LogoMotive: logodetectie voor het identificeren van malafide websites

Thijs van den Hout & Michiel Henneke

PvIB, 7 maart 2023

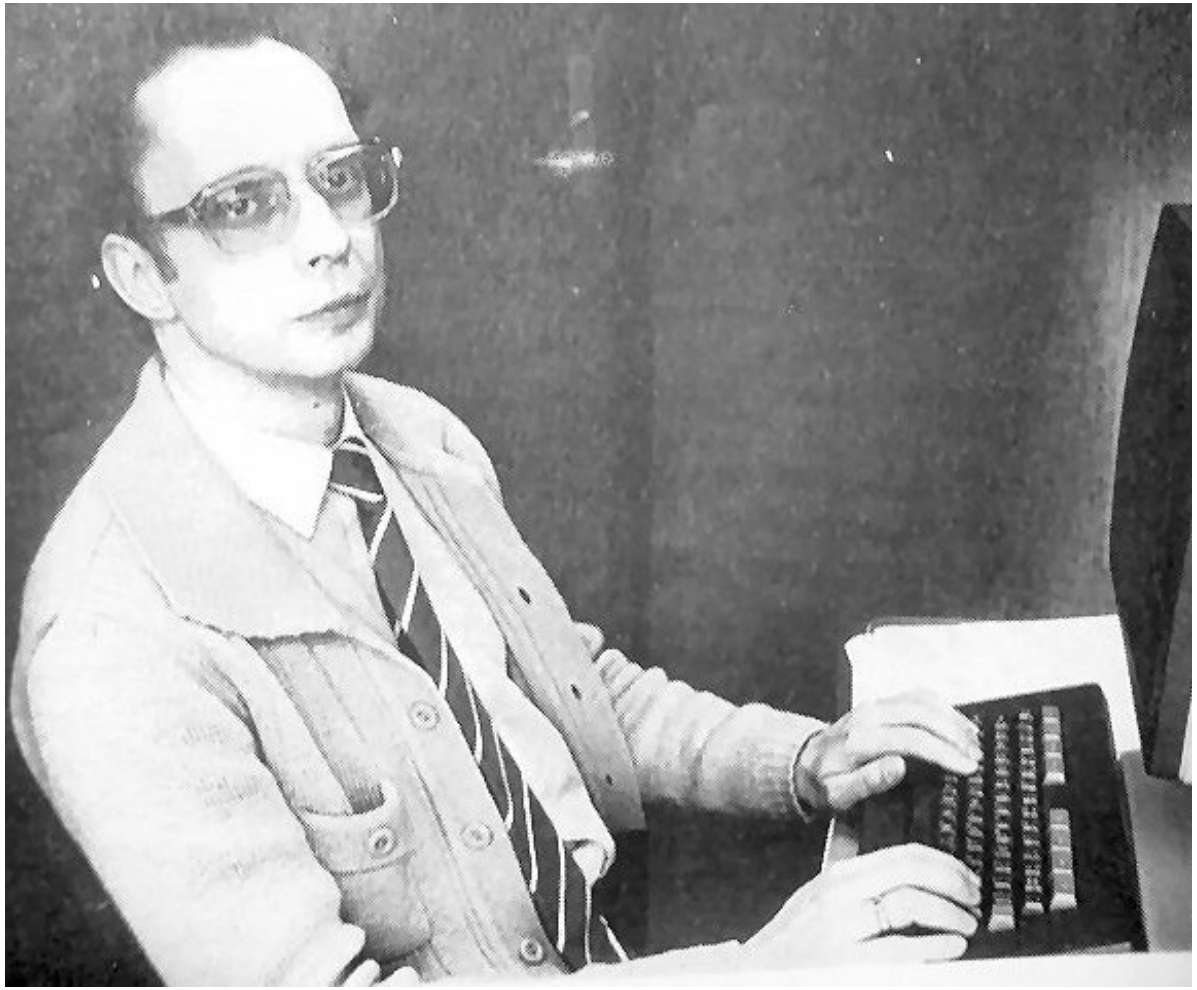
SIDN: ons verhaal

Piet Beertema:
Dé grondlegger van .nl

Aanvrager .nl-topleveldomein voor Nederland.

Legde 1ste .nl-domeinnaam vast: cwi.nl op 30 april 1986.

.nl was daarmee het 1ste actieve landendomein buiten de VS.

