige record en 1 Tbps groter dan een recente aanval waarover cyberbeveiligingsverslaggever Brian Krebs van KrebsOnSecurity berichtte.



Nieuw wereldrecord: 7,3 Tbps DDoS-aanval autonoom geblokkeerd door Cloudflare

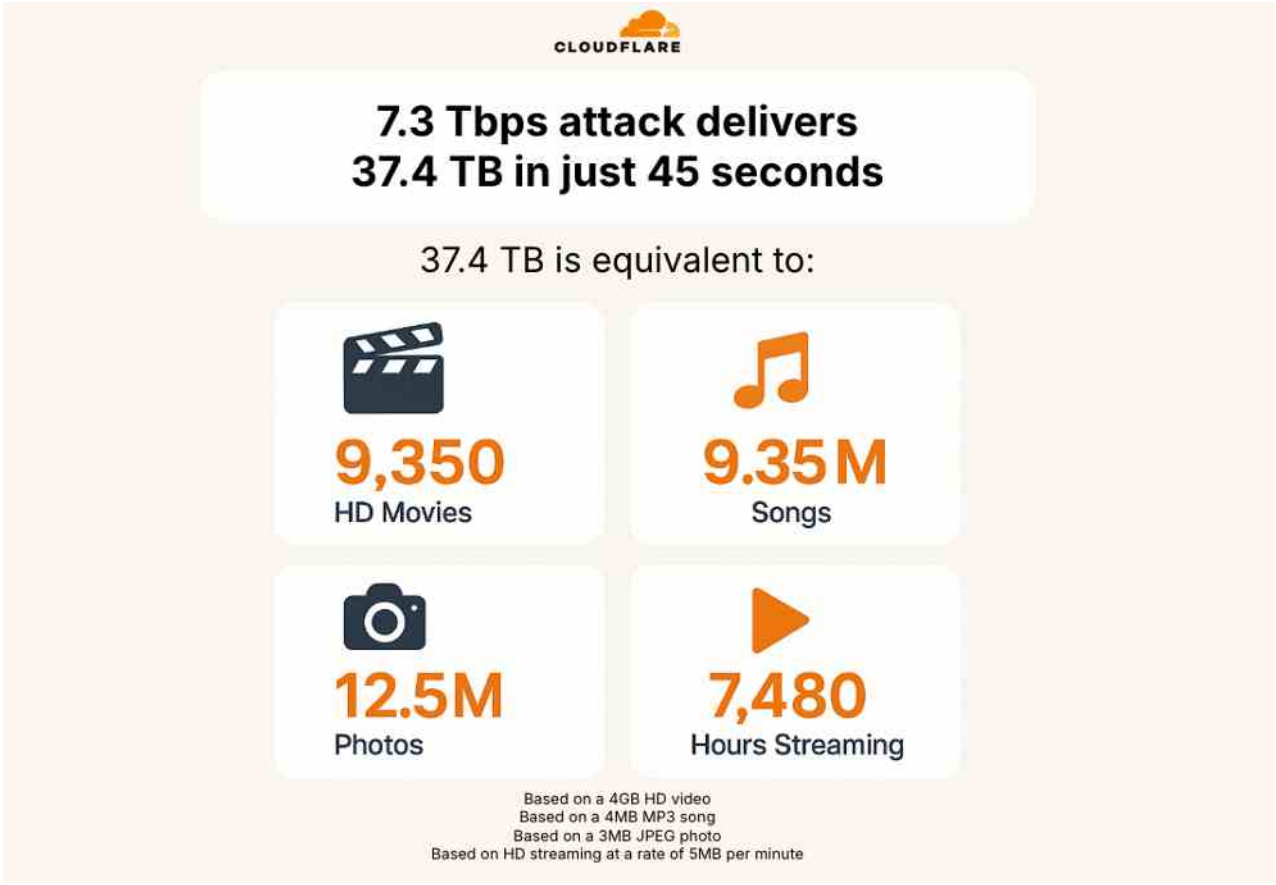
De aanval was gericht op een Cloudflare-klant, een hostingprovider die Magic Transit gebruikt om zijn IP-netwerk te verdedigen. Hostingproviders en belangrijke Internetinfrastructuur zijn steeds vaker het doelwit van DDoS-aanvallen, zoals we meldden in ons nieuwste DDoS-dreigingsrapport. Hieronder zie je een aanvalscampagne uit januari en februari 2025, waarbij meer dan 13,5 miljoen DDoS-aanvallen werden uitgevoerd op de infrastructuur van Cloudflare en de hostingproviders die door Cloudflare werden beschermd.



