



Deleting Your Domain?

Preventing Data Leaks at TLD Scale



Who Are We?



Maarten Wullink
Research engineer
SIDN Labs



Moritz Müller
Research engineer
SIDN Labs

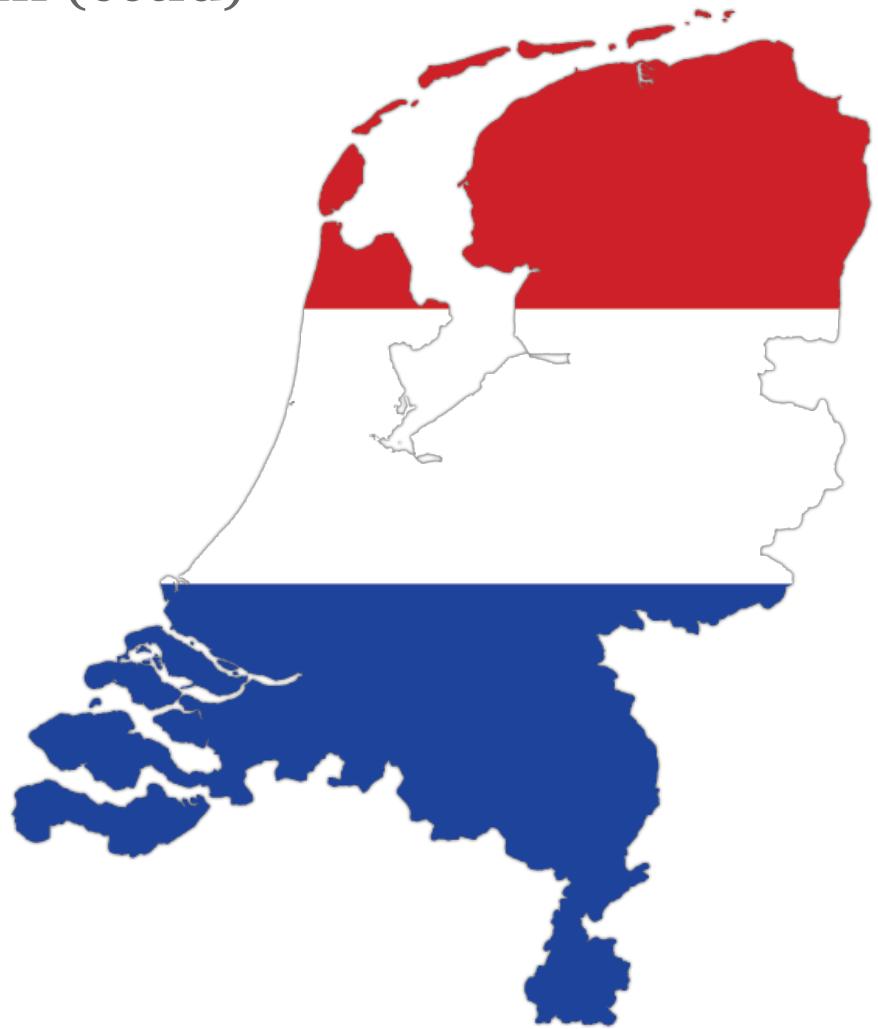
What to expect?

- Introduction
- Data leaks and email
- LEMMINGS System
- DNS and email
- System functionality
- Results

About SIDN

Registry for the **.nl** country code top-level domain (ccTLD)

- **6.3** million .nl domains
- **61%** uses DNSSEC
- Global Anycast DNS network



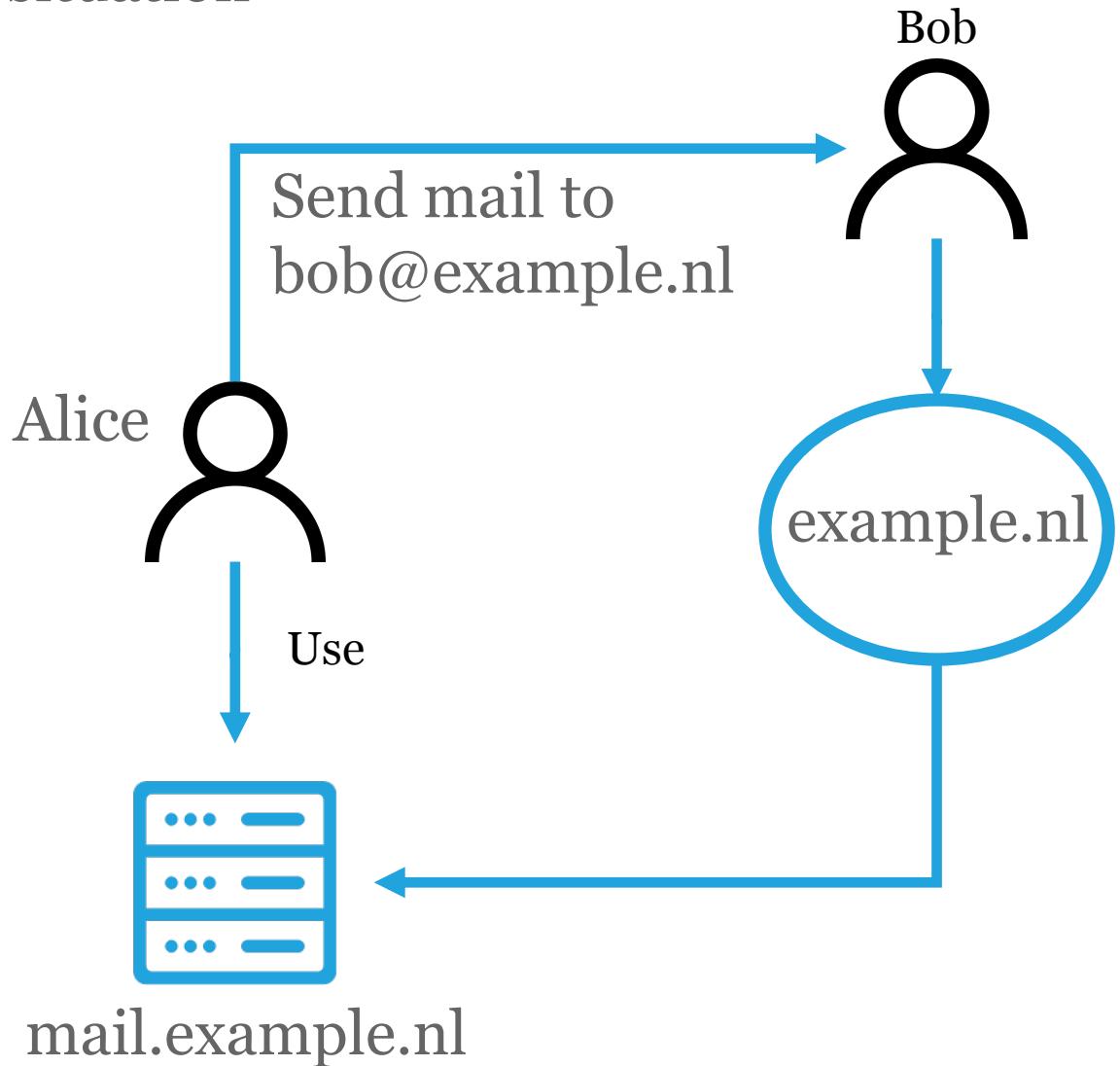
About SIDN Labs

Research arm of SIDN

- Applied technical research into the safety and stability of the Internet
- Main research themes
 - Domain name security
 - Infrastructure security
 - Emerging Internet technologies

