DDoS Clearing House for Europe (Task 3.2)

3rd CONCORDIA review

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

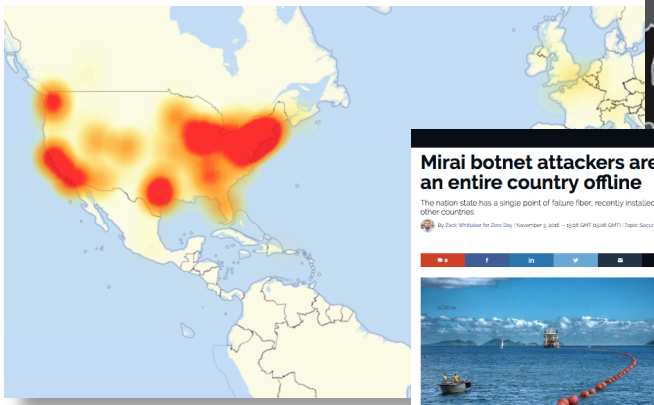
- Key achievements Y2: advanced clearing house prototype's core components and supplementary services (videos)
- Y3 focus: (1) coupling with production systems, (2) further technical improvements, (3) publish first version of cookbook
- Dutch ADC: moving to sustainable ecosystem (funding, CA)
- DDoS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

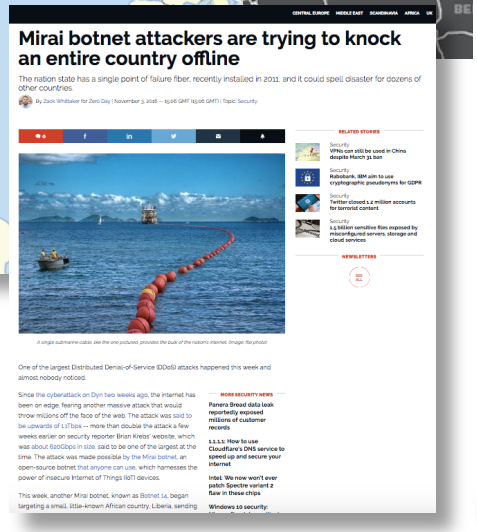
High-impact DDoS Examples

Mirai botnet, 2016: Dyn, OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

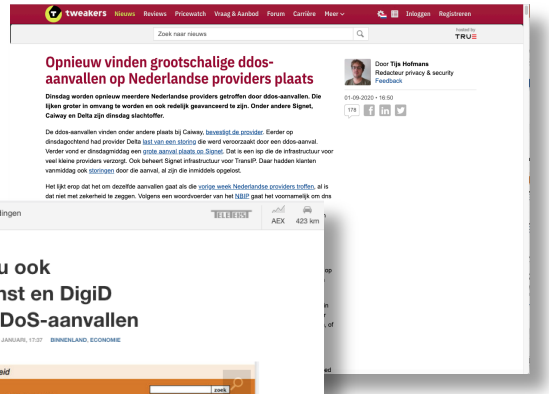


Estonia, 2007

Liberia, 2016



The Netherlands, September 2020



The Netherlands, January 2018

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

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

Tweede Kamer
DER STATEN-GENERAAL

House of Representatives
of The Netherlands,
October 2020

- 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

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!