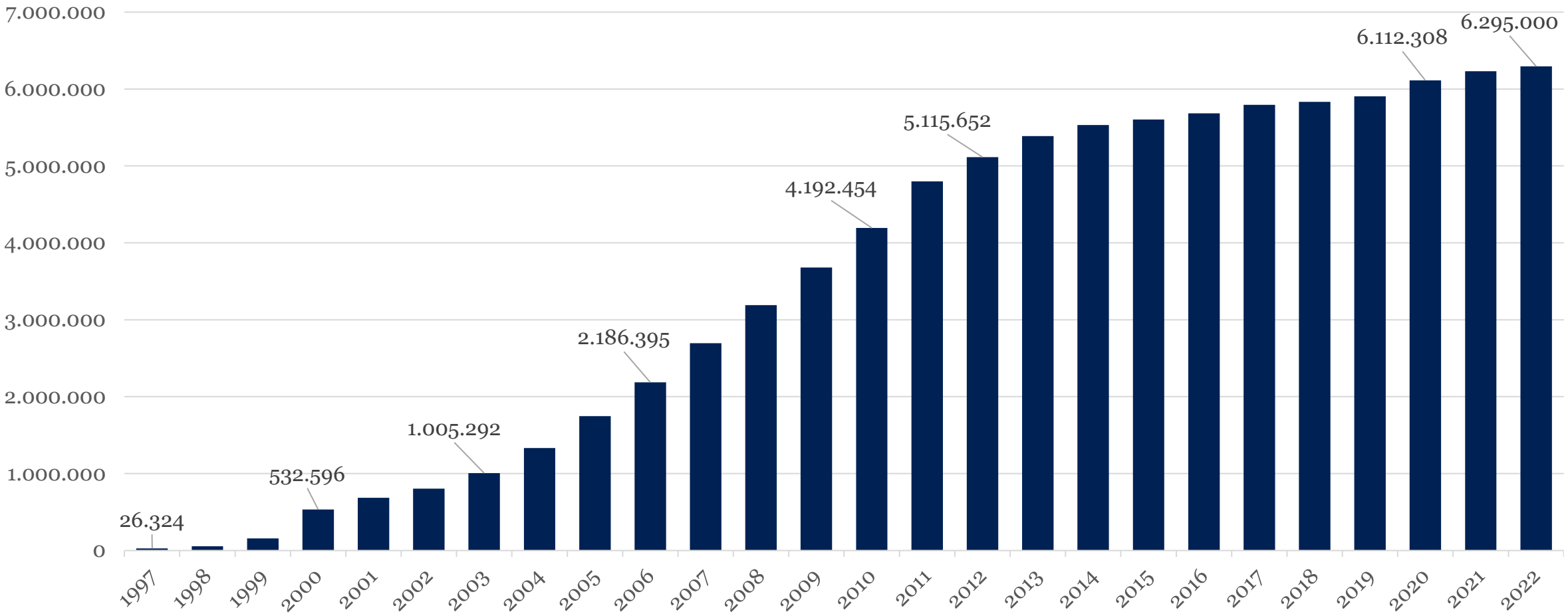


In 1996 oprichting van SIDN

De explosieve groei van .nl vereiste professionalisering.
In 1996 werd daarom SIDN opgericht:

De Stichting Internet Domeinregistratie Nederland.

Aantal .nl-domeinnamen sinds oprichting



2020

SIDN LABS

Wat is SIDN Labs?

- Onderzoeksteam van SIDN
- Doel: veiligheid van en vertrouwen in het internet verhogen, voor .nl en Nederland in het bijzonder

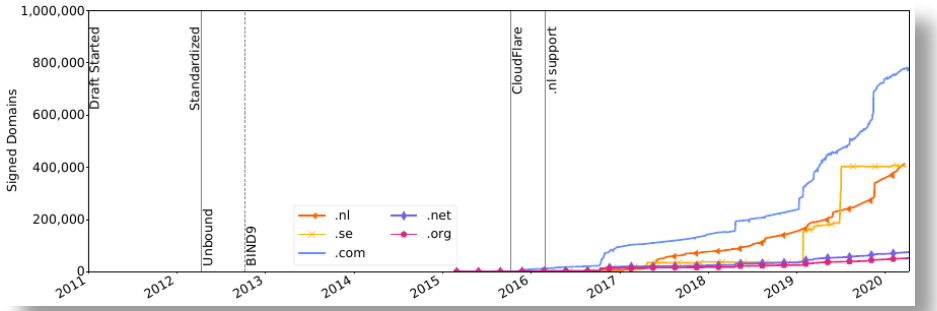
.nl = the Netherlands
~17M inwoners
6.2M+ domeinnamen
3.4M DNSSEC-signed
2.5B DNS queries/dag
8.6B NTP queries/dag

- Strategieën:
  - Toegepast technisch onderzoek (metingen, design, prototyping, evaluatie)
  - Resultaten publiek beschikbaar maken
  - Samenwerking met universiteiten, infrastructuur operators, onderzoek labs

- Drie onderzoeksgebieden: Network security (DNS, NTP, BGP), domeinnaam security, secure future internet infrastructure

