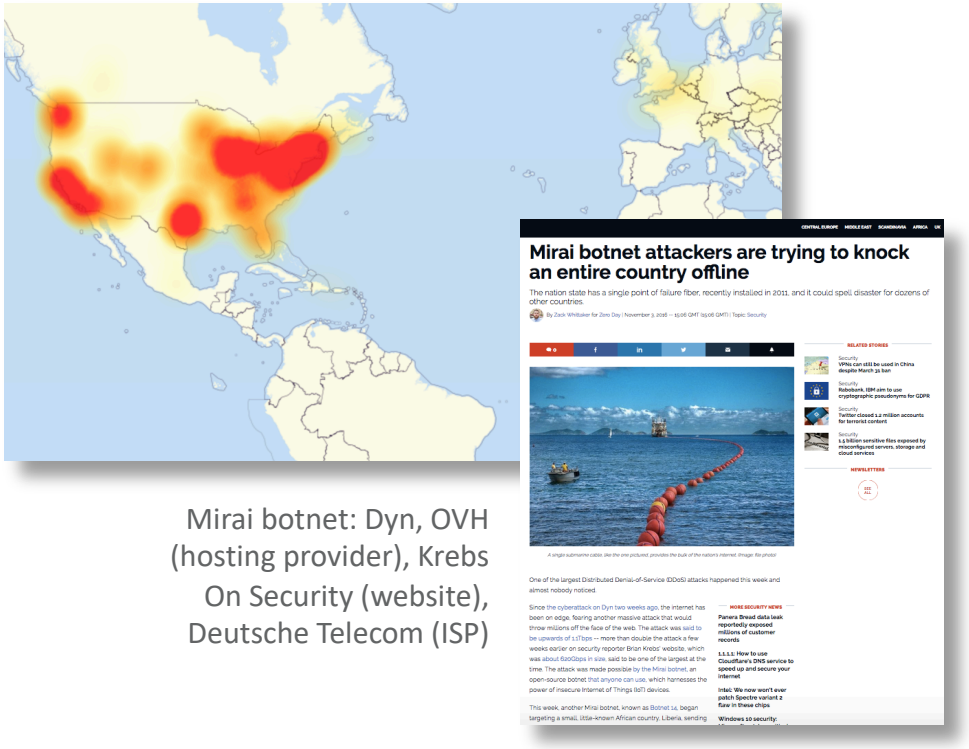
Fighting DDoS attacks together on a national scale

ONE Conference
Wed Oct 2, 2019
The Hague, The Netherlands

Cristian Hesselman (SIDN)
Dr. Jair Santanna (University of Twente)

DDoS examples



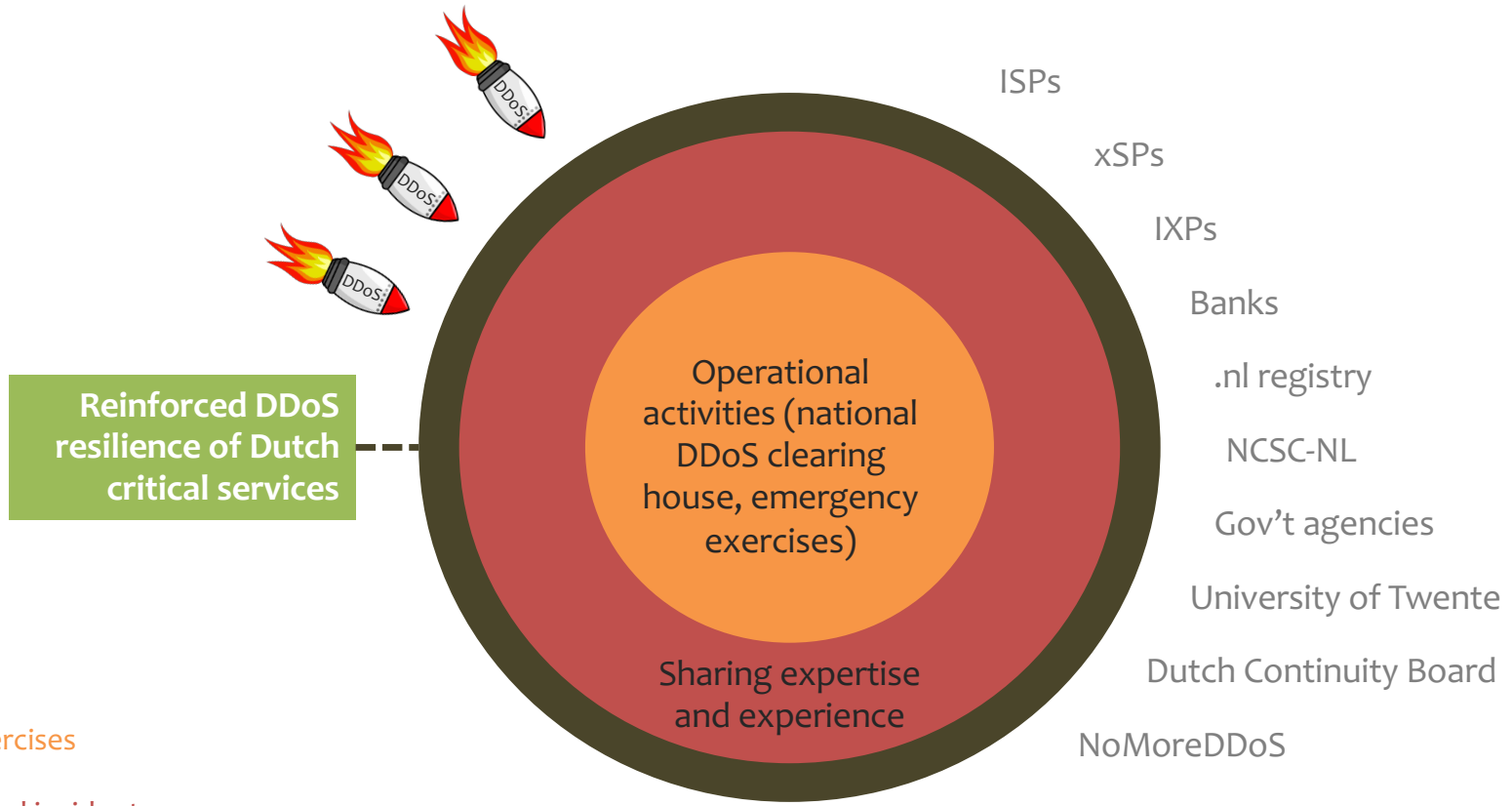
Mirai botnet: Dyn, OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)

