Legal stability and risks analysis Interim Report
Action No: 2017-LU-IA-0099
Distributed Denial of Services Detection Devices (D4) Platform

CIRCL*

This interim report describes the current progress of D4 platform's legal stability and risk analysis. At this data (early 2020), only the legal stability is completed.

Contents

*Electronic address: info@circl.lu; URL: http://www.circl.lu/
[1]Domain Name Service
[2]Secure Socket Layer

I. ORGANIZATION OF THE DOCUMENT

Analyzing D4 project's legal stability requires an understanding of several aspects that we introduce in 4 sections:

- D4's overall technical architecture,
- what data is planned to be collected, by whom and why, and who are the data subjects if any,
- who may expose this data, how, and who may access it,
- what is the legal frame of the project.

Ultimately we analyze the legal risk around the project and how these should be controlled.

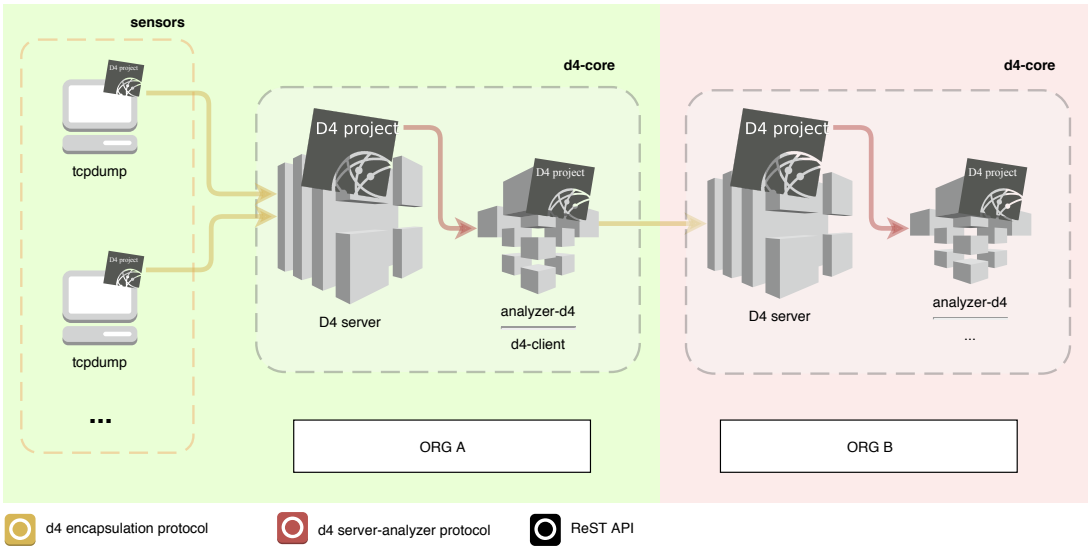
II. D4 ARCHITECTURE

The D4 platform is composed of two main components that work in chain: (1) a sensor that collects data and forwards it, (2) a server that collects data from sensors and analyzes it. Sensors and servers are aggregates of pieces of software that vary depending of the goal their operator:

- **Sensors** are the combination of a piece of software responsible for collecting data (eg. tcpdump[1], passivedns[2], etc.) and of a d4-client[3] that sends the data to a server using d4 protocol,
- **Servers** receive data emitted by sensors and expose the result through (redis[4]) streams to analyzers: plug-ins software that consume servers output to perform various security related tasks (eg. DDoS[5] detection, Database Store for API[6] exposure, etc.), or forward the data to another server (using a d4-client as would do a sensor).

Each component described above can be hosted and operated by different organizations. For instance see Fig.1: ORG A operates sensors and a server that forwards data to ORG B for further processing.

