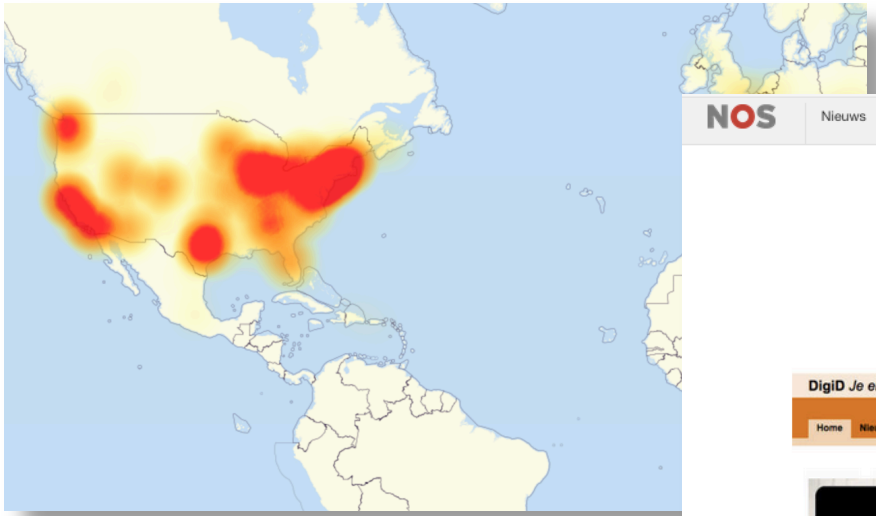
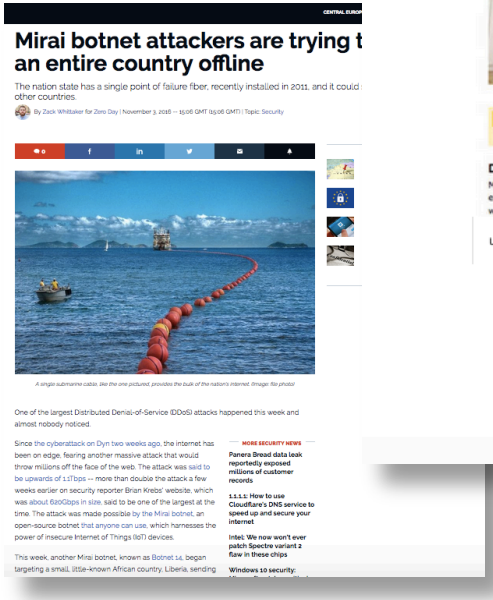
Increasing the Netherlands' DDoS resilience together

SURF Security and Privacy Conference
Fri Feb 7, 2020
Tilburg University
Netherlands

Cristian Hesselman (SIDN)

Impact of DDoS attacks





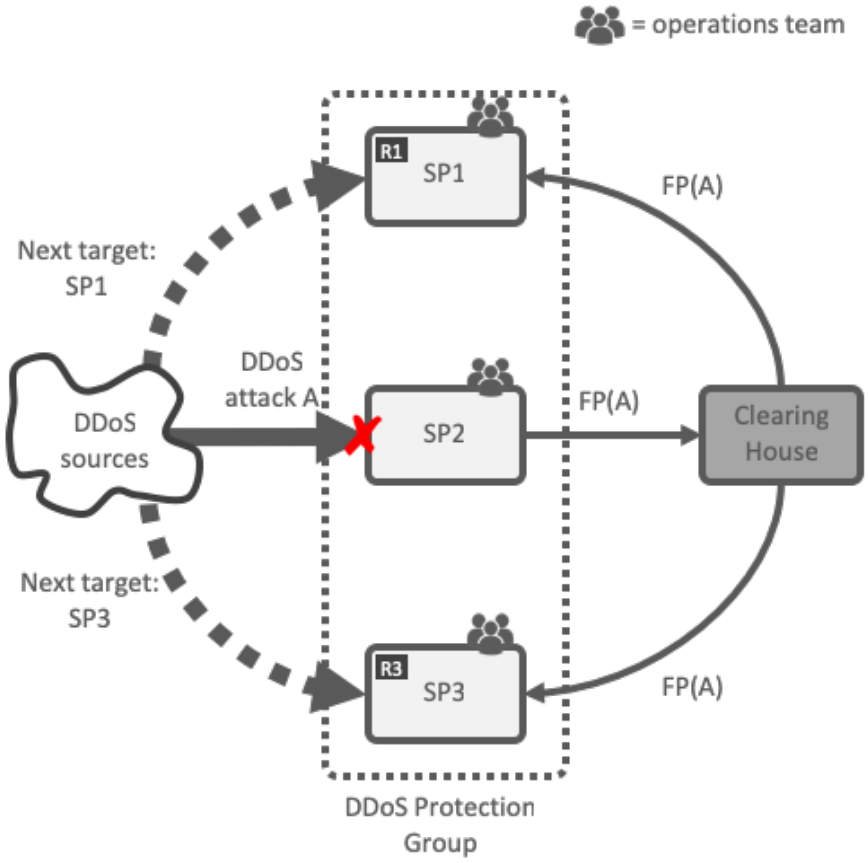
Mirai botnet: Dyn, OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