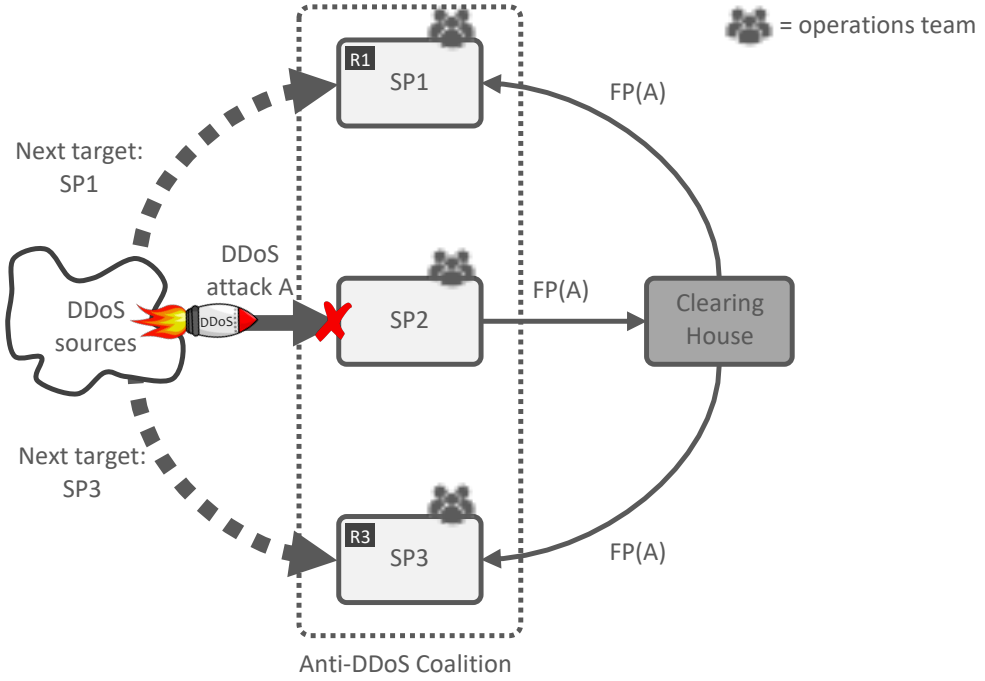
Key challenge: increase to TRL 5-7 and grow deployment

NL IT ... EU

- 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

Dutch National Anti-DDoS Coalition

Betaalvereniging Nederland

SURF

CONCORDIA partner

VNO NCW

SIDN

CONCORDIA partner

NBIP NaWas

UNIVERSITY OF TWENTE.