DDoS-aanvalscampagne richt zich op Cloudflare-infrastructuur en hostingproviders die door Cloudflare worden beschermd

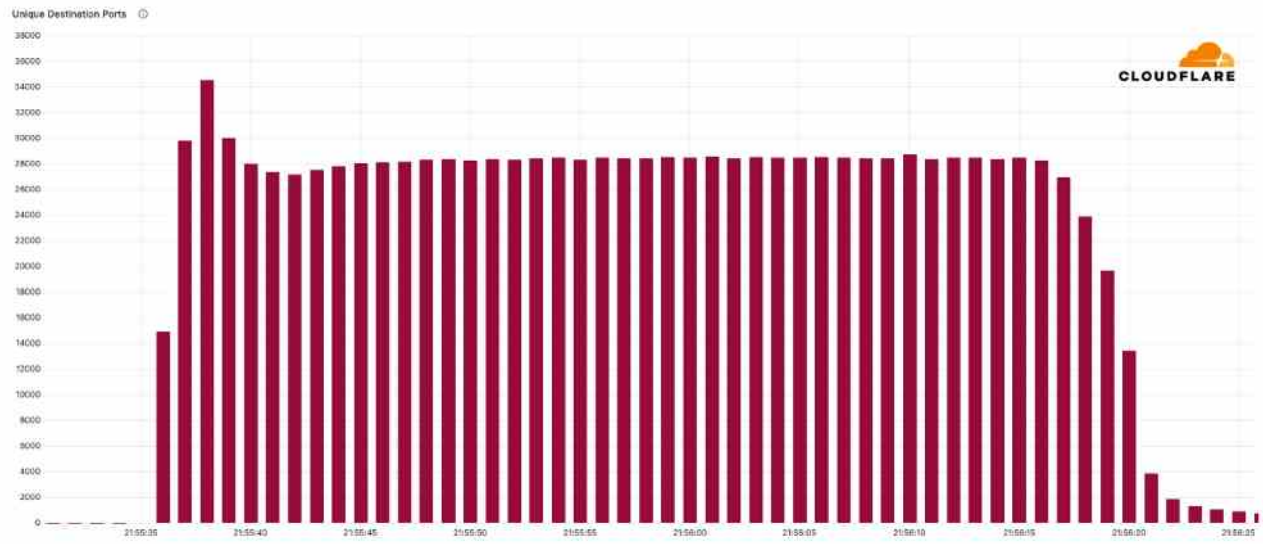
Laten we beginnen met enkele cijfers en daarna kijken we hoe onze systemen deze aanval hebben gedetecteerd en bestreden.

37,4 terabyte is tegenwoordig geen schokkend getal, maar 37,4 terabyte in slechts 45 seconden verzetten is dat wel. Het staat gelijk aan het overspoelen van je netwerk met meer dan 9.350 volledige HD-films, of het non-stop streamen van 7.480 uur aan high-definition video (dat is bijna een jaar lang achter elkaar kijken) in slechts 45 seconden. Als het muziek was, zou je in minder dan een minuut ongeveer 9,35 miljoen nummers downloaden. Genoeg om een listener 57 jaar lang te vermaken. Stel je voor dat je 12,5 miljoen foto's met een hoge resolutie kunt maken met je smartphone en dat je nooit zonder opslagruimte komt te zitten. Zelfs als je elke dag maar één foto zou maken, zou je 4000 jaar bezig zijn met het maken van foto's, maar dan wel in 45 seconden.



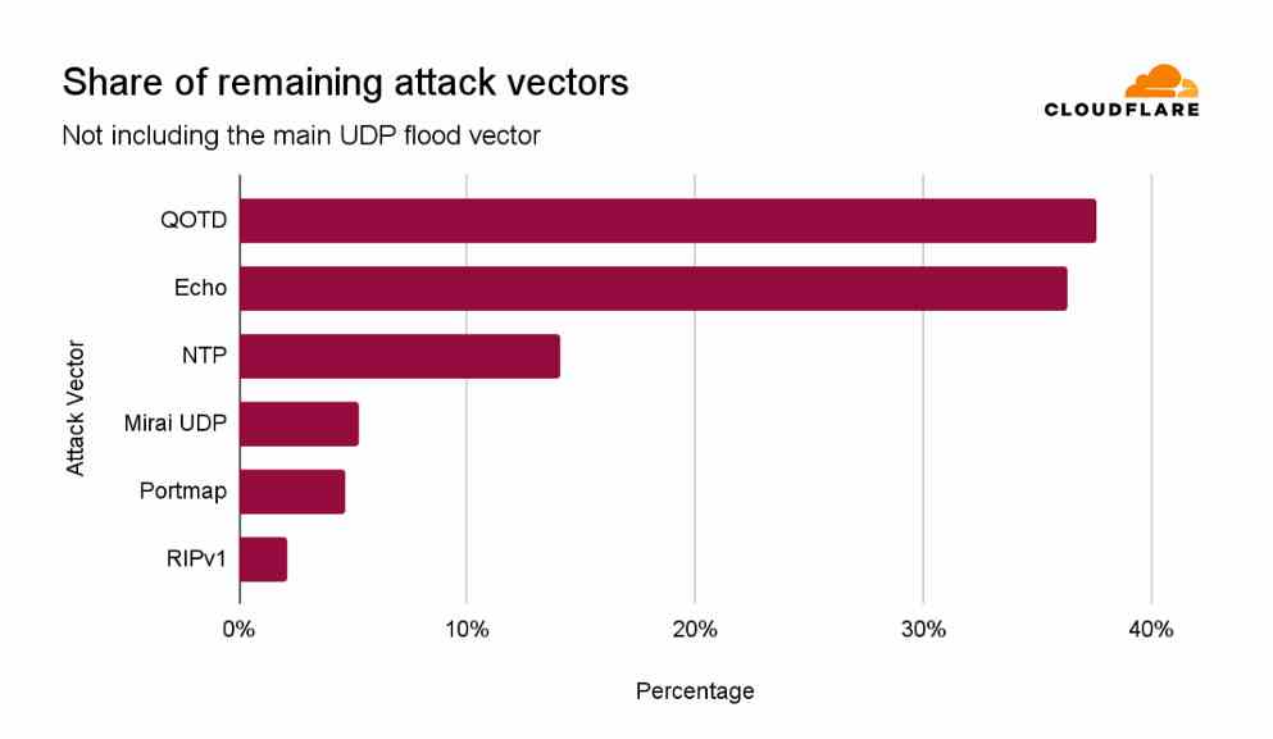
De recordbrekende DDoS-aanval van 7,3 Tbps leverde 37,4 TB in 45 seconden

