# Using machine learning to boost internet and DNS security

Thymen Wabeke | Ofcom

8 December 2021

# SIDN: operator of the .nl ccTLD

Registration of domain names

6.2M .nl-domains


Publish domain names via DNS

2.5B DNS queries/day

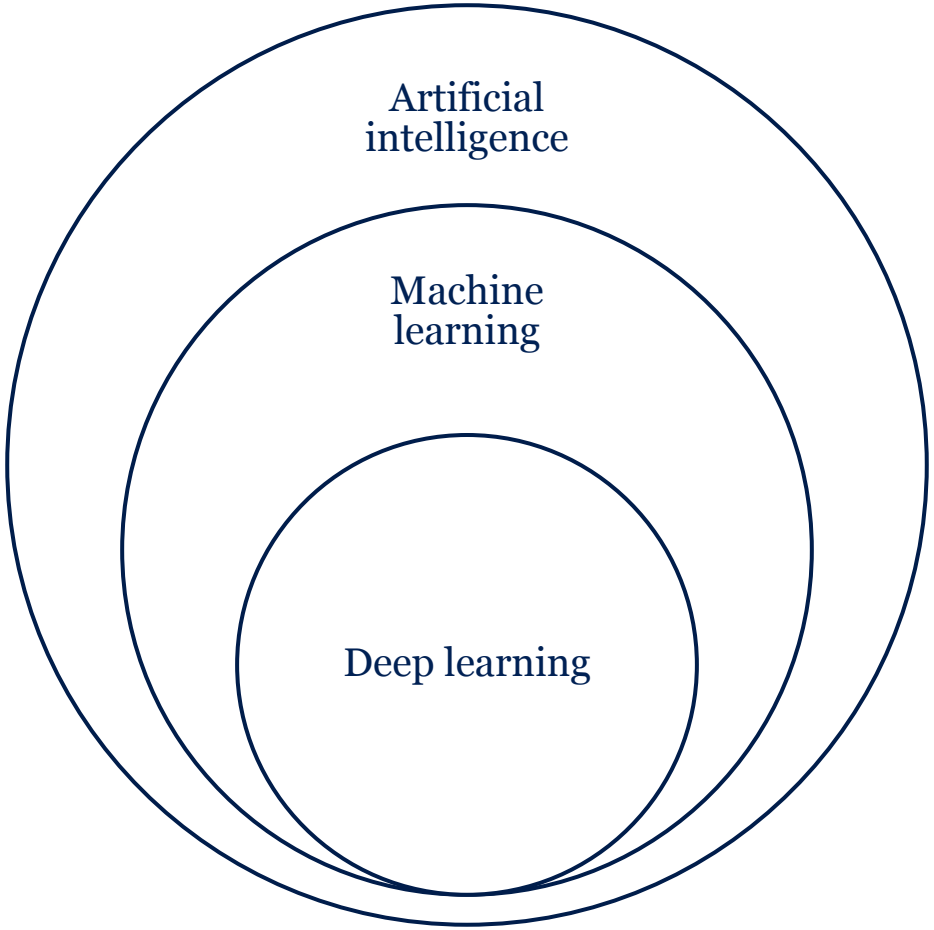
# SIDN Labs: research team

- Goal: increase the trustworthiness (security, stability, resilience, and transparency) of our society's internet infrastructure, for .nl and the Netherlands in particular

- Strategies:
  - Applied research (measurements, design, prototyping, evaluation)
  - Make results publicly available and useful for various target groups
  - Work with universities, infrastructure operators, and other labs

- Three research areas: network security, **domain name security**, trusted future internet infrastructures

# Machine learning in perspective



# Research agenda

- Apply ML to increase security of the Internet and DNS

- Approach: explore and integrate promising algorithms, papers and tools
  - Innovating *with* ML, not innovation *of* ML

- Target group: DNS actors (registries, registrars and DNS operators)

# Research topics

RQ1: How can we get even better at proactive abuse detection?


RQ2: How can we train shared abuse models without exchanging data?

RQ3: How can we use ML to improve our anycast infrastructure monitoring and management?

