D4 Project

Open and collaborative network monitoring

Team CIRCL
https://www.d4-project.org/

2019/05/21

Jean-Louis Huynen

Problem statement

- CSIRTs (or private organisations) build their **own honeypot, honeynet or blackhole monitoring network**
- Designing, managing and operating such infrastructure is a tedious and resource intensive task
- **Automatic sharing** between monitoring networks from different organisations is missing
- Sensors and processing are often seen as blackbox or difficult to audit

Objective

- Based on our experience with MISP[1] where sharing played an important role, we transpose the model in D4 project
- Keeping the protocol and code base **simple and minimal**
- Allowing every organisation to **control and audit their own sensor network**
- Extending D4 or **encapsulating legacy monitoring protocols** must be as simple as possible
- Ensuring that the sensor server has **no control on the sensor** (unidirectional streaming)
- Don't force users to use dedicated sensors and allow **flexibility of sensor support** (software, hardware, virtual)

[1] https://github.com/MISP/MISP

(short) History

- D4 Project (co-funded under INEA CEF EU program) started - 1st November 2018
- D4 encapsulation protocol version 1 published - 1st December 2018
- v0.1 release of the D4 core[2] including a server and simple D4 C client - 21st January 2019
- First version of a golang D4 client[3] running on ARM, MIPS, PPC and x86 - 14th February 2019

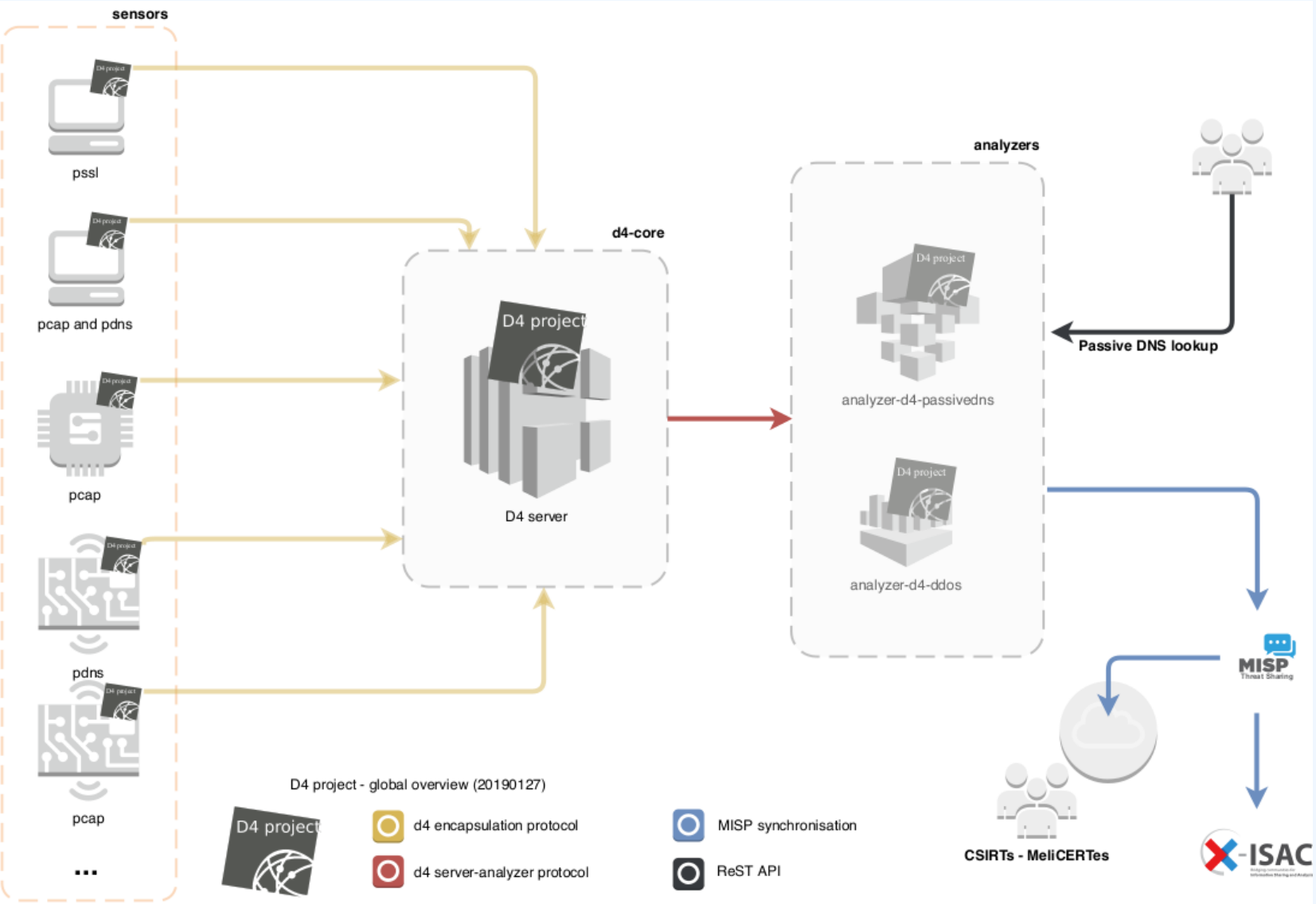
[2] https://www.github.com/D4-project/d4-core
[3] https://www.github.com/D4-project/d4-goclient/

