Fake webshops, real counterattacks

Chiel van Spaandonk (SIDN R&S), Thymen Wabeke (SIDN Labs)

Lunchlezing NCSC| 21 maart 2019

Over SIDN .nl registry met 5,8 miljoen domeinnamen

Wij zorgen voor een veilig en stabiel .nl
en helpen misbruik te voorkomen op gebieden zoals:

- Phishing & malware
- Inbreuk op (IP) rechten
- Strafbare of onrechtmatige content
- En… fake-webshops…

Over R&S

Registratie & Service. Het Support / Contact center van SIDN

- 10 eerstelijns en 3 tweedelijns medewerkers

Alle support voor domeinnaam registratie maar ook:

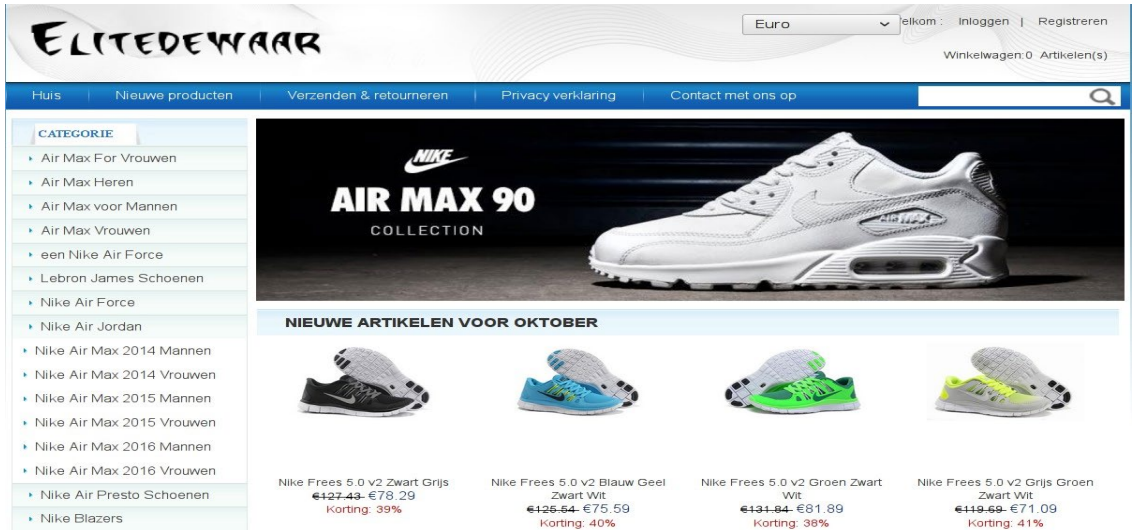
- WIPO en Mediation
- Notice and Takedown
- Abuse204.nl

Agenda

- Wat zijn fake webshops? Hoe herken je ze?
- Cijfers & bestrijding
- Hoe kan een algoritme fake webshops proactief detecteren (Labs)?

Achtergrond fake webshops

- Begonnen in 2016
- Gemeld door consumenten en merkbeschermers
- Herregistratie domeinnamen voor winkels met
  - Luxe artikelen
  - Grote kortingen
  - Heel veel schoenen
  - Vreemde domeinnamen
  - Vreemde producten..



Best vreemd toch?..

Deze Nikes bestaan echt niet..

www.beleefbaantjer.nl

Inloggen Registratie Euro

beleefbaantjer.nl

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]