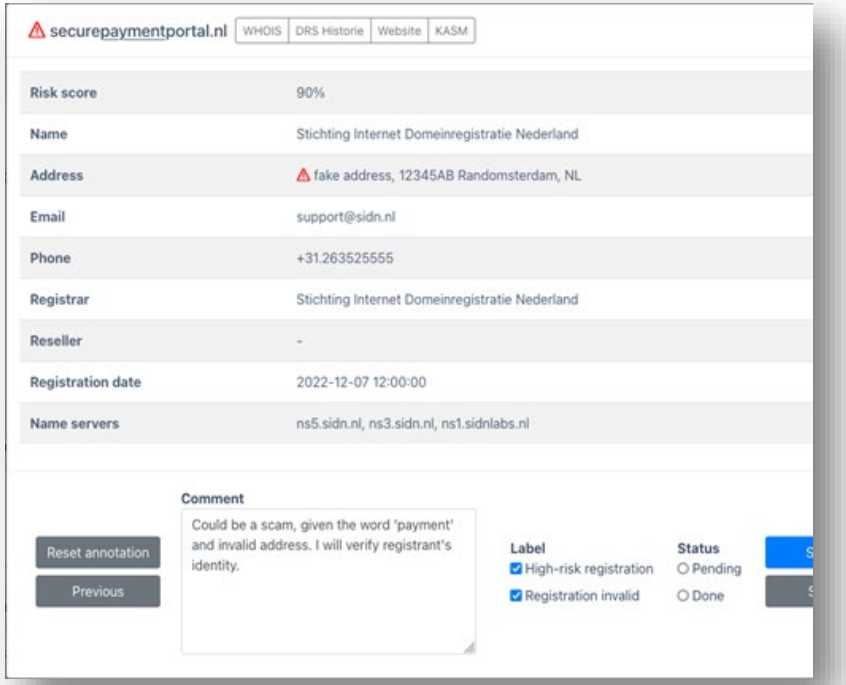
SIDN LABS

Voorbeeld projecten

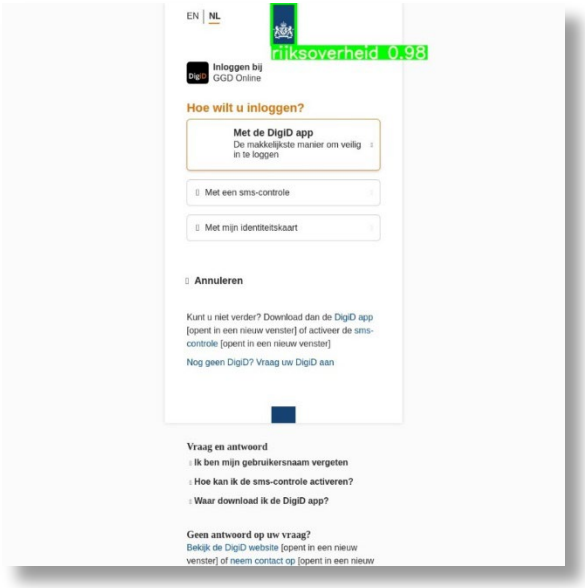


Measuring the deployment of newly standardized DNSSEC algorithms

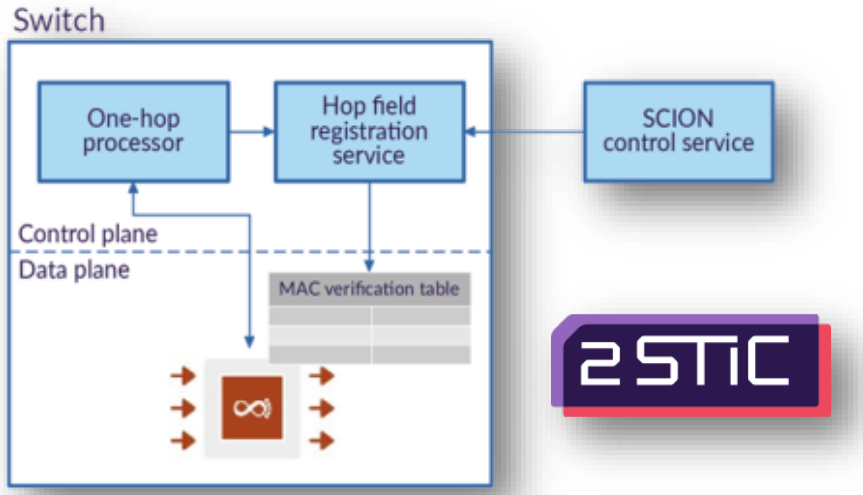
Provide well-managed and secure time services



