



CONCORDIA

Cyber security cOmpeteNCe fOr Research and InnovAtion

DDoS Clearing House for Europe (Task 3.2) 3rd CONCORDIA review

Cristian Hesselman
(SIDN Labs)

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






Key takeaways

- Key achievements Y2: advanced clearing house prototype's core components and supplementary services (videos)
- Y3 focus: (1) coupling with production systems, (2) further technical improvements, (3) publish first version of cookbook
- Dutch ADC: moving to sustainable ecosystem (funding, CA)
- DDoS clearing house selected for EC's Innovation Radar! (Jan 2021)





Feedback Sep 2020 Review

- “The project has made a good progress concerning the threat intelligence sharing and the DDoS clearing house platforms” 
- Reached out to Multistate ISAC/Center for Internet Security, no luck yet
- However, an ADC is different from an ISAC
 - Cross sector nature (ISACs are single sector)
 - Includes facilities for real-time sharing of DDoS measurements (fingerprints)
 - Includes large-scale collaborative DDoS drills
 - Focused on DDoS attacks rather than all kinds of threats
 - Flexible concept that works for any group of orgs, ISACs or other



DDoS Attacks and Digital Sovereignty

- Increased dependency on online services, especially after Covid
- Risk: increased impact of DDoS attacks, reduces EU's digital sovereignty
 - Loss of control over critical processes
 - Safety risk due to interaction with physical space (cf. WP2)
 - Increased awareness at the policy level
- Key problem: limited access to and sharing of DDoS data
 - Lowers response time and learning because of limited victim-specific view
 - Reduces innovation of processes and systems



House of Representatives
of The Netherlands,
October 2020



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



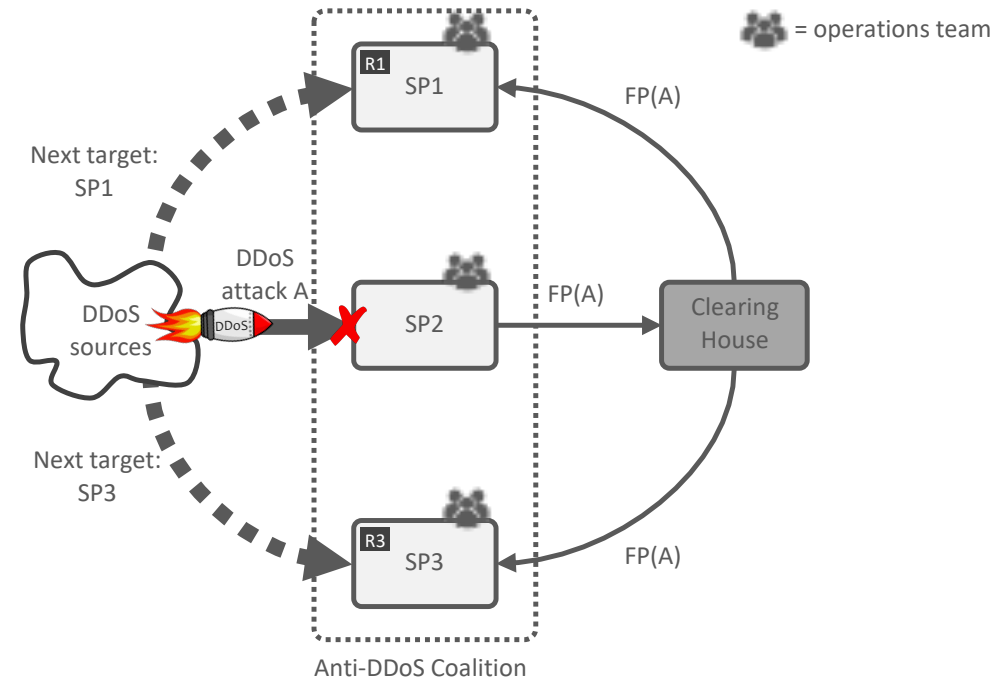
Key challenge: increase to TRL 5-7 and grow deployment





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": [
    "0x0000800"
  ],
  "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



