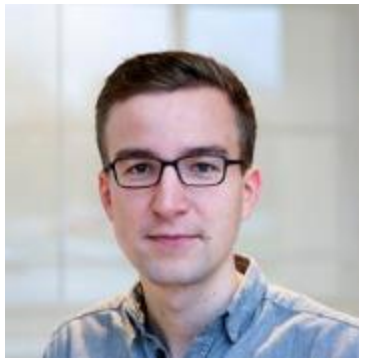
Your world. Our domain.

Hoe je big data inzet voor de veiligheid en stabiliteit van het internet

15-11-2017 | Technisch Webinar | SIDN Labs

Agenda

15:00	Intro Webinar *Sebastiaan Assink (relatiebeheerder SIDN)*
15:05 – 15:15	Signalen die duiden op malafide activiteiten *Moritz Müller (research engineer SIDN Labs)*
15:15 – 15:30	Wat is ENTRADA en hoe werkt het? *Maarten Wullink (research engineer SIDN Labs)*
15:30 – 15:45	Gebruik van ENTRADA binnen SIDN (use cases)
15:45 – 15:55	Uitloop + mogelijkheid tot stellen van vragen



Poll: Analyseer jij je DNS-verkeer?

Signals for malicious activities

Suspicious Domain Name Signals

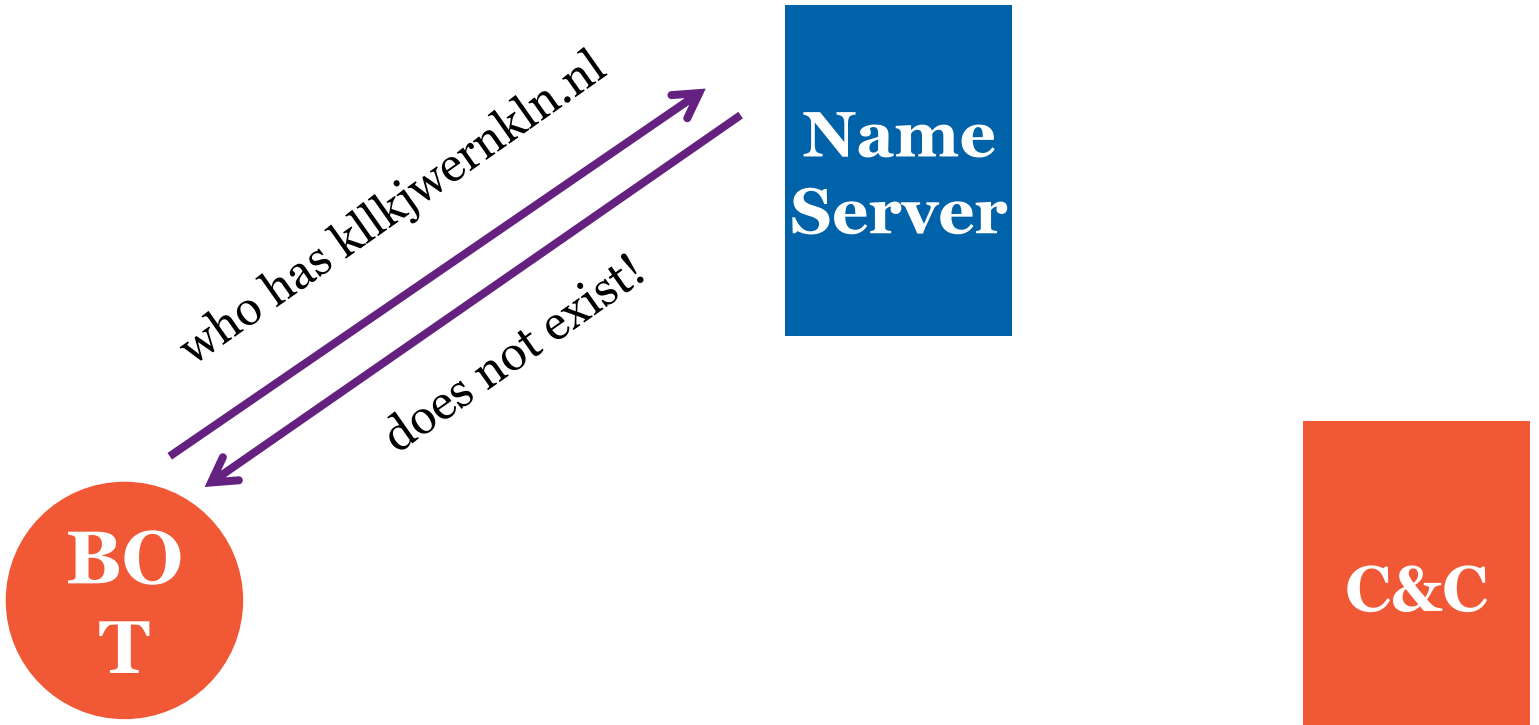
- The “look” of a domain name
- Features of the domain name records
- Query patterns
- Domain registration features

Suspicious Domain Name Activities

- The “look” of a domain name
  - Domain Name Generation Algorithms (DGA)