Detecting high-risk domain name registrations

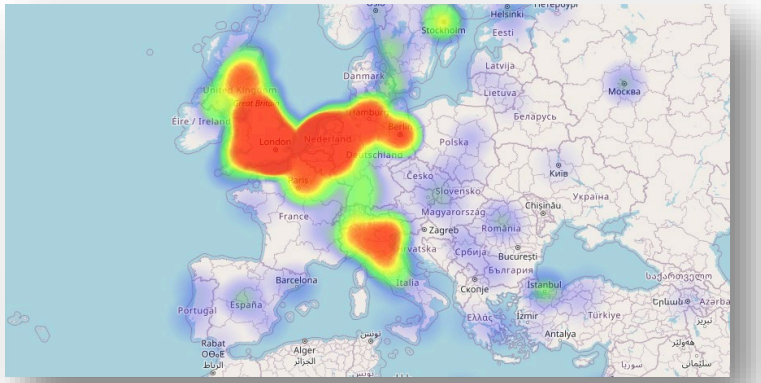


Logo detection technology to identify malicious .nl websites



2STiC

Experimenting with secure future networks and programmable networks

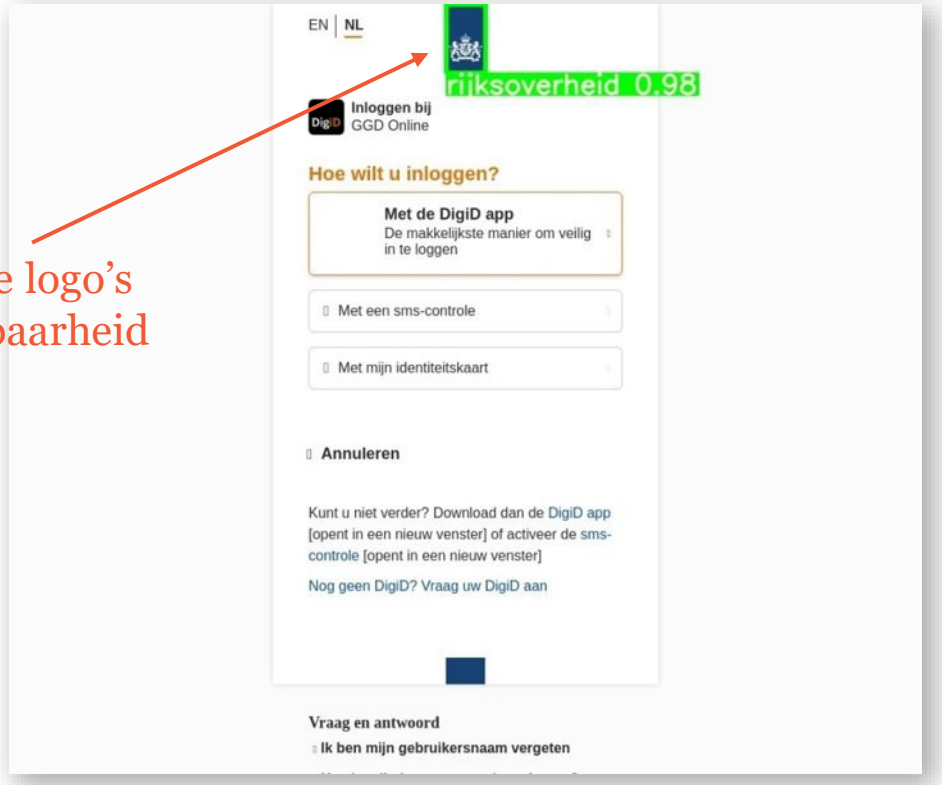


Optimize anycast routing

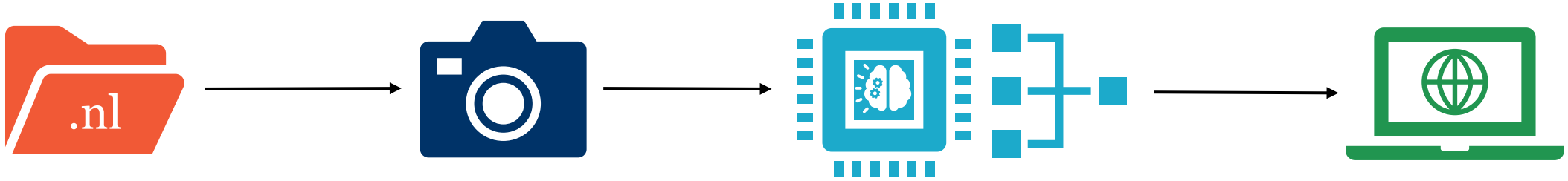
SIDN LABS

LogoMotive: malafide .nl-domeinen vinden met logodetectie

Gedetecteerde logo's
met betrouwbaarheid



Hoe werkt LogoMotive?



Lijst van 6.2M+ .nl domeinnamen

Automatisch bezoeken en screenshotten van websites

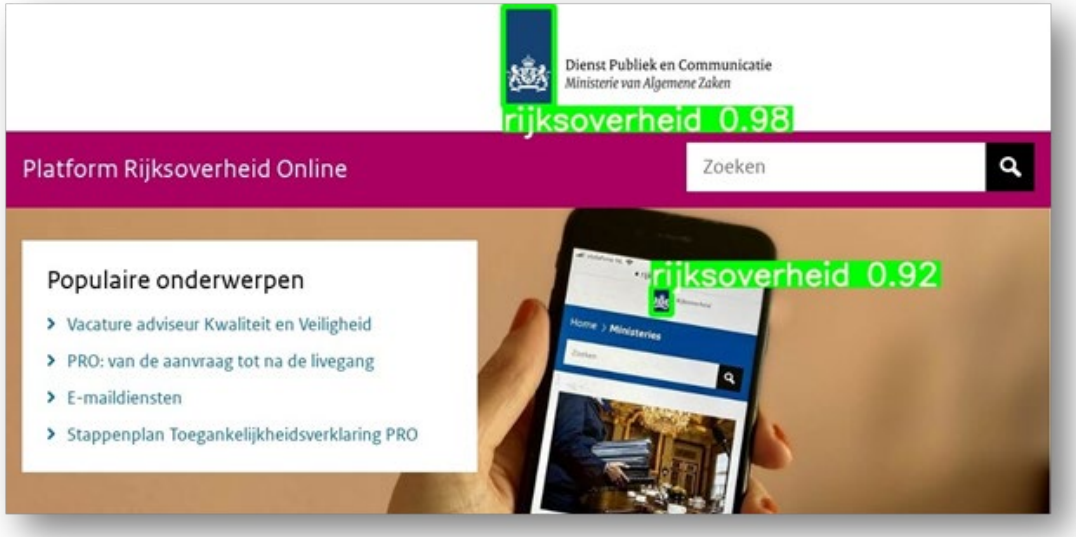
Logodetectie toepassen op gemaakte screenshots

