



# CONCORDIA

*Cyber security cOmpeteNCe fOr Research and InnovAtion*

## DDoS Clearing House for Europe

ICANN71 vTechDay

June 14, 2021

Cristian Hesselman

(SIDN Labs)

**Partners:** SIDN, UT, TI, FORTH, UZH, SURF, ULANC, CODE





# High-impact DDoS Examples

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 stop other countries.

By Zach Whitaker for ZDNet | November 3, 2016 - 10:08 GMT (UTC) Topic: Security

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 operated by L3370 - made that double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 400,000 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 2.0, began targeting a small, little-known African country, Liberia, sending

**HERE SECURITY NEWS**  
Powers Broad data leak reportedly exposed millions of customer records  
LLN: How to use Cloudflare's DNS service to speed up and secure your internet  
How: We now won't ever patch Spectre variant 2  
See in these clips  
Windows 10 security...

Liberia, 2016

Estonia, 2007



**Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen**

13 MA 19 JANUARI, 10:55 AANGESMET MA 19 JANUARI, 17:37 BINNENLAND ECONOMIE

DigiD de eigen inlogcode voor de hele overheid

Home Nieuws Over DigiD Maatregelen Veiligheid Waag en erandoer

**DigiD** DigiD aanvragen DigiD activeren Machtiging regelen Inloggen Mijn DigiD

Huid uw burgersvoornummer (of uw mobiele telefoon) bij de hand. DigiD de de hand

Handige links  
• Wachtwoord vergeten?  
• Hoe mijn naam wijzigen?  
• Hoe mijn wachtwoord wijzigen?

Laatste nieuws  
• Wachtwoord vergeten? DigiD  
• Wachtwoord wijzigen DigiD  
• Is uw computersysteem geschikt om...

Waar u kunt inloggen  
U kunt uw DigiD gebruiken bij ruim 500 organisaties.

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, January 2018

The Netherlands, September 2020

**Opnieuw vinden grootschalige ddoS-aanvallen op Nederlandse providers plaats**

Dinsdag worden opnieuw meerdere Nederlandse providers getroffen door ddoS-aanvallen. Dit is het grootste in omvang te worden en ook ruimelijk governance te zijn. Onder andere Sigent, Calway en Delta zijn dinsdag slachtoffer.

De ddoS-aanvallen vinden onder andere plaats bij Calway, Delta, Sigent, Calway, Delta, Sigent, Calway en Delta zijn dinsdag slachtoffer. Eerder op donsdagochtend had provider Delta (01.01.01.01.01.01) de werkdag vooraf door een ddoS-aanval. Verder vond er dinsdagmiddag een grote aanval plaats op Sigent. Dit is een tip die de infrastructuur voor veel kleine providers verzorgt. Dit betreft Sigent infrastructuur voor TransIP. Daar hadden klanten vreesde om uitgesloten door de aanval, al zijn die inmiddels opgelost.

Het lijkt erop dat het om dezelfde aanvallen gaat als die vorig week Nederlandse providers troffen, al is dat niet met zekerheid te zeggen. Volgens een woordvoerder van het NISII gaat het voornamelijk om drie applicatie- en top-aanvallen. Het Nederlands Belastingagentschap (Belastingdienst) bevestigt de applicatie- en top-aanvallen. Het NISII heeft een bericht over de aanvallen. Het NISII heeft een bericht over de aanvallen. Het NISII heeft een bericht over de aanvallen.

