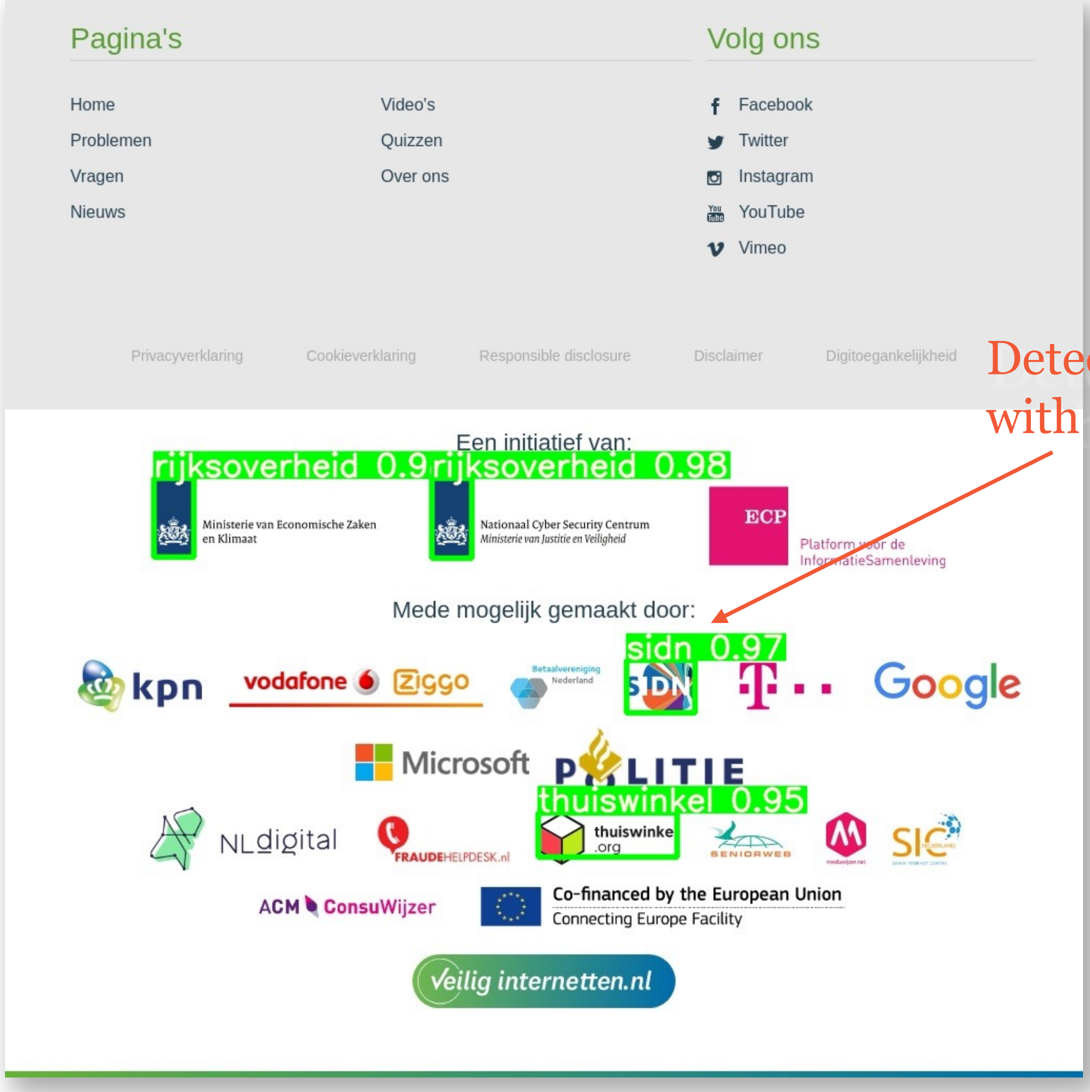
# LogoMotive: detecting logos on websites to identify online scams - a TLD case study

Thijs van den Hout | PAM 2022

# LogoMotive: finding malicious .nl-domains with logo detection



Pagina's

| | |
|---|---|
| Home | Video's |
| Problemen | Quizzen |
| Vragen | Over ons |
| Nieuws | |

