



Developing a DDoS Clearing House for Europe

Dynamic Countering of Cyber-Attacks Workshop 2

Feb 08, 2022

Thijs van den Hout (SIDN Labs)

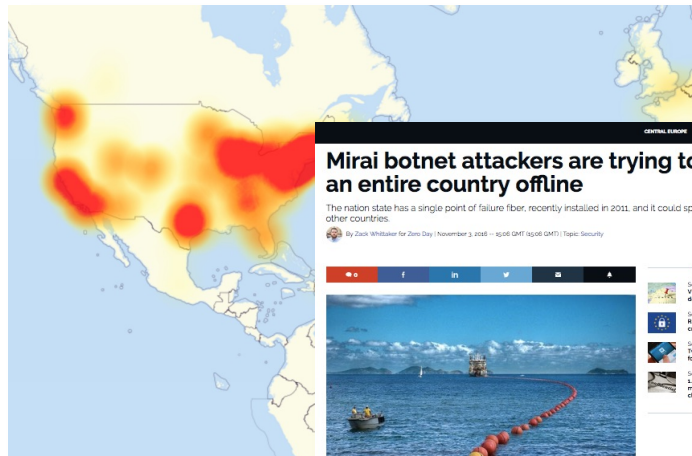
Partners: SIDN, University of Twente, Telecom Italia, FORTH, University of Zurich, SURF, University of Lancaster, CODE





DDoS remains relevant

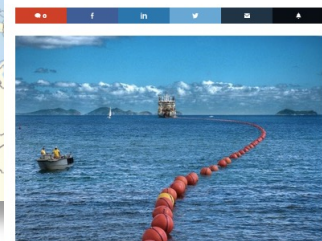
Mirai botnet, 2016



Mirai botnet attackers are trying to knock an entire country offline

The nation state has a single point of failure fiber, recently installed in 2011, and it could spread to other countries.

By Zack Whitaker for Zero Day | November 3, 2016 -- 10:06 GMT (10:06 GMT) | Topic: Security



A single submarine cable, like the one pictured, provides the bulk of the nation's internet. (Image: Ito photo)

One of the largest Distributed Denial-of-Service (DDoS) attacks happened this week and almost nobody noticed.

Since the cyberattack on Dyn two weeks ago, the internet has been on edge, fearing another massive attack that would throw millions off the face of the web. The attack was said to be upwards of 1.1 Tbps -- more than double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 600Gbps in size, said to be one of the largest at the time. The attack was made possible by the Mirai botnet, an open-source botnet that anyone can use, which harnesses the power of insecure Internet of Things (IoT) devices.

This week, another Mirai botnet, known as Botnet 14, began targeting a small, little-known African country, Liberia, sending

PARIS BREXIT DATA LEAK
Panama Bread data leak reportedly exposed millions of customer records

LLNL How to use Cloakflare DNS service to speed up and secure your internet

Intel We saw won't ever patch Spectre variant 2 flaw in these chips

Windows 10 security

Estonia, 2007



Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen

MA 29 JANUARI, 10:50 AANGEPAST MA 29 JANUARI, 11:37 BINNENLAND, ECONOMIE

DigiD Je eigen inlogcode voor de hele overheid

Home Nieuws Over DigiD Mochtigen Veiligheid Waag en antwoord Startpagina Lees meer

DigiD aanvragen

DigiD activeren

Machtiging regelen

Inloggen Mijn DigiD

9 januari 2013 - DigiD is op dit moment niet beschikbaar. Naar verwachting kunt u morgenochtend weer gebruikmaken van DigiD. Onze excuses voor het ongemak.

DigiD Met uw persoonlijke DigiD (een gebruikersnaam en wachtwoord) kunt u zich identificeren op websites van de overheid en van organisaties die ongedefinieerd ANP

De golf van DDoS-aanvallen op Nederlandse instellingen houdt aan. Vandaag is de Belastingdienst tweemaal getroffen, en sinds 15.45 uur heeft ook DigiD last van een DDoS-aanval waardoor de site slecht bereikbaar is.