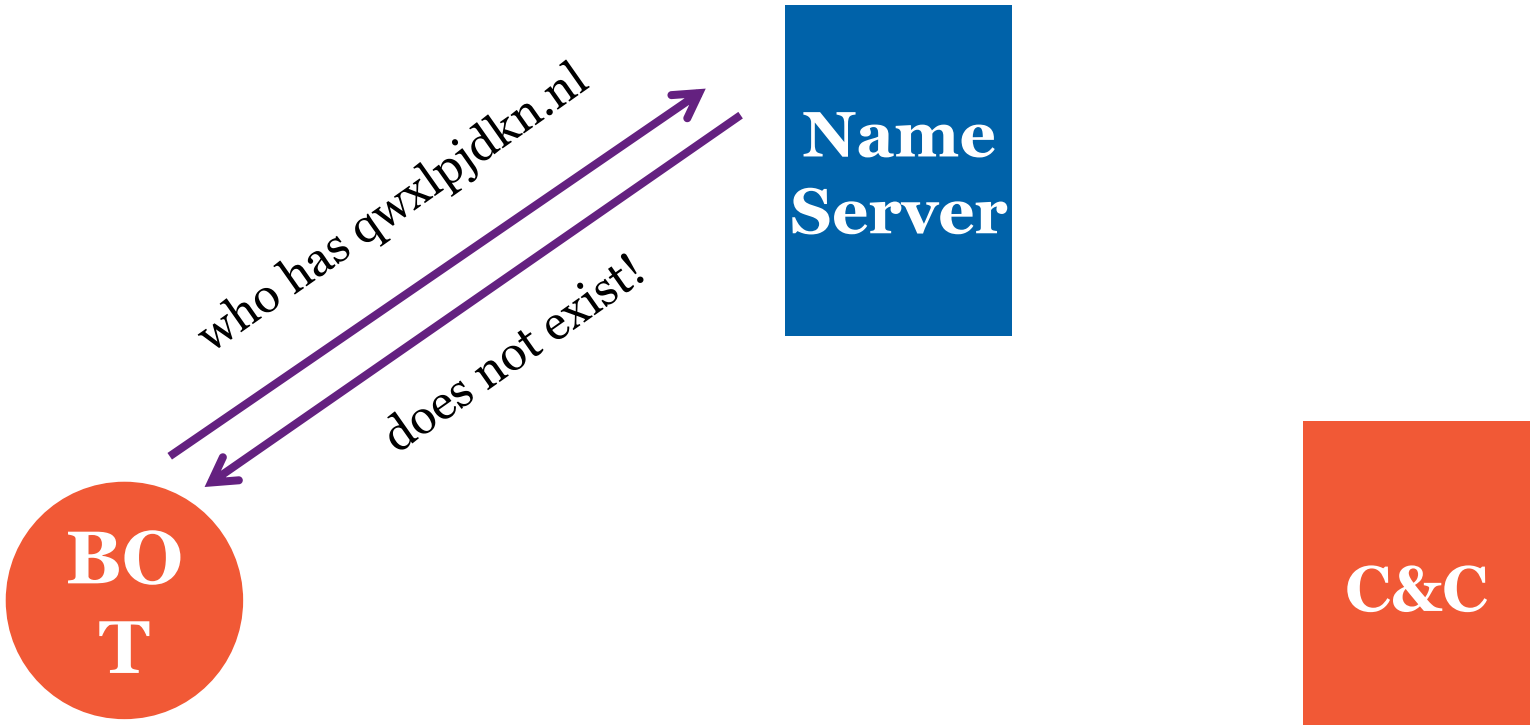
Suspicious Domain Name Activities

- The “look” of a domain name
  - Domain Name Generation Algorithms (DGA)



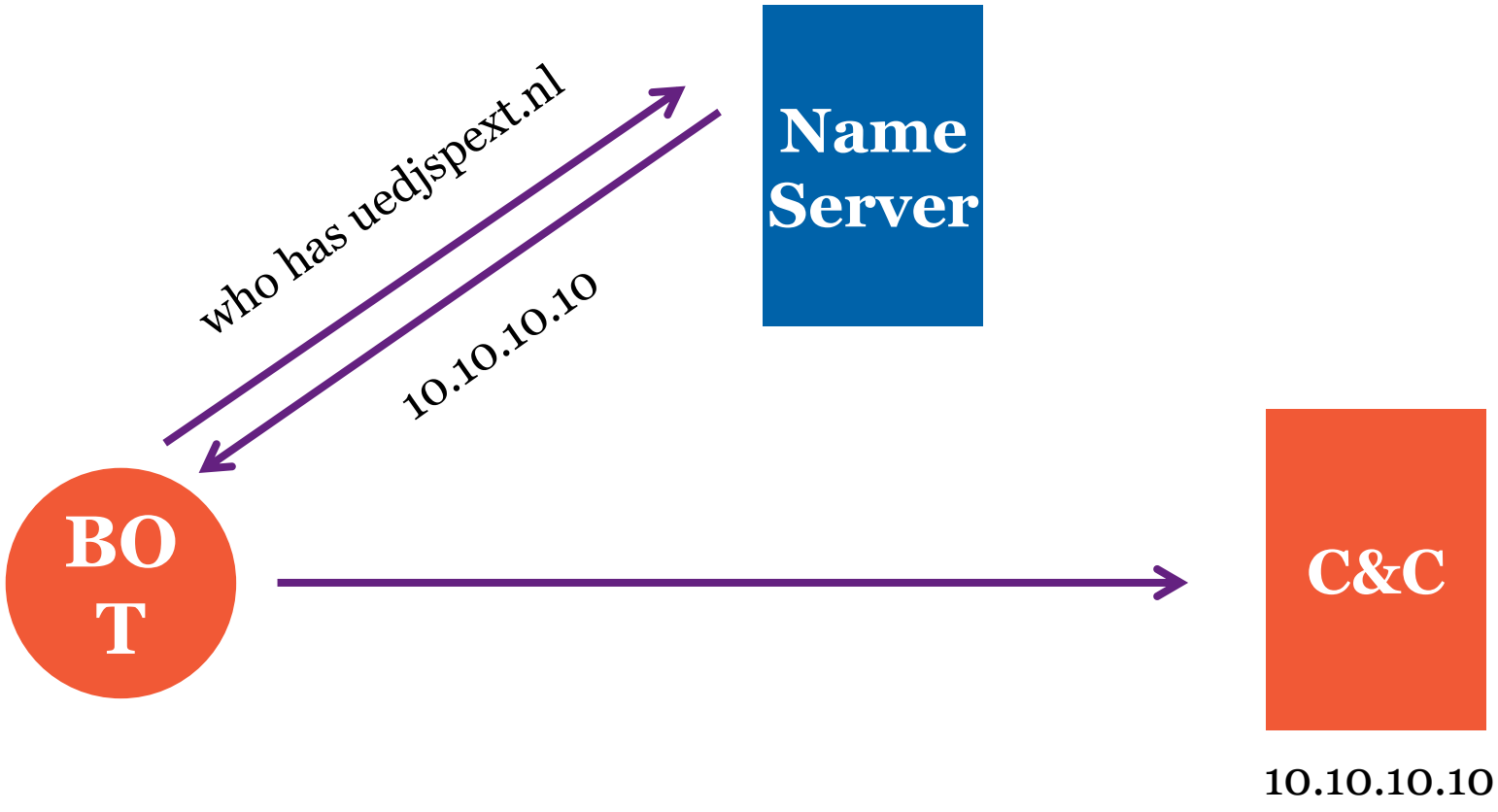
Suspicious Domain Name Activities

- The “look” of a domain name
  - Domain Name Generation Algorithms (DGA)



Suspicious Domain Name Activities

- The “look” of a domain name
  - Domain Name Generation Algorithms (DGA)