Bij de aanval werden gemiddeld 21.925 bestemmingspoorten van één IP-adres, dat eigendom is van en wordt gebruikt door onze klant, gebombardeerd, met een piek van 34.517 bestemmingspoorten per seconde. De aanval vond ook plaats via een vergelijkbare verdeling van bronpoorten.



Verdeling van bestemmingspoorten

De 7,3 Tbps-aanval was een multivector DDoS-aanval. Ongeveer 99,996% van het aanvalsverkeer werd gecategoriseerd als UDP-floods. De resterende 0,004%, goed voor 1,3 GB van het aanvalsverkeer, werd geïdentificeerd als QOTD-reflectie-aanvallen, Echo-reflectie-aanvallen, NTP-reflectie-aanvallen, Mirai UDP-flood-aanvallen, Portmap-flood-aanvallen en RIPv1 amplification attacks.



De aanvalsvectoren naast de UDP-floods

Hieronder vind je informatie over de verschillende aanvalsvectoren die bij deze aanval voorkomen, hoe organisaties kunnen voorkomen dat ze deelnemen aan reflectie en versterking, en hoe je je tegen deze aanvallen kunt verdedigen zonder dat dit gevolgen heeft voor legitiem verkeer. Klanten van Cloudflare zijn beschermd tegen deze aanvallen.

UDP DDoS-aanval

- **Type**: Flood
- **Werkwijze:** Een groot volume aan UDP-pakketten wordt verzonden naar willekeurige of specifieke poorten op de doel-IP-adressen. Ze kunnen proberen de Internetverbinding te verzadigen of de aangesloten apparaten te overbelasten met meer pakketten dan het kan verwerken.
- **Zo verdedig je je tegen de aanval:** implementeer cloudgebaseerde volumetrische DDoS-bescherming, pas slimme rate limiting toe op UDP-verkeer en verwijder ongewenst UDP-verkeer volledig.

- **Hoe je onbedoelde gevolgen kunt voorkomen:** Agressieve filtering kan legitieme UDP-services zoals VoIP, videoconferenties en online games verstoren. Pas drempels zorgvuldig toe.

QOTD DDoS-aanval

- **Type:** Reflectie + Versterking
- **Werkwijze:** Maakt misbruik van het Quote of the Day (QOTD) Protocol, dat luistert op UDP-poort 17 en reageert met een kort citaat of bericht. Aanvallers sturen QOTD-verzoeken naar blootgestelde servers vanaf een vervalst IP-adres, waardoor het slachtoffer steeds sterkere reacties krijgt.
- **Voorkom dat je een reflectie-/versterkingselement wordt:** schakel de QOTD-service uit en blokkeer UDP/17 op alle servers en firewalls.
- **Zo verdedig je je tegen de aanval:** blokkeer binnenkomende UDP/17. Verwijder abnormale pieken in kleine UDP-pakketten.
- **Hoe je onbedoelde gevolgen kunt voorkomen:** QOTD is een verouderd diagnostisch/debugprotocol en wordt niet meer gebruikt door moderne toepassingen. Het uitschakelen hiervan zou geen negatieve gevolgen voor legitieme services mogen hebben.

Echo DDoS-aanval

- **Type:** Reflectie + Versterking
- **Werkwijze:** Maakt gebruik van het Echo-protocol (UDP/TCP-poort 7), dat antwoordt met dezelfde gegevens die het ontvangt. Aanvallers vervalsen het IP-adres van het slachtoffer, waardoor apparaten de gegevens kopiëren en de aanval sterker wordt.
- **Voorkom dat het een reflectie-/versterkingselement wordt:** Schakel de Echo-service uit op alle apparaten. Blokkeer UDP/TCP-poort 7 aan de rand.
- **Zo verdedig je je tegen de aanval:** schakel de Echo-service uit en blokkeer TCP/UDP-poort 7 aan de netwerkperimeter.
- **Hoe je onbedoelde gevolgen kunt voorkomen:** Echo is een verouderd diagnostisch hulpmiddel. Het uitschakelen of blokkeren ervan heeft geen negatieve gevolgen voor moderne systemen.

