LogoMotive, Merkbewaking & Domeinportfoliochecker

Thymen Wabeke, Pim Pastoors | BID-overleg

11 januari 2022

SIDN LABS

SIDN in een notendop

- Stichting Internet Domeinregistratie Nederland
- De Stichting achter een van de meest succesvolle en veiligste landen-domeinen (cc TLD's): .nl
- > 6,2 miljoen .nl-domeinnamen geregistreerd
  > 3,5 miljoen extra beveiligd met DNSSEC
- Onafhankelijke non-profitorganisatie opgericht in 1996 en gevestigd in Arnhem
- >135 medewerkers
- Delen kennis, steunen initiatieven voor een veiliger internet en ontwikkelen nieuwe diensten

SIDN LABS

Onderzoeksagenda machine learning

- ML toepassen met als doel verhogen van de internetveiligheid en het DNS

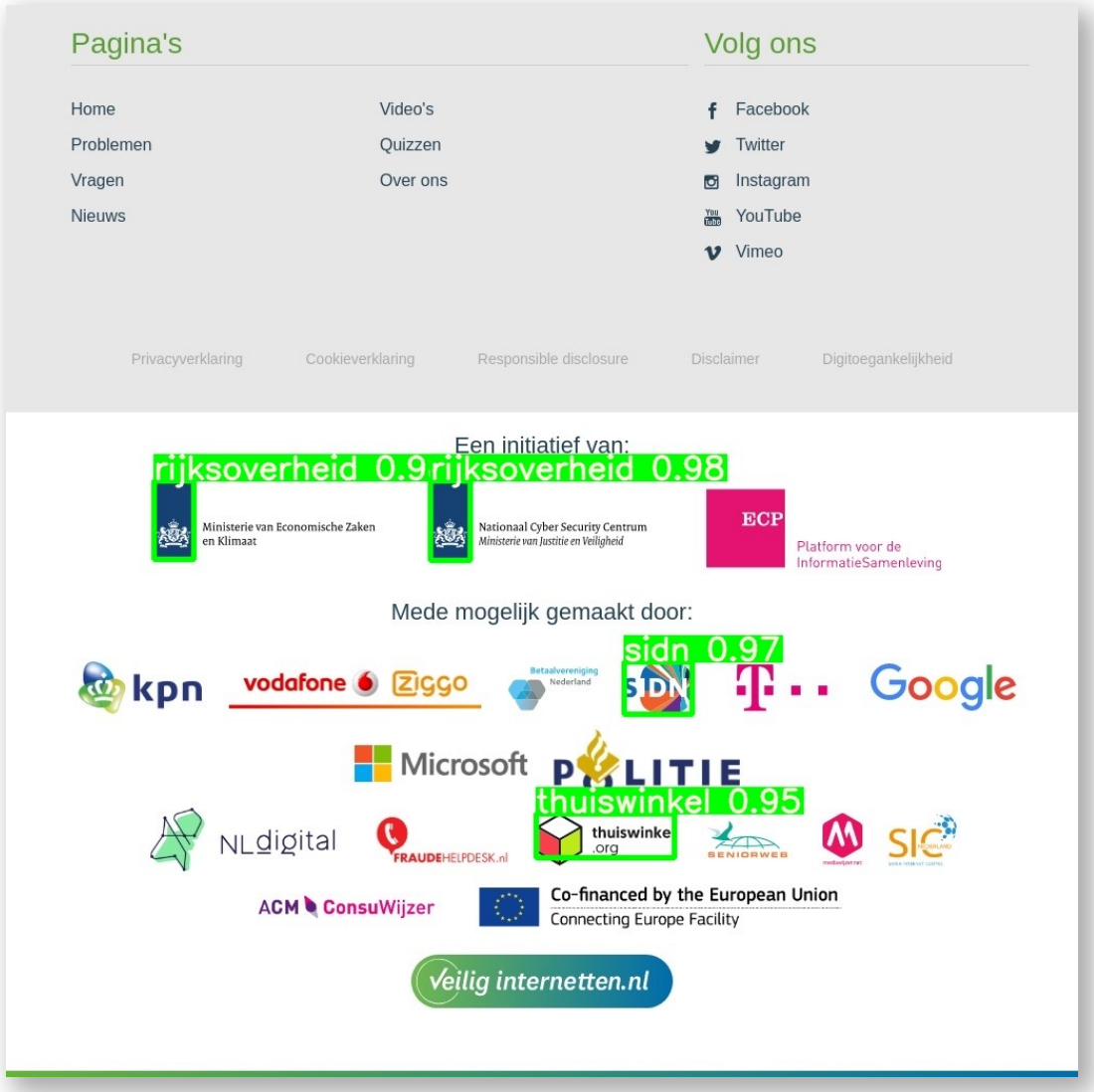
- Veelbelovende algoritmes, papers en tools verkennen en integreren
  - Innoveren *met* ML, niet innoveren *van* ML
  - ML verantwoord toepassen