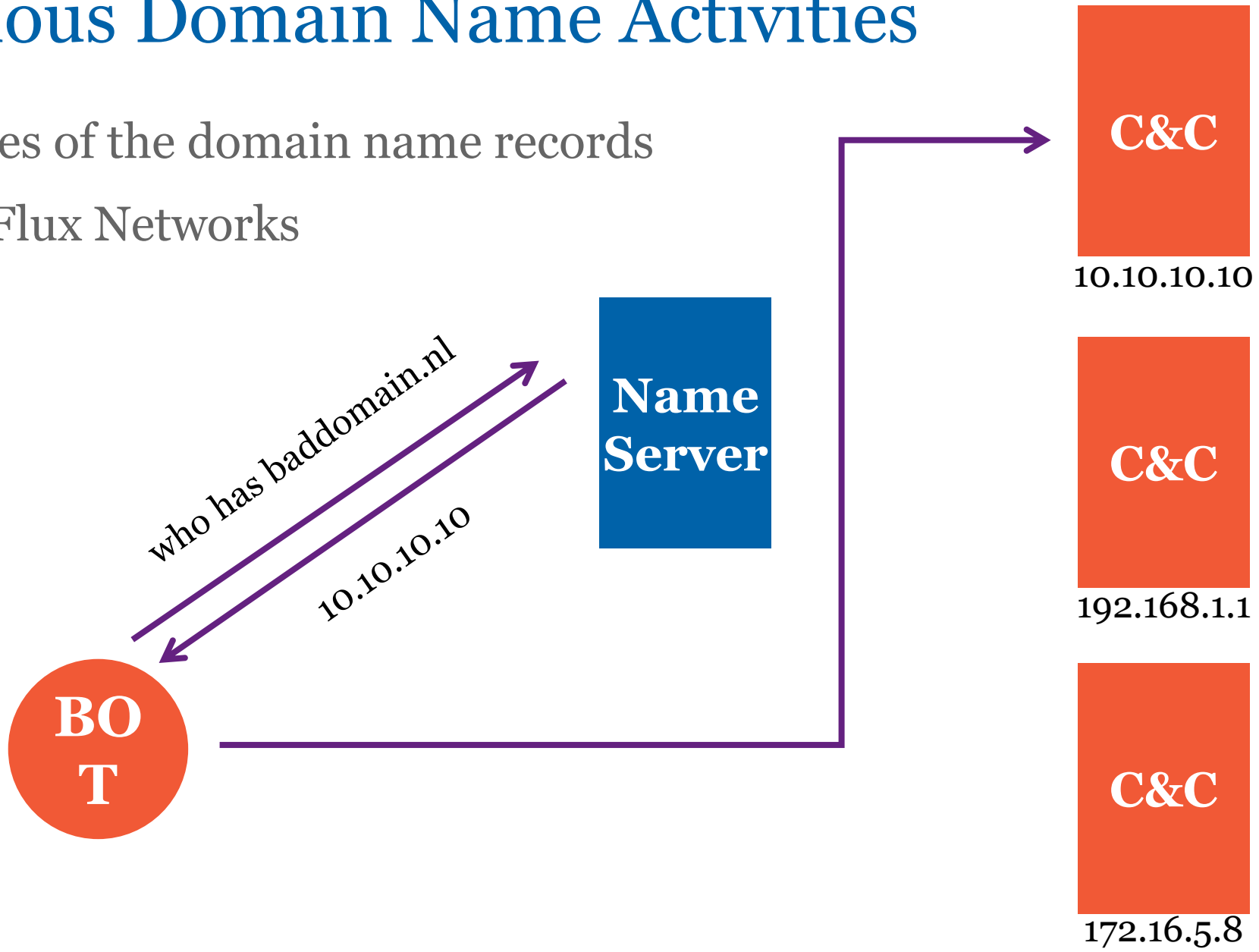


Suspicious Domain Name Activities

- Features of the domain name records
  - Fast Flux Networks

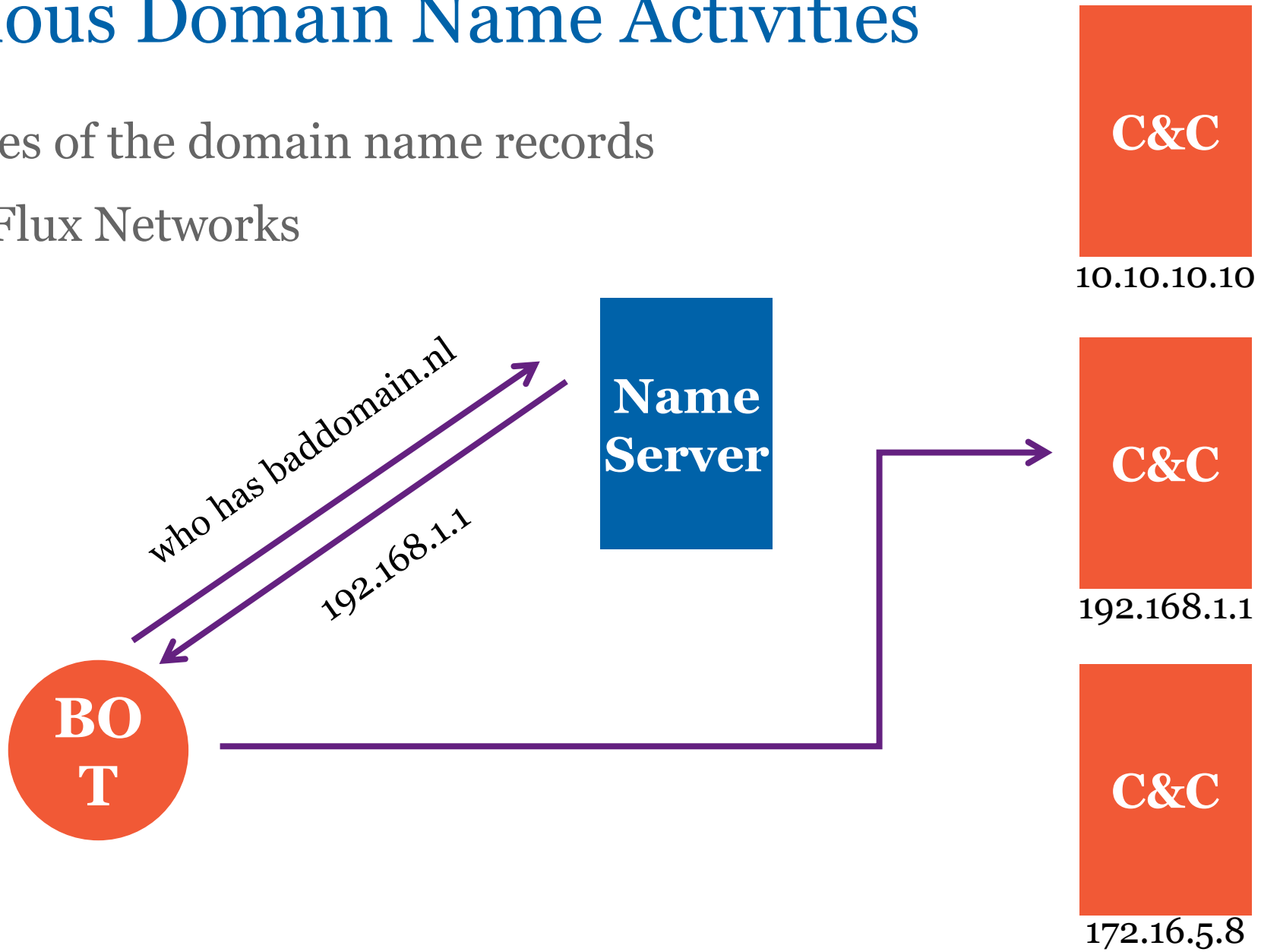
Suspicious Domain Name Activities