FIG. 1: D4 workflow example



[1] tcpdump is the goto tool for performing network captures
[2] a tool to record DNS records
[3] https://github.com/D4-project/d4-core/tree/master/client
[4] https://redis.io/topics/streams-intro
[5] Distributed Denial of Service
[6] Application Programming Interface

Before digging deeper into D4 platform's use-cases, it is well worth clarifying the points in the processing chain where organizations can act upon the data to comply with existing regulations and directives, and what are the foreseen challenges regardless of specifics:

- **Sensors:** in the simple case of an organization that operates its own sensors, it appears that the organization can choose what data it feeds its D4 platform with. For instance, when collecting network packets, BPFs[1] filters can be applied to the collection to prevent ingesting personal data. But as we will explain below, this task is actually challenging because D4 is meant to ingest data coming from various types of sensors, as for instance honeypots. This kind of data is difficult to qualify reliably automatically and therefore unexpected personal data may be ingested without means to detect this ingestion. This problem also arises when an organization consumes data from other parties.
- **Servers:** servers mix data streams by design: data is treated by type regardless of its origin. For instance all incoming passive DNS data is gathered in the same stream without keeping track of which sensor sent which record. This in itself is not a reliable safeguard to protect personal data but, depending on the number of sensors and volume of data, is already a first step in the D4 data processing chain that helps mitigating potential personal data exploitation efforts.
- **Analyzers:** unlike client and servers that focus on communication, analyzers focus on data processing and are therefore a right place for sanitizing data streams. In Fig.1 for instance, ORG A could use tcprewrite[2] to sanitize its data collection before forwarding the output to ORG B.

III. DATA COLLECTION AND ANALYSIS IN D4

As explained in Section II, D4 is built in a modular fashion. Its streaming protocol can be used to carry any data, and analyzers be built to perform unknown data processing. We have no control over what users actually do with D4. Therefore, we only discuss the use-cases that are officially developed within the frame of the project.

A. Honeypots and Darknets

Honeypots [6] operations is related to baiting, and deceiving. It consists of diverting adversary's interests onto a software component specially crafted to appeal to the adversary. All networking and computer services can be turned into honeypots: routers, websites, servers, remote administration services are all good candidates to such operations.

Honeypots collect data in the sense that these are meant to be probed and attacked while recording any activities that reach them in order to perform threat intelligence: these are used by CSIRTs[3] or private organizations to detect attacks in a network or perform research on threat actor TTP[4]. More specifically these are tools used to:

- gather information about existing threats, their objectives, modus-operandi, and capabilities,
- detect new attack trends,
- collect malicious software for further analysis,
- measure (distributed) denial of service attacks,
- estimate size of botnets,
- discover misconfigured machines to inform security point of contacts,
- get early warnings of attacks and system compromise (canaries),
- diverts adversary's energy onto component one controls and monitors.

[1] Berkeley Packet Filters
[2] a tool for rewriting parts of network captures
[3] Computer Security Incident Response Teams
[4] Techniques Tactics and Procedures

The types of honeypots which are not in scope of this question are honeypots involving social engineering, tar-pitting[1], or used in the process of catching and prosecuting criminals, for example by Law enforcement (e.g. setting up websites targeted at online child predators). In other words, D4 honeypot includes only low interaction honeypots related to enticement mechanisms, not entrapment.

D4 make heavy use of a special kind of honeypots the we commonly call 'darknets' or networks that should not receive any legitimate traffic to build a 'network telescope[2]'. This is a tool to measure the 'background noise' of the Internet and in particular on-going DDoS attacks and their premises. Such Honeypots operated within D4 settings for detecting DDoS attacks collect data emanating two types of entities:

- Legitimate actors operating misconfigured systems:
  - badly configured networking equipments (eg. DNS resolvers leaking DNS requests),
  - badly configured printers,
- Adversaries performing malicious activities:
  - backscatter traffic consequential to requests spoofing honeypot's IP[3] adresses,
  - attack traffic: (automated) exploit code, brute force attacks, amplification attacks, reconnaissance and scanning operations,

This data can be subdivided in two categories:

- the contents of communication (eg. data section of ICMP[4] packets),
- metadata of the communication, or information to establish communication (eg. IP addresses)

Analyzing backscatter traffic in this way brings information that can not be obtained otherwise as the observer is not part of the commumication between adversaries and victims, darknets offers external points of view of ongoing DDoS attacks (see the first part of D4 project's state of the art about DDoS for a detailed primer [5]). It helps in particular in: (1) confirming that there is an ongoing DDoS attack, (2) identifying victims and affected services, (3) observing victim's counter measures and their effects, and (4) assessing the state of the victim's infrastructure during the attack.

