RegCheck: risicobeoordeling van nieuwe .nl-registraties

Thymen Wabeke | Dag van de Domeinnaam

12 september 2023

Aanleiding RegCheck

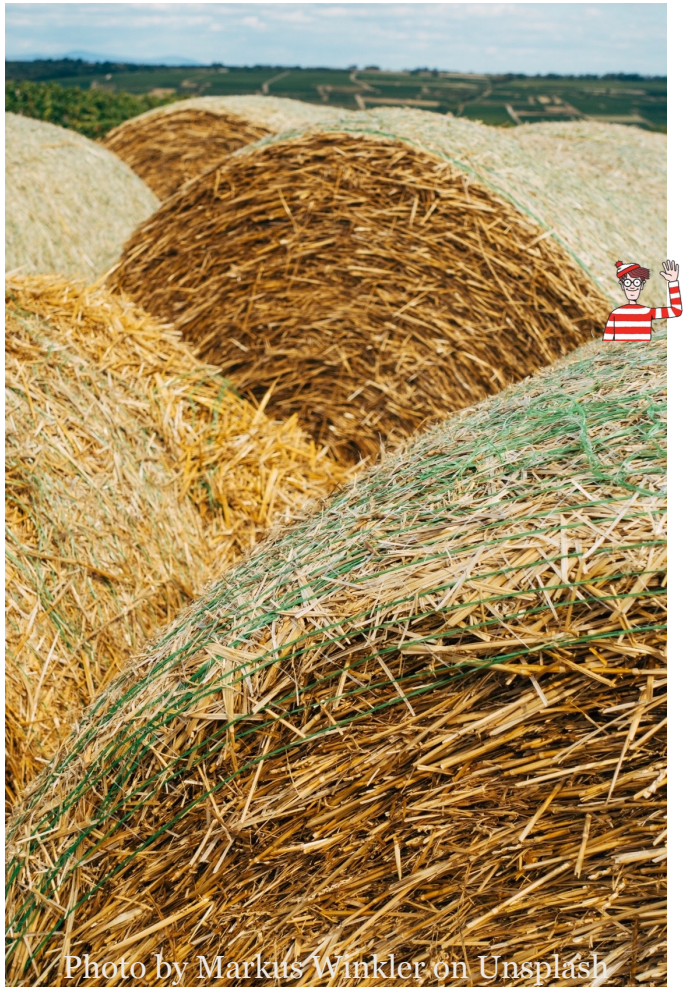
- SIDN staat voor een veilig .nl-domein

- Malafide intenties soms vrij duidelijk
  - Risicovolle domeinnaam
  - Ongeldige houdergegevens

Dus… Waarom wachten tot de abusemelding?

- Proactief valideren van domeinnaam registraties maakt .nl veiliger

- Handmatige alles controleren is geen optie:
  - Ruim 2.000 registraties per dag
  - Slechts 3 registraties hiervan binnen 30 dagen op Netcraft (0,15%)