January 2018

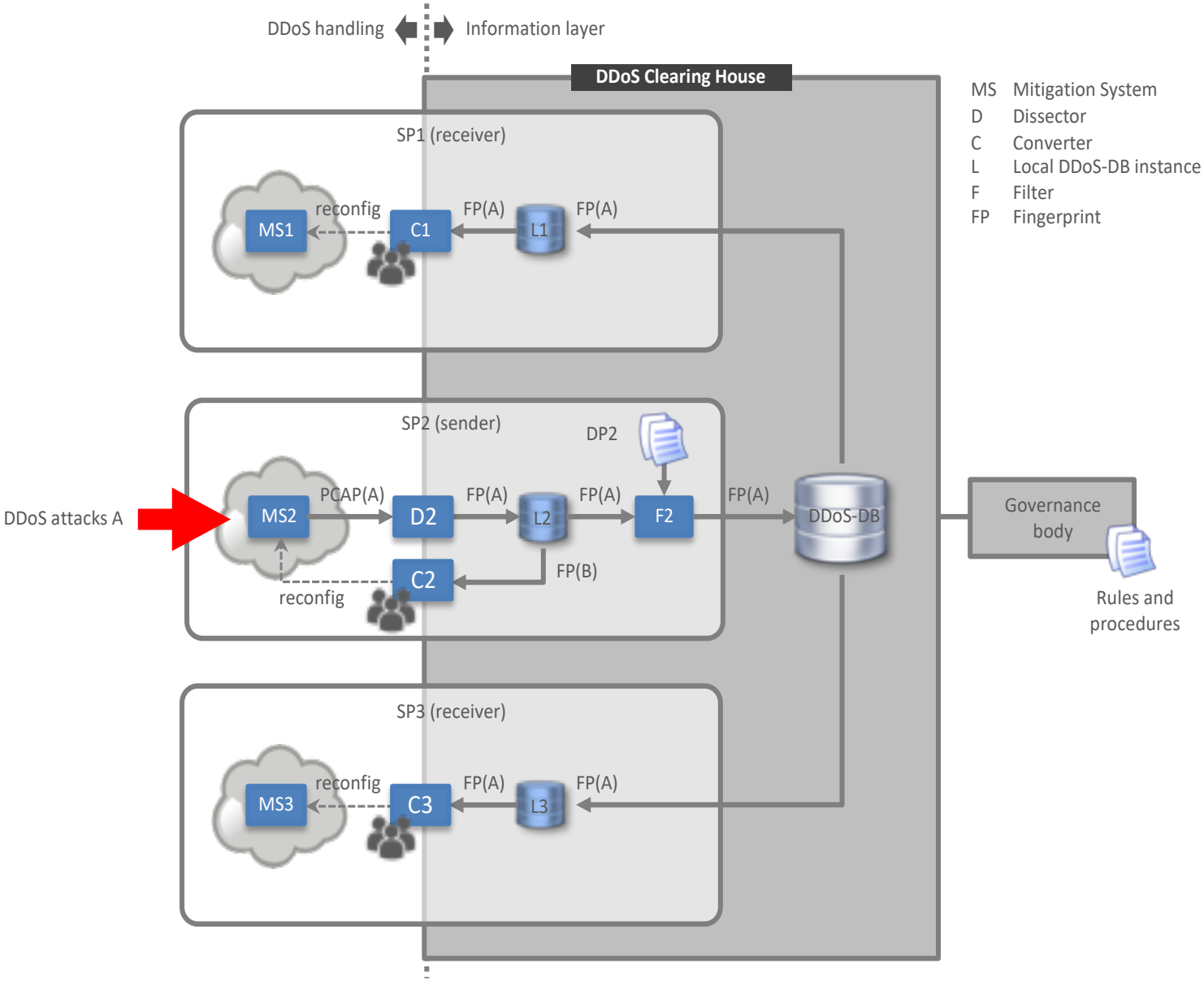
https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