Dutch National Anti-DDoS Coalition



CONCORDIA partner

CONCORDIA partner

CONCORDIA partner





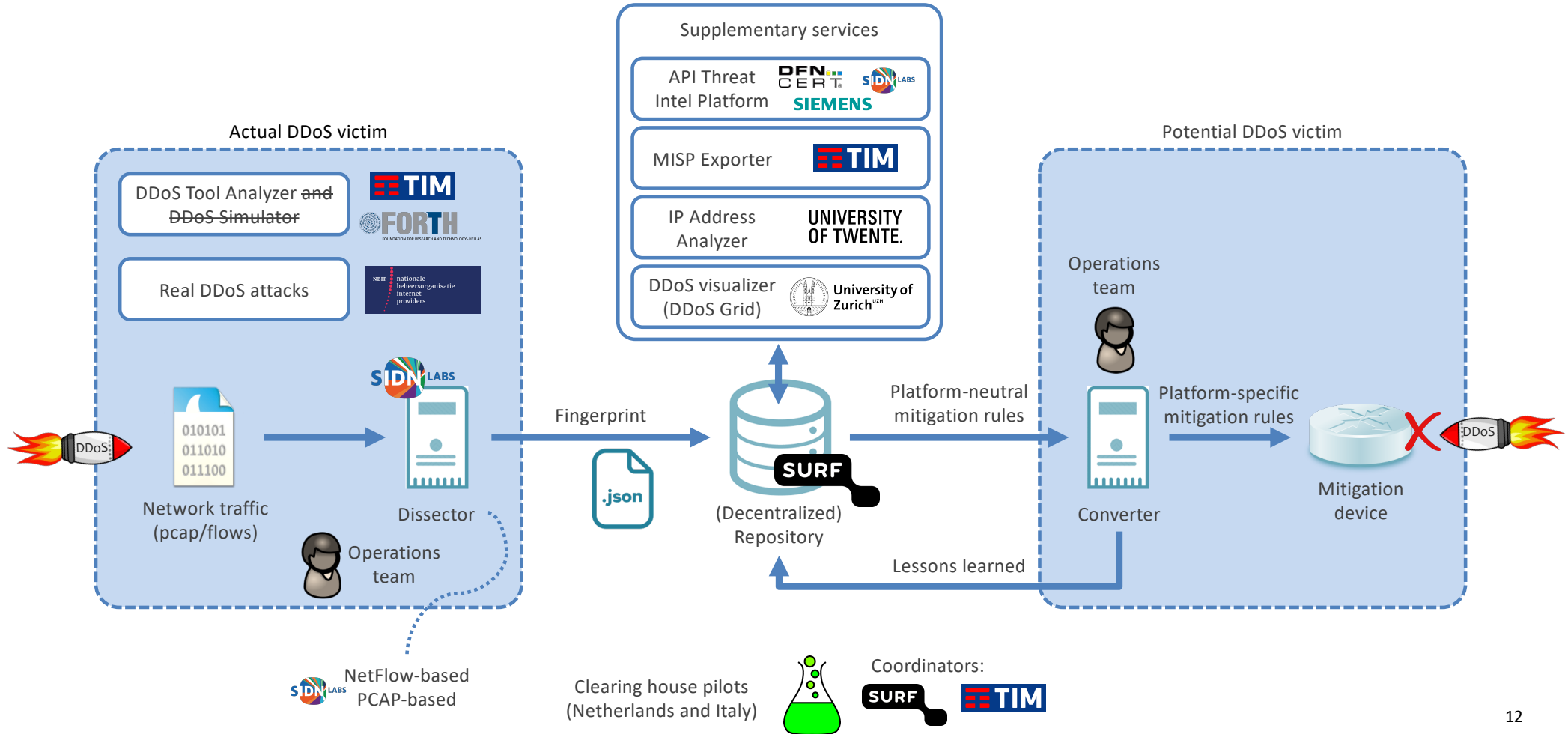
Status Dutch Anti-DDoS Coalition

- 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





Main Components and Data Flows





Component Maturity

	Name	Function	Maturity
	Dissector	Generate DDoS fingerprints based on PCAP files and flow data	High
	DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High
	Converter	Generate mitigation rules based on DDoS fingerprints	Low
Demo #3	DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High
Demo #4	IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Low
Demo #1	DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks (e.g., Hulk, hping3, ddos_sim)	Low
Demo #2	MISP Exporter	Generate MISP events based on DDoS fingerprints	Low
	Traffic generator	Generation of DDoS fingerprints using a TIM's DDoS traffic simulator	Low