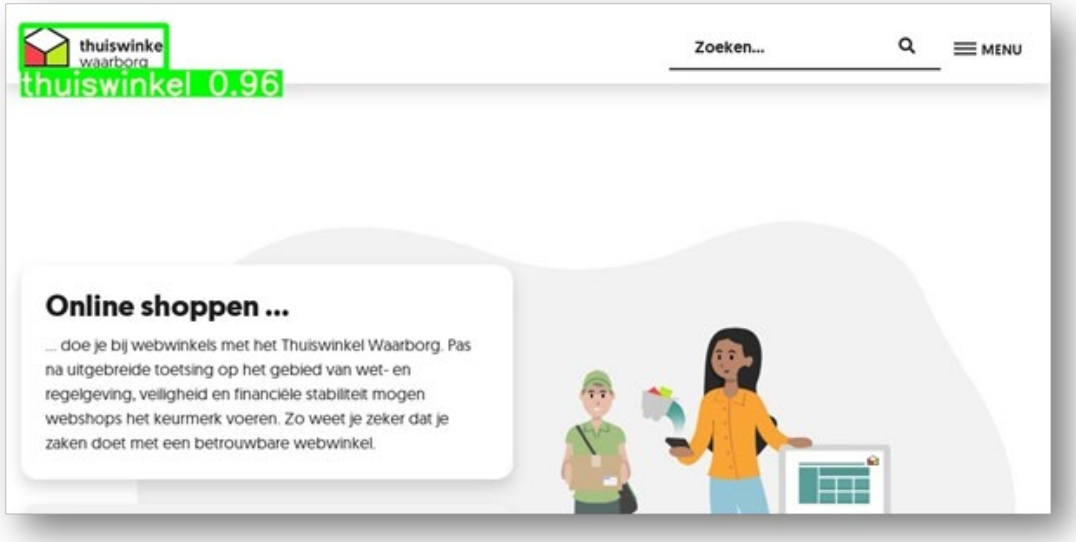
Resultaten uploaden naar online dashboard

Twee logodetectie pilots

We evalueerden het systeem in twee pilots met toonaangevende partijen op .nl

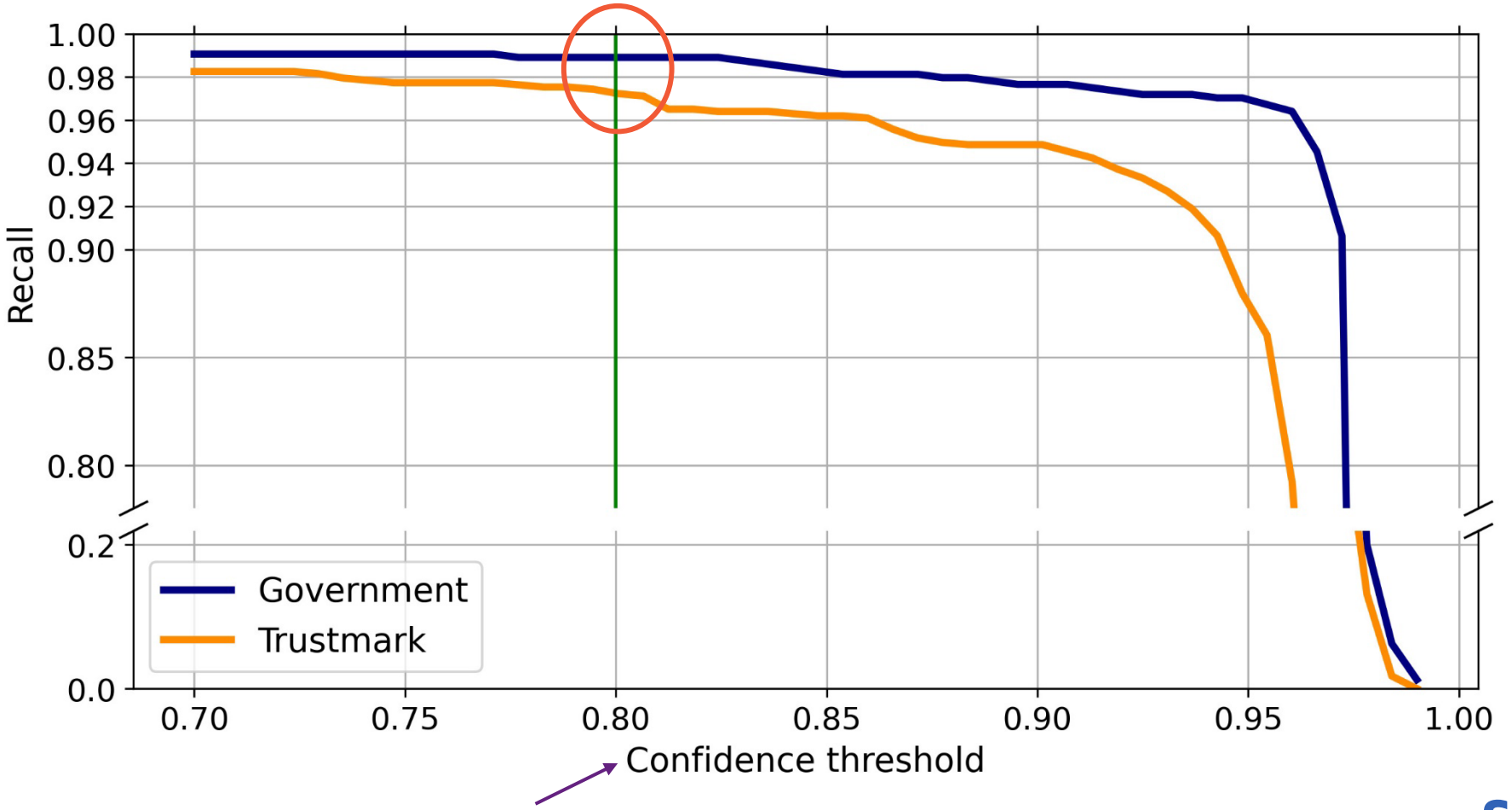
- Rijksoverheid
  - 11.700 domeinnamen gevonden
- Thuiswinkel waarborg
  - 10.600 domeinnamen gevonden