# Applying ML in a responsible way

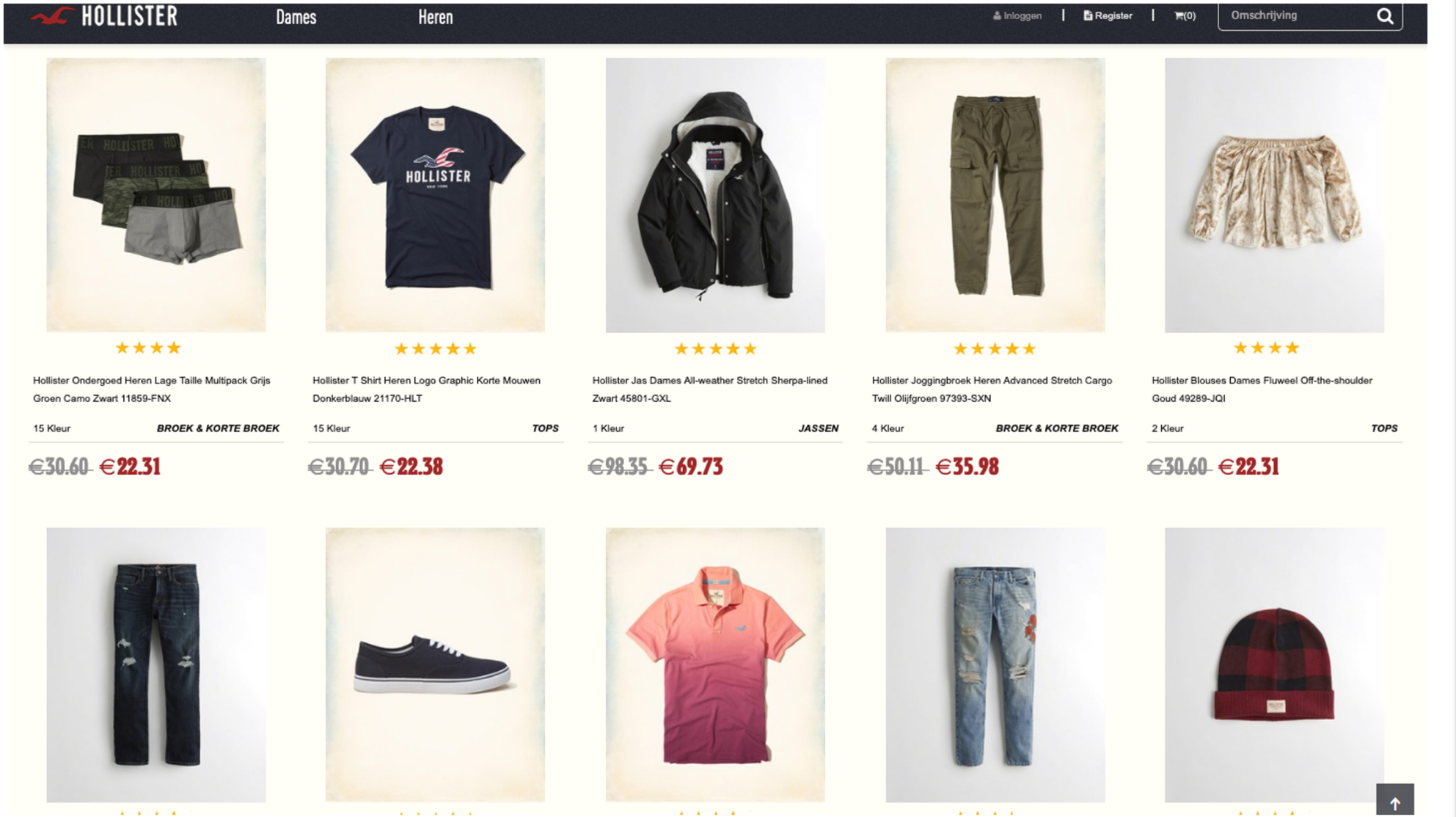
- Human-in-the-loop
- Simple and interpretable models
- Collaborate and publish
- Monitor performance