Activities Image Viewer Feb 2 12:27

Events - MISP

```
File Edit Tools
```

Home

- List Events
- Add Event
- Import from REST client
- List Attributes
- Search Attributes
- View Properties
- Events with View deleg
- Export
- Automation

```
{  "dns_gry_type": 1.0,  "ip_proto": ["UDP"],  "highest_protocols": ["DNS"],  "dns_gry_name": "mydomain.c",  "eth_type": ["0x0000800"],  "frame_len": 72,  "udp_length": 38,  "ip_ttl": 32,  "dstport": 53,  "fragmentation": false,  "tags": ["DNS", "DNS_QUERY", "UDP_SUSPECT"],  "start_time": "2021-02-02T12:22:49",  "duration_sec": 10,  "total_dst_ports": 1,  "avg_bps": 3388,  "total_packets": 1,  "key": "ca56c6c",  "key_sha256": "8b1a111c5d1797217b40751085914a6d",  "multivector_key": "f7",  "total_ips": 10,  "amplifiers": "188.81.0.8", "188.81.0.6", "188.81.0.5", "188.81.0.5"}
```

T3.2_architecture.png

MISP Interaction (work in progress)

```
graph TD; Dissector[Dissector] -- Fingerprint --> Repo["(Decentralized) Repository (SURF)"]; Repo -- Fingerprint --> MISP[MISP]; MISP -- SNORT mitigation rules --> AuthToolA[MISP-based Authoring Tool]; AuthToolA --> MISP; MISP -- MISP events --> MISP_Exp[MISP Exporter]; MISP_Exp -- SNORT rules --> AuthToolB[Authoring Tool]; AuthToolB -- Platform-specific mitigation rules (now) --> Converter[Converter]; Converter -- mitigation rules --> Mitigation[Mitigation device]; Mitigation -- Lessons learned --> Repo; AuthToolB -.->|Platform-specific mitigation rules (future)| MISP; AuthToolA -.->|Platform-specific mitigation rules (future)| MISP;
```

Operations team A

Operations team B

Dissector

Authoring Tool

Converter

Mitigation device

Dissemination Partners: SIDN LABS, OPEN SIEMENS, TIM

Powered by MISP 2.4.129 - 2021-02-02 12:22:49

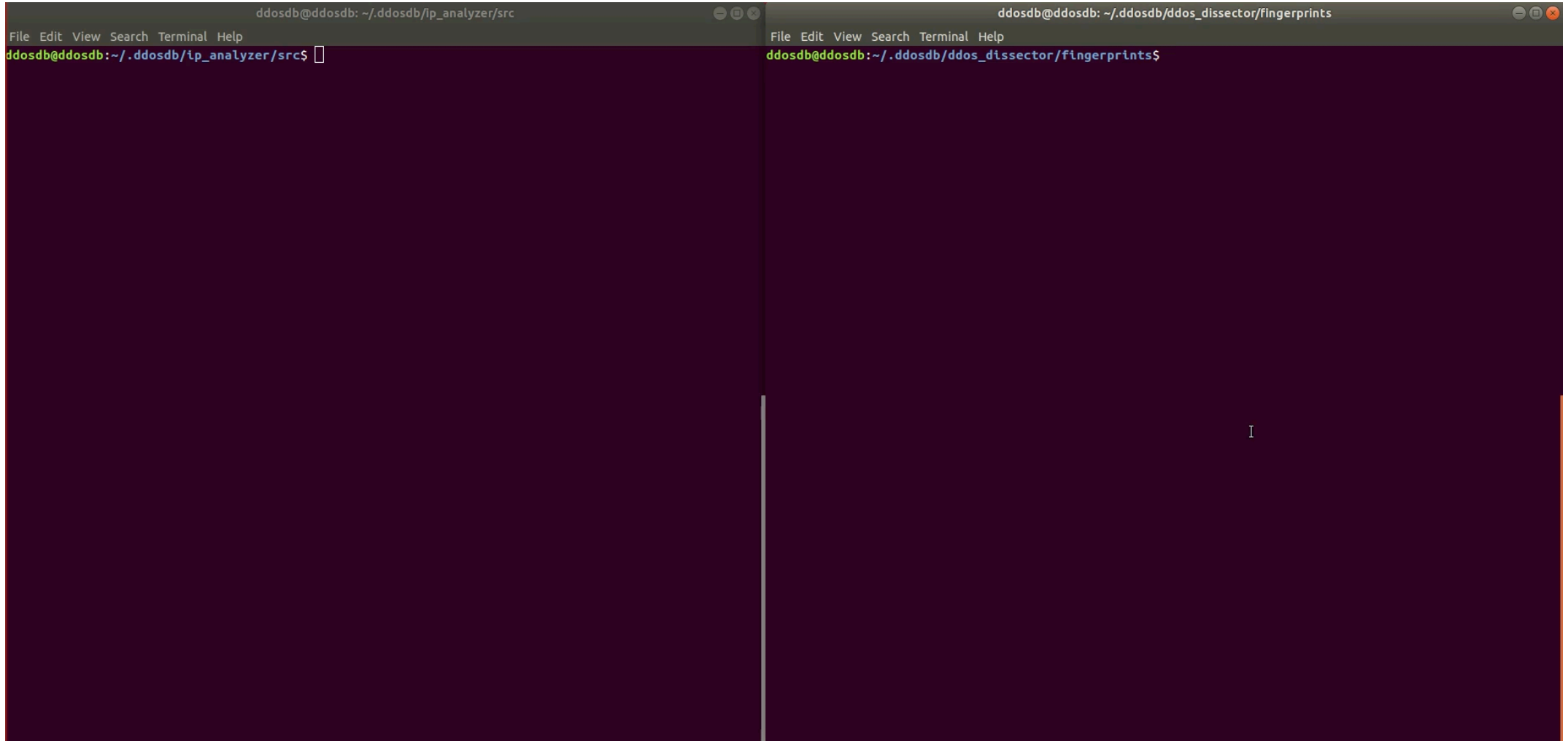
Could not locate the GnuPG public key.



