

# 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



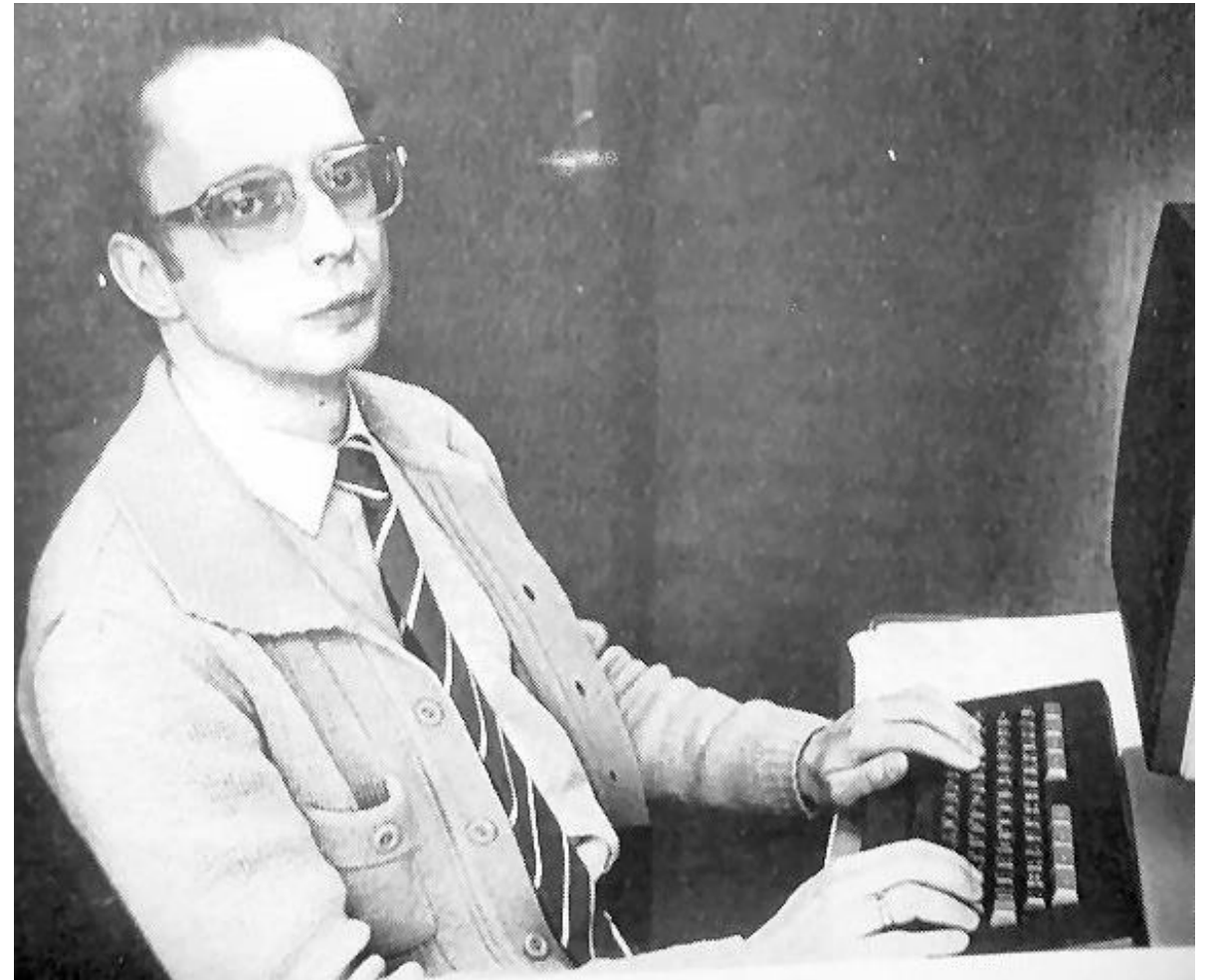
Aanvrager .nl-toppleveldomein  
voor Nederland.



Legde 1ste .nl-domeinnaam vast:  
[cwi.nl](http://cwi.nl) op 30 april 1986.



