CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

DDoS Clearing House for Europe (Task 3.2)

6th CONCORDIA General Assembly

Cristian Hesselman
(SIDN Labs)

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

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

Key takeaways

- Key achievements Y2: advanced clearing house prototype's core components and supplementary services (demos, not today though)
- DDoS clearing house selected for EC's Innovation Radar (Jan 2021)
- Dutch ADC: moving to sustainable ecosystem (funding, CA) and draft planning to take clearing house into production

No More DDoS
Anti-DDoS-Coalitie

- Y3 focus: (1) coupling with production systems for NL pilot, (2) further technical improvements, (3) publish first version of cookbook

Deployment in the Netherlands

- 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

T3.2 objective

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

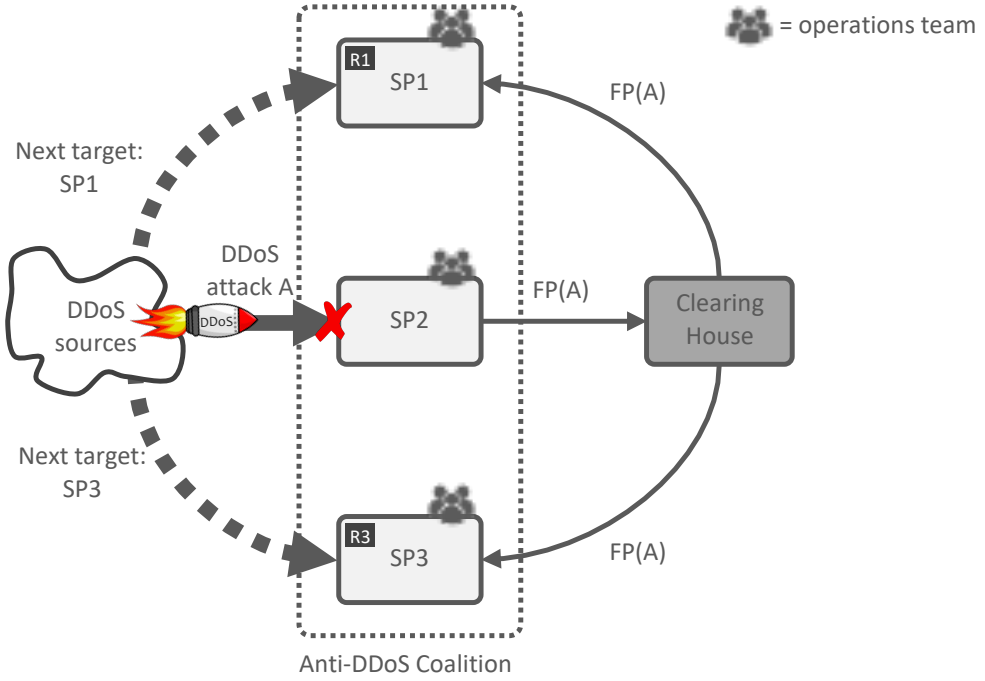
- Learn how to bridge **multidisciplinary gap** to deployment, more than tech!

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

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

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: per Member State, per sector, per business unit, etc.



Fingerprint Example


```
<snip>
{
  "dns_qry_type": [
    255
  ],
  "ip_proto": [
    "UDP"
  ],
  "highest_protocol": [
    "DNS"
  ],
  "dns_qry_name": [
    "evil.com"
  ],
  "eth_type": [
    "0x00000800"
  ],
  "srcport": [
    53
  ],
  "fragmentation": [
    false
  ],
  "tags": [
    "DNS",
    "DNS_QUERY",
    "AMPLIFICATION"
  ],
"start_time": "2013-08-14 23:32:40",
"total_dst_ports": 1043,
"avg_bps": 28406714,
"total_packets": 19183,
"total_ips": 393,
}

<snip>
```