# Remainder of presentation


FaDe


LogoMotive

# nederlandwebshop.nl



# SIDN's interest

- Consumer losses
- Trust in Internet may decrease

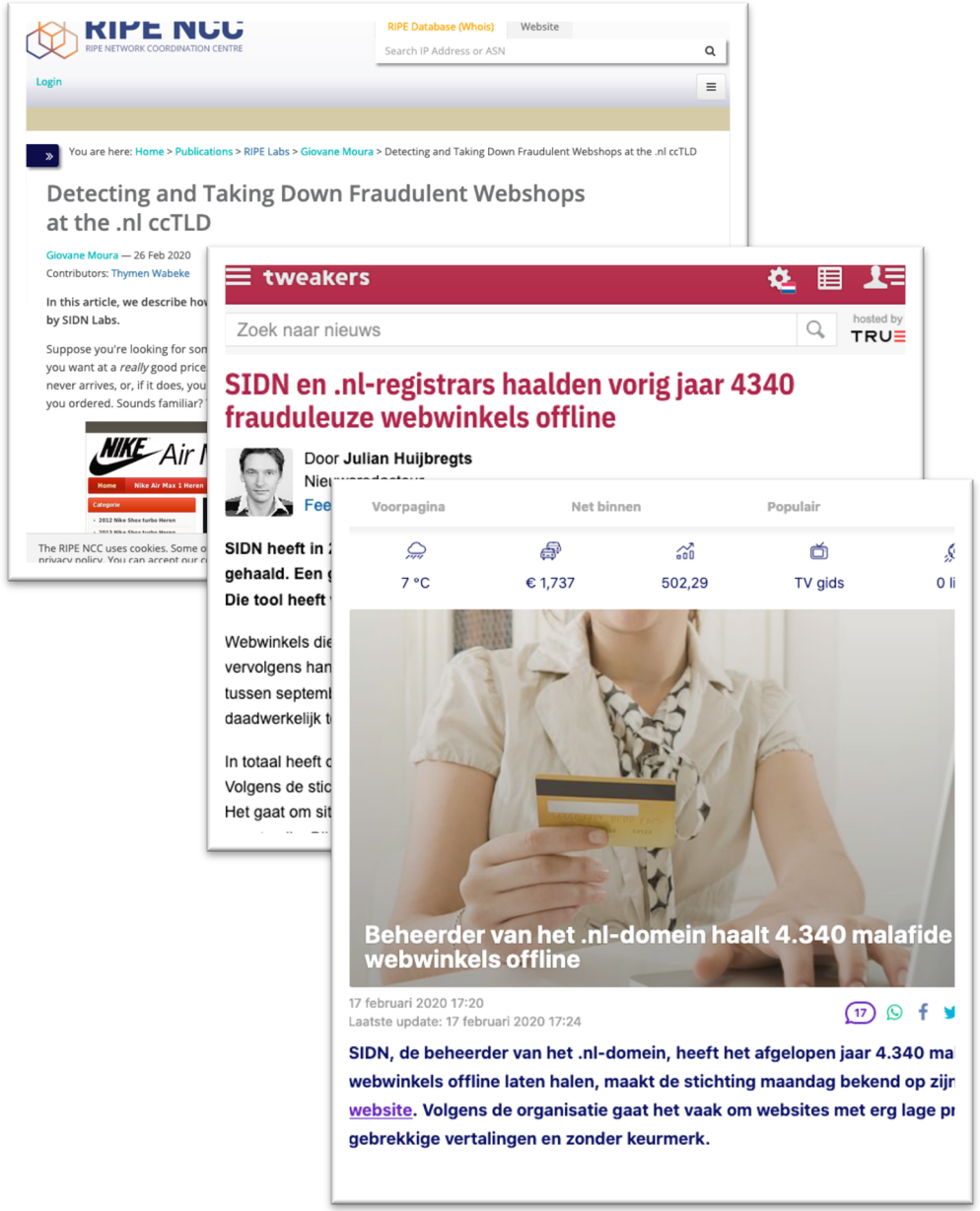
**Perfect vantage point:**

- List of *all* `.nl`-domains
- Passive and active measurements

# Main results

- Detected thousands since 2016
- Protected users from being scammed

- PAM2020 paper:
  - BrandCounter (2018 Q1-2)
  - FaDe (2019 Q1)




Published at PAM2020: https://doi.org/10.1007/978-3-030-44081-7_10
Video at RIPE80: https://ripe80.ripe.net/archives/video/322/

