


# Fake webshop-bestrijding

## Detectie en bestrijding van frauduleuze webshops

Gepubliceerd bij PAM2020: [https://doi.org/10.1007/978-3-030-44081-7\\_10](https://doi.org/10.1007/978-3-030-44081-7_10)



**HOLLISTER** Dames Heren Inloggen | Register | (0) Omschrijving




★★★★

Hollister Ondergoed Heren Lage Taille Multipack Grijs Groen Camo Zwart 11859-FNX

15 Kleur **BROEK & KORTE BROEK**

~~€30.60~~ **€22.31**




★★★★★

Hollister T Shirt Heren Logo Graphic Korte Mouwen Donkerblauw 21170-HLT

15 Kleur **TOPS**

~~€30.70~~ **€22.38**




★★★★★

Hollister Jas Dames All-weather Stretch Sherpa-lined Zwart 45801-GXL

1 Kleur **JASSEN**

~~€98.35~~ **€69.73**




★★★★★

Hollister Joggingbroek Heren Advanced Stretch Cargo Twill Olijfgroen 97393-SXN

4 Kleur **BROEK & KORTE BROEK**

~~€50.11~~ **€35.98**




★★★★


Hollister Blouses Dames Fluweel Off-the-shoulder Goud 49289-JQI

2 Kleur **TOPS**


~~€30.60~~ **€22.31**




★★★★




★★★★★



★★★★



★★★★



★★★★

# Beleefbaantjer.nl

2017 Super Populair Schoener x  
www.beleefbaantjer.nl

Inloggen Registratie Euro


Winkelwagen: 0 items Zoektermen...

Home Dames Jurken Dames Schoenen Heren Truien Accessoires Contact







**Categorie**

- ▶ Accessoires->
- ▶ Dames Jurken->
- ▶ Dames Rokken->
- ▶ Dames Schoenen->
- ▶ Dames Shirts->
- ▶ Dames Truien->
- ▶ Heren Overhemden->
- ▶ Heren Schoenen->
- ▶ Heren Shirts->
- ▶ Heren Truien->

**Nieuw in ons assortiment [lees meer]**



**Nieuwe artikelen voor juli**

 <p>Beste Online Prijs Liu Jo Jurk Divers Dames Outlet Online J3b6blzE <del>€78.49</del> €44.29 Korting: 44%</p>	 <p>Extra Uitverkoop Liu Jo Army dress Groen Dames Laagste Prijs Op G2GwgCLw <del>€99.70</del> €47.00 Korting: 53%</p>	 <p>Een Goedkope Prijs Marjoly Paris zwarte jurk met kanten mouw Zwart Dames Allemaal Te Koop 6jcx1YZO <del>€121.75</del> €41.55 Korting: 66%</p>
		

# watzullenwijeten.nl

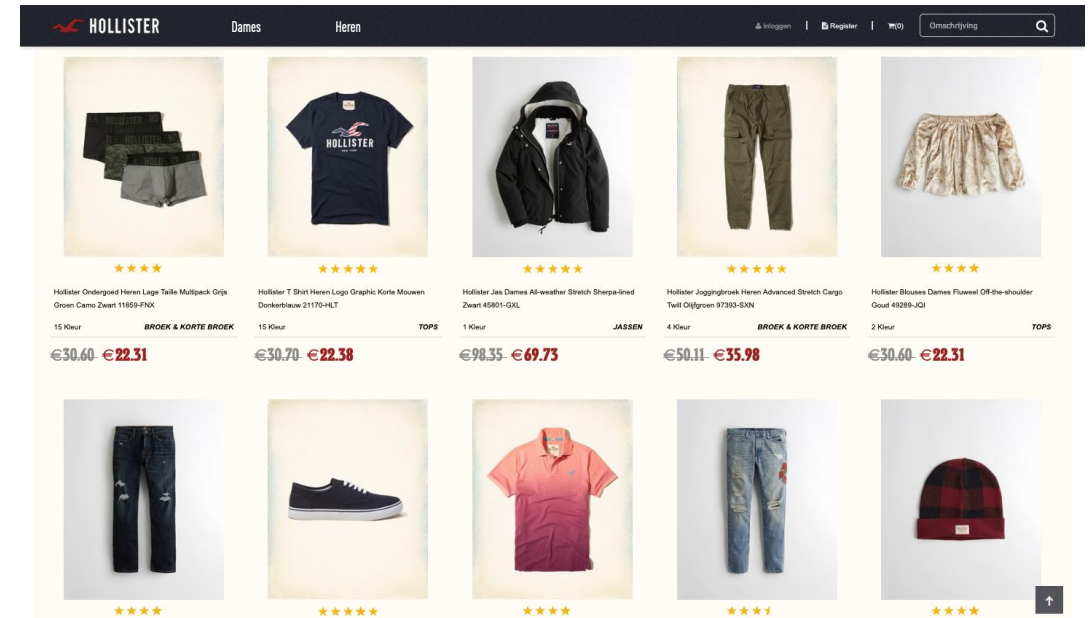
The screenshot shows the website watzullenwijeten.nl in a Mozilla Firefox browser window. The browser tabs include 'Mozilla Firefox Start Page', 'Domeinnaam historie - DRS Ra...', and 'New Balance WL574 Hoge...'. The address bar shows 'www.watzullenwijeten.nl' and the search bar contains 'fiod douane'. The website header features the logo 'Watzullenwijeten' and a shopping cart icon labeled 'Winkelwagen' with '0 product(en) - €0,00'. A navigation menu includes 'Home', 'Verlanglijst (0)', 'Mijn Account', 'Winkelwagen', and 'Afrekenen'. A secondary menu lists product categories: 'Dames Muiltjes', 'Dames Lage Skate Sneakers', 'Dames Sandalen op sleehak', 'Dames Hoge Sportieve Sneakers', and 'Dames High heels Sandalen'. The main content area is titled 'Nieuw' and displays three product cards. The first card shows a white sneaker with a yellow accent, labeled 'Dames Victoria DEPORTIVO BASKET PIEL Wit / Geel 4767093 Dames Hoge' with a price of €104,84 (crossed out) and €51,78. The second card shows a gold high-heeled sandal, labeled 'New Look Wide Fit VAMSTER Sandalen gold Kunststof Lente /' with a price of €99,90 (crossed out) and €54,62. The third card shows a red high-heeled shoe, labeled 'Evita Hoge hakken pink Veloursleer Lente / zomer Dames High heels' with a price of €94,95 (crossed out) and €58,26. Each card has a 'Bestellen' button. A sidebar on the left titled 'Categorieën' lists various shoe categories such as 'Dames Ballerina's', 'Dames Slip-on Sneakers', 'Dames Runner Sneakers', 'Dames Muiltjes', 'Dames Sneakers met Sleehak', 'Dames Lage Skate Sneakers', 'Dames Lage Sneakers', 'Dames Lage Sportieve Sneakers', 'Dames Lage Geklede Sneakers', 'Dames Geklede Sandalen', 'Dames Sandalen met Plateau', 'Dames Platte Sandalen', 'Dames Comfortabele Sandalen', 'Dames Loafers', and 'Dames Sandalen high heels'.