DDoS clearing house concept

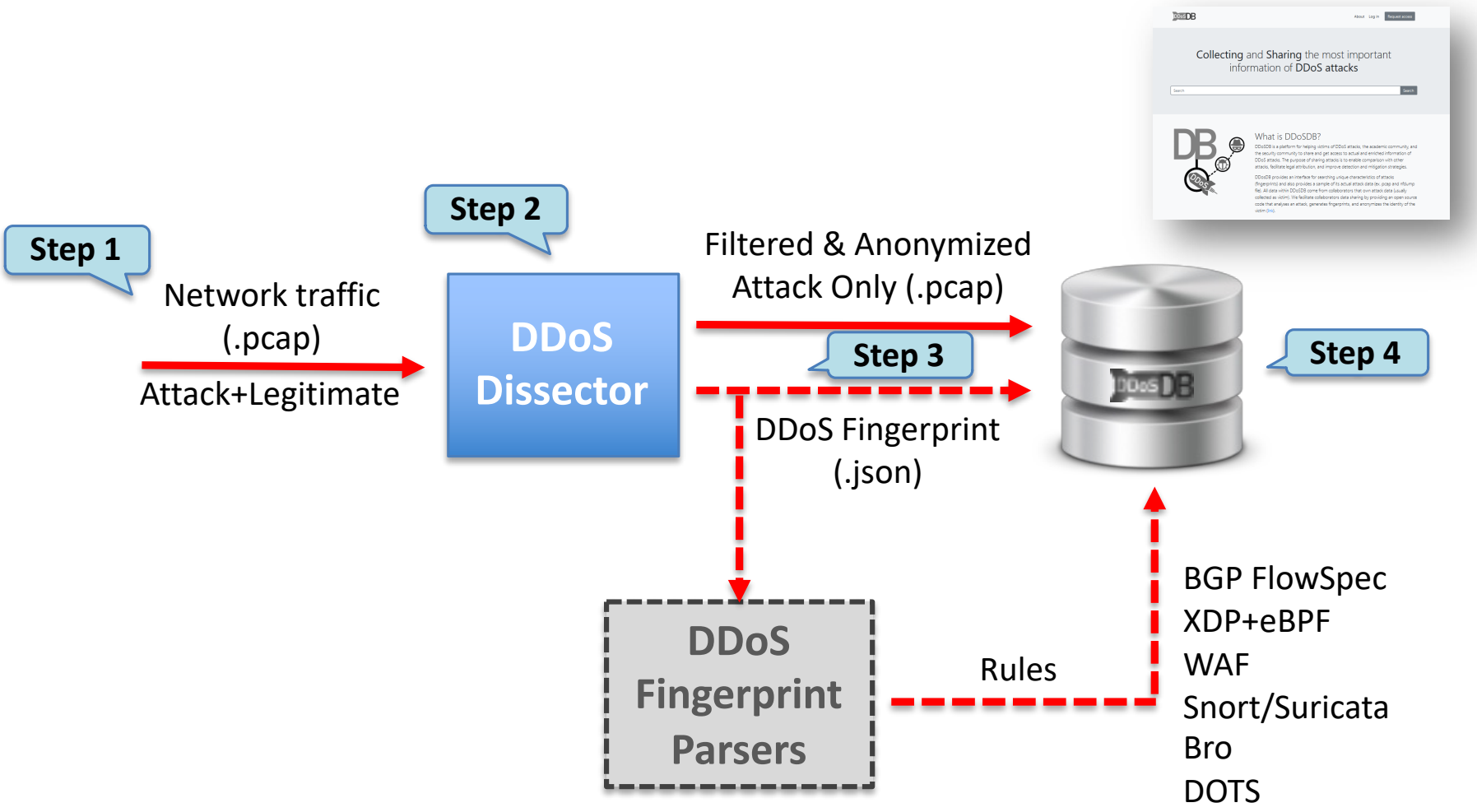
- Continuous and automatic sharing of "DDoS fingerprints" buys providers time
- Extends DDoS protection services that critical service providers use and does not replace them
- Generic: for example, per EU Member State, per sector, per business unit
- Cooperative DDoS mitigation – existing idea, but no deployment