**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 (UTC+01:00) 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

Security Ransomware: There's been a big rise in double extortion attacks as gangs try out new tricks

Security This malware has been rewritten in the Rust programming language to make it harder to spot

Belgium, May 2021

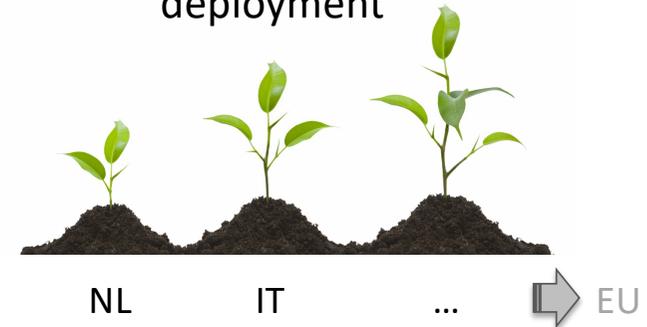


# Objective

- Enable European critical infrastructure to proactively and collaboratively protect themselves against DDoS attacks
- Pilot a DDoS Clearing House with European industry for Europe that can also be used elsewhere
- Key outputs: pilots in the Netherlands and Italy, DDoS clearing house blueprint



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





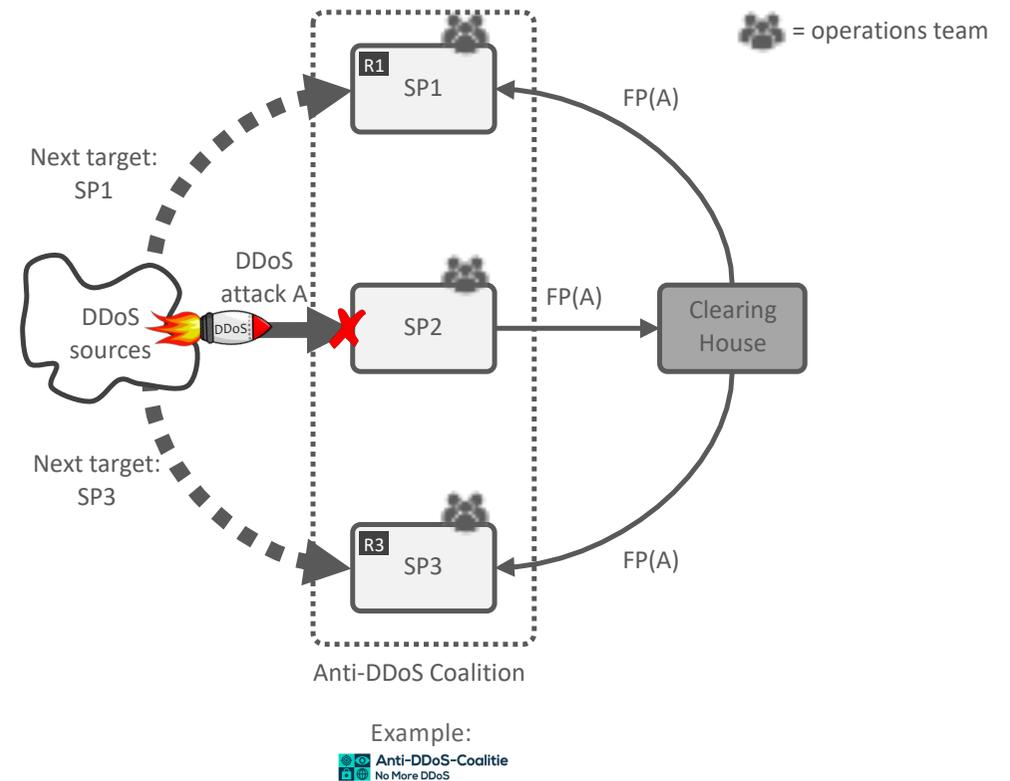
# Key innovations

- Bridge **multidisciplinary gap** to deployment, more than tech!
- **Opensource design** that we make available through a “cookbook”
  - Technology, legal, organizational, experiences, lessons learned
  - Main use case is Dutch Anti-DDoS Coalition
  - Enable other groups of organizations to set up their clearing house
- Can operate across **heterogeneous networks**



# DDoS Clearing House Concept

- Continuous and automatic sharing of “DDoS fingerprints”, buys providers time (proactive)
- Extends DDoS protection services that critical service providers use and does not replace them
- Generic concept: across sectors, Member States, business units, etc.





