



DDoS Clearing House for Europe (Task 3.2) T2.1 Workshop on DDoS attacks and 5G networks

Cristian Hesselman (SIDN Labs)



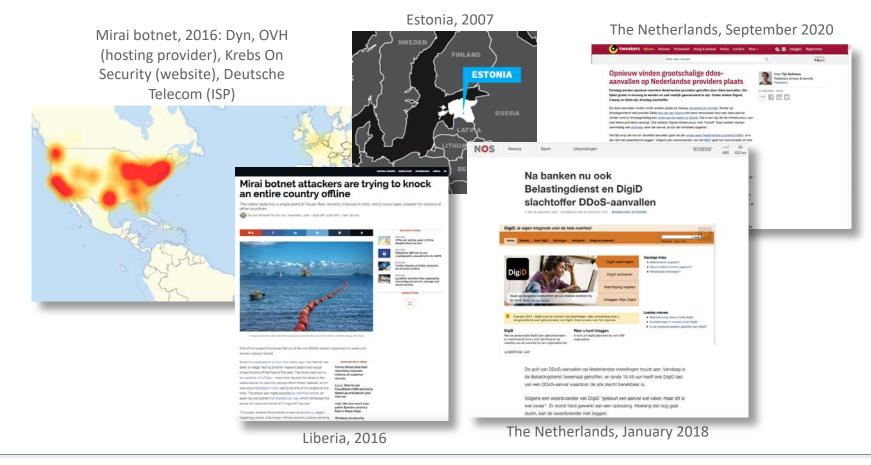
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

CONCORDIA T2.1 Workshop, 25.11.2020





High-impact DDoS Examples



https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

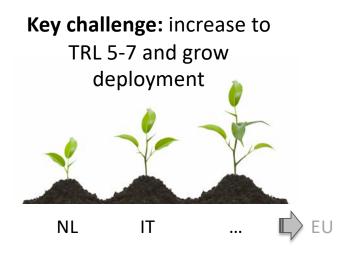
CONCORDIA T2.1 Workshop, 25.11.2020

https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

T3.2 objective

- Pilot a DDoS Clearing House with European industry for Europe to proactively and collaboratively protect European critical infrastructure against DDoS attacks
- Contributes to increased European digital sovereignty thru better insight in and control over DDoS attacks
- Key outputs: pilots in NL >> IT, DDoS clearing house blueprint





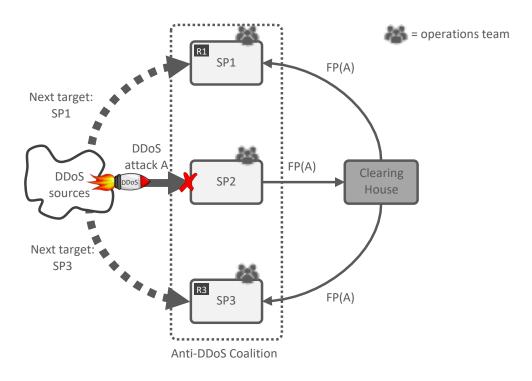


3



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

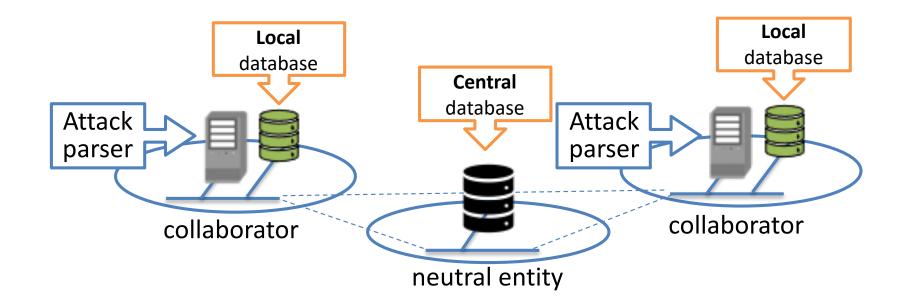
```
{
    "multivector_key": "fa0a8f21a1816a6531acb543743124ec",
    "key": "fa0a8f21a1816a6531acb543743124ec",
    "src_ips": [
        "109.26.226.136",
        ... ],
    "dst_ports": [80],
    "src_ports": [123 ],
    "ip_protocol": "17",
    "service": "NTP",
    "additional": {"ntp_reqcode": 42 },
```

```
"total_src_ips": 1798,
"total_packets": 2387741,
"duration_sec": 120.32017302513123,
"start_time": "2014-12-22 11:12:56",
"avg_bps": 9545941.59169052,
"avg_pps": 19844.893337223457,
"start_timestamp": 1419243176.663222
```