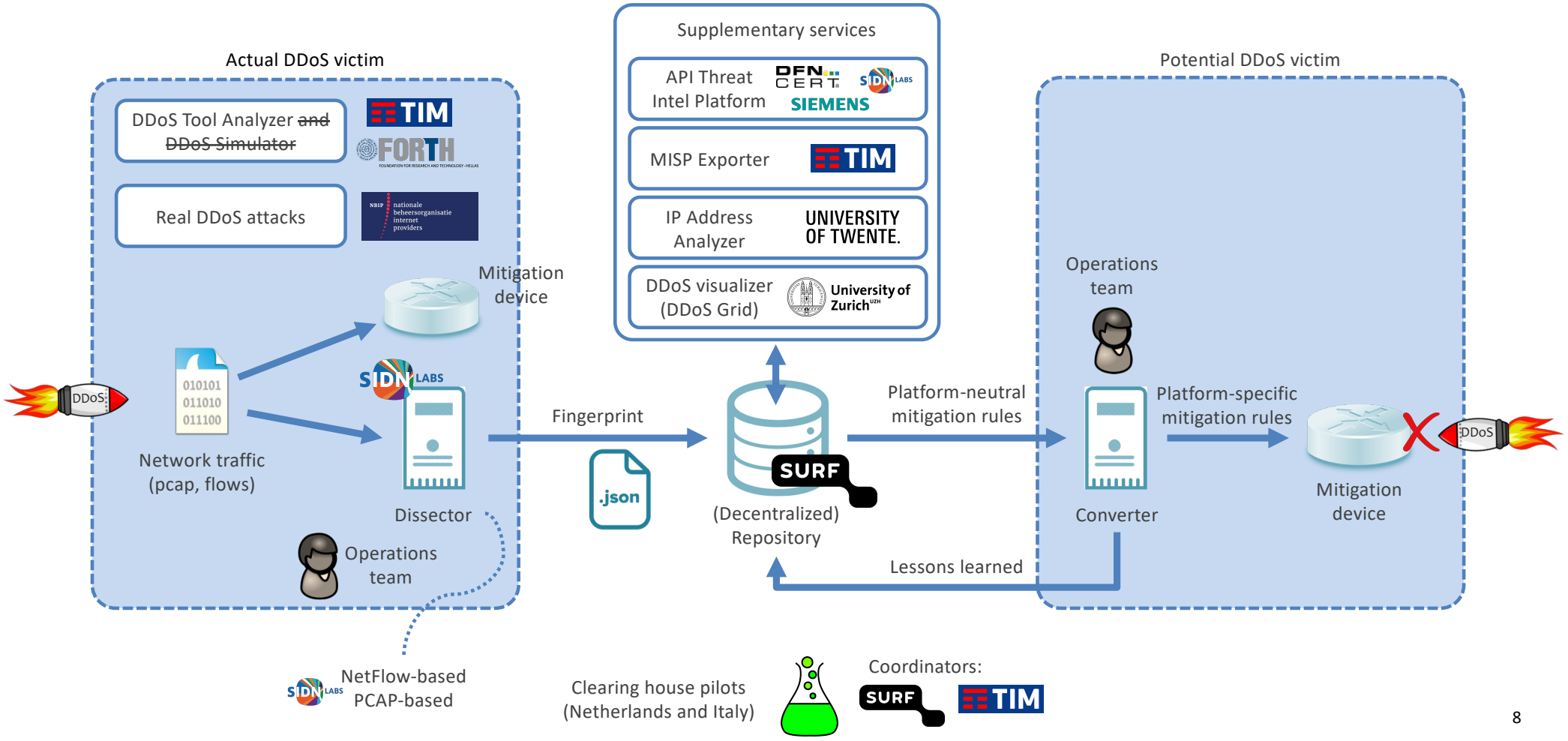
Clearing House increases Digital Sovereignty

- Increased **insight** of potential victims into DDoS attacks from their own narrow view to an ecosystem-wide view