January 2018

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

Dutch anti-DDoS coalition

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



Working groups:

- Clearing house
- Emergency exercises
- Outreach
- Ground rules and incident response
- Sustainable collaboration

Status and next steps

- Pilot in the Netherlands (short-term)
  - Approach: start small and iteratively scale up to more partners
  - Key challenge: data sharing agreement clearing house

- DDoS clearing house for Europe
  - Part of CONCORDIA project (www.concordia-h2020.eu)
  - Development of a clearing house "cookbook"
  - Second pilot in Italy

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

- Envisioned long-term growth paths
  - Netherlands → Europe → global
  - Extend to "non-critical" service providers

Technical (and scientific) challenges

Classification
Reduction
Anonymization
Conversion
Distribution

Demo ahead!

Jair Santanna

https://github.com/ddos-clearing-house

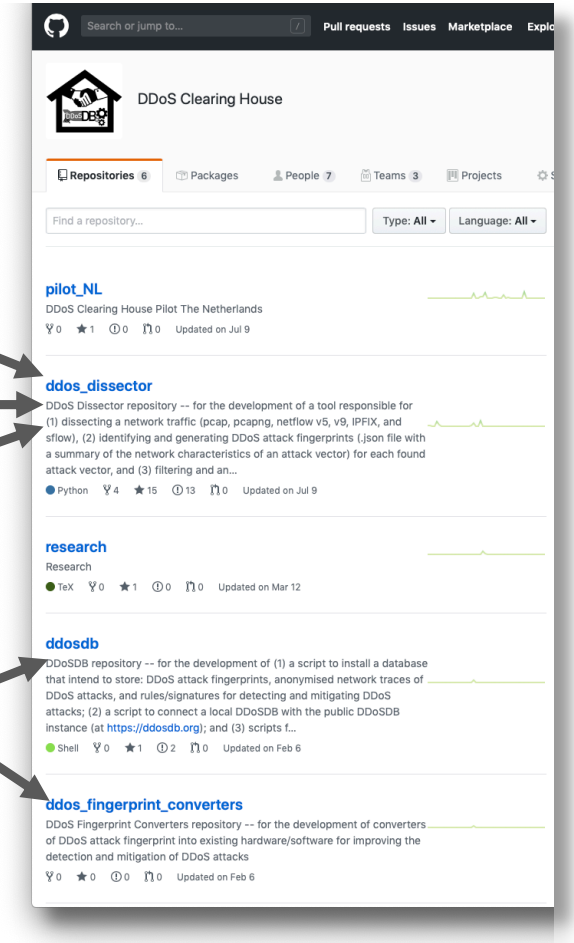
Classification

Reduction

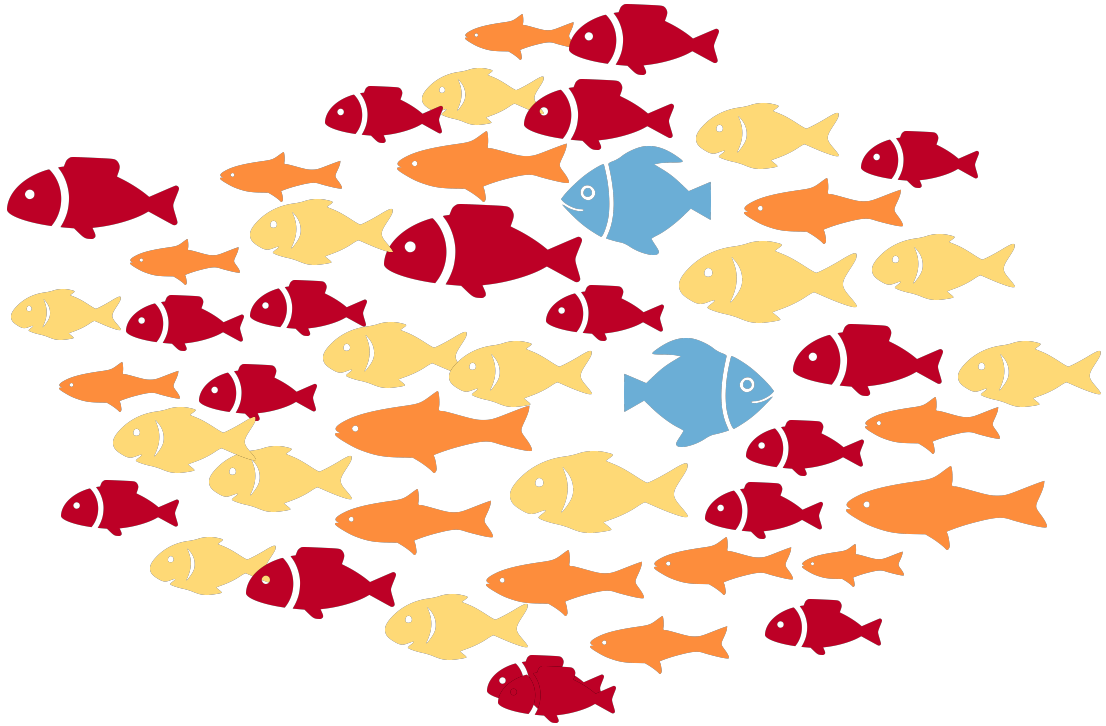
Anonymization

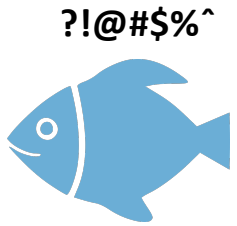
Conversion

Distribution



Definition of DDoS attack

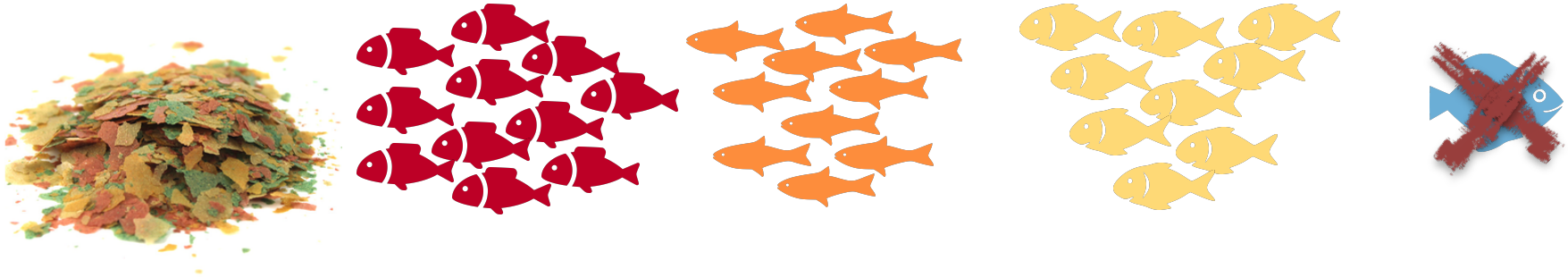




LARGE/ABNORMAL **frequency** of incoming network traffic with **same characteristics** aiming to deny legitimate users to access a computational/network resource.