Identifying data subject and personal data in the data collected through honeypots is made difficult by the fact that there is no way to know which kind of data is collected at time of collection:

- data collected depends on the service attacked and the capabilities of the honeypot,
- there are doubts about how data should be interpreted (i.e. endianness[6], parsing of uninitialized memory),
- NAT (Network address translation) hides many machines behind an IP address,
- network packets observed can be spoofed,
- adversaries make use of deception to disguise their activities.

B. Passive DNS

What is commonly called a passive DNS is a database storing historical DNS records. This database can by fed by collecting feeds of DNS records from partners, or directly one's own network.

The main purpose of a passive DNS database is to be able to observe the changes of DNS records / IP addresses couples over time. This proves very useful for incident response, as well as for threat intelligence as it brings additional data points on which an analyst can pivot to link incidents and threats together.

---

[1] a tarpit is a kind of honeypot service that is made purposely unreliable to bog down the attacker.
[2] https://en.wikipedia.org/wiki/Network_telescope
[3] Internet Protocol
[4] Internet Control Message Protocol
[5] https://d4-project.org/2019/08/29/state-of-the-art-DDoS.html
[6] the ordering of bytes

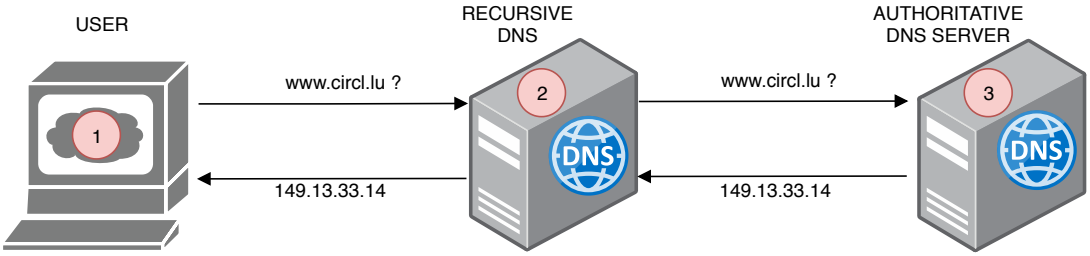
Recording data queries and response can also prove useful in detecting a particular form of DDoS attack called Slowdrip or Water Torture Attacks. Indeed Slowdrip attack consists of flooding the victim's domain's authoritative resolver with queries to inexistant sub-domains (via recursive resolvers and open resolvers). Detecting these attack at DNS level is the most effective as is can potentially be done even before adverse effects impact the victim's server [7].

The data collected for passive DNS are described an IETF[1] draft[4] and contain the following fields:

- name of the queried resource,
- resource record type as seen by the passive DNS,
- resource records of the queried resource,
- timestamps: first seen, last seen,

To understand legal implication of this collection, it is necessary to present the DNS lookup chain of requests[2]: when users use DNS to know which IP corresponds to a domain name, their computer will either ask to a 'recursive resolver' that belongs either to their ISP[3] or their hosting organization, or ask to an 'open recursive resolver'. These resolvers will provide the result by asking to the 'authoritative DNS server' corresponding to this domain (see Fig.2).

FIG. 2: DNS query chain



In D4, passive DNS sensors can potentially everywhere along the chain of requests, and depending on their location (see red circles in Fig.2), data subject can or cannot be identified:

- Sensor is hosted in 3: the data subject initiating the request is shielded by the recursive resolver. Therefore the entity operating the D4 passive DNS sensor can not link DNS records to data subjects.
- Sensor is hosted in 1 or 2: the data subjects and their DNS requests can be linked by the entity operating the D4 passive DNS sensor.

Furthermore, As seen in Fig. 1, D4 server can be chained. This has an impact on the data processor capability to identify data subjects. In the case of an ORG A forwarding PassiveDNS data to an ORG B: ORG A may be in a position to identify data subjects (as explained above) but it is technically impossible for ORG B.

In any case, the D4 system operator shall not link data subjects to the collected IP addresses as this link is useless for cyber incident response.

