NaWas Anti-DDoS

Frank Dupker

https://www.nbip.nl/nawas/

whois ORG-SN292-RIPE

- org-name: **Stichting NBIP** - https://www.nbip.nl/en/

- Independent non-profit foundation

- Sector initiative started in 2002

- Services for Internet Providers

  - Lawful Interception

  - Clean Networks Platform – www.cleannetworks.net

  - DDoS Scrubbing Center – NaWas

    - Mitigation

    - Reporting
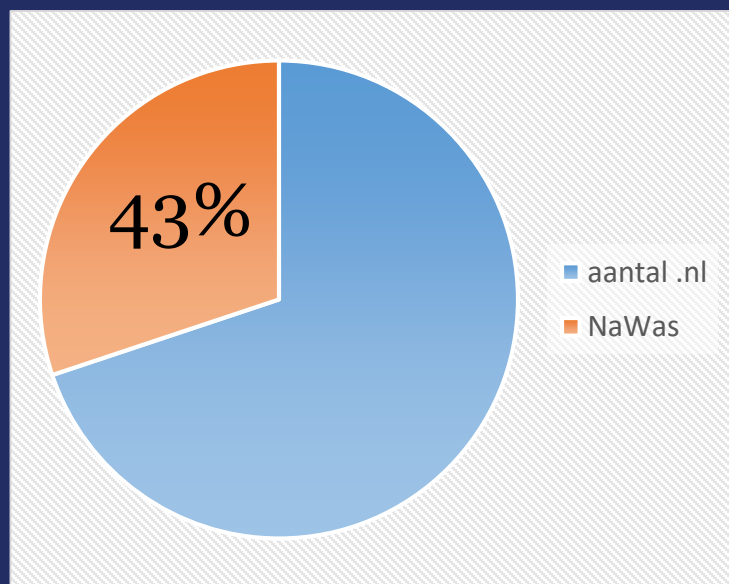
    - Research and cooperation

NBIP nationale
beheersorganisatie
internet
providers

20 jaar!

whois ORG-SN292-RIPE

- 6,5 M .nl domains protected by NaWas (2020)

- Aprox 1,6 M websites

- In 2013 request for anti DDoS solution

- Started POC 2nd ½ 2013

- NaWas operational in 2014

- NaWas connected to LINX in 2019

- NaWas connected to Italian IX and Netix in 2020

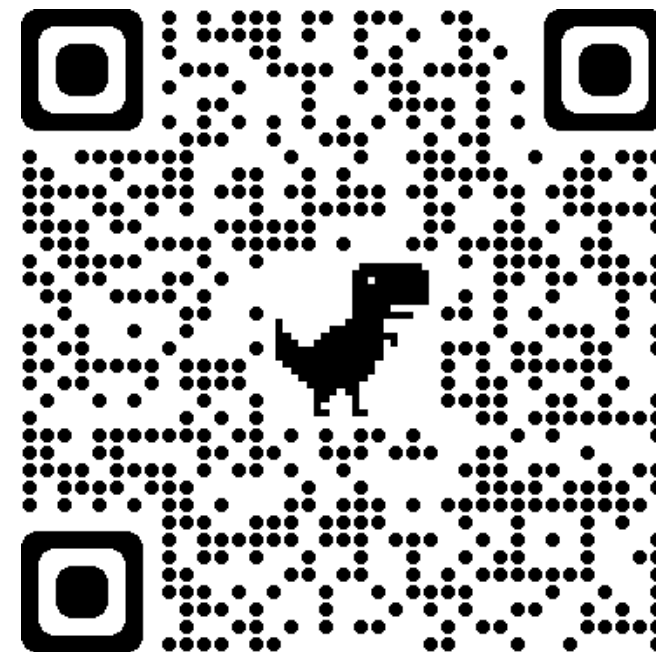**NBIP** nationale beheersorganisatie internet providers

20 jaar!

