

RegCheck: Detecting malicious domain name registrations at .nl

Thijs van den Hout (.nl)

ICANN 78 TechDay, Hamburg

October 23, 2023



Motivation for RegCheck

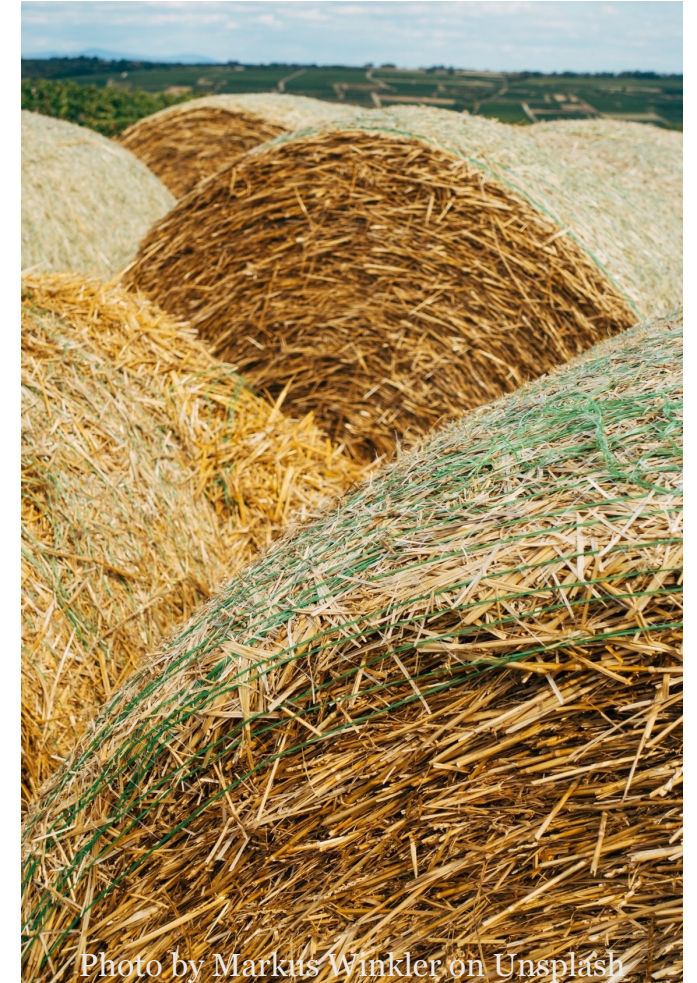
- SIDN is committed to a safe .nl domain
- Malicious intensions are sometimes obvious
 - High-risk domain name
 - Invalid or bogus registrant information
- 25% of abuse reports concern recent registrations¹



¹ stats.sidnlabs.nl

... So why wait for an abuse report?

- Proactively validating domain name registrations increases .nl's safety and trustworthiness
- Manually verify all registrations is infeasible:
 - Over 2.000 registrations per day
 - Only 3 registrations on average are reported within 30 days on Netcraft (0.15%)