The Classification Challenge

"The DDoS Dissector"



DDoS Dissector is tool for identifying (multi)vectors of attack
in **post-mortem** network trace
[meant for after an anomaly-based detection tool]

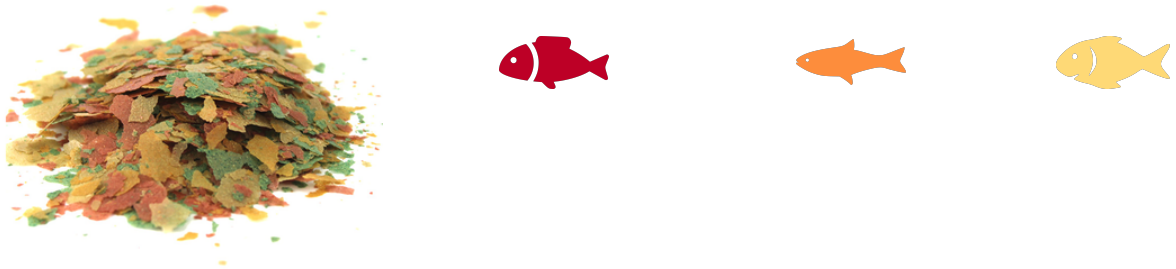
DDoS Dissector is based on a **ranking algorithm**

DDoS Dissector is **NOT** an anomaly-based detection tool!

PROBLEMS?
Encrypted Traffic!
Flash crowd!

The Reduction Challenge

“The DDoS Dissector”



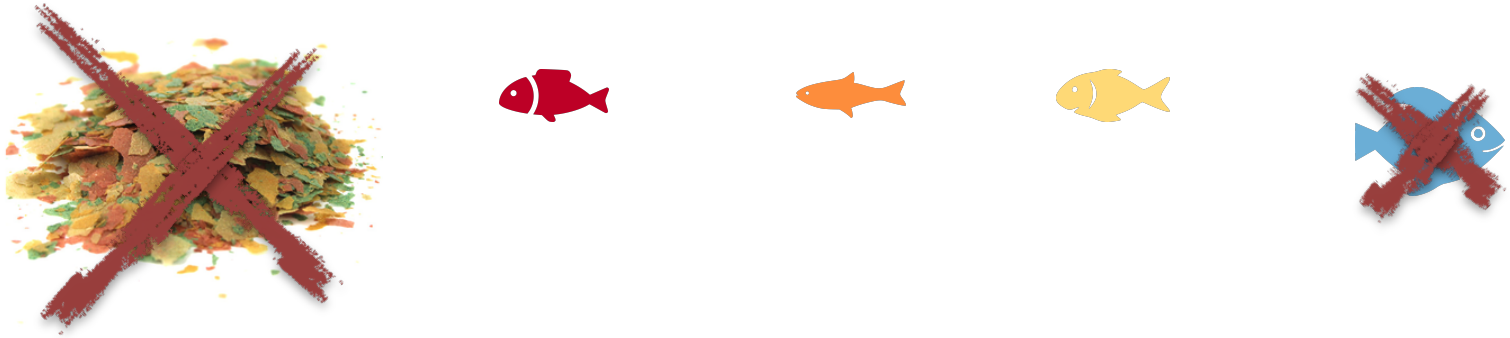
The **main** output of the DDoS Dissector is
a **summary** of the characteristics of a DDoS attack,
called ***DDoS fingerprint***

Each attack vector is **one** DDoS fingerprint (with one **“key"**)

Multiple attack vectors in a network trace are linked (“**multivector_key"**)

The Anonymization Challenge

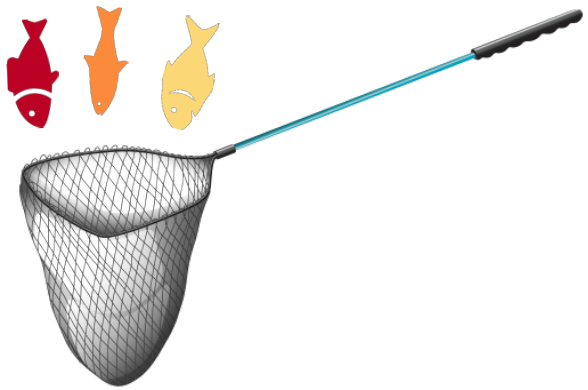
“The DDoS Dissector”



The DDoS Dissector removes **ANY** information related to the **attack target**, remaining ONLY source IP add. information

The Conversion Challenge

“The DDoS Fingerprint Converters”



EMPTY??