(short) History

Release	Date
analyzer-d4-passivedns-v0.1	Apr. 5, 2019
analyzer-d4-passivessl-0.1	Apr. 25, 2019
analyzer-d4-pibs-v0.1	Apr. 8, 2019
BGP-Ranking-1.0	Apr. 25, 2019
d4-core-v0.1	Jan. 25, 2019
d4-core-v0.2	Feb. 14, 2019
d4-core-v0.3	Apr. 8, 2019
d4-goclient-v0.1	Feb. 14, 2019
d4-goclient-v0.2	Apr. 8, 2019
d4-server-packer-0.1	Apr. 25, 2019
IPASN-History-1.0	Apr. 25, 2019
sensor-d4-tls-fingerprinting-0.1	Apr. 25, 2019

see `https://github.com/D4-Project`

D4 Overview

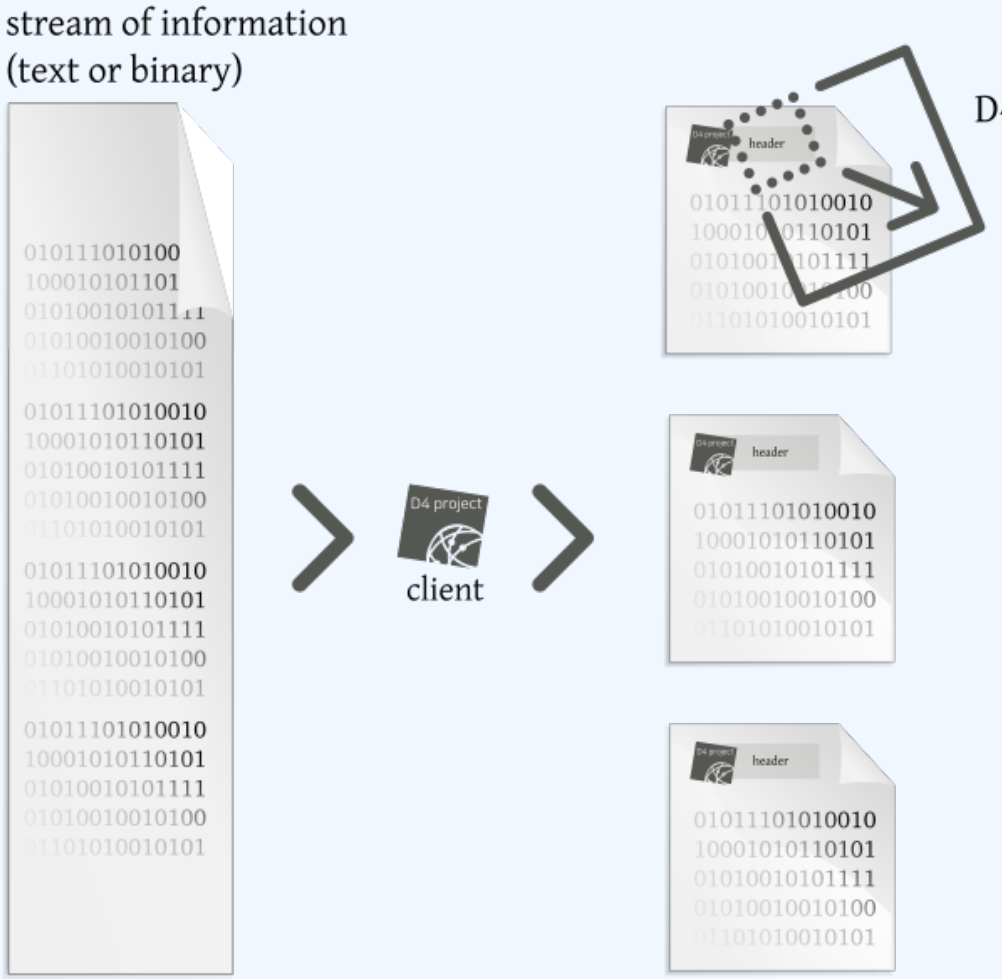

sensors
pssl
pcap and pdns
pcap
pdns
pcap
...
d4-core
D4 project
D4 server
analyzers
D4 project
analyzer-d4-passivedns
D4 project
analyzer-d4-ddos
Passive DNS lookup
MISP
Threat Sharing
CSIRTs - MeliCERTes
X-ISAC
D4 project - global overview (20190127)
D4 project
d4 encapsulation protocol
d4 server-analyzer protocol
MISP synchronisation
ReST API

Roadmap - output

CIRCL will host a server instance for organisations willing to contribute to a public dataset without running their own D4 server:

- ✓ Passive SSL
- ✓ Passive DNS
- ✓ Blackhole DDoS
- BGP mapping
- egress filtering mapping
- Radio monitoring
- ...

D4 encapsulation protocol



D4 encapsulation protocol version 1

D4 project

header

version (8) - Version of the header
type (8) - Data encapsulated type
uuid (128) - Sensor UUID
timestamp (64) - Encapsulation time