SIDN LABS

- Support Vector Machine
- Optimized using grid search

Dataset

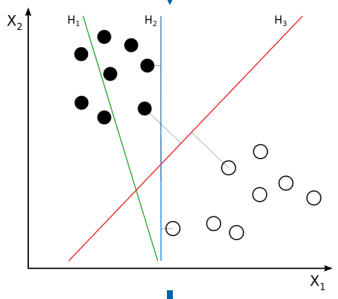
- 231 counterfeit
- 229 legitimate

Features

- 6 registration
- 3 infrastructure

Training samples

Train model




Testing samples

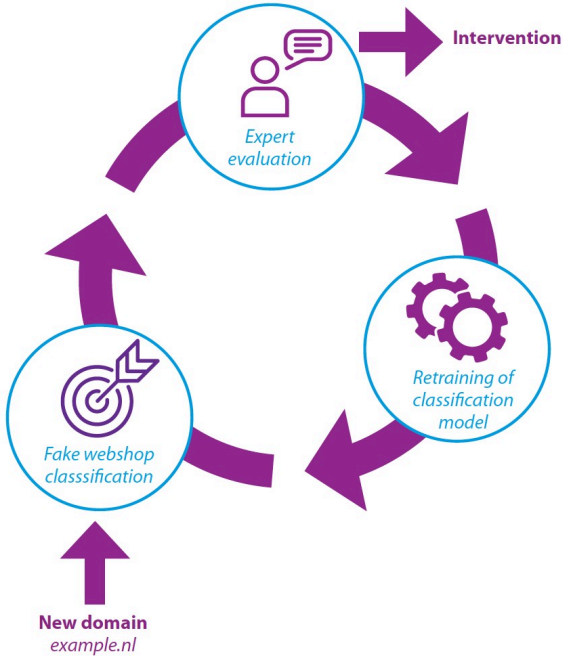
Apply model

| Samples | Precision | Recall |
|---|---|---|
| Train (cross-validation) | 0.98 | 0.97 |
| Test | 1.0 | 1.0 |

SIDN LABS

# Lessons learned

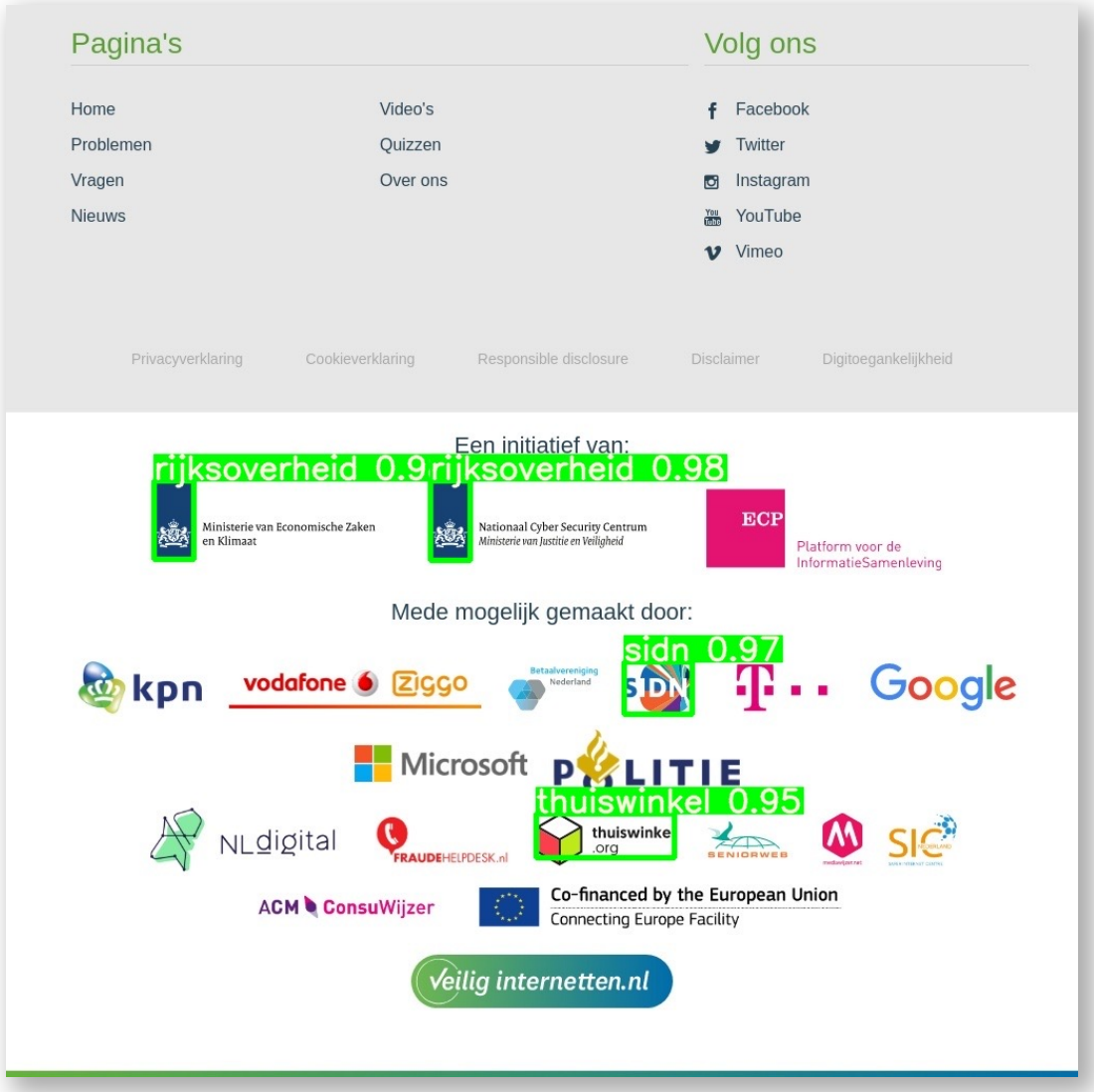
- Registrar and ICS collaboration was key
- Detectors are simple yet effective
  - Registries have perfect vantage point
  - Suggests little pressure
- It's an ever-going whack-a-mole game
  - Monitor features and evaluate model regularly
  - Fewer takedowns = fewer scams?

