Developing a DDoS Clearing House for Europe

Dynamic Countering of Cyber-Attacks Workshop 2

Feb 08, 2022

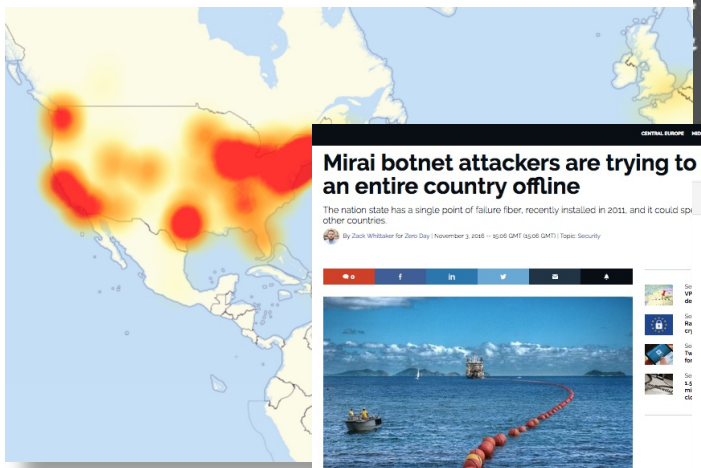
Thijs van den Hout (SIDN Labs)

Partners: SIDN, University of Twente, Telecom Italia, FORTH, University of Zurich, SURF, University of Lancaster, CODE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

DDoS remains relevant

Mirai botnet, 2016



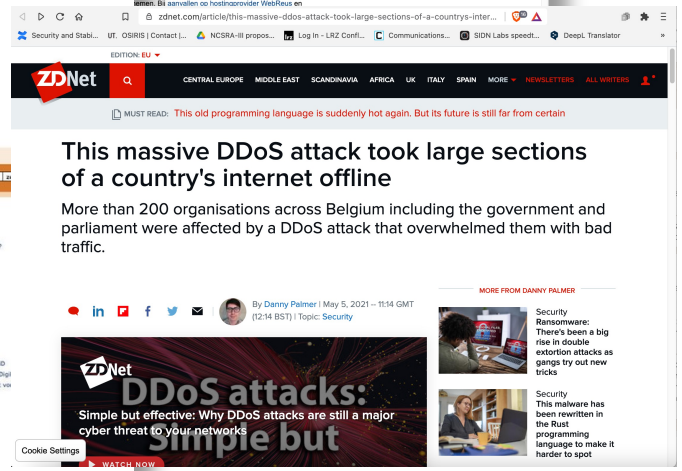
Liberia, 2016

Estonia, 2007

The Netherlands, September 2020

House of Representatives of The Netherlands, Oct 2020

The Netherlands, January 2018



Belgium, May 2021

Problem

- Mature DDoS mitigation services (e.g., scrubbing), routinely handling large numbers of DDoS attacks

- BUT no sharing of DDoS data and expertise across organizations
  - Increases response time and prevents learning because of limited view
  - Reduces innovation of mitigation processes and systems at ecosystem level
  - DDoS data “stuck” in systems of (US-based) DDoS mitigation providers

- Increases probability of societal disruptions through online services

DDoS Clearing House Concept

- Generic concept: **Anti-DDoS Coalitions** across sectors, Member States, business units, etc.
- Sharing of **DDoS fingerprints** between coalition members
- **Extends DDoS protection services** that service providers use and does not replace them