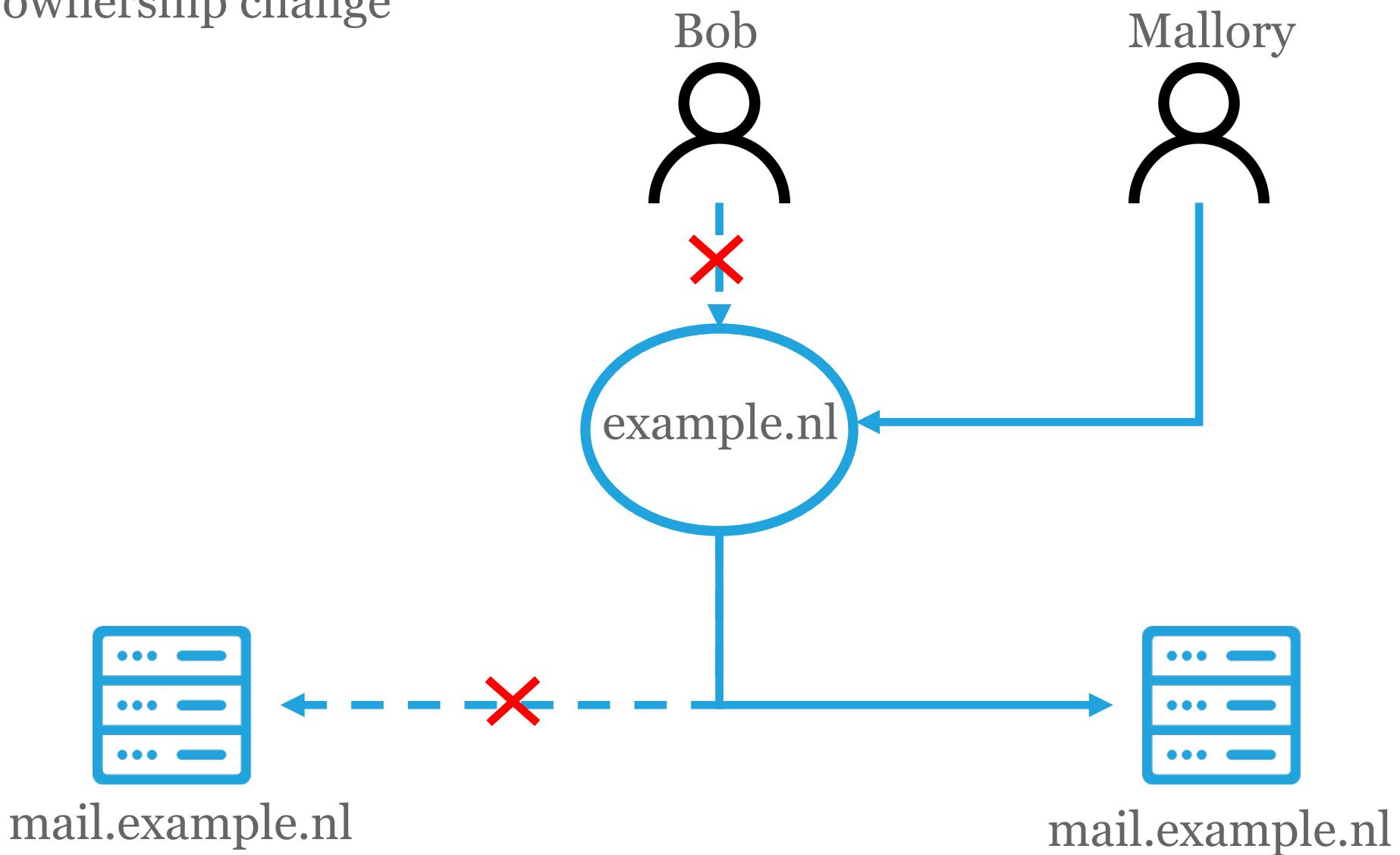
Data leaks and Email

Normal situation



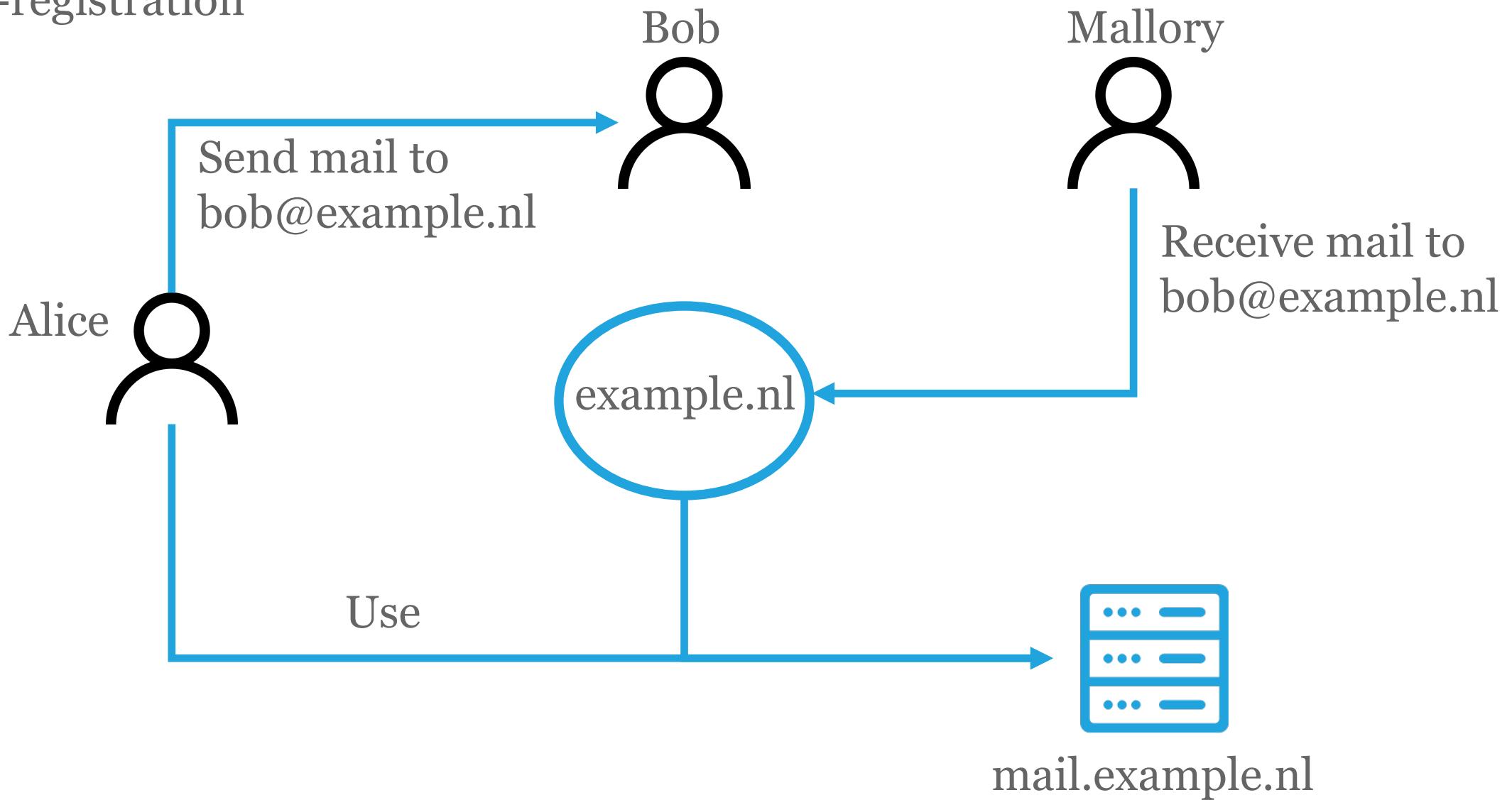
Data leaks and Email

Domain ownership change



Data leaks and Email

After re-registration



Data leak - Example

EXCLUSIVE

Major data breach at Jeugdriagg: medical records of vulnerable children leaked



By means of Daniel Verlaan

October 1, 2020 12:56 PM • Modified October 1, 2020 1:45 PM



Image for illustration.



Due to an error at Jeugdriagg, the files of children with often serious psychological problems have been leaked. Despite efforts by Minister Hugo de Jonge to better secure healthcare institutions, hardly anything seems to have changed in a year and a half.



Just in

- 08:47 Anderlech...
to go to P...
- 08:41 Greek tra...
ranking a...
- 08:19 Eloise en...
with Prid...
- 08:17 Barbie is...
director t...
dollars
- 08:11 Lost Rob...
surgery t...

Data leak - Example

articles ▾ Community ▾ Career ▾ Topics ▾ Awards ▾ Live ▾ Whitepapers ▾ More ▾ Service ▾

COMPUTABLE

To search

Home | Articles | News | Security

Police leak data via expired email domains

January 20, 2017 11:50 | Pim van der Beek | 3

TopicSecurity _

[f](#) [t](#) [in](#) [e](#)



The police have allowed a number of domain names linked to e-mail addresses to expire. Third parties can purchase those domains and gain access to emails containing information about arrests and event security. An ethical hacker has demonstrated this on behalf of BNR (Business News Radio).