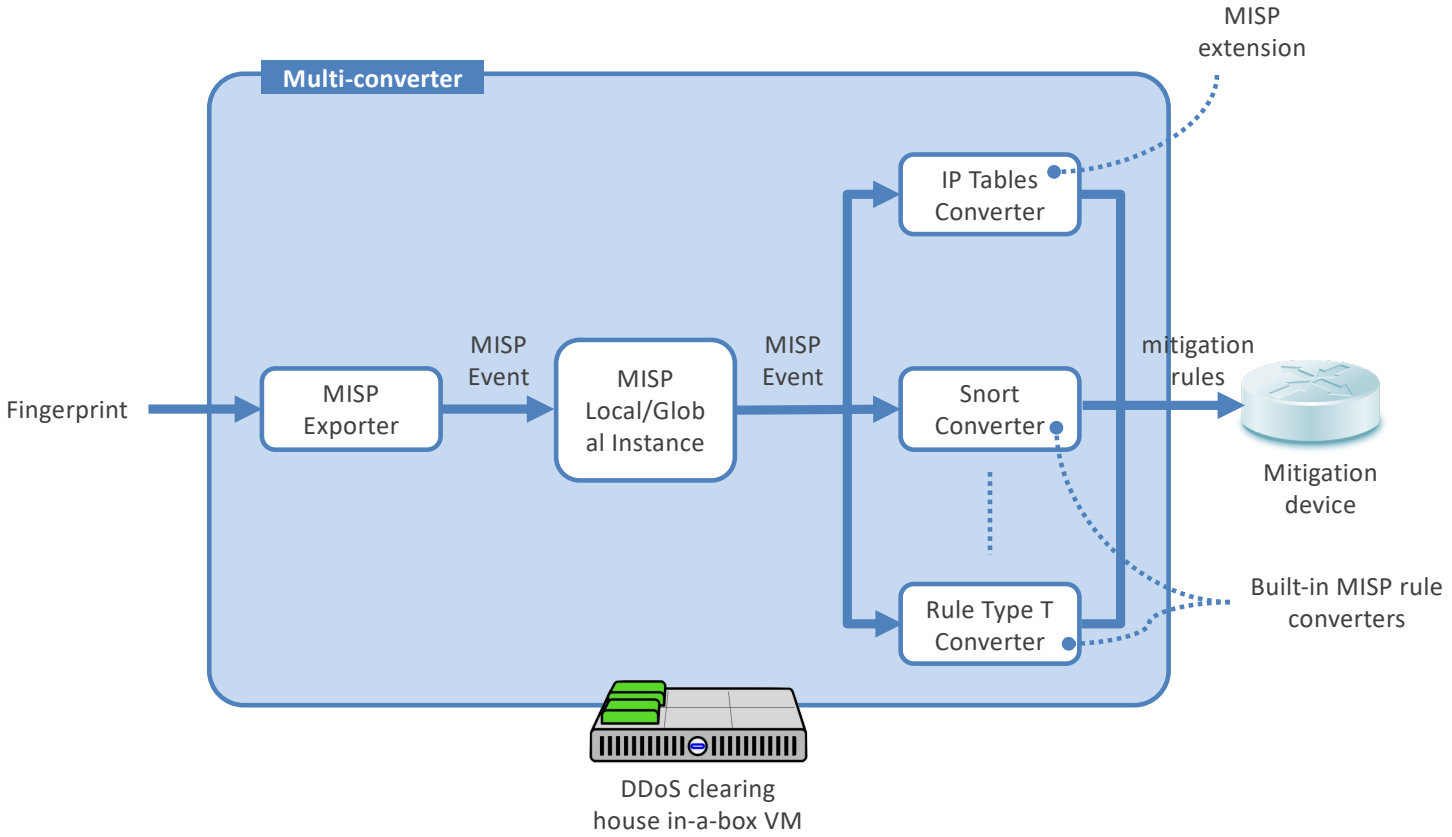
- Increased **control** because the new insights give organizations more grip on how to handle DDoS attacks and the requirements for their DDoS mitigation facilities (their own or those of a contracted third party)

- 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



Advancements of components in Y2

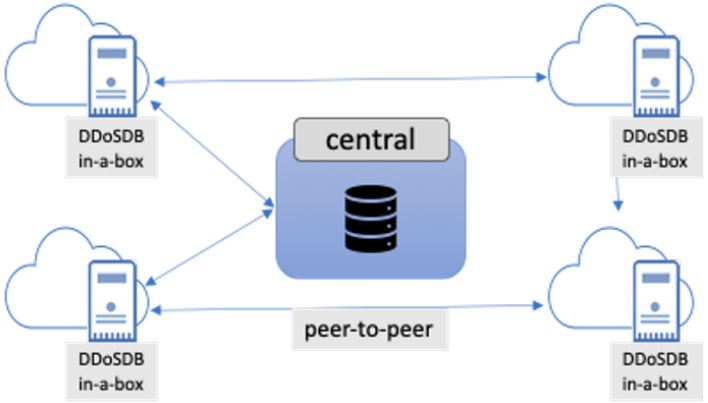
- Dissector: new fingerprint generation algorithms, support for netflow
- DDoSDB: added fingerprint synch between DBs, improved web interface
- Converter: investigating how to incorporate it into MISP

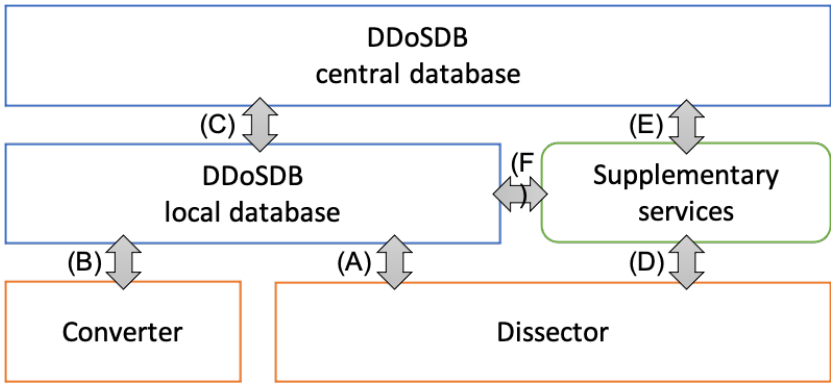
- MISP exporter: first version that maps fingerprints to MISP events
- Tool analyzer: fingerprints nmap, hping3, ddos_sim powered attacks
- DDoS grid: interactive analysis and generation of fingerprints
- IP address analyzer: first basic implementation

