

Counterfighting Counterfeit

Detecting and taking down fraudulent webshops

Thymen Wabeke | RON++





The screenshot shows the Puma website interface. At the top left is the Puma logo. To the right, there is a search bar with the placeholder text 'Omschrijving', a search icon, and a currency selector set to 'Valuta: Euro'. Below the search bar is a navigation menu with links: 'Contacteer Ons', 'Betaling', 'Scheepvaart & Tracking', 'Privacy Policy', and 'FAQ'. On the left side, there is a 'Categorie' sidebar with links to 'Converse Schoenen Aanbieding Nederland->', 'Converse Schoenen Kopen Nederland->', 'Puma Schoenen Aanbieding Nederland->', and 'Puma Schoenen Kopen Nederland->'. Below this is a 'Nieuw in ons assortiment' section with a link to 'Converse Dames Sneakers Converse Dames Sneakers' priced at €60.35. The main content area is titled 'Nieuwe artikelen voor januari' and displays a grid of 16 women's sneakers. Each item is shown in a card format with an image, a title, and a price. The prices are: €57.43, €58.60, €57.43, €59.77, €60.35, €58.60, €60.35, €57.43, €58.01, €58.60, €60.35, €57.43, €58.01, €58.60, €60.35, €57.43, and €58.01. The grid is organized into four columns and four rows.

Item	Price
Dames Converse	€57.43
Converse Dames Leer	€58.60
Dames Converse	€57.43
Dames Converse	€59.77
Converse Dames Leer	€60.35
Dames Converse	€58.60
Converse Dames Leer	€60.35
Dames Converse	€57.43
Dames Converse	€58.01
Converse Dames Leer	€58.60
Dames Converse	€60.35
Converse Dames Leer	€57.43
Dames Converse	€58.01
Converse Dames Leer	€58.60
Dames Converse	€60.35
Converse Dames Leer	€57.43
Dames Converse	€58.01

nederlandwebshop.nl

The screenshot displays the Hollister website interface. At the top, there is a navigation bar with the Hollister logo, 'Dames' and 'Heren' category tabs, and links for 'Inloggen', 'Register', and 'Winkelwagen'. A search bar is located on the right side of the navigation bar.

The main content area features a grid of ten clothing items, each with a product image, a star rating, a title, a description, and a price. The items are:

- Item 1:** Hollister Ondergoed Heren Lage Taille Multipack Grijs Groen Camo Zwart 11859-FNK. 15 Kleur. BROEK & KORTE BROEK. Price: €30.60 - €22.31. Rating: 4 stars.
- Item 2:** Hollister T Shirt Heren Logo Graphic Korte Mouwen Donkerblauw 21170-HLT. 15 Kleur. TOPS. Price: €30.70 - €22.38. Rating: 5 stars.
- Item 3:** Hollister Jas Dames All-weather Stretch Sherpa-lined Zwart 45801-GXL. 1 Kleur. JASSEN. Price: €98.35 - €69.73. Rating: 5 stars.
- Item 4:** Hollister Joggingbroek Heren Advanced Stretch Cargo Twill Olijfgroen 97393-SXN. 4 Kleur. BROEK & KORTE BROEK. Price: €50.11 - €35.98. Rating: 5 stars.
- Item 5:** Hollister Blouses Dames Fluwel Off-the-shoulder Goud 49289-JQI. 2 Kleur. TOPS. Price: €30.60 - €22.31. Rating: 4 stars.
- Item 6:** (Image of dark jeans). Rating: 4 stars.
- Item 7:** (Image of a black sneaker). Rating: 4 stars.
- Item 8:** (Image of a red polo shirt). Rating: 4 stars.
- Item 9:** (Image of blue jeans). Rating: 4 stars.
- Item 10:** (Image of a red and black beanie). Rating: 4 stars.

Who? Why?

- Consumer demand for counterfeit goods
 - \$1.2 billion seized at US border in 2017
 - €670 million seized at EU border in 2016
- Low investments, easy money
- Less attention by law enforcement



Louis van Dijk on Twitter: "@kle... X +
 https://twitter.com/AllsenzA/status/10...