- Features of the domain name records
  - Fast Flux Networks



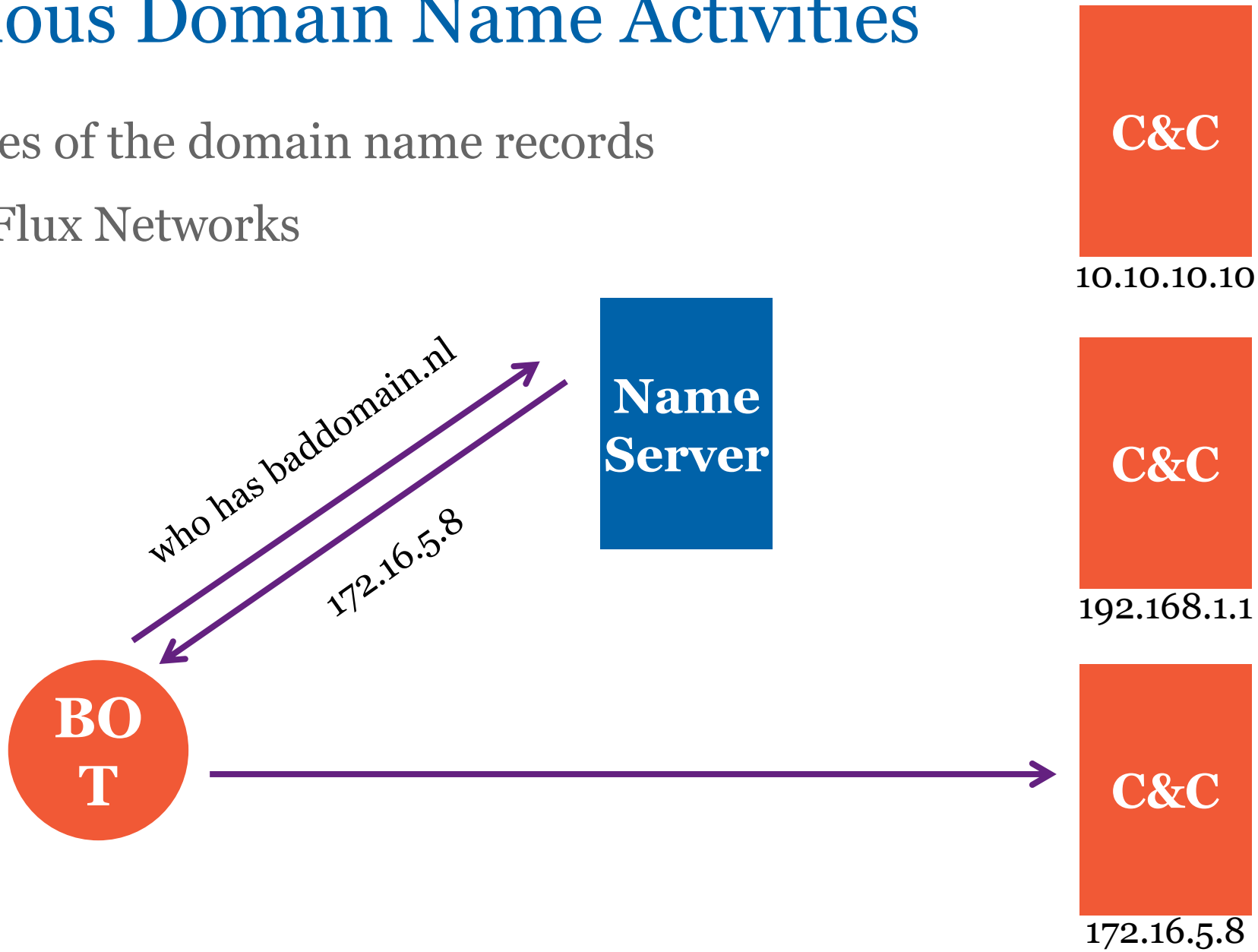
Suspicious Domain Name Activities

- Features of the domain name records
  - Fast Flux Networks



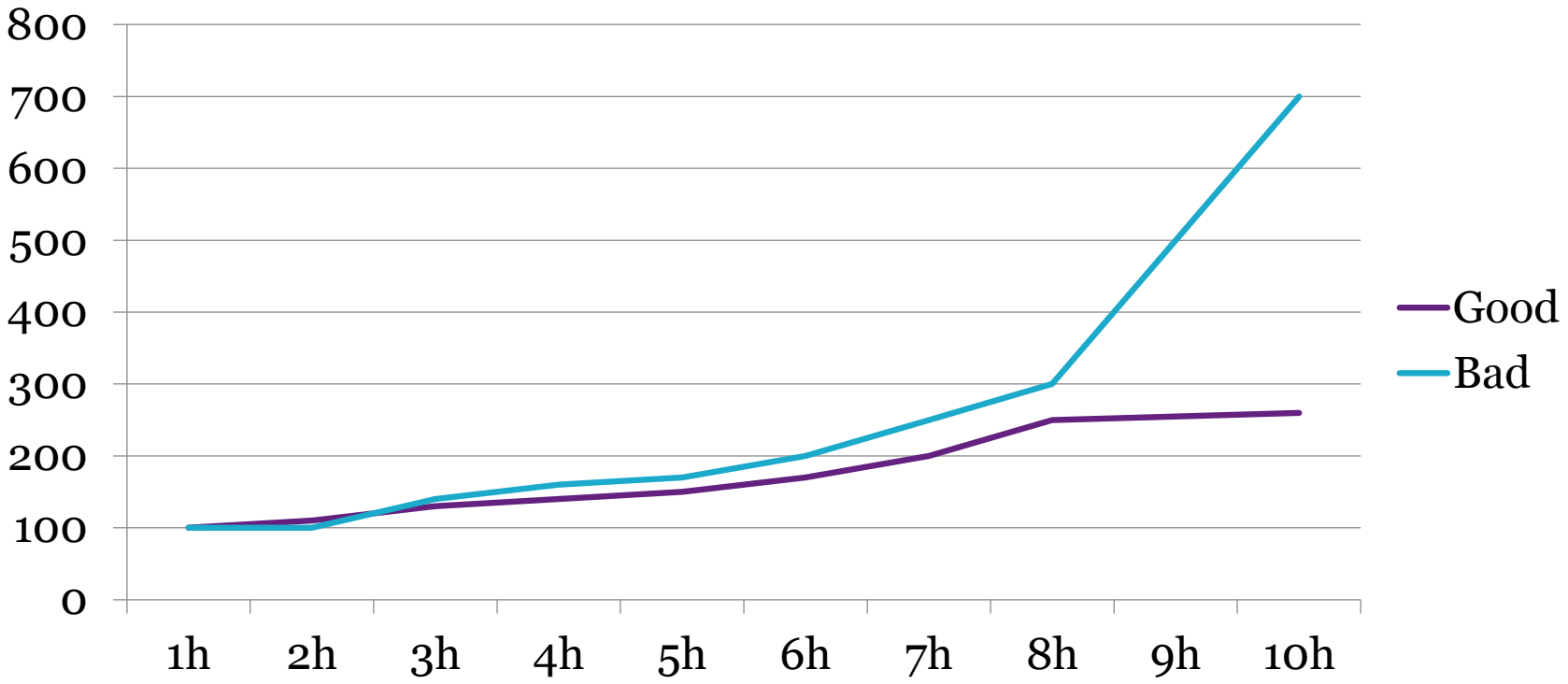