# Nepwebshops werken omdat gebruikers het niet weten



of



# Waarom houdt SIDN er zich mee bezig

- Schade bij consumenten
- Minder vertrouwen in Internet

## Goed uitgangspunt:

- Lijst van alle .nl-domeinnamen
- Registratiedata en bevragingmetingen



Kleding, make-up en technische gadgets: mensen kopen het steeds vaker via sociale media. En dat brengt risico's met zich mee, zegt de Autoriteit Consument en Markt (ACM). De schade voor consumenten door oplichting bedroeg vorig jaar bijna 5 miljoen euro. Daarom start de waakhond vandaag een campagne waarin ze consumenten waarschuwt voor nepwinkels op sociale media.



# Resultaten tot nu toe

- Sinds 2016 duizenden fake webshops aangepakt
- Gebruikers daarmee beschermd
- 2 detectie-systemen, 2 case studies
  - BrandCounter (2018)
  - FaDe (2019)



RIPE NCC  
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website  
Search IP Address or ASN

Login

You are here: Home > Publications > RIPE Labs > Giovane Moura > Detecting and Taking Down Fraudulent Webshops at the .nl ccTLD

## Detecting and Taking Down Fraudulent Webshops at the .nl ccTLD

Giovane Moura — 26 Feb 2020  
Contributors: Thymen Wabeke

In this article, we describe how we detect and take down fraudulent webshops at the .nl ccTLD.

Suppose you're looking for some new shoes you want at a *really* good price. So you decide to buy a pair of shoes. The shoes never arrives, or, if it does, you receive a counterfeit pair of shoes. Sounds familiar? The chances are high.



The RIPE NCC uses cookies. Some of these cookies are necessary for the operation of our site. You can adjust your cookie preferences in our [privacy policy](#). You can accept our cookies either by clicking the button below or by continuing to use our site.



tweakers

Zoek naar nieuws

## SIDN en .nl-registrars haalden vorig jaar 4340 frauduleuze webwinkels offline

7 °C € 1,737 502,29 TV gids 0 live

### Beheerder van het .nl-domein haalt 4.340 malafide webwinkels offline

17 februari 2020 17:20  
Laatste update: 17 februari 2020 17:24

**SIDN, de beheerder van het .nl-domein, heeft het afgelopen jaar 4.340 malafide webwinkels offline laten halen, maakt de stichting maandag bekend op zijn website.** Volgens de organisatie gaat het vaak om websites met erg lage prijsgebrekkige vertalingen en zonder keurmerk.

Als de stichting constateert dat achter een .nl-website een nepwebwinkel schuilt

## 3 Vragen die we behandelen:

- 1) Hoeveel fake webshops?
- 2) Hoe haal je ze weg?
- 3) Hoe werken ze?



# BrandCounter

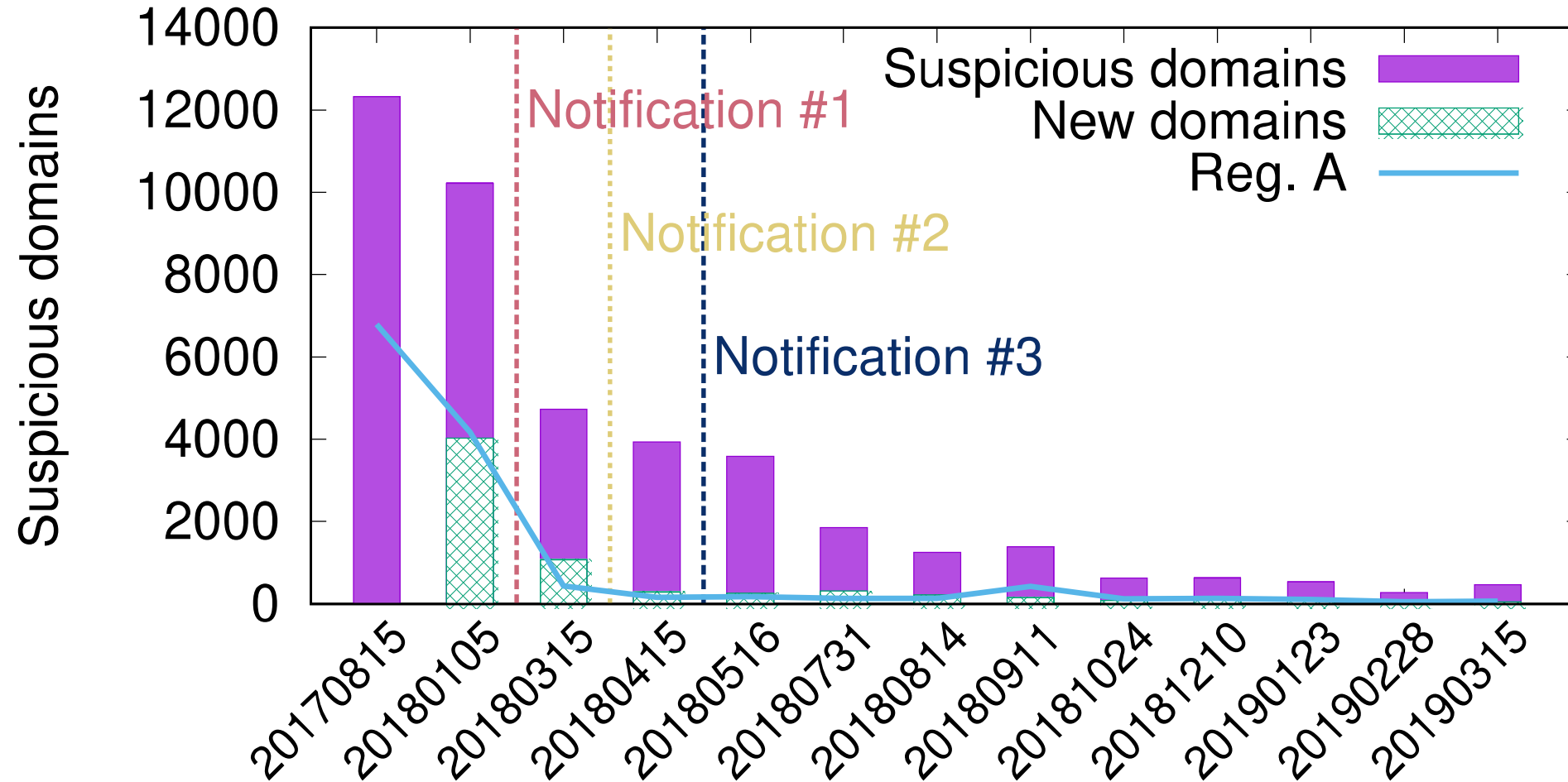
## Observaties:

- Lange html <title> tags met merknamen (Nike, Reebok, Gucci, etc.)
- Daarmee hoge SEO-score op zoekmachines [5]

## Methode:

- Lijst gemaakt van 1100 merknamen en woorden als 'korting'
- Aantal verdachte woorden geteld in <title> tags van alle .nl-sites
- Bij meer dan 5, markeer als verdacht

# BrandCounter metingen



# Een domeinnaam 'weghalen'

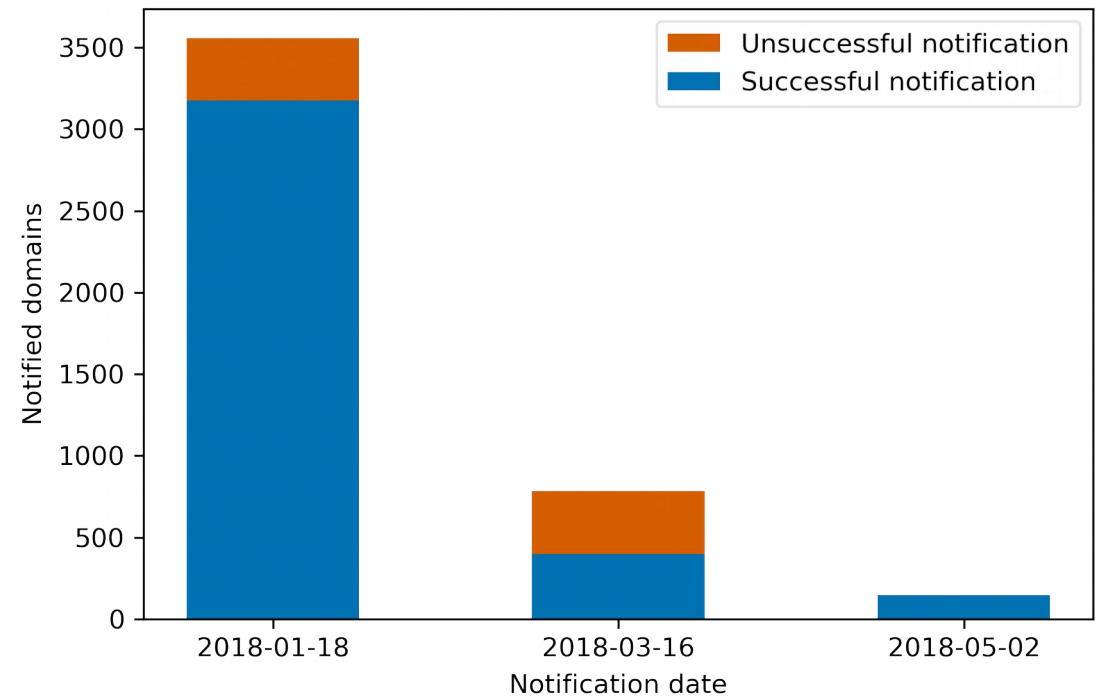
- Een domeinnaam **zelf** is nooit illegaal
- Wat ermee **gedaan wordt** kan dat wel zijn
- SIDN is ook geen 'content-politie'

Dus kan (en mag) SIDN niet zomaar een domeinnaam weghalen, behalve in opdracht van een rechter.

Dat moet dus altijd in samenwerking met de registrar en/of hoster.