hmac (256) - Header authentication (HMAC-SHA256-128)
size (32) - Payload size

D4 project https://www.d4-project.org

D4 Header

Name	bit size	Description
version	uint 8	Version of the header
type	uint 8	Data encapsulated type
uuid	uint 128	Sensor UUID
timestamp	uint 64	Encapsulation time
hmac	uint 256	Authentication header (HMAC-SHA-256-128)
size	uint 32	Payload size

D4 Header

Type	Description
0	Reserved
1	pcap (libpcap 2.4)
2	meta header (JSON)
3	generic log line
4	dnscap output
5	pcapng (diagnostic)
6	generic NDJSON or JSON Lines
7	generic YAF (Yet Another Flowmeter)
8	passivedns CSV stream
254	type defined by meta header (type 2)

D4 meta header

D4 header includes an easy way to **extend the protocol** (via type 2) without altering the format. Within a D4 session, the initial D4 packet(s) type 2 defines the custom headers and then the following packets with type 254 is the custom data encapsulated.

```
{
  "type": "ja3-jl",
  "encoding": "utf-8",
  "tags": [
    "tlp:white"
  ],
  "misp:org": "5b642239-4db4-4580-adf4-4ebd950d210f"
}
```

D4 server

- D4 core server[4] is a complete server to handle clients (sensors) including the decapsulation of the D4 protocol, control of sensor registrations, management of decoding protocols and dispatching to adequate decoders/analysers.
- D4 server is written in Python 3.6 and runs on standard GNU/Linux distribution.