DDoS Clearing House: use-inspired research

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

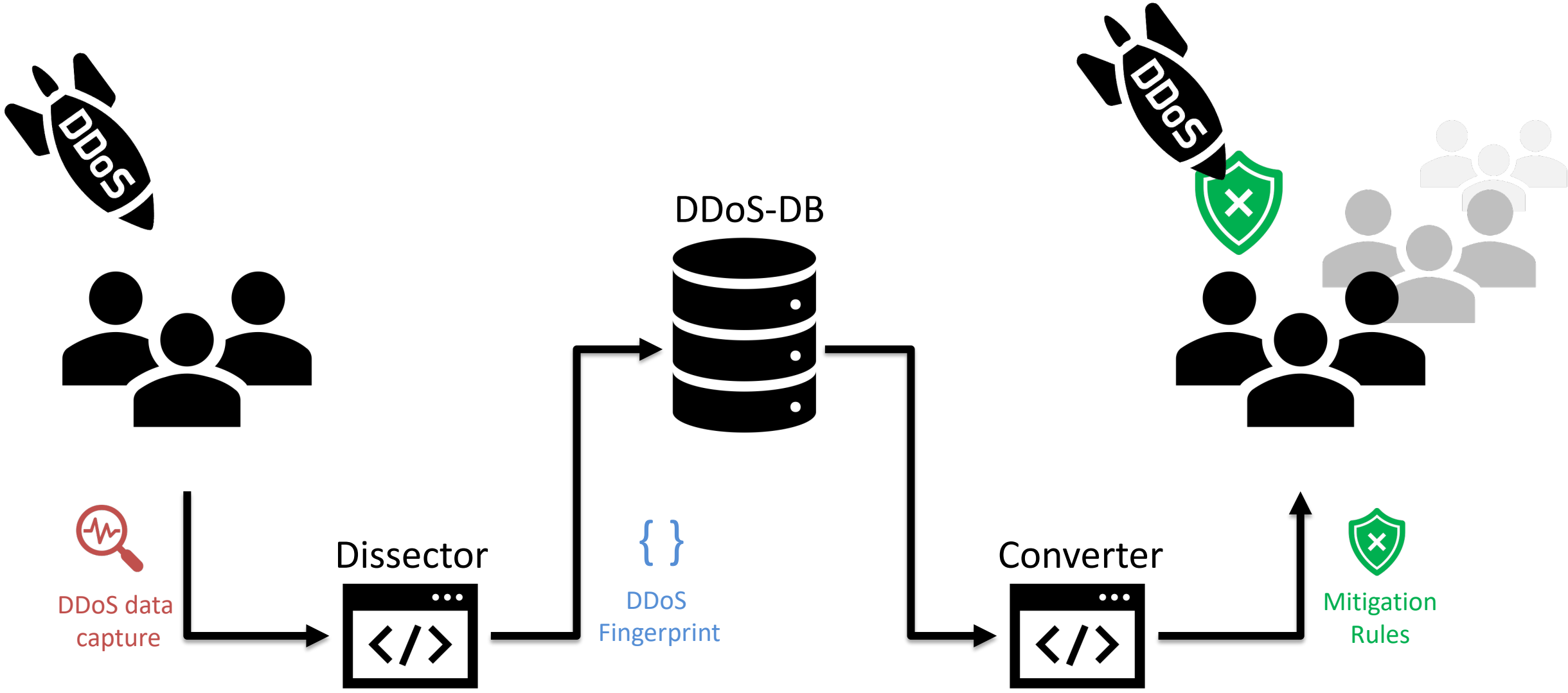
Anti-DDoS-Coalitie
No More DDoS

- DDoS clearing house **R&D**
- Clearing house distributed **testbed**
- Technical **evaluation through pilots** in the Netherlands and Italy
- DDoS clearing house **cookbook**

- Operational ADC **organization**
- Sharing of operational **experience**
- Large-scale multi-party **DDoS drills**
- **DDoS clearing house operations**

CONCORDIA is funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/

DDoS Clearing House



DDoS Fingerprint Example

fingerprint a38e5062b69fd7b8c5194fa7698398a7


```
{
  attack_vectors: [
    {
      service: "HTTP"
      protocol: "TCP"
      source_port: 80
      fraction_of_attack: 1.0
      destination_ports: "random"
      TCP_flags: {
        ...A....: 0.989
      }
      nr_flows: 5077
      nr_packets: 20308000
      nr_megabytes: 30599
      time_start: "2022-01-23 01:28:00"
      time_end: "2022-01-23 01:29:56"
      duration_seconds: 116
      source_ips: [
        "[redacted]"
        "[redacted]"
        "[redacted]"
        "[redacted]"
      ]
    }
  ]
  target: "Anonymous"
  tags: [
    "TCP"
    "TCP ACK flag attack"
  ]
  key: "a38e5062b69fd7b8c5194fa7698398a7"
  time_start: "2022-01-23 01:28:00"
  duration_seconds: 116
  total_flows: 5077
  total_megabytes: 30599
  total_packets: 20308000
  total_ips: 4
  avg_bps: 2110318068
  avg_pps: 175068
  avg_Bpp: 1506
  submitter: "thijs"
  submit_timestamp: "2022-01-25T13:50:13.818348"
  shareable: False
}
```