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



# In 1996 oprichting van SIDN

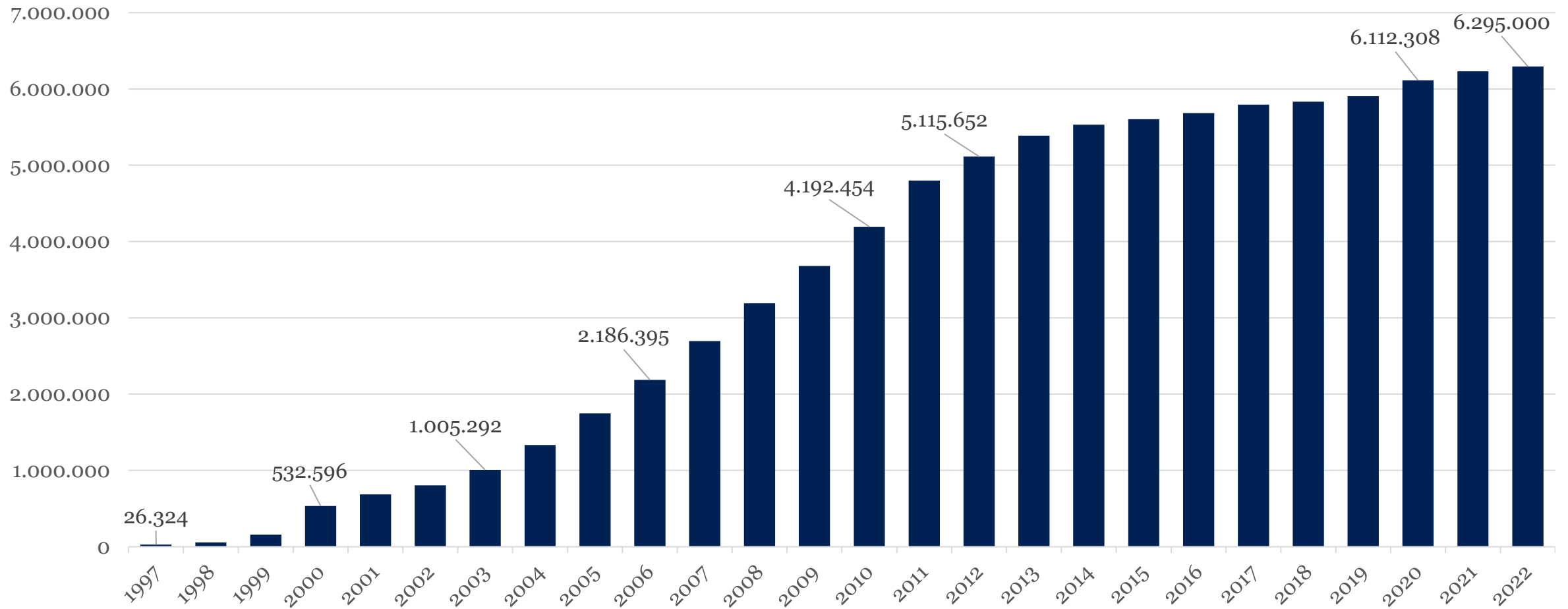


De explosieve groei van .nl vereiste professionalisering.  
In 1996 werd daarom SIDN opgericht:

**De Stichting Internet Domeinregistratie Nederland.**



# Aantal .nl-domeinnamen sinds oprichting



2020



# Wat is SIDN Labs?

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

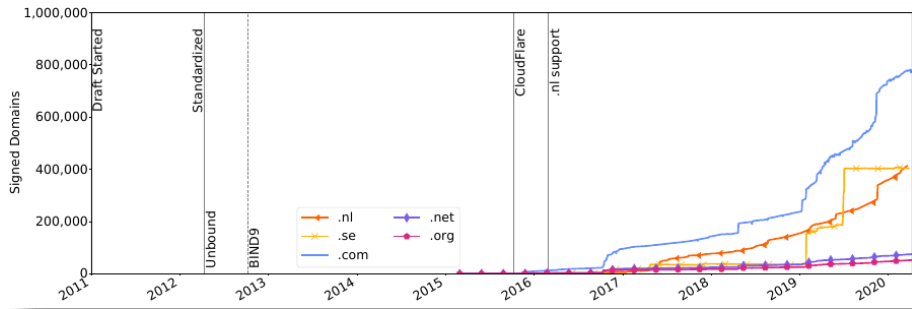


**.nl = the Netherlands**  
~17M inwoners  
6.2M+ domeinnamen  
3.4M DNSSEC-signed  
2.5B DNS queries/dag  
8.6B NTP queries/dag