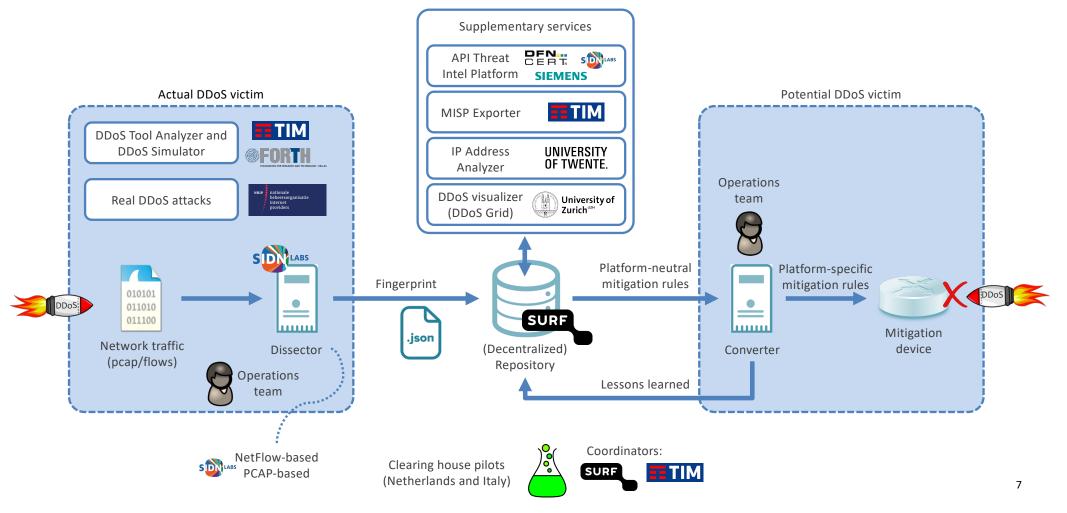
DDoS Clearing House-in-a-box







Main Components and Data Flow







Component Maturity Indication

Name	Function	Maturity	T3.2 experts (<u>owner</u>)
Dissector	Generate DDoS fingerprints based on PCAP files and flows data	High	<u>João</u>
DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High	<u>Remco</u> , João
Converter	Generate mitigation rules based on DDoS fingerprints	Low	João, Marco, Paolo
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High	<u>Bruno</u> , Muriel
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Low	<u>Ramin</u> , Mattijs
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Low	<u>Christos</u>
MISP Exporter	Generate MISP events based on DDoS fingerprints	Low	<u>Madalina</u> , Marco
Synthetic traffic generator	Generation of DDoS fingerprints using a TIM's DDoS traffic simulator	Low	<u>Paolo</u>