That ethical hacker, Wouter Slotboom, warned the police about the security risk two years ago and is now raising the alarm because the risk still exists. Six months after his report, Slotboom bought a number of expired police domains. Information such as arrest warrants and a security plan for a large Christmas market in Dordrecht still regularly arrives on these email accounts.

LEMMINGS

DeLetEd doMain MaIl warNinG System

A system for detecting mail traffic
involving deleted domains and alerting
registrants



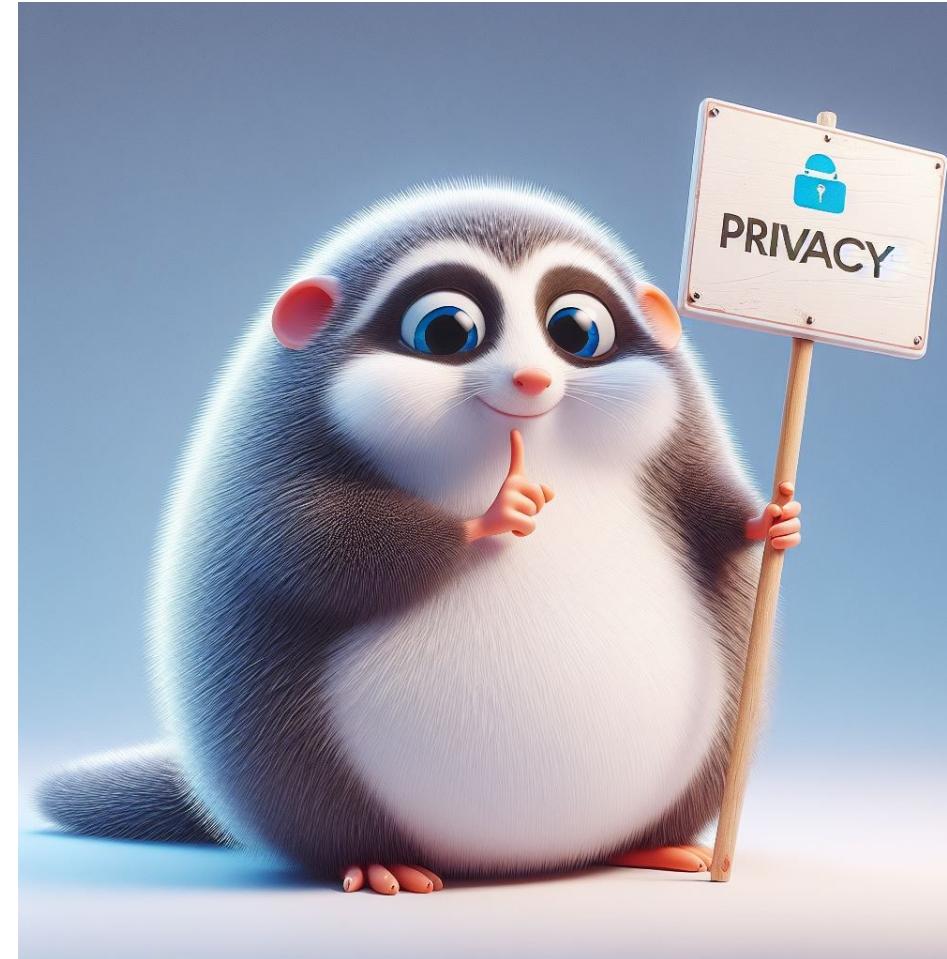
LEMMINGS

- Method:
 - Analyse DNS queries for all deleted domains
 - Combine with web crawler and domain abuse data
- Alert the former registrant, when following is true
 - Indication domain is used for email
 - Domain has not yet exited quarantine period



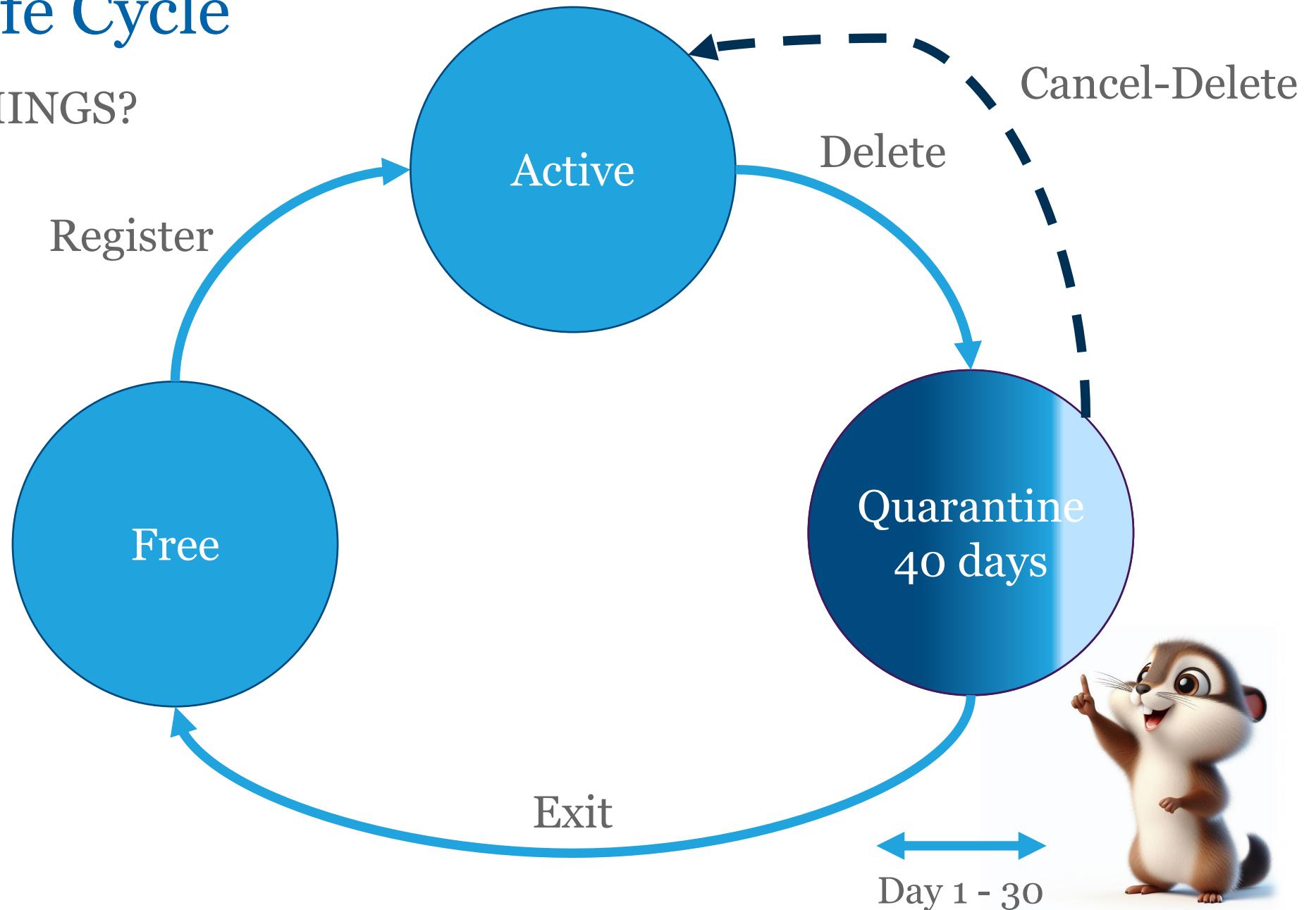
Privacy Considerations

- Not capturing or analysing actual mail content
- No trackers in mail alert to registrants
- Removing PII data after process is completed
- Published privacy policy



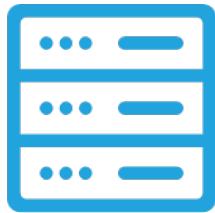
Domain Life Cycle

Where is LEMMINGS?



