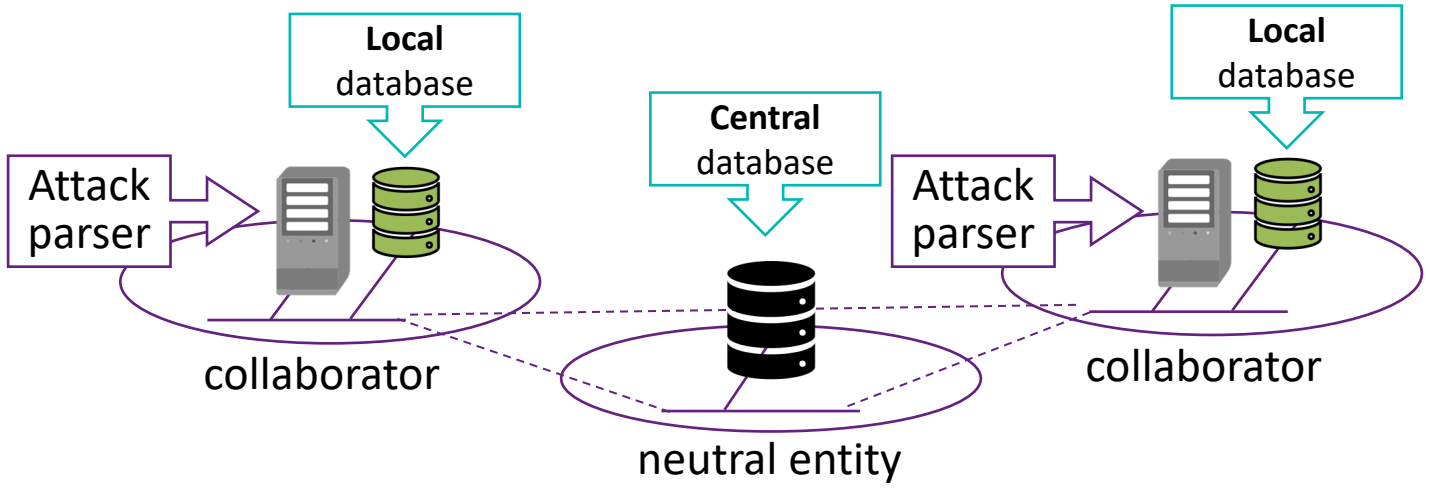
DDoS Clearing House: technical updates

Dr. João M. Ceron -Plenairesessieanti-DDoS coalitie

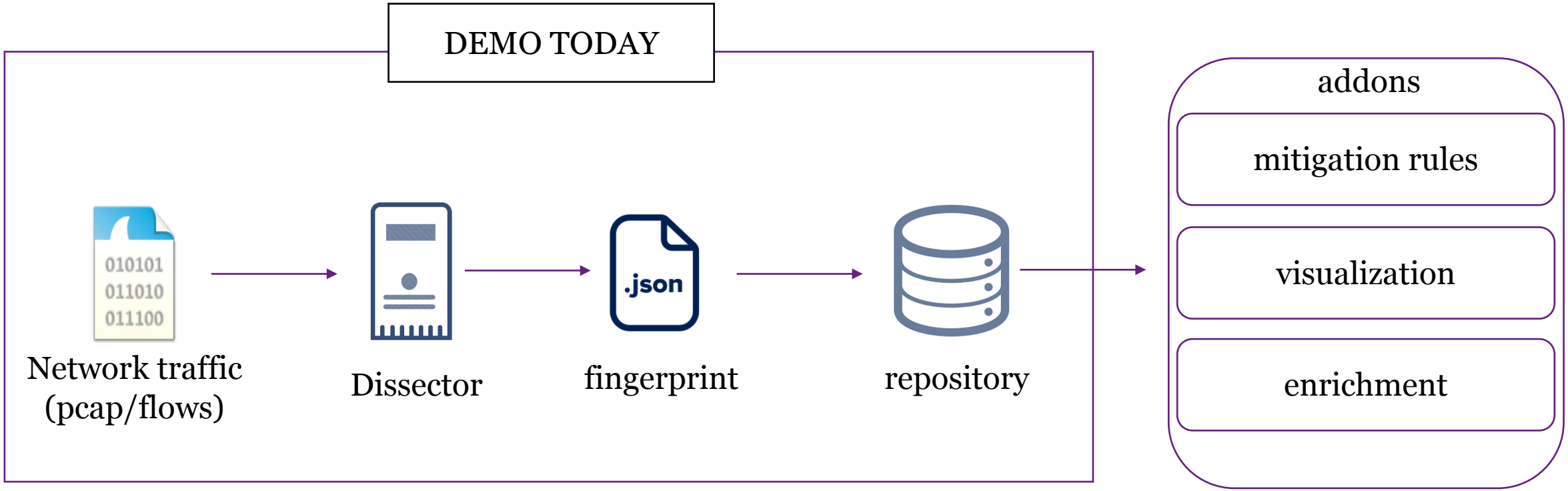
DDoS Clearing House Concept

- Continuous and automatic sharing of “DDoS fingerprints” buys providers time (proactive)

- Extends DDoS protection services that critical service providers use and <u>does not replace them</u>



DDoS Clearing House pipeline



NBIP nationale beheersorganisatie internet providers

1. Full cycle process (generation, upload, storage)
2. Dashboard for fingerprint visualization
3. Fingerprint enrichment

SIDN LABS


Overview of all

Technical progress: DISSECTOR

- Current version
  1. Infer attack targets
  2. Cluster attack characteristics
  3. Fingerprint evaluation
  4. Upload to the central repository
  5. Documentation