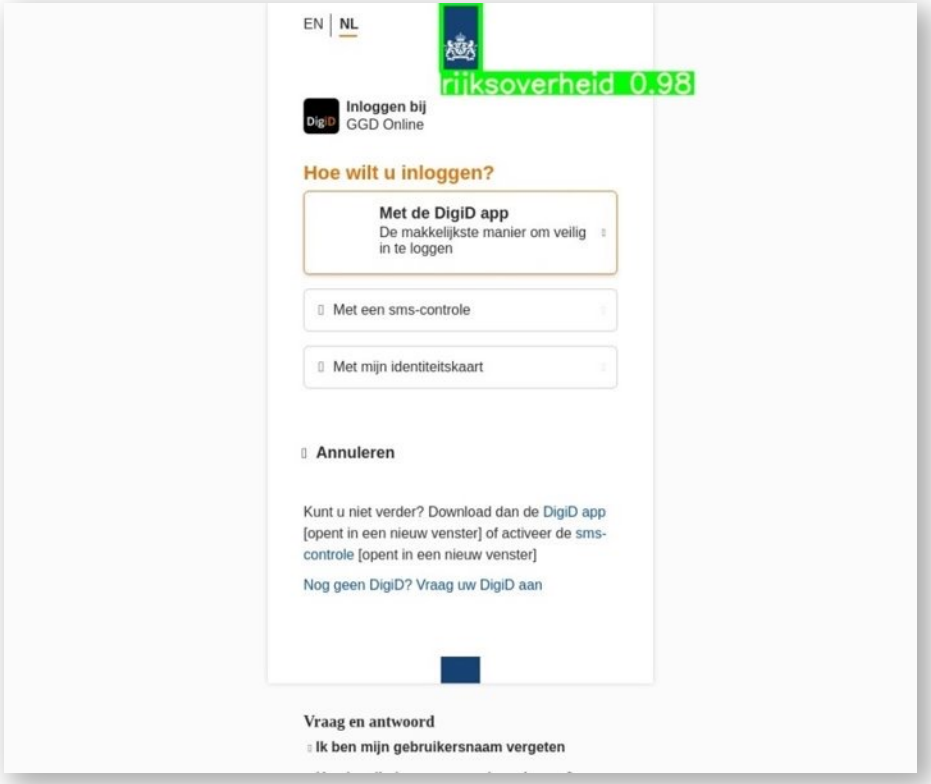



| Year | Taken down |
|---|---|
| 2018 | ~12,000 |
| 2019 | 4,340 |
| 2020 | 481 |

*Number of counterfeit webshops taken down*

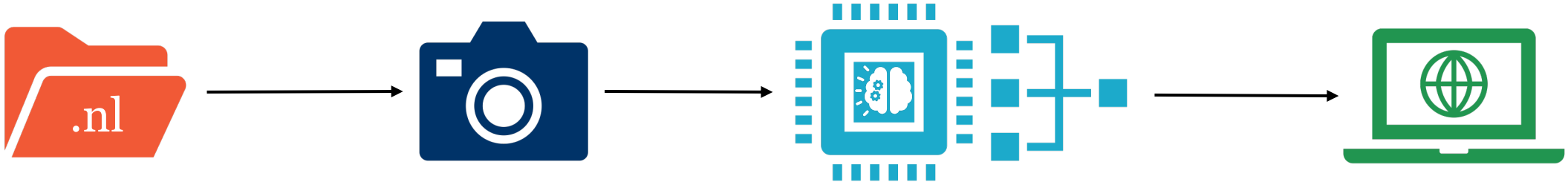
# LogoMotive: finding malicious .nl-domains with logo detection