CONCORDIA partner

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

amsix

DeNederlandscheBank
EUROSYSTEEM

vodafone ziggo

POLITIE

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Belastingdienst

NLIX
The Interconnect Exchange

kpn

DINL
Stichting Digitale Infrastructuur Nederland

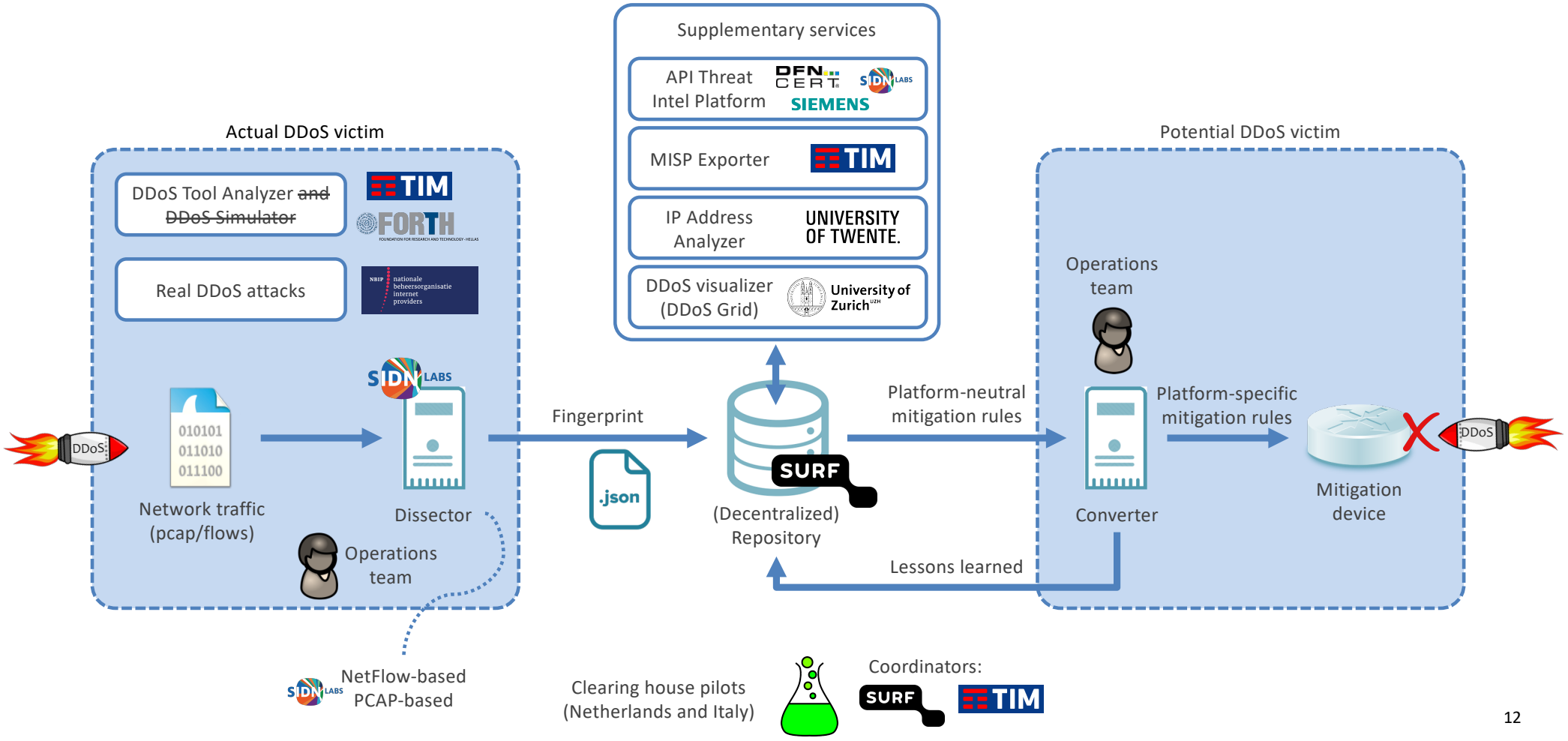
Status Dutch Anti-DDoS Coalition

- 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

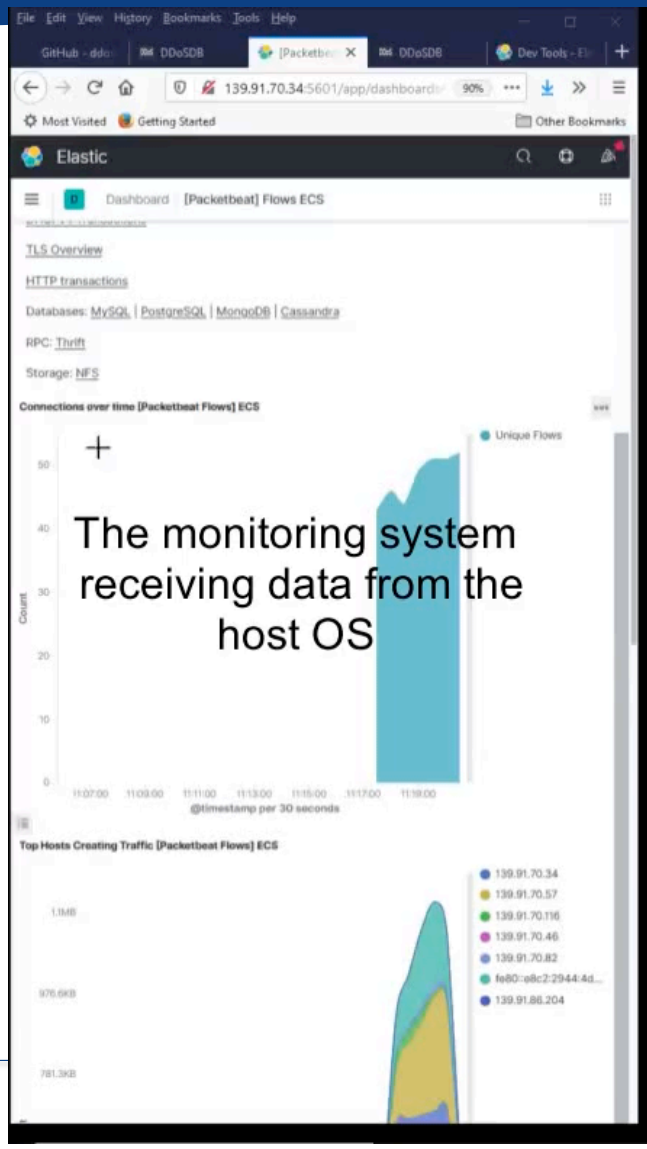
- Core team governing the Dutch ADC

