

D4 Project

Open and collaborative network monitoring

Team CIRCL

<https://www.d4-project.org/>

20190307



Aurélien Thirion, Jean-Louis Huynen

- 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

- Based on our experience with MISP¹ 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)

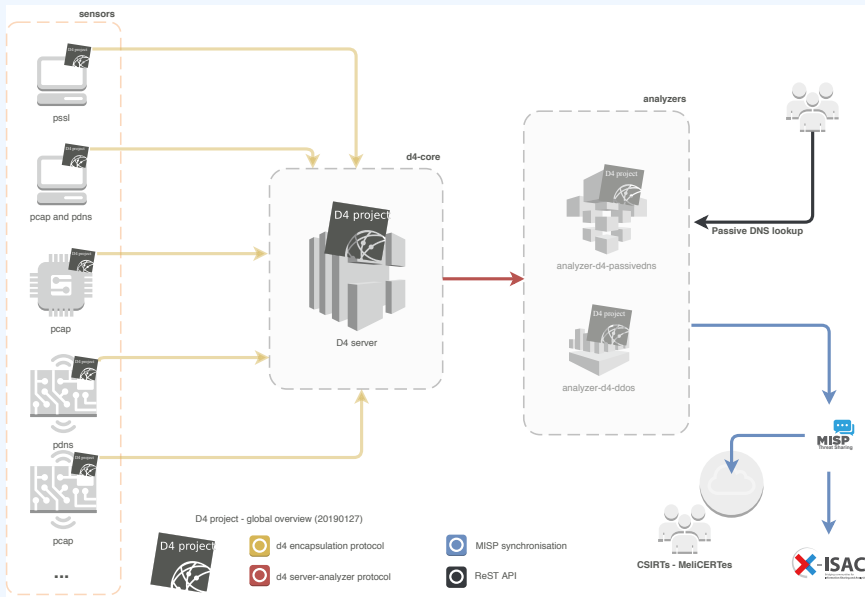
¹<https://github.com/MISP/MISP>

- D4 Project (co-funded under INEA CEF EU program) started - 1st November 2018
- D4 encapsulation protocol version 1 published - 1st December 2018
- vo.1 release of the D4 core² including a server and simple D4 C client - 21st January 2018
- First version of a golang D4 client³ running on ARM, MIPS, PPC and x86 - January 2018

²<https://www.github.com/D4-project/d4-core>

³<https://www.github.com/D4-project/d4-goclient/>

D4 OVERVIEW



ROADMAP (NEXT 2 MONTHS)

- Passive DNS analyzer (alpha version released)
- Passive SSL collector and analyzer
- Backscatter DDoS traffic analyzer
- **Default server** (blackhole monitoring or Passive DNS collector) at CIRCL for organisations willing to contribute without running their own D4 server

D4 ENCAPSULATION PROTOCOL

stream of information
(text or binary)

```
010111010100
100010101101
010100101011
010100100100
011010100101
01011101010010
100010101101
010100101111
010100100100
011010100101
01011101010010
100010101101
010100101111
010100100100
011010100101
01011101010010
100010101101
010100101111
010100100100
011010100101
```



D4 encapsulation protocol version 1



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



<https://www.d4-project.org>

D4 SERVER - MAIN INTERFACE

The screenshot displays the main interface of the D4 project, featuring a navigation bar with 'Home', 'Sensors Status', and 'Server Management'. The interface is divided into two main panels: 'UUID' and 'Types'. The 'UUID' panel lists two server entries with their IDs and UUIDs. The 'Types' panel lists two server entries with their IDs and counts. A 'Delete All Data (Demo)' button is located at the bottom center. The footer includes logos for CIRCL, the European Union, and the D4 project, along with text indicating co-financing by the Connecting Europe Facility of the European Union.

D4 project Home Sensors Status Server Management

UUID

13100	67034674dbe44fa18793186d05secf67
6798	fc84f70adb39440d875b1ce80aac90d5

2019/02/06

Types

12639	8
7259	1

2019/02/06

[Delete All Data \(Demo\)](#)

CIRCL
Computer Incident
Response Center
Luxembourg

Co-financed by the Connecting Europe
Facility of the European Union

D4 SERVER - SERVER MANAGEMENT

Da 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 (libcap 2.4)	Remove Type
4	dnscap output	Remove Type
8	passivedns CSV stream	Remove Type

Showing 1 to 3 of 3 entries Previous 1 Next

Add New Types

1
Add New Type

Add New Analyzer Queue

1

D4 SERVER - SENSOR OVERVIEW

D4 project [Home](#) [Sensors Status](#) [Server Management](#)

Active Connection

UUID: fc84f70adb39440d875b1ce80aac90d5

First Seen	Last Seen	Status
2019-02-02 12:30:00 - (1549107000)	2019-02-06 23:27:26 - (1549492046)	OK ✔ Connected

UUID: 67034674dbe44fa18793186d05ecfc67

First Seen	Last Seen	Status
2019-02-06 07:06:10 - (1549433170)	2019-02-06 23:29:49 - (1549492189)	OK ✔ Connected

D4 SERVER - SENSOR MANAGEMENT

D4 project Home Sensors Status Server Management

UUID: fc84f70adb39440d875b1ce80aac90d5

First Seen	Last Seen	Status
2019-02-02 12:30:00 - (1549107000)	2019-02-06 23:29:53 - (1549492193)	OK Connected

Change Stream Max Size

UUID Blacklist

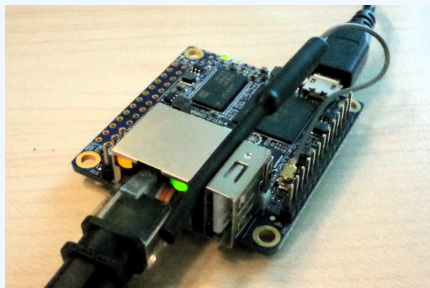
Blacklist IP Using This UUID

Change UUID Key

Last IP Used:

127.0.0.1 - 2019/2/06 - 23:02.16
127.0.0.1 - 2019/2/06 - 22:58.46
127.0.0.1 - 2019/2/06 - 22:56.10
127.0.0.1 - 2019/2/06 - 18:11.23
127.0.0.1 - 2019/2/06 - 11:44.50

D4 CLIENT EXAMPLE : A PASSIVE SSL FINGERPRINTER



- 1 desktop monitored during 15 days
- 3327 TLS sessions fingerprinted
- 600 unique certificates collected

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