SIDN LABS

# How does LogoMotive work?



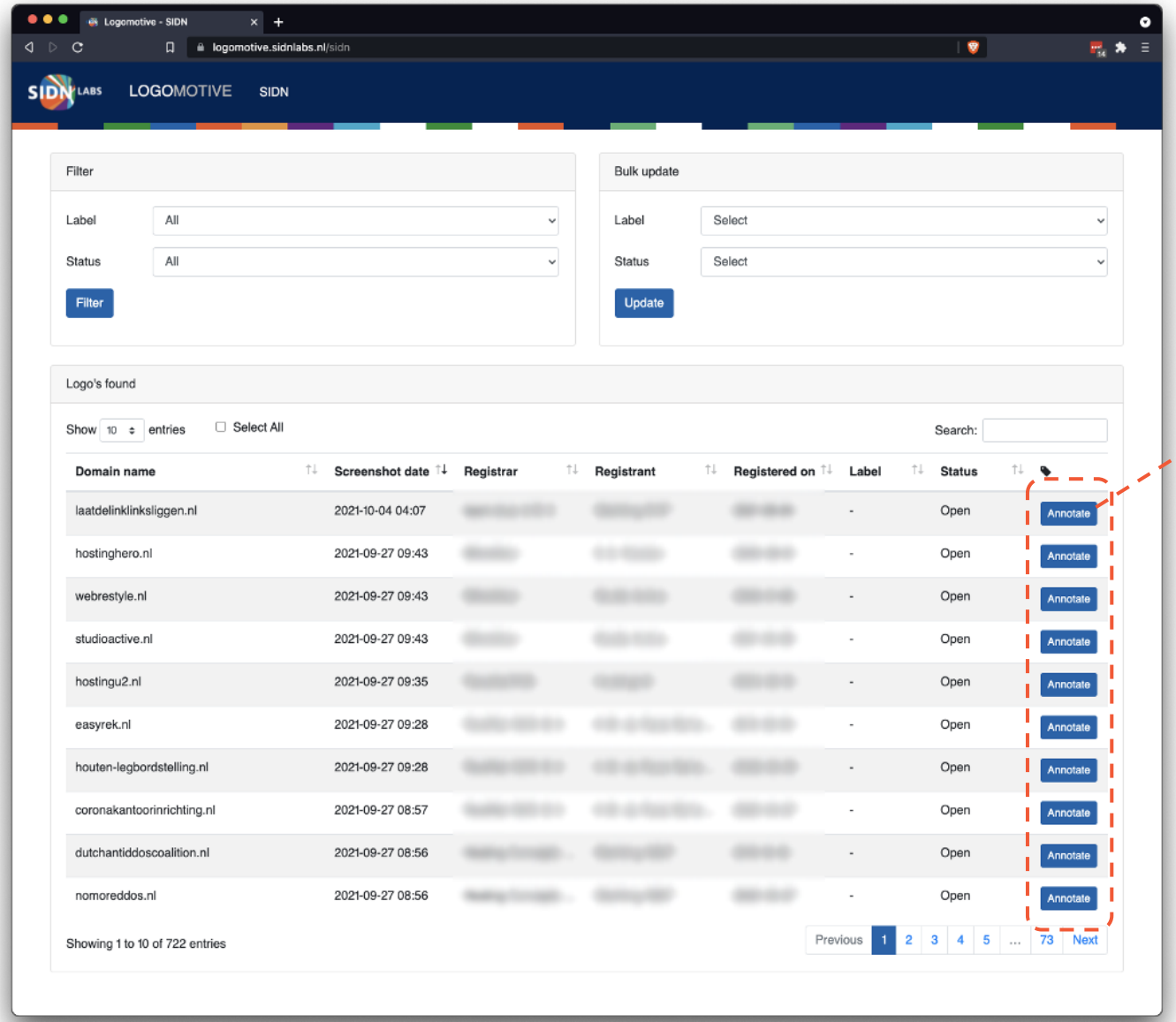

List of .nl
Domain names

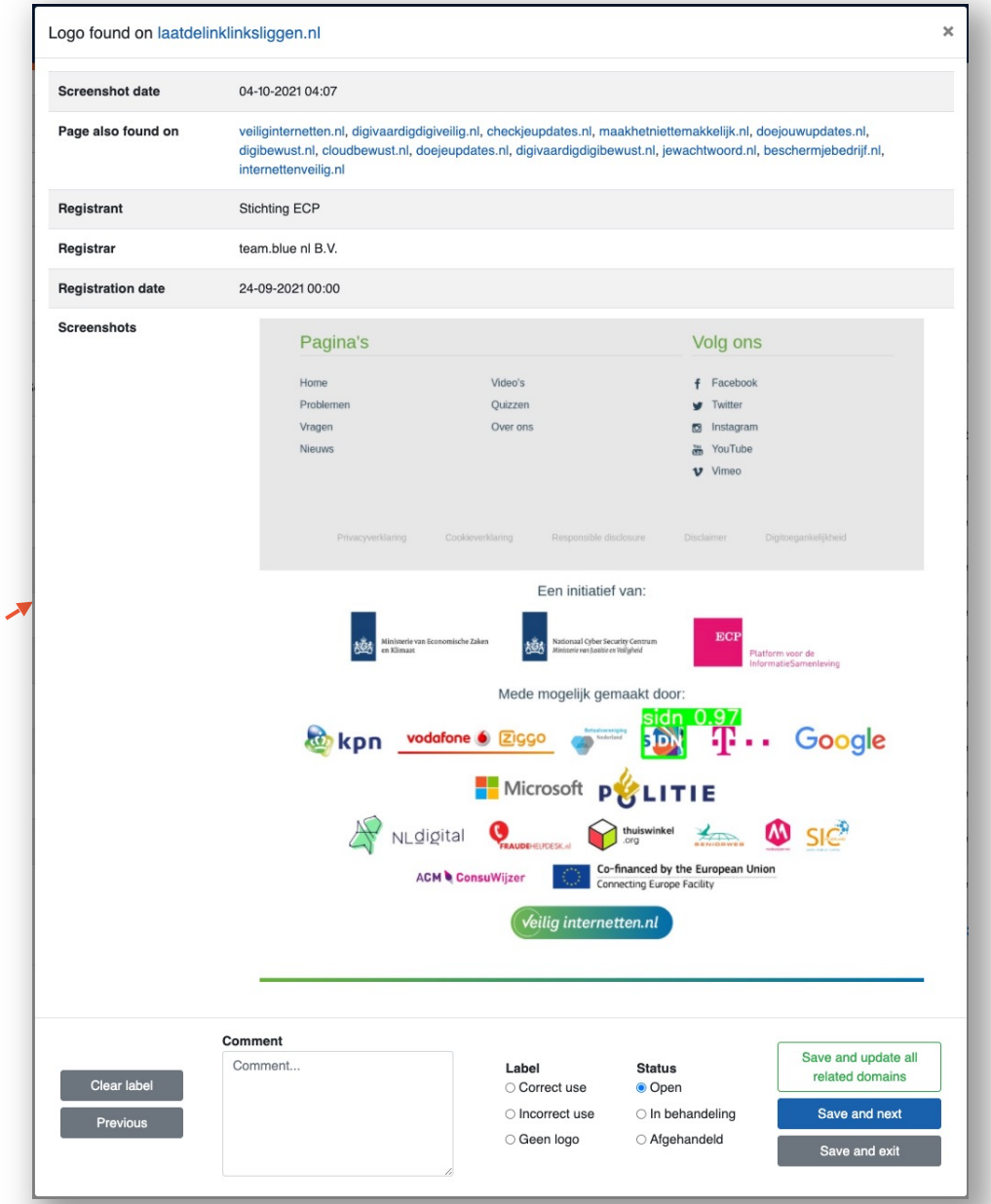
Automatically visit
and screenshot
websites

Apply logo detection
to the screenshots

Upload results to
online dashboard

# Online dashboard



# Can logo detection contribute to a safe .nl-zone?

- Case study with Dutch national government
  - Goal: find government impersonation attacks
  - Apply to full zone (6.2M domains) and to new domains (2 month)