DDoS Reporting

- ## Every quarter
  - ### nbip.nl/ddos-report

- ## Annually
  - ### Appears early April

DDoS attack figures from the first quarter of 2022

Number of attacks:

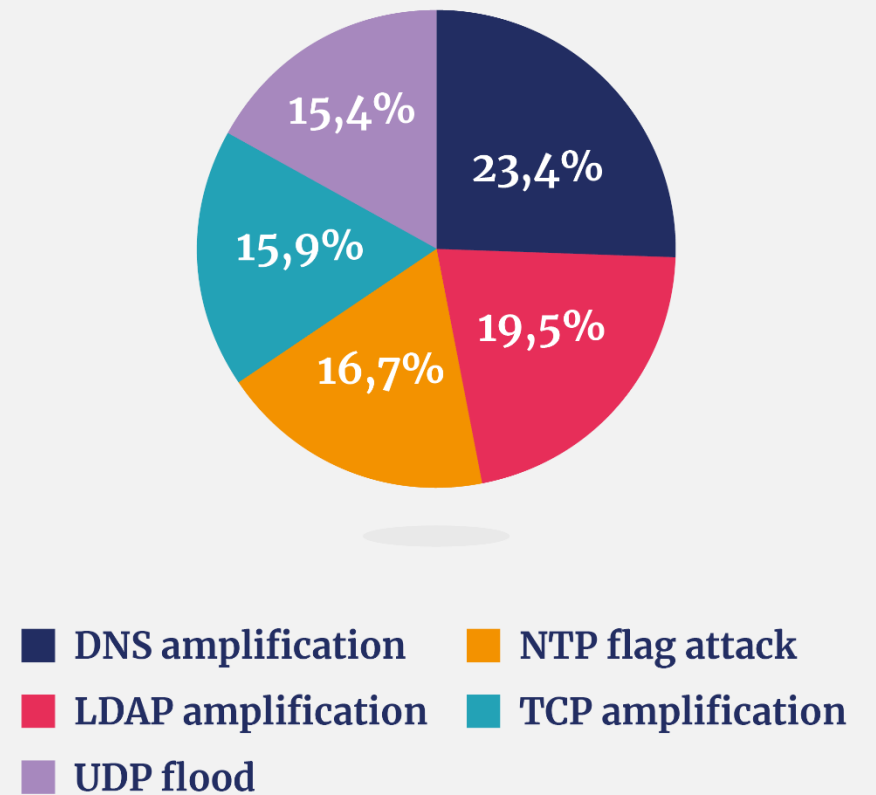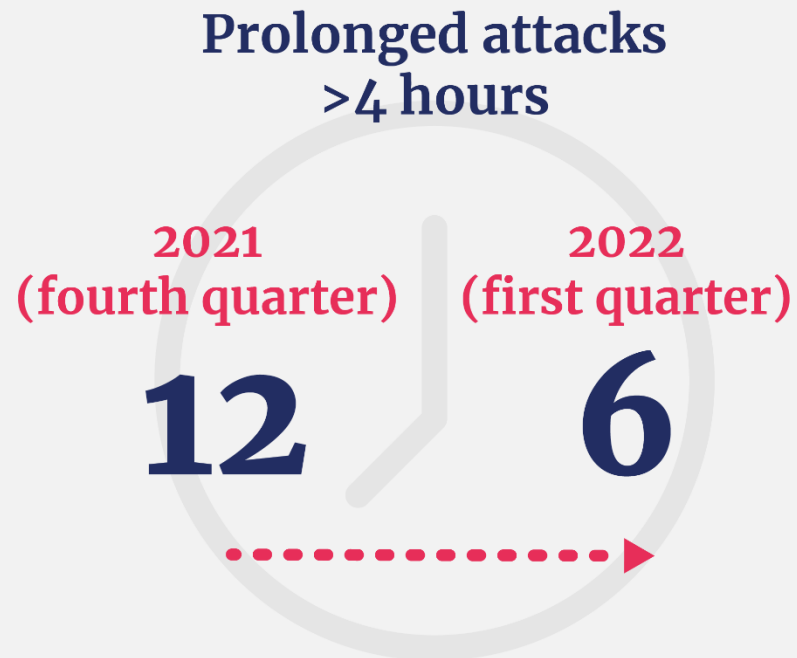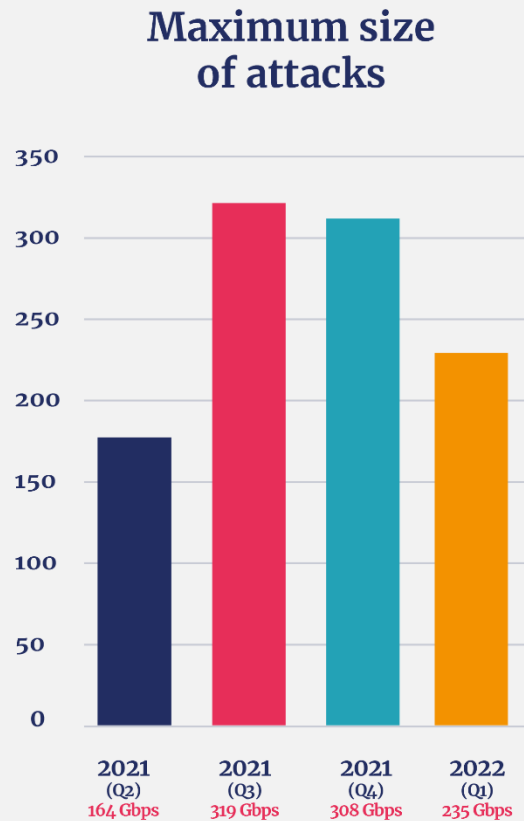**666**