The image shows a desktop environment with two windows. On the left is a terminal window with the following text:

```
jan@tpj: ~/ddos_dissector
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
```

On the right is a Mozilla Firefox Private Browsing window. The page displays the Firefox logo and the text "Firefox". Below the logo is a search bar with the text "Search the Web". A message box says "You're in a Private Window" and explains that Firefox clears search and browsing history. At the bottom of the message box, there is a link: [Common myths about private browsing](#). Below the message box, there is a link: [Need more privacy? Try Mozilla VPN](#). The system tray at the bottom shows the date "Oct 7 11:42" and various icons.





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

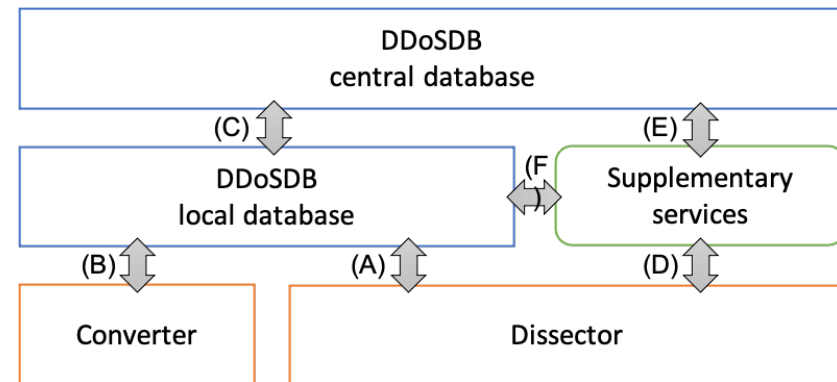
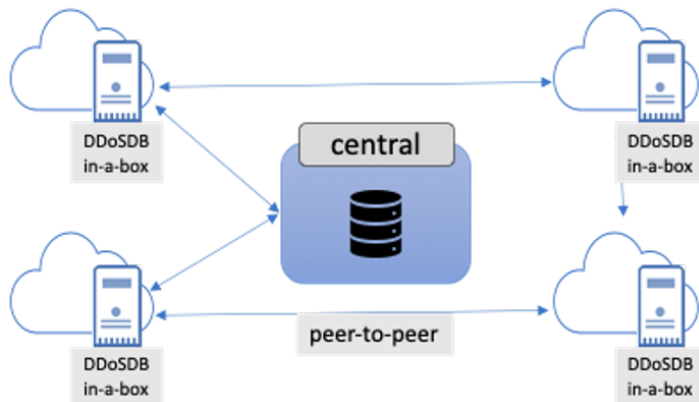
- MISP exporter: first version that maps fingerprints to MISP events
- Tool analyzer: fingerprints nmap, hping3, ddos_sim powered attacks
- DDoS grid: interactive analysis and generation of fingerprints
- IP address analyzer: first basic implementation

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 fullt 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

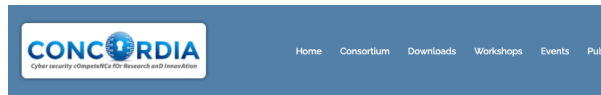


Outlook Y4 (project end)

- Pilot in the Netherlands: 3+ member organizations of the Dutch ADC sharing fingerprints (inter-organization)
 **No More DDoS**
Anti-DDoS-Coalition
- 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



POSTED APRIL 9, 2020 ADMIN CONCORDIA

Increasing the Netherlands' DDoS resilience together

First lessons learned from setting up a national anti-DDoS initiative, part I of III

The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together. In this series of three blogs, we'll first discuss the rationale behind our initiative, then describe a technical facility called the DDoS clearing house that enables coalition members to automatically measure and share the properties of DDoS attacks (e.g. attack duration and source IP addresses), before finally reviewing our key challenges, the lessons learned and the way forward. Our lessons learned are an important input for a "cookbook" to set up anti-DDoS coalitions elsewhere in Europe.