Details in D3.2, “2nd year report on community building and sustainability”, Dec 2020

Architecture advancements in Y2

- Refined clearing house overall architecture (components, interfaces)
- Introduced DDoS clearing house-in-a-box, including auto-update
- Coupled components through APIs





Details in D3.2, “2nd year report on community building and sustainability”, Dec 2020

Dissemination in Y2

- 14 external and internal presentations
- External talks at the Dutch ADC, ICANN68, and ETNO, amongst others
- 6 blogs, 1 paper

Details in D3.2, “2nd year report on community building and sustainability”, Dec 2020

Lessons learned in Y2

- Modular design is key to decentralized architecture, our demo-driven way of working, and to compensate for Covid
- The Dissector needs to support multiple types of traffic capturing formats (PCAP, netflow) because of differences in operators' networks
- MISP might be a good candidate for sharing fingerprints (e.g., supports communities and DB-synch), but is also limited in filtering rules and for representing fingerprints

Details in D3.2, "2nd year report on community building and sustainability", Dec 2020

Outlook Y3

- 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)

Details in D3.2, "2nd year report on community building and sustainability", Dec 2020

Collaboration Y3

- T1.2 (Network-Centric Security): for research that might be required to develop new types of Dissectors or to measure attackers' infrastructure
- T2.1 (Telco Pilot) and T2.3 (Charging Pilot): study how the Clearing House can help mitigating DDoS attacks on these infrastructures
- T3.1 (Building a Threat Intelligence for Europe): to refine CONCORDIA Treat Intelligence Platform and interaction with the DDoS Clearing House
- T4.2 (Legal aspects): to develop a "code of engagement" document for organizations to join the DDoS Clearing House as it continues to evolve.

Details in D3.2, "2nd year report on community building and sustainability", Dec 2020

Dutch National Anti-DDoS Coalition

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

No More DDoS
Anti-DDoS-Coalitie

- Core team governing the Dutch ADC

DDoS Clearing House Planning @Dutch ADC

- Phase 0: pilot, March through ~July 2021
  - Development by CONCORDIA T3.2 team
  - Operations with CONCORDIA and Dutch ADC partners
- Phase 1: basic production, July 2021 through ~Dec 2021
  - Development by CONCORDIA T3.2 team
  - Operations with Dutch ADC partners
- Phase 2: full production, Jan 2022 and onward
  - Development and operations with Dutch ADC partners

Phase 0 (Pilot)

- Operations
  - 3+ partners use Dissector in their networks and share fingerprints ◉◉
  - Initial set of fingerprints in ddosdb.nl ◉
  - SIDN Labs is the DDoS-DB operator ◉◉
  - Data sharing based on existing agreement with SIDN ◉
- Development
  - Further improved clearing house software ◉
  - BCOP to connect ADC members and operate the clearing house ◉◉
  - BCOP and other learnings captured in DDoS clearing house cookbook ◉

◉ CONCORDIA T3.2 responsibility ◉ Dutch ADC responsibility

Phase 1 (Basic Production)

- Operations
  - NBIP is the DDoS-DB operator (to be OK'ed by Dutch ADC members)
  - Additional ADC members connected

- Development
  - CONCORDIA s/w updates regularly transitioned into production
  - DDoS clearing house cookbook updated
  - Contracted software company to replace CONCORDIA T3.2 in phase 2

CONCORDIA T3.2 responsibility Dutch ADC responsibility

Phase 2 (Full Production)

- Operations
  - NBIP is the DDoS-DB operator (see Phase 1)
  - Additional ADC members connected (continued from Phase 1)

- Development
  - Software development company improves s/w (open source)
  - DDoS clearing house cookbook updated
  - CONCORDIA T3.2 focuses on development for pilot in Italy

CONCORDIA T3.2 responsibility Dutch ADC responsibility

Outlook Y4 (project end)

- Pilot in the Netherlands: 3+ member organizations of the Dutch ADC sharing fingerprints (inter-organization)

No More DDoS
Anti-DDoS-Coalitie

- Pilot in Italy: 3+ TI departments sharing fingerprints (intra-organization)
  - Security Lab, internal SOC, anti-DDoS team
  - Optionally with other orgs in Italy (e.g., universities)

TIM

- Cookbook and tech report combined in a peer-reviewed paper

Further reading

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 (T3.2 lead)
cristian.hesselman@sidn.nl
@hesselma
+31 6 25 07 87 33

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/