Search Twitter Q Have an account? Log in X

Louis van Dijk
 @AllsenzA Follow

@kleeman DM Hallo Mandy, 19 november heb ik via mandykleewein.nl een paar Dr. Martens schoenen besteld. Via creditcard betaald maar schoenen zijn nooit geleverd en maar de betaling van € 95 is bij mij wel afgeschreven. Wil je voor mij uitzoeken waar het is misgegaan.

8:11 AM - 7 Jan 2019

1 Like

mandy kleewein @kleeman · Jan 10
 Replying to @AllsenzA
 Vreemd. Deze domeinnaam is al een half jaar niet meer door mij in gebruik en het is ook nooit een webshop geweest maar een site met mijn journalistieke stukken. Ik zou contact opnemen met je bank en aangifte doen.

2 1
 1 more reply



NOS TELEERST 133 km 1°

Waar komen al die nep-webshops toch vandaan?

02-05-2018, 19:57 AANGEPAST 03-05-2018, 14:57 ECONOMIE

Minimaal 1 op de 5 webshops is nep, denkt de Consumentenbond. Wereldwijd zijn er naar schatting 700.000 nep-webshops actief. Hoe kan het dat er online zoveel malafide webshops zijn?

De Consumentenbond liet na eigen onderzoek 850 malafide webshops verwijderen. Op die websites werden vooral merkproducten aangeboden voor spotprijzen. De producten werden niet geleverd of bleken nep.

Webshopnamen overnemen

De werkwijze van de oplichters is inmiddels wel bekend, zegt



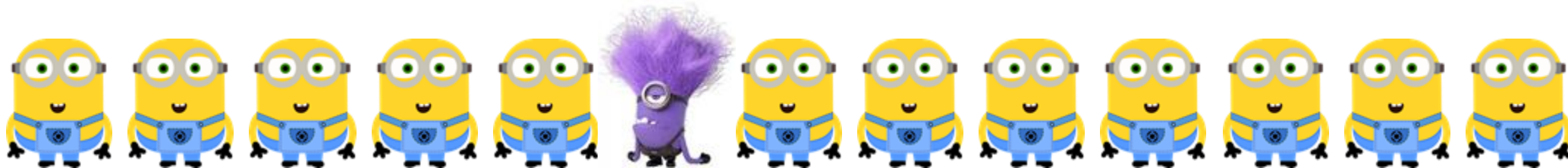
Rabobank

ICs VISA MasterCard
 INTERNATIONAL CARD SERVICES



How to detect fake webshops at scale?

(.nl has over 5,9 million domain names)



2016

- BrandCounter
- Study with registrar (~3.7k domains removed)

2018

- Student project machine-learning based detection

2019

- Study with International Card Services (747 domains removed)
- **Development of FaDe (2088 domains removed)**

2020

- **Publication at PAM2020 ☺**
- **Future research...**

FaDe: a robust fake detector



Adaptive



Pro-active

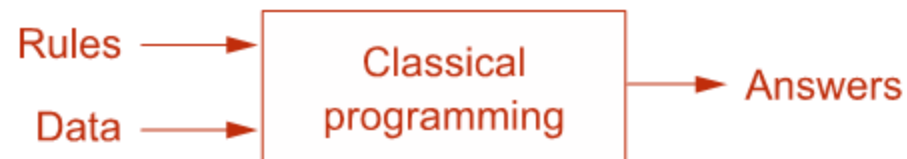


Accurate

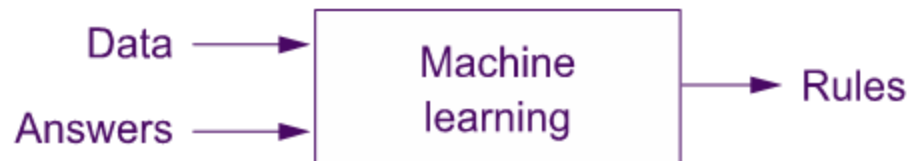


Adaptive by extracting rules

Knowledge-driven programming:



Data-driven programming:





Machine-learning ingredients

Answers (i.e. ground truth):

- Examples found during earlier studies (469, Sept '19)

Data (i.e. features):

- WHOIS (registrar, registrant e-mail, re-registration)
- Content (html title, description, page type)
- Infrastructure (AS, SMTP configured, TLS issuer)