DNS and Email

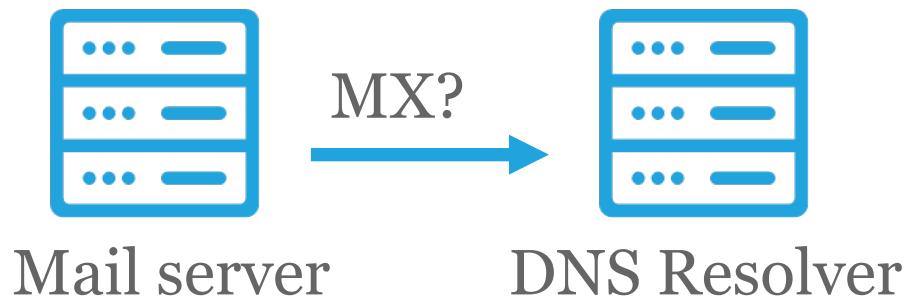
Delivering mail for bob@example.nl



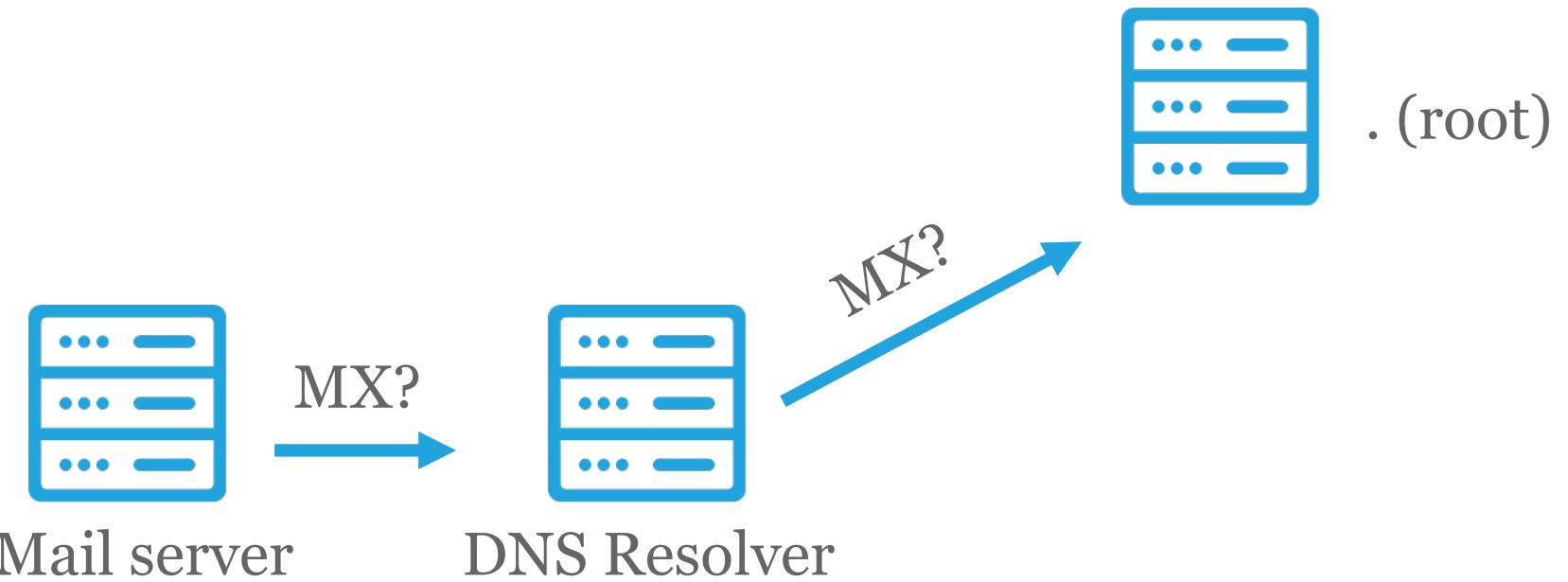
Mail server



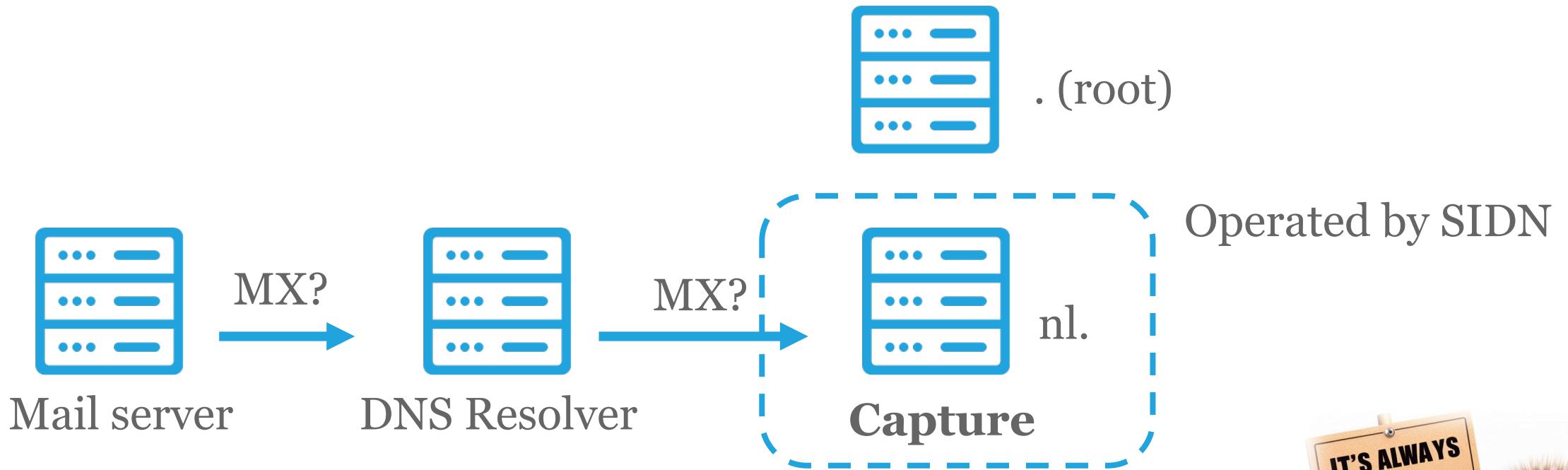
DNS and Email



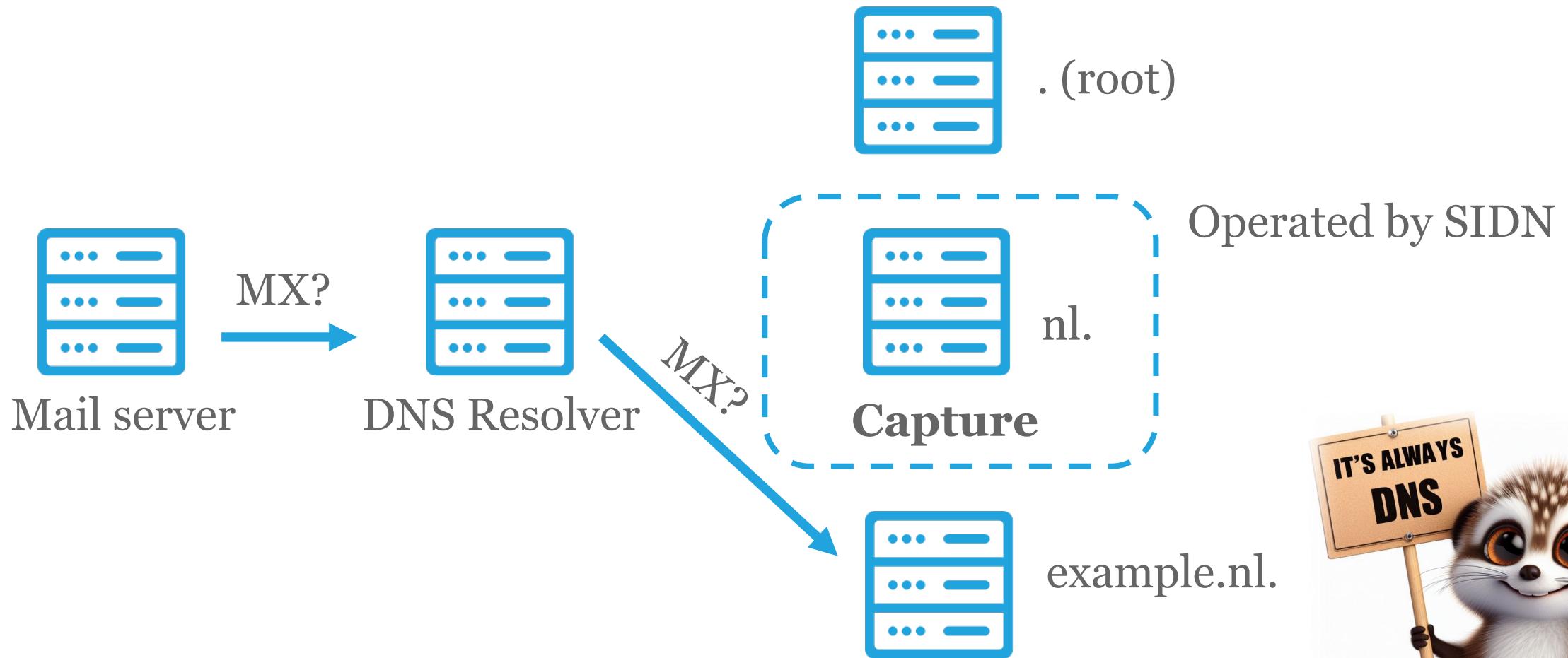
DNS and Email



DNS and Email



DNS and Email



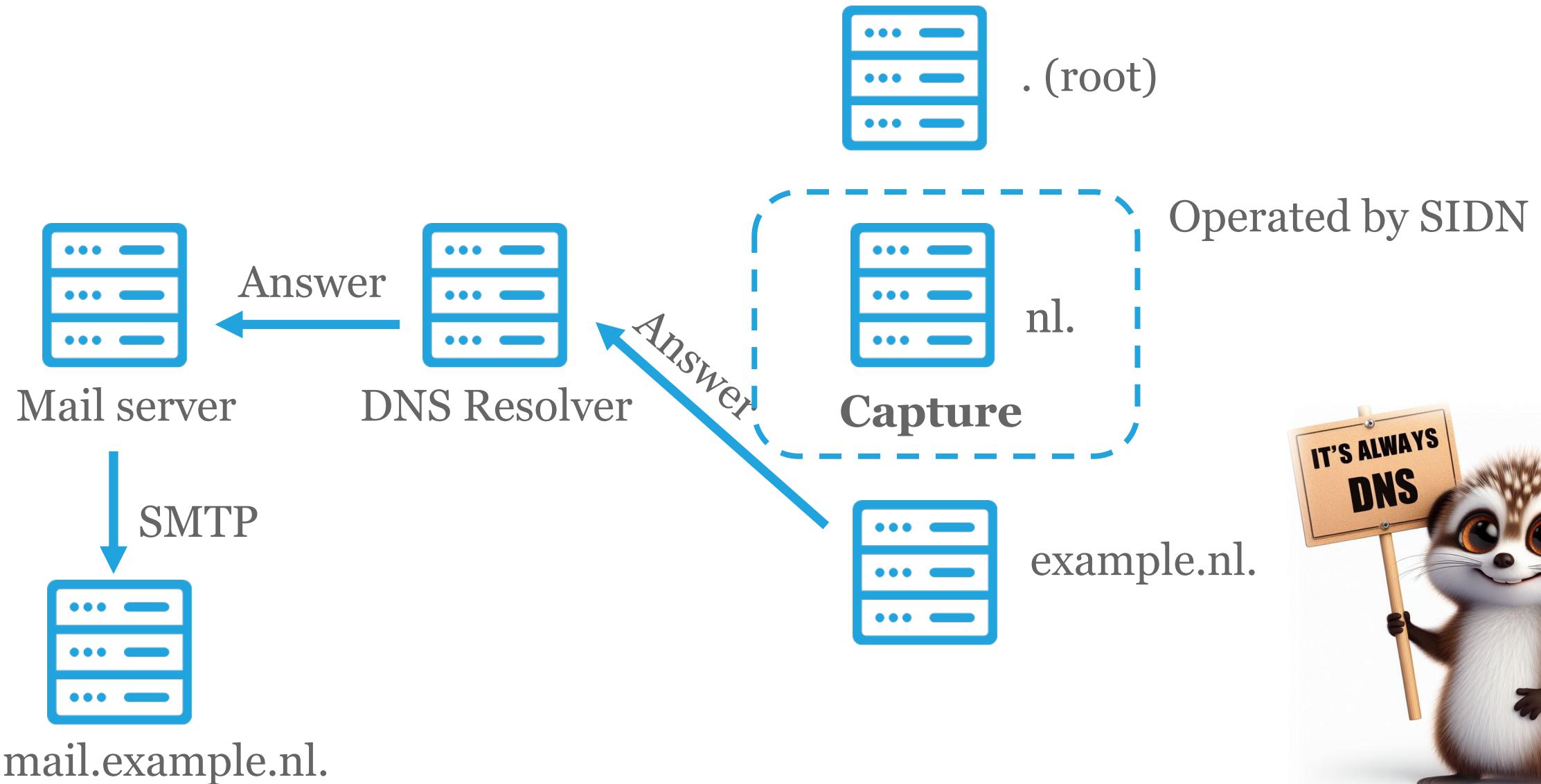
Operated by SIDN

nl.

example.nl.
Capture



DNS and Email



Challenges

- Analysing large volume of DNS data
- Filtering noise (marketing, spam mail)
- Explaining the security risk to registrants



Challenges

- Try not to make the alert look like a spam message
- Registrant contact email address is not reachable
 - Privacy proxy
 - In-zone email address