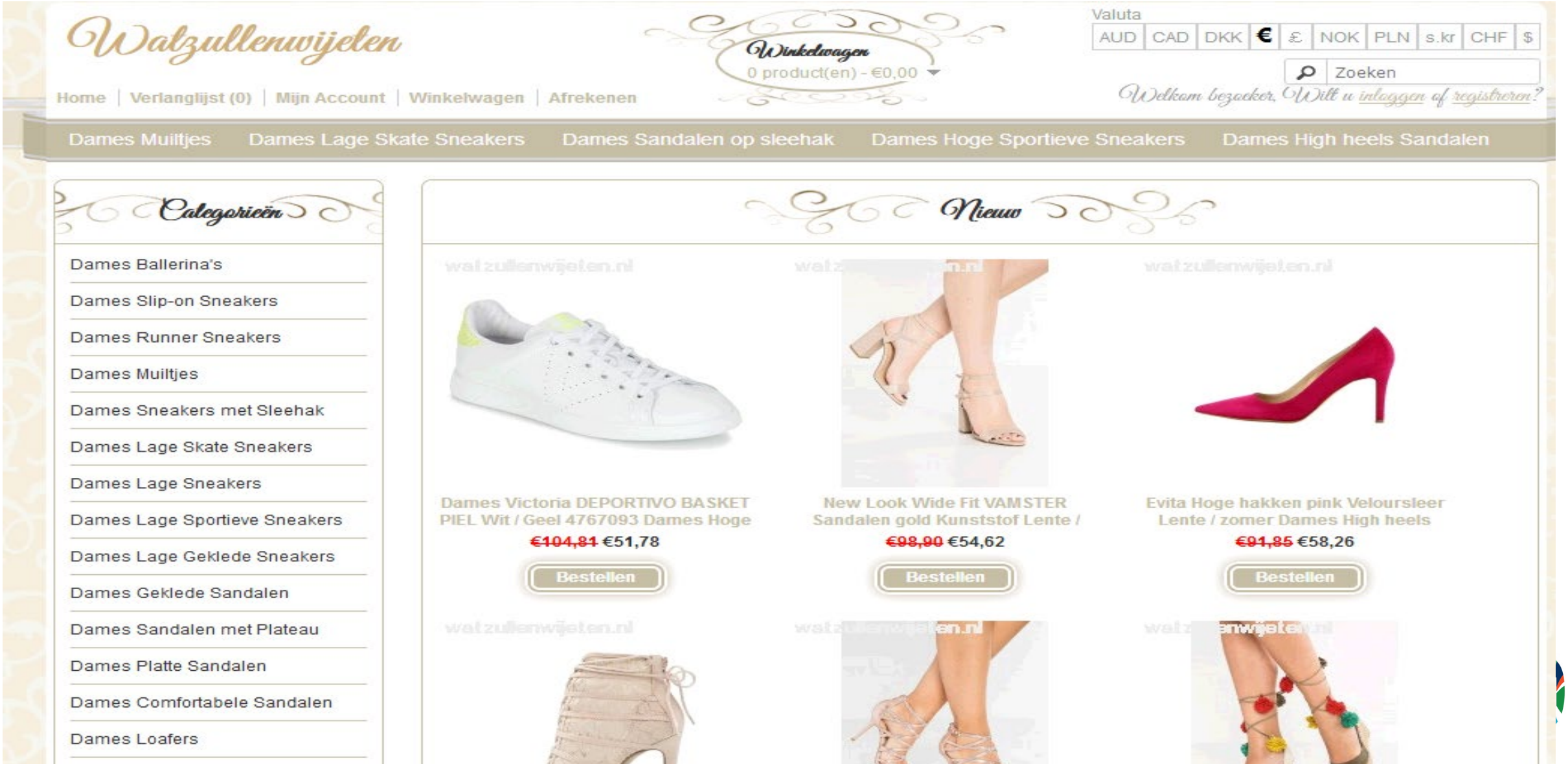
Nieuwe artikelen voor juli

Beste Online Prijs Liu Jo Jurk Divers Dames Outlet Online J3b6blzE
~~€78.49~~ €44.29
Korting: 44%

Extra Uitverkoop Liu Jo Army dress Groen Dames Laagste Prijs Op G2GwgCLw
~~€99.70~~ €47.00
Korting: 53%

Een Goedkope Prijs Marjoly Paris zwarte jurk met kanten mouw Zwart Dames Allemaal Te Koop 6jcx1YZO
~~€121.75~~ €41.55
Korting: 66%

watzullenwijeten.nl



Wie? Waarom?

- Internetcriminaliteit lucratief en moeilijk op te sporen
- Minder serieus genomen en krijgt minder aandacht dan andere criminaliteit, zoals drugs
- Belangrijkste oorzaak: consumentenvraag (koopjes)
- Zeer winstgevend, wereldwijd en weinig riskant

Hoe herken je fake webshops?

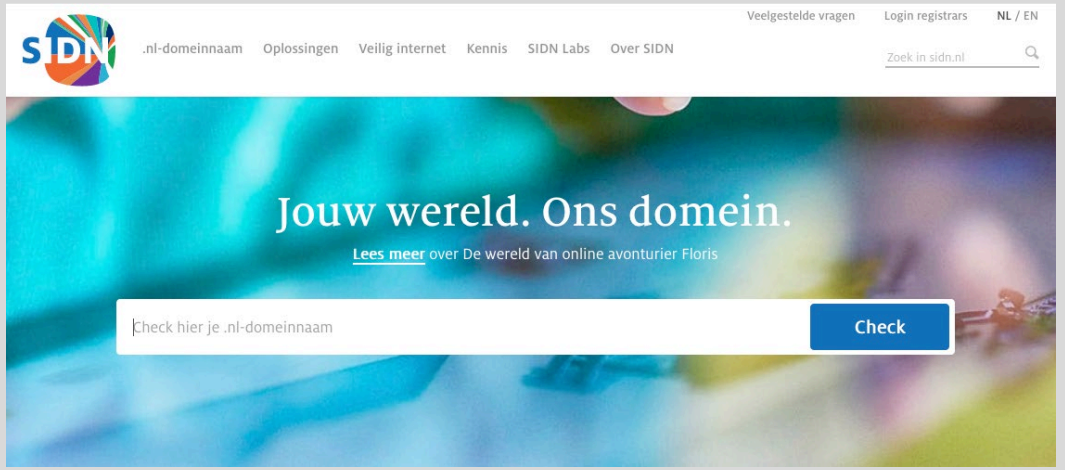
Niet altijd gemakkelijk, maar …

- Controleer de Whois-gegevens
- Net geregistreerde domeinnamen
- Grote kortingen en alles is op voorraad
- Afbeeldingen (keurmerken & creditcards) linken niet door
- Geen contactgegevens voor bedrijf
- Hotmail or Gmail-adres
- Google gebruikerservaringen, bv. reviews

Hoe herken je fake webshops?

Niet altijd gemakkelijk, maar …

- Controleer de Whois-gegevens
- Net geregistreerde domeinnamen
- Grote kortingen en alles is op voorraad
- Afbeeldingen (keurmerken & creditcards) linken niet door
- Geen contactgegevens voor bedrijf
- Hotmail or Gmail-adres
- Google gebruikerservaringen, bv. reviews



Hoe herken je fake webshops?

Niet altijd gemakkelijk, maar …

- Controleer de Whois-gegevens
- Net geregistreerde domeinnamen
- Grote kortingen en alles is op voorraad
- Afbeeldingen (keurmerken & creditcards) linken niet door
- Geen contactgegevens voor bedrijf
- Hotmail or Gmail-adres
- Google gebruikerservaringen, bv. reviews

