

LogoMotive, Merkbewaking & Domeinportfoliochecker

Thymen Wabeke, Pim Pastoors | BID-overleg

11 januari 2022



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



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)

LogoMotive: malafide .nl-domeinen vinden met logo detectie

Pagina's

- Home
- Problemen
- Vragen
- Nieuws

Video's

- Video's
- Quizen
- Over ons

Volg ons

- Facebook
- Twitter
- Instagram
- YouTube
- Vimeo

Privacyverklaring Cookieverklaring Responsible disclosure Disclaimer Digtogankelijkheid

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...
- Google
- Microsoft
- NLdigital
- FRAUDEHELPDESK.nl
- thuiswinkel 0.95
- thuiswinke.org
- SENIORWEB
- SIC
- ACM ConsuWijzer
- Co-financed by the European Union Connecting Europe Facility
- veilig internetten.nl

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en
rijksoverheid 0.98

Home

Direct naar

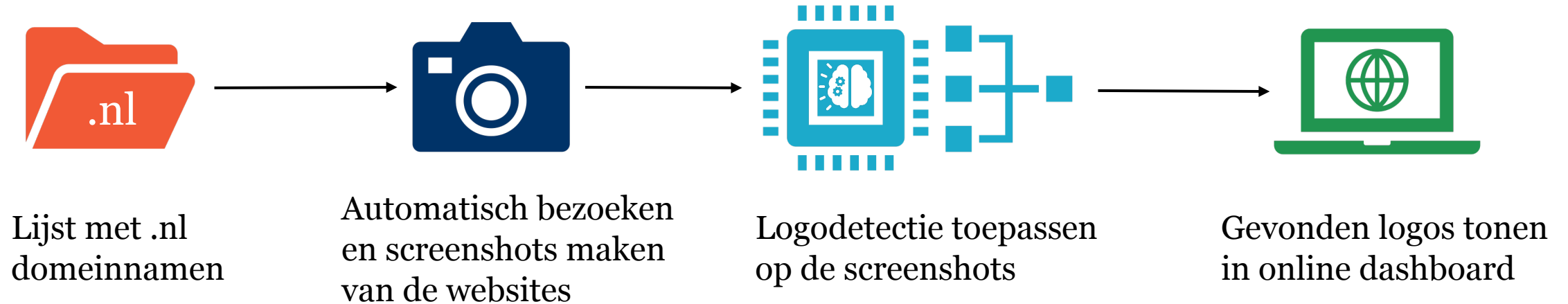
- > Jaarverslag 2020
- > Veiligheidsonderzoeken
- > Cyberdreiging
- > Vacatures bij de AIVD

rijksoverheid 0.89

Actueel Organisatie Documenten

Het laatste nieuws en actuele Over de AIVD Publicaties, Kamerstukken en

Hoe werkt LogoMotive?



Online dashboard

The dashboard features a navigation bar with 'SIDN LABS', 'LOGOMOTIVE', and 'SIDN'. It includes filter and bulk update sections, and a main table of found logos.

Filter

Label: All
Status: All
Filter

Bulk update

Label: Select
Status: Select
Update

Logo's found

Show 10 entries Select All Search:

Domain name	Screenshot date	Registrar	Registrant	Registered on	Label	Status	
laatdelinksliggen.nl	2021-10-04 04:07				-	Open	Annotate
hostinghero.nl	2021-09-27 09:43				-	Open	Annotate
webrestyle.nl	2021-09-27 09:43				-	Open	Annotate
studioactive.nl	2021-09-27 09:43				-	Open	Annotate
hostingu2.nl	2021-09-27 09:35				-	Open	Annotate
easyrek.nl	2021-09-27 09:28				-	Open	Annotate
houten-legbordstelling.nl	2021-09-27 09:28				-	Open	Annotate
coronakantoorinrichting.nl	2021-09-27 08:57				-	Open	Annotate
dutchantiddoscoalition.nl	2021-09-27 08:56				-	Open	Annotate
nomoredos.nl	2021-09-27 08:56				-	Open	Annotate

