

D4 Project

Open and collaborative network monitoring

Team CIRCL

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

2019/05/21

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 2019
- First version of a golang D4 client³ running on ARM, MIPS, PPC and x86 - 14th February 2019

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

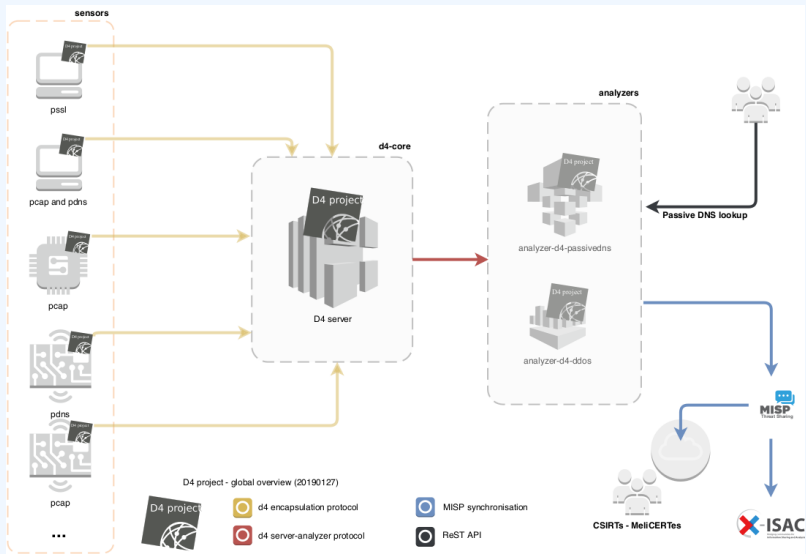
³<https://www.github.com/D4-project/d4-goclient/>

(SHORT) HISTORY

Release	Date
analyzer-d4-passivedns-vo.1	Apr. 5, 2019
analyzer-d4-passivessl-0.1	Apr. 25, 2019
analyzer-d4-pibs-vo.1	Apr. 8, 2019
BGP-Ranking-1.0	Apr. 25, 2019
d4-core-vo.1	Jan. 25, 2019
d4-core-vo.2	Feb. 14, 2019
d4-core-vo.3	Apr. 8, 2019
d4-goclient-vo.1	Feb. 14, 2019
d4-goclient-vo.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



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

stream of information
(text or binary)

```
010111010100
100010101101
010100101011
010100100100
011010100101

01011101010010
10001010110101
01010010101111
01010010010100
01101010010101

01011101010010
10001010110101
01010010101111
01010010010100
01101010010101
```



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>

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

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 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 core server⁴ 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>

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 blacklist
- Create Analyzer Queues

D4 SERVER - MAIN INTERFACE

The screenshot displays the main interface of the D4 Server. At the top, there is a navigation bar with the D4 Server logo and menu items: Home, Sensors Status, and Server Management. The interface is divided into two main panels: 'UUID' and 'Types'. Each panel contains a table of data points.

UUID	
13100	67034674dbe44fa18793186d05ecfc57
6798	fc84f70adb09440d875b1ce80aac90d5

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

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

Blacklist IP

Blacklist UUID

Header Accepted Types

Show entries Search:

Type	Description	Remove Type
1	pcap (libpcap 2.4)	<input type="button" value="Remove Type"/>
2	meta header (JSON)	<input type="button" value="Remove Type"/>
4	dnsmap output	<input type="button" value="Remove Type"/>
8	passivedns CSV stream	<input type="button" value="Remove Type"/>
254	type defined by meta header (type2)	<input type="button" value="Remove Type"/>

Showing 1 to 5 of 5 entries Previous Next

Add New Types

Show entries Search:

D4 SERVER - SERVER MANAGEMENT

Show entries Search:

Type Name	Description	Remove Type
ja3-ij		Remove Extended Type

Showing 1 to 1 of 1 entries Previous **1** Next

Analyzer Management

Show entries Search:

Type	uuid	last updated	Change max size limit	Analyzer Queue
1	404d4594-7881-4643-85bf-b1f7d9436e8	1553608013.429933	10000 <input type="text"/> Change Max Size	
4	ccb9548c380f4dd19ad3b1e94412e79a	Never	10000 <input type="text"/> Change Max Size	

Showing 1 to 2 of 2 entries Previous **1** Next

Add New Analyzer Queue

[Add New Analyzer](#)

Show entries Search:

Type Name	uuid	last updated	Change max size limit	Analyzer Queue
ja3-ij	ccb9548c380f4dd19ad3b1e94412e79a	Never	10000 <input type="text"/> Change Max Size	

Showing 1 to 1 of 1 entries Previous **1** Next

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: 67034674dbe44fa18793186d05efc67

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

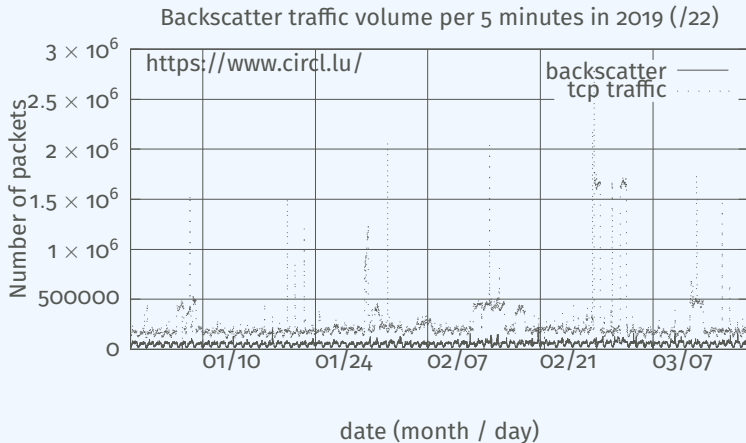
Last IP Used:

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

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

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

- CIRCL (and other CSIRTs) have their own passive DNS⁵ collection mechanisms
- Current **collection models** are affected with DoH⁶ 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/>

⁶DNS over HTTPS

- 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

- analyzer-d4-passivedns⁷ is an analyzer for a D4 network sensor. The analyser can process data produced by D4 sensors (in passivedns CSV format⁸)
- 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 Format⁹

⁷<https://github.com/D4-project/analyzer-d4-passivedns>

⁸<https://github.com/gamlinux/passivedns>

⁹<https://tools.ietf.org/html/draft-dulaunoy-dnsop-passive-dns-cof-04>

Passive SSL revamping

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.

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>

Mind your Ps and Qs:

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

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

¹¹github.com/D4-project/sensor-d4-tls-fingerprinting

¹²github.com/D4-project/analyzer-d4-passivessl

¹³github.com/D4-project/lookup-d4-passivessl

- **Mixing models for passive collection streams** (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