Suspicious Domain Name Activities

- Features of the domain name records
  - Fast Flux Networks



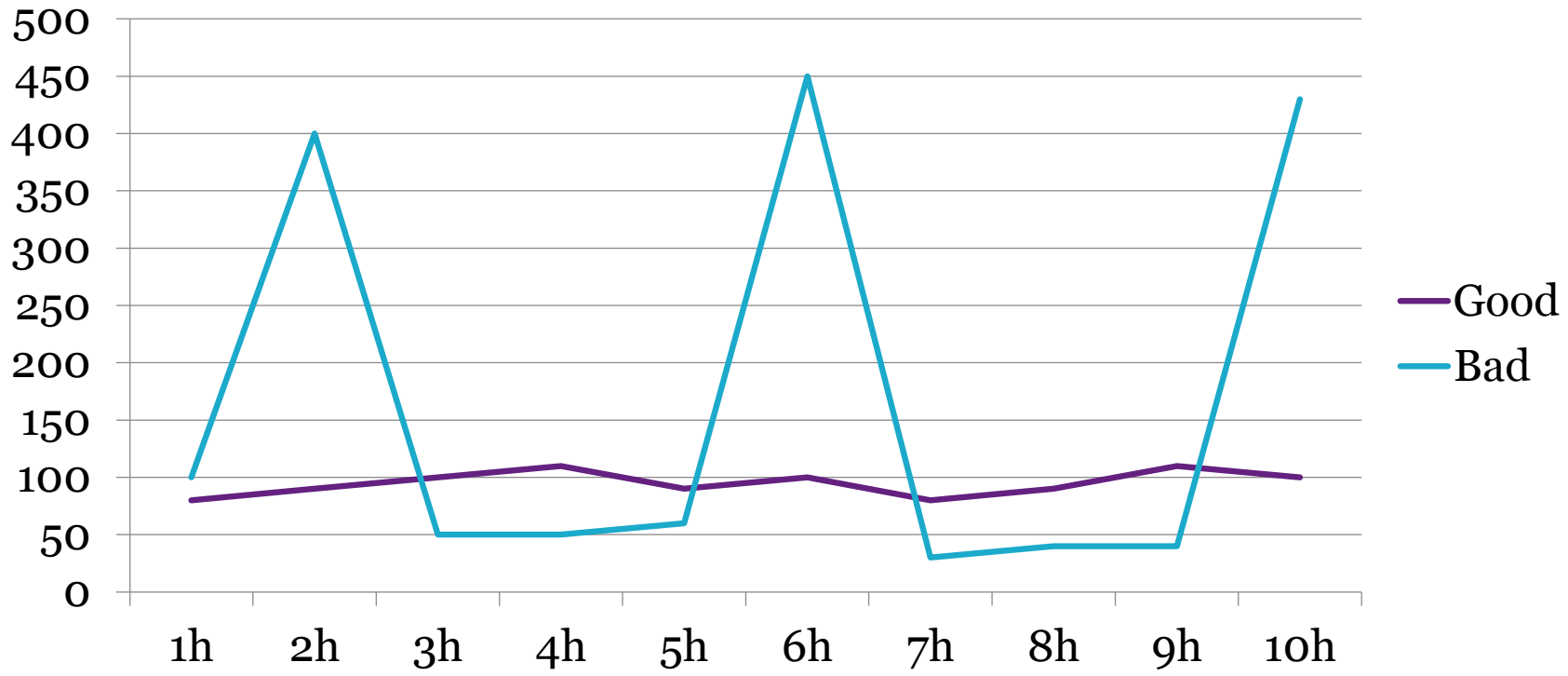
Suspicious Domain Name Activities

- Query patterns: Steep query increase