# Voorbeeld projecten



Measuring the deployment of newly standardized DNSSEC algorithms



Provide well-managed and secure time services

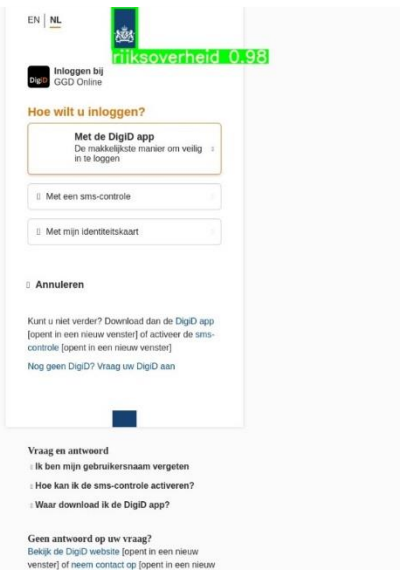
Field	Value
Risk score	90%
Name	Stichting Internet Domeinregistratie Nederland
Address	fake address, 12345AB Randomsterdam, NL
Email	support@sidn.nl
Phone	+31.263525555
Registrar	Stichting Internet Domeinregistratie Nederland
Reseller	-
Registration date	2022-12-07 12:00:00
Name servers	ns5.sidn.nl,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

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

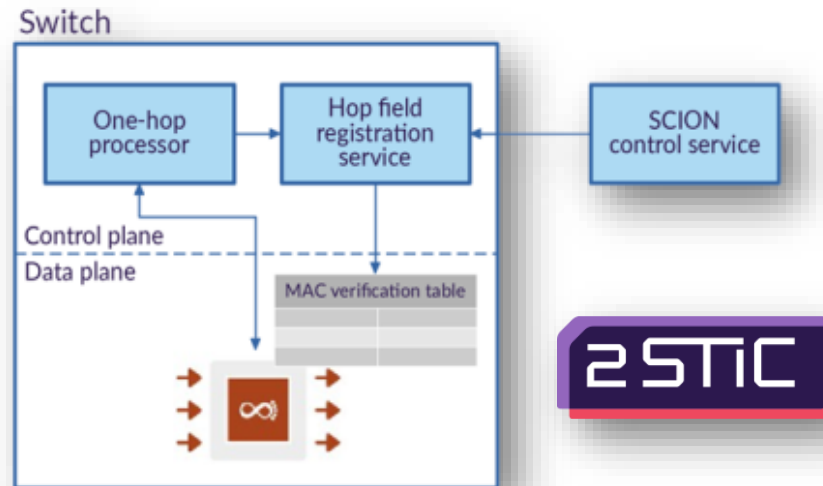
**Label:**  High-risk registration,  Registration invalid

**Status:**  Pending,  Done

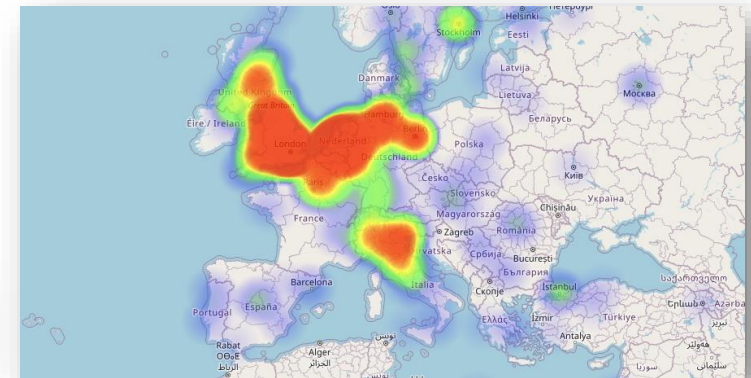
Detecting high-risk domain name registrations



