nationale
beheersorganisatie
internet providers

NaWas DDoS overzicht 2024

De Nederlandse Nationale Wasstraat (NaWas) beschermt aanbieders van digitale infrastructuur zoals ISP's, hosting- en VoIP-providers tegen DDoS-aanvallen.

De NaWas geeft tegelijkertijd inzicht in de veranderende trends in het DDoS-landschap. Hieronder vind je de belangrijkste cijfers en een beknopte toelichting bij de DDoS cijfers van 2024.

Kerncijfers

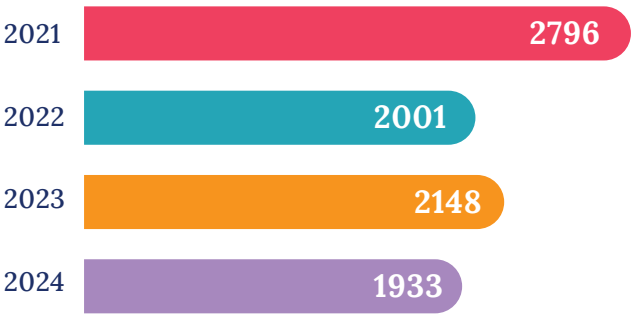
Het dreigingslandschap voor DDoS-aanvallen was ook in 2024 divers en veranderde snel. Hoewel aanvalsaantallen veel zeggen over het dreigingslandschap, zijn de laatste jaren andere variabelen van groter belang geworden voor een geïnformeerde inschatting van de dreiging van DDoS. Hacktivistische organisaties die gerelateerd zijn aan statelijke actoren, zijn een veel grotere bedreiging geworden in vergelijking met slechts een paar jaar geleden. Ze maken vaak gebruik van complexere aanvallen en richten zich op specifieke organisaties, met de bedoeling om te ontregelen. Daarnaast creëren dit soort groepen ook geavanceerdere methoden om aanvallen uit te voeren dan bijvoorbeeld de booters die beschikbaar zijn via het dark web.

1933
gemitigeerde aanvallen

5.27
gemiddeld aantal gemitigeerde aanvallen per dag

353 Gbps
maximale omvang

Aantal aanvallen per jaar



NaWas mitigeerde bijna 2000 DDoS-aanvallen in 2024, iets minder dan in 2023 toen 2148 aanvallen werden gemitigeerd. Vergeleken met 2021, toen het aantal aanvallen piekte tijdens de covid-19 pandemie, is het aantal aanvallen aanzienlijk gedaald. Het aantal aanvallen is echter vergelijkbaar met 2022 en 2023.

Top 5 aanvallen in 2024

01. DNS Amplification
02. NTP Amplification
03. TCP SYN Flood
04. IP low TTL Flood
05. UDP HTTP/3 QUIC Flood

Trends:

DNS Amplification aanvallen zijn intensievere geworden. DNS amplification is daarmee in 2024 de meestvoorkomende aanvals vector.

Afname van het aantal aanvallen aan het einde van 2024.

NTP Amplification was consistent een top 3 aanvalsvector.

Hoewel we veelvoorkomende aanvalsvectoren weer terugzagen in 2024, was ook sprake van een toename van minder veelvoorkomende aanvallen. Aanvallen zoals DNS reflection met het .sl domein en IP low TTL floods komen nu voor in de top 5 aanvalsvectoren voor 2024.

Een andere trend die opviel tijdens 2024, is dat het aantal aanvallen dat lastig te mitigeren is door het gebruik van meerdere aanvalsvectoren flink hoger lag dan in voorgaande jaren. Dit soort aanvallen hebben de potentie om meer te ontregelen dan andere typen aanvallen omdat ze vaker slagen.

In Nederland hebben meerdere aanvallen plaatsgevonden met enige mate van succes, vooral op publieke organisaties. Dit heeft impact gehad op de perceptie van het brede publiek op de effectiviteit en dreiging van cyberaanvallen.

Verwachtingen voor 2025

Voor 2025 verwachten we een DDoS-landschap dat sterk in beweging is. We hebben in 2025 reeds impactvolle DDoS-aanvallen waargenomen op publieke instellingen in Nederland en daarbuiten. Dit soort incidenten benadrukken nog eens het belang van open, gemeenschappelijke oplossingen voor een betrouwbaar internet. NBIP blijft het DDoS dreigingslandschap monitoren en daar ieder kwartaal over rapporteren.

Over deze cijfers

Dit beknopte overzicht van DDoS-aanvallen in het jaar 2024 is in de eerste plaats gericht op DDoS-aanvaltrends in Nederland, maar weerspiegelt ook steeds meer DDoS-aanvaltrends in Europa.

NaWas beschermt voornamelijk aanbieders van digitale infrastructuur, die vele tienduizenden klanten bedienen. Via NaWas wordt een groot deel van de Nederlandse en ook Europese digitale infrastructuur en haar gebruikers beschermd tegen DDoS-aanvallen.

Het aantal deelnemers aan NaWas is meer dan 130, waarvan ongeveer 80% in Nederland en 20% in andere landen in Europa.

Zie voor meer informatie **nbip.nl/nawas**