- Doelgroep: DNS actoren (registries, registrars en DNS operatoren)

https://www.sidnlabs.nl/nieuws-en-blogs/meer-internetveiligheid-door-nieuwe-machine-learning-toepassingen

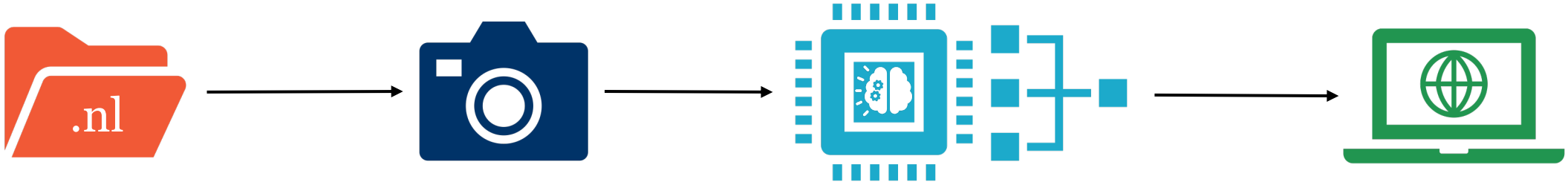
SIDN LABS

LogoMotive: malafide .nl-domeinen vinden met logo detectie



SIDN LABS

Hoe werkt LogoMotive?