Volg ons

- Facebook
- Twitter
- Instagram
- YouTube
- Vimeo

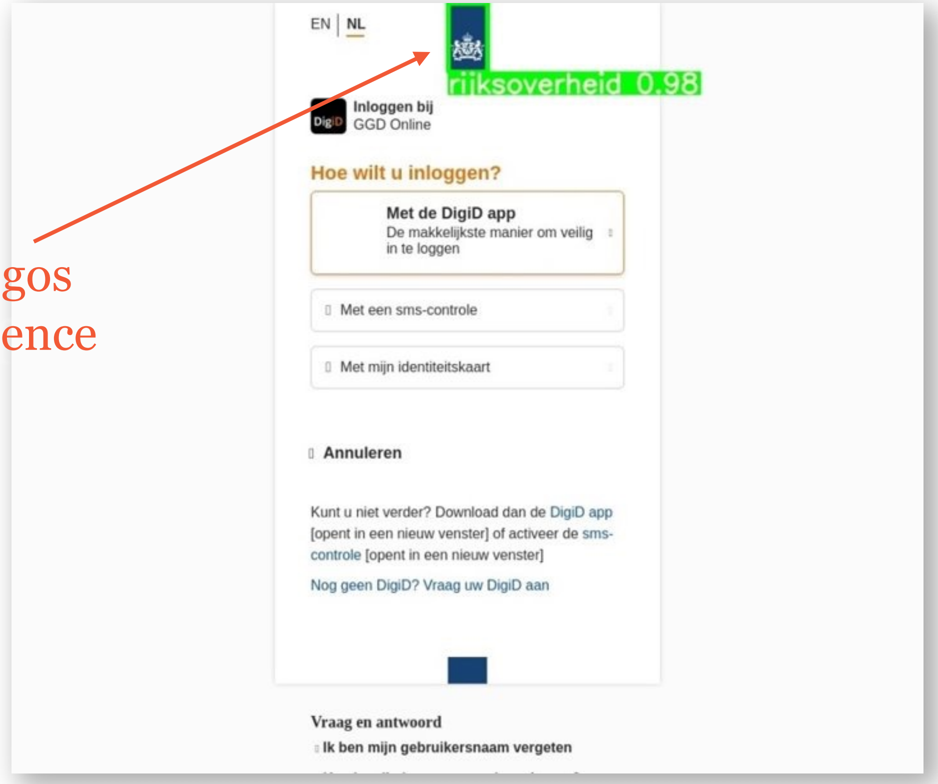
Privacyverklaring Cookieverklaring Responsible disclosure Disclaimer Digitoegankelijkheid

Een initiatief van:

Mede mogelijk gemaakt door:

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
sidn 0.97
kpn
vodafone
Ziggo
Betaalvereniging Nederland
SIDN
Google
Microsoft
POLITIE
thuiswinkel 0.95
NLdigital
FRAUDEHELPDESK.nl
thuiswinkel.org
SENIORWEB
SIC
ACM ConsuWijzer
Co-financed by the European Union
Connecting Europe Facility
Veilig internetten.nl

Detected logos with confidence



EN | NL

Inloggen bij 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

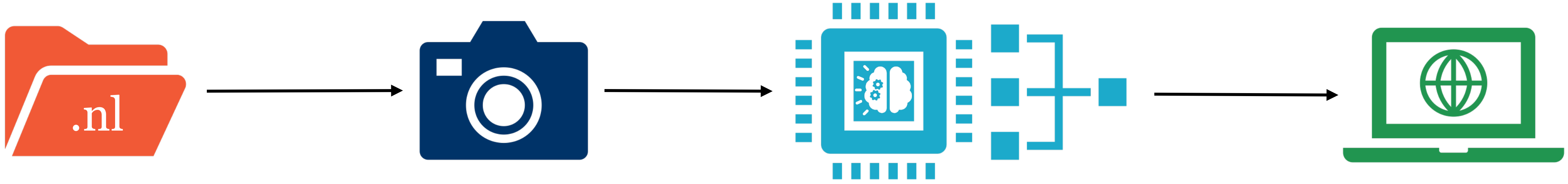
Kunt u niet verder? Download dan de DigiD app [opent in een nieuw venster] of activeer de sms-controle [opent in een nieuw venster]

Nog geen DigiD? Vraag uw DigiD aan

Vraag en antwoord

Ik ben mijn gebruikersnaam vergeten

# How does LogoMotive work?



List of 6.2M+ .nl domain names

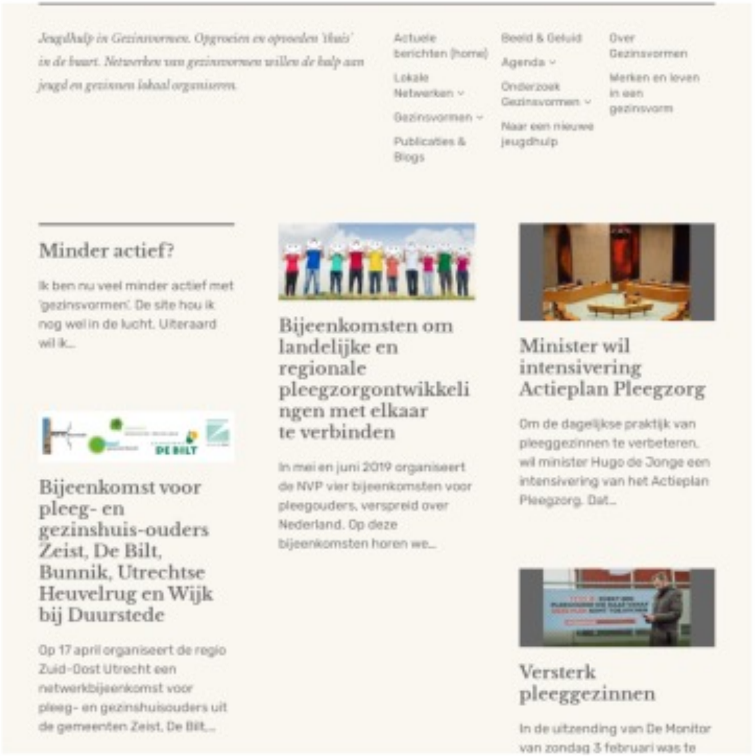
Automatically visit and screenshot websites

