D4 Project

Revamping Passive SSL with D4

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

20190329

Jean-Louis Huynen

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.

Objectives

History of links between:

- x509 certificates (And therefore their fields),
- 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."*[1]

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

Problem statement

- CIRCL already offers a similar service based on SSLDump[2],
- SSLDump needs some love - maintaining it is hard,
- SSLDump needs some love - extending it even harder,
- nlternatives do not span the entire TLS Handshake (Salesforce's ja3[3]),
- TCP reassembly is not an easy problem to solve (Cloudfare's uses tshark[4]),

[2] https://www.circl.lu/services/passive-ssl/
[3] https://github.com/salesforce/ja3
[4] https://github.com/cloudflare/mitmengine

sensor-d4-tls-fingerprinting

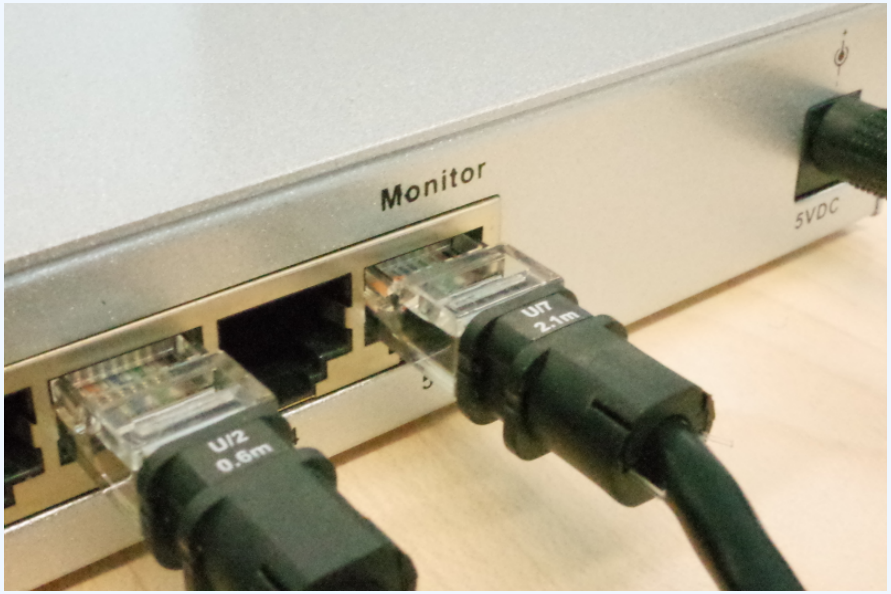
Main features:

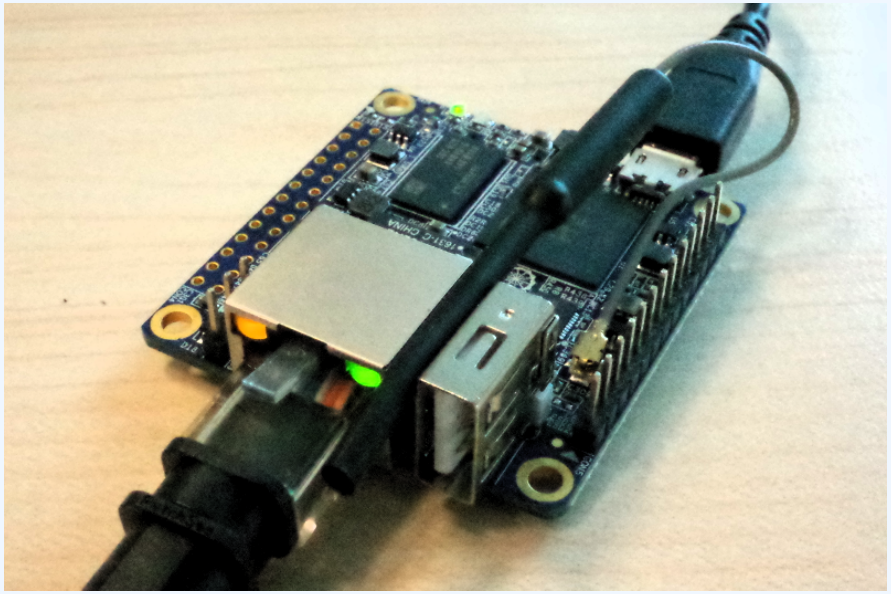
- take over SSLDump's duty,
- written in Golang
- uses Go packet for tcp reassembly and spans whole TLS handshake
- ja3, ja3s, certificates, ip src / dst, port src / dst, TLSH

Current caveats:

- Support for TLS 1.3 pending
- Reassembly consumes a lot of RAM

SENSOR-D4-TLS-FINGERPRINTING





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

```
./d4-tlsf-amd64 -r|-i [-w -j -d -mbpc -mbpt -v]
```

Options	Explanations
-r	read pcap file
-i	read from the interface
-w	dump certificates to folder
-j	write TLS session JSON descriptions to folder
-mbcp	max buffered pages per connection (16)
-mbpt	max total buffered pages (1024)
-d	debug
-v	verbose

Available on the D4 project's github page[5]. Depends on libpcap.