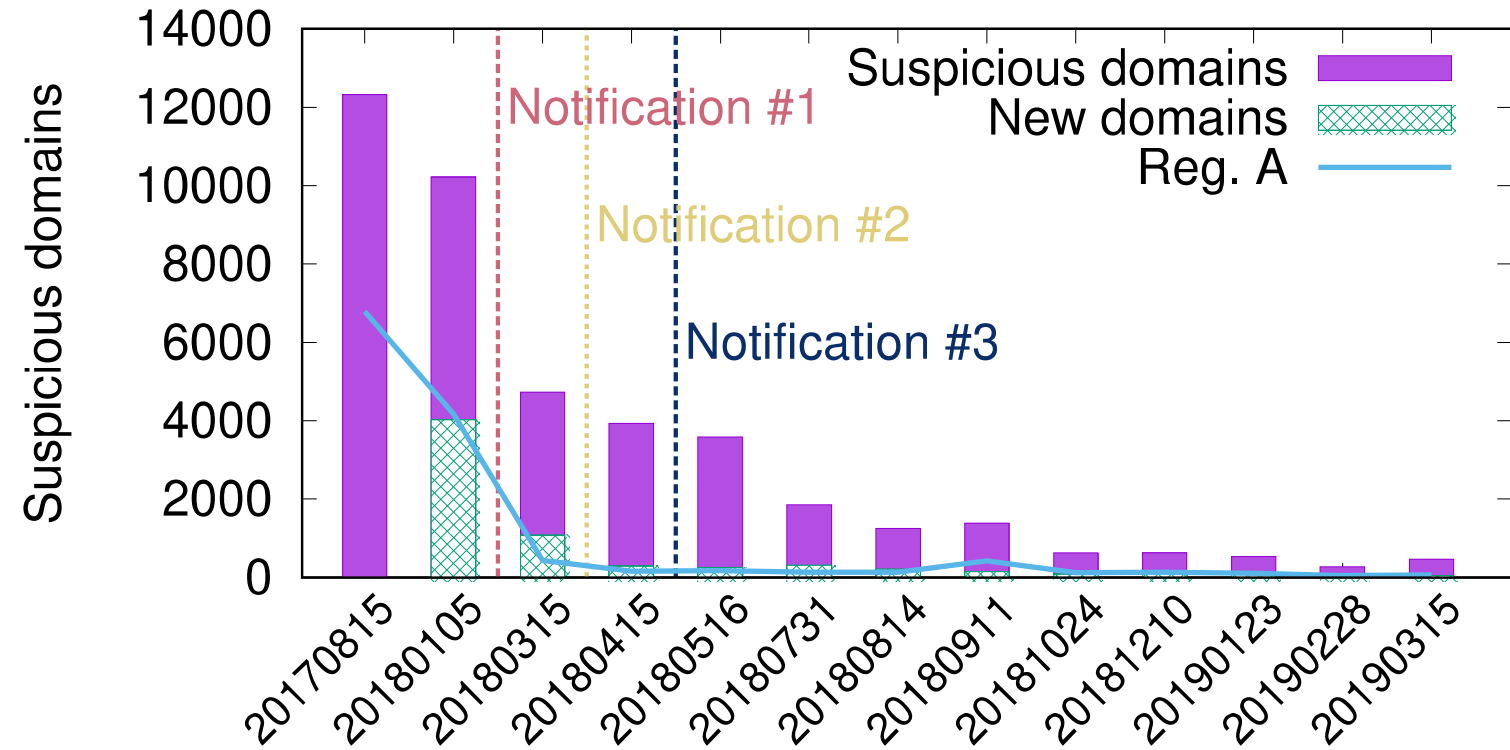
# Melding bij “Registrar A”

- Wij (SIDN) hebben maar beperkte mogelijkheden om domeinnamen rechtstreeks te verwijderen
  - 42,3% van de verdachte domeinnamen bij *Registrar A*
- 4107 meldingen verstuurd naar *Registrar A*
  - 3708 door ze verwijderd (90,31%)





# BrandCounter metingen



Hebben ze het opgegeven?  
Of geleerd hoe BrandCounter te omzeilen?

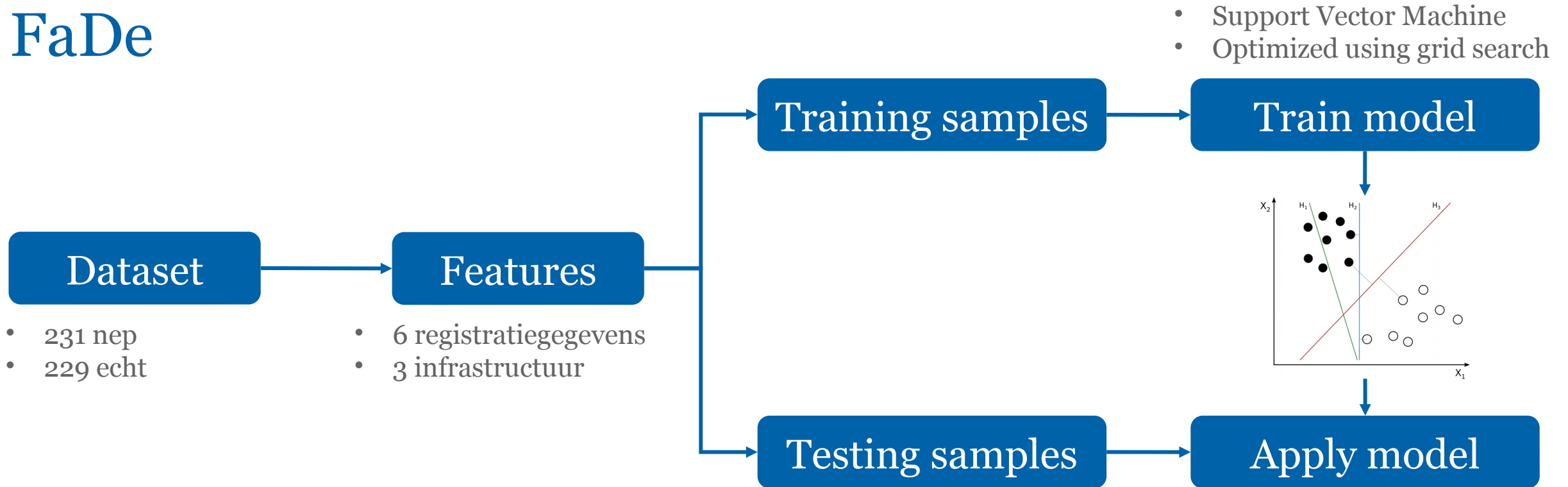
# Fake Detector (FaDe)

- Niet afhankelijk van de <title> tag
- Niet bevooroordeeld door SIDN's zichtpunt (.nl)

## Aanpak:

- Samenwerking met ICS, een creditcard-maatschappij
- ICS leverde 231 webshops die betrokken waren bij fraude
- 'Supervised Machine Learning' om een classificatiemodel te maken