Key innovations

- Bridge **multidisciplinary gap** to deployment, more than tech!
- **Opensource design** that we make available through a “cookbook”
  - Technology, legal, organizational, lessons learned based on pilots
  - Enable federations of organizations to set up their own anti-DDoS coalition
  - Main use case is the Dutch Anti-DDoS Coalition (NL-ADC)
- Operates across **heterogeneous networks** and offers rich set of services

Dutch Anti-DDoS Coalition (NL-ADC)

Betaalvereniging Nederland

SURF

CONCORDIA partner

VNO NCW

SIDN

CONCORDIA partner

NBIP NaWas

UNIVERSITY OF TWENTE.

CONCORDIA partner

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

amsix

DeNederlandscheBank
EUROSYSTEEM

vodafone Ziggo

POLITIE

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Belastingdienst

NLIX
The Interconnect Exchange

kpn

DINL
Stichting Digitale Infrastructuur Nederland

Key achievements

- Stable version of the DDoS Clearing House components
- Completed technical preparations for the pilots
- Developed the DDoS Clearing House testbed
- Selected for EC Innovation Radar
- NL-ADC: €200k additional funding from the Dutch government
- NL-ADC: Signed consortium agreement – on its way to production

From prototype (TRL5) to production (TRL8/9)

Phase		Q1-2021	Q2-2021	Q3-2021	Q4-2021	Q1-2022	Q2-2022	Q3-2022
-1	**Distributed testbed**							
0	Pilot							
1	Basic production							
2	Full production							

Dev: CONCORDIA team
Ops: SIDN Labs + CONCORDIA team

Dev: CONCORDIA team
Ops: database operator (NBIP) + NL-ADC members

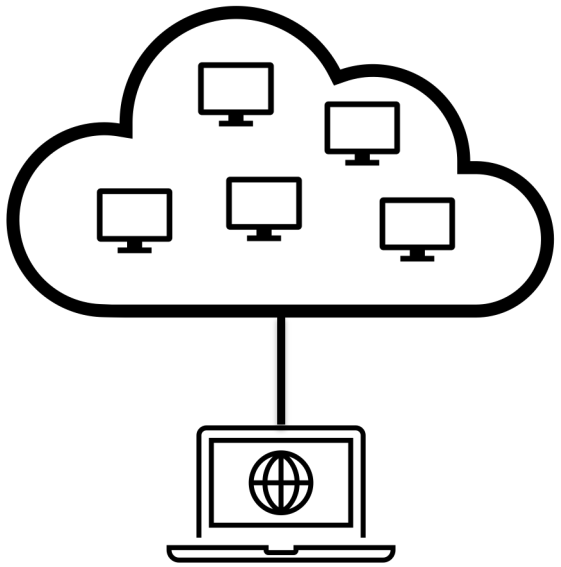
Dev: CONCORDIA team
Ops: SIDN Labs + NL-ADC members

Dev: software engineer (TBD)
Ops: database operator (NBIP) + NL-ADC members

Clearing House testbed

- Goal: pilots in the Netherlands & Italy
- Obstacle: production systems and legal agreements
- Intermediate step: representative environment in which to test the technical developments of the Clearing House