NTP DDoS-aanval

- **Type:** Reflectie + Versterking

- **Werkwijze:** Maakt misbruik van het Network Time Protocol (NTP), dat wordt gebruikt om klokken via internet te synchroniseren. Aanvallers misbruiken het commando monlist op oude NTP-servers (UDP/123), dat een grote lijst met recente verbindingen retourneert. Vervalste verzoeken veroorzaken versterkte reflecties.
- **Voorkom dat het een reflectie-/versterkingselement wordt:** Werk de NTP-servers bij of configureer ze om monlist uit te schakelen. Beperk NTP-query's tot vertrouwde IP-adressen.
- **Zo verdedig je je tegen de aanval:** schakel het monlist-commando uit, werk de NTP-software bij en filter of beperk het UDP/123-verkeer.
- **Hoe je onbedoelde gevolgen kunt voorkomen:** het uitschakelen van monlist heeft geen effect op de tijdsynchronisatie. Het filteren of blokkeren van UDP/123 kan echter van invloed zijn op de tijdsynchronisatie als dit te algemeen wordt gedaan. Zorg ervoor dat alleen niet-vertrouwde of externe bronnen worden geblokkeerd.

Mirai UDP-aanval

- **Type:** Flood
- **Werkwijze:** Het Mirai-botnet, dat bestaat uit gecompromitteerde IoT-apparaten, overspoelt slachtoffers met willekeurige of servicespecifieke UDP-pakketten (bijvoorbeeld DNS, gameservices).
- **Voorkom dat je onderdeel wordt van een botnet:** beveilig je IoT-apparaten, wijzig de standaardwachtwoorden, upgrade naar de nieuwste firmwareversies en volg de best practices voor IoT-beveiliging om te voorkomen dat je onderdeel wordt van een botnet. Controleer indien mogelijk het uitgaande verkeer om onregelmatigheden te detecteren.
- **Zo verdedig je je tegen de aanval:** implementeer cloudgebaseerde volumetrische DDoS-bescherming en rate limiting voor UDP-verkeer.
- **Hoe je onbedoelde gevolgen kunt voorkomen:** Zorg er allereerst voor dat je inzicht hebt in je netwerk en het type verkeer dat je ontvangt, met name de protocollen, hun bronnen en hun bestemmingen. Bepaal welke services via UDP worden uitgevoerd en die je niet wilt beïnvloeden. Zodra je deze eindpunten hebt geïdentificeerd, kun je rate limiting toepassen. Deze beperkingen worden toegepast op de eindpunten, of op de normale verkeersniveaus. Anders kan agressief rate limiting van UDP-verkeer een impact hebben op je legitieme verkeer en op services die via UDP lopen, zoals VoIP-gesprekken en VPN-verkeer.

Portmap DDoS-aanval

- **Type:** Reflectie + Versterking

- **Werkwijze:** richt zich op de Portmapper-service (UDP/111) die door Remote Procedure Call (RPC)-toepassingen wordt gebruikt om beschikbare services te identificeren. Vervalste verzoeken resulteren in gereflecteerde reacties.
- **Voorkom dat het een reflectie-/versterkingselement wordt:** schakel de Portmapper-service uit als deze niet nodig is. Indien je ze intern nodig hebt, beperk het gebruik dan tot vertrouwde IP-adressen.
- **Zo verdedig je je tegen de aanval:** schakel de Portmapper-service uit als deze niet nodig is en blokkeer binnenkomend UDP/111-verkeer. Gebruik toegangscontrolelijsten (ACL's) of firewalls om de toegang tot bekende RPC-services te beperken.
- **Hoe je onbedoelde gevolgen kunt voorkomen:** het uitschakelen van Portmapper kan de werking van toepassingen verstoren die afhankelijk zijn van RPC (bijvoorbeeld het Network File System-protocol). Valideer serviceafhankelijkheden voordat je het verwijdert.