Main Components and Data Flows

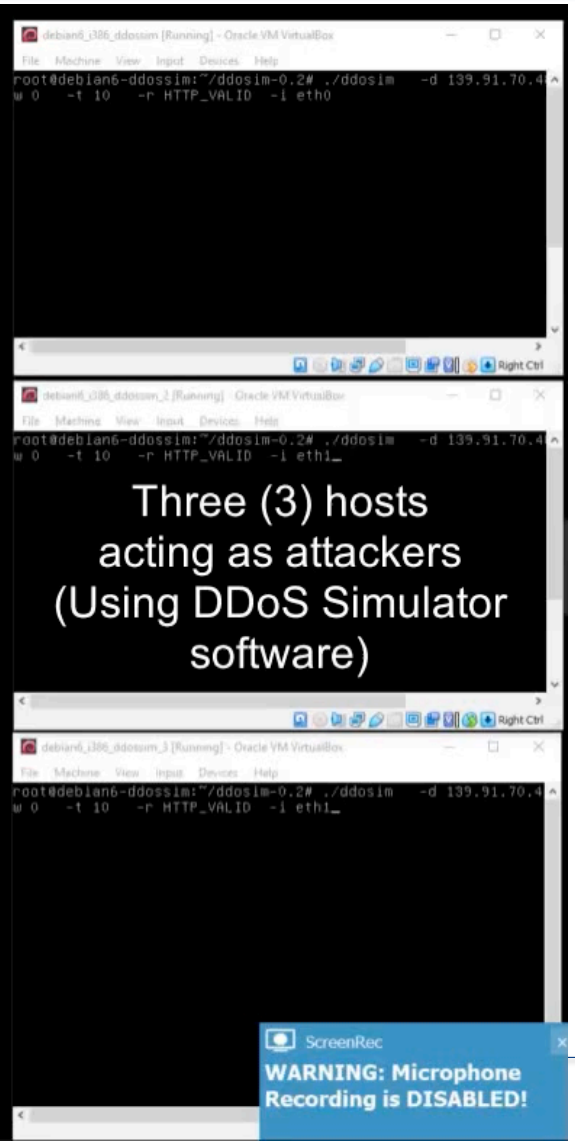


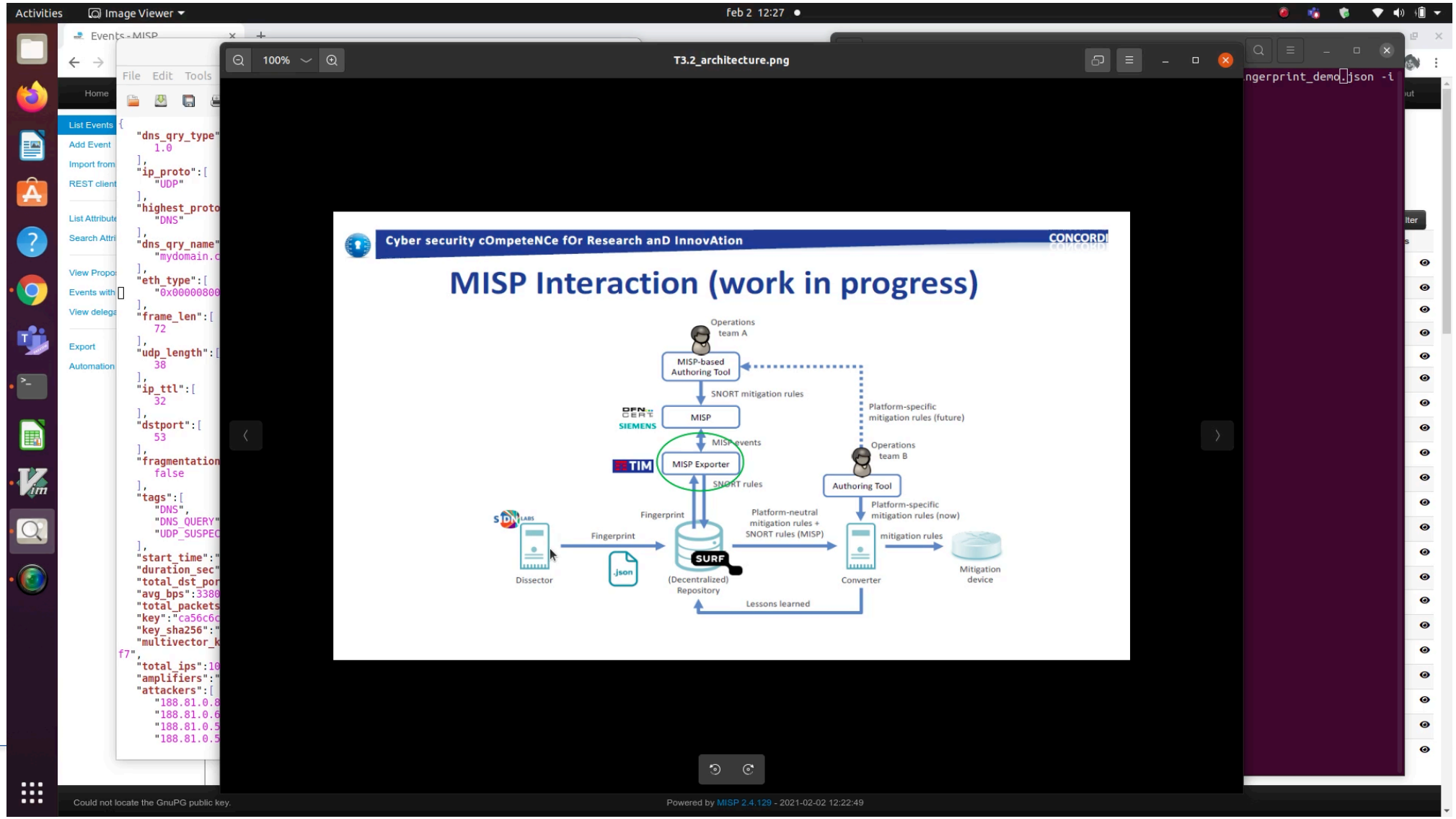
Component Maturity

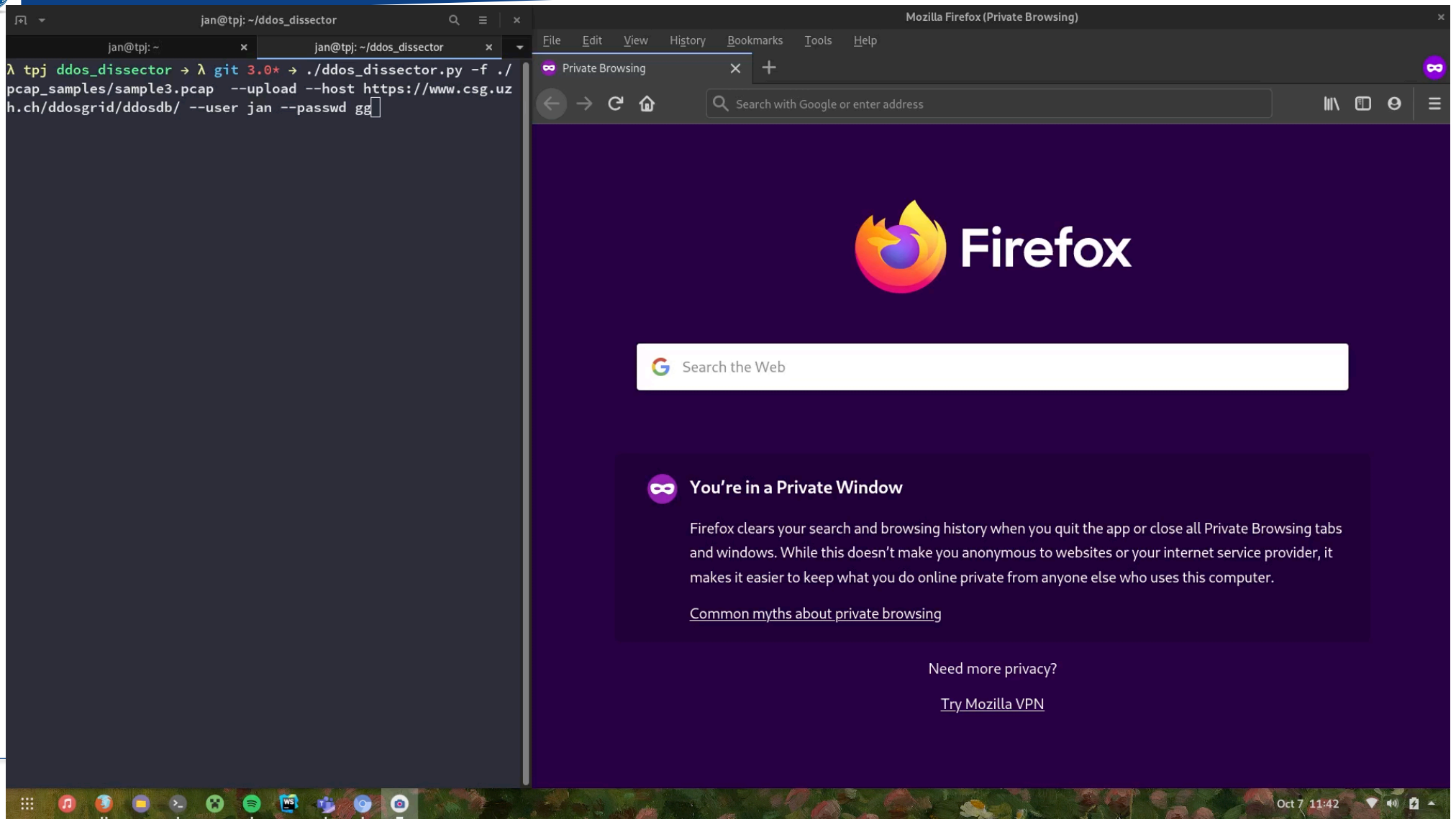
	Name	Function	Maturity
	Dissector	Generate DDoS fingerprints based on PCAP files and flow data	High
	DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High
	Converter	Generate mitigation rules based on DDoS fingerprints	Low
Demo #3	DDoS Grid	Dashboard for the visualization of DDoS fingerprints	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~~