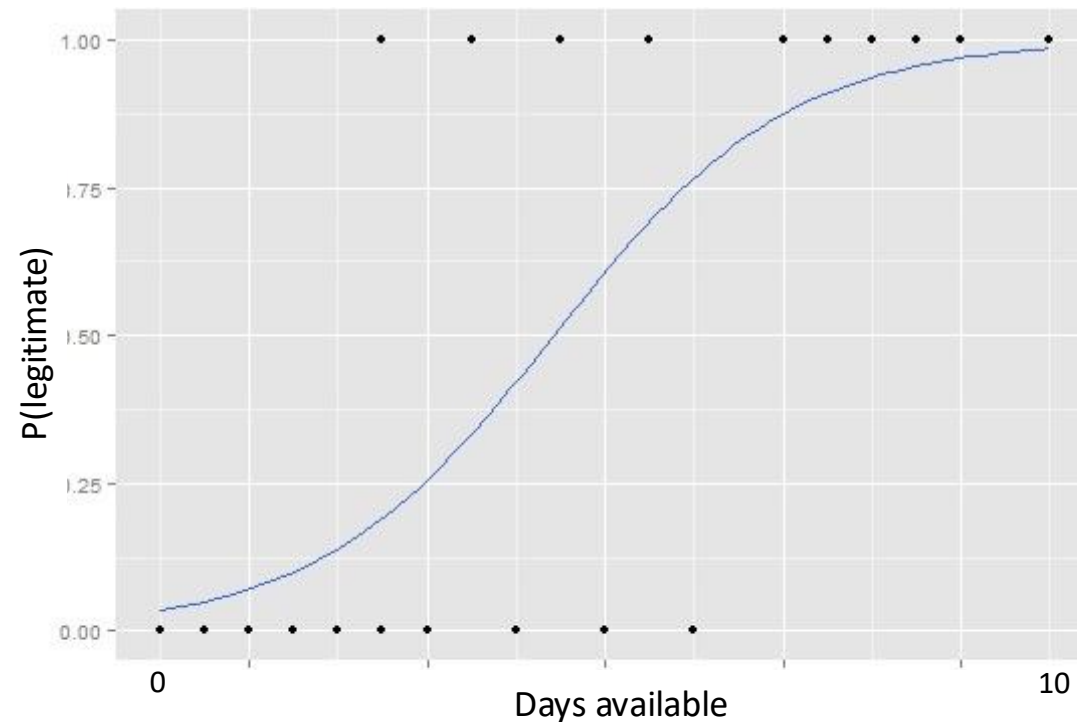
Algorithm:

- Logistic regression

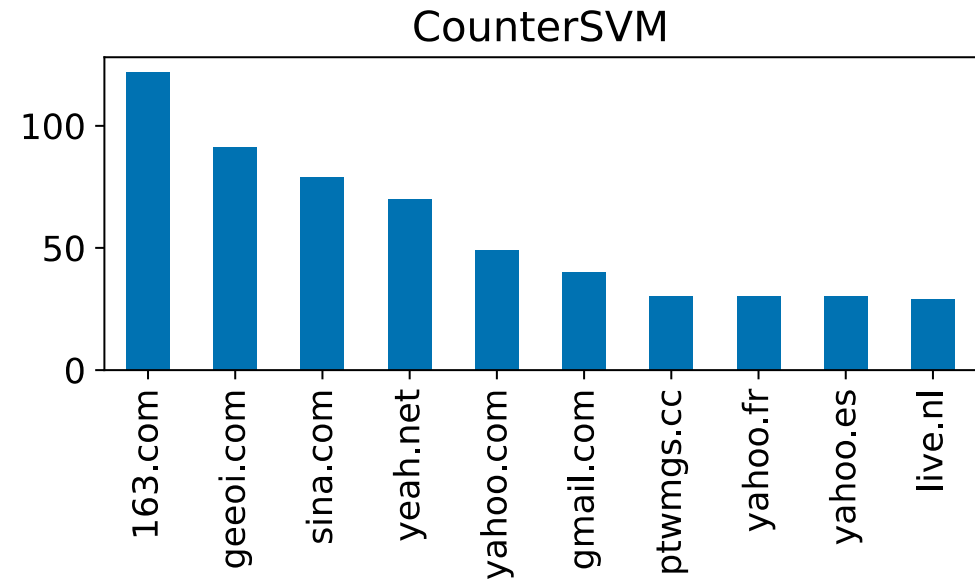
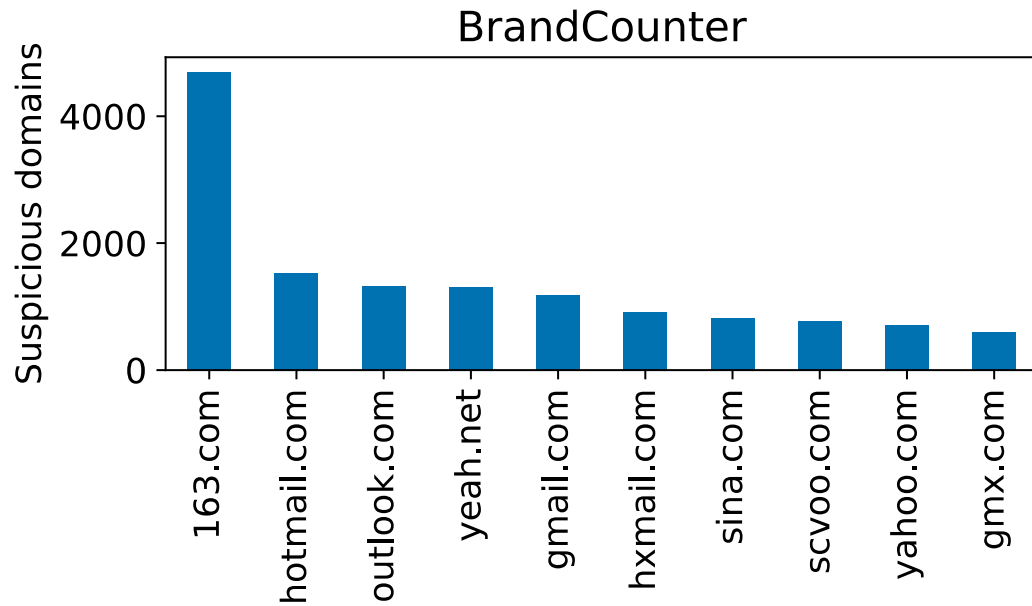


Why logistic regression?

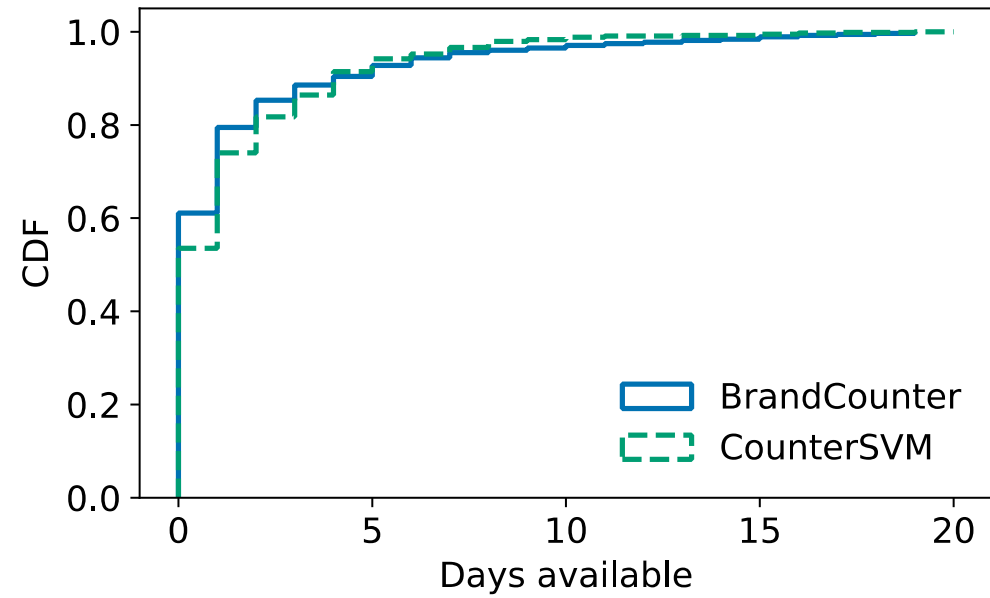
- Linear: interpretable by default
- Calibrated: inferences have confidence measure
- Simple: less chance of overfitting, computes fast