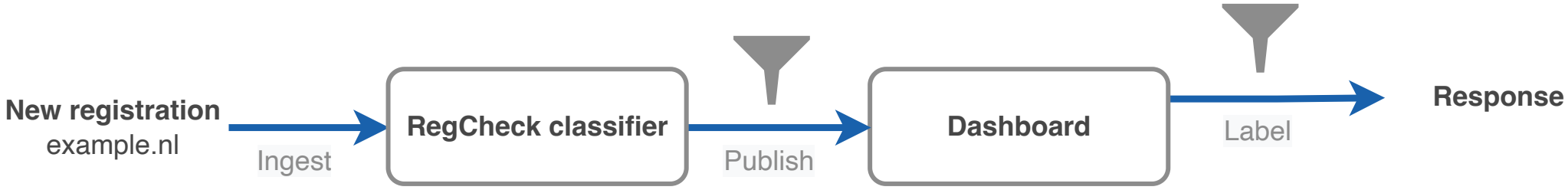
Op het menu…

Methode en resultaten

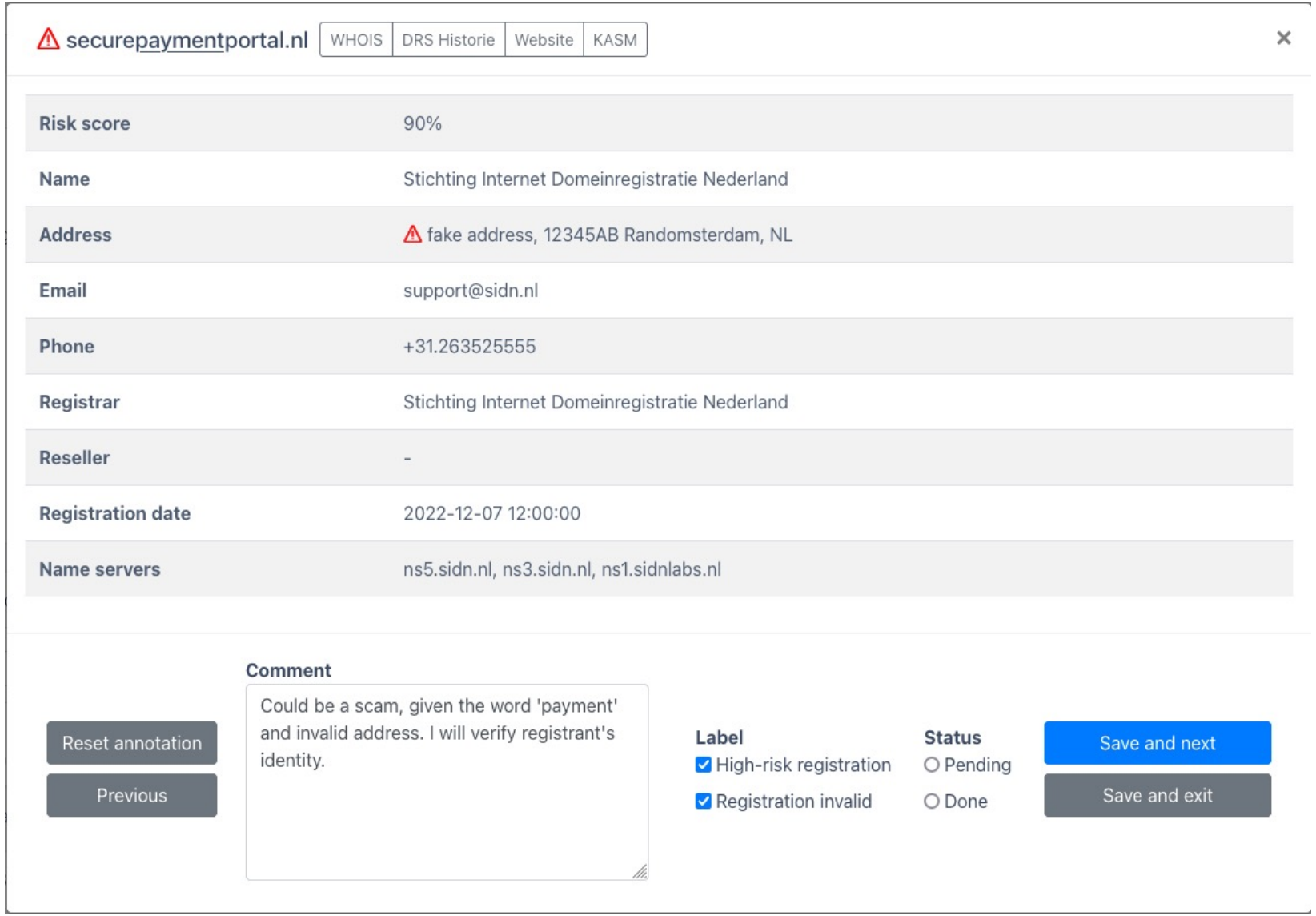
Samenwerking .be

Photos by Amélie Mourichon and Marvin Meyer on Unsplash

RegCheck: potentieel malafide registraties filteren



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.
Reset annotation
Previous
Label
High-risk registration
Registration invalid
Status
Pending
Done
Save and next
Save and exit