[5] github.com/D4-project/sensor-d4-tls-fingerprinting

Required setting:

- type should be set to 2 or 254
- metaheader.json should state type: ja3-jl

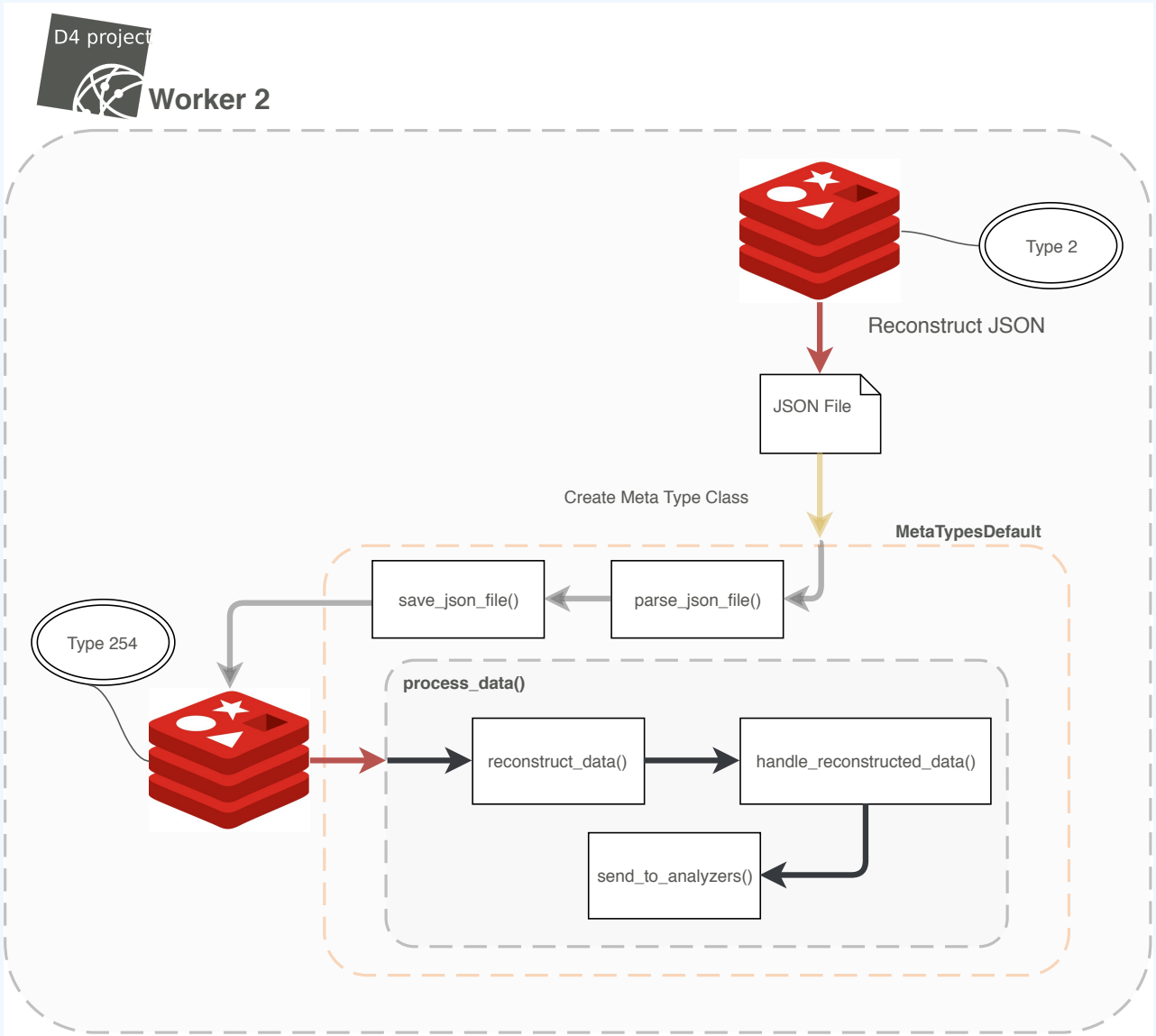
```
{
      "type": "ja3-jl"
}
```

```
./d4-tlsf-amd64 -i eth0 | ./d4-amd64 -c conf.crq
```

In the present setting the sensor will:

- describe every TLS Sessions,
- marshal this description in JSON format
- ship this description to the D4 server

SENSOR-D4-TLS-FINGERPRINTING - JA3-JL PLUGIN



SENSOR-D4-TLS-FINGERPRINTING - JA3-JL WORKER

```
def __init__(self, uuid, json_file):
    super().__init__(uuid, json_file)
    self.set_rotate_file_mode(False)

def process_data(self, data):
    self.reconstruct_data(data)

def handle_reconstructed_data(self, data):
    ...
```

- processes each reassembled JSON description,
- extracts x509 certificates and write to disk,
- writes JSON description to disk,
- push the files paths to the analyzer.

sensor-d4-tls-fingerprinting - ja3-jl analyzer

(Work in Progress)

Populates a database:

- LPOP a redis list populated by the worker
- push JSON descriptions into a postgres database

sensor-d4-tls-fingerprinting - passivessl API

(Work in Progress)

Exposes a REST API to query the collected data:

- /index : returns the full DB (PoC),
- /ja3/ : returns all TLS sessions with a given JA3 Signature,
- /ja3s/ : returns all TLS sessions with a given JA3S Signature,

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`