C. Passive SSL

A Passive SSL collector replicates Passive DNS's concept by storing all X.509 certificates used in SSL/TLS[4] connections, associated IP addresses, communication ports, and timestamps. Additional meta data are also collected regarding the TLS connection in order to identify the pieces of software taking part to the connection.

For each connection, data are collected about both the connection's source and destination:

[1] Internet Engineering Task Force
[2] we present here a rough overview of the mechanism–without caching–for the sake of simplicity.
[3] Internet Service Provider
[4] Transport Layer Security

- The source is usually a data subject. The data collected about it is the IP address, source port, and a "JA3" fingerprint of the connection (see [2] for further details),
- The destination is the service reached by the source. In addition to the IP address and destination port, data contained within the X.509 certificate (see [3] for a detailed overview of X.509 certificates and their data fields). This data can potentially leak information about the source data subject (these certificate are sometimes generated on-the-fly, per client). In the same fashion as the source, the destination software stack is fingerprinted by computing a "JA3S" hash.

As for Passive DNS, Passive SSL data is valuable for Incident Response, Threat Intelligence, and overall Situational awareness. Indeed, one specific use of Passive SSL in D4 is the detection of specific IoT[1] devices on a network by the X.509 certificates they use. This can prove useful for further mitigate possible DDoS attacks involving the said devices.

D. Cryptography sanity checks

Collecting X.509 certificates opens the door to the analysis of the cryptographic material they contain. The main concern here is again IoT devices: as these devices have usually low memory to store certificates, low computing power, and low bandwidth; they tend to use flawed implementations of TLS that are worth investigating.

There are several ways in which IoT devices can fail at crypto and D4 offers a 'crypto sanity check' in the form of a D4 analyzer called snake-oil-crypto [2] to identify the most common ones:

- Material key reuse: devices can share cryptographic parameters that defeats encryption,
- bad PRNG[3]: not choosing numbers randomly has catastrophic effects on cryptography,
- keys too small, ill parameters, leaked or cracked keys, etc.

We already ran snake-oil-crypto checks on some of our network collections and it yielded results regarding unpatched network devices vulnerable to CVE-2015-6418[4] and CVE-2015-6358[5].

Identifying early these low-hanging fruit helps in mitigating the risk that IoT and other devices with long patching cycle represent.

IV. DATA ACCESS IN D4

Data will be publicize in three ways within the project: (1) by providing online services as webpages as well as APIs, (2) by pushing results of analysis (eg. services under DDoS attacks) through MISP[6] instances, and (3) by providing raw data sets to academic researchers and security practitioners. D4 API shall expose detailed analyses's results, in particular: backscatter analysis daily digests, vulnerable cryptographic material, and provide additional relevant (or pivotal) information (IP addresses, DNS, BGP[7], IoCs[8], etc.) though MISP.

In the following table we summarize what data shall be made available, to whom, and through what mean, see Fig.I.

	API	Web	MISP	Access	Notify
passive DNS	✓	✓	✓	restricted	na
passive SSL	✓	✓	✓	restricted	na
DDoS detection	✓	✓	✓	public	✓
Crypto	✓	✓	✓	restricted	✓

TABLE I: Summury of data access and publication in D4

[1] Internet of Things
[2] https://github.com/D4-project/snake-oil-crypto/
[3] Pseudo Random Number Generator
[4] https://cve.circl.lu/cve/CVE-2015-6418
[5] https://cve.circl.lu/cve/CVE-2015-6358/
[6] https://www.misp-project.org/
[7] Border Gateway Protocol
[8] Indicator of Compromises

Notifications shall be done on a best effort basis, as victim can not always be identified.

Regarding the compliance of sharing such data through MISP within the GDPR[1] framework, we direct the reader to CIRCL Technical Report 48 [5] and and MISP project's website [1] that explain in detail why such sharing is not only lawful but actually required by the regulation (Article 32, 1, d; Recital 49).

V. LEGAL STABILITY AND RISK ANALYSIS

We presented the D4 platform, and the data and processing over this data that is foreseen in the frame of the project. We now dig into directives and regulations that are applicable to D4 (eg. GDPR [8]), and the justifications for CSIRTs for embracing D4 for their data collection operations.