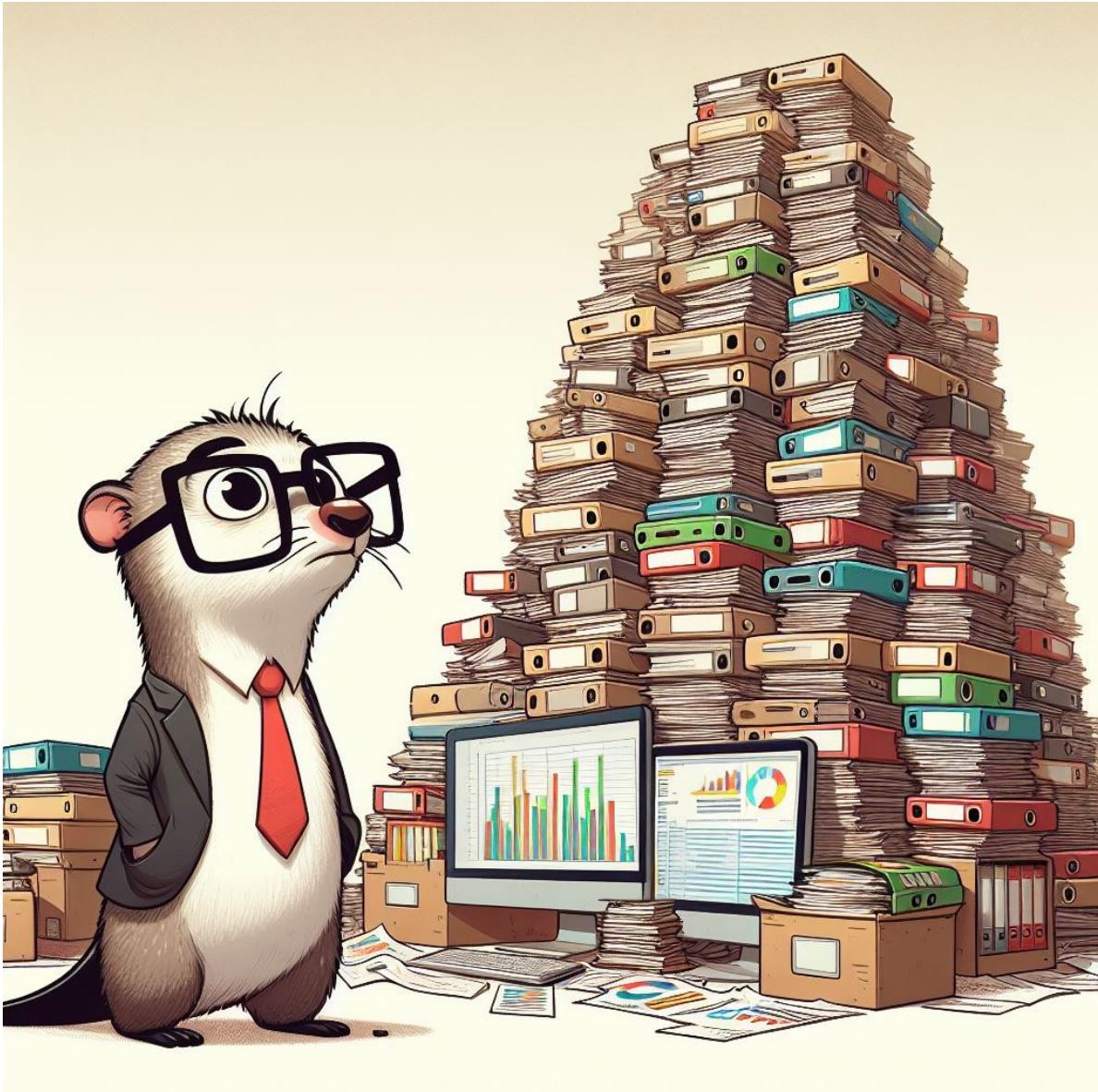
Data Sources

- DNS queries for 6.3 million .nl domains
 - ~4 billion daily
 - ~180 million email related



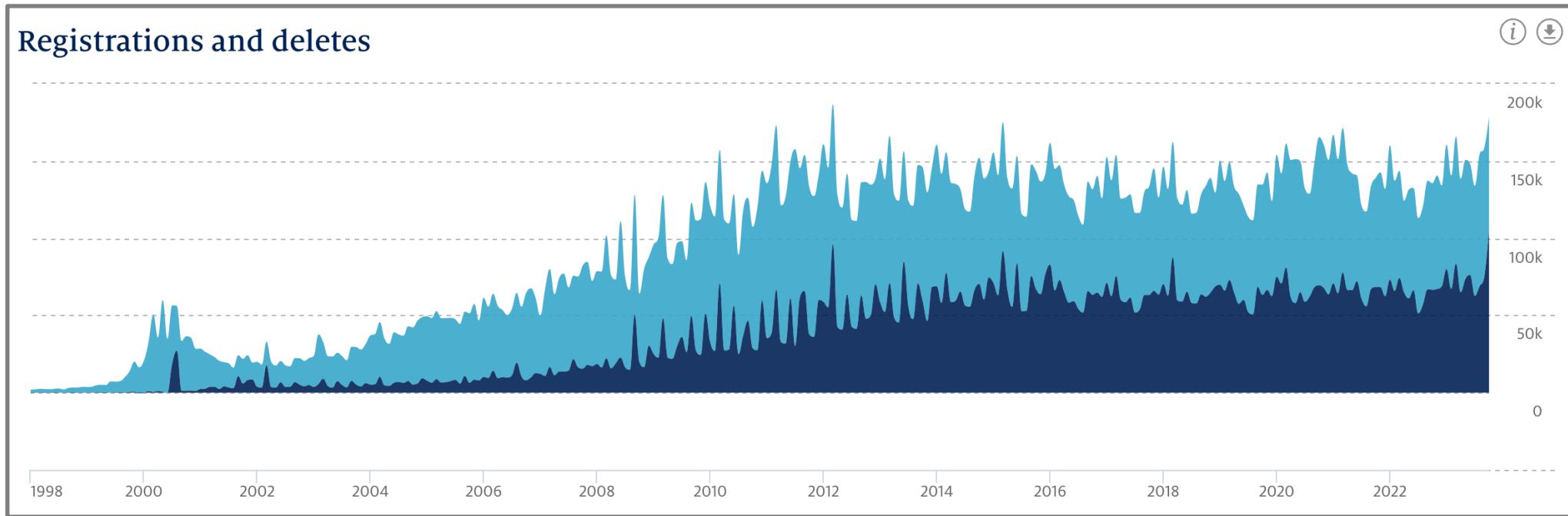
Data Sources

- Web crawler data
 - 6.3 million .nl domains
 - Attributes
 - Web content-type
 - Detected email addresses
- Abuse feeds (Spamhaus, APWG)
- Sinkhole (botnet C&C domains)



Data Sources

Domain registration database

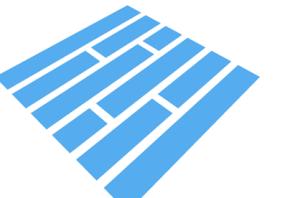


Registrations (light blue) and deletes (dark blue)

<https://stats.sidnlabs.nl>



Data Platform



Parquet



<https://entrada.sidnlabs.nl>

528 CPU cores
1408G memory
500TB storage



Workflow



Filters

- Use of multiple filters for removing noise
 - Spam, marketing related
- Based on attributes such as
 - IP address
 - ASN
 - Web content-type



Filters

Filter types

- Static
 - Manually maintained
- Dynamic
 - Automatically generated



Static Filters

Static and manually maintained lists

- **AS Number:** e.g. mail marketing company networks
- **Country:** High volume SPAM countries
- **IP Address:** e.g. other researchers



Dynamic Filters

Automatically generated each day

- **High Nxdomain:** DNS resolvers showing a high ratio of NXDOMAIN
- **Newly Seen:** IP addresses of resolvers that have not been seen before
- **Suspicious**
 - Open resolvers
 - Sinkhole clients
 - Abuse feeds (Spamhaus, APWG)



Alert Rules

Distinct risk categories

Based on 10-day average of daily DNS queries (after filtering)

- Low: ≤ 5
- Medium: $> 5 \text{ en } \leq 10$
- High > 10



Alert Rules

Special conditions

- Is keyword or business activity match?
 - then risk is high
- Is email address found by web crawler?
 - then risk at least medium



Alert Message

- Designed in collaboration with registrars and registrants
- Sent on day 30 of 40 day quarantine period
- Registrant has 10 days to take action



Alert Message

- Designed to explain the risk and suggest actions, e.g.
 - Informing contacts
 - Restoring the domain
- Multiple alert modes
 - To registrant
 - To registrar, who then forwards the alert
 - Registrar opt-out, no alerts are sent



Alert Message - Example

Belangrijke informatie over je opgeheven domeinnaam



Belangrijke informatie over je opgeheven domeinnaam **mariethereseheijnen.nl**

Er is mogelijk nog mailverkeer naar de domeinnaam

An English version of this e-mail can be found at www.sidn.nl

Dit is een bericht van SIDN, wij beheren het .nl-domein en ook de domeinnaam mariethereseheijnen.nl. Je hebt deze domeinnaam opgezegd op 2023-05-06. Met het opheffen van mariethereseheijnen.nl vervallen ook alle daaraan gekoppelde e-mailadressen. We sturen je dit bericht, omdat er waarschijnlijk nog gemaild wordt naar een of meerdere e-mailadressen die gekoppeld waren aan de opgeheven domeinnaam. Hier schuilt een risico in. We vertellen je er graag meer over.

Anonymisation

PII information is deleted after a domain exits the 40-day quarantine period

- Registrant
 - Identifier
 - Name
 - Email address



2 Pilots

Do registrants understand the warning?