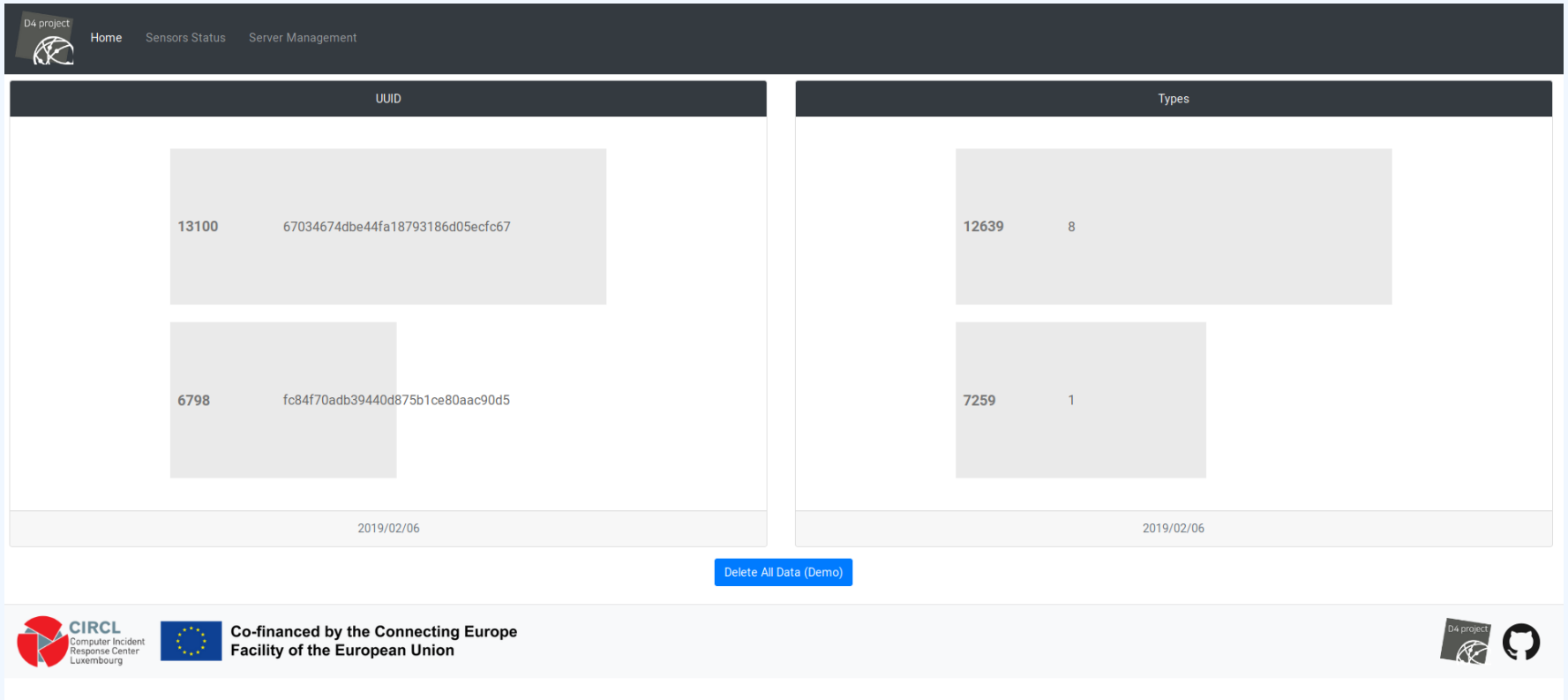
[4] https://github.com/D4-project/d4-core

D4 server - management interface

The D4 server provides a web interface to manage D4 sensors, sessions and analyzer.

- Get Sensors status, errors and statistics
- Get all connected sensors
- Manage Sensors (stream size limit, secret key, ...)
- Manage Accepted types
- UUID/IP blocklist
- Create Analyzer Queues

D4 SERVER - MAIN INTERFACE



D4 SERVER - SERVER MANAGEMENT

D4 project

Home Sensors Status Server Management

Blacklist IP

Blacklist IP
IP Address
Blacklist IP

Manage IP Blacklist
Show Blacklisted IP

Unblacklist IP
IP Address
Unblacklist IP

Blacklist UUID

Blacklist UUID
UUID
Blacklist UUID

Manage UUID Blacklist
Show Blacklisted UUID

Unblacklist UUID
UUID
Unblacklist UUID

Header Accepted Types

Show 10 entries Search:

Type	Description	Remove Type
1	pcap (libpcap 2.4)	Remove Type
2	meta header (JSON)	Remove Type
4	dnscap output	Remove Type
8	passivedns CSV stream	Remove Type
254	type defined by meta header (type2)	Remove Type

Showing 1 to 5 of 5 entries Previous 1 Next

Show 10 entries Search:

Add New Types
1
Add New Type

D4 SERVER - SERVER MANAGEMENT

Show 10 entries

Search:

Type Name	Description	Remove Type
ja3-jl		Remove Extended Type

Showing 1 to 1 of 1 entries

Previous 1 Next

Analyzer Management

Show 10 entries

Search:

Type	uuid	last updated	Change max size limit	Analyzer Queue
1	404d4594-7881-4643-85bf-b11f7d9436e8	1553608013.429933	10000 Change Max Size	3
4	ccb9548c380f4dd19ad3b1e94412e79a	Never	10000 Change Max Size	0

Showing 1 to 2 of 2 entries

Previous 1 Next

Add New Analyzer Queue

1

Analyzer uuid

Add New Analyzer

Show 10 entries

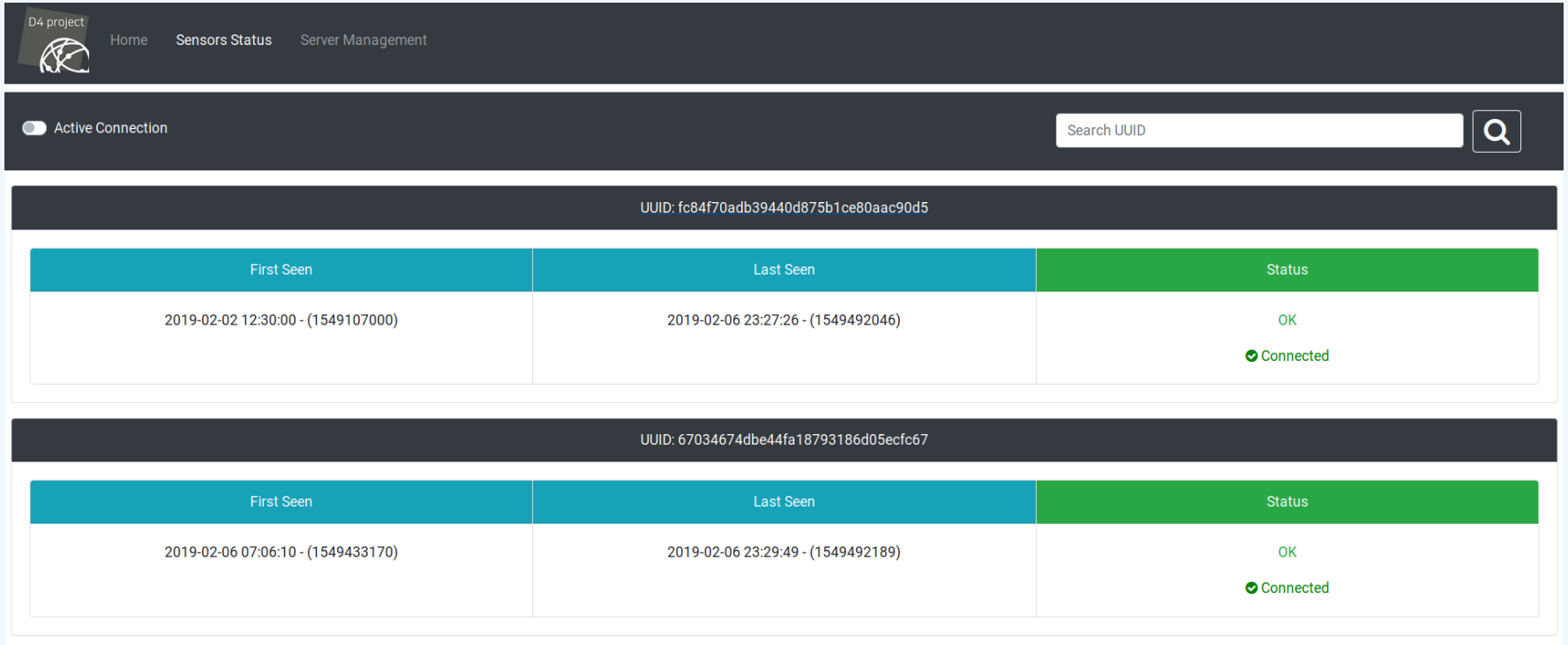
Search:

Type Name	uuid	last updated	Change max size limit	Analyzer Queue
ja3-jl	ccb9548c380f4dd19ad3b1e94412e79a	Never	10000 Change Max Size	0

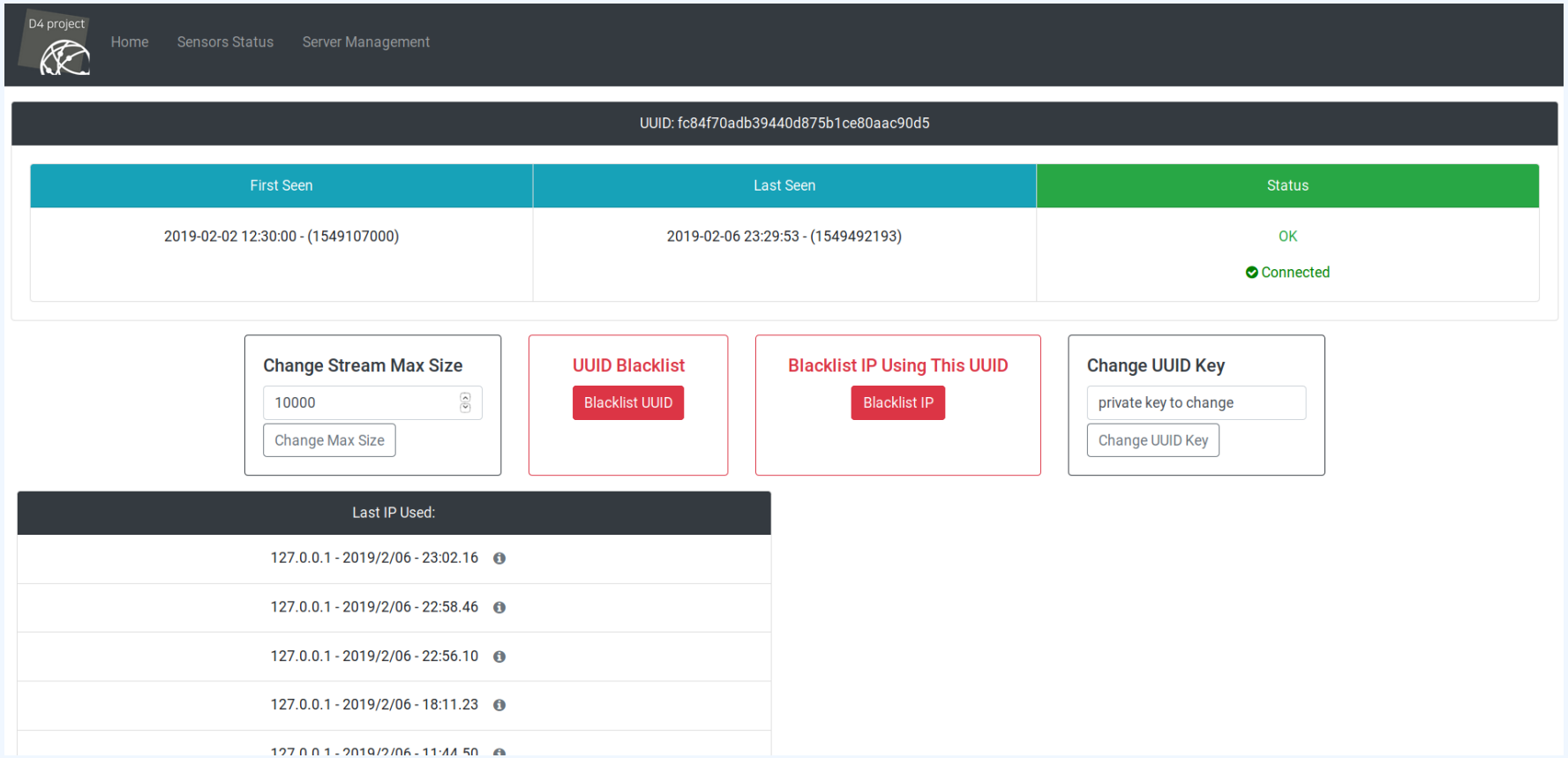
Showing 1 to 1 of 1 entries

Previous 1 Next

D4 SERVER - SENSOR OVERVIEW