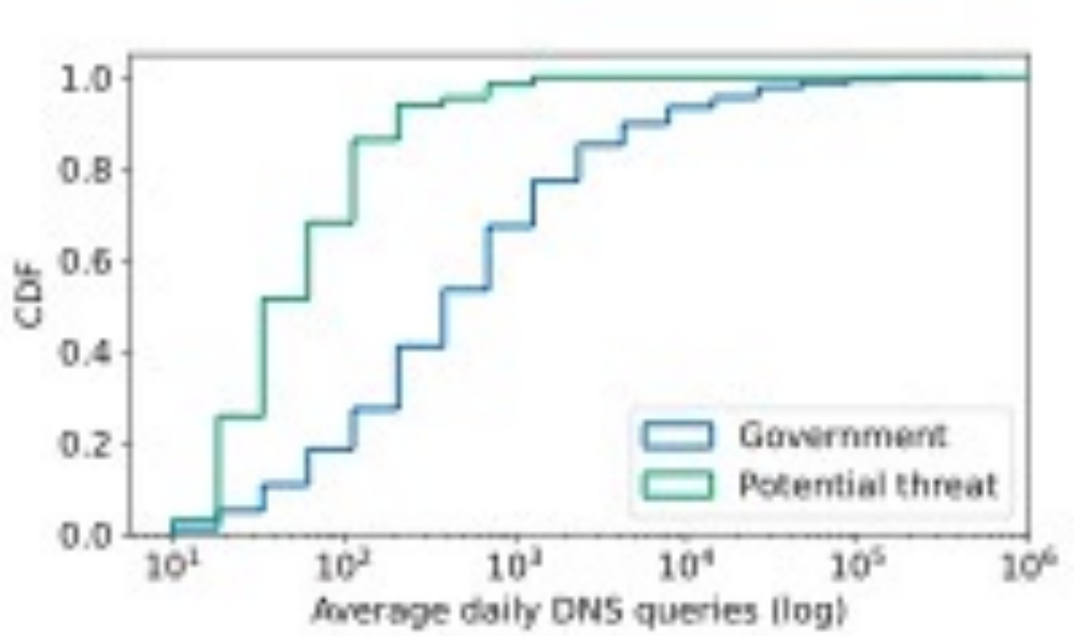
- Case study with Dutch e-commerce trustmark (Thuiswinkel.org)
  - Goal: find webshops that abuse the trustmark
  - Apply to full zone (6.2M domains)

SIDN LABS

# Manual validation results for government study

| Label | Full-Zone | Newly-Registered |
|---|---|---|
| Total | 12862 (100.00%) | 53 |
| Without gov. logo (FP) | 1164 (9.05%) | 0 (0.00%) |
| With gov. logo (TP) | 11698 (90.95%) | 53 (100.0%) |
| Benign | 10595 (82.37%) | 32 (60.38%) |
| Government impersonation | 151 (1.17%) | 17 (32.09%) |
| Phishing | 3 (0.02%) | 3 (5.66%) |
| Potential threat | 73 (0.57%) | 9 (16.98%) |
| Other (false endorsements, satire, etc.) | 75 (0.58%) | 5 (9.43%) |
| Government domains | 952 (7.40%) | 4 (7.55%) |
| In portfolio | 636 (4.94%) | 2 (0.00%) |
| Not in portfolio | 316 (2.46%) | 2 (3.77%) |
| Added | 109 (0.85%) | 1 (1.89%) |
| Pending | 207 (1.61%) | 1 (1.89%) |

# DNS queries seen at .nl authoritative name servers



# Adoption rate of security standards

| | Government Domains | |
|---|---|---|
| | **In portfolio** | **Not in portfolio** |
| Total | | |
| with DNSSEC | 623 (98%) | 230 (74%) |
| without DNSSEC | 13 (2%) | 79 (26%) |
| with DMARC | 584 (92%) | 126 (41%) |
| without DMARC | 52 (8%) | 183 (59%) |

# Lessons learned and future work

- Visual aspects like logo's help us to detect abuse
- Logo's also help to keep domain portfolio accurate
- Large gray area of unwanted, but not abusive content

**Next steps:**

- Publish academic paper (under review)
- Share code with peers and university
- Integrate with '*SIDN BrandGuard*'

*Volg ons*

SIDN.nl

@SIDN

SIDN

# Q&A

www.sidnlabs.nl | stats.sidnlabs.nl

Thymen Wabeke
Research engineer
thymen.wabeke@sidn.nl