# Fingerprint Example

```
{
  "attack_vector": [
    "src_ips": [
      omitted;
    ],
    "attack_vector_key": "66f2e83fde0e6351d3f5ad967c6230aa3b60dbc498ad13b074296cb5f84c7734",
    "one_line_fingerprint": "{ 'dns_qry_type': 1, 'ip_proto': 'UDP',
    'highest_protocol': 'DNS', 'dns_qry_name': 'a.packetdevil.com',
    'frame_len': 1514, 'udp_length': 4103, 'srcport': 53,
    'fragmentation': True, 'src_ips': 'omitted' }"
  ],
  "start_time": "2013-08-14 23:04:00",
  "duration_sec": 0.16,
  "total_dst_ports": 4649,
  "avg_bps": 143426993,
  "total_packets": 16471,
  "ddos_attack_key": "44518107642b9ac7098174a16cbf220395c862bf26389c734e0b109b318e9291",
  "key": "44518107642b9ac",
  "total_ips": 2065,
  "tags": [
    "AMPLIFICATION",
    "DNS",
    "FRAGMENTATION",
    "UDP_SUSPECT_LENGTH",
    "DNS_QUERY",
    "SINGLE_VECTOR_ATTACK"
  ]
}
```

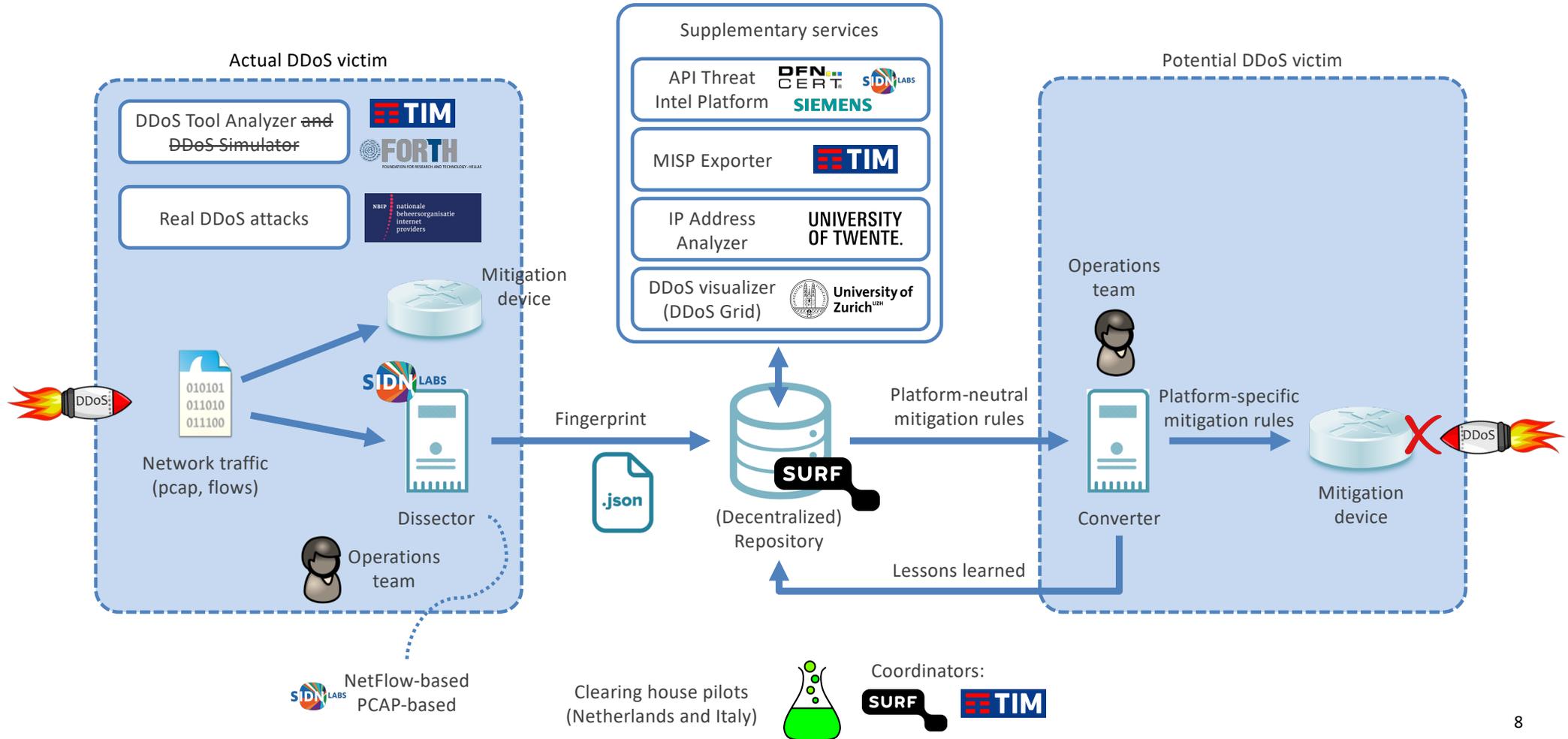


# Clearing House increases Digital Autonomy

- Increased **insight** of potential victims into DDoS attacks from their own narrow view to an ecosystem-wide view
- Increased **control** because the new DDoS insights give organizations more grip on how to handle DDoS attacks and the requirements for their DDoS mitigation facilities (their own or those of a contracted third party)
- ADCs also build up a joint **pool of expertise** independent of particular DDoS mitigation providers through drills and best common practices