Volgens een woordvoerder van DigiD "gebeurt een aanval wel vaker, maar dit is wel zwaar". Er wordt hard gewerkt aan een oplossing. Hoelang dat nog gaat duren, kan de woordvoerder niet zeggen.

The Netherlands, September 2020

Opnieuw vinden grootschalige ddos-aanvallen op Nederlandse providers plaats

Dinsdag worden opnieuw meerdere Nederlandse providers getroffen door ddos-aanvallen. Die lijken groter in omvang te worden en ook redelijk gevarieerd te zijn. Onder andere Signet, Calway en Delta zijn dinsdag slachtoffer.

De ddos-aanvallen vinden onder andere plaats bij Calway, bevestigd de provider. Eerder op dinsdagochtend had provider Delta last van een ddos-aanval die werd veroorzaakt door een ddos-aanval. Verder wordt er dinsdagochtend een grote aanval plaats op Signet. Dit is een signaal van de infrastructuur voor veel kleine providers verzorgd. Ook beheert Signet infrastructuur voor TransIP. Daar hadden klanten vernidigd ook slachtoffer door de aanval, al zijn die inmiddels opgelost.

Het lijkt erop dat het om dezelfde aanvallen gaat als de vorige week. Nederlandse providers treffen, al is dat niet met zekerheid te zeggen. Volgens een woordvoerder van het NISII gaat het voornamelijk om drie ernstigere en vroege aanvallen. Het Nederlandse Beheersorgaan voor Internet Providers beheert de en bedrijven ddos-verkeer naar toe kunnen lossen om energie capaciteit om de aanvallen af te slaan, zegt de

House of Representatives of The Netherlands, Oct 2020



This massive DDoS attack took large sections of a country's internet offline

More than 200 organisations across Belgium including the government and parliament were affected by a DDoS attack that overwhelmed them with bad traffic.

By Danny Palmer | May 5, 2021 -- 11:14 GMT (12:14 BST) | Topic: Security

DDoS attacks: Simple but effective: Why DDoS attacks are still a major cyber threat to your networks

Simple but effective: Why DDoS attacks are still a major cyber threat to your networks

Belgium, May 2021

Liberia, 2016

The Netherlands, January 2018



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

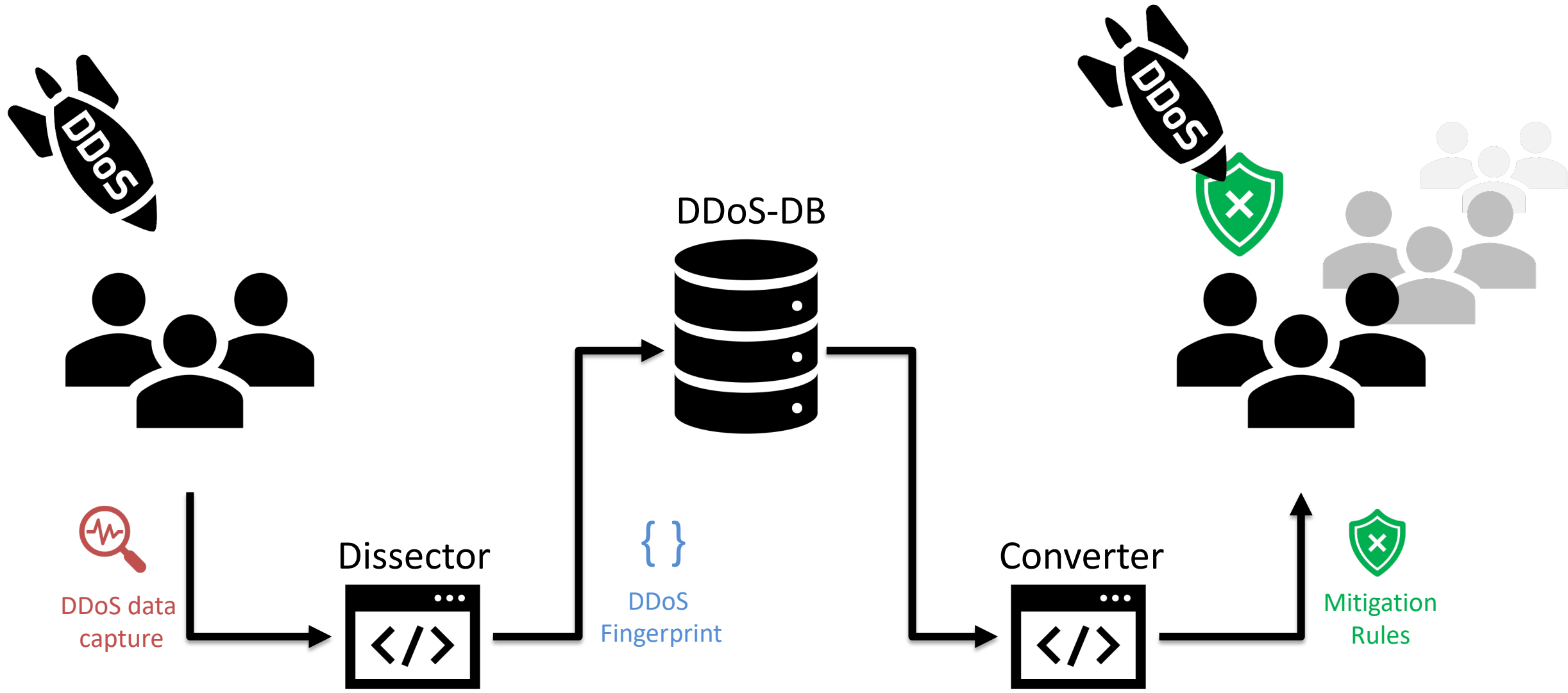
DDoS Clearing House: use-inspired research