# FaDe



Samples	Precision	Recall
Train (cross-validation)	0.98	0.97
Test	1.0	1.0

# FaDe meldingen

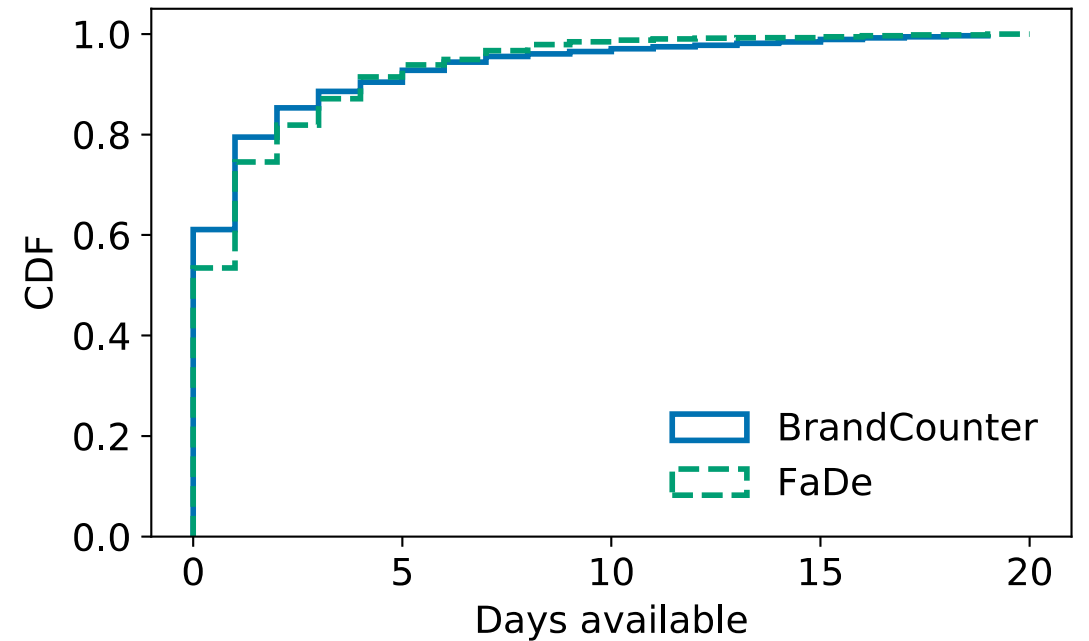
- Model toegepast op 30000 .nl-domeinen
  - 1407 als 'verdacht' aangemerkt
  - 894 (73%) daarvan terecht (true positives)
- 894 meldingen verstuurd naar registrars
  - 747 (84%) aangepakt



Hoe gaan nepwebshops te werk?

# Fabriek van webshops: automatisering

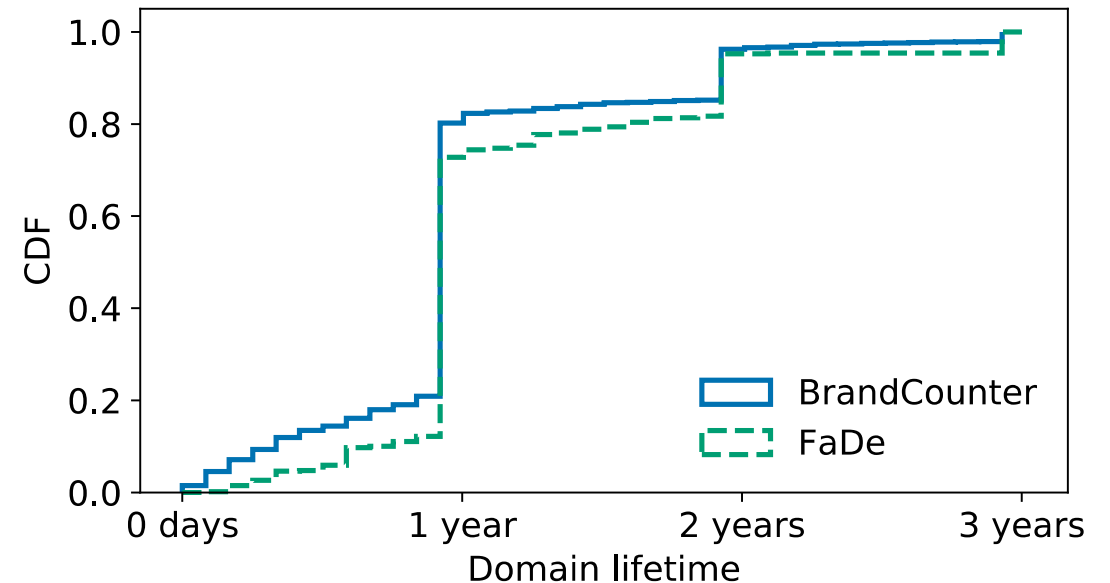
- Voornamelijk via goedkope registrars die een API aanbieden
- Website templates die dezelfde structuur hebben maar er anders uit zien
- 80% van de gebruikte domeinnamen heeft eerder bestaan
  - Merendeel direct geregistreerd na opheffing
  - Voordeel: “residual reputation” (nog bekend bij zoekmachines, etc.) [6]