Apply logo detection to the screenshots

Upload results to online dashboard

# Automatic training data generation

+



*Jeugdhulp in Gezinsvormen. Opgroeien en opvoeden 'thuis' in de buurt. Netwerken van gezinsvormen willen de hulp aan jeugd en gezinnen lokaal organiseren.*

Minder actief?

Ik ben nu veel minder actief met 'gezinsvormen'. De site hou ik nog wel in de lucht. Uiteraard wil ik...

Bijeenkomst voor pleeg- en gezinshuis-ouders Zeist, De Bilt, Bunnik, Utrechtse Heuvelrug en Wijk bij Duurstede

Op 17 april organiseert de regio Zuid-Oost Utrecht een netwerkbijeenkomst voor pleeg- en gezinshuisouders uit de gemeenten Zeist, De Bilt,...

Bijeenkomsten om landelijke en regionale pleegzorgontwikkelingen met elkaar te verbinden

In mei en juni 2019 organiseert de NVP vier bijeenkomsten voor pleegouders, verspreid over Nederland. Op deze bijeenkomsten horen we...

Minister wil intensivering Actieplan Pleegzorg

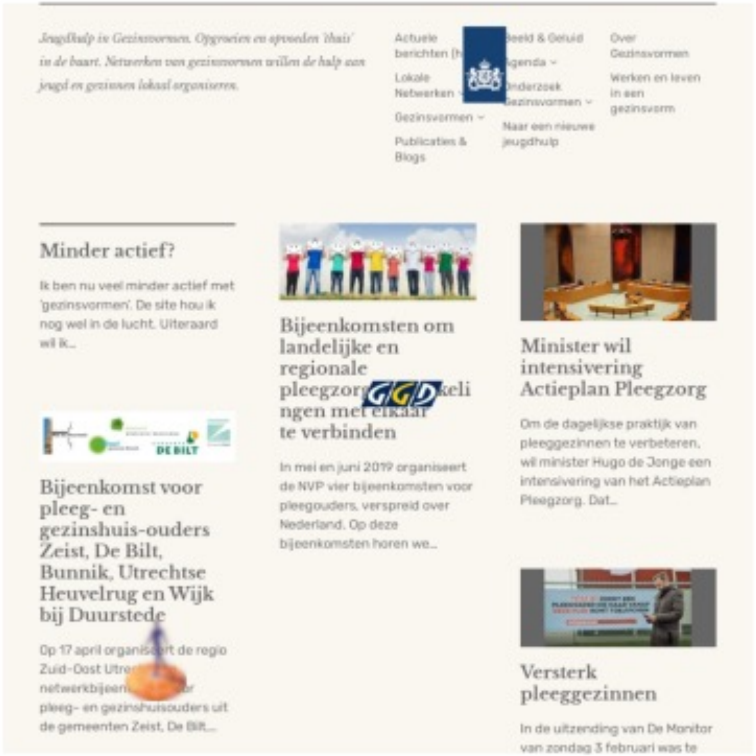
Om de dagelijkse praktijk van pleeggezinnen te verbeteren, wil minister Hugo de Jonge een intensivering van het Actieplan Pleegzorg. Dat...

Versterk pleeggezinnen

In de uitzending van De Monitor van zondag 3 februari was te

Random screenshot

=



*Jeugdhulp in Gezinsvormen. Opgroeien en opvoeden 'thuis' in de buurt. Netwerken van gezinsvormen willen de hulp aan jeugd en gezinnen lokaal organiseren.*

Minder actief?

Ik ben nu veel minder actief met 'gezinsvormen'. De site hou ik nog wel in de lucht. Uiteraard wil ik...

Bijeenkomst voor pleeg- en gezinshuis-ouders Zeist, De Bilt, Bunnik, Utrechtse Heuvelrug en Wijk bij Duurstede

Op 17 april organiseert de regio Zuid-Oost Utrecht een netwerkbijeenkomst voor pleeg- en gezinshuisouders uit de gemeenten Zeist, De Bilt,...

Bijeenkomsten om landelijke en regionale pleegzorgontwikkelingen met elkaar te verbinden

In mei en juni 2019 organiseert de NVP vier bijeenkomsten voor pleegouders, verspreid over Nederland. Op deze bijeenkomsten horen we...