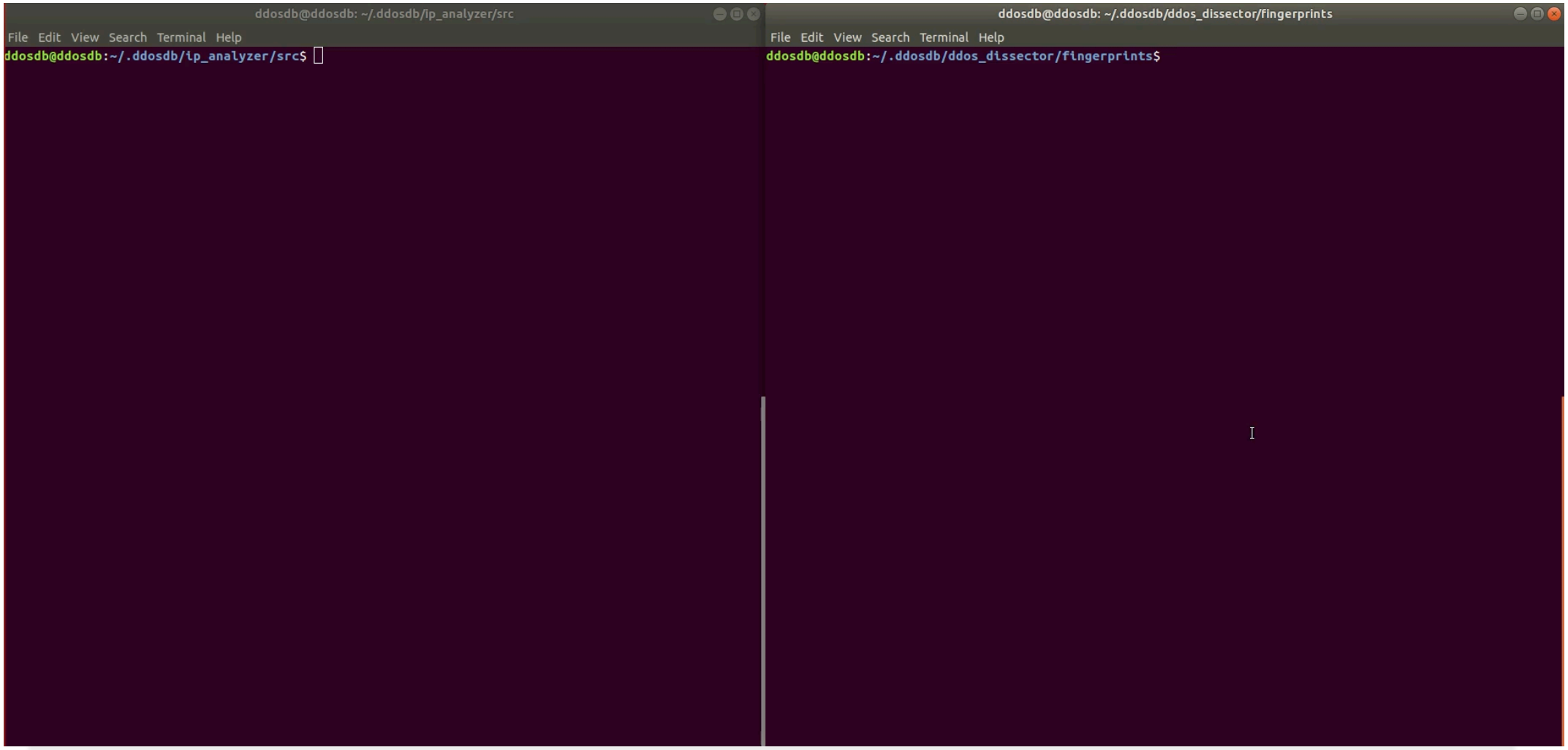

Elastic
Dashboard
[Packetbeat] Flows ECS
TLS Overview
HTTP transactions
Databases: MySQL | PostgreSQL | MongoDB | Cassandra
RPC: Thrift
Storage: NFS
Connections over time [Packetbeat Flows] ECS
Unique Flows
Top Hosts Creating Traffic [Packetbeat Flows] ECS
The monitoring system receiving data from the host OS


The host OS (Proxmox) running:
- the IDS
- the capturing mechanism
- the ddos_dissector


Three (3) hosts acting as attackers (Using DDoS Simulator software)
ScreenRec
WARNING: Microphone Recording is DISABLED!


