NBIP nationale beheersorganisatie internet providers

NaWas DDoS attack statistics of 2024

The Dutch National Scrubbing Center (NaWas) protects digital infrastructure providers such as ISP's, hosting- and VoIP-providers from DDoS attacks. The NaWas simultaneously provides insight into the changing trends in the DDoS landscape. Below are the key figures and limited guidance on DDoS attacks observed in 2024 by NaWas.

Key figures

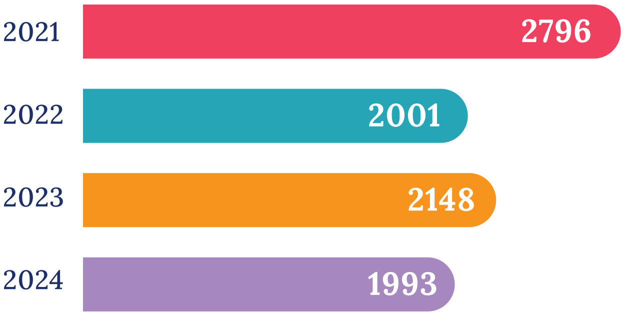
Even though the number of attacks is a significant variable when it comes to assessing the DDoS threat landscape, it is important to be aware that targets, intent, perpetrator and skillfulness have become much more significant variables when assessing the DDoS threat landscape in the past few years. In short, hacktivist organizations that are related to state actors have become a far bigger threat compared to just a few years ago. They tend to utilize more complex attacks and target specific organizations, with the intent of causing disruption. In addition, these types of groups also create more sophisticated methods to carry out attacks than, for example, the booters available via the dark web.

1993
attacks mitigated

5.27
average number of mitigated attacks per day

353 Gbps
maximum mitigated attack size

Number of attacks per year



NaWas mitigated nearly 2000 DDoS attacks in 2024, which is slightly less than in 2023, when 2148 attacks were mitigated. Compared to 2021, when the number of DDoS attacks was at an all-time high due to the covid-19 pandemic, the number of attacks has decreased significantly. The total number of attacks is on par with 2022 and comparable to 2023.

Top 5 attacks 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 attacks moved up in intensity. DNS amplification attacks moved from 5th in attack vectors at the first quarter of 2024, to being 1st for the rest of 2024.

Decrease in the number of attacks towards the end of the year

NTP Amplification was a consistent top 3 attack vendor.

Though we saw a lot of common attack vectors make a comeback in 2024, there was also a significant increase in less common attacks. Attacks like DNS reflection with the .sl domain and IP low TTL floods made it into top 5 attack vectors this year, which marks a significant increase in these types of attacks.

If there was one trend that stood out during 2024, it would be that the amount of difficult to mitigate attacks utilizing multiple attack vectors was significantly higher than in previous years. These types of attacks have the potential to cause more (societal) disruption than most other types of attacks because they succeed more often.

In The Netherlands alone, we have witnessed multiple successful attacks on governmental bodies and other public organizations in 2024, which had an impact on the public perception on public safety and security.

Expectations for 2025

Looking ahead, we believe we will continue to see a very fluid DDoS landscape. Already in 2025, we have witnessed large, sustained DDoS attacks on public institutions in the Netherlands and abroad. Events like these once again emphasize the importance of open, collaborative solutions to ensure a resilient internet. NBIP will continue to monitor the DDoS threat landscape closely and report its findings in quarterly reporting.

About these statistics

This brief overview of the year 2024 is first and foremost skewed towards DDoS attack trends in the Netherlands, but increasingly also reflects DDoS attack trends in Europe.

NaWas predominantly protects digital infrastructure providers, who together serve tens of thousands of customers. Through NaWas, a large portion of the Dutch and also European digital infrastructure and its users are protected against DDoS attacks. This not for profit collaborative approach made in Europe, allows for a more resilient internet.

The number of participants in NaWas exceeds 130, with about 80% located in the Netherlands and 20% in other countries across Europe.

For more information, see **nbip.nl/en/nawas**