Recursive DNS. Is There A Problem?

* We all know that recursive DNS is much more complicated than authoritative DNS.
    * We also know that recursive DNS, traditionally, is where you lose money, as it is expected to be free.
* However, to further complicate matters, the requirements on recursive DNS are changing.

Why Are The Requirements Changing?

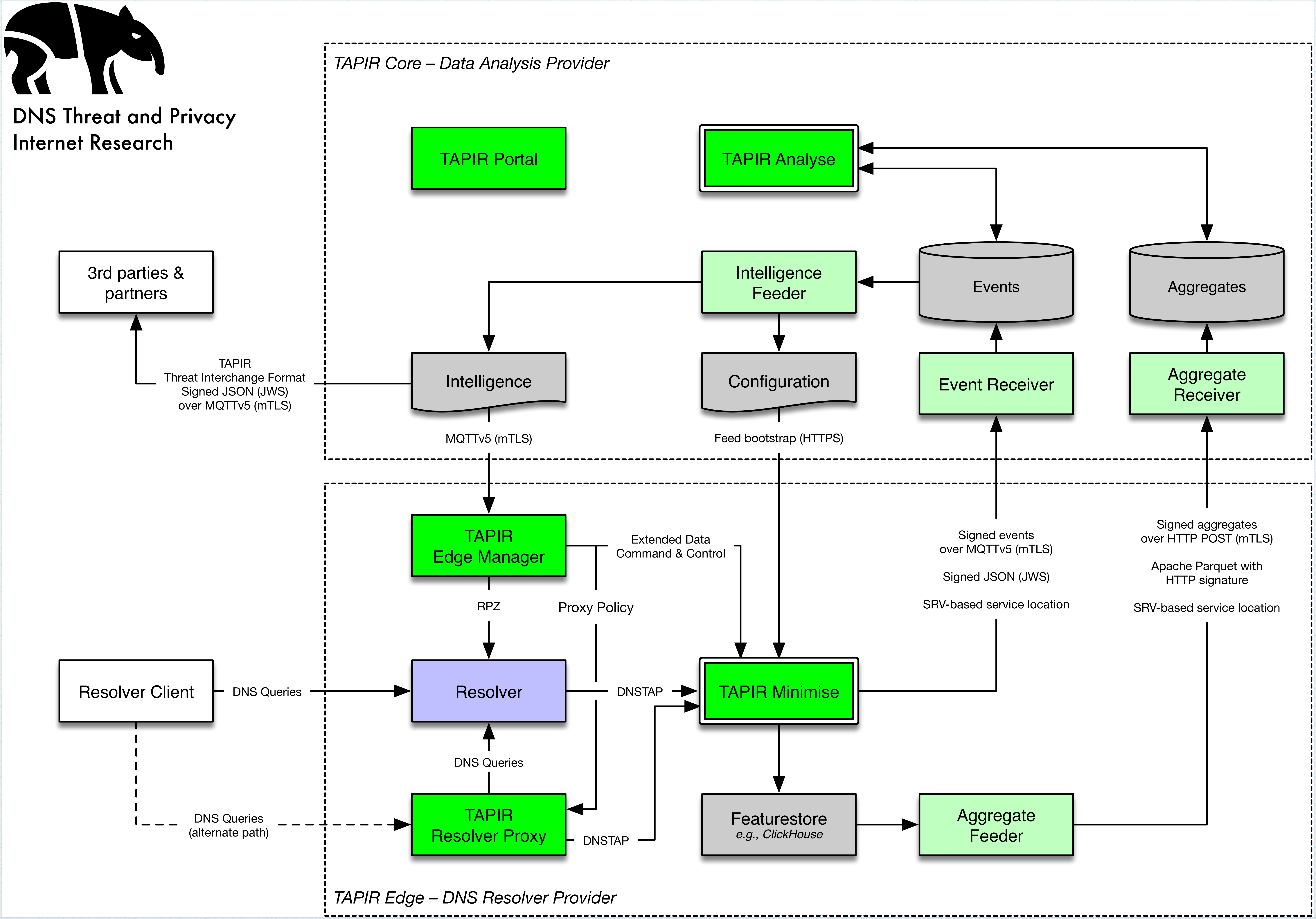
* Growing amounts of “malicious traffic”.
* Growing amounts of “legitimate” tracking of various kinds.
* Increasing concerns about leakage of privacy-sensitive user data via DNS.
* The problems are not new, but the awareness of the problems is “improving”.

There Are Solutions

* There is a plethora of "threat feed" providers. Mostly commercial.
* There are several commercial providers of different types of "protected DNS", i.e. recursive DNS plus some sort of filtering based on one or more threat feeds.
* There are several "national initiatives" for recursive DNS (Canada, UK, etc).
    * DNS4EU is also sort of in this category.

Introducing DNS TAPIR

* DNS TAPIR is a Swedish, government funded, development project.
* One goal is a national "analysis service" using aggregated data from resolvers as input and generating "intelligence" as output.
* Another goal is pre-packaged "kit" that provides collection infrastructure around a resolver that generates the aggregates.
* DNS TAPIR is not a recursive DNS service.



DNS Threat and Privacy
Internet Research
TAPIR Core – Data Analysis Provider
TAPIR Portal
TAPIR Analyse
3rd parties & partners
Intelligence Feeder
Events
Aggregates
TAPIR
Threat Interchange Format
Signed JSON (JWS)
over MQTTv5 (mTLS)
Intelligence
Configuration
Event Receiver
Aggregate Receiver
MQTTv5 (mTLS)
Feed bootstrap (HTTPS)
TAPIR Edge Manager
Extended Data
Command & Control
Signed events
over MQTTv5 (mTLS)
Signed JSON (JWS)
SRV-based service location
Signed aggregates
over HTTP POST (mTLS)
Apache Parquet with
HTTP signature
SRV-based service location
RPZ
Proxy Policy
Resolver Client
DNS Queries
Resolver
DNSTAP
TAPIR Minimise
DNS Queries
DNS Queries
(alternate path)
TAPIR Resolver Proxy
DNSTAP
Featurestore
e.g., ClickHouse
Aggregate Feeder
TAPIR Edge – DNS Resolver Provider

How To Gain Trust?

* All code will be open source.
* It should be possible for anyone to essentially replicate the analysis to reach the same result.
* It should be possible for a resolver operator to build the local collection infrastructure from open source and get the same result as if using the "kit" provided by DNS TAPIR.

How To Protect Privacy?

* The analysis service should never see the individual queries, only aggregates.
* The decision to act on resulting intelligence is local to the edge (i.e. the local resolver).