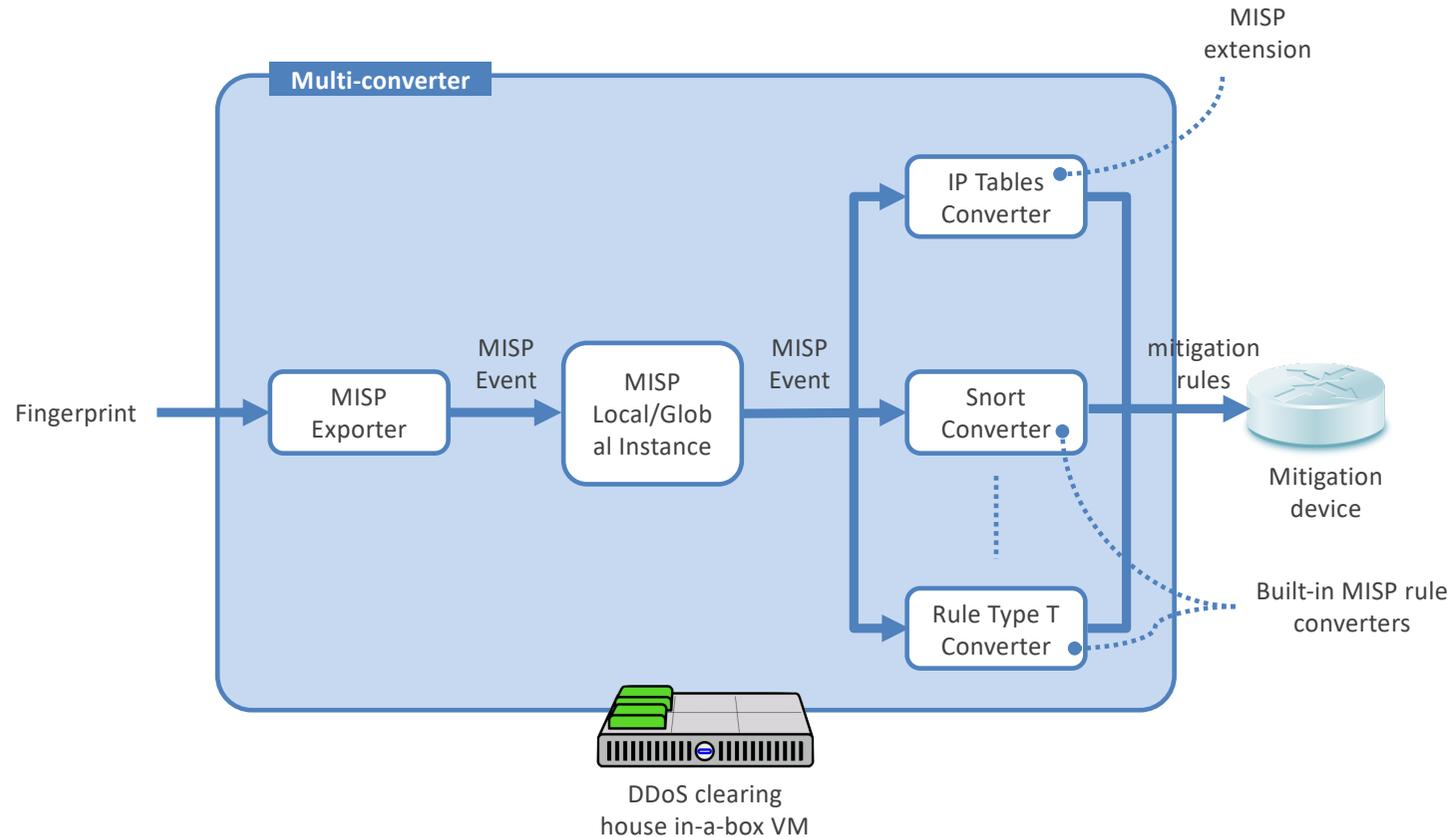


# Main Components and Data Flows





# Multi-converter





# Component Maturity Indication

Name	Function	Maturity
Dissector	Generate DDoS fingerprints based on PCAP files and flows data	High
DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High
Converter	Generate mitigation rules based on DDoS fingerprints	Medium
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Low
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Low
MISP Exporter	Generate MISP events based on DDoS fingerprints	Medium





```
jan@tpj: ~/ddos_dissector
jan@tpj: ~
λ tpj ddos_dissector → λ git 3.0* → ./ddos_dissector.py -f ./pcap_samples/sample3.pcap --upload --host https://www.csg.uzh.ch/ddosgrid/ddosdb/ --user jan --passwd gg
```

Search the Web

**You're in a Private Window**

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

[Common myths about private browsing](#)

Need more privacy?  
[Try Mozilla VPN](#)

Oct 7 11:42



# DDoS clearing house in the Netherlands



**Anti-DDoS-Coalitie**  
No More DDoS

- DDoS clearing house R&D
- DDoS clearing house cookbook
- Technical evaluation through pilots in the Netherlands and Italy
- Sharing of operational experience
- Large-scale multi-party DDoS drills
- **DDoS clearing house operations**
- Operational ADC organization



# Dutch National Anti-DDoS Coalition



CONCORDIA partner

CONCORDIA partner

CONCORDIA partner





# Status Dutch Anti-DDoS Coalition

- Members committed to a more sustainable model (Dec 2020)
- Approved fee-based budget (EUR 114K total)
- Structure of WGs, **clearing house** operator and software developer
- Consortium agreement under development
- Core team governing the Dutch ADC