2 Pilots

Registrars worried about an increase in support calls



Alerts sent

After running LEMMINGS for 10-month period

- **587.778** deleted domains analysed
- Filtering removed 75% of mail related DNS queries
 - The average daily number of queries for a domain dropped from **4.7 to 1.2**
- **54.410** alerts have been sent to registrants



Alerts sent

54.410 alerts have been sent (**9.2%** of deleted domains)

| Risk category | Alerts | Percentage |
|---------------|--------|------------|
| Low | 44.701 | 82.15% |
| Medium | 8.080 | 14.85% |
| High | 4.639 | 8.53% |



Measuring the Effect

- Not possible to directly measure the number of prevented data leaks
- Using a proxy:
 - Cancel-delete request as a proxy for prevented data leaks
 - Registrant survey



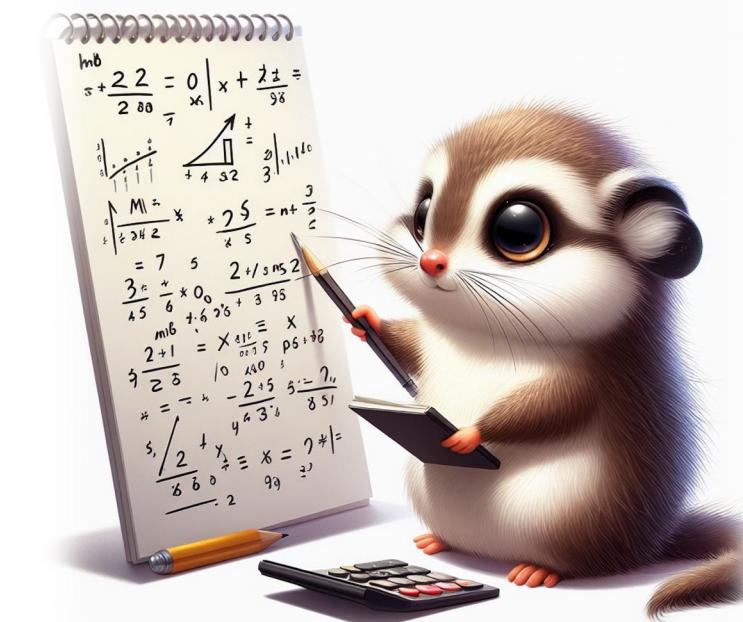
Cancel-delete Proxy

- Cancel-delete as proxy for prevented data leaks
- Cancel-delete baseline for the 12-month period before using LEMMINGS
 - **0.13%** of **627.285** deleted domains received cancel-delete

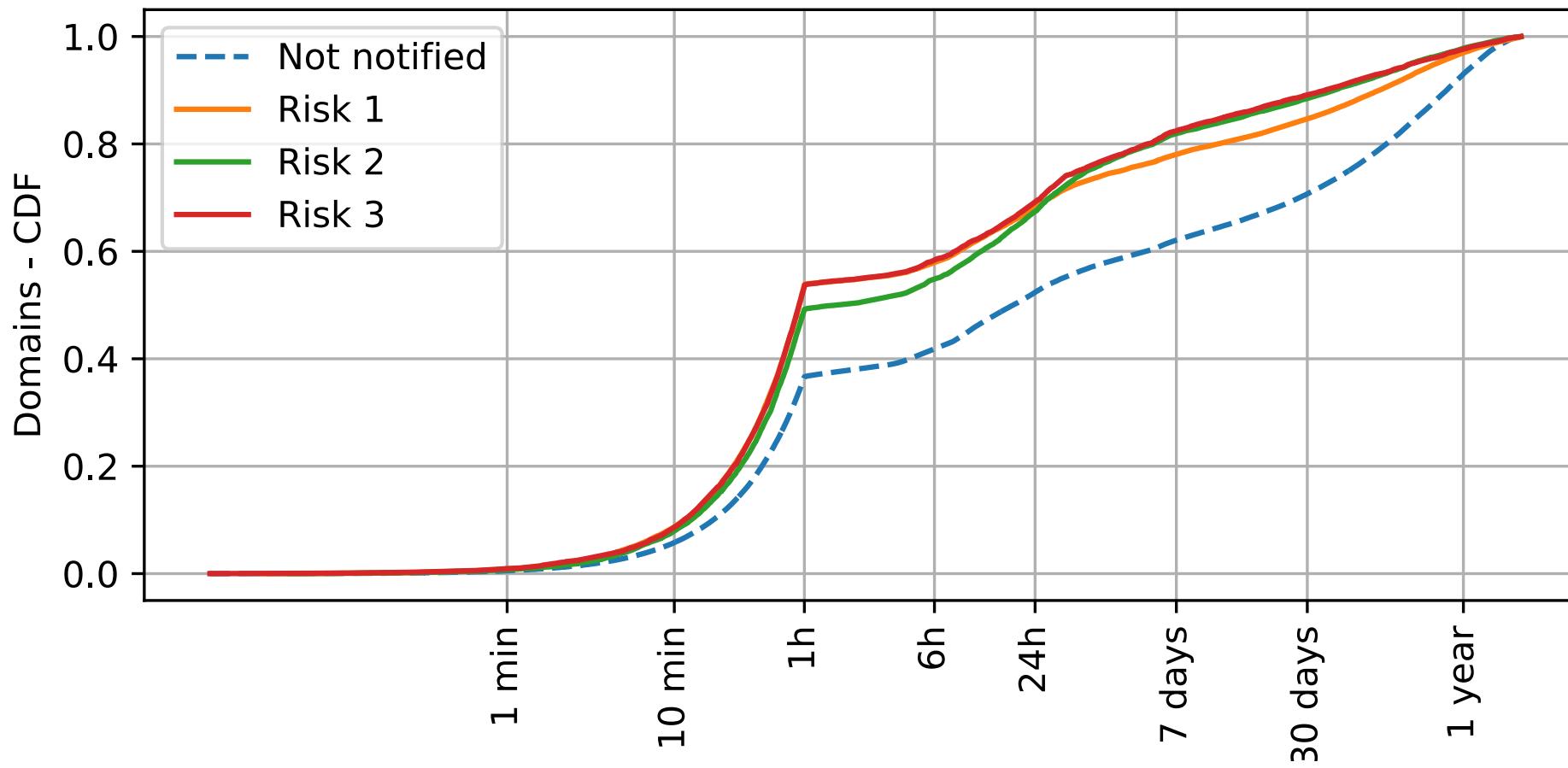
Cancel-delete Proxy

LEMMINGS cancel-delete ratio vs. baseline (**0.13%**)

| Risk category | Cancel-delete | Percentage | Increase |
|---------------|---------------|------------|----------|
| Low | 237 | 0.53% | 3.8x |
| Medium | 38 | 0.84% | 6.0x |
| High | 50 | 1.08% | 7.7x |

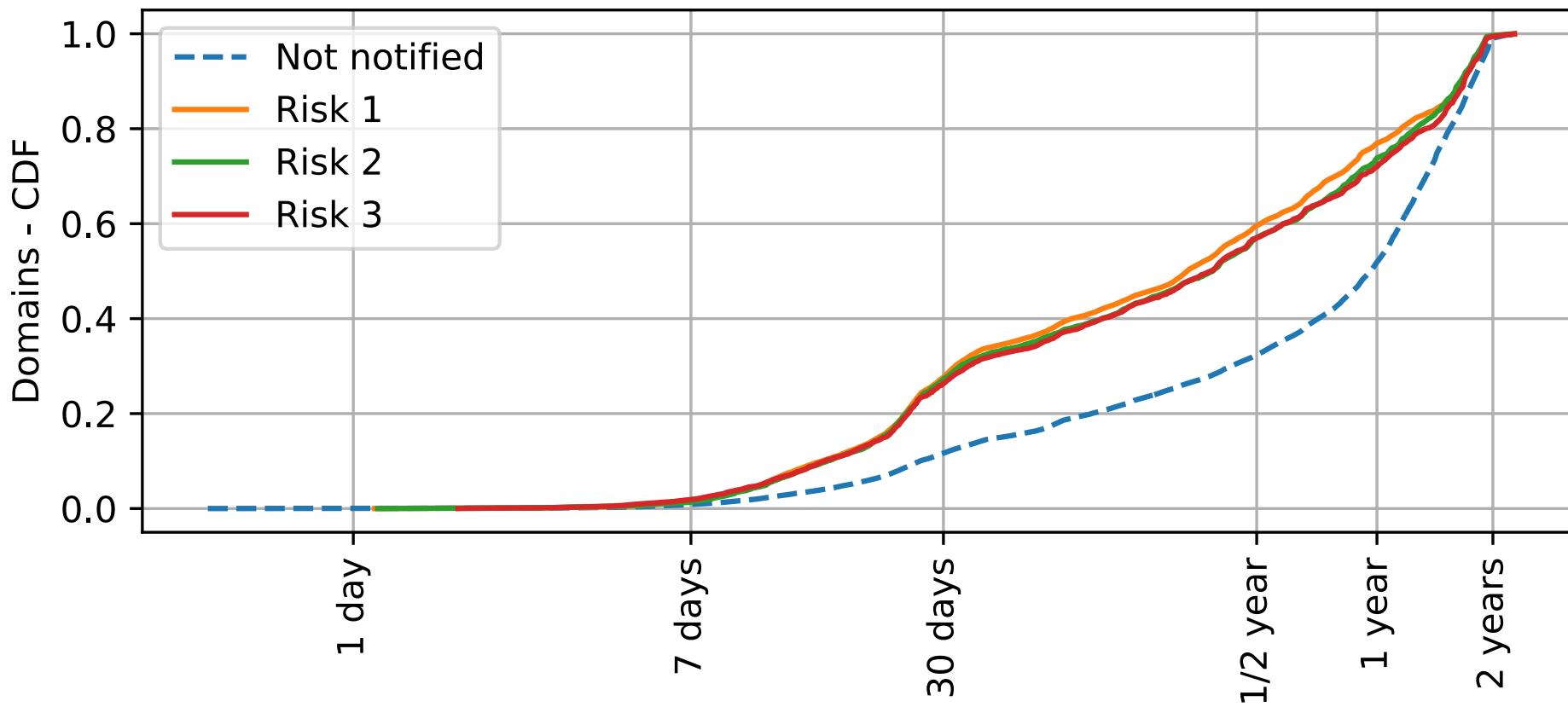


Do we alert the correct domains?



