DDoS attack figures from the second quarter 2022

The Dutch National Scrubbing Center (NaWas) protects participants against DDoS attacks. Besides protection, NaWas offers valuable insights about the changing landscape of DDoS. To better combat these malicious attacks, we share our up-to-date knowledge with interested parties. Together we stand strong against DDoS attacks. Below you'll find some of the most important figures of DDoS attacks from the second of 2022.

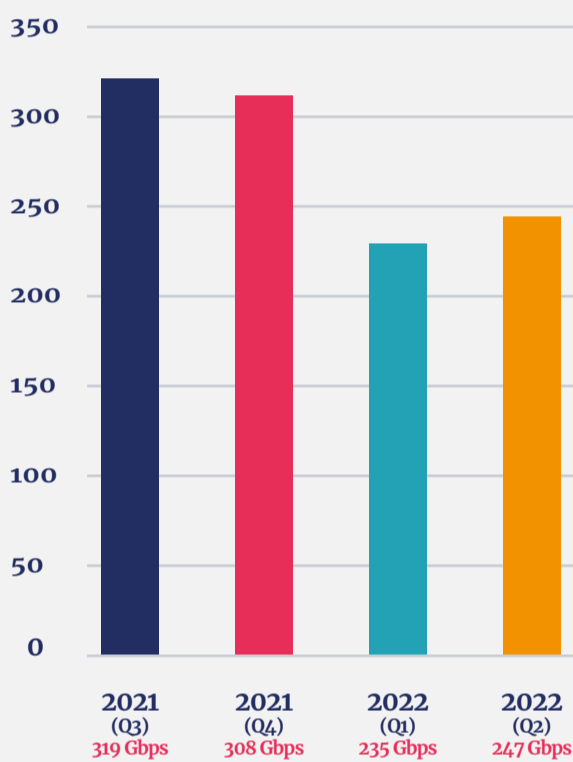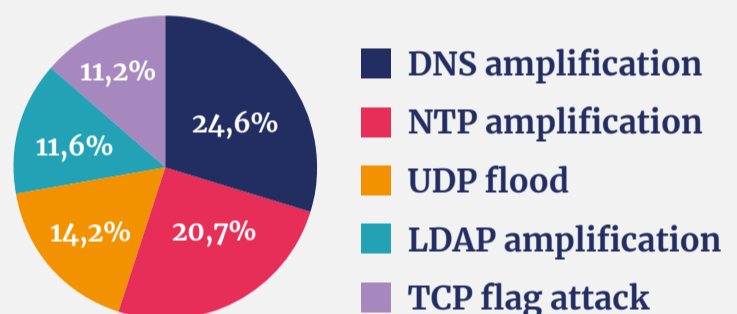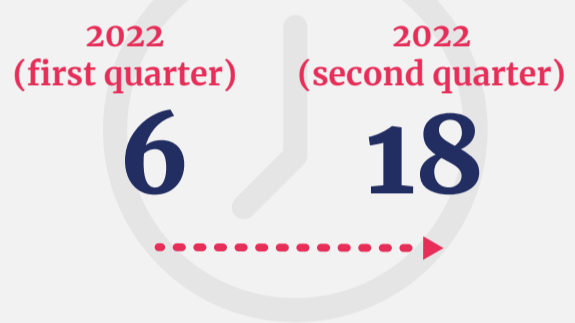**Number of attacks:**

514

Average number of attacks per day:

5,6

Maximum attack size:
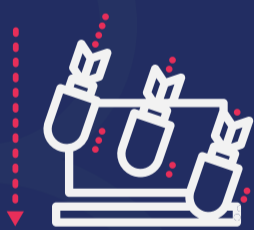
247 Gbps

Maximum size of attacks

Year	Gbps
2021 (Q3)	319 Gbps
2021 (Q4)	308 Gbps
2022 (Q1)	235 Gbps
2022 (Q2)	247 Gbps

Prolonged attacks >4 hours

2022 (first quarter)

6

2022 (second quarter)

18

- DNS amplification — 24,6%
- NTP amplification — 20,7%
- UDP flood — 14,2%
- LDAP amplification — 11,6%
- TCP flag attack — 11,2%

Trends

Fewer attacks than in Q1, downward trend since Q4 2021 continues

Number of attacks (>4 hours) increases rapidly

Increase in the easy to deploy "UDP flood"

Most common type of attacks: DNS amplification & NTP amplification

In the second quarter of 2022, we see an increase in the number of DDoS attacks that last longer than 4 hours. In addition, DDoS is more often used as a means to make Extortion Ransomware attacks more effective. DDoS attacks are also used to mask other attacks, for example on applications and databases. In addition, DDoS is more often used as a means to make Extortion Ransomware attacks more effective. But DDoS attacks are also used to mask other attacks, for example on applications and databases. DDoS attacks have thus become more difficult, more powerful, more frequent and increasingly part of a more broadly deployed attack.