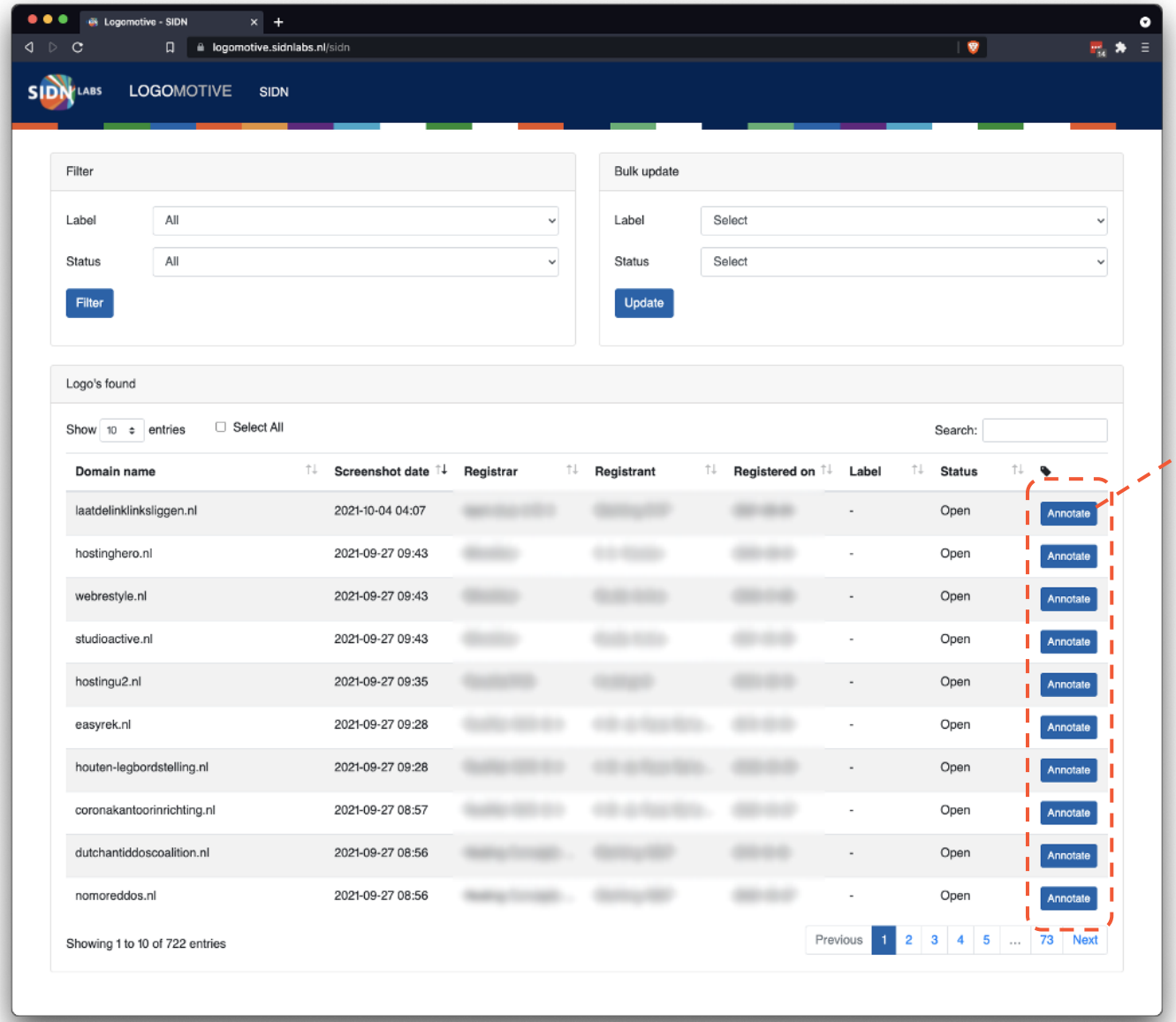
Lijst met .nl domeinnamen

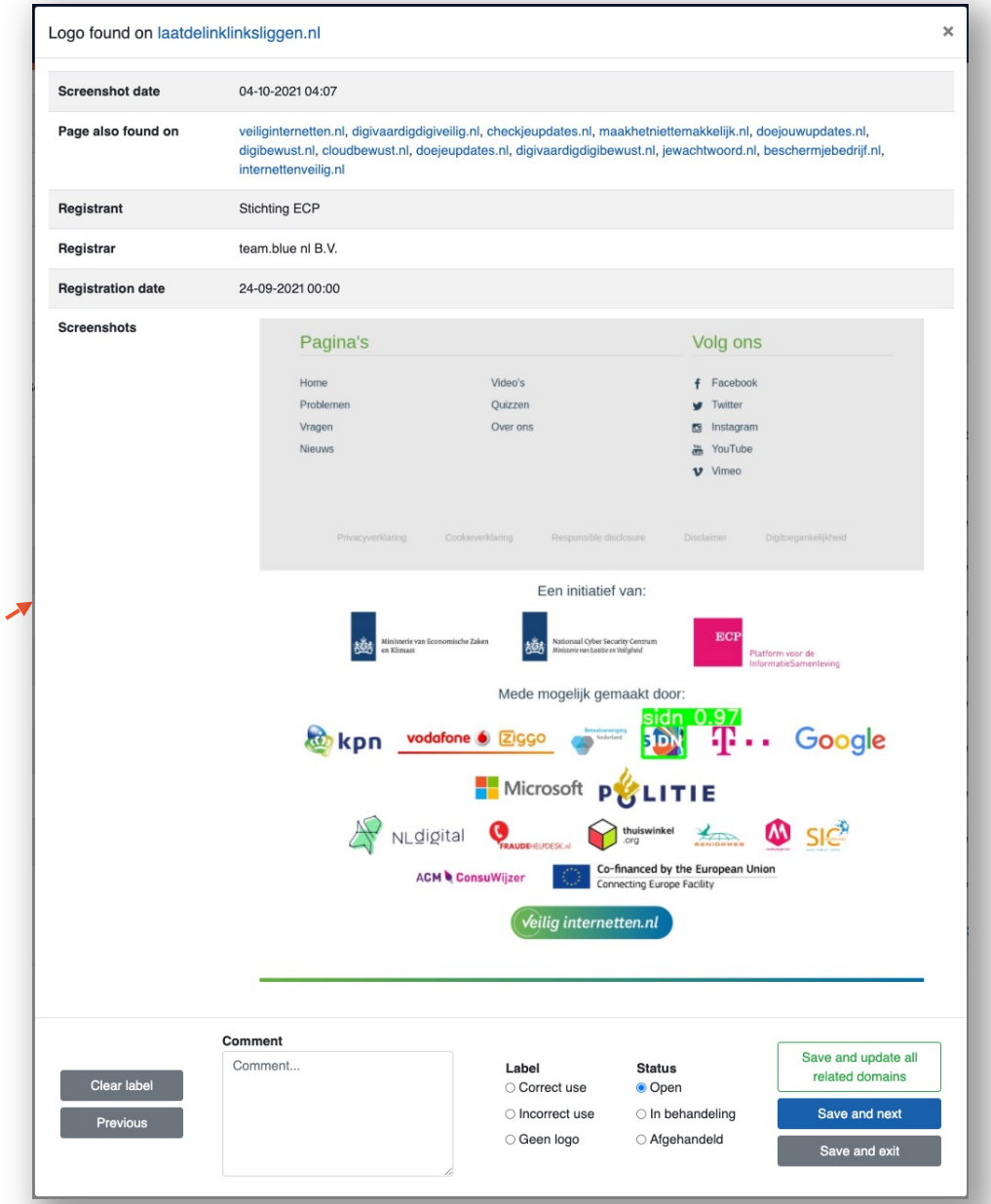
Automatisch bezoeken en screenshots maken van de websites