Gebrekkig taalgebruik

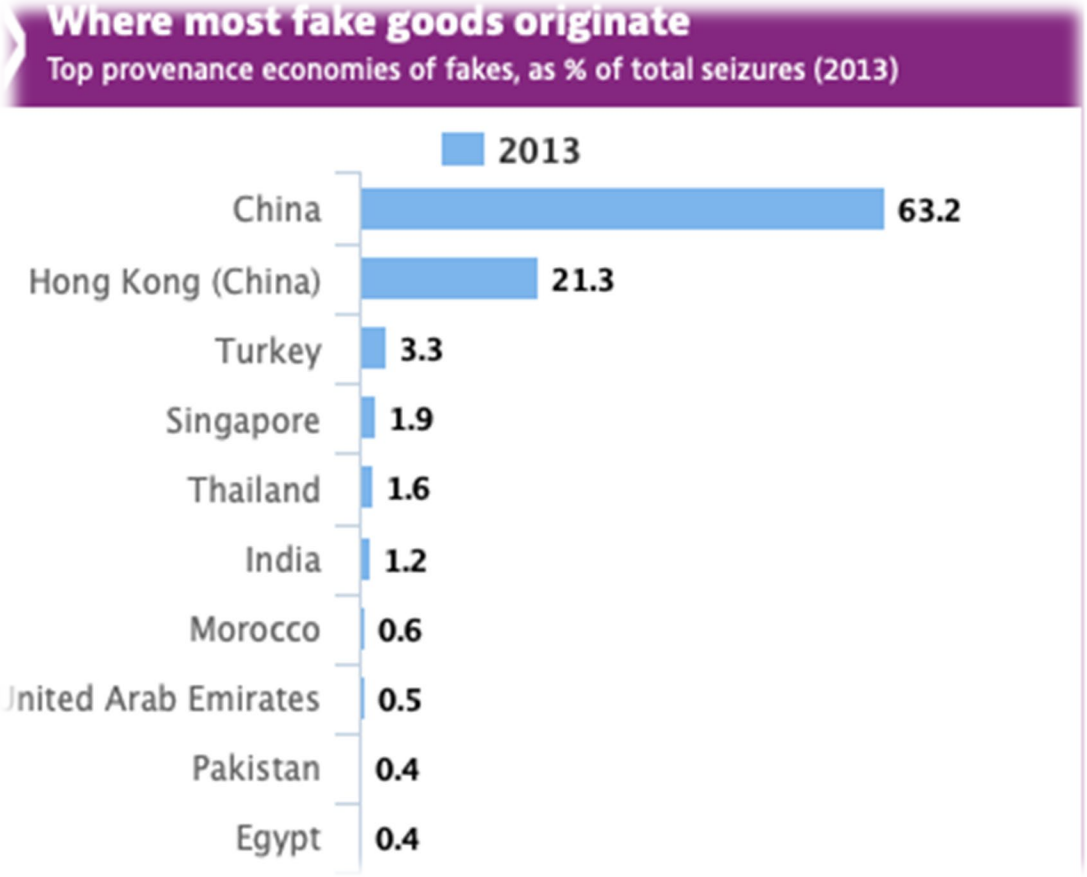
Als de tekst leest als een slechte Google-vertaling…

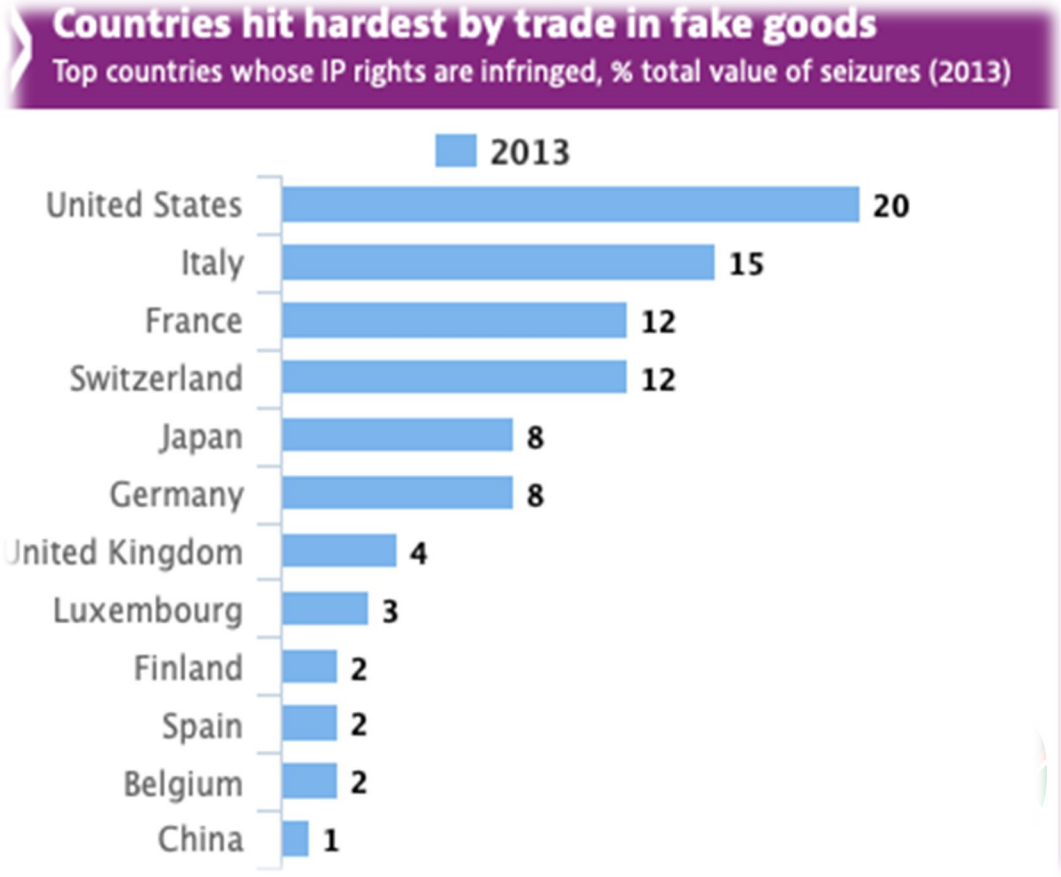
Heb je toch besteld?