Minister wil intensivering Actieplan Pleegzorg

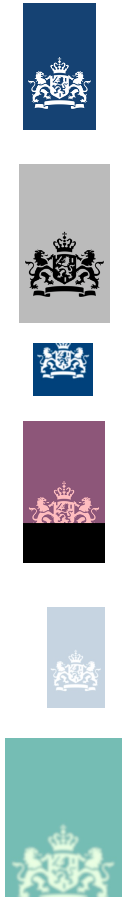
Om de dagelijkse praktijk van pleeggezinnen te verbeteren, wil minister Hugo de Jonge een intensivering van het Actieplan Pleegzorg. Dat...

Versterk pleeggezinnen

In de uitzending van De Monitor van zondag 3 februari was te

Resulting datapoint

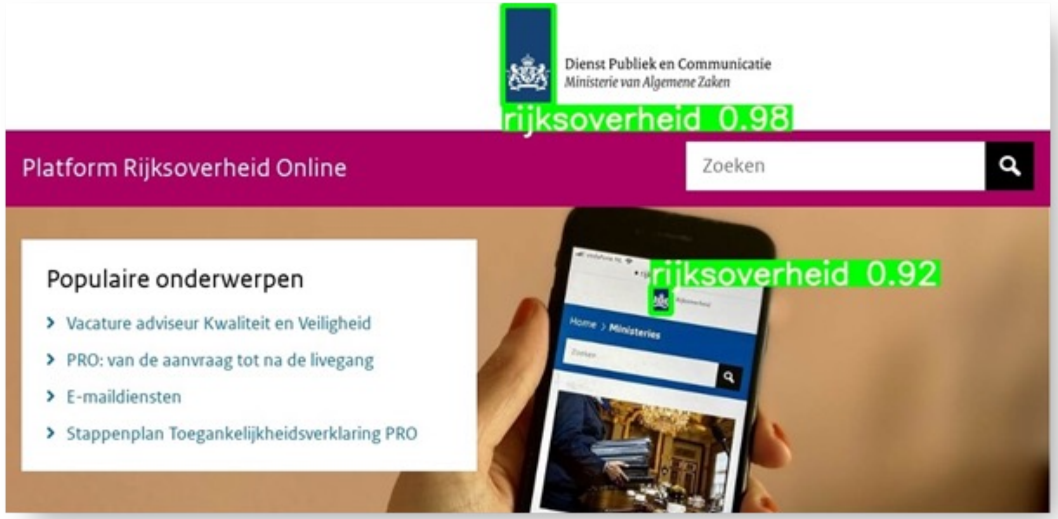
Example Augmentations:



# Evaluation in practice

Two pilots with distinguished organizations in **.nl**

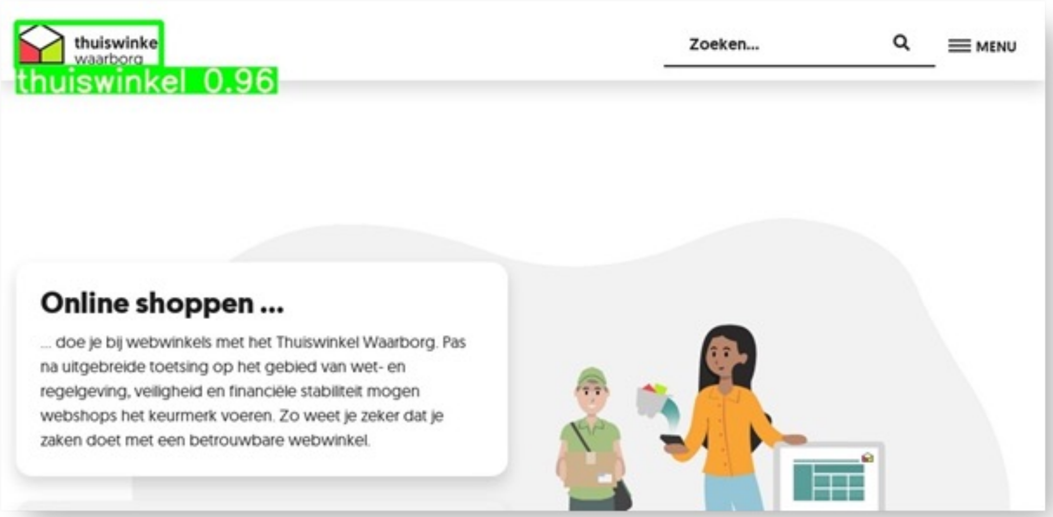
- Dutch National Government
  - 11.700 domain names
- Webshop Trustmark
  - 10.600 domain names



Platform Rijksoverheid Online

Populaire onderwerpen

- Vacature adviseur Kwaliteit en Veiligheid
- PRO: van de aanvraag tot na de livegang
- E-maildiensten
- Stappenplan Toegankelijkheidsverklaring PRO