Anti-DDoS-Coalition
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**

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: [
        "10.100.100.100"
        "10.100.100.100"
        "10.100.100.100"
        "10.100.100.100"
      ]
    }
  ]
  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)



CONCORDIA partner

CONCORDIA partner

CONCORDIA partner



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: SIDN Labs + NL-ADC members

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

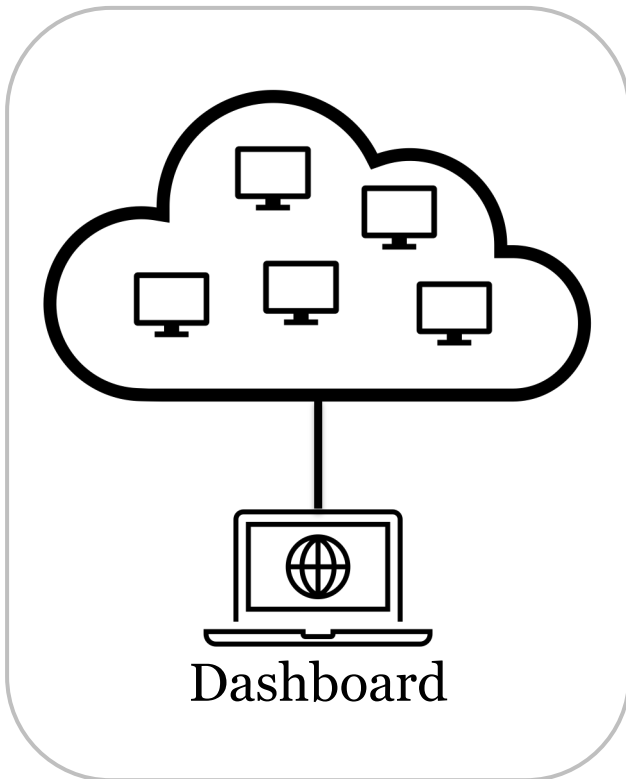
Dev: software engineer (TBD)
Ops: database operator (NBIP) + NL-ADC members