Logo detection technology to identify malicious .nl websites



Experimenting with secure future networks and programmable networks



Optimize anycast routing



# LogoMotive: malafide .nl-domeinen vinden met logodetectie

**Pagina's**

- Home
- Problemen
- Vragen
- Nieuws
- Video's
- Quizen
- Over ons

**Volg ons**

- Facebook
- Twitter
- Instagram
- YouTube
- Vimeo

Privacyverklaring   Cookieverklaring   Responsible disclosure   Disclaimer   Digitoegankelijkheid

Een initiatief van:

**rijksoverheid 0.9**   **rijksoverheid 0.98**

Ministerie van Economische Zaken en Klimaat   Nationaal Cyber Security Centrum Ministerie van Justitie en Veiligheid   ECP Platform voor de InformatieSamenleving

Mede mogelijk gemaakt door:

kpn   **vodafone**   Ziggo   Betaalvereniging Nederland   **sidn 0.97**   SIDN   T-Mobile   Google

Microsoft   **POLITIE**   thuiswinkel **0.95**   thuiswinke.org   SENORWEB   medanportal   SIC

NLdigital   FRAUDEHELPDESK.nl

ACM   ConsuWijzer   Co-financed by the European Union Connecting Europe Facility

veilig internetten.nl

Gedetecteerde logo's met betrouwbaarheid

EN | **NL**

**rijksoverheid 0.98**

Inloggen bij DigiD GGD Online

**Hoe wilt u inloggen?**

**Met de DigiD app**  
De makkelijkste manier om veilig in te loggen

Met een sms-controle

Met mijn identiteitskaart

**Annuleren**

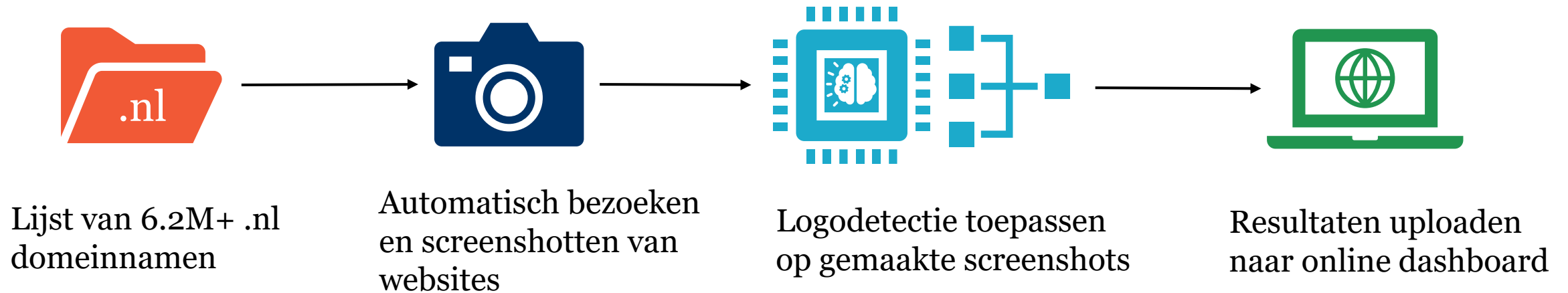
Kunt u niet verder? Download dan de DigiD app [opent in een nieuw venster] of activeer de sms-controle [opent in een nieuw venster]