Suspicious Domain Name Activities

- Query patterns: Regular patterns



Suspicious Domain Name Activities

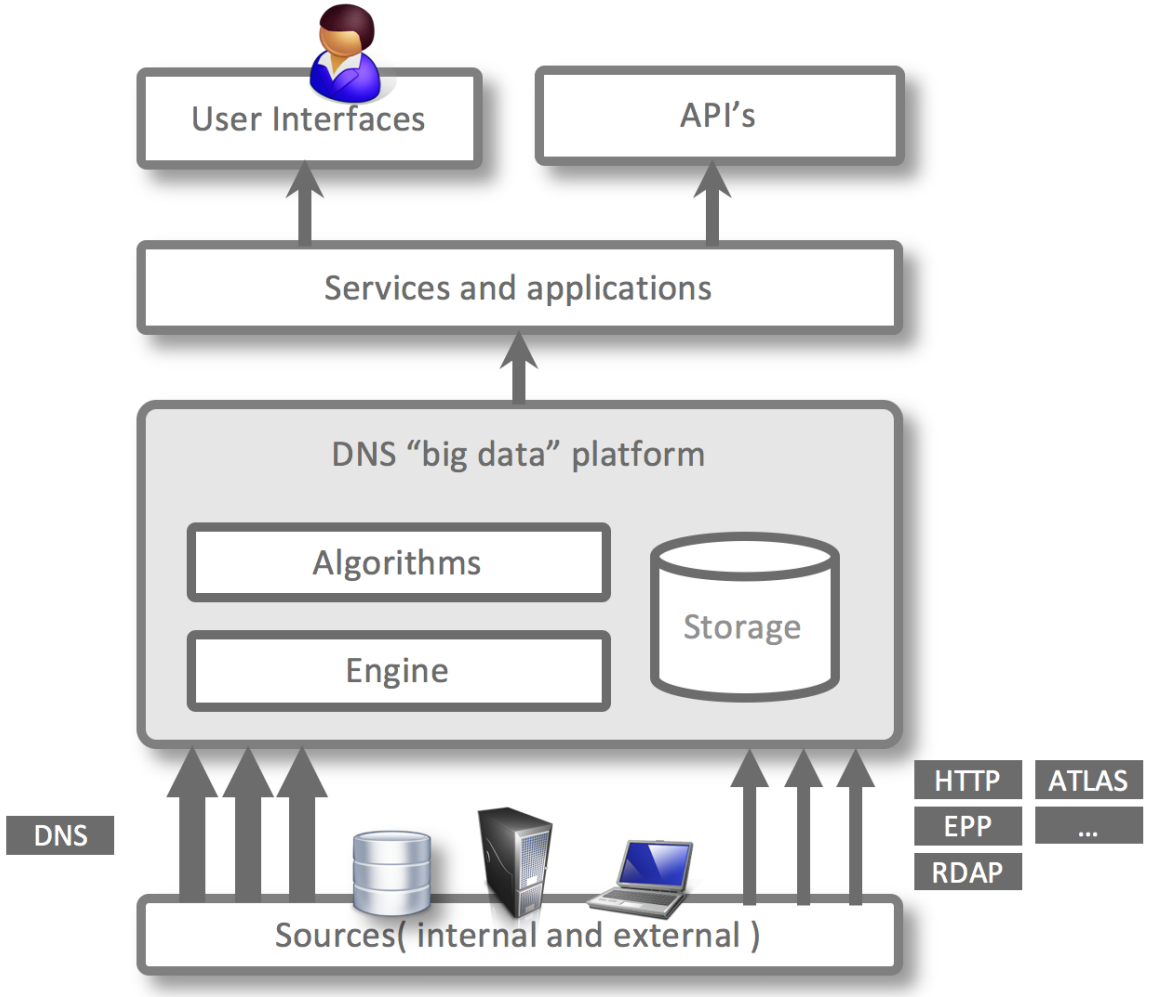
- Domain registration features
  - Very young and active domains
  - Suspicious registration data