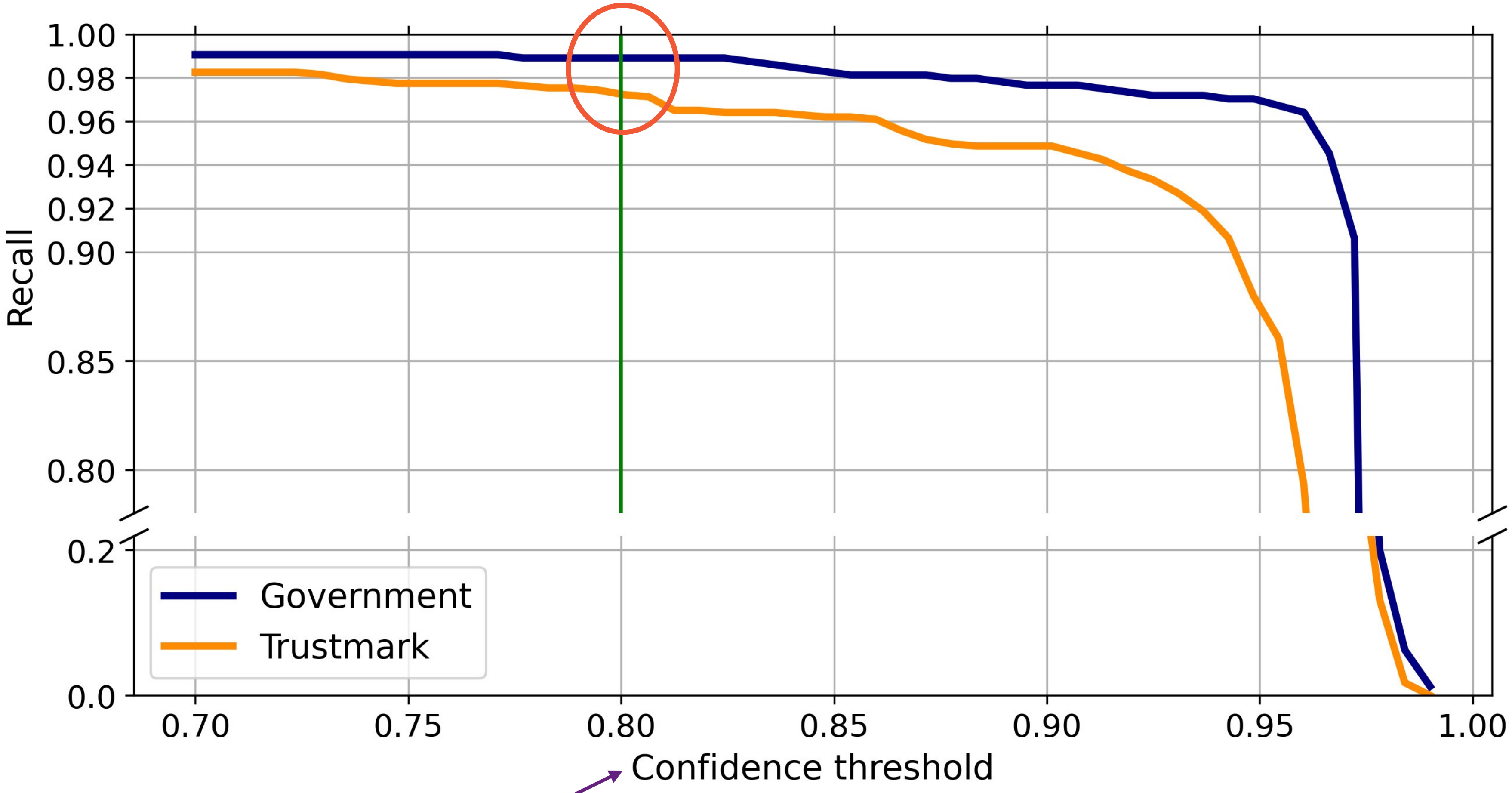


**Online shoppen ...**

... doe je bij webwinkels met het Thuiswinkel Waarborg. Pas na uitgebreide toetsing op het gebied van wet- en regelgeving, veiligheid en financiële stabiliteit mogen webshops het keurmerk voeren. Zo weet je zeker dat je zaken doet met een betrouwbare webwinkel.