*Days in between domain expiration and re- registration.*

# Fabriek van webshops: automatisering

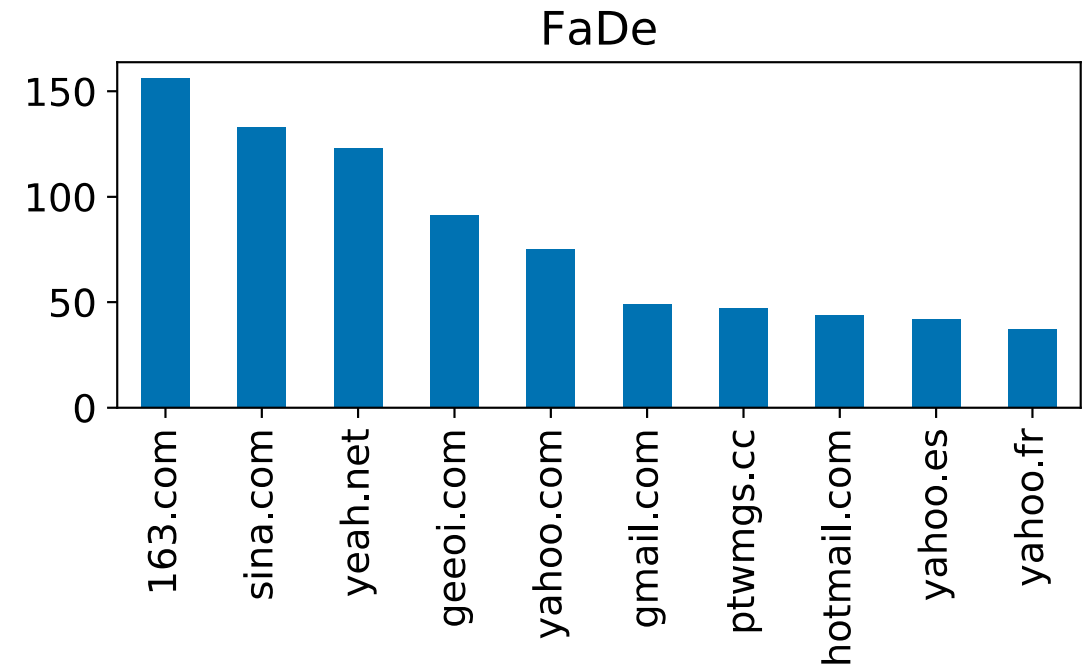
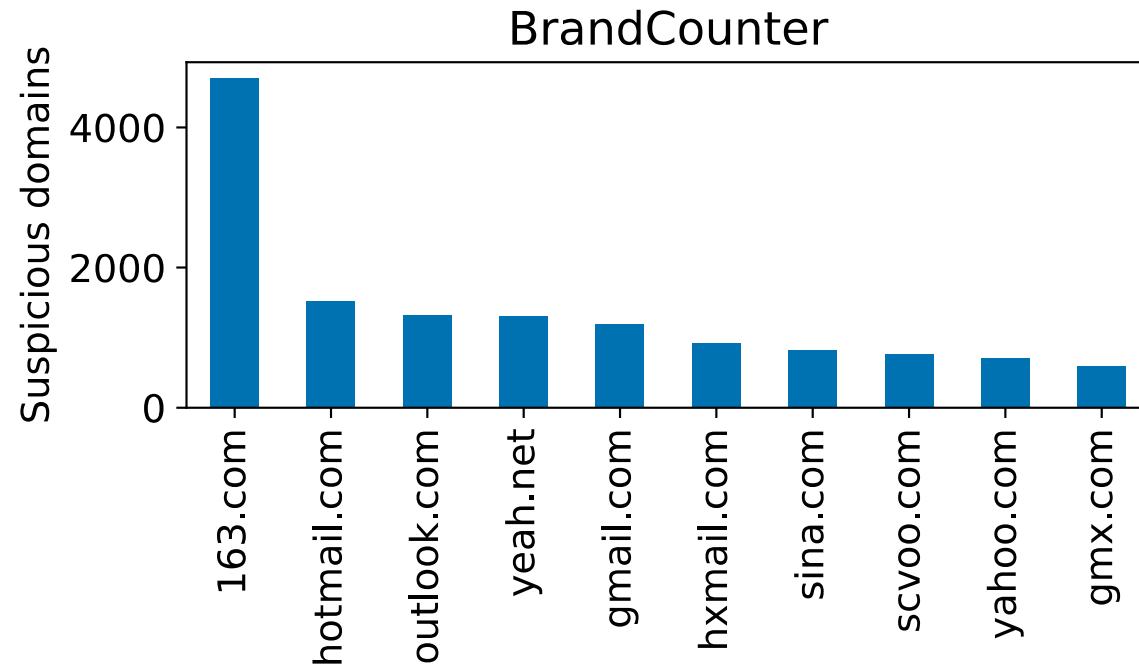
- Domeinnamen komen niet overeen met inhoud
- Spelfouten, vertalingsfouten
- Domeinnamen bestaan niet lang