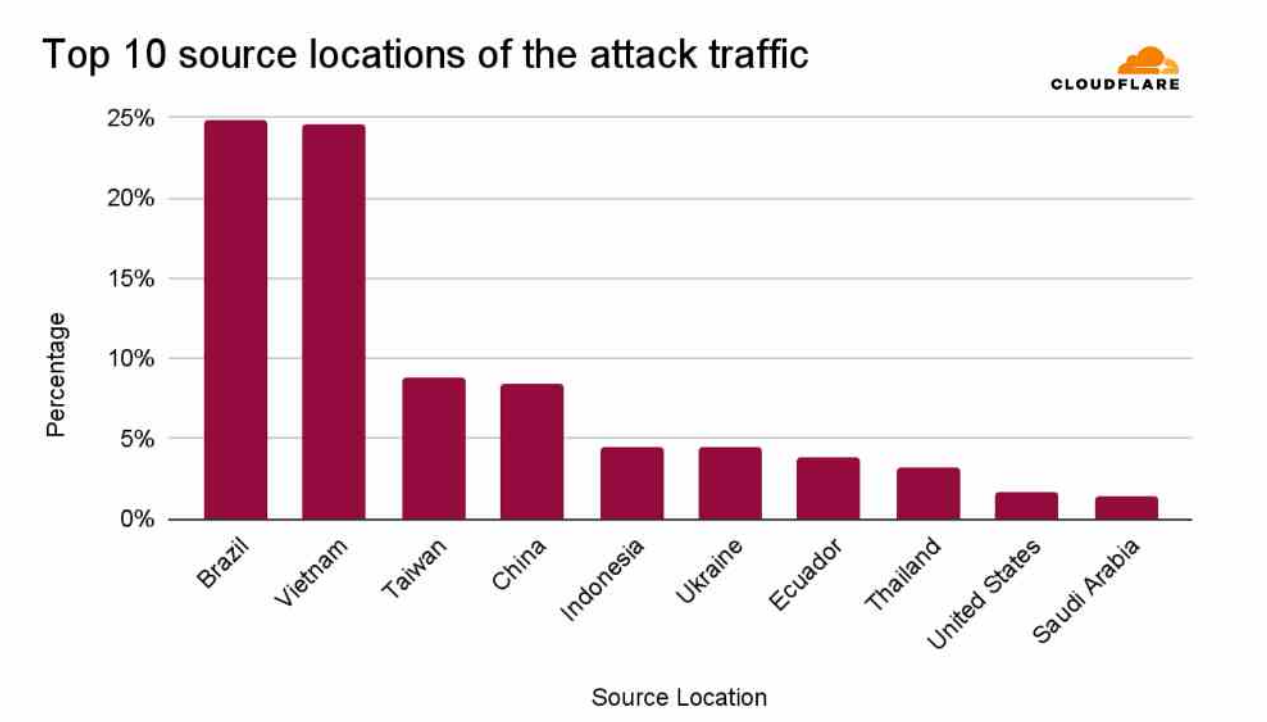
RIPv1 DDoS-aanval

- **Type:** Reflectie + (lage) versterking
- **Werkwijze:** Maakt gebruik van het Routing Information protocol versie 1 (RIPv1), een oud, niet-geverifieerd afstandsvector-routingsprotocol dat UDP/520 gebruikt. Aanvallers versturen vervalste routingupdates om netwerken te overspoelen of te verwarren.
- **Voorkom dat het een reflectie-/versterkingselement wordt:** schakel RIPv1 uit op routers. Gebruik RIPv2 met authenticatie wanneer routing nodig is.
- **Zo verdedig je je tegen de aanval:** blokkeer binnenkomende UDP/520 van niet-vertrouwde netwerken. Controleer op onverwachte routingupdates.
- **Hoe je onbedoelde gevolgen kunt voorkomen:** RIPv1 is grotendeels verouderd; het uitschakelen ervan is over het algemeen veilig. Als oudere systemen hiervan afhankelijk zijn, valideer dan het routinggedrag voordat je wijzigingen aanbrengt.

Alle hier genoemde aanbevelingen moeten in acht worden genomen met de context en het gedrag van elk uniek netwerk of elke unieke toepassing om onbedoelde gevolgen voor legitiem verkeer te voorkomen.

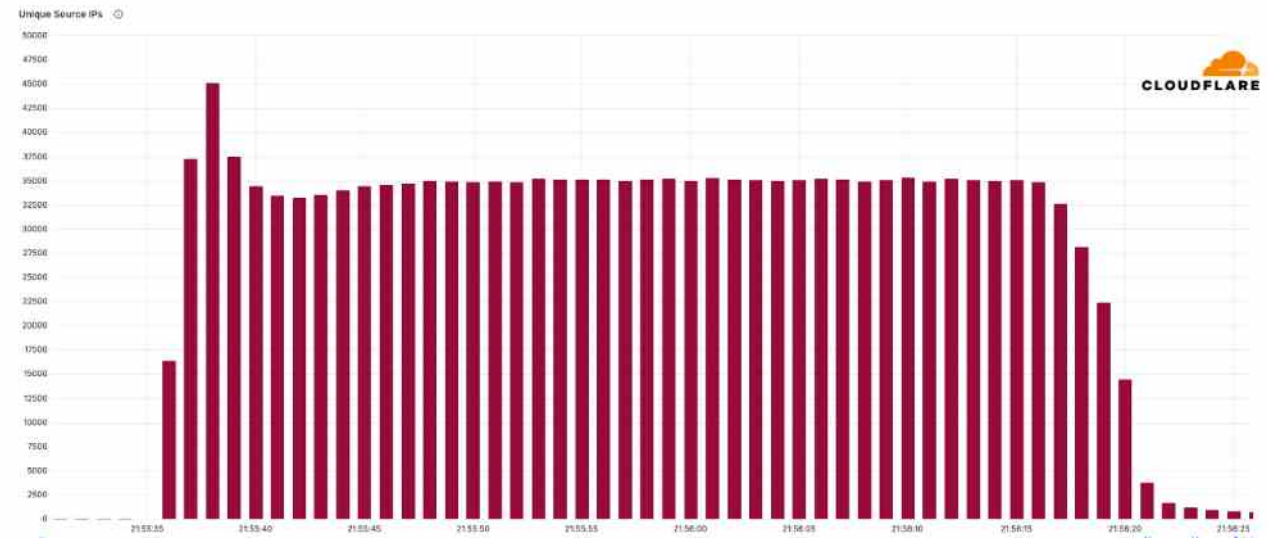
De aanval was afkomstig van meer dan 122.145 bron-IP-adressen verspreid over 5.433 autonome systemen (AS) in 161 landen.