Pilot in the Netherlands



Website: nomoreddos.org

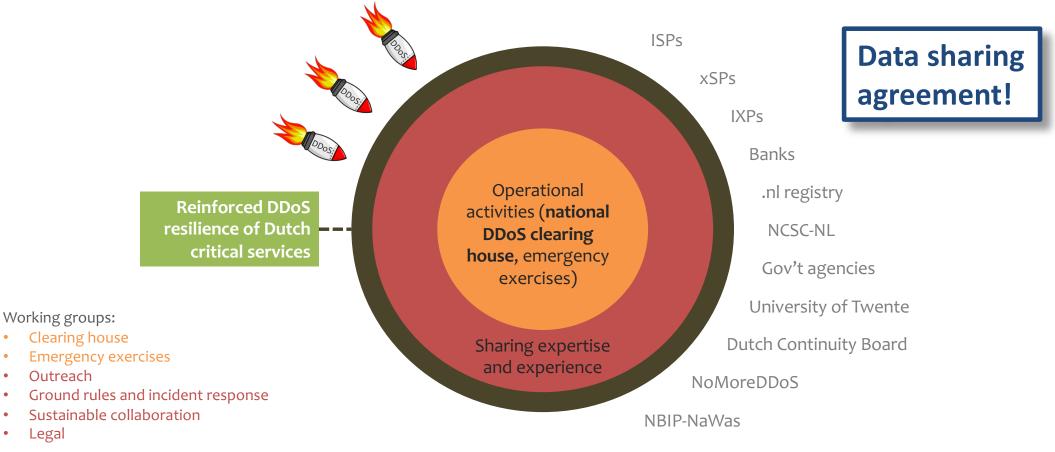
Outreach

Legal



Broader view: Dutch anti-DDoS coalition

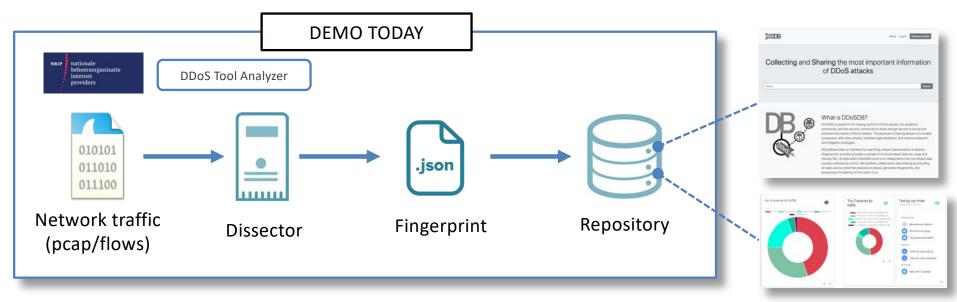
Objective: further improve the protection of Dutch critical services by sharing expertise, experiences, and operational data on DDoS attacks







Today's Demo



- 1. Full cycle process (generation, upload, storage)
- 2. Dashboard for fingerprint visualization
- 3. Fingerprint enrichment
- 4. DDoS Tool Analyzer automatically uploads fingerprints



Cyber security cOmpeteNCe fOr Research anD InnovAtion



Fingerprint generation, storage, enrichment

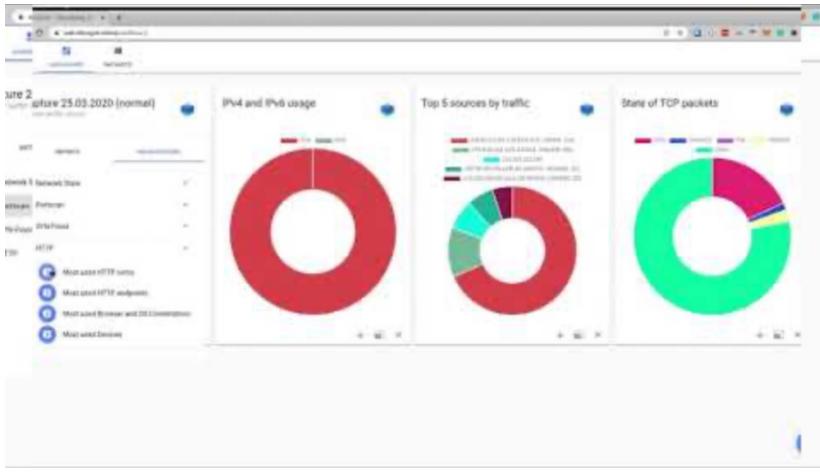
				00000000
	BOREDE			HULLINGER (manufacture from (manufacture)
		Ove	rview of al	Provide a second of advanta (17 11) the par-
+ her	1.000	(1 Statement	The second
	1241-00-04 12 More	21.000	1118	the same
(144-111-141)	Sitisti Attains	0.003	1000	To an
e constante a constante da prima d	2012/06/14 12:12:00	0.556	aw.	L DIE L
			CONC	Provide and a second se
				Band Langence a
				Analysis and the second s