In this presentation

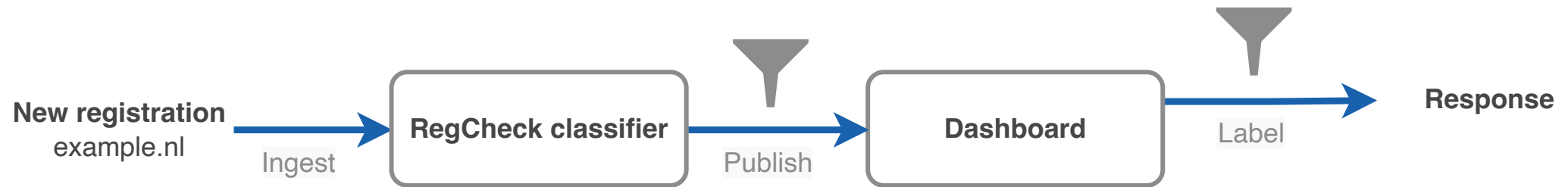


Method and results

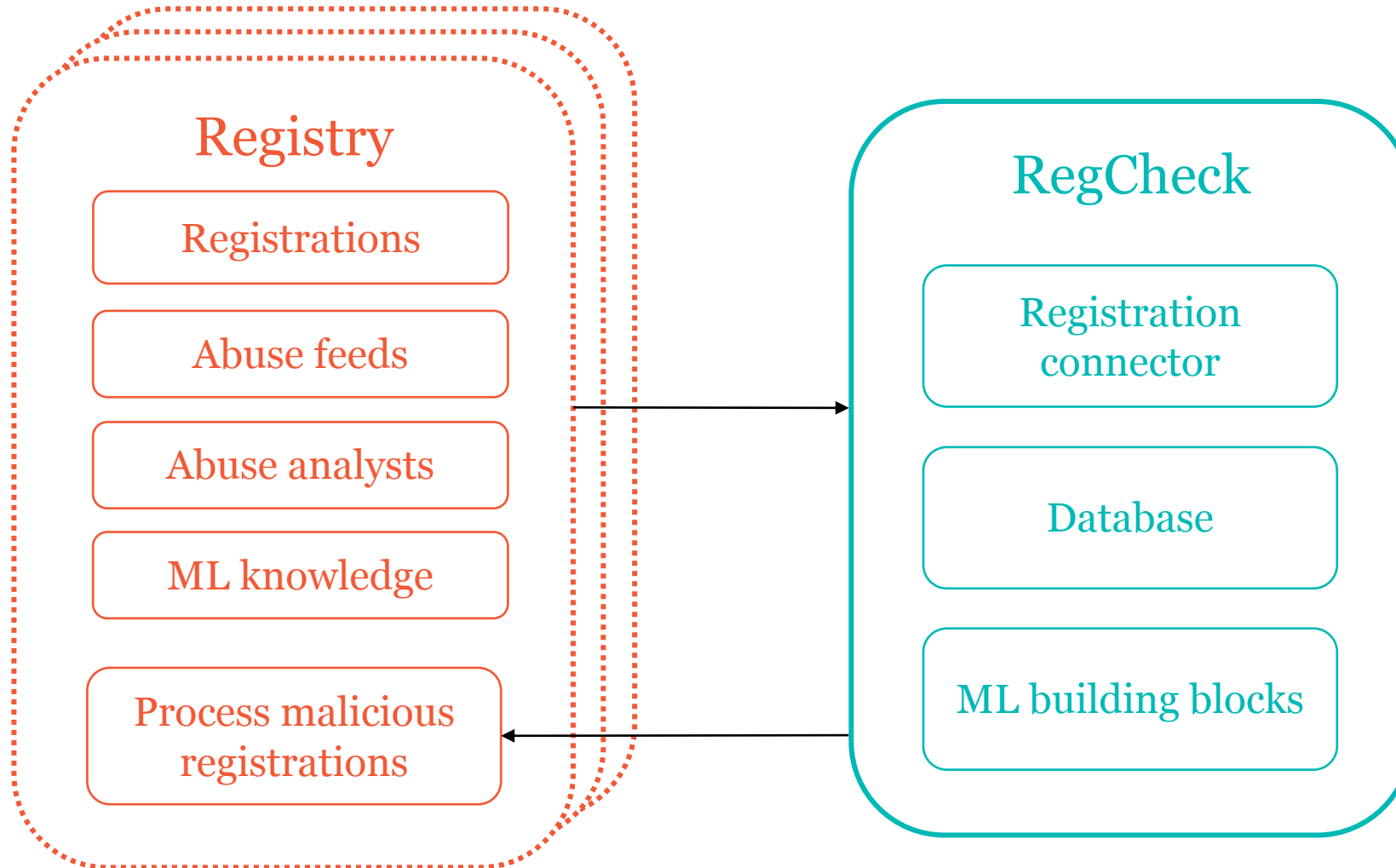


Collaboration with .be

RegCheck at .nl: filter suspicious registrations



RegCheck design



Calculating risk score

- Risk factors: characteristic that increases risk of abuse
- Explored rule-based + various machine learning approaches
- Since August 2022 logistic regression model in use
- Scikit-learn pipeline for efficient ML engineering