*Most domains not renewed after 1 year— the registration period.*

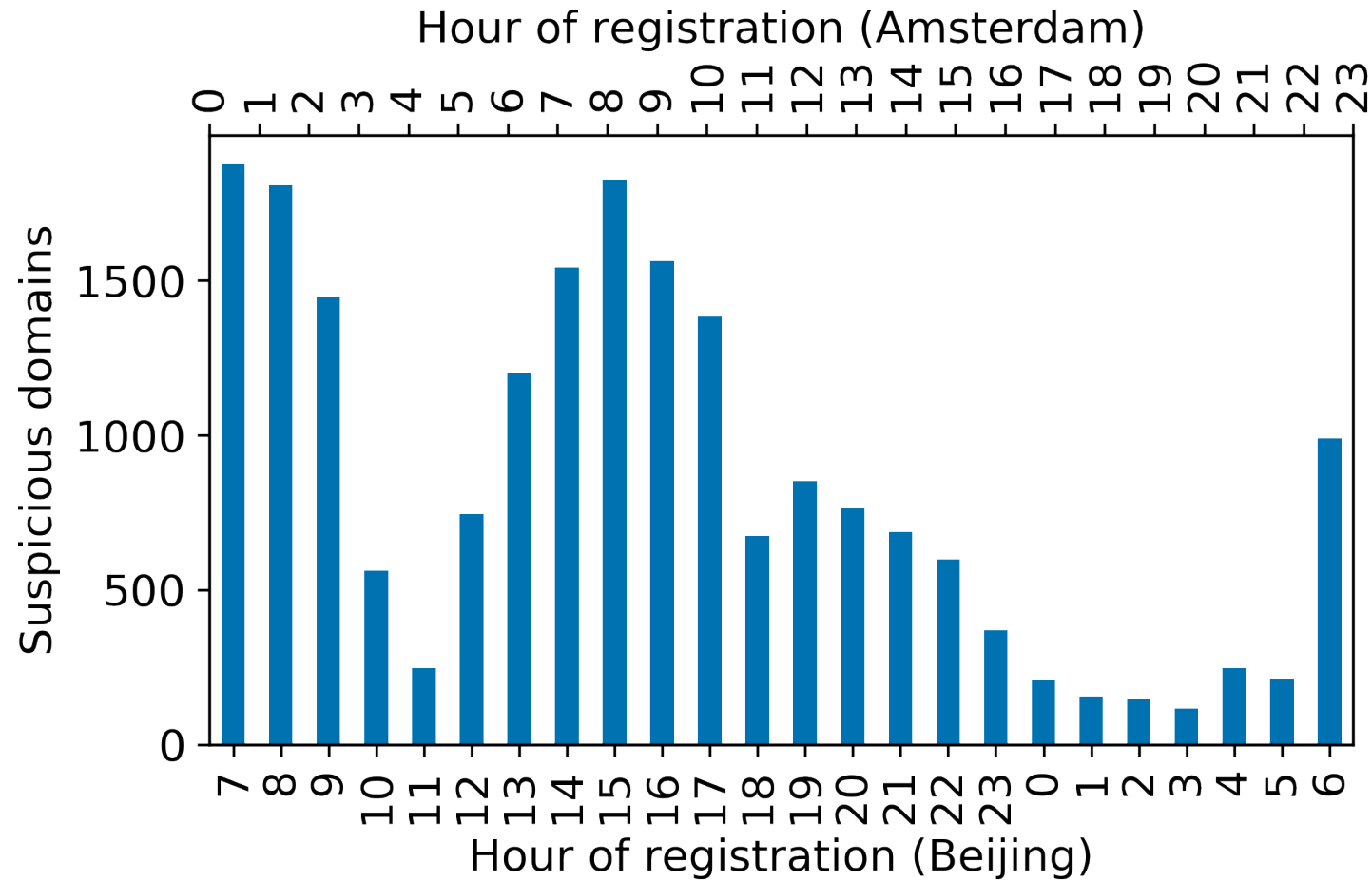
# Registraties vanuit China

## E-mailadres van de 'eigenaar'

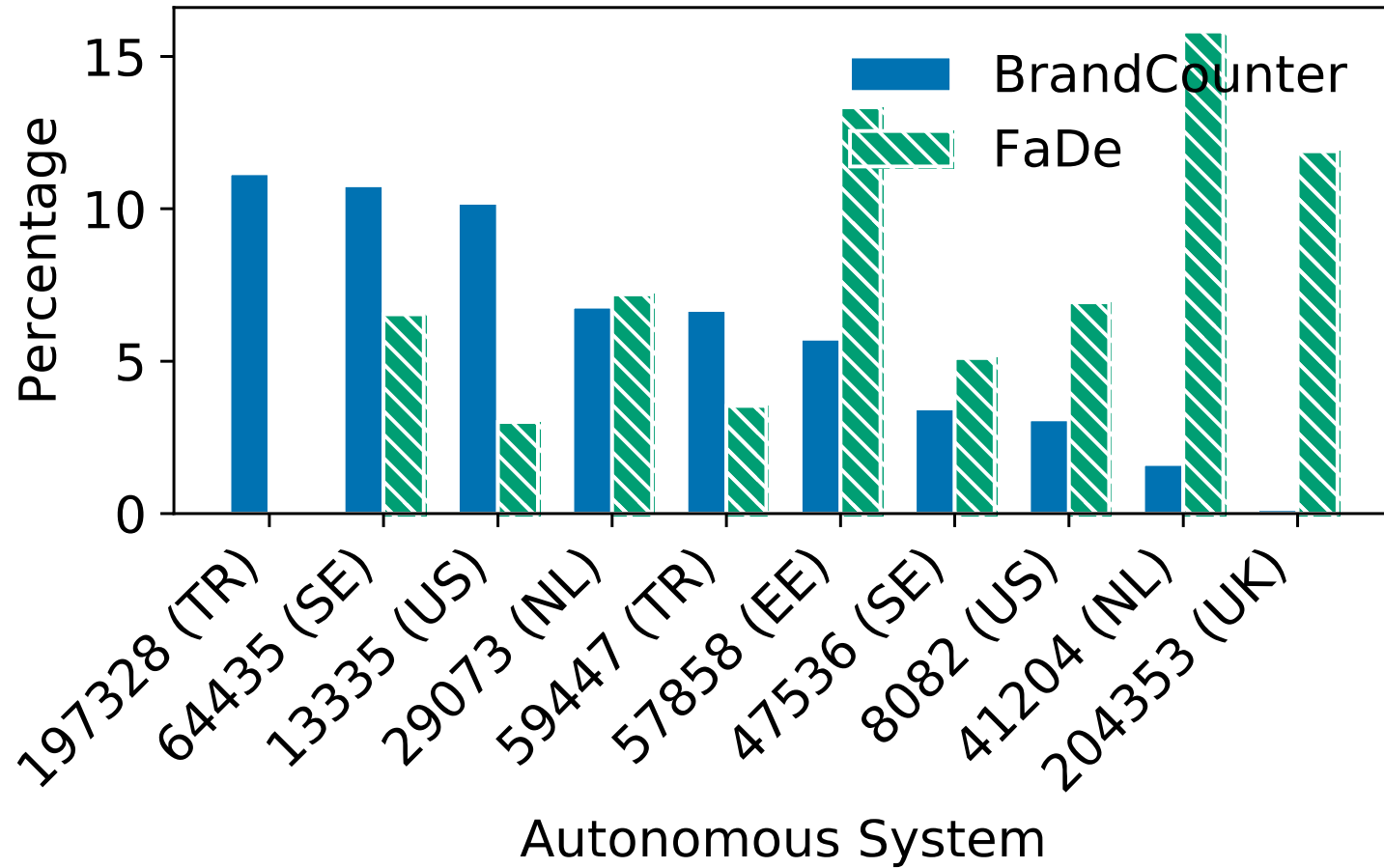




# Registraties vanuit China



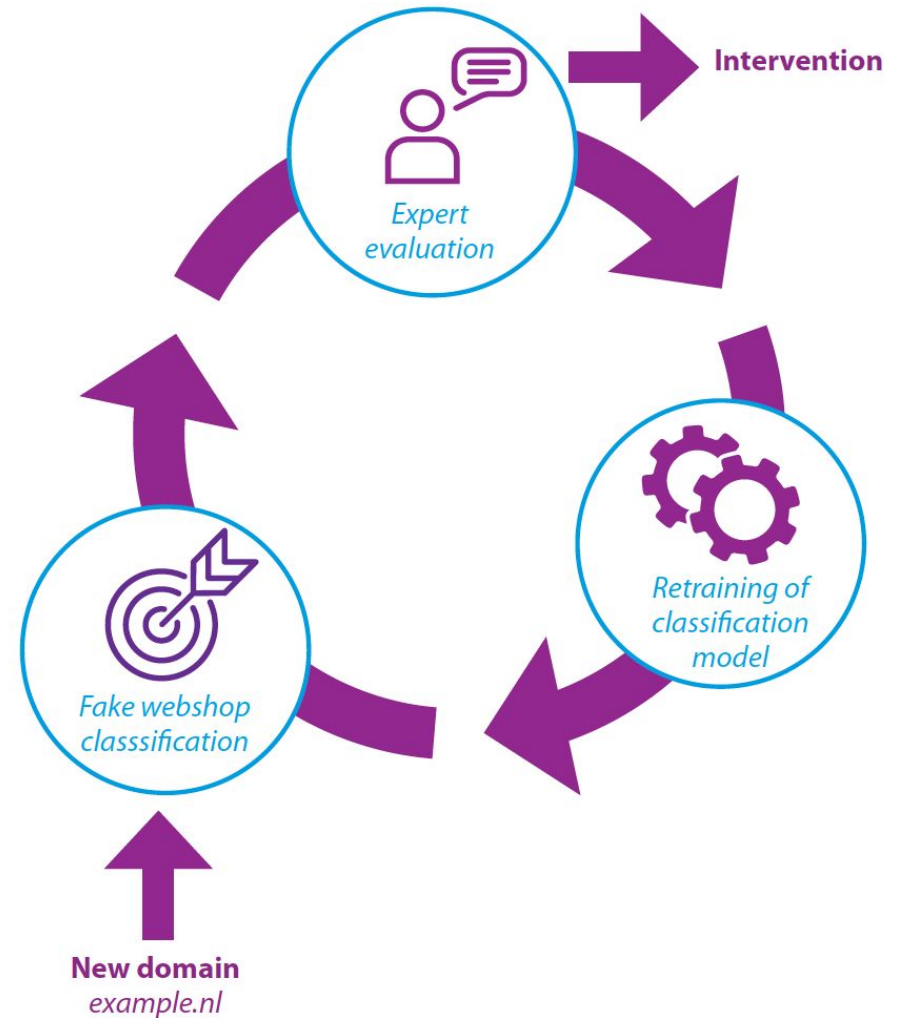
# Maar niet gehost in China



Zo hebben wij 4455 fake webshops helpen neerhalen

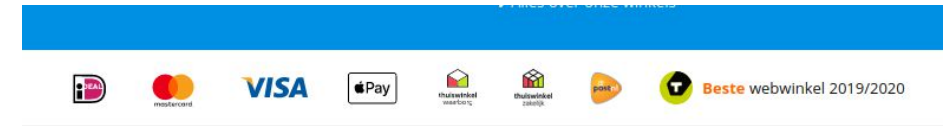
# Lessen

- Samenwerking met registrars en ICS was essentieel
- Detectors zijn simpel maar effectief
  - Registries hebben goed zichtsveld
  - Moeten wel wat druk uitoefenen
- Het blijft 'mollenmeppen'
  - Webshops passen zich aan



# Wat kun je zelf doen?

- Aanbiedingen te goed om waar te zijn?  
Dan is dat vaak zo
- Check keurmerken:
  - Thuiswinkel-waarborg etc. zijn links naar het officiële certificaat
- Slecht taalgebruik is een red flag
- Enigszins verdacht?
  - Check het kvk-nummer op kvk.nl, en vergelijk adresgegevens
  - Geen kvk-nummer op website? Wegblijven.



[Algemene voorwaarden](#) | [Privacy](#) | [Cookies](#) | [English \(EN\)](#)

© 1999 - 2020 - Coolblue B.V.

**bol.com**<sup>®</sup>  
de winkel van ons allemaal



Geldt voor aankopen bij [Thuiswinkel-leden](#) | [Algemene voorwaarden](#) | [Privacy](#) | [Cookie](#)

floris.cc

kvk Breda 20146119

VAT: NL001806878B27

Bank Account