https://www.youtube.com/watch?feature=oembed&v=1QIC3SwwYAU





Fingerprint visualization (not integrated yet)





DDoS Tool Analyzer (not integrated yet)

େ ଜ ଜ							
	DeesDB					Atusta And	·°L.7!!-48
		Over	view of a	all finger	prints (13)		्राणीमा तूथ्य
t kuy-	atory fima	duration parenter)	IP kinvotynd	wits/caremi	packatsionwood		same.
13744 im 8964 (108585) #9577 cms0	105834	0.845	B.572	608.575	10 1-13		ករដូប្រដាំ! ហៅកំពុទ្ធលោកត
ujan indonan indataooon	2020-10-27 12:59:44	S1.2005	159,284	306,4395	3, 160	1	143 Halanan Marin I. Haranan Haranan Maranan II Karalar
Prosenteseterntuth (antroadiloro)	0072 2020-10-20 08:04:20	26,014		and the		-	
		Le de la constante de la consta Le constante de la constante de	In the second se	The Lemma Le March and Francisco Francisco Labor International Con- Participation of the March and American International Control International Control Internatione Control International Control International Control Int	4 04 10 27 19 17 2 10 1 2 3 0 0 12 5 10 1 2 5 10 1 1 10 11 5 10 1 10 11 10	Нана (255,455 н. Гол 47 (41) 10 (4) 10 (4) (4) 10 (4) (4) 45 (4) 45 (4) 10 (4	<pre>Mill</pre>
nernel denne grant - Canada e	enimetranii (Cepaini (~04)						The fig and the second





Demo v2.3 (Dec 31, 2020)

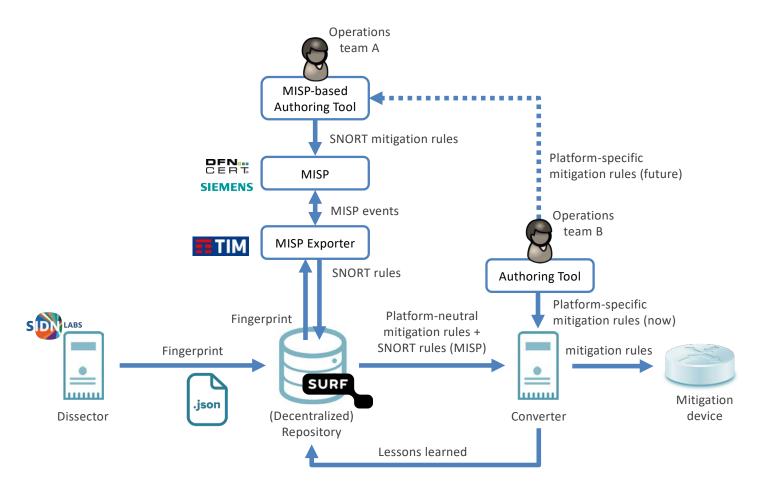
Name	Objective
Dissector	Dissector provides better APIs to other components (P2P communication, interface to supplementary services)
DDoSDB	DDoSDB provides APIs for DDoS Grid and other supplementary services.
Converter	Converter uses a MISP module to convert DDoS fingerprints from DDoSDB into mitigation rules (to be discussed on Oct 9)
DDoS Grid	Grid supports new kinds of fingerprint visualization, interworks with DDoSDB to add/get fingerprints
IP Address Analyzer	Analyzer reads fingerprints from DDoSDB, adds metadata based on measurements (e.g., host's network capacity and connection type), writes back to DDoSDB
DDoS Tool Analyzer	Profiler automatically and continually profiles DDoS tools and automatically uploads fingerprints to DDoS-DB
MISP Exporter	Exporter takes a fingerprint from DDoSDB and injects it into MISP as a MISP event. Detailed scenario description), based on Sep 2020 blog
Synthetic traffic generator	To be provided by mid Nov