Nog geen DigiD? Vraag uw DigiD aan

Vraag en antwoord

Ik ben mijn gebruikersnaam vergeten

# Hoe werkt LogoMotive?

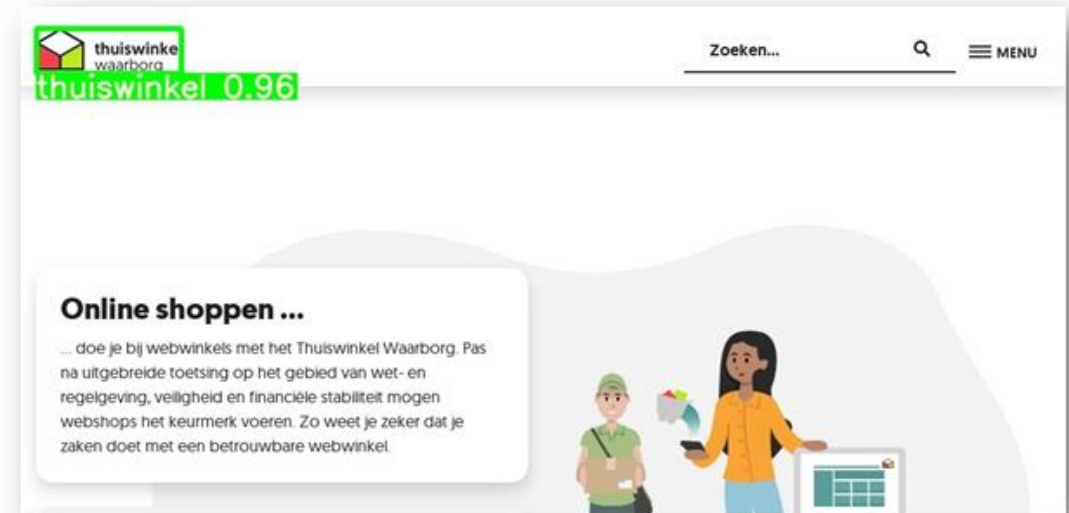




# Twee logodetectie pilots

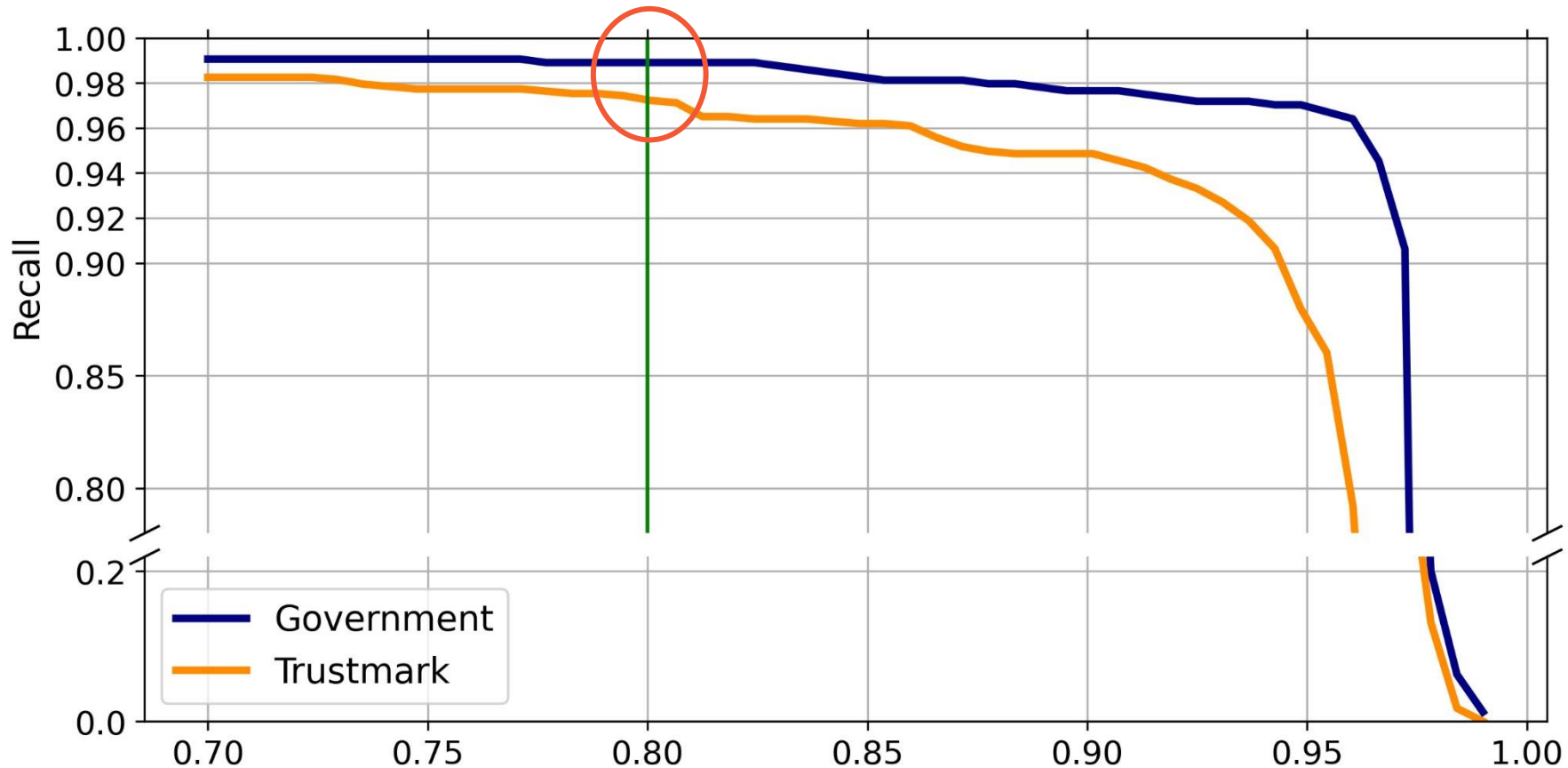
We evalueerden het systeem in twee pilots met toonaangevende partijen op .nl