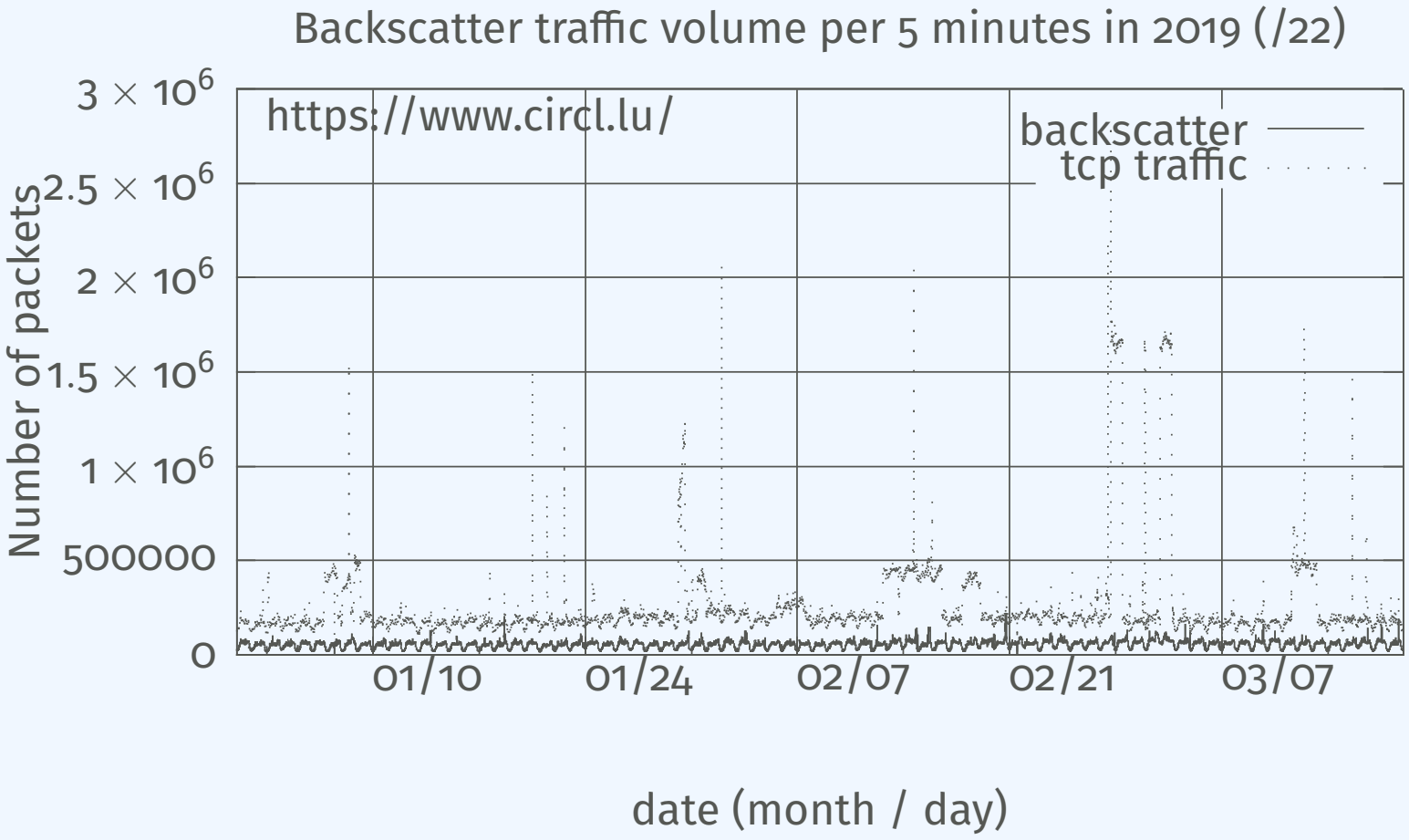


D4 SERVER - SENSOR MANAGEMENT



A distributed Network telescope to observe DDoS attacks

DDoS Attacks produce an observable side-effect:



What can be derived from backscatter traffic?