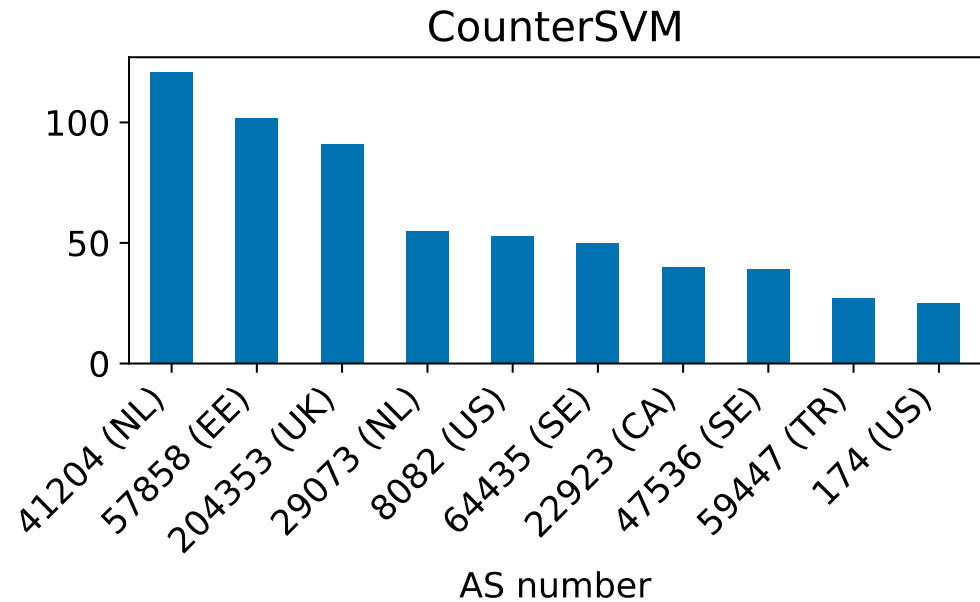
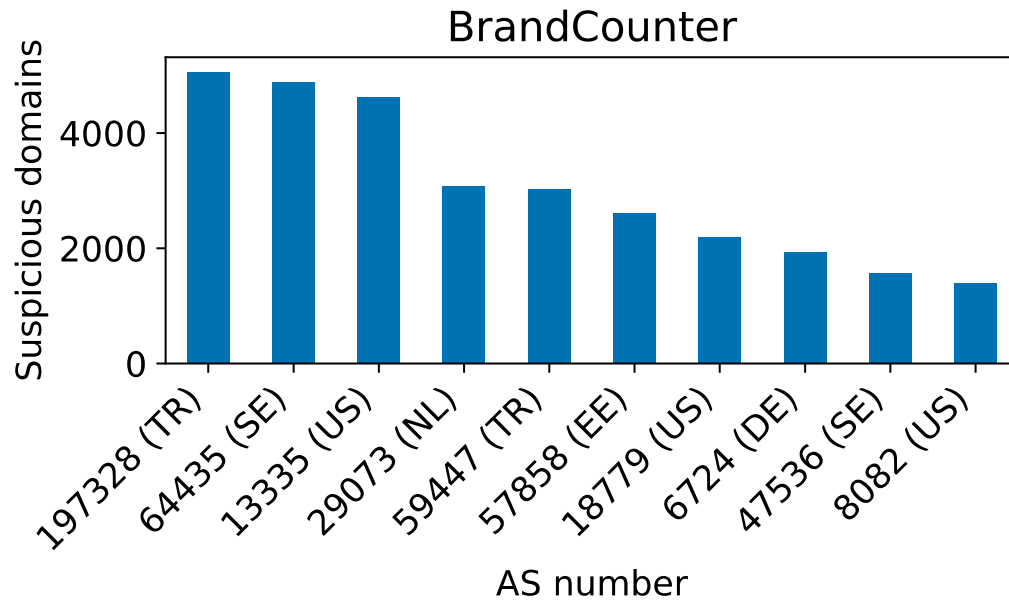
Registrant e-mail domain



Days before registration



Hosting AS





Detect before they harm

Fake Webshops

This page lists the domain names that are found by Padawans.

Show entries

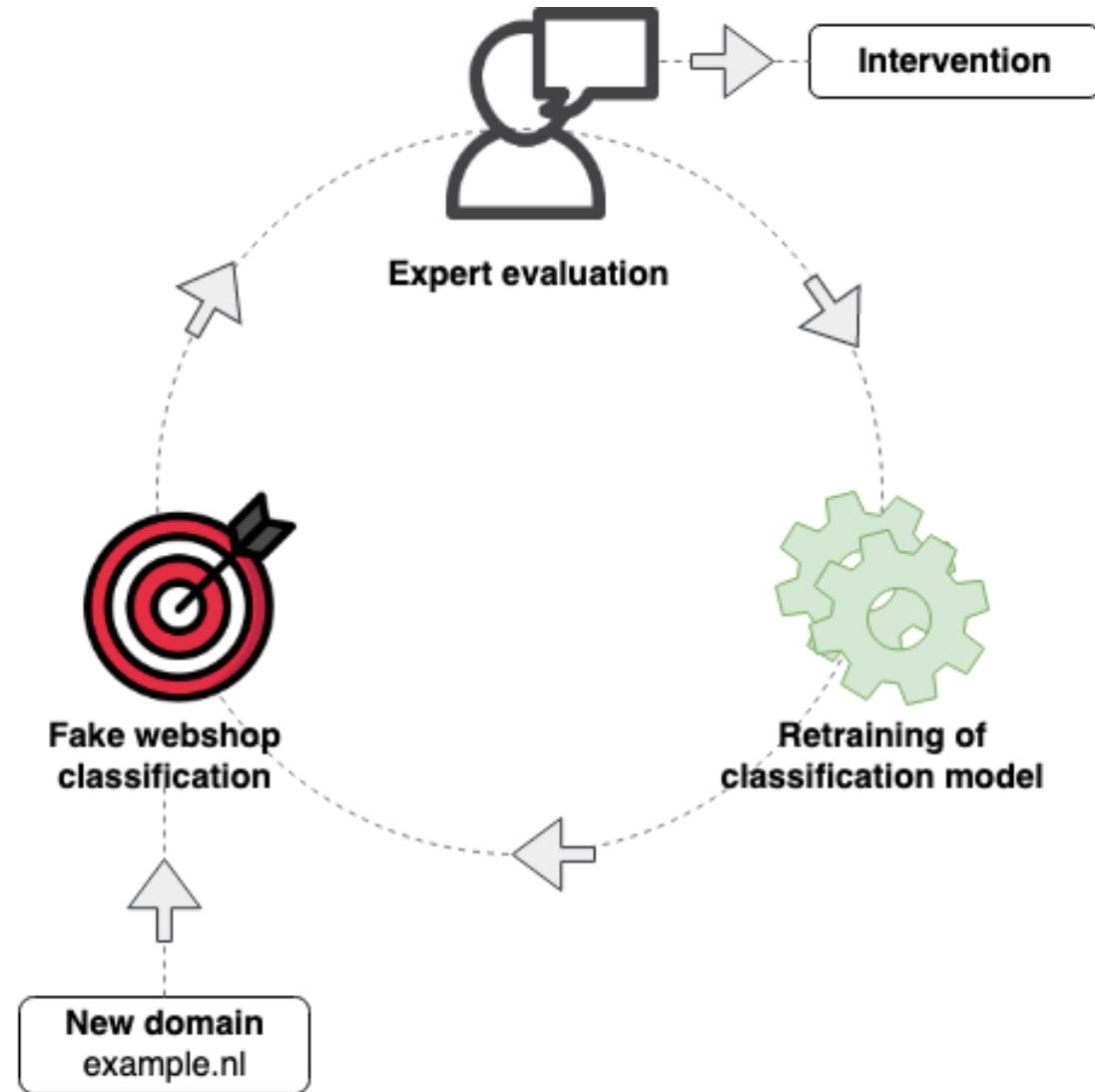
Search:

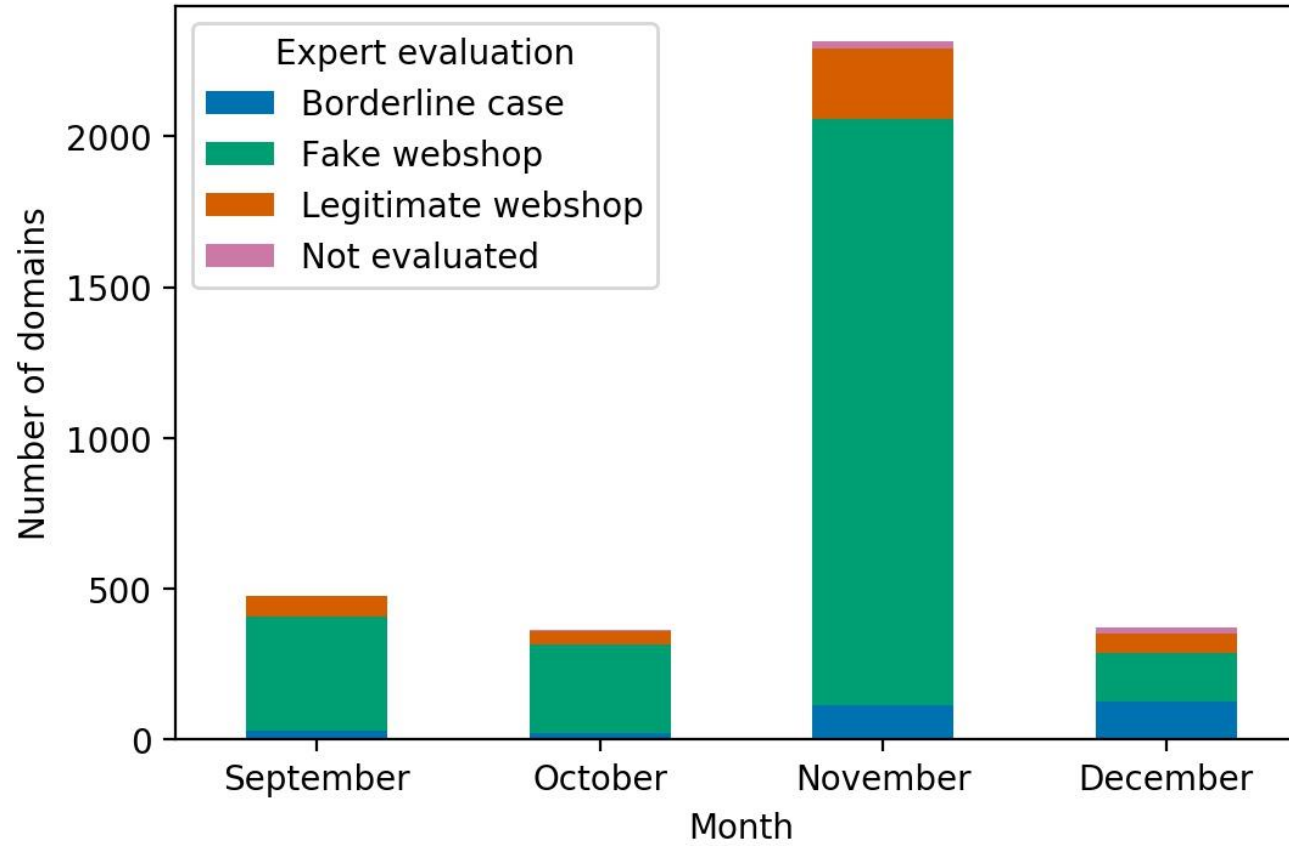
Domain Name	Added	Registrar	Registrant	Mail	Feedback	Submit Feedback	Link	Phone	Whois
+ echo	2020-01-03 08:04:51.432482					Fake Valid Unknown	click	+49.0	click
+ npot	2019-12-26 08:23:01.263207					Fake Valid Unknown	click	+84.3	click
+ tank	2019-12-23 08:08:08.768590					Fake Valid Unknown	click	+45.3	click
+ only	2019-12-23 08:07:45.236334					Fake Valid Unknown	click	+86.1	click
+ nikel	2019-12-23 08:07:43.051879					Fake Valid Unknown	click	+86.3	click
+ mtk	2019-12-23 08:07:42.009627					Fake Valid Unknown	click	+1.67	click
+ mrw	2019-12-23 08:07:41.722979					Fake Valid Unknown	click	+45.3	click
+ miko	2019-12-23 08:07:39.971509					Fake Valid Unknown	click	+93.1	click
+ bega	2019-12-23 08:07:06.592282					Fake Valid Unknown	click	+45.3	click
+ drm	2019-12-21					Fake Valid Unknown	click	+49.0	click