- Reken op namaakproducten of helemaal niets
- Pas op voor identiteitsdiefstal
- Informeer het creditcardbedrijf en controleer creditcard-afschriften
- Informeer de registrar

Herkomst namaakproducten

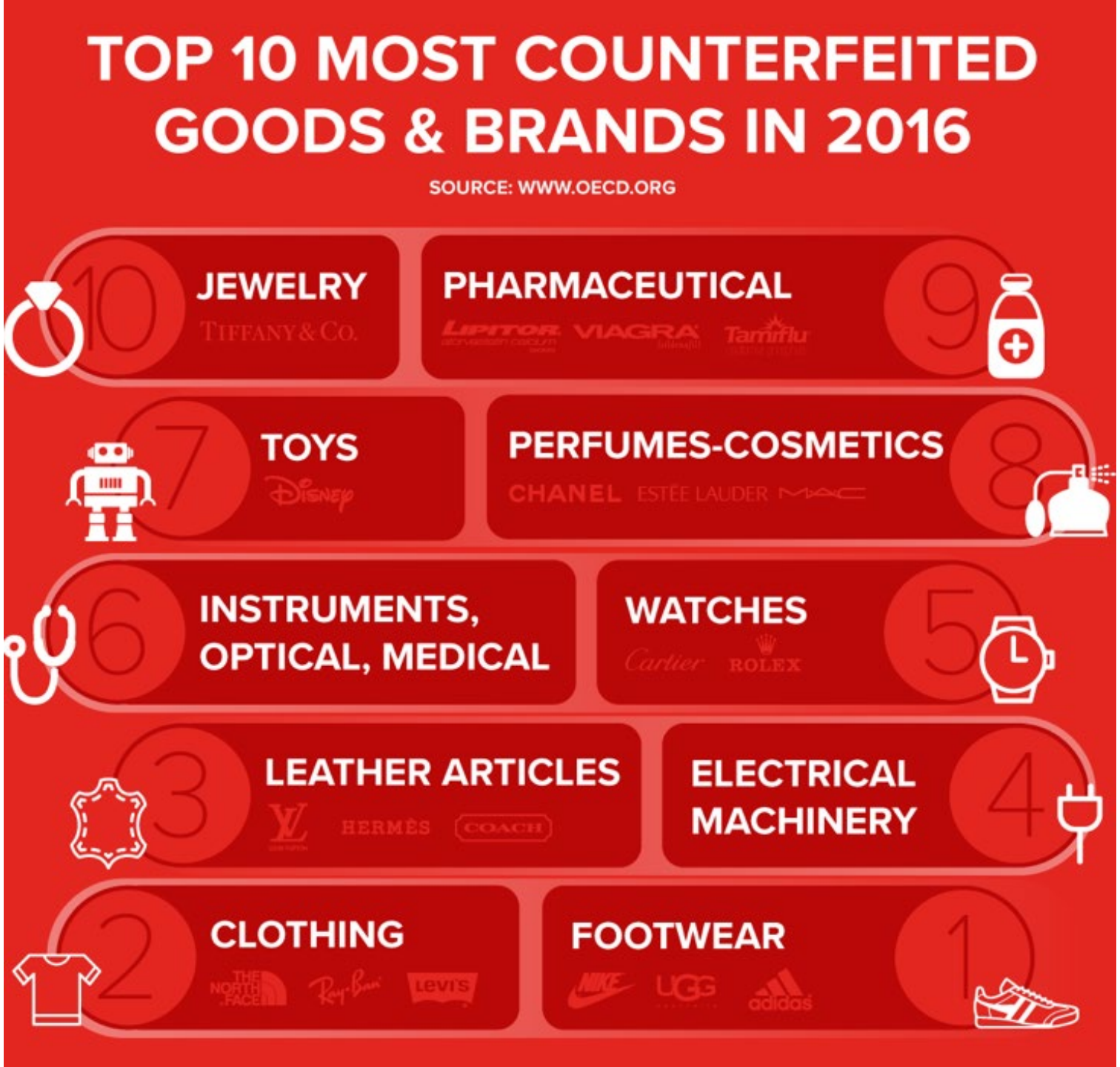
- Vooral China (EU en VS grootste afnemers)
- VS (IP rechten) meest getroffen





TOP 10 MOST COUNTERFEITED GOODS & BRANDS IN 2016

SOURCE: WWW.OECD.ORG



Cijfers

- 2,5 procent van de wereldhandel is namaak
- 500 biljoen dollar industrie (naar verwachting 1 triljoen in 2022)
- Handel in namaak is de afgelopen vijf jaar met 80 procent toegenomen

Rapport Fraudehelpdesk:

- Schade in 2016 meer dan €500.000,-
- 25 klachten per maand in 2018

Bronnen:
Fraudehelpdesk
Organisatie voor Economische Samenwerking en Ontwikkeling (OECD)

Stand van zaken bij SIDN

- Probleem toegenomen sinds 2016-2017
- Consumenten begonnen te klagen
- We ontdekten patronen in registratiegegevens (houders en registrars)
- We gingen samenwerken met verschillende partijen, zoals…