Remote cloud-hosted Traffic simulator



Dashboard

Coalition

Member 1

Member 2

DDoS Clearing House

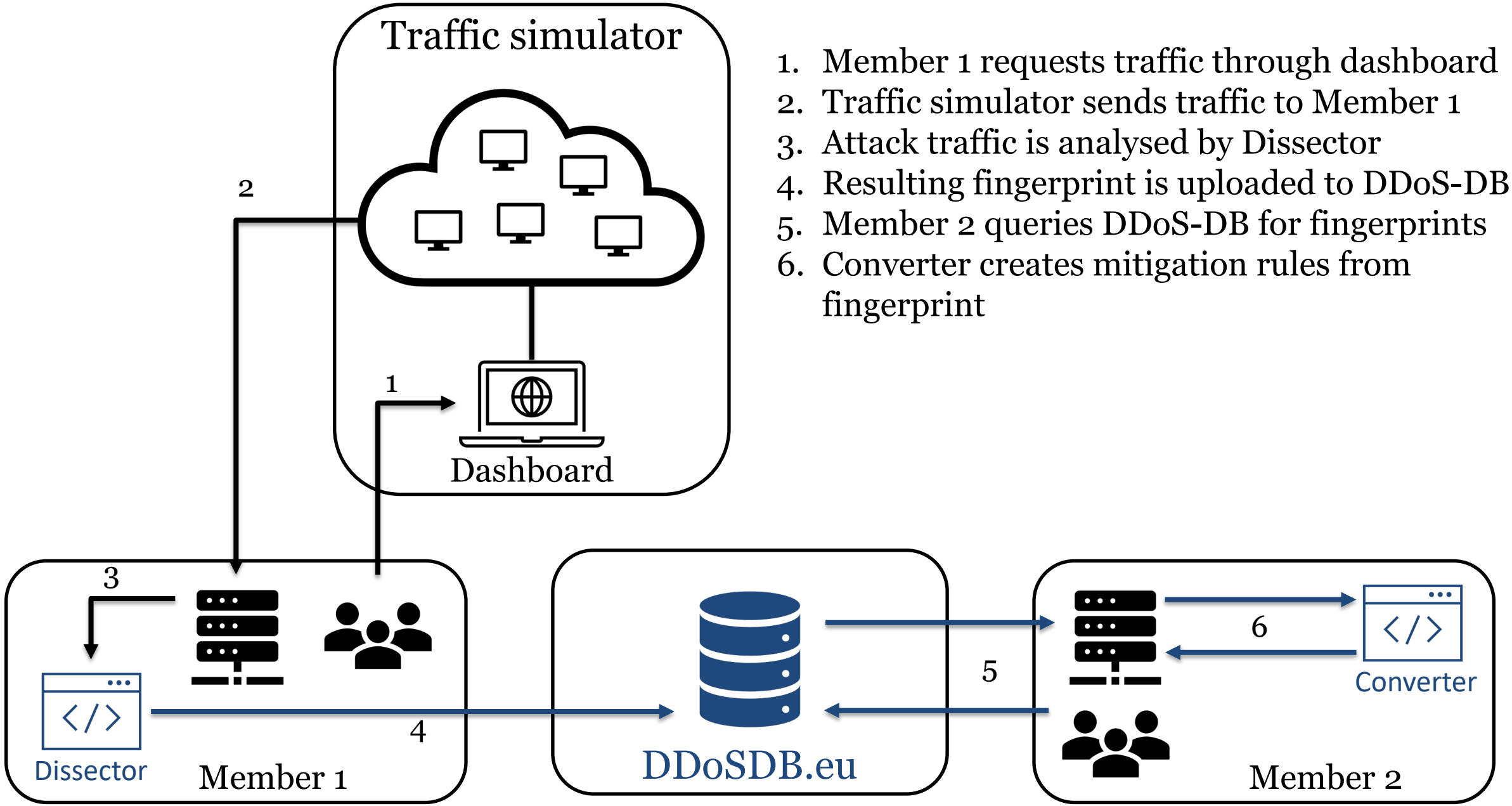
Converter

Dissector

Converter

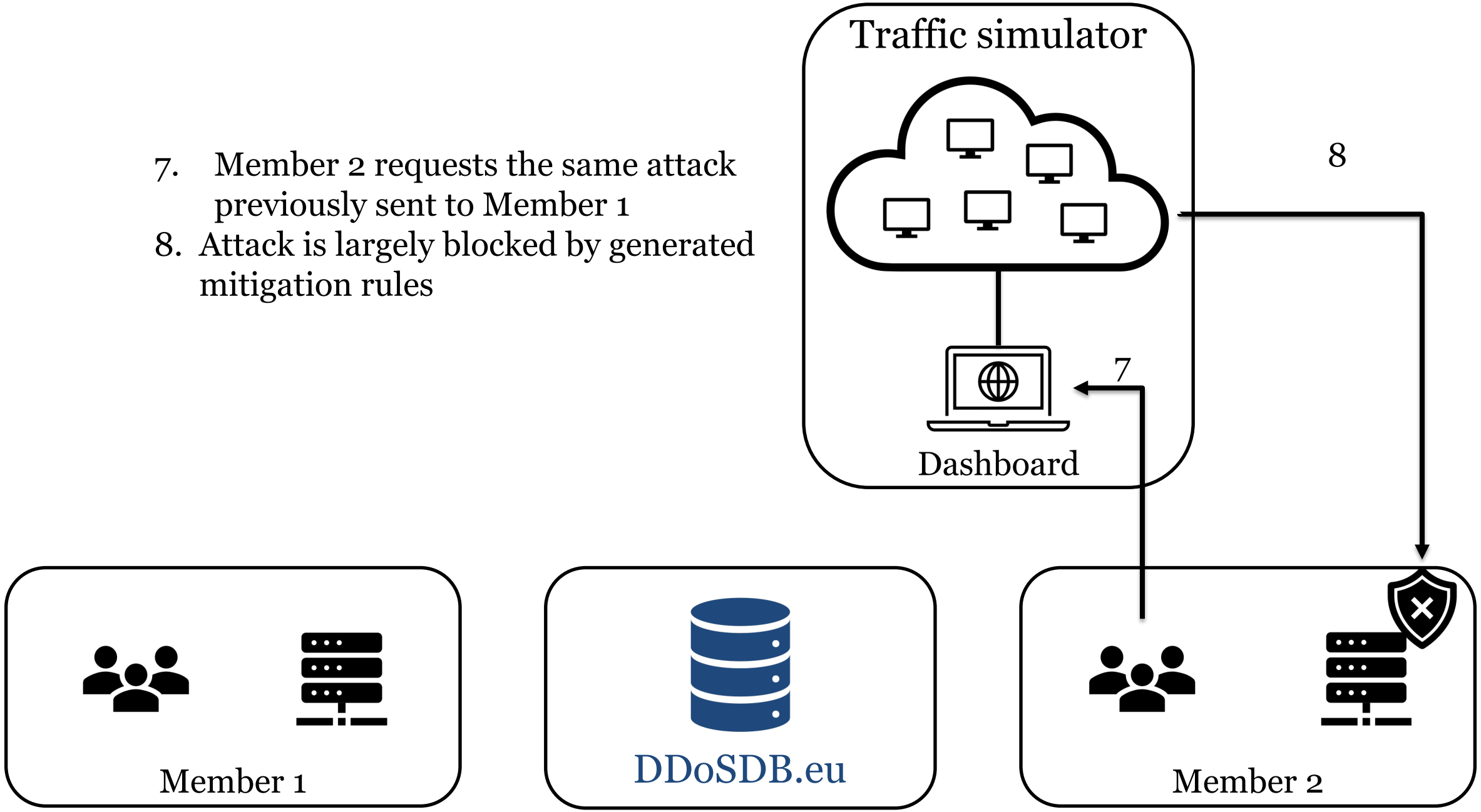
Dissector

DDoS DB



1. Member 1 requests traffic through dashboard
2. Traffic simulator sends traffic to Member 1
3. Attack traffic is analysed by Dissector
4. Resulting fingerprint is uploaded to DDoS-DB
5. Member 2 queries DDoS-DB for fingerprints
6. Converter creates mitigation rules from fingerprint

7. Member 2 requests the same attack previously sent to Member 1
8. Attack is largely blocked by generated mitigation rules




Watch the video at youtu.be/UwRB74kabn8

Outlook

- Scale up testbed to pilots in the Netherlands and Italy
- Summarize our lessons learned in a *cookbook*
- Proposal for fingerprint **standardization** (DOTS WG, IETF)
- MISP-DDoS-DB interworking
- Closing workshop in Sep/Oct

Further reading

https://www.sidnlabs.nl/en/news-and-blogs

https://nomoreddos.org/

https://www.concordia-h2020.eu/

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.youtube.com/concordiah2020

Dutch Anti-DDoS Coalition:
https://www.nomoreddos.org/en/

Clearing house on GitHub:
https://github.com/ddos-clearing-house/

Cristian Hesselman
cristian.hesselman@sidn.nl
@hesselma
+31 6 25 07 87 33

Thijs van den Hout
thijs.vandenhout@sidn.nl
@thijsvandenhout

This work was funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/