LogoMotive's recall

- Recall = percentage van websites met logo dat succesvol wordt gedetecteerd



Het model moet zo zeker zijn voor het een logo als zodanig aanmerkt

Onze inzichten uit de pilots

1. Logodetectie kan helpen malafide websites naar boven te brengen

2. Logodetectie onthult spear-phishing en andere risico's

3. Logodetectie kan helpen domeinnaamportfolio's up-to-date te brengen

1. Malafide websites ontdekken

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%)

thuiswinkel waarborg

Label	Domains	Unique-URLs
Total	10669	3890
Without trust mark	83 (0.78%)	64 (1.65%)
With trust mark	10586 (99.22%)	3826 (98.35%)
Benign	10324 (96.77%)	3691 (94.88%)
Trustmark abuse	208 (1.95%)	106 (2.72%)
Discovered	54 (0.51%)	29 (0.75%)

SIDN LABS

2. Spearphishing en verdachte redirects

- govenrment.nl → HTTP redirect → government.nl
- Spear-phishing: specifieke medewerkers als doelwit
- Verdacht emailverkeer van typosquatted domeinnamen

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%)

3. Domeinnaamportfolio in kaart brengen

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%)

	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%)

Label	Domains	Unique-URLs
Total	10669	3890
Without trust mark	83 (0.78%)	64 (1.65%)
With trust mark	10586 (99.22%)	3826 (98.35%)
Benign	10324 (96.77%)	3691 (94.88%)
Trustmark abuse	208 (1.95%)	106 (2.72%)
Discovered	54 (0.51%)	29 (0.75%)

SIDN LABS

Van onderzoek naar productiedienst

- Opstellen onderzoeksvraag
- Ontwikkelfase
- Pilots
- Delen van resultaten (logomotive.sidnlabs.nl)
  - Source code voor collega registries en onderzoekers
  - Wetenschappelijk paper
- Samenwerking met ICT Team van SIDN
- Implementatie in SIDN Merkbewaking: Logo search
- Onderhoud en support

Logodetectie in de praktijk

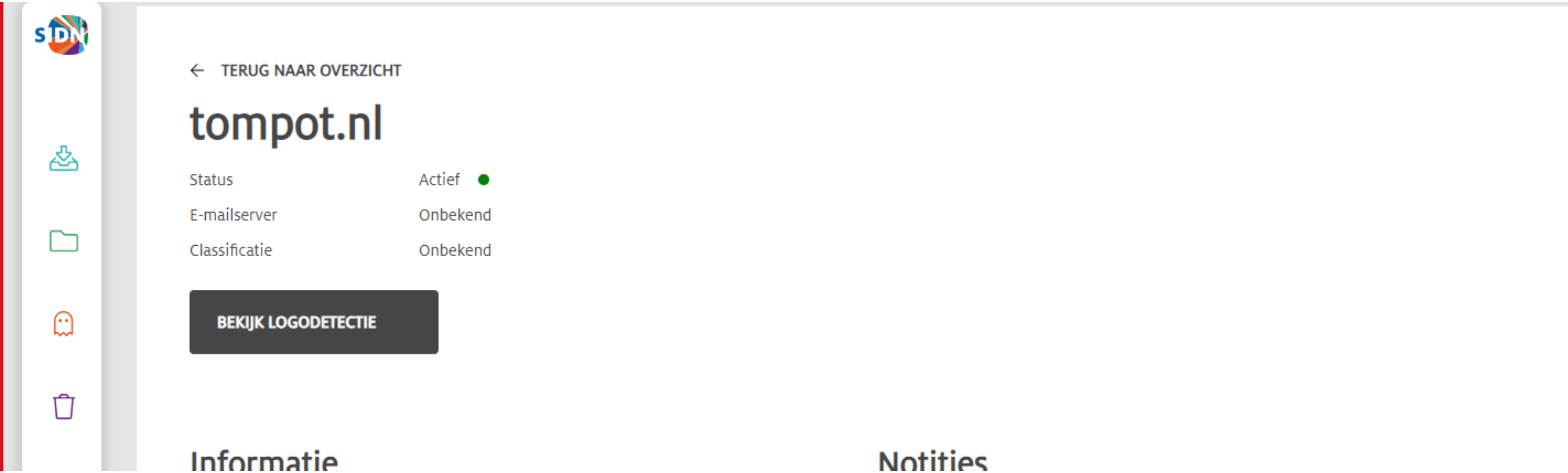
Inbox

Welkom, tester EN | NL

Filters instellen

Geselecteerde filters: Merknaam *sidn* ×

Domeinnaam	Wijzigingsdatum	Detectiedatum	Classificatie	Status
tompot.nl	08-09-2022 11:24	08-09-2022 11:25	Onbekend	Actief
tolkonline.nl	08-09-2022 10:51	08-09-2022 11:05	Onbekend	Actief
teeners.nl	08-09-2022 05:33	08-09-2022 05:50	Onbekend	Actief
technicaltrainees.nl	08-09-2022 04:55	08-09-2022 05:50	Onbekend	Actief
techbelasting.nl	08-09-2022 04:51	08-09-2022 05:50	Onbekend	Actief
tealovers.nl	08-09-2022 04:31	08-09-2022 05:00	Onbekend	Actief
tdeled.nl	08-09-2022 04:24	08-09-2022 05:00	Onbekend	Actief
tca-vloerdecor.nl	08-09-2022 04:11	08-09-2022 05:00	Onbekend	Actief
t-boothuys.nl	08-09-2022 04:09	08-09-2022 05:00	Onbekend	Actief
taxivervoer.nl	08-09-2022 03:59	08-09-2022 05:00	Onbekend	Actief