# Referenties

- RTL Nieuws: Dit jaar al 307 nep-webwinkels oine gehaald door politie (in Dutch) (Dec 12 2018), <https://www.rtlnieuws.nl/geld-en-werk/artikel/4520646/dit-jaar-al-307-nep-webwinkels-offline-gehaald-door-politie>
- NOS: Consumenten voor 5 miljoen euro opgelicht via nepwinkels op sociale media (in Dutch) (Dec 12 2018), <https://nos.nl/artikel/2258095-consumenten-voor-5-miljoen-euro-opgelicht-via-nepwinkels-op-sociale-media.html>
- NOS: Waar komen al die nep-webshops toch vandaan? (in Dutch) (May 5 2018), <https://nos.nl/artikel/2230087-waar-komen-al-die-nep-webshops-toch-vandaan.html>
- Peter Hornung: Gefalschte Sneaker von der FDP? (In German). <https://www.tagesschau.de/wirtschaft/fakeshops-plagiate-sneaker-china-101.html> (2019)
- Wang, D.Y., Der, M., Karami, M., Saul, L., McCoy, D., Savage, S., Voelker, G.M.: Search + seizure: The effectiveness of interventions on seo campaigns. In: Proceedings of the 2014 Conference on Internet Measurement Conference. pp. 359--372. IMC '14, ACM, New York, NY, USA (2014). <https://doi.org/10.1145/2663716.2663738>
- Lever, C., Walls, R., Nadji, Y., Dagon, D., McDaniel, P., Antonakakis, M.: Domainz: 28 registrations later measuring the exploitation of residual trust in domains. In: 2016 IEEE Symposium on Security and Privacy (SP). pp. 691{706 (May 2016). <https://doi.org/10.1109/SP.2016.47>