In the following, we consider that the case for Passive DNS, Passive SSL and honeypots are similar: **at the time of collection, data may be linked to data subjects but this link shall not be fed into the system** (for passiveDNS run in case 1 and 2 for instance, see Section III B). **Data subject information shall enter the system only accidentally without realistic means of preventing or detecting it** (see for instance honeypot collection in Section III A).

A. Data subject rights

The most important risk to D4 system's data controller is failing to ensure the respect of data subject's rights:

- **right of access by the data subject** (article 15)
- **right of rectification** (article 16)
- **right of erasure ('right to be forgotten')** (article 17)
- **right of restriction of processing** (article 18)
- **right of data portability** (article 20)
- **right to object and automated individual decision making, including profiling** (article 21 & 22)

We now discuss how a data controller can ensure running D4 services does not violate these rights.

We can differentiate two cases:

- **the case where one collects data on his own network, for its own interests:** in this case one has to inform data subjects that honeypots are included in its networks, and one has to disclose the reasons of this collection.

  Article 13 Regulation 2016/679 **Information to be provided where personal data are collected from the data subject**:

  1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

  (d) **where the processing is based on point (f) of Article 6(1)[2], the legitimate interests pursued by the controller or by a third party;**

- **the case of distributed open networks, personal data have not been obtained from the data subject:** in this case, the operator can not obviously identify data subjects although there is a strong need to identify responsible point of contact to remediate situations such as fixing misconfigured systems, information leaks, or others.

  Article 14 Regulation 2016/679 **Information to be provided where personal data have not been obtained from the data subject**:

  5. Paragraphs 1 to 4 shall not apply where and insofar as:

[1] General Data Protection Regulation
[2] discussed below

(b) **the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1)**[1] or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

Additionally, D4 honeypots are most likely to be operated under one of the two following legal grounds Article 6 **Lawfulness of processing**:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) **processing is necessary for the performance of a task carried out in the public interest**.

(f) **processing is necessary for the purposes of the legitimate interests pursued by the controller**.

This aforementioned article can be further interpreted in the light of Recital 49 Regulation 2016/679. Indeed, it further consolidates the argument that CERTs and CSIRTS operating honeypot or performing data collection and other data processing to improve their level of security is Lawful:

(49) **The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.**

Finally, D4 processings shall also fit Article 89 Regulation 2016/679 **Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**:

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. **Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.**

As discussed above, D4 provides pseudonymisation means has defined by Article 4 Regulation 2016/679 **definitions**:

(5) **pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;**

Furthermore, D4 data processing do not require to identify data subjects to succeed and the GDPR specifies exceptions in the case of processing that do not require identification Article 11 Regulation 2016/679 **Processing which does not require identification**:

(1) **If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.**

[1] discussed below

(2) **Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.**

In this setting, the main challenge resides in identifying data subjects when they exert their right to article 15 to 20, in particular:

- How to prove the identity of a data subject?
- How to prove that the requested data belongs to the data subject?
- How much effort should be put into reverting D4 pseudonymisation?
- How to ensure no interference with ongoing investigations by law enforcement (i.e. evidences collected by the honeypot)

The Regulation 2016/679 specifies that the data controller when in doubt, should not release the data because of doubt about the data subject's identity:
Article 12: Regulation 2016/679 **Transparent information, communication and modalities for the exercise of the rights of the data subject** :

6. **Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.**

Or also because of the crossing of best effort boundaries:

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. **Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:**

   (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

   (b) refuse to act on the request.

B. Impact assessment

Article 35 of Regulation 2016/679 **Data protection impact assessment** specifies when an impact assessment is necessary for a data processing:

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, **is likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

   (a) a systematic and extensive **evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling**, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

   (b) processing on a large scale of **special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or**

   (c) **a systematic monitoring of a publicly accessible area on a large scale.**

In the setting of Passive DNS, Passive SSL and honeypot operations, we consider that D4 is out of the scope of this article for the following reasons:

- The data collected does not constitute a high risk to the rights and freedoms of natural persons, nor is used for producing effects on these persons.
- **The data collected in only used for gathering information about cyber security threats or to support cyber security incident response. Its link to a natural person is only consequential to the fact that some collected artifacts are the results of the activities of natural persons. Nevertheless, no effort shall be put into removing this link as this would damage incident response capabilities.**
- In case a D4 system was to be used for more pervasive data collection and analysis as the latter case (c) (and unlike passive DNS / SSL and honeypot operations considered here), the data controller should perform an impact assessment that implements Article 35 of Regulation 2016/679 **Data protection impact assessment** paragraph 7.