FRAUDE HELPDESK.nl

ICS INTERNATIONAL CARD SERVICES

VISA MasterCard

EUROPOL

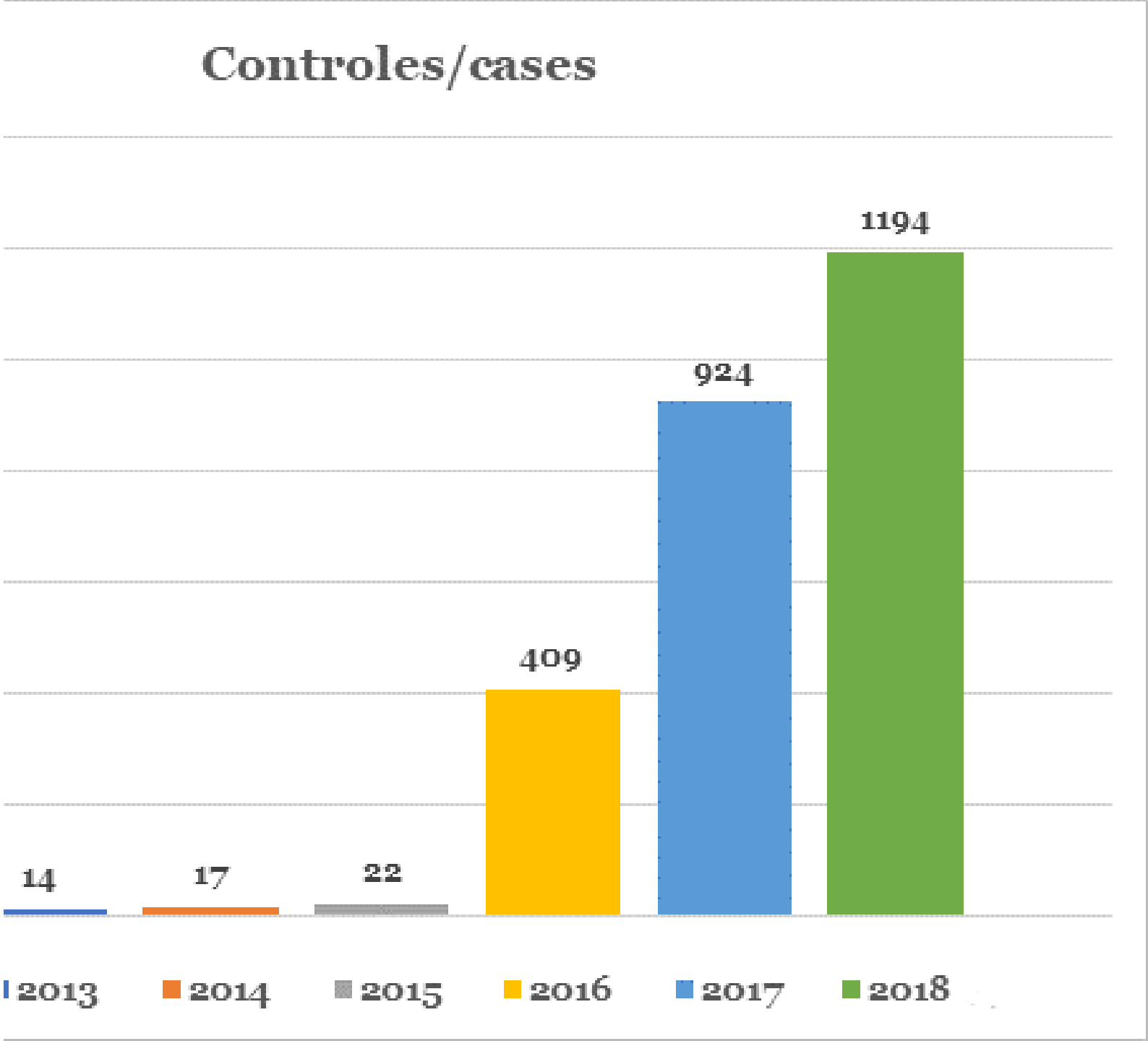
POLITIE Landelijk Meldpunt internetoplichting

Autoriteit Consument & Markt

Grondslag voor NTD: identiteitscontrole

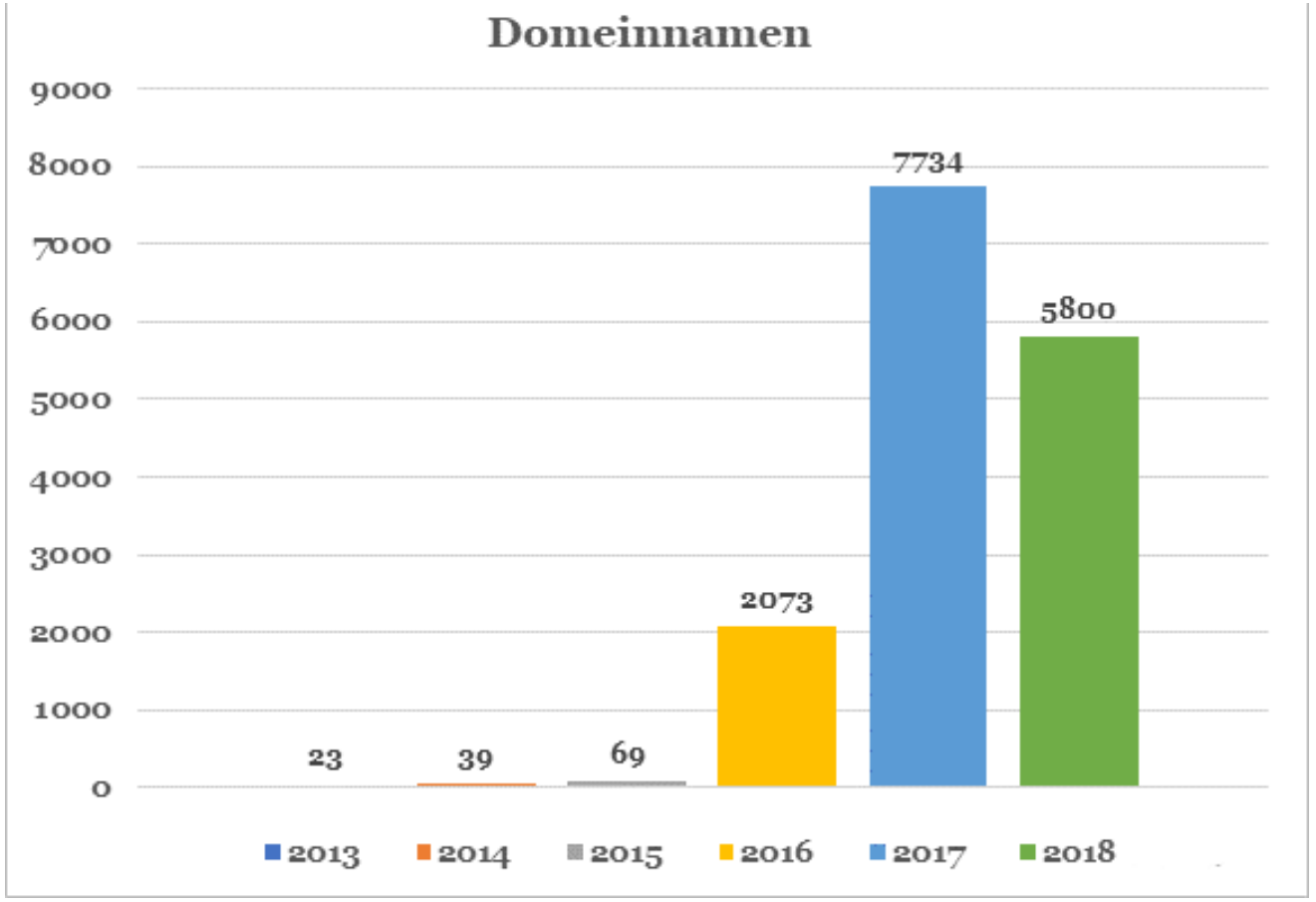
- **Identiteitscontrole / art.16** Algemene voorwaarden

Artikel 16 cases



Uit de lucht genomen domeinnamen

- We wijzen registrars in bulk op domeinnamen met fake webshops.
- Zij ondernemen hier vaak zelf actie op en haalden ten minste nog eens 10.000 fakewebshops uit de lucht.