Logodetectie toepassen op de screenshots

Gevonden logos tonen in online dashboard

Online dashboard





Kan logodetectie bijdragen aan een veiligere .nl-zone?

- Casestudy met Rijksoverheid
  - Doel: vinden nabootsing-aanvallen gericht op overheid
  - Toepassen op hele zone (6.2M domeinen) en nieuwe registraties (2 maanden)

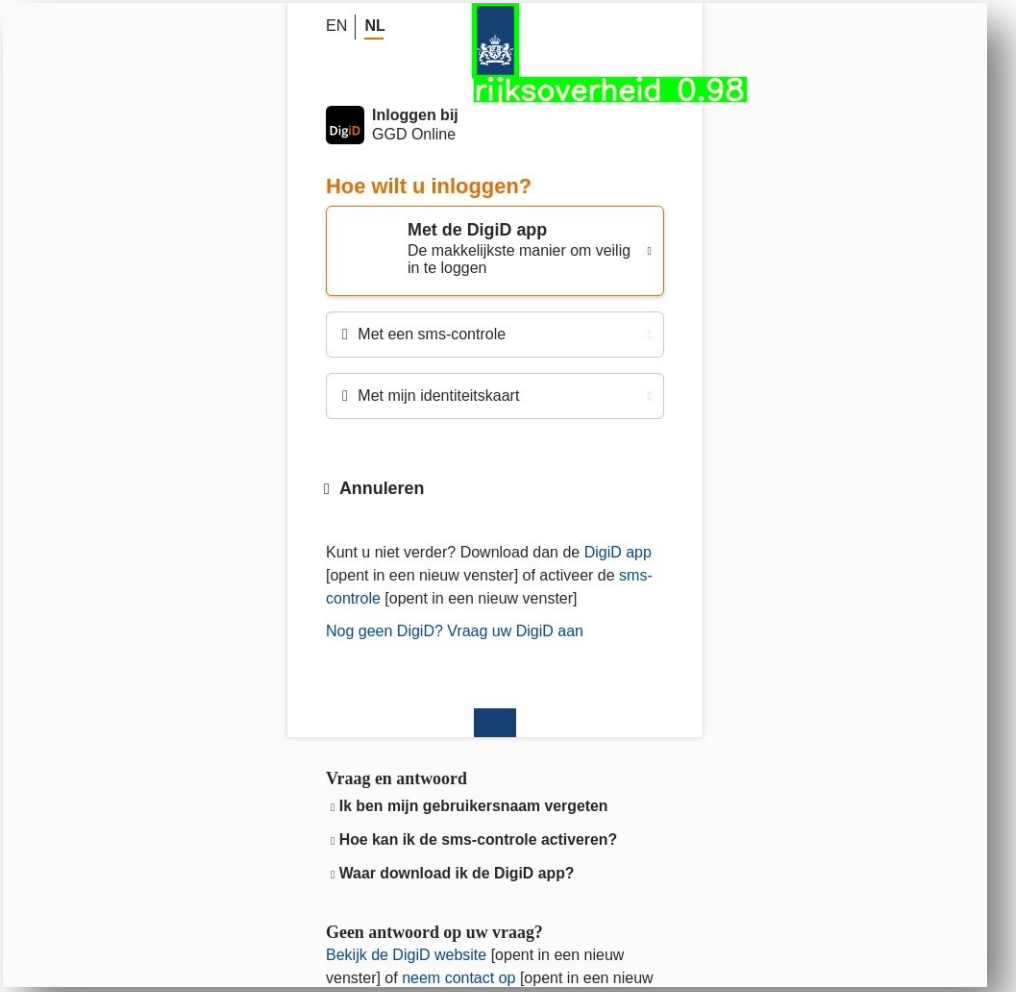
- Casestudy Thuiswinkel.org keurmerk
  - Doel: vinden webshops die het keurmerk misbruiken
  - Toepassen op hele zone (6.2M domeinen)