Technical Background of ENTRADA

ENTRADA Architecture

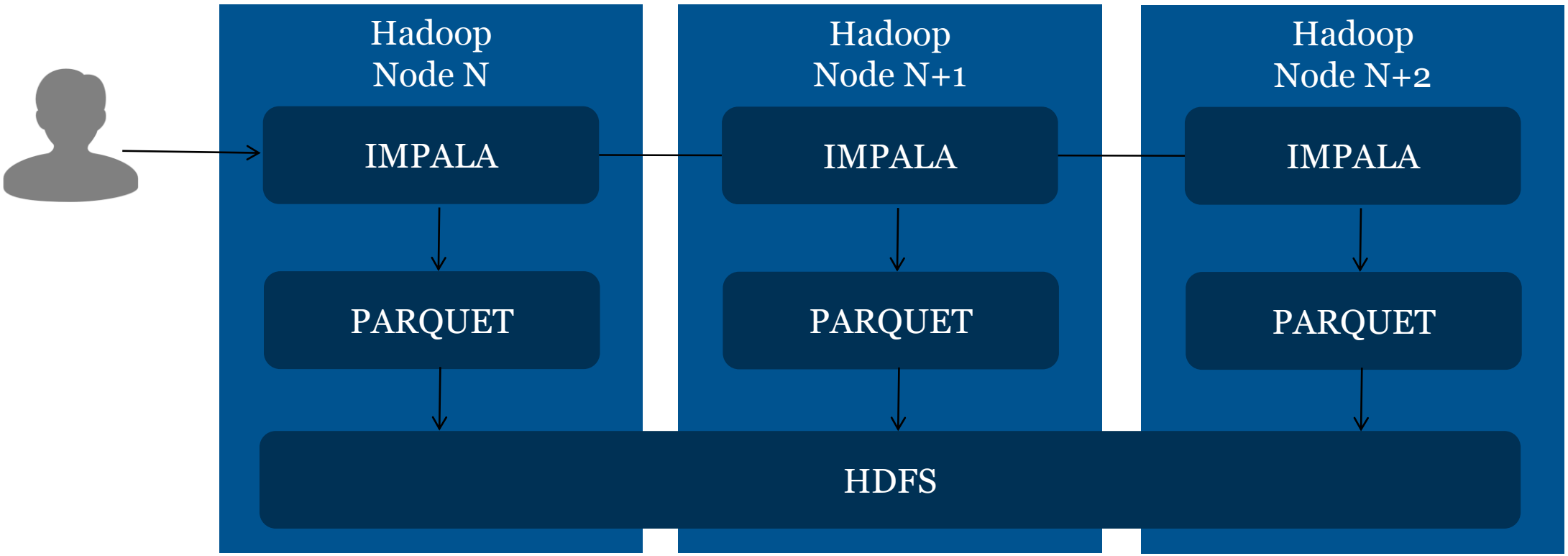
Main components

- Data sources
- Platform
- Applications and services
- Privacy framework



SQL on Hadoop

Best fit for our requirements



Impala

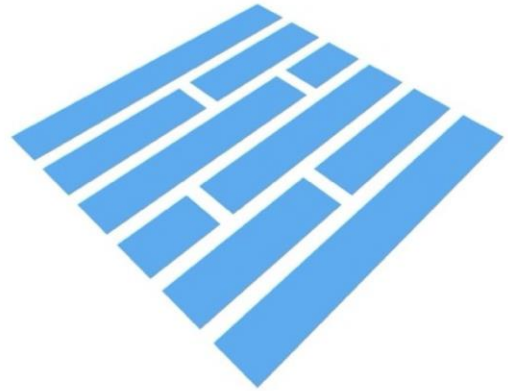
Data formats

- Text
- Hadoop formats
- Apache Avro
- Apache Parquet

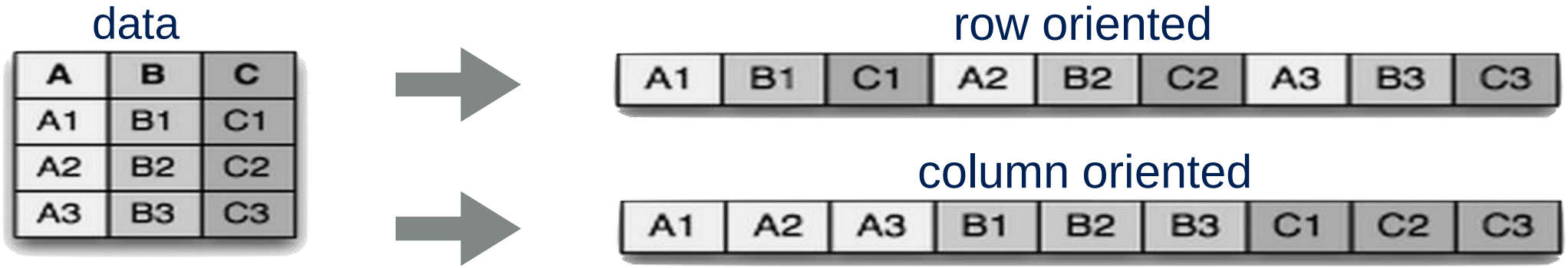
Interfaces

- Web-based GUI
- Command line (impala-shell)
- Python (Impyla)
- JDBC

Apache Parquet



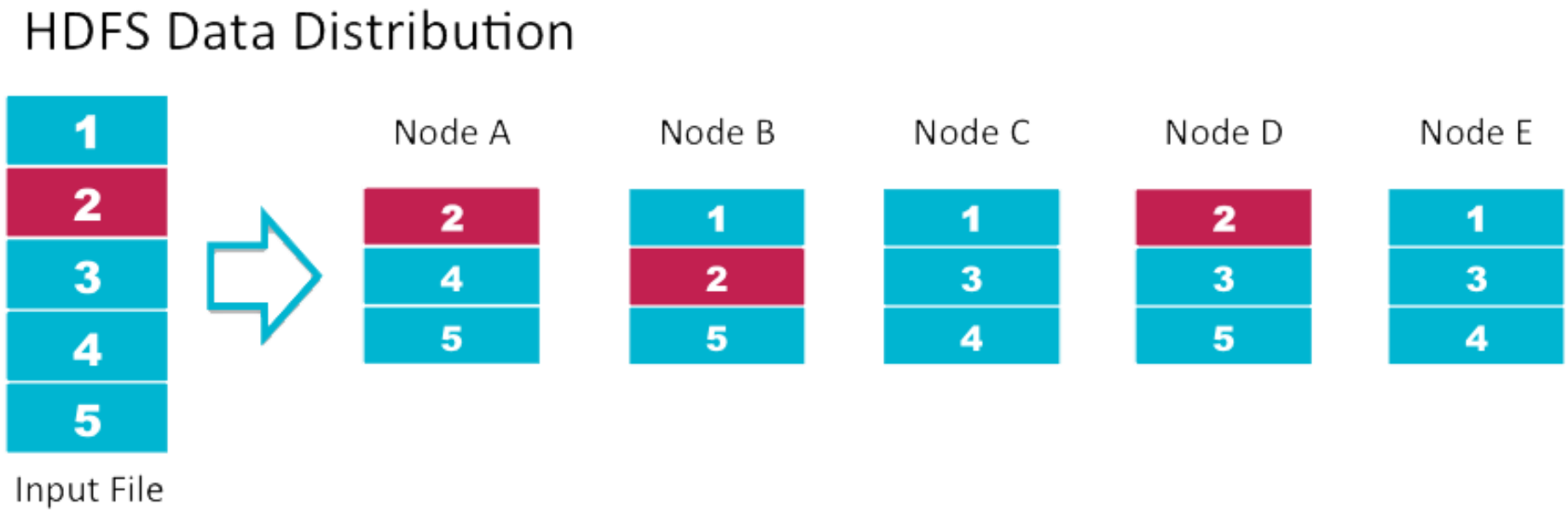
- Why not just use the PCAP files?
  - Reading (compressed) PCAP data is just too slow
  - Analytical engines cannot read PCAP files



Stel je vraag over ENTRADA!

HDFS

- Distributed file system for storing large volumes of data
- High availability through replication of data blocks
- Scalable to hundreds of PB's and thousands of servers