CONCORDIA T2.1 Workshop, 25.11.2020



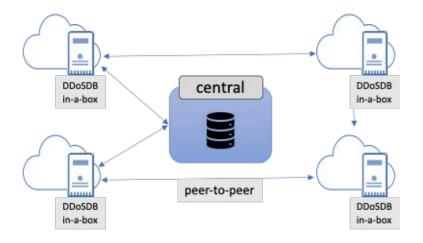


MISP Interaction (work in progress)





- Advance clearing house pilot in NL
- Improve and integrate components
- DDoS clearing house long-term roadmap
- Continue demo-driven approach
- Future challenge: get fingerprints from production systems







Cyber security cOmpeteNCe fOr Research anD InnovAtion



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-DDaS Coglitian is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, agvernment gaencies 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. Pour lessons learned are an d D C O D & nomereddos org/en/blog 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 ([]) link to in-depth technic papers.

DDoS attack landscape

A Distributed Denial-of-Service (DDoS) attack overwhelms a network with traffic, thus den network the ability to service legitimate requests from their clients. The attacker ty simultaneously transmitting traffic from a large number of machines distributed across example by infecting those machines with malware that carries out the attack. Another ty attacking machines exhausts a server's resources (rather than swamping the network) attacker could reneatedly start a locon session with the server thus forcine it to make ma

New version of the DDoS Clearing House core components

Oplosingen Veilig internet Renets SIDN Labs Over S/ON

The next round of improvements to get it deployed

tions + 1058.148 + Nexes.45.854) + New version of the Diol Country House

S D LABS

TW/

0 Cybr

The

CON

sect mos

area

http

800

4

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 a BOX, a System that charges between experiments and the system of the s and Italy

Anti-DDoS Coalition and CONCORDIA

SIDN and SURF are proud to be part of the Dusch Anti-Doo Cosilition as well as of the CONCORDIA public, where we work on mechanism and tools that enable service providers to handle Doos attacks more providently, but properties involve numerous organizations including portements, internet providers, internet exchanges, academic institutions, non-profit organizations and banks.

An important building block in both projects is the DDoS Clearing House, a shared system that As important building block is both projects is the DobG Gauring House, a shared system Mar-enables participating sprice provides to automatically share the characteristics of DOB attacka they handle in the Ioms of us-called 'Dob6 fingerprints'. The trene here is that to be forewared by the be forewared. Statistic Dob6 fingerprints' with other participants warns them that new attacka may be underway and extends the DOBs intigration services that participants already have in place such as scrubbing provices like the XPACC, Comparing attacka currengli in gengers with attacks where details are already accorded in the Clearing House can also provide pointers as to the best women multimation anisms barbon. way to mitigate ongoing attacks.

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







0000



HBER 24, 2020 ADMIN CONCORDIA

Work in Progress: the **ONCORDIA Platform for Threat** Intelligence

ps to improve Europe's information position in cybersecurit

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

hat is threat intelligence?

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

DNCORDIA'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 rted botnet infections and DDoS attacks, see the scenario be



Cyber security cOmpeteNCe fOr Research anD InnovAtion



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

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 www.facebook.com/concordia.eu

in

www.linkedin.com/in/concordia-h2020

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