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



Coalition



Member 1

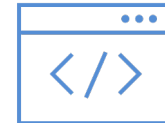


Member 2

DDoS Clearing House



Converter



Dissector



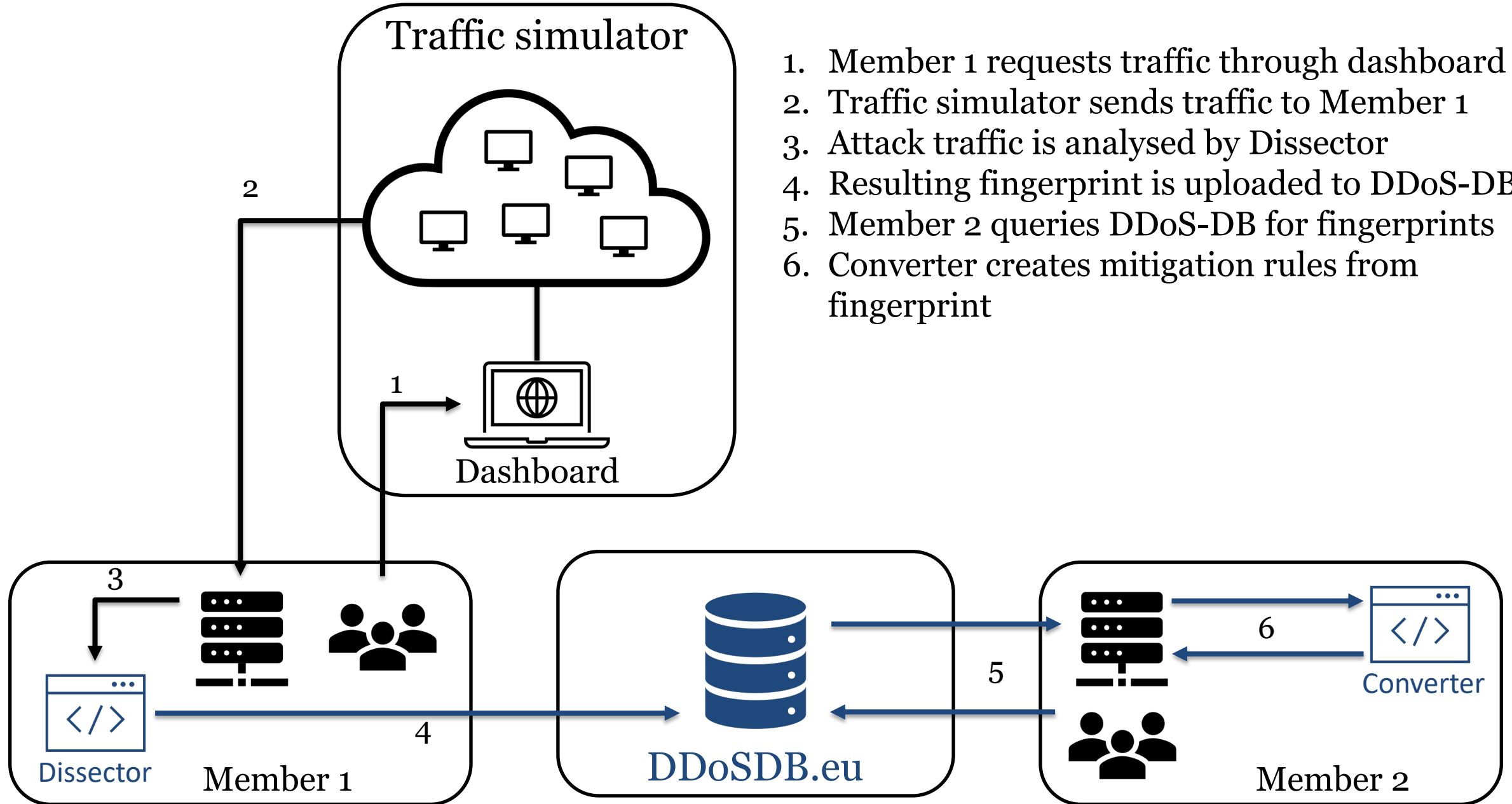
Converter



Dissector