Showing 1 to 10 of 722 entries

Previous 1 2 3 4 5 ... 73 Next

Logo found on laatdelinksliggen.nl

Screenshot date: 04-10-2021 04:07

Page also found on: veiliginternetten.nl, digivaardigdigiveilig.nl, checkjeupdates.nl, maakhetniettemakkelijk.nl, doejouupdates.nl, digibewust.nl, cloudbewust.nl, doejeupdates.nl, digivaardigdigibewust.nl, jewachtwoord.nl, beschermjebedrijf.nl, internettenveilig.nl

Registrant: Stichting ECP

Registrar: team.blue nl B.V.

Registration date: 24-09-2021 00:00

Screenshots

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:

- Ministerie van Economische Zaken en Klimaat
- Nationaal Cyber Security Centrum
- ECP

Mede mogelijk gemaakt door:

- kpn, vodafone, Ziggo, sidn 0.97, Google
- Microsoft, POLITIE
- NLdigital, FRAUDEBUDESK.nl, thuiswinkel.org, SIE
- AGM ConsuWijzer, Co-financed by the European Union

Veilig internetten.nl

Comment

Clear label Previous

Comment...

Label

- Correct use
- Incorrect use
- Geen logo

Status

- Open
- In behandeling
- Afgehandeld

Save and update all related domains Save and next Save and exit



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

EN | NL


Rijksoverheid 0.98

 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

Hoe kan ik de sms-controle activeren?

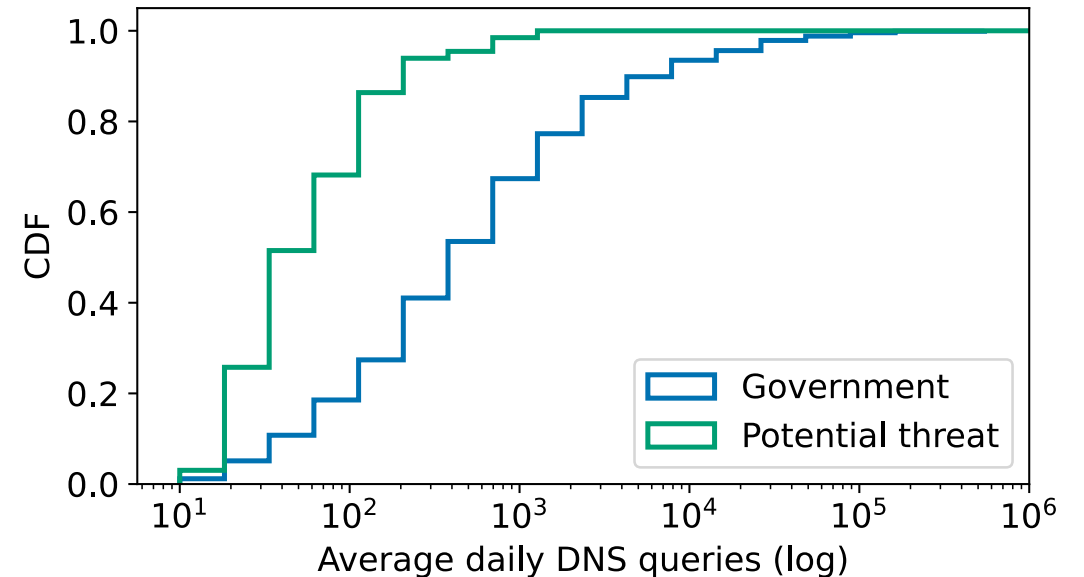
Waar download ik de DigiD app?

Geen antwoord op uw vraag?
[Bekijk de DigiD website](#) [opent in een nieuw venster] of [neem contact op](#) [opent in een nieuw venster]

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