Handmatige validatieresultaten

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%)

Phishing domeinnamen (6)

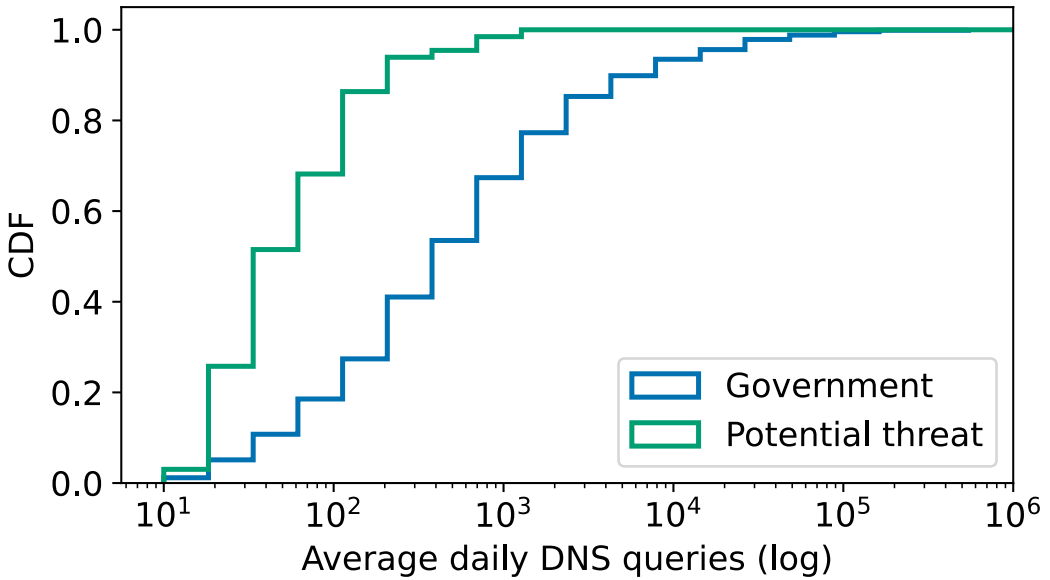
- Slechts enkele gevallen in .nl-zone
- Soms sneller dan abuse feeds
- Hoger aandeel in recente registraties
- Enkele gevallen zeer specifiek,
  zou spear phishing kunnen zijn



Potentieel gevaarlijke domeinnamen (82)

Domein lijkt op overheidsdomein,
en redirect naar overheidswebsite,
maar geen connectie met overheid.

- Wat als houder redirect aanpast?
- Wat als houder valse e-mail verstuurt?



Ontdekte overheidsdomeinnamen (318)

Domein en website gebruikt door overheid, maar domein is niet bekend bij DPC.

- Wat als website niet voldoet aan veiligheidseisen en standaarden?
- Wat als domein per ongeluk wordt opgezegd?

	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%)

Geleerde lessen en toekomstig werk

- Visuele aspecten zoals logo's helpen ons misbruik op te sporen
- Logo's helpen ook om de domeinportfolio accuraat te houden
- Groot grijs gebied met ongewenste, maar niet malafide inhoud

Volgende stappen:

- Publiceren wetenschappelijk paper (Q1 ‘22)
- Code delen met peers en universiteiten (Q1 ‘22)
- Integreren in ‘*SIDN Merkbewaking*’

Volg ons

SIDN.nl

@SIDN

SIDN

Q&A

Thymen Wabeke
Research engineer
thymen.wabeke@sidn.nl

Pim Pastoors
Productmanager
pim.pastoors@sidn.nl