# LogoMotive's recall

- Recall = fraction of websites with logos that are succesfully detected



The model must be this confident
before labeling a logo as such

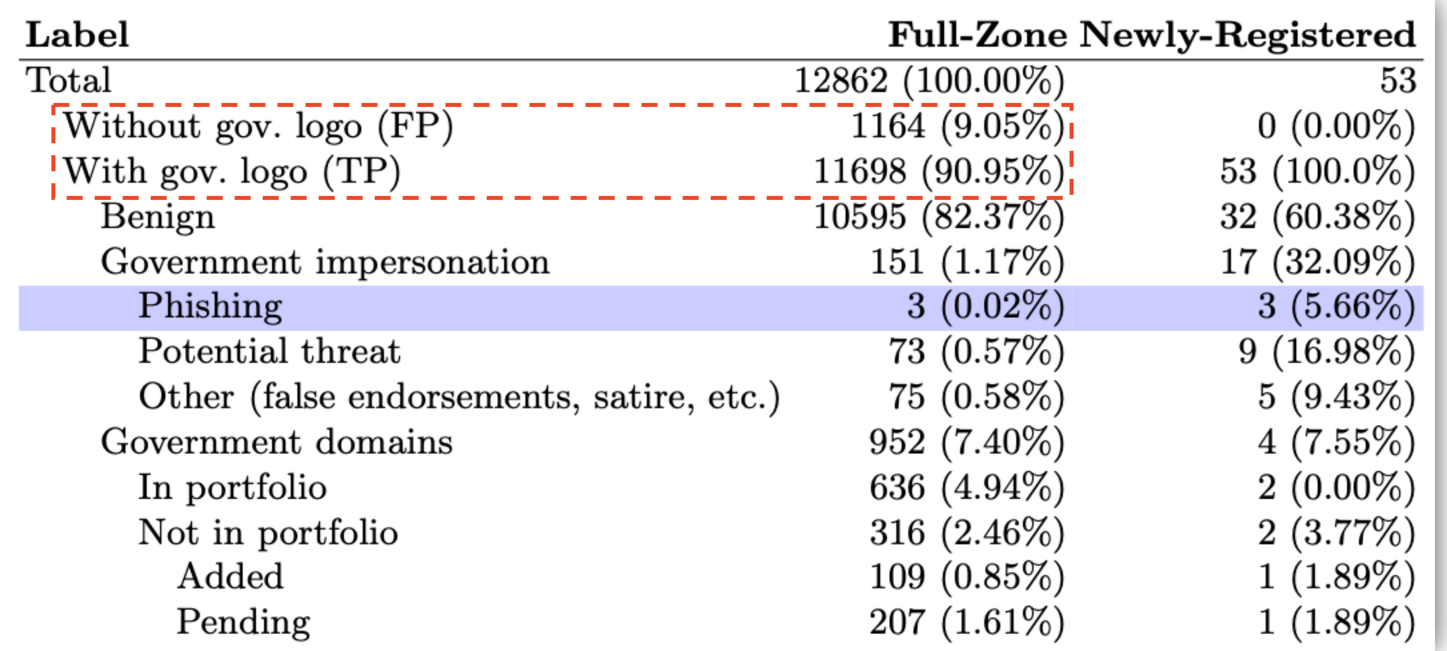
# Our insights and contributions

1. Logo detection can help find malicious websites

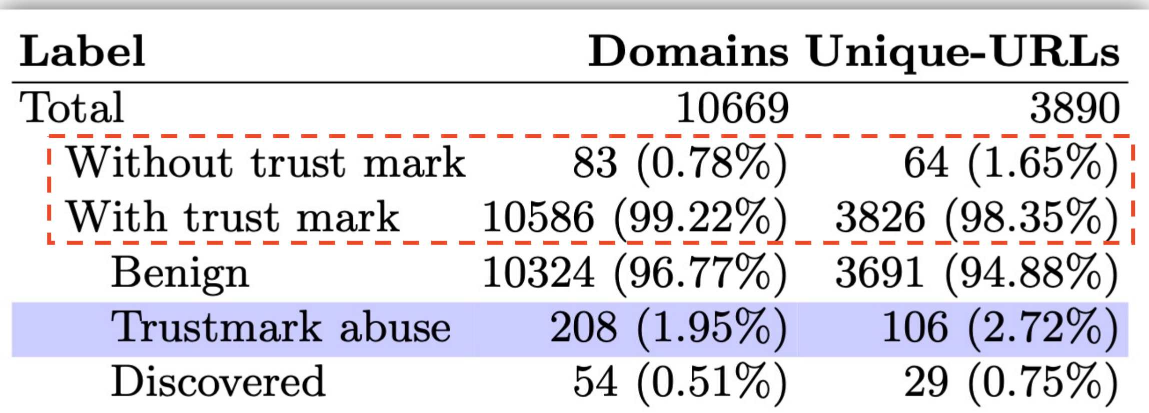
2. Logo detection reveals spear-phishing and other dormant risks