Bijna de helft van het aanvalsverkeer was afkomstig uit Brazilië en Vietnam, met elk ongeveer een kwart. Een derde was afkomstig uit Taiwan, China, Indonesië, Oekraïne, Ecuador, Thailand, de Verenigde Staten en Saoedi-Arabië.



Top 10 bronlanden van het aanvalsverkeer

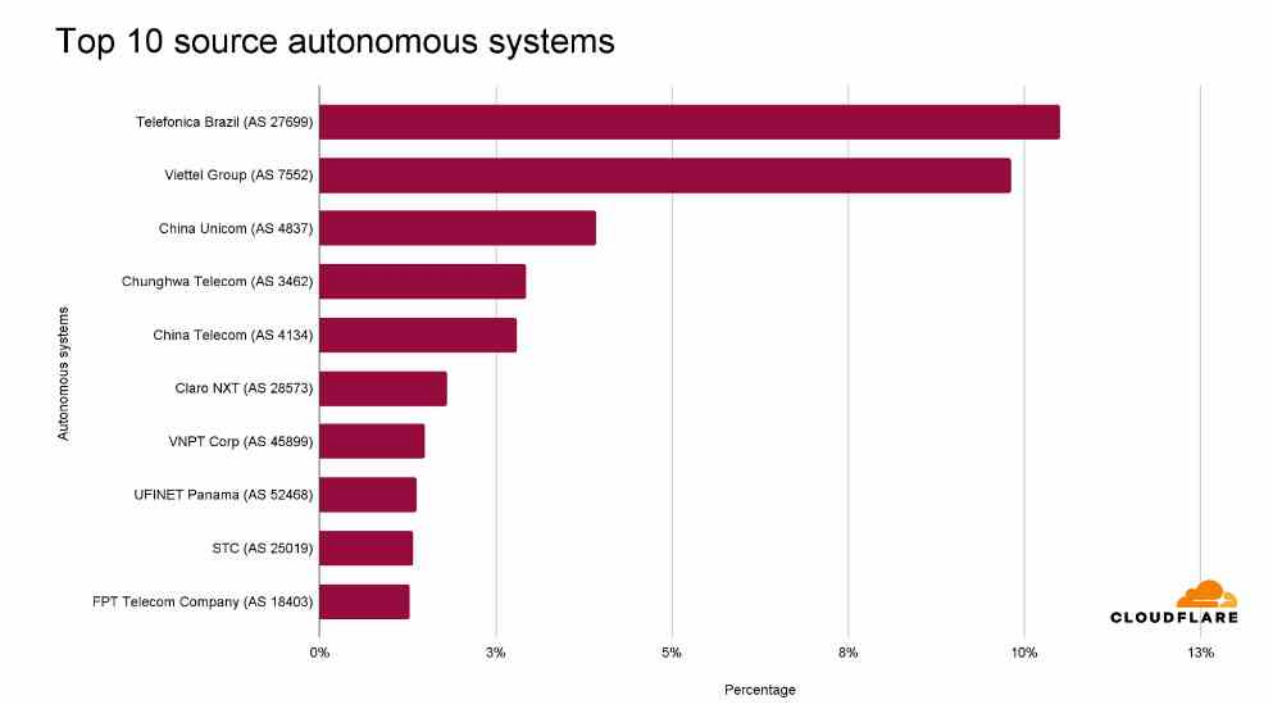
Het gemiddelde aantal unieke bron-IP-adressen per seconde bedroeg 26.855, met een piek van 45.097.



Verdeling van unieke bron-IP-adressen

De aanval was afkomstig van 5.433 verschillende netwerken (AS'en). Telefonica Brazil (AS27699) was verantwoordelijk voor het grootste deel van het DDoS-aanvalsverkeer, namelijk 10,5% van het totaal. Viettel Group (AS7552) volgt op de voet met 9,8%, terwijl China Unicom (AS4837) en Chunghwa Telecom (AS3462) respectievelijk 3,9% en 2,9%

bijdroegen. China Telecom (AS4134) was goed voor 2,8% van het verkeer. De overige ASN's in de top 10, waaronder Claro NXT (AS28573), VNPT Corp (AS45899), UFINET Panama (AS52468), STC (AS25019) en FPT Telecom Company (AS18403), droegen elk tussen de 1,3% en 1,8% bij aan het totale DDoS-aanvalsverkeer.