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



# LogoMotive's recall

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



Confidence threshold

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%)



## 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%)

# Van onderzoek naar productiedienst

- Opstellen onderzoeksvraag
- Ontwikkelfase
- Pilots
- Delen van resultaten ([logomotive.sidnlabs.nl](http://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

[Filters instellen](#)Geselecteerde filters: [Merknaam \*sidn\* x](#)

<input type="checkbox"/>	Domeinnaam 	Wijzigingsdatum 	Detectiedatum 	Classificatie 	Status 	
<input type="checkbox"/>	tompot.nl	08-09-2022 11:24	08-09-2022 11:25	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	tolkonline.nl 	08-09-2022 10:51	08-09-2022 11:05	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	teeners.nl	08-09-2022 05:33	08-09-2022 05:50	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	technicaltrainees.nl	08-09-2022 04:55	08-09-2022 05:50	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	techbelasting.nl	08-09-2022 04:51	08-09-2022 05:50	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	tealovers.nl	08-09-2022 04:31	08-09-2022 05:00	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	tdeled.nl	08-09-2022 04:24	08-09-2022 05:00	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	tca-vloerdecor.nl	08-09-2022 04:11	08-09-2022 05:00	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	t-boothuys.nl	08-09-2022 04:09	08-09-2022 05:00	Onbekend	<span style="color: green;">●</span> Actief	
<input type="checkbox"/>	taxivervoer.nl 	08-09-2022 03:59	08-09-2022 05:00	Onbekend	<span style="color: green;">●</span> 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

Klik op een schermafdruck om in te zoomen.





### Schermafdruck 1




**BESTE WEBHOSTING PAKKETTEN INCL. PLESK CONTROL PANEL MET WORDPRESS TOOLKIT EN +100 ONE CLICK INSTALL CMS SYSTEMEN**

**VEILIGE POP3/IMAP E-MAIL ACCOUNTS INCL. WEBMAIL, SMTP SERVER EN AUTORESPONDERS OP SNELLE EN RUIME RAZENDSNELLE SSD DISKEN**

**EENVOUDIGE CONTROL PANNEL OM UW DNS RECORDS, DOMEINCONTACTEN, WACHTWOORDEN EN E-MAIL INSTELLINGEN TE BEHEREN**

**UNIEK;BEZOEKERS STATISTIEKEN, ONE-PAGER PARKEERPAGINA MET DIVERSE TEMPLATES EN GRATIS SSL VOOR ALLE GEREgistreERDE DOMEINEN**

**VERHUIZEN WEBSITE EN .NL DOMEINNAMEN**

Domainnaam **tompot.nl** al vastgelegd in opdracht van een klant.

U kunt deze domeinnaam helaas niet meer registreren, in plaats van de .nl versie van deze domein kunt u via de onderstaande domein check tool controleren of er andere domeinextensies voor "tompot" beschikbaar zijn.

**tompot**

**DomeinHost**

Ervaren en deskundige website hoster sinds 1999

DomeinHost, een onderdeel van InterIP Networks BV, is sinds 1999 actief met het bieden van webhosting, managed servers en domeinregistratie diensten van hoge kwaliteit. Wij hebben een garanteerde klantentevredenheid verspreid over heel Nederland die positief uit kijkt op wereldwijd lonenarbeidende bedrijven. Ook als particulier of ZZP'er bent u bij ons bij het juiste adres. Onze helpdesk medewerkers zijn uiterst behulpzaam en helpen u graag met al uw webhosting, e-mail en overige technische vragen. Lees hier de [levenden reacties](#) van onze klanten en wordt ook snel klant bij de beste en meest ervaren webhosting provider van heel Nederland.