TERUG NAAR OVERZICHT
tompot.nl
Status
Actief
E-mailserver
Onbekend
Classificatie
Onbekend
BEKIJK LOGODETECTIE
Informatie
Notities

← TERUG NAAR OVERZICHT

tompot.nl

Status

E-mailserver

Classificatie

BEKIJK LOGODETECTIE

Informatie

Houder

Houder adres

E-mailadres

Registratiedatum

Detectiedatum

Wijzigingsdatum

Nameserver

Registrar naam

Registrar adres

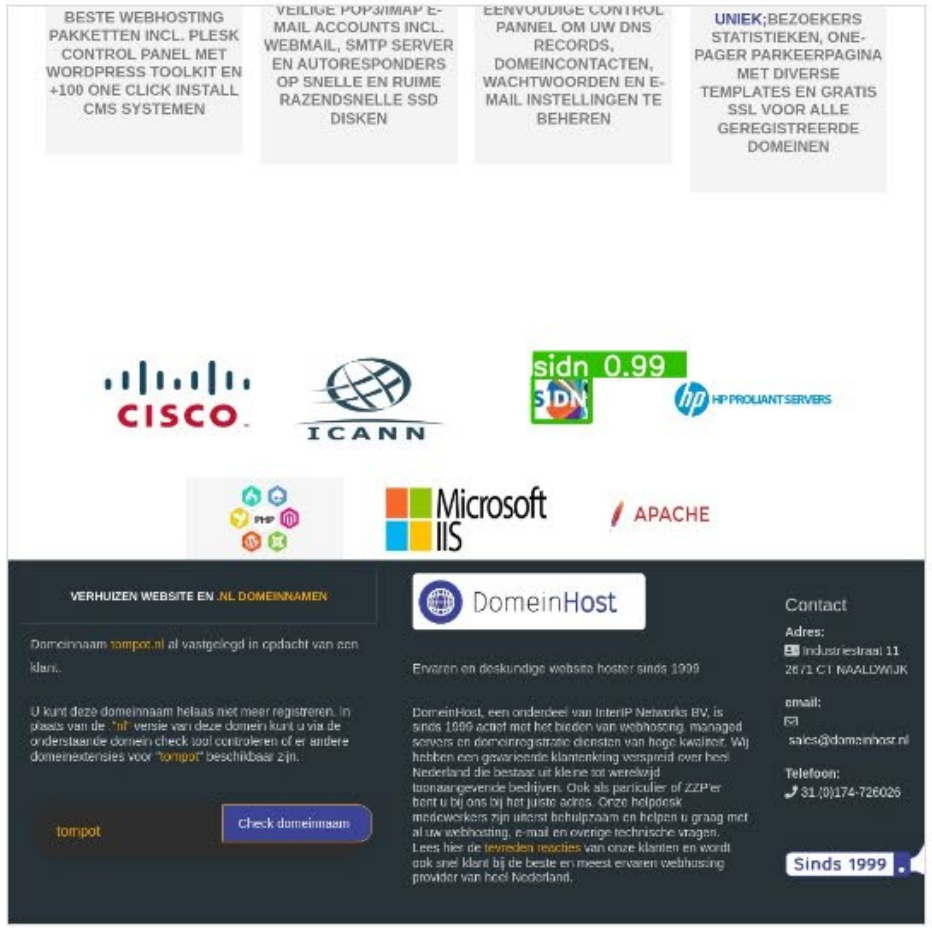
Abuse contactgegevens

Bekijk logodetectie

Sluiten

Klik op een schermafdruk om in te zoomen.