Onderzoek fake webshop detectie

We detecteren al veel fake webshops, maar…

Kwaadwillende proberen detectie te vermijden door:

- naar een andere registrar te verhuizen
- op het oog legitieme domeinen te registreren
- vaak van hosting provider te wisselen
- duizenden webwinkels te registreren

Dus… hoe zijn we ze te slim af? En ook nog geautomatiseerd?

Over SIDN Labs

- Doel: bijdragen aan veiligheid en weerbaarheid van internetcommunicatie door empirisch onderzoek en ontwikkeling van prototypen.
- Onderzoeksgebieden: cruciale internetsystemen en evolutie van het internet
- Werkzaamheden: ondersteuning operationele teams, open source software, data-analyses, wetenschappelijke publicaties en samenwerken met universiteiten.

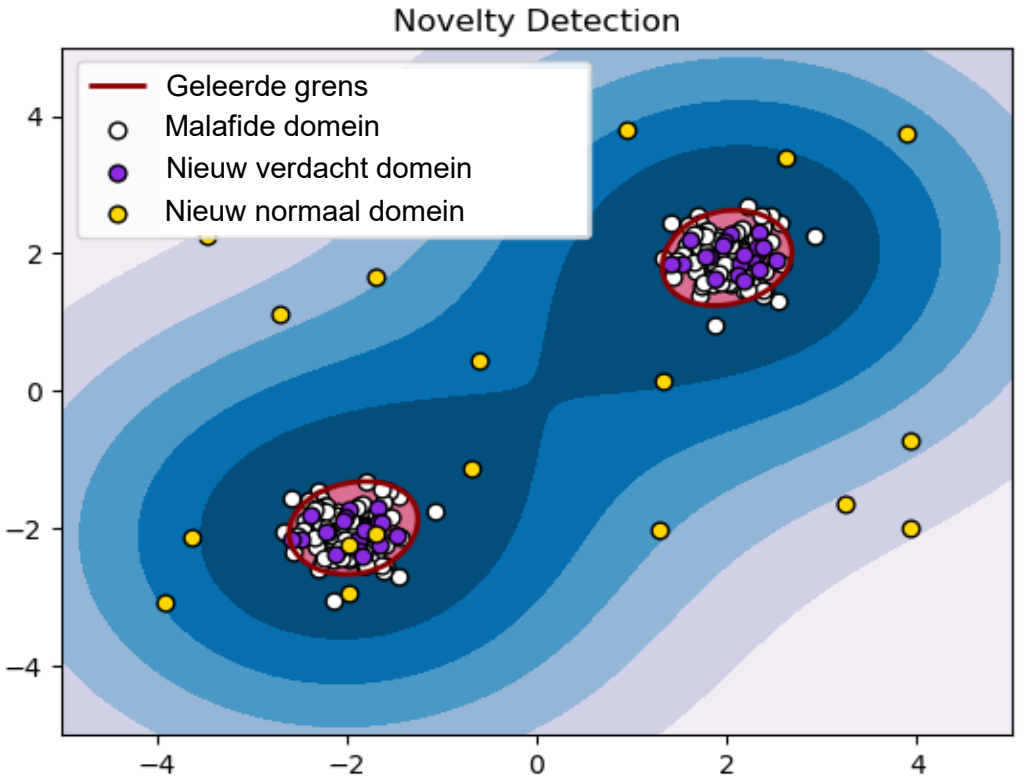
Onderzoek fake webshop detectie

Doel:

- Verdachte webshops proactief detecteren

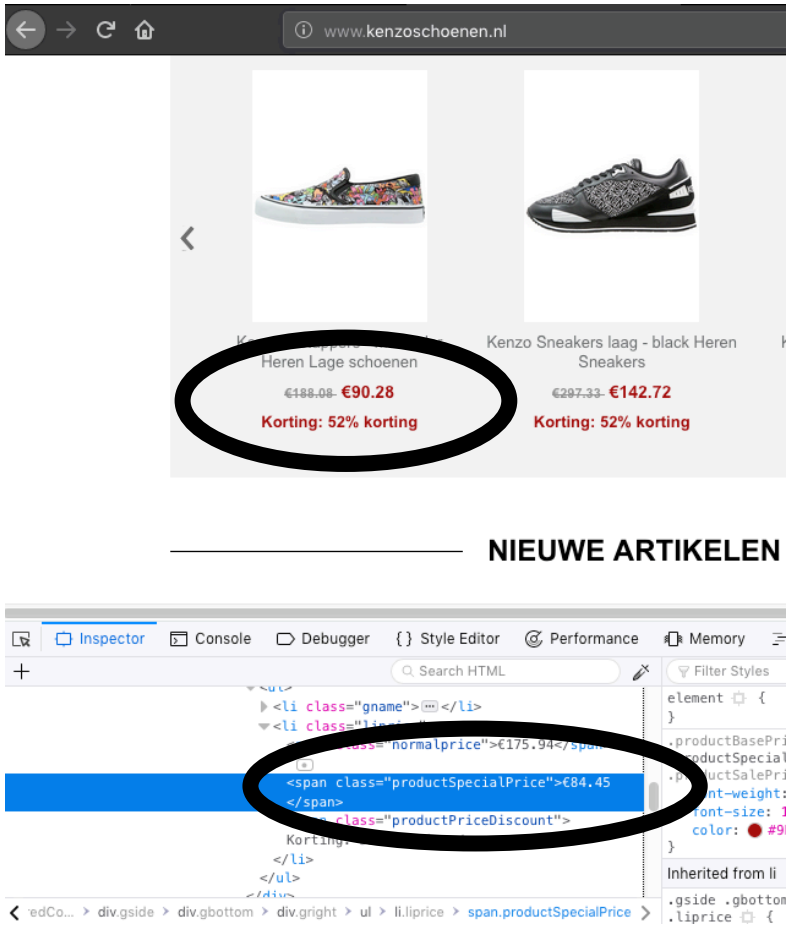
Aanpak:

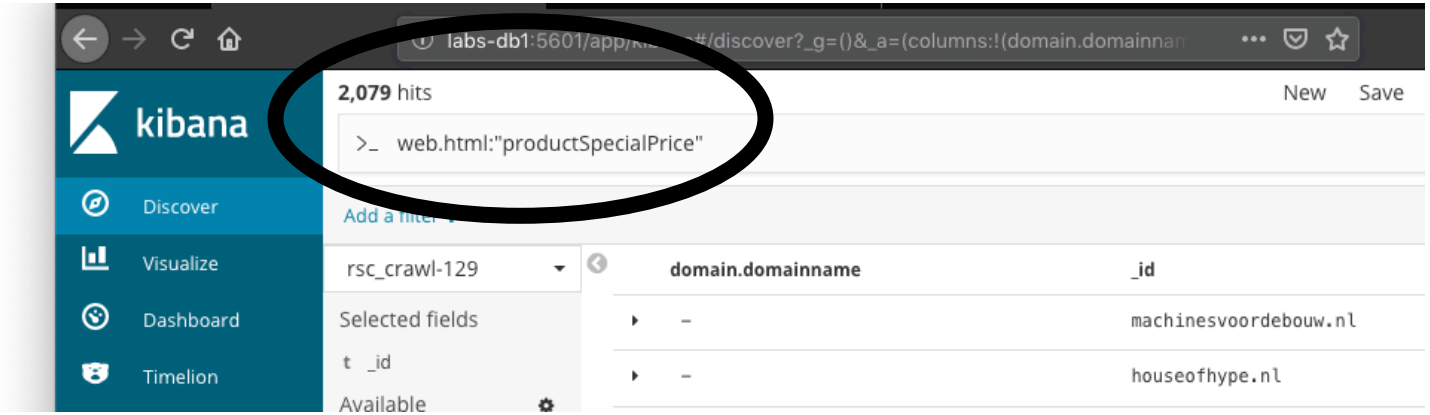
- Een machine learning algoritme leert de patronen achter fakeshops. Deze patronen noemen we het model.
- Het model passen we toe op nieuwe domeinnamen. Domeinen die lijken op fakeshops zijn verdacht.



Voorbeeld van een patroon

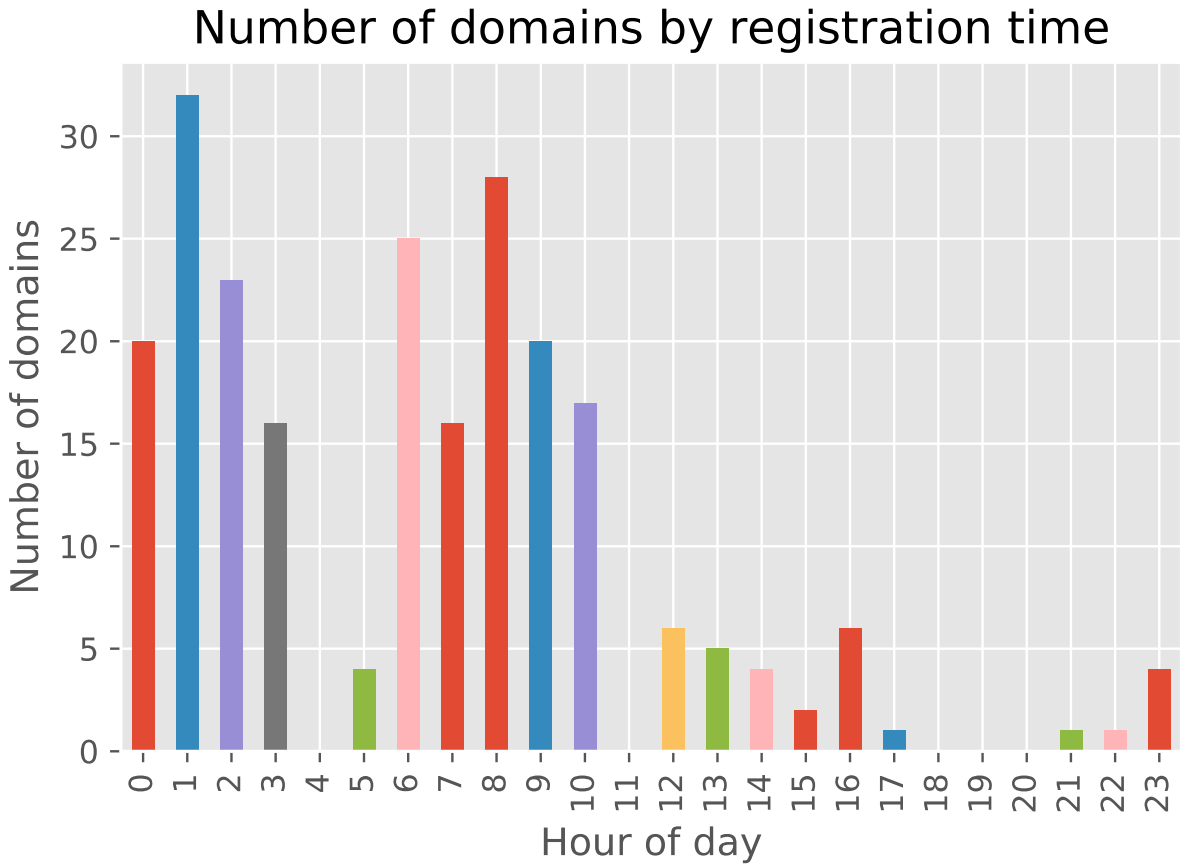
- Fake webshops onderscheiden zich door (visuele) kenmerken zoals aanbiedingen;
- Onderstaand patroon komt 2079 keer voor in de .nl-zone.