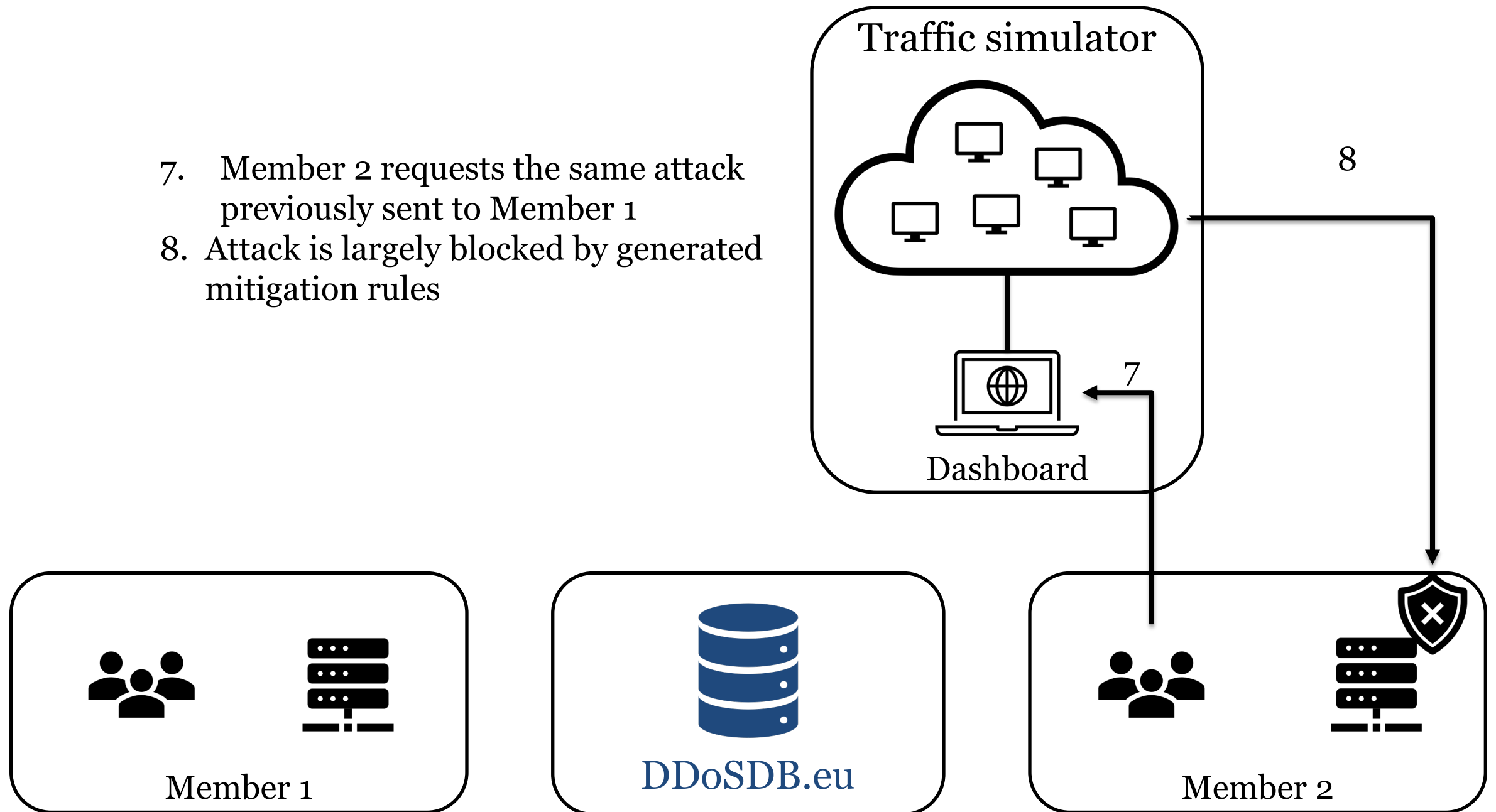


DDoS DB



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](https://twitter.com/hesselma)
+31 6 25 07 87 33

Thijs van den Hout
thijs.vandenhout@sidn.nl
[@thijsvandenhout](https://twitter.com/thijsvandenhout)