Berekening risico

- Risicofactor: kenmerk dat risico verhoogt (21 momenteel)
- Verschillende regel-gebaseerde en machine learning classifiers verkend
- Sinds augustus 2022 een logistische regressiemodel in gebruik
- Registry onafhankelijke code

Evaluatie (feb t/m juni ‘23)

9.4% recall

20.4% precision

	✓ 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

Evaluatie (feb t/m juni ‘23)

9.4% recall

20.4% precision

	✓ 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

Opvolging van RegCheck meldingen (jan t/m sept ’23)

	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.

Kanttekening bij evaluatie

- Recall is heuristiek, omdat werkelijke aantal malafide registraties onbekend is
- Niet zuiver, omdat RegCheck de dataset beïnvloed
- Niet volledig, omdat we niet weten hoeveel schade we voorkomen
- Kwalitatieve evaluatie is positief en Support collega's pakken veel notificaties op

Samenwerking DNS Belgium

- Verkennen of we samen effectiever risicovolle registraties kunnen detecteren
- Gezamenlijke methode ontwikkelen om risicovolle registraties te herkennen
- Onderzoeken of we een blauwdruk kunnen ontwikkelen en deze beschikbaar kunnen stellen aan andere DNS actoren

Activiteiten

- Elkaars methodes getest en beoordeeld ✓
- Geleerd van elkaars methode en aanpak ✓
- Gezamenlijke publicatie over samenwerking ✓

- Samenvoegen code beide methodes (jul – okt)
- Aanhaken andere registries (vanaf +/- nov)

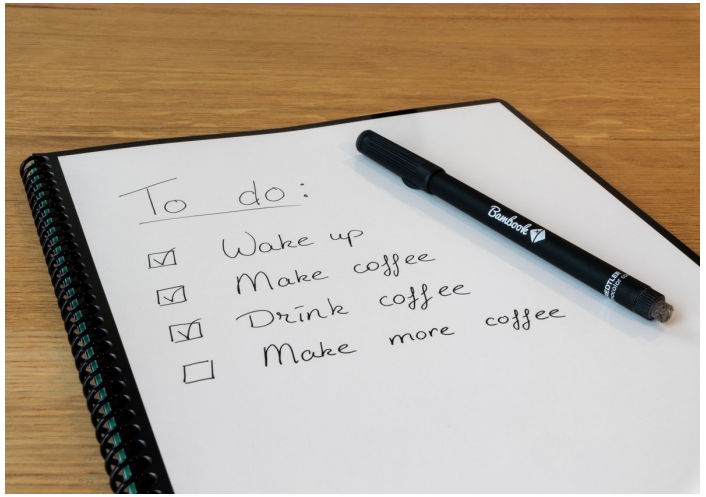


Photo by Thomas Borgmans on Unsplash

Toekomstplannen

- Prototype blijven gebruiken en verbeteren
- Mogelijk automatisch houderonderzoek starten
- Samenwerking DNS Belgium continueren, mogelijk andere registries aanhaken
- Verkennen samenwerking registrars

Photo by Jess Bailey on Unsplash

Q&A

https://www.sidnlabs.nl/nieuws-en-blogs/risicobeoordeling-van-nieuwe-nl-registraties-met-behulp-van-regcheck
https://www.sidnlabs.nl/nieuws-en-blogs/dns-belgium-en-sidn-werken-samen-aan-ml-project-voor-detectie-van-verdachte-domeinnaamregistraties

thijs.vandenhout@sidn.nl
thymen.wabeke@sidn.nl