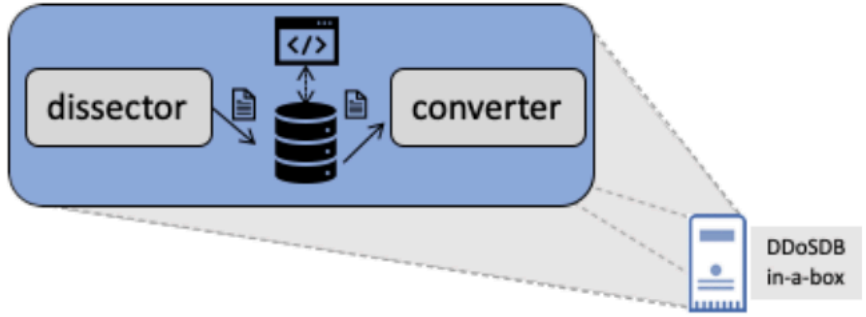

```
<snip>
  "ip_proto": [
    17
  ],
  "highest_protocol": [
    "DNS"
  ],
  "dns_qry_name": [
    "anonsc.com"
  ],
  "eth_type": [
    "0x00000800"
  ],
  "frame_len": [
    397
  ],
  "srcport": [
    53
  ],
  "fragmentation": [
    true
  ],
  "amplifiers": [
    "109.93.47.83",
  ],
  "start_time": "2020-08-08 21:36:23"
}
</snip>
```

How can I test the software?

First steps:

1. Download the Virtual Machine DOWNLOAD
2. Run the Virtual Machine using the software Virtual Box
3. Connect to the IP using your browser: http://IP/
4. Generate fingerprints using `Dissector`
5. List the fingerprints generated on Web Interface

https://github.com/ddos-clearing-house/dddosdb-in-a-box



README.md

DDoS ClearingHouse

python v3.6+ | build passing | dependencies up to date | issues 3 open | contributions welcome | license MIT

Basic Overview

The software is responsible for summarizing the DDoS attack traffic. The key point of this module is to develop a heuristic/algorithm that can find similarities among different types of attacks. Performance and information granularity is a trade-off that should be investigated by considering attacks type. For example, DNS reflection attacks should consider DNS queries fields while TCP SYN flood attack might not require evaluating the TCP packet payload.

- Input [PCAP]
- Output [Fingerprint]

Usage

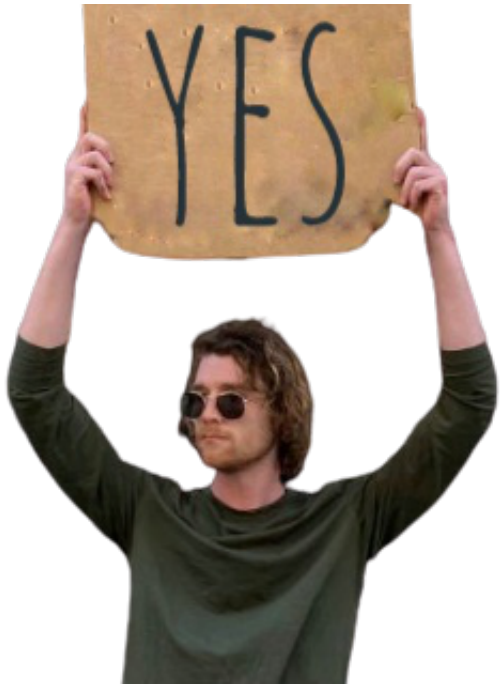
```
usage: new_dissector.py [options]

optional arguments:
  -h, --help            show this help message and exit
  --version             print version and exit
  -v, --verbose         print info msg
```

SDN LABS

FAQ

- Can I use the software without sharing my pcaps?
- Can I share anonymized pcaps?
- Can I help you to code the software?

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



RDoS extortion campaign

TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

28 AUG 2020

Alert Number

MU-000132-DD

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately.**

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA and US Treasury.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Criminals Claiming to be Fancy Bear Conduct Ransom Denial of Service Attacks Against Financial Institutions, Other Industries Worldwide

Summary

SDN LABS

RDoS extortion campaign

```
# Based on FBI Flash Report MU-000132-DD
df_length = (df.groupby(['srcport'])['udp_length'].max()).reset_index()
if (len(df_length.udp_length>468)):
    label.append("UDP_SUSPECT_LENGTH")

my_dict = {
    1121: 'Memcached',
    1194: 'OpenVPN',-
    123:  'NTP',
    1434: 'SQL server',
    1718: 'H323',
    1900: 'SSDP',-
    20800: 'Game Server',
    25:   'SMTP',
    27015: 'Game Server',
    30718: 'IoT Lantronix',
    3074: 'Game Server',
    3283: 'Apple Remote Desktop',
    33848: 'Jenkins Server',
    3702: 'WSD - Web Services Discovery',-
    37810: 'DVR DHCPDiscover',
    47808: 'BACnet',-
    5683: 'CoAP',
```

Summary

- New software dissector: new clusterization method and functions to evaluate fingerprint matching rate
- Improvements on the repository (DDoSDB). Remco did a great job and now we have a summarization page and other visualization enhancements
- We are tagging some attacks (amplification, fragmentation, etc)
- New DDosDB-in-a-box with auto-update function (for software components)
- We are writing a blog post to publicize our last achievements
- Everything is already on our public repository (Github)

SIDN LABS

SIDN and SURF were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/