Activities
Image Viewer
Feb 2 12:27
T3.2_architecture.png
100%
Cyber security cOmpeteNCe fOr Research anD InnovAtion
CONCORDI
MISP Interaction (work in progress)
Operations team A
MISP-based Authoring Tool
SNORT mitigation rules
MISP
MISP events
MISP Exporter
SNORT rules
Platform-specific mitigation rules (future)
Operations team B
Authoring Tool
Platform-specific mitigation rules (now)
Fingerprint
Fingerprint
Platform-neutral mitigation rules + SNORT rules (MISP)
mitigation rules
Dissector
.json
SURF
(Decentralized) Repository
Converter
Mitigation device
Lessons learned
Could not locate the GnuPG public key.
Powered by MISP 2.4.129 - 2021-02-02 12:22:49


jan@tpj: ~/ddos_dissector
jan@tpj: ~
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
Mozilla Firefox (Private Browsing)
File Edit View History Bookmarks Tools Help
Private Browsing
Search with Google or enter address
Firefox
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


ddosdb@ddosdb: ~/.ddosdb/ip_analyzer/src
File Edit View Search Terminal Help
ddosdb@ddosdb:~/.ddosdb/ip_analyzer/src$
ddosdb@ddosdb: ~/.ddosdb/ddos_dissector/fingerprints
File Edit View Search Terminal Help
ddosdb@ddosdb:~/.ddosdb/ddos_dissector/fingerprints$

Advancements of components in Y2

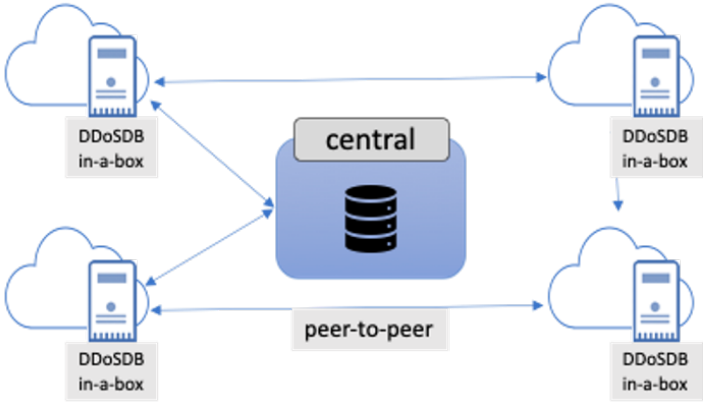
- Dissector: new fingerprint generation algorithms, support for netflow
- DDoSDB: added fingerprint synch between DBs, improved web interface
- Converter: investigating how to incorporate it into MISP

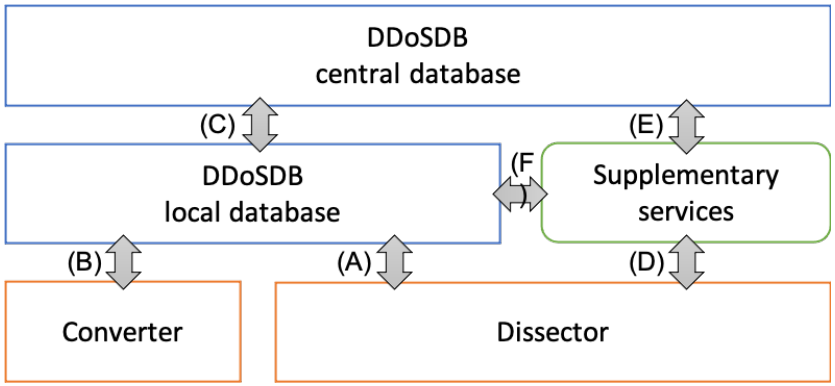
- MISP exporter: first version that maps fingerprints to MISP events
- Tool analyzer: fingerprints nmap, hping3, ddos_sim powered attacks
- DDoS grid: interactive analysis and generation of fingerprints
- IP address analyzer: first basic implementation

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-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/