**Anti-DDoS-Coalitie**  
No More DDoS

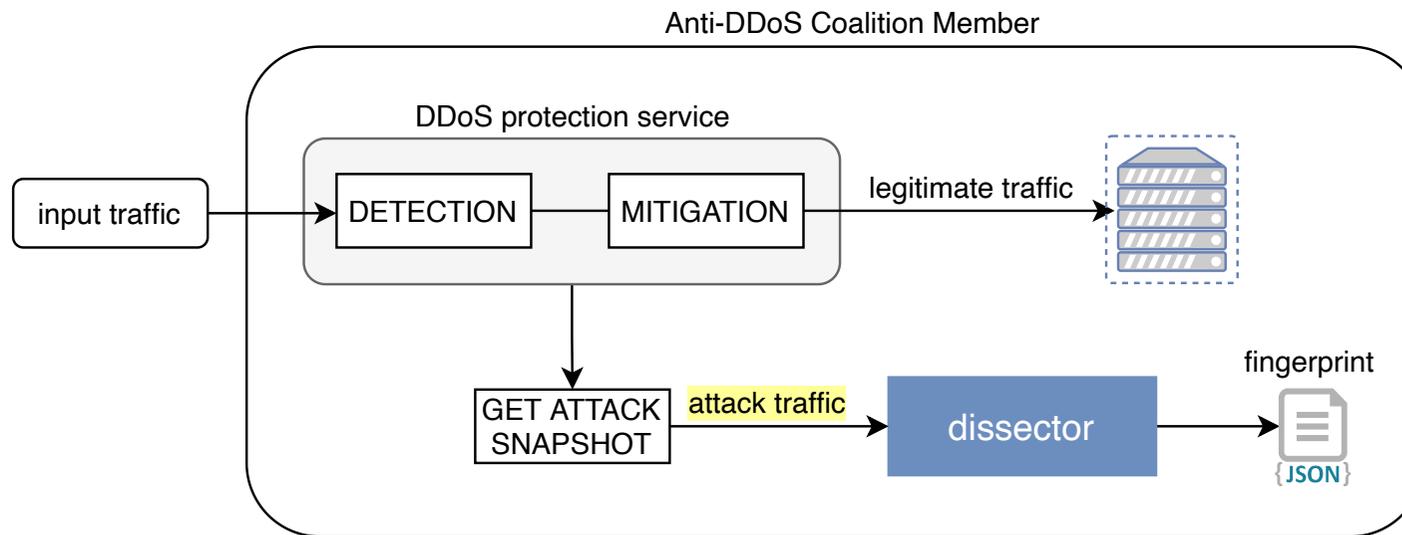


# DDoS Clearing House Planning @Dutch ADC

- Phase 0: pilot, Q2 and Q3 2021
  - Development by CONCORDIA T3.2 team
  - Operations with CONCORDIA and Dutch ADC partners
- Phase 1: basic production, Q4 2021
  - Development by CONCORDIA T3.2 team
  - Operations with Dutch ADC partners
- Phase 2: full production, Q1 2022 and onward
  - Development and operations with Dutch ADC partners



# Key challenge: deployment in networks





# Outlook 2021

- Couple with **production systems** of partners in the Dutch ADC, initially at our partner NBIP (Dutch ADC)
- Further **mature the clearing house's components**, such as
  - Extend the Dissector with additional fingerprint generation modules
  - Develop a MISP extension for authoring and distributing DDoS filtering rules
- First published version of the DDoS clearing house **cookbook** (e.g., as a paper for the Journal on Internet Services and Applications)



## Further reading

<https://www.sidnlabs.nl/en/news-and-blogs/new-ddos-classifiers-for-the-ddos-clearing-house>

<https://www.sidnlabs.nl/en/news-and-blogs/work-in-progress-the-concordia-platform-for-threat-intelligence>

<https://www.sidnlabs.nl/en/news-and-blogs/new-version-of-the-ddos-clearing-house-core-components>

<https://www.sidnlabs.nl/en/news-and-blogs/dutch-anti-ddos-coalition-lessons-learned-and-the-way-forward>

<https://www.sidnlabs.nl/en/news-and-blogs/setting-up-a-national-ddos-clearing-house>

<https://www.sidnlabs.nl/en/news-and-blogs/increasing-the-netherlands-ddos-resilience-together>



### Contact

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

[contact@concordia-h2020.eu](mailto:contact@concordia-h2020.eu)

### Follow us



[www.concordia-h2020.eu](http://www.concordia-h2020.eu)



[www.twitter.com/concordiah2020](https://www.twitter.com/concordiah2020)



[www.facebook.com/concordia.eu](https://www.facebook.com/concordia.eu)



[www.linkedin.com/in/concordia-h2020](https://www.linkedin.com/in/concordia-h2020)



[www.youtube.com/concordiah2020](https://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](mailto:cristian.hesselman@sidn.nl)  
[@hesselma](https://twitter.com/hesselma)  
+31 6 25 07 87 33

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