Cluster Design

nano sized

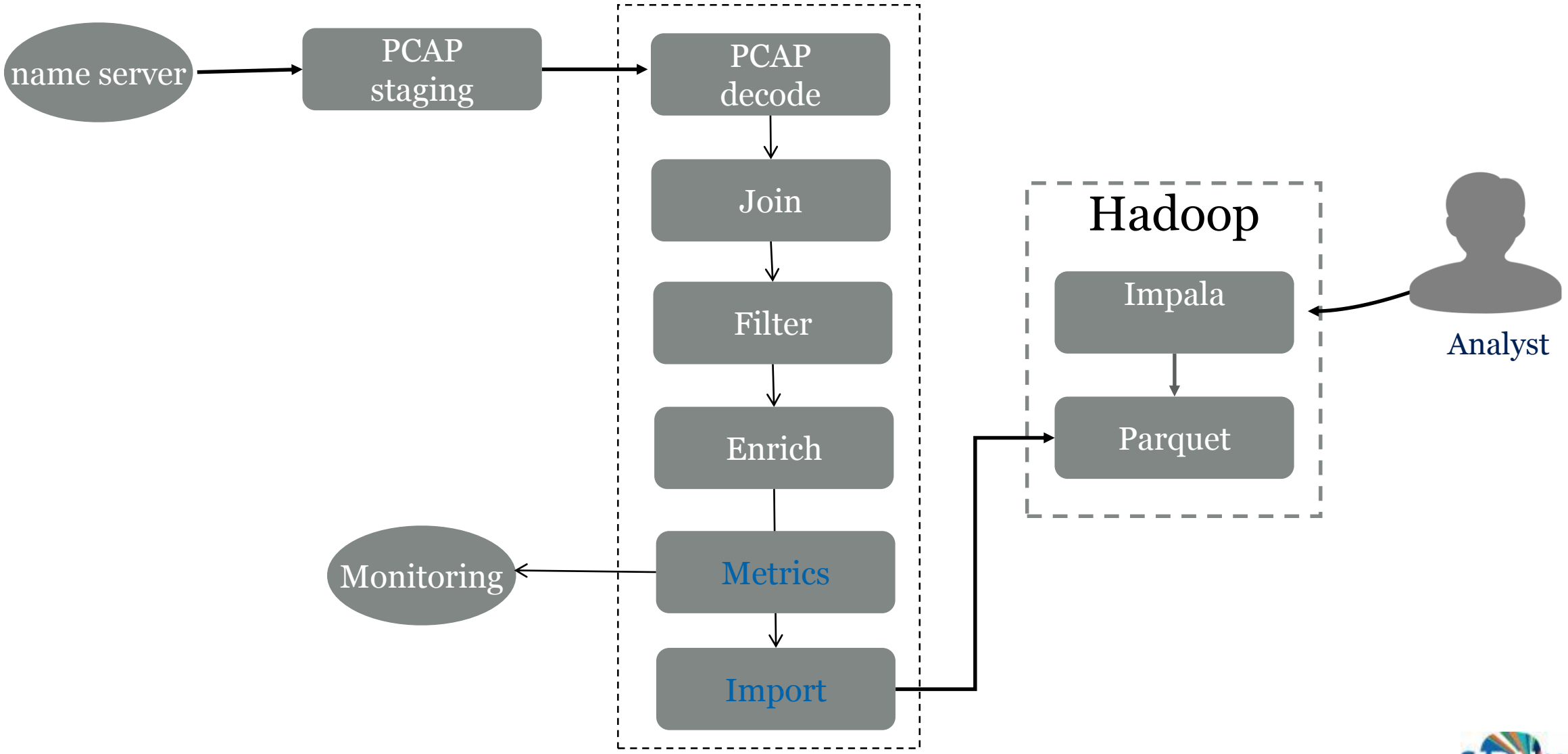
location I
management node

location II
data nodes

location III
data nodes

2Gb/s network

Workflow



Query data available for analysis within 10 minutes

Security Use Cases at SIDN

Security Use Cases

- DGA detection
- nDEWS
- Botnet infection
- Phishes on subdomains
- Data exchange Fraudehelpdesk

- Wat zijn jullie use cases?

Security Use Cases

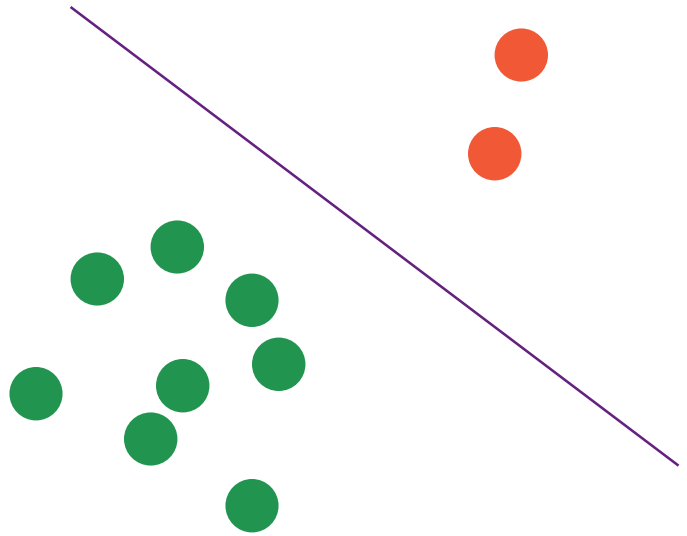
- DGA detection
  - based on lexical features (using tool by SANS ISC)
  - and NX queries
  - e.g. vufrx4xjje1y5spwle2kp8g4qn5uag2nq636apww9mhyk03k4z.nl

Security Use Cases

- DGA detection
  - based on lexical features (using tool by SANS ISC)
  - and NX queries
  - e.g. vufrx4xjje1y5spwle2kp8g4qn5uag2nq636apww9mhyko3k4z.nl

Security Use Cases

- nDEWS: Detection of new malicious domain names
  - checks for every new domain name:
    - number of queries, unique sources, unique ASes, unique countries
    - uses k-means (k=2) clustering to split domains



Security Use Cases

- Detect botnet infections
  - Cutwail botnet used for sending SPAM
  - Bots use their own, *home-brew*, recursive resolver
    - limited port range
    - limited DNS query ID range
    - many MX queries
    - many NX queries

Security Use Cases

- Detect phishes on subomains
  - e.g. *paypal.com.login*.example.com
  - filter ENTRADA for keywords in subdomain labels

Security Use Cases

- Detect phishes on subomains
  - e.g. paypal.com.login.example.com
  - filter ENTRADA for keywords in subdomain labels

- Verify user submissions automatically
  - e.g. from PhishTank or Fraudehelpdesk
  - features: domain name age, registrar, *DNS query peak*

Other Use Cases

- Stats: stats.sidnlabs.nl
- Research, e.g.:
  - How do recursive resolvers select authoritative name servers? (tech report)
  - How to understand and predict changes of anycast catchments? (tech report)
- Adhoc queries, e.g.:
  - Do we see strange queries for a domain name?
  - What else is a resolver querying?
- Policy changes, e.g.:
  - What happens if we change zone file updates from 2h to 1h?
  - What would happen if QNAME minimization gets widely adopted?

Use cases in other organizations

- DNS Magnitude: Measure the popularity of domain names (nic.at) https://ccnso.icann.org/meetings/copenhagen58/presentation-dns-magnitude-13mar17-en.pdf
- Anomaly Detection
- …

afnic

dnsbelgium

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

SWITCH

cz.nic

cira

nic.at

.dk hostmaster

SDN LABS

Use cases in other organizations

- DNS Magnitude: Measure the popularity of domain names (nic.at) https://ccnso.icann.org/meetings/copenhagen58/presentation-dns-magnitude-13mar17-en.pdf
- Anomaly Detection
- …
- *Your use case here!*

afnic

dnsbelgium

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

SWITCH

cz.nic

cira

nic.at

.dk hostmaster

SDN LABS

Resources

- ENTRADA
  - Documentation: http://entrada.sidnlabs.nl/
  - Software: https://github.com/SIDN/ENTRADA/
- Malicious Domain Names
  - General background: https://www.sidnlabs.nl/downloads/publications/Muller_Master_Thesis_EIT_SP.pdf (chapters 2 and 3)
  - nDEWS: https://www.sidn.nl/a/veilig-internet/realtime-kwaadaardige-domeinregistraties-herkennen
  - Cutwail: https://www.sidnlabs.nl/a/weblog/entrada-koppeling-met-abusehub

Poll: Is er interesse in een praktische vervolgworkshop?

Volg ons


SIDN.nl


@SIDN


SIDN

Dankjewel voor je aandacht!