Top 10 bronnen autonome systemen

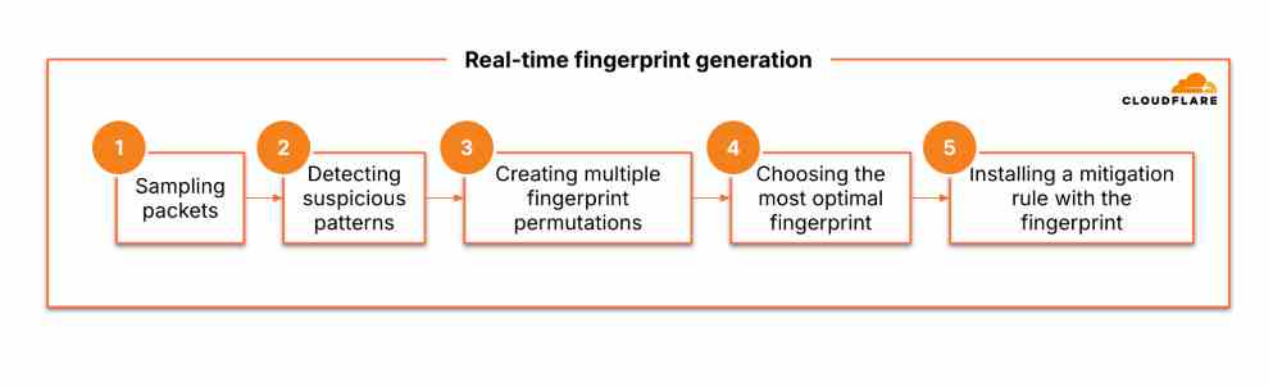
Om hostingproviders, cloudcomputing-providers en alle internetproviders te helpen bij het identificeren en verwijderen van de accounts die dergelijke aanvallen uitvoeren, maken we gebruik van Cloudflare's unieke positie om een gratis DDoS-botnetdreigingsfeed voor serviceproviders te leveren. Wereldwijd hebben meer dan 600 organisaties zich al voor deze feed aangemeld. Ze 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 feed ophalen via API.

Het aangevallen IP-adres werd geadverteerd vanuit het netwerk van Cloudflare met behulp van global anycast. Dit betekent dat de aanvalspakketten die het IP-adres targetten, naar het dichtstbijzijnde Cloudflare-datacenter werden geleid. Met global anycast kunnen we het aanvalsverkeer spreiden en het verdeelde karakter ervan tegen het verkeer gebruiken. Zo kunnen we de impact op botnetknooppunten beperken en gebruikers blijven bedienen vanuit de dichtstbijzijnde datacenters. Deze aanval werd gedetecteerd en bestreden in 477 datacenters verspreid over 293 locaties wereldwijd. Op locaties met veel dataverkeer zijn we aanwezig in meerdere datacenters.

Het wereldwijde netwerk van Cloudflare draait elke service in elk datacenter. Dit omvat onze DDoS-detectie- en bestrijdingssystemen. Dit betekent dat aanvallen volledig autonoom kunnen worden gedetecteerd en bestreden, ongeacht waar ze vandaan komen.

Wanneer een pakket ons datacenter binnenkomt, wordt het door middel van load balancing slim verdeeld naar een beschikbare server. Vervolgens nemen we monsters van pakketten rechtstreeks uit de diepten van de Linux-kernel, uit het *eXpress Data Path (XDP),* met behulp van een extended Berkley Packer Filter (eBPF) -programma om pakketmonsters naar de gebruikersruimte te routeren waar we de analyse uitvoeren.

Ons systeem analyseert de pakketmonsters om verdachte patronen te identificeren op basis van onze unieke heuristische engine genaamd *dosd* (denial of service daemon). Dosd zoekt naar patronen in de pakketmonsters, door bijvoorbeeld overeenkomsten te vinden in de pakketheadervelden en te zoeken naar pakketanomalieën. Daarnaast past Dosd andere bedrijfseigen technieken toe.



Stroomdiagram van de realtime vingerafdrukgeneratie

Voor onze klanten is dit complexe vingerafdruksysteem samengevat in een gebruiksvriendelijke groep *beheerde regels*: de DDoS-bescherming beheerde regelsets.

Wanneer dosd patronen detecteert, genereert het programma meerdere permutaties van die vingerafdrukken om de nauwkeurigste vingerafdruk te vinden die het meest effectief en nauwkeurig is in het bestrijden van aanvallen. Zo wordt geprobeerd om deze nauwkeurig te vergelijken met aanvalsverkeer zonder dat het legitieme verkeer wordt beïnvloed.