**Sinds 1999**

**Contact**

Adres:  
 Industriestraat 11  
 2611 CT NAALDWIJK

email:  
 sales@domeinhost.nl

Telefoon:  
 31 (0)174-726026

✕ Sluiten

### Schermafdruck 2

**BESTE WORDPRESS WEBHOSTING PAKKETTEN INCL. PLESK CONTROL PANEL MET WORDPRESS TOOLKIT EN +100 ONE CLICK INSTALL CMS SYSTEMEN**

**BESTE MAIL EN DOMEIN PAKKETTEN MET 1 GB MAILBOX RUIMTE - €35,00**

**RAZENDSNELLE VIRTUELE SERVERS (20 GB OPSLAG + 16 TB TOT MAX. CORES + 32 GB) €325,00**

**AFZAKERS DOMEINNAAM REGISTREREN ACTIEVE DOMEINEN**















**VERHUIZEN WEBSITE EN .NL DOMEINNAMEN**

Domainnaam **tompot.nl** al vastgelegd in opdracht van een klant.

**DomeinHost**

Ervaren en deskundige website hoster sinds 1999

**Contact**

Adres:  
 Industriestraat 11  
 2611 CT NAALDWIJK

# Aandachtspunten

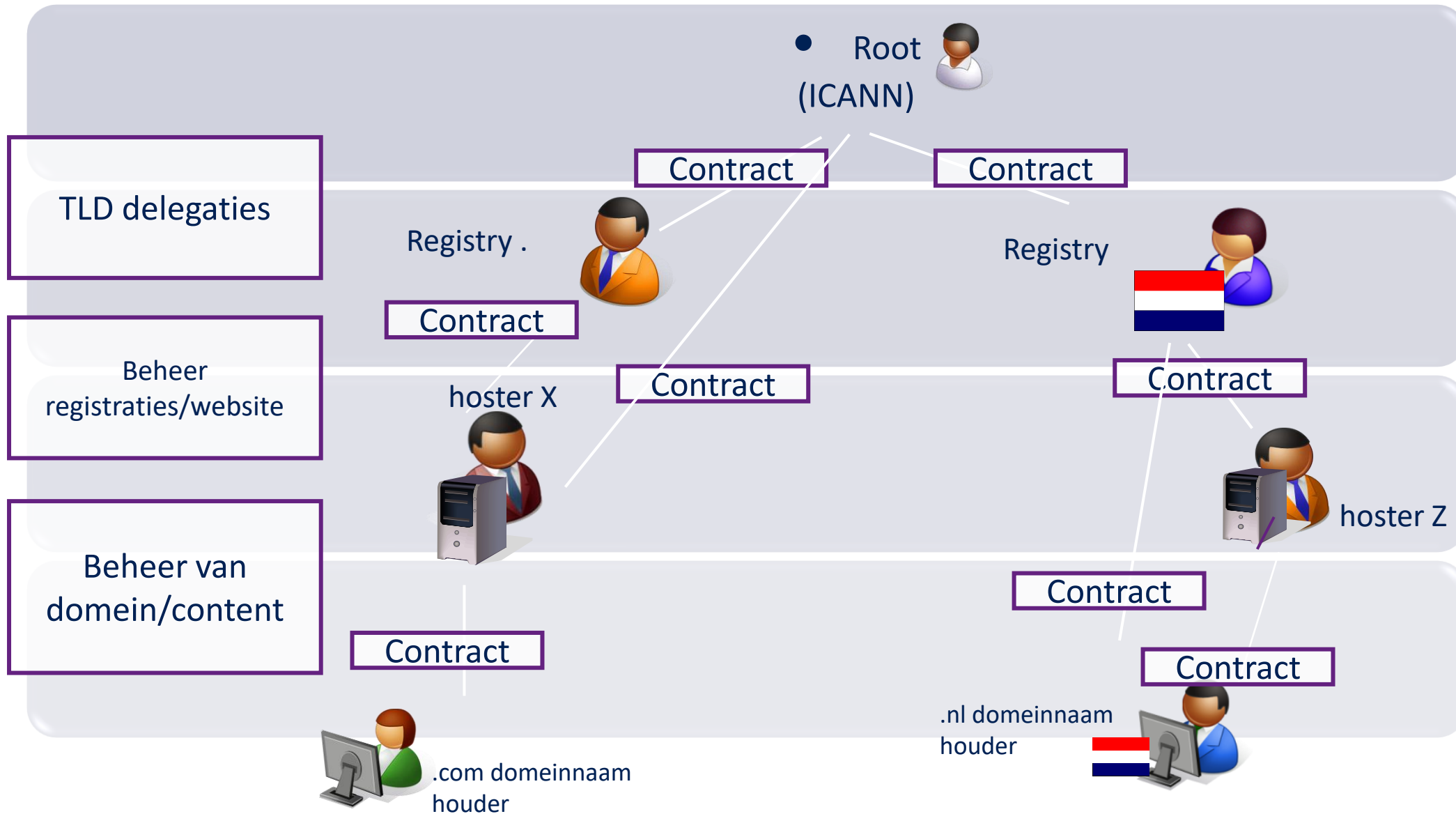
- Niet ieder logo is goed te onderscheiden. Machine Learning en negeerlijst nodig.
- Niet iedere rechthebbende heeft een goede lijst van legitieme sites (VB. iDEAL).