Average number of attacks per day:

7,4

Largest recorded attack:

235 Gbps

DDoS attack figures from the first quarter of 2022

Maximum size of attacks

350			
300			
250			
200			
150			
100			
50			
0			

2021 (Q2) 164 Gbps
2021 (Q3) 319 Gbps
2021 (Q4) 308 Gbps
2022 (Q1) 235 Gbps

Prolonged attacks >4 hours

2021 (fourth quarter)

12

2022 (first quarter)

6

Pie chart

- 23,4%
- 19,5%
- 16,7%
- 15,9%
- 15,4%

■ DNS amplification
■ LDAP amplification
■ UDP flood
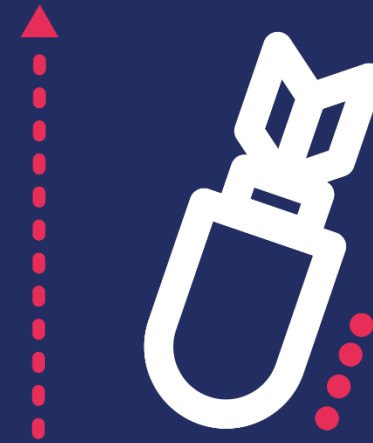■ NTP flag attack
■ TCP amplification

DDoS attack trends from the first quarter of 2022

Increase LDAP amplification attacks in Q1 2022
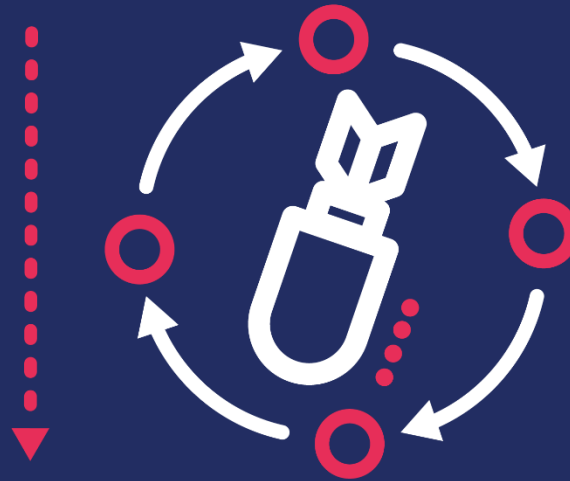
Number of attacks (> 40 Gbps) strongly decreases

Increase DDoS attacks < 15 minutes

Anti-DDoS-Coalitie

- Cooperation on knowledge sharing about DDoS attacks (2018)
  - Universities, IX's, ISP's, banks, goverment, law inforcement
  - National Cyber Security Centre (NCSC) facilitator

New version of the DDoS Clearing House core components
30 September 2020
SIDN Labs and SURF have released a new version of the DDoS Clearing House in a Box, a system that enables network operators to automatically
Read More »

DDoS coalition is working together during the current DDoS attacks
4 September 2020
The website reflects coalition's joint efforts over the past two years In recent weeks, dozens of companies in The Netherlands and Europe have been targeted
Read More »

