DDoS Clearing House for Europe
Cross-sector Pilot Demo

Cristian Hesselman
(SIDN Labs)

Ramin Yazdani
(UT)

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

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

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: for example, per Member State, per sector, per business unit
T3.2 Objectives

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

• Key outputs: pilots in NL >> IT, DDoS clearing house cookbook

• Build on existing components

Key challenge: increase to TRL 5-7 and grow deployment
Starting Point: Pilot in the Netherlands

Plus NoMoreDDoS and Dutch Continuity Board
Y1 Accomplishments

- Experimental setup (ddosdb.nl) pilot NL
- Draft data sharing agreement for pilot phase 1
- Draft organizational structure
- Draft overall architecture
- System requirements (funded by NBIP, SURF, NCSC-NL)
- Extensive dissemination (e.g., One Conference, Open Door Event)
Y1 Lessons Learned

• Key lesson learned: much more than a technical challenge
• Need for a DDoS clearing house widely acknowledged
• Clearing house needs to be anchored in an “anti-DDoS coalition”
• Value of clearing house community goes beyond sharing fingerprints
• An anti-DDoS coalition needs a legal working group
• Start small, then grow (personal trust is crucial in early stages)
• Keep initial data sharing agreement crisp, simple, and scalable
• Early collaboration with legal experts and ops teams is a must
• CONCORDIA partners play a challenging bridging role
Y2 Plans

• NL pilot: blog on lessons learned, sign data sharing agreement, start sharing in non-production environment, improve software

• Set up an instance of the clearing house at specifically for T3.2 (ddosdb.eu), run experiments, translate the data sharing agreement from Dutch to English

• Further reinforce collaboration within Task 3.2 as well as with other related tasks in CONCORDIA (Tasks 1.1., 1.2, 3.1, 3.3, and 3.5)
Demo: Clearing House Prototype

Step 1: Network traffic (pcap)
Step 2: Attack + Legitimate
Step 3: Filtered & Anonymized Attack Only (pcap)
Step 4: DDoS Fingerprint (json)

Rules:
- BGP FlowSpec
- XDP+eBPF
- WAF
- Snort/Suricata
- Bro
- DOTS

DDoS Dissector
DDoS Fingerprint Parsers
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
Backup Slides
Input: Network Traffic

- Captured traffic (.pcap) includes attack traffic as well as legitimate traffic containing private info about the target network
DDoS Dissector

- *ddos_dissector* library filters, anonymizes and summarizes the input traffic and provides a fingerprint (.json) and anonymized attack only trace (.pcap) as outputs.
DDoS Dissector

- *ddos_dissector* library filters, anonymizes and summarizes the input traffic and provides a fingerprint (.json) and anonymized attack only trace (.pcap) as outputs.
Output: Attack Trace

- Anonymized and filtered attack only trace (.pcap)
Output: DDoS Fingerprint

- Attack fingerprint (.json)
DDoSDB

- Outputs are stored in DDoSDB database for data sharing and proactive mitigation of attacks
Future Work

• Developing DDoS fingerprint parsers to convert fingerprints to rules and share these rules with stakeholders

• These rules can be applied to different mitigation boxes in the network with different levels of specificity to mitigate DDoS attacks