Note: we're using two types of reference in this blog series: hyperlinks refer to information, while numbers between straight brackets ([1]) link to in-depth technical papers.

DDoS attack landscape

A Distributed Denial-of-Service (DDoS) attack overwhelms a network with traffic, thus denuding the network's ability to service legitimate requests from their clients. The attacker typically does this by simultaneously transmitting traffic from a large number of machines distributed across the Internet, often by infecting those machines with malware that carries out the attack. Another type of attack is when an attacker exhausts a server's resources (rather than swamping the network) by repeatedly starting a login session with the server, thus forcing it to make more connections than it can handle.



New version of the DDoS Clearing House core components

The next round of improvements to get it deployed

Geplubliceerd op: donderdag 17 september 2020

SIDN Labs and SURF have released a new version of the DDoS Clearing House in a Box, a system that enables network operators to automatically share details of the DDoS attacks they handle, in the form of 'DDoS fingerprints'. In this blog, we briefly outline our improvements and how they contribute to the trials we'll be carrying out in the Netherlands and Italy.

Anti-DDoS Coalition and CONCORDIA

SIDN and SURF are proud to be part of the Dutch Anti-DDoS Coalition as well as of the CONCORDIA project, where we work on mechanisms and tools that enable service providers to handle DDoS attacks more proactively. Both projects involve numerous organisations including governments, internet providers, internet exchanges, academic institutions, non-profit organisations and banks.

An important building block in both projects is the DDoS Clearing House, a shared system that enables participating service providers to automatically share the characteristics of DDoS attacks they handle in the form of so-called 'DDoS fingerprints'. The tenet here is that to be forewarned is to be forearmed. Sharing DDoS fingerprints with other participants warns them that new attacks may be underway and extends the DDoS mitigation services that participants already have in place, such as scrubbing services like the [hulks](#). Comparing attacks currently in progress with attacks whose details are already recorded in the Clearing House can also provide pointers as to the best way to mitigate ongoing attacks.

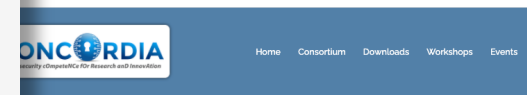
Recent [developments](#) show that DDoS attacks are still very much an issue and - more worryingly - are increasing in size, making our work with the DDoS Clearing House all the more relevant and pressing.



Jojo Ceron
Research engineer
[@jojoceeron](#)



Remco Poortinga-van Wijnen
Team Lead Security @ SURF
[@remco.van.wijnen](#)



POSTED SEPTEMBER 24, 2020 ADMIN CONCORDIA

Work in Progress: the CONCORDIA Platform for Threat Intelligence

First steps to improve Europe's information position in cybersecurity

Present CONCORDIA's vision for a cross-sector, pan-European platform for collecting, analyzing, and sharing threat intelligence, which combines datasets built up in different parts of the project.

What is threat intelligence?

Threat intelligence can be defined as the process of acquiring knowledge from multiple sources about threats to an organisation. Threat intelligence supports informed decision-making on cybersecurity by providing information about threat actors, techniques, indicators of compromises, and vulnerabilities. The process is essentially collaborative and based on shared datasets.

CONCORDIA's approach

The two cross-sector pilots in CONCORDIA ("Building a Threat Intelligence for Europe" and "Piloting a DDoS Clearing House for Europe") are developing the basic building blocks for a pan-European and cross-sector threat intelligence platform, which conceptually forms a central point of contact for all services within the CONCORDIA ecosystem that are related to threat intelligence.

We are developing the CONCORDIA threat intelligence platform based on three primary principles:

- **Multi-source:** the platform uses multiple datasets available through heterogeneous technologies and providing different data management services (e.g., two clearing houses and their specific services).
- **Combine datasets:** the platform uses algorithms to integrate datasets into new derived datasets (e.g., coupling reported botnet infections and DDoS attacks, see the scenario below).



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