Domains receiving an alert are re-registered more quickly

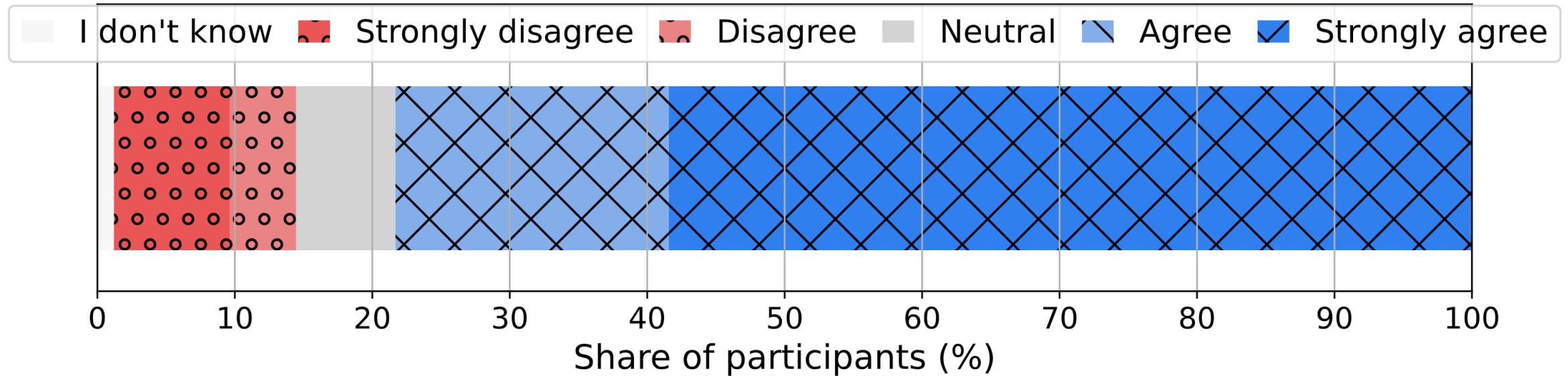
Do we alert the correct domains?



Alerted and re-registered domains have a new mail server
more quickly

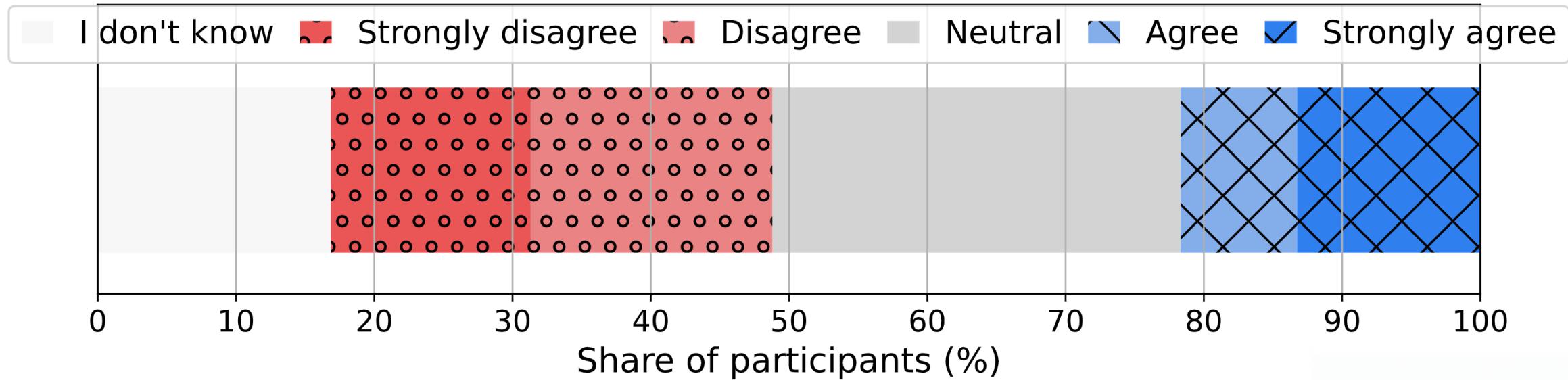
Registrant Survey

"The mail was useful"



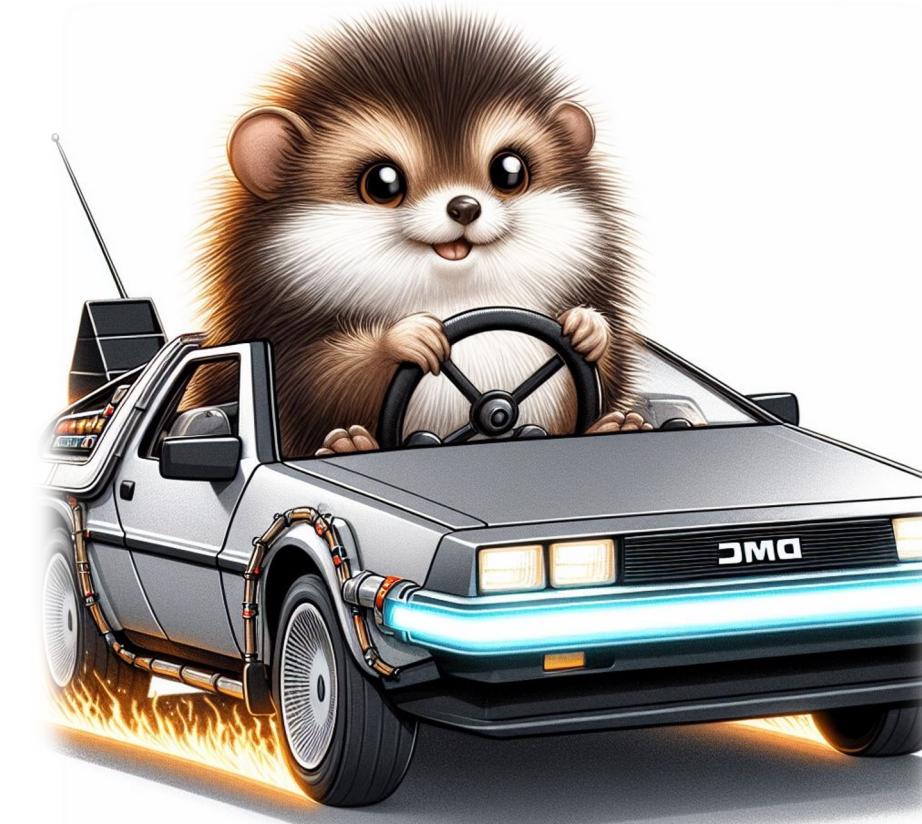
Registrant Survey

"The mail helped to prevent problems like the leakage of information"



Future Work

- Analyse the impact of DNS Qname Minimisation
- Improve DNS filters



Black Hat Sound Bytes

Key takeaways

- Data leaks due to deleted domains are a real thing
- Difficult to directly measure the effect of LEMMINGS
- Explaining the problem to registrants is challenging
 - Low number of registrant and registrar questions
 - Positive response from Dutch Internet community



.nl SIDN.nl

@SIDN

in SIDN

Questions?

www.sidnlabs.nl | stats.sidnlabs.nl