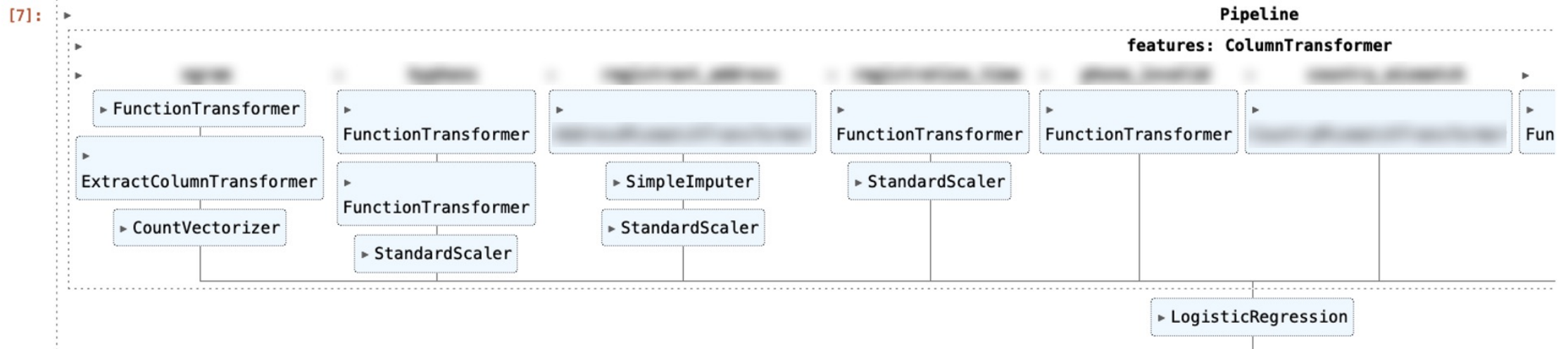
Example of a scikit-learn utility: printing our pipeline

```
[6]: from detection.lr import LrDetector


training_options['model_options'] = {
    'C': 1.0,
    'class_weight': 'balanced',
    'l1_ratio': 0.25,
    'max_iter': 50, # increase value to 100 or higher in production
    'penalty': 'elasticnet',
    'solver': 'saga'
}


detector = LrDetector(model_name='test', training_options=training_options, datasets=dataset_names_train)
```

```
[7]: detector.model # print Pipeline
```



Support dashboard

 **securepaymentportal.nl** WHOIS DRS Historie Website KASM ×

Risk score	90%
Name	Stichting Internet Domeinregistratie Nederland
Address	 fake address, 12345AB Randomsterdam, NL
Email	support@sidn.nl
Phone	+31.263525555
Registrar	Stichting Internet Domeinregistratie Nederland
Reseller	-
Registration date	2022-12-07 12:00:00
Name servers	ns5.sidn.nl, ns3.sidn.nl, ns1.sidnlabs.nl

Comment

Could be a scam, given the word 'payment' and invalid address. I will verify registrant's identity.

Label
 High-risk registration
 Registration invalid

Status
 Pending
 Done

Follow-up on RegCheck notifications (since January)

	Art. 16	Art. 18
Domain names	1100 (45% of total)	390 (40% of total)
ID verified	56	28
Registrants	258	208
ID verified	10	12

Table 1: Verification of registration data procedures initiated due to a RegCheck notification.

Evaluation (Feb through Jun '23)

	✓ RegCheck	✗ RegCheck
✓ Netcraft	46	442
✗ Netcraft	2,247	369,279
	2,293	369,721

Table 1: Comparison between RegCheck and Netcraft notification

	✓ RegCheck
✓ High-risk	425
✗ Low-risk	1,658
	2,083

Table 2: Analyst labels for RegCheck notifications

Evaluation is hard!

- Recall is a heuristic metric
- Deployment in the wild = interaction with evaluation set
- How much abuse is prevented?
- Qualitative results are positive

Collaboration with DNS Belgium (.be)

Exchange ideas for more effective detection

Jointly develop code

Blueprint for other registries

Collaboration phases

March - December 2022

Exploration

December 2022

Agreement

January 2023 - now

Joint development

Benefits of collaboration

- Improved reputation smoothing
- Validation of geographical features (e.g., city, timezone)
- Added TF-IDF-based features on registrant fields
- Handle high-cardinality n-gram features
- Discussion about design and policy choices

Collaboration goals update

Exchange ideas for more effective detection



Jointly develop code



Blueprint for other registries

Lessons learned

- Detection of malicious domain names is feasible
- A good problem definition and outcome expectation is crucial
- Collaboration works, even with diverging policies
- More people = more opinions

What's next?

- Keep using and improving prototype
- Automatically start ID verification process
- Continue collaboration with .be, introduce more registries
- Explore how we can help .nl registrars by sharing RegCheck scores



Photo by Jess Bailey on Unsplash

Q&A

thijs.vandenhout@sidn.nl
thymen.wabeke@sidn.nl
maarten.bosteels@dnsbelgium.be