3. Logo detection can help complete domain name portfolios

# 1. LogoMotive finds malicious websites



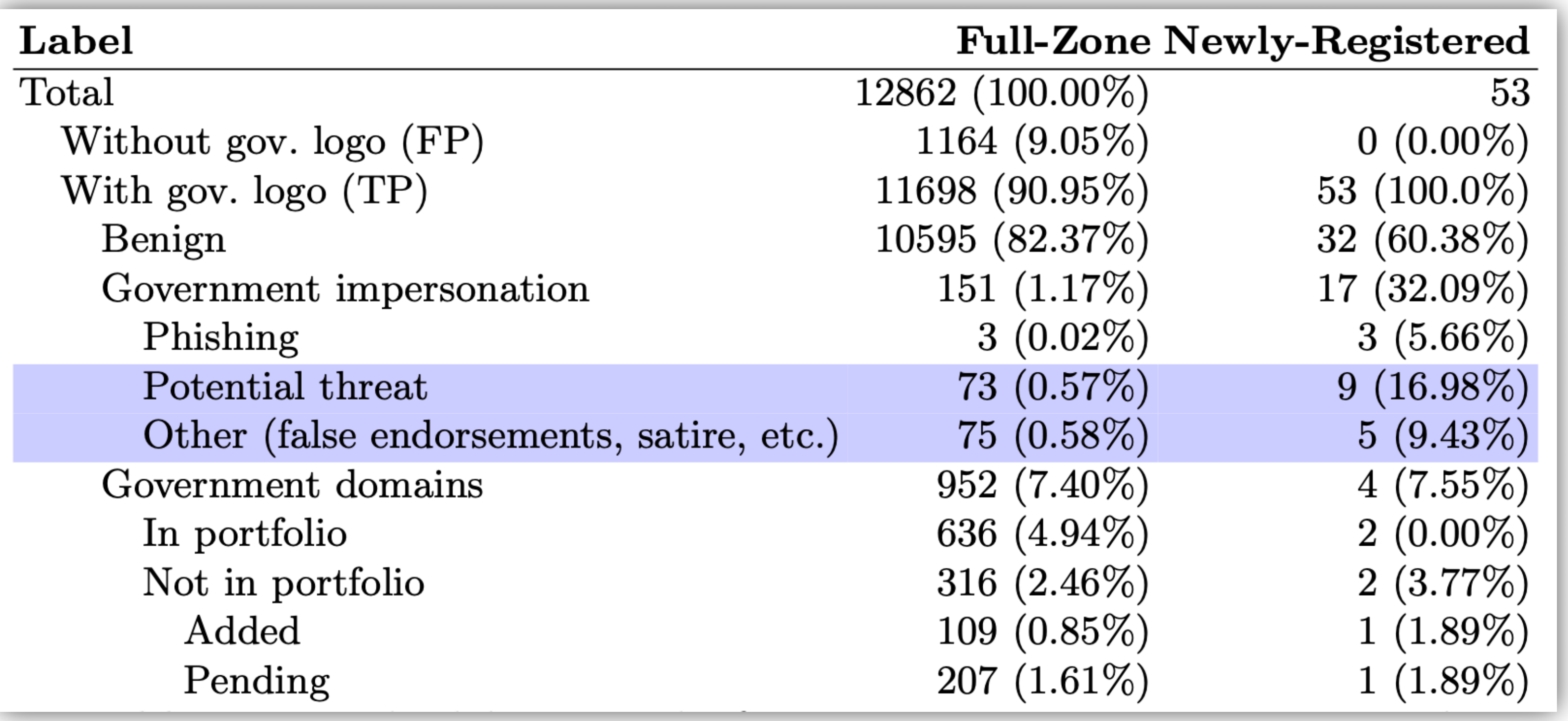
| Label | Full-Zone | Newly-Registered |
|---|---|---|
| Total | 12862 (100.00%) | 53 |
| Without gov. logo (FP) | 1164 (9.05%) | 0 (0.00%) |
| With gov. logo (TP) | 11698 (90.95%) | 53 (100.0%) |
| Benign | 10595 (82.37%) | 32 (60.38%) |
| Government impersonation | 151 (1.17%) | 17 (32.09%) |
| Phishing | 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%) |