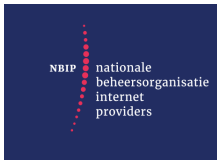
Overall architecture



Zoom in: fingerprint generation



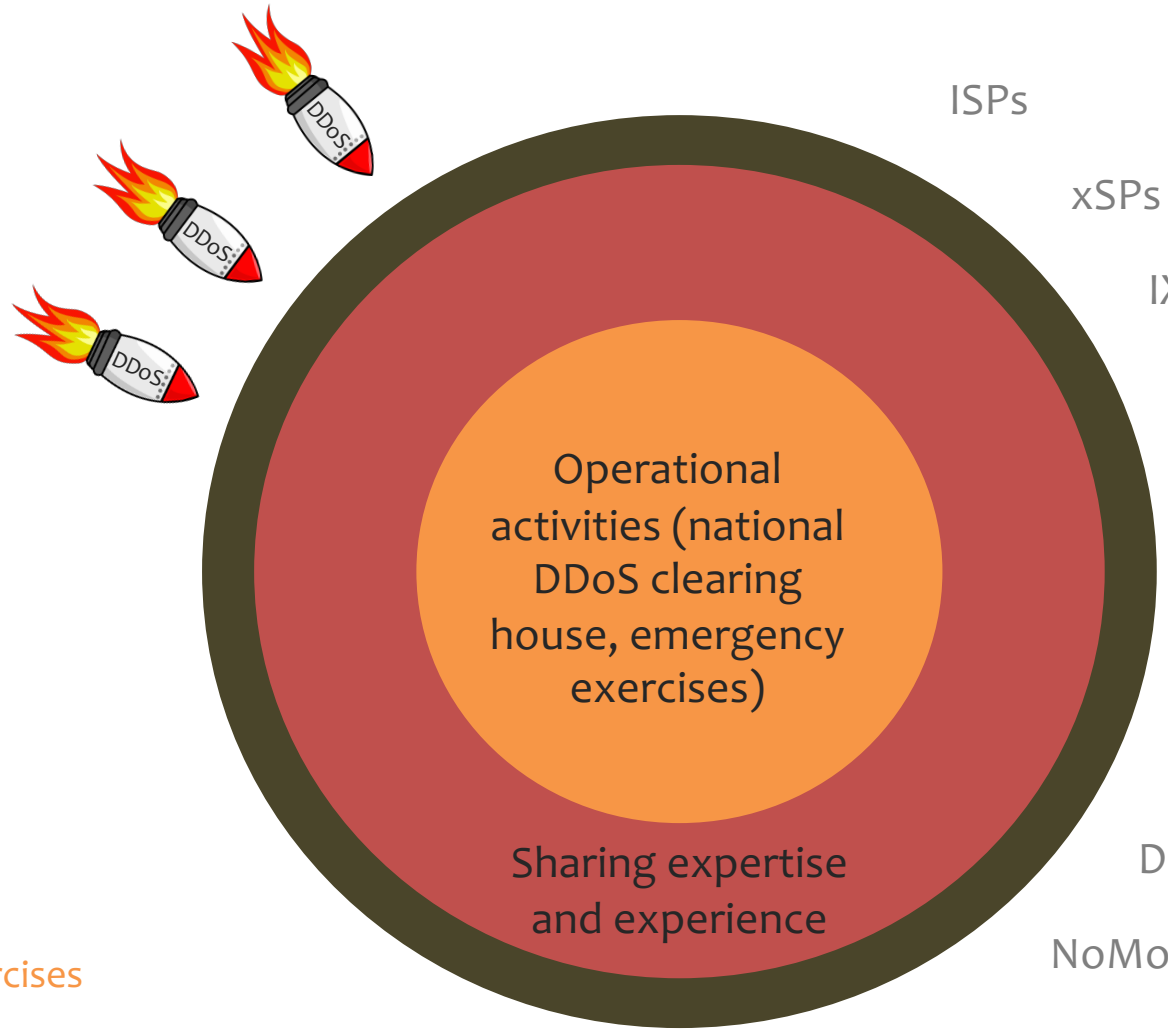
Pilot partners



Plus NoMoreDDoS and Dutch Continuity Board

Anchor point: Dutch anti-DDoS coalition

Objective: further improve the resilience of Dutch critical services by sharing expertise, experiences, and operational data on DDoS attacks



ISPs

xSPs

IXPs

Banks

.nl registry

NCSC-NL

Gov't agencies

University of Twente

Dutch Continuity Board

NoMoreDDoS

NBIP-NaWas

Working groups:

- Clearing house
- Emergency exercises
- Outreach
- Ground rules and incident response
- Sustainable collaboration

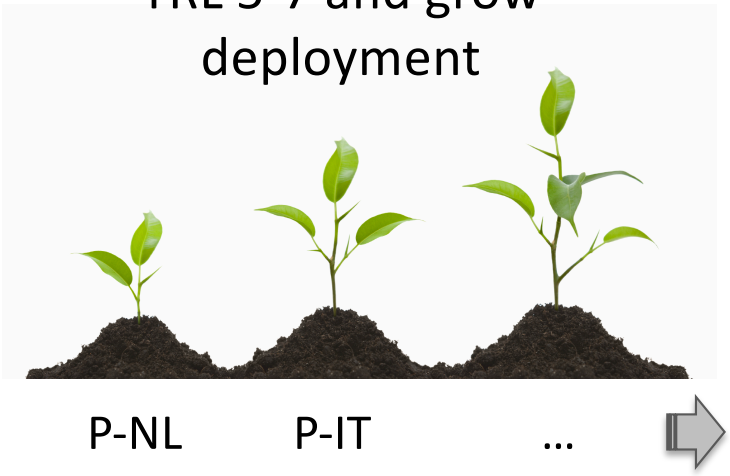
DDoS clearing house for Europe: CONCORDIA`

- Objective: pilot a DDoS Clearing House with European industry for Europe to proactively and collaboratively protect European critical infrastructure against DDoS attacks

- Key outputs: pilots in NL >> IT, DDoS clearing house cookbook

- Build on existing components

Key challenge: increase to TRL 5-7 and grow deployment



CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

SIDN SURF UNIVERSITY OF TWENTE.

Status Dutch DDoS clearing house

- Experimental setup (ddosdb.nl) pilot NL
- Draft data sharing agreement for pilot phase 1
- Draft organizational structure
- Draft overall architecture
- System requirements (funded by NBIP, SURF, NCSC-NL, Dutch Payment Association)
- Extensive dissemination (e.g., One Conference, Open Door Event)

Lessons learned so far

- **Much more than a technical challenge**
- Need for a DDoS clearing house widely acknowledged
- Value of clearing house community goes beyond fingerprints
- Clearing house needs to be anchored in an “anti-DDoS coalition”
- Organization required working groups with clear charters
- Start with a small trusted group, then grow (trust scaling)
- Keep initial data sharing agreement crisp, simple, and scalable
- Working across disciplines early on is even more important

Next steps

- NL pilot: sign data sharing agreement, start sharing in non-production setting, improve software, blog on lessons learned

- Examples of future work:
  - DDoS fingerprint parsers to convert fingerprints to rule suggestions and share them with clearing house users
  - Apply rules to different mitigation boxes in the network with different levels of specificity to mitigate DDoS attacks
  - Evaluate effectiveness of the suggested rules using attack traffic (rule set mitigates p% of attack, depending on network box)

- Set up an instance of the clearing house specifically for experiments in CONCORDIA (ddosdb.eu)

SIDN, SURFnet, and the University of Twente were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.
Project website: https://www.concordia-h2020.eu/