Voorbeeld van een patroon

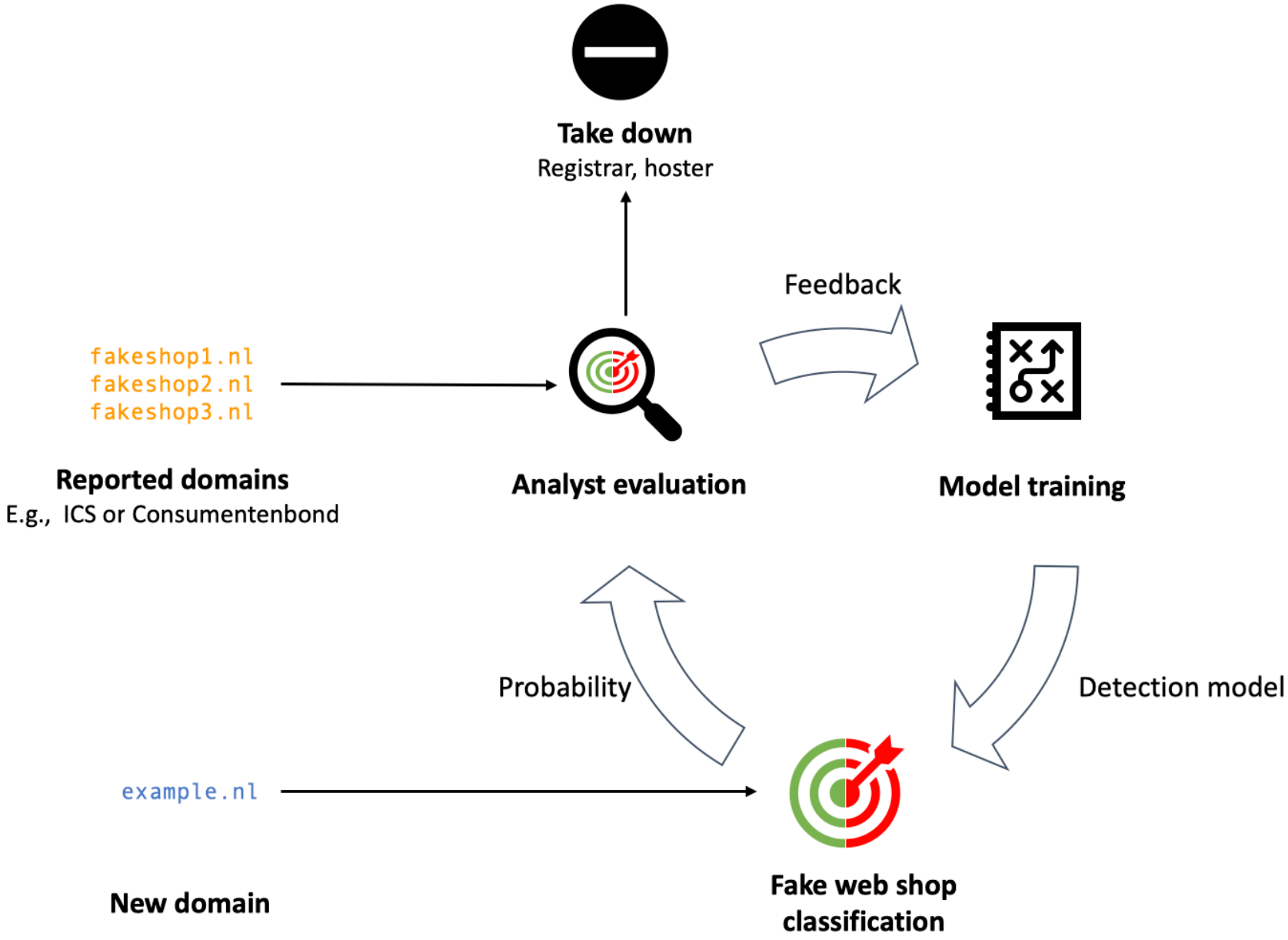
- Malafide webshops worden vaak geregistreerd tijdens onze nacht en ochtend.



Aandachtspunten voor robuuste detectie

Randvoorwaarde	Implicatie
Adaptief	• Continue hertrainen en evalueren
Accuraat	• Heterogene databronnen • Analisten evalueren verdachte shops • Feedback van analisten gebruiken
Proactief	• Vroegtijdige detectie • Efficiënte takedown procedure

Proces voor robuuste detectie



Pilot i.s.m. International Card Services (ICS)

Aanpak:

- Classifier trainen o.b.v. 231 gerapporteerde domeinnamen
- Classifier toepassen op de hele NL-zone
- ICS-analisten evalueren verdachte shops

Category	Features
WHOIS	Registrar, drop-catch, age
Web	Web hoster, TLS issuer
Mail	Mail hoster

Resultaten:

- 893 fake webshops gevonden in eerste iteratie
- Expert evaluaties zijn waardevolle feedback

	Precision	Recall
One-Class SVM	0.95	0.83
Two-Class SVM	1.00	1.00
Evaluations by ICS	0.73	N/A

Vervolgonderzoek

- Aanvullende voorspellers toevoegen (bijvoorbeeld fake registrants of domeinnamen die geen betrekking hebben op content)
- Automatiseren van bijwerken detectiemoel (active learning)
- Automatiseren van proces (CRM)
- Samenwerking met meer partijen (registrars, wetshandhaving, in NL en buitenland etc.)


27.08.2018 19:28 Uhr

Bericht: Fake-Shops betrügen Verbraucher im großen Stil

Vorkassezahlungen kassieren und dann nichts liefern – mittels gefälschten Shops werden zunehmend mehr Online-Käufer betrogen.

dpa

298

Wer im Netz auf Shopping-Tour geht, liest vielleicht die Warnung: «nur noch drei Artikel verfügbar». Die Versuchung ist groß, schnell zuzuschlagen. (Bild: dpa, Arno Burgi/Symbolbild)

Vragen?

Chiel van Spaandonk (chiel.vanspaandonk@sidn.nl)

Thymen Wabeke (thymen.wabeke@sidn.nl)