| 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%) |

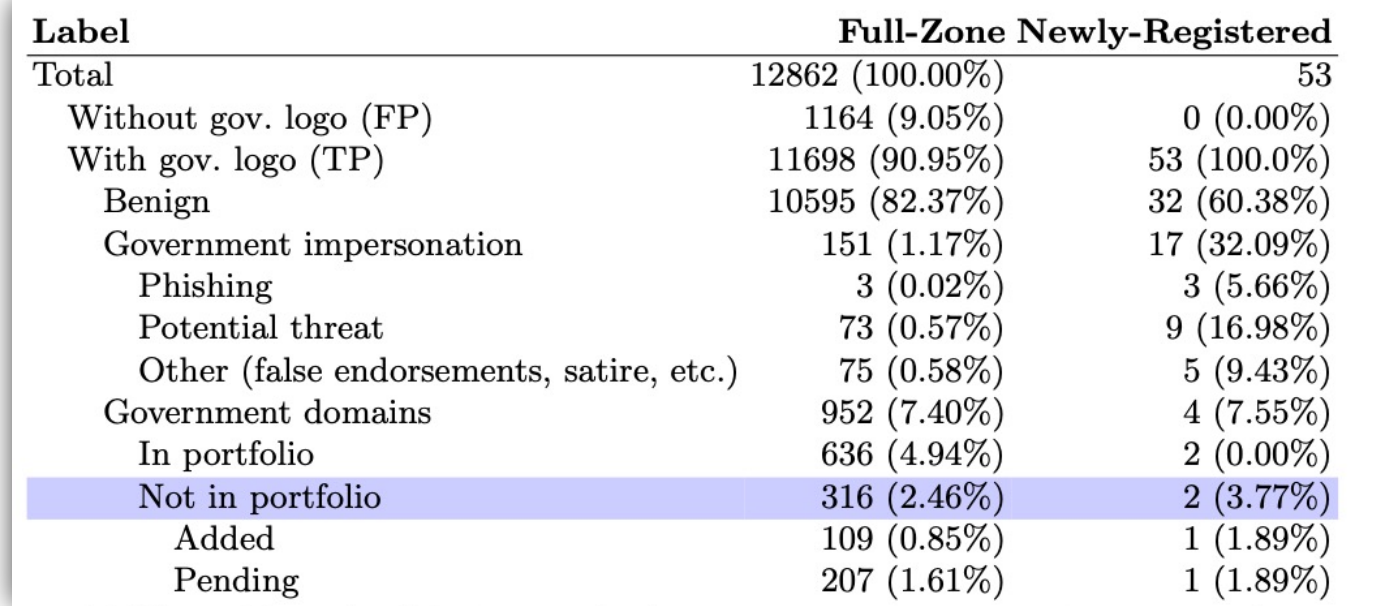
# 2. Spear-phishing and suspicious redirects

- govenrment.nl → HTTP redirect → government.nl
- Spear-phishing: targeted at specific employees
- Malicious email traffic from typosquat domain names

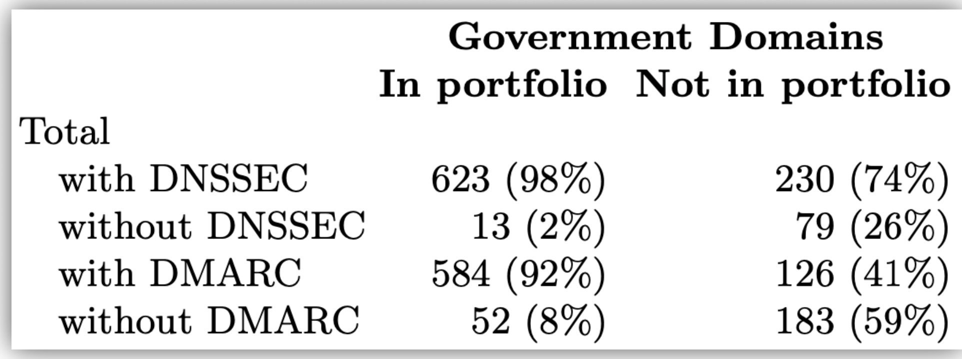


| Label | Full-Zone | Newly-Registered |
|---|---|---|
| Total | 12862 (100.00%) | 53 |
| Without gov. logo (FP) | 1164 (9.05%) | 0 (0.00%) |
| With gov. logo (TP) | 11698 (90.95%) | 53 (100.0%) |
| Benign | 10595 (82.37%) | 32 (60.38%) |
| Government impersonation | 151 (1.17%) | 17 (32.09%) |
| Phishing | 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%) |

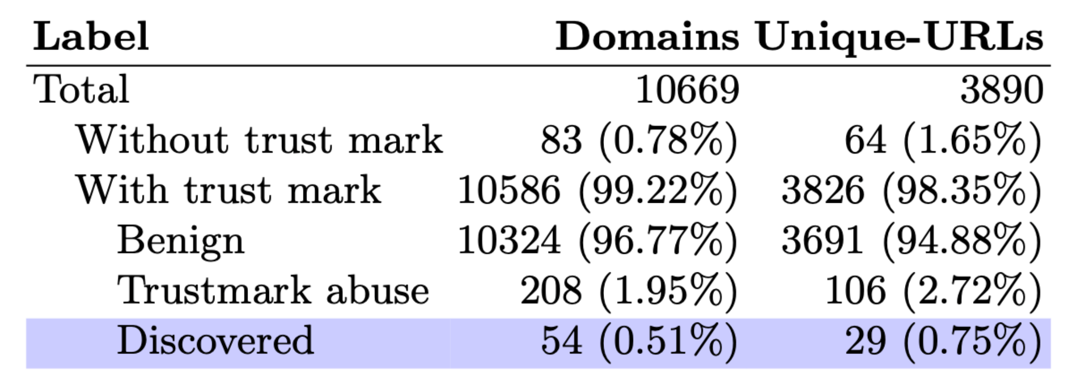
# 3. Complete domain name portfolios



| 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%) |

# Conclusions and future plans

- Pilots show added value of logo detection in tackling malicious content
- Implementation in SIDN BrandGuard
- Source code for academics and other registries
- Future research:
  - Prioritization of results
  - More than just the home-page

# Questions?

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