Online betalen  
via uw eigen bank

# Opvolging: van detectie naar acties

# Beheren van domeinnamen en websites (juridisch)

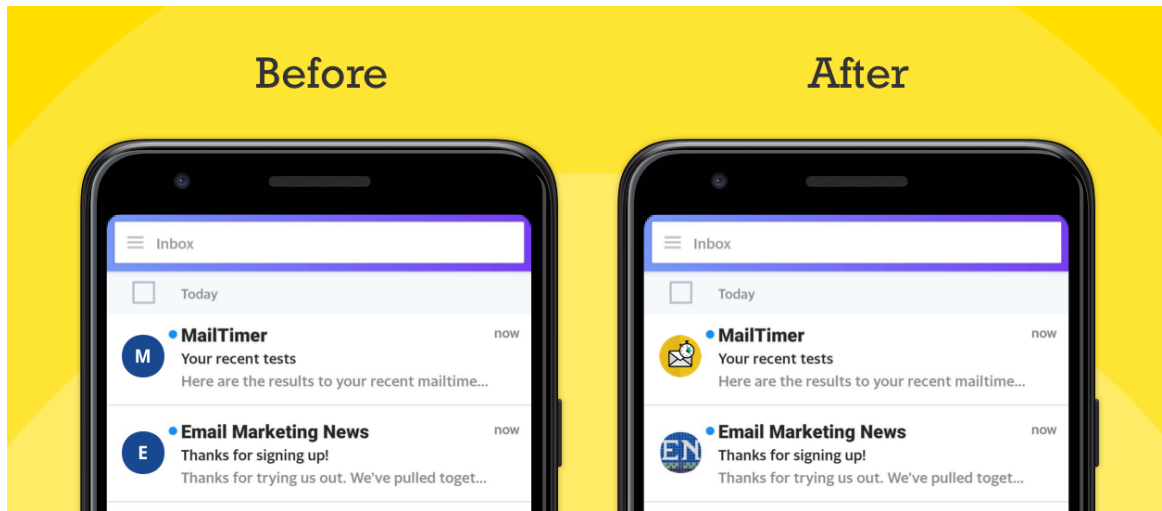


# Procedures & geschillen

	.NL	.COM
<b>Inbreuk op Intellectueel Eigendomsrecht</b>	<ul style="list-style-type: none"><li>• Geschillenregeling SIDN</li><li>• Rechter</li></ul>	Uniform Domain Name Dispute Resolution Policy (ICANN.org)
<b>Onrechtmatige Content</b>	<ul style="list-style-type: none"><li>• Notice-and-Take-Down-procedure (EU)</li></ul>	Notice-and-Take-Down-procedure (US)
<b>Klacht over Registrar of hoster</b>	<ul style="list-style-type: none"><li>• Geschillencommissie</li></ul>	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 officiële 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](mailto:thijs.vandenhout@sidn.nl)  
[michiel.henneke@sidn.nl](mailto:michiel.henneke@sidn.nl)