NaWas
Scrubbing Center

NaWas

- **North: Internet**
  - Several Tier-1 Transit
  - Public peering on Internet Exchanges
  - Amsterdam as one of major hubs in Europe

- **West – East: 3-stage scrubbing**
  - Multiple vendors
  - Fail-over on multiple sites
  - Prefiltering with NaWas filters
    (migrating to FlowSpec)

- **South: Clean Traffic**
  - private connections
  - Only reachable through NaWas
  - PoP's via AMS-IX, NL-IX, Dcspine, Linx, Mix, Top-IX, Namex, Netix
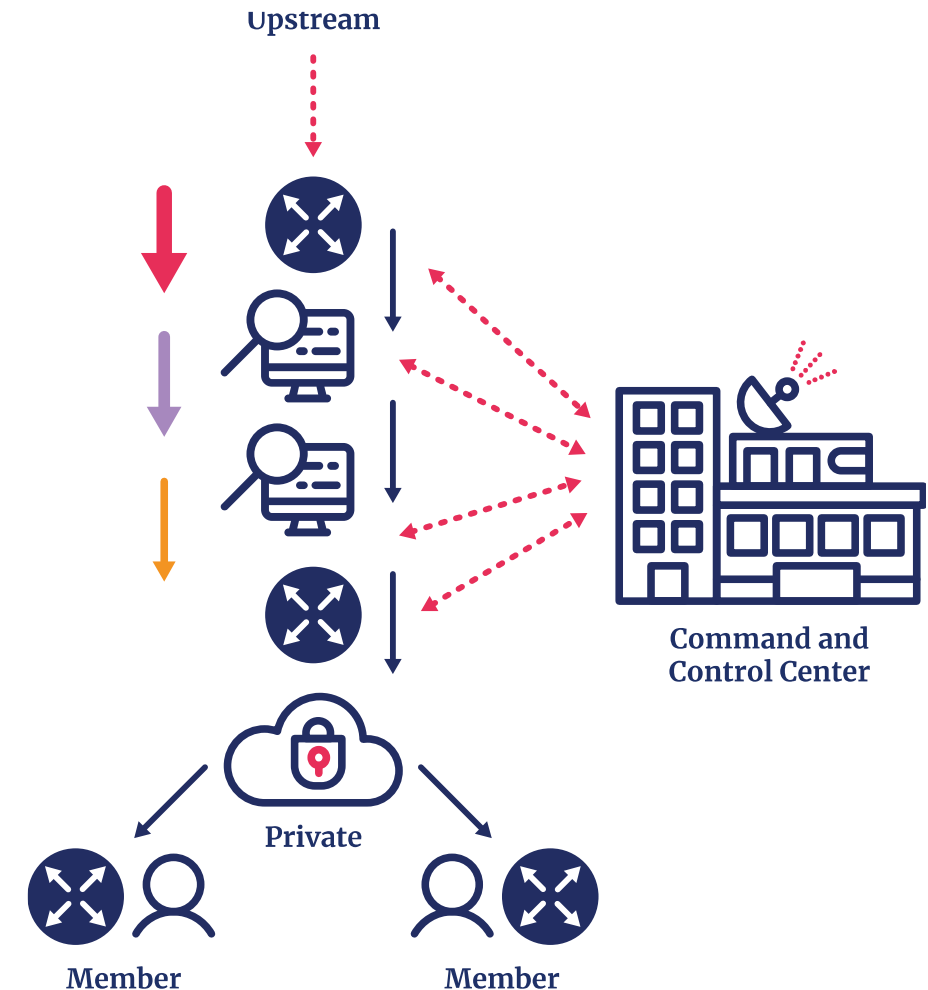
Upstream

Command and
Control Center

Private

Member   Member

Future plans

R&D NaWas

- DDoS Detectie as a Service (DaaS)

- Web Application Firewall (WAF-dp)

- Clearing House (Anti-DDoS coalition)

- DDoS Pattern Recognition - generate filter rules (Dissector)

NBIP

nationale
beheersorganisatie
internet
providers

20 jaar!

Together
Smarter and Stronger

https://www.nbip.nl/nawas/

f.dupker@connect.nbip.nl