C. Security of processing

Following Article 32 of Regulation 2016/679 **Security of processing**:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate**:
   (a) **the pseudonymisation and encryption of personal data;**
   (b) the ability to **ensure the ongoing confidentiality, integrity**, availability and resilience of processing systems and services;
   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

We consider that points (c) and (d) are the responsibilities of the D4 instance data controller. D4 project provides several means to ensure (a) and (b):

(a) As described in Section II, **D4 mix streams of data, and analyzers provide means to pseudonimize personal data**. We don't deem encryption at rest to be mandatory once the data is pseudonymised as it would hinder performances for questionable confidentiality gains (indeed, reversing pseudomisation is always possible but is costly and required to cross the data with other datasets, we don't think the data held in D4 system would appeal so much to an attacker that it could go through the hassle to performing such computation–the threat is therefore negligible)

(b) **D4 protocol ensures the confidentiality of personal data before it reaches D4 server for pseudomisation using TLS protocol (it is encrypted, authenticated, and its integrity is guaranteed)**. Users of the system authenticate through the use of a password or an API key that are stored properly hashed and salted in database.

As mentioned above, in the setting of D4 passive DNS / SSL and honeypot operations, the data processed shall not pose a risk to the rights and freedoms of natural persons. Therefore, following Article 33 of Regulation 2016/679 **Notification of a personal data breach to the supervisory authority** there is not need to notify the supervisory authority competent in accordance with Article 55 of the same regulation in the case of a breach.

VI. CONCLUSION

Given the present analysis, we can confidently affirm that D4 is capable to reach its objectives while respecting EU regulations and directives, in particular regarding:

- internal collection of data,
- distributed collection of data,
- information sharing regarding D4 analyses results.

VII. ACRONYMS

DNS Domain Name Service . . . 1
SSL Secure Socket Layer . . . 1
BPF Berkeley Packet Filter . . . 3
API Application Programming Interface . . . 2
DDoS Distributed Denial of Service . . . 2
TTP Techniques Tactics and Procedures . . . 3
CSIRT Computer Security Incident Response Team . . . 3
IP Internet Protocol . . . 4
IETF Internet Engineering Task Force . . . 5
ICMP Internet Control Message Protocol . . . 4
IoT Internet of Things . . . 6
TLS Transport Layer Security . . . 5
ISP Internet Service Provider . . . 5
BGP Border Gateway Protocol . . . 6
IoC Indicator of Compromise . . . 6
PRNG Pseudo Random Number Generator . . . 6
GDPR General Data Protection Regulation . . . 7

[1] Information sharing and cooperation enabled by gdpr, January 2018.
[2] John Althouse. TLS Fingerprinting with JA3 and JA3S, January 2019.
[3] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. RFC 5280, RFC Editor, May 2008. `http://www.rfc-editor.org/rfc/rfc5280.txt`.
[4] Alexandre Dulaunoy, Aaron Kaplan, Paul A. Vixie, and Henry Stern. Passive DNS - Common Output Format. Internet-Draft draft-dulaunoy-dnsop-passive-dns-cof-06, Internet Engineering Task Force, April 2019. Work in Progress.
[5] Matthieu Farcot. TR-48 - Cyber-Threats Indicators Sharing, security-related actionable information and future of Personal Data Protection framework in the EU - MISP and GDPR. Technical report, CIRCL, 2017.
[6] Lance Spitzner. *Honeypots: Tracking Hackers*. Addison-Wesley Professional, 2002.
[7] Yuya Takeuchi, Takuro Yoshida, Ryotaro Kobayashi, Masahiko Kato, and Hiroyuki Kishimoto. Detection of the dns water torture attack by analyzing features of the subdomain name. *Journal of Information Processing*, 24(5):793–801, 2016.
[8] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). *Official Journal of the European Union*, 2016.