- External point of view on ongoing denial of service attacks
- Confirm if there is a DDOS attack
- Recover time line of attacked targets
- Confirm which services (DNS, webserver, . . .)
- Infrastructure changes
- Assess the state of an infrastructure under denial of service attack
  - Detect failure/addition of intermediate network equipments, firewalls, proxy servers etc
  - Detect DDoS mitigation devices
- Create probabilistic models of denial of service attacks

D4 in this setting

Aggregating backscatter traffic collected from D4 sensors:

- have various points of observation (non contiguous address space)
- perform analysis on bigger amount of data

D4 lookup should provide:

- backscatter analysis results,
- daily updates,
- additional relevant information (DNS, BGP, etc.).

Passive DNS

Problem statement

- CIRCL (and other CSIRTs) have their own passive DNS[5] collection mechanisms
- Current **collection models** are affected with DoH[6] and centralised DNS services
- DNS answers collection is a tedious process
- **Sharing Passive DNS stream** between organisation is challenging due to privacy

[5] https://www.circl.lu/services/passive-dns/
[6] DNS over HTTPS

Potential Strategy

- Improve **Passive DNS collection diversity** by being closer to the source and limit impact of DoH (e.g. at the OS resolver level)
- Increasing diversity and **mixing models** before sharing/storing Passive DNS records
- Simplify process and tools to install for **Passive DNS collection by relying on D4 sensors** instead of custom mechanisms
- Provide a distributed infrastructure for mixing streams and filtering out the sharing to the validated partners

First release

- analyzer-d4-passivedns[7] is an analyzer for a D4 network sensor. The analyser can process data produced by D4 sensors (in passivedns CSV format[8])
- Ingest these into a **Passive DNS server** which can be queried later to search for the Passive DNS records
- The lookup server (using on redis-compatible backend) is a Passive DNS REST server compliant to the Common Output Format[9]

[7] https://github.com/D4-project/analyzer-d4-passivedns
[8] https://github.com/gamelinux/passivedns
[9] https://tools.ietf.org/html/draft-dulaunoy-dnsop-passive-dns-cof-04

Passive SSL revamping

A passive SSL fingerprinter

CSIRT's rationale for collecting TLS handshakes:

- pivot on additional data points,
- find owners of IP addresses,
- detect usage of CIDR blocks,
- detect vulnerable systems,
- detect compromised services,
- detect Key material reuse,
- detect weak keys.

Objectives

History of links between:

- x509 certificates,
- ports,
- IP address,
- client (ja3),
- server (ja3s),

> *"JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence."*[10]

[10] https://github.com/salesforce/ja3

Objectives

Mind your Ps and Qs:

- Public keys type and size,
- modulos and exponents,
- curves parameters.

First release

- ✓ sensor-d4-tls-fingerprinting [11]: Extracts and fingerprints certificate
- ✓ analyzer-d4-passivessl [12]: Stores Certificates / PK details in a PostgreSQL DB
- lookup-d4-passivessl [13]: Exposes the DB through a public REST API

[11] github.com/D4-project/sensor-d4-tls-fingerprinting
[12] github.com/D4-project/analyzer-d4-passivessl
[13] github.com/D4-project/lookup-d4-passivessl

Future

- **Mixing models for passive collection stream** (for privacy) in next version of D4 core server
- Interconnecting private D4 sensor networks with other D4 sensor networks (sharing to partners filtered stream)
- Previewing dataset collected in D4 sensor network and providing **open data stream** (if contributor agrees to share under specific conditions)

Get in touch if you want to join the project, host a sensor or contribute

- Collaboration can include research partnership, sharing of collected streams or improving the software.
- Contact: info@circl.lu
- `https://github.com/D4-Project` - `https://twitter.com/d4_project`