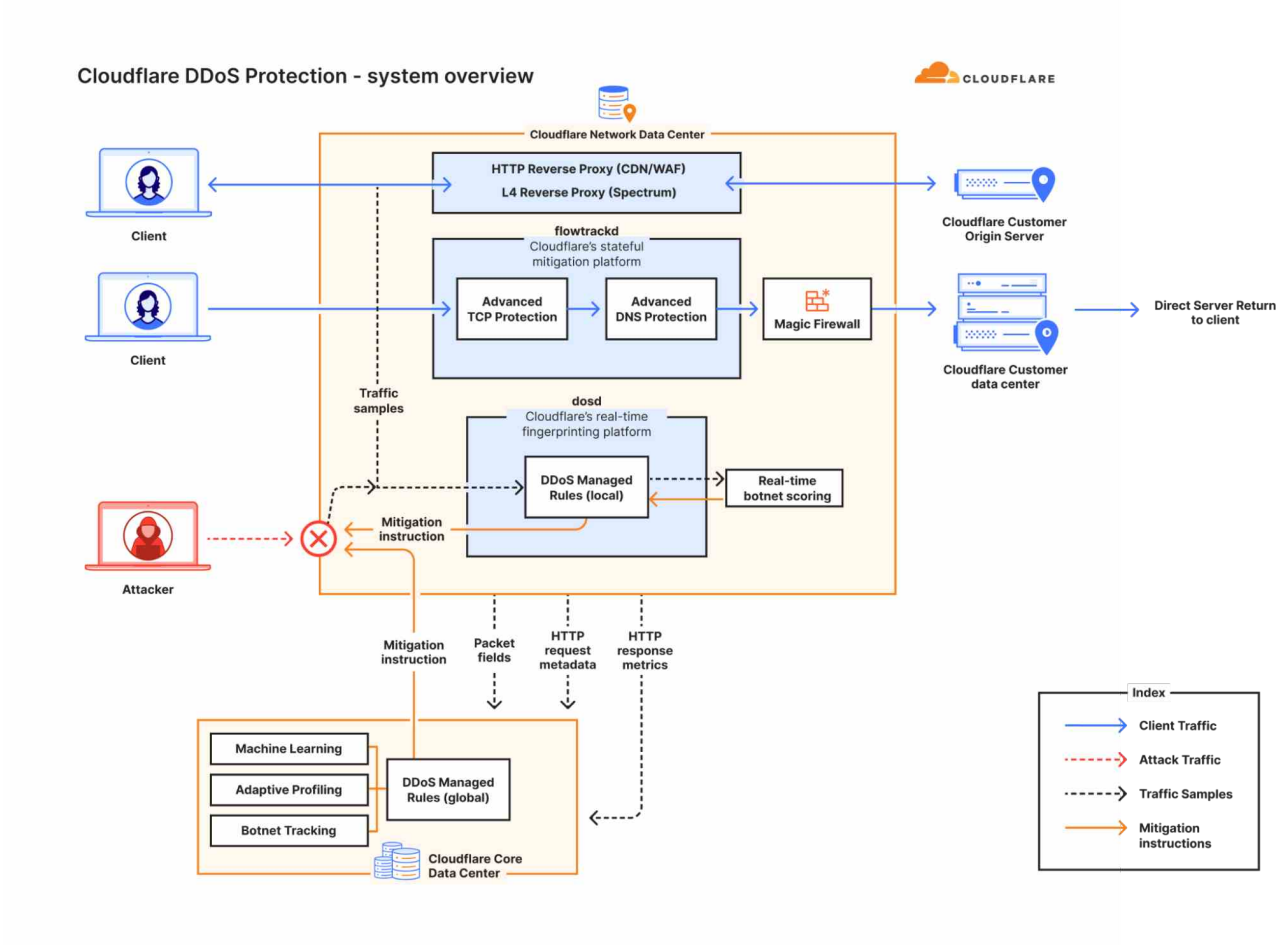


Diagram van de DDoS-beschermingssystemen van Cloudflare

We tellen de verschillende pakketmonsters die overeenkomen met elke vingerafdrukpermutatie en met behulp van een datastreamingalgoritme selecteren we de vingerafdruk met de meeste hits. Wanneer activeringsdrempels worden overschreden, wordt ter voorkoming van fout-positieve resultaten een mitigatieregel met behulp van de vingerafdruksyntaxis gecompileerd als een eBPF-programma. Deze regel verwijdert pakketten die overeenkomen met het aanvalspatroon. Zodra de aanval eindigt, verloopt de regel automatisch en wordt deze verwijderd.

Zoals we al zeiden, detecteert en bestrijdt elke server aanvallen volledig autonoom. Hierdoor is ons netwerk uiterst efficiënt, veerkrachtig en snel in het blokkeren van aanvallen. Bovendien *verzendt* elke server door middel van *multicasting* de belangrijkste vingerafdrukpermutaties binnen een datacenter en wereldwijd. Door realtime dreigingsinformatie te delen, kunnen we de effectiviteit van de risicobestrijding in een datacenter en wereldwijd verbeteren.

Onze systemen hebben deze recordbrekende DDoS-aanval met een snelheid van 7,3 Tbps volledig autonoom geblokkeerd, zonder dat er menselijke tussenkomst nodig was, zonder dat er waarschuwingen werden gegenereerd en zonder dat er incidenten

ontstonden. Dit toont de effectiviteit van onze toonaangevende DDoS-beschermingssystemen aan. Wij hebben dit systeem ontwikkeld als onderdeel van onze missie om een beter Internet te creëren door middel van gratis, onbeperkte DDoS-bescherming.

We beschermen complete zakelijke netwerken, helpen klanten toepassingen op internet-schaal efficiënt te bouwen, versnellen websites en internettoepassingen, weren DDoS-aanvallen af, houden hackers op afstand, en kunnen je helpen bij je reis richting Zero Trust.

Bezoek 1.1.1.1 vanaf elk apparaat om aan de slag te gaan met onze gratis app die je internet sneller en veiliger maakt.