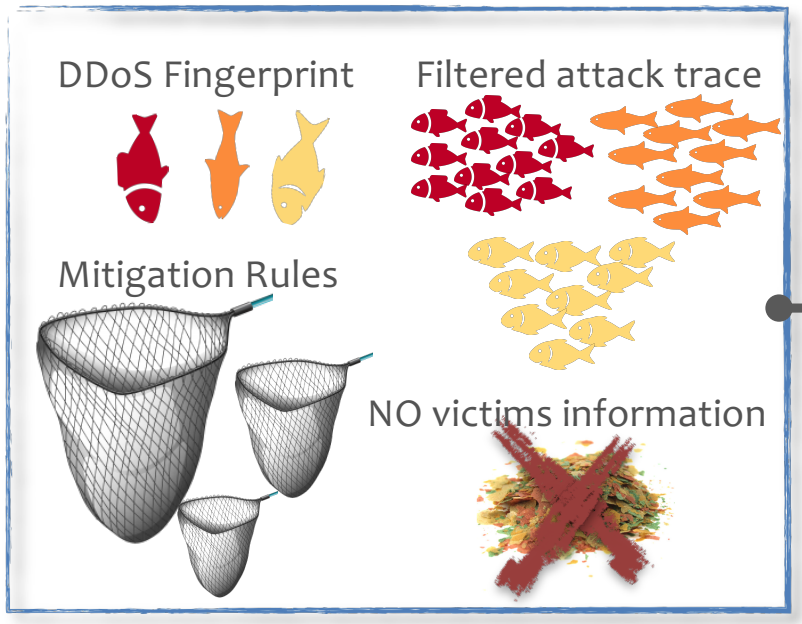
DDoS Fingerprints are converted to detection/mitigation **specific “boxes"**

Candidates: NetFilter/IPTables, SNORT, SURICATA, BRO/ZEEK, MODSECURITY, BGP Flowspec, XDP+eBPF, IETF DDoS Open Threat Signaling (DOTS),
<what else do YOU consider important?>

Check the impact of a mitigation rule (to YOUR network) **BEFORE** deploying it!

The Distribution Challenge

“DDoSDB”



What?
Public? Private?
Open? Closed?
With whom?
Automatic? Manual?

NOSQL database (Elasticsearch) + “FileSystem”

Feed? To CERTs/CSIRTs?

Malware Information Sharing Platform (MISP)?

Common Attack Pattern Enumeration and Classification (CAPEC)?

https://github.com/ddos-clearing-house

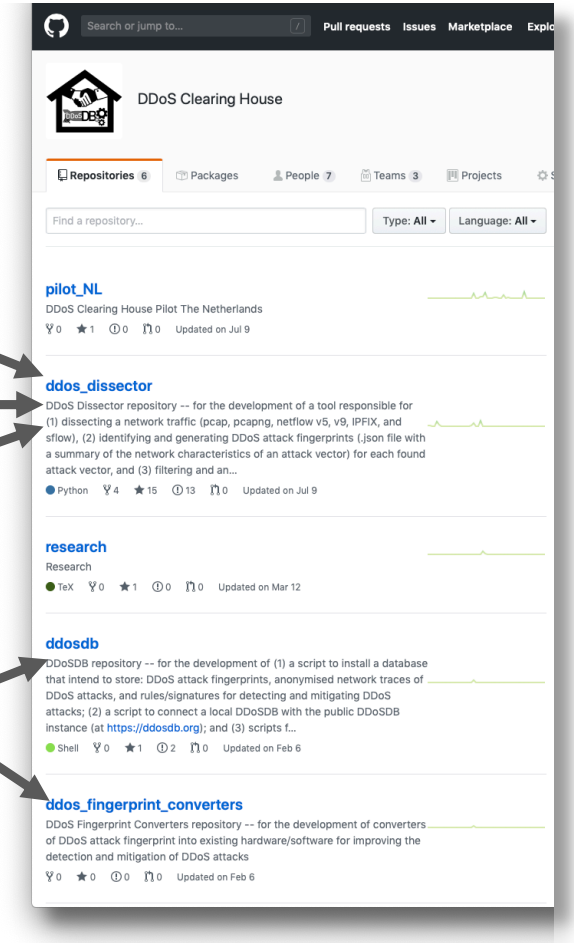
Classification

Reduction

Anonymization

Conversion

Distribution



Panel discussion

Panelists: Marco Doeland (Dutch Payment Association), Oscar Koeroo (KPN), Karl Lovink (Belastingdienst), Benno Overeinder (NLnet Labs, on behalf of NCSC-NL), Octavia de Weerdt (NBIP)

Moderator: Raymond Doijen (NCSC-NL)

Plus NoMoreDDoS and Dutch Continuity Board

SIDN, SURFnet, and the University of Twente were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.