Schermafdruk 1



Schermafdruk 2

Aandachtspunten

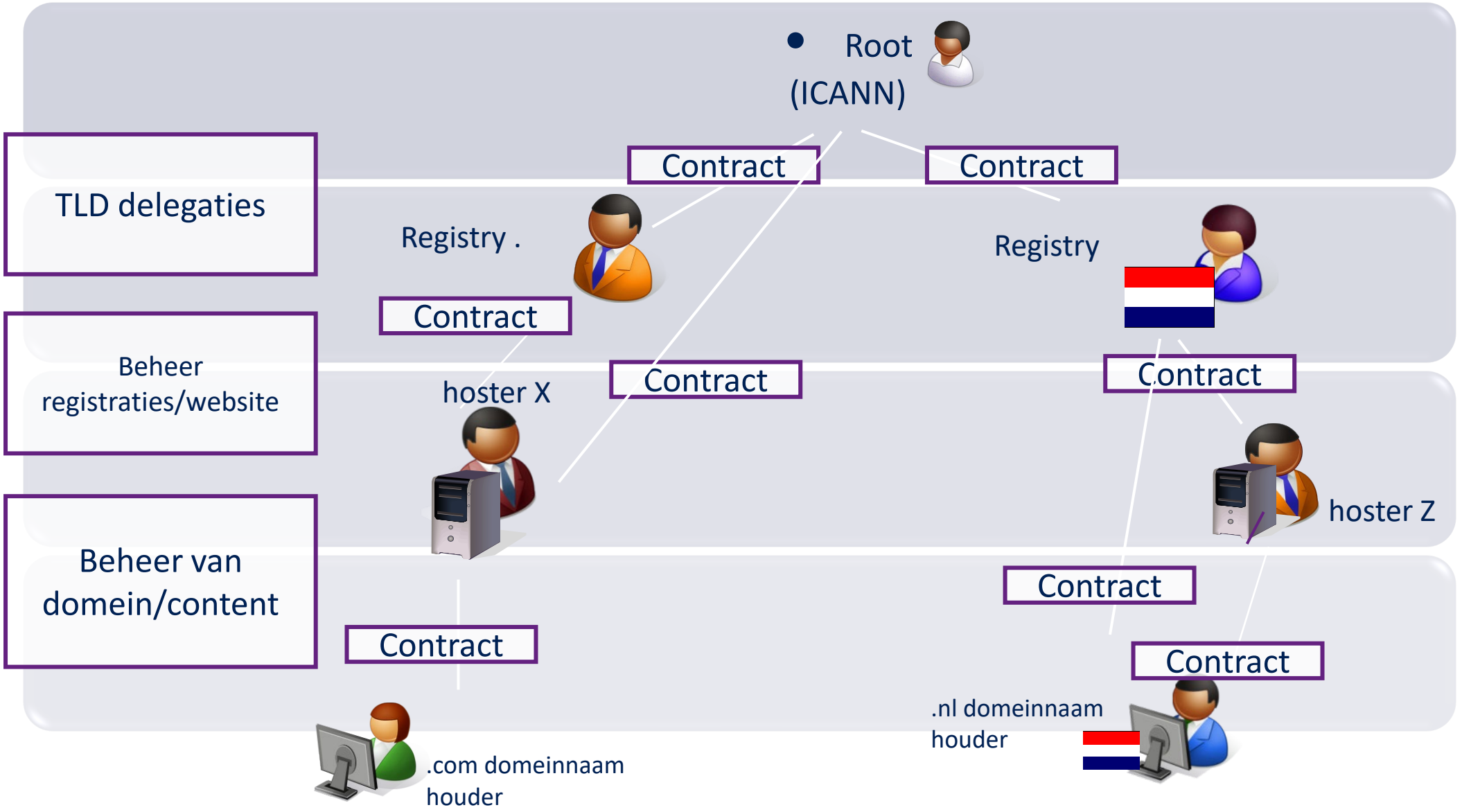
- Niet ieder logo is goed te onderscheiden. Machine Learning en negeerlijst nodig.

- Niet iedere rechthebbende heeft een goede lijst van legitieme sites (VB. iDEAL).

SIDN LABS

Opvolging: van detectie naar acties

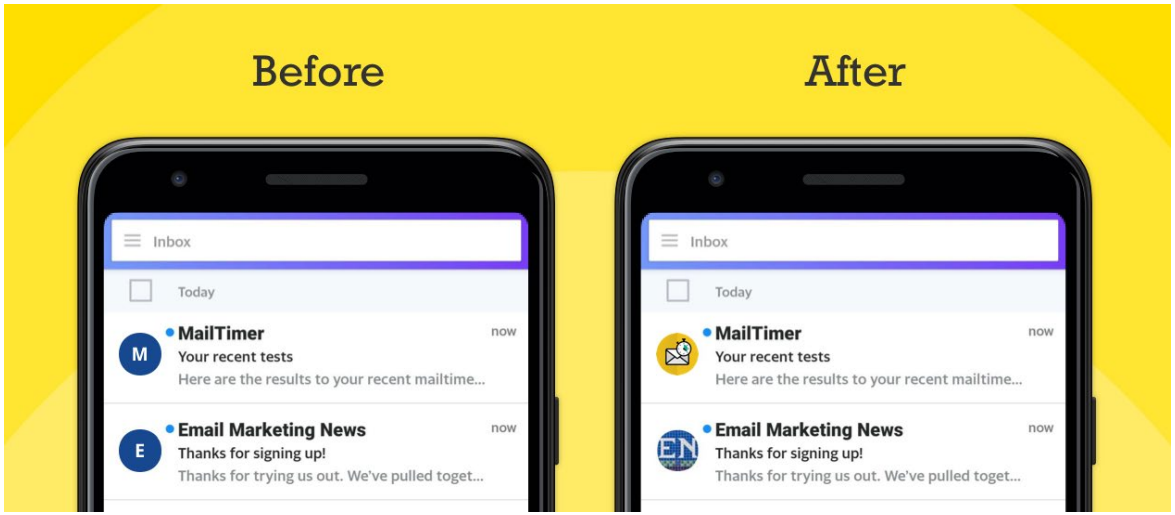
Beheren van domeinnamen en websites (juridisch)



Procedures & geschillen

	.NL	.COM
Inbreuk op Intellectueel Eigendomsrecht	• Geschillenregeling SIDN • Rechter	Uniform Domain Name Dispute Resolution Policy (ICANN.org)
Onrechtmatige Content	• Notice-and-Take-Down-procedure (EU)	Notice-and-Take-Down-procedure (US)
Klacht over Registrar of hoster	• Geschillencommissie	Uniform Domain Name Dispute Resolution Policy (ICANN.org)

Brand Indicators for Message Identification (BIMI)



- Sinds 2020.
- BIMI is een combinatie van e-mail header en DNS TXT-record.
- Met BIMI wordt je logo toegevoegd aan je officiele mail.
- Hiermee kunnen alle ontvangers visueel dat een mail echt van jou is.
- Security- en marketingvoordelen.
- Universeel (niet providerspecifiek)

Nadelen:

- Vergt een geregistreerd EU- of US beeldmerk.
- Vergt Certificaat bij issuer en met tussenkomst notaris (ca. € 1500)

Vragen en opmerkingen

thijs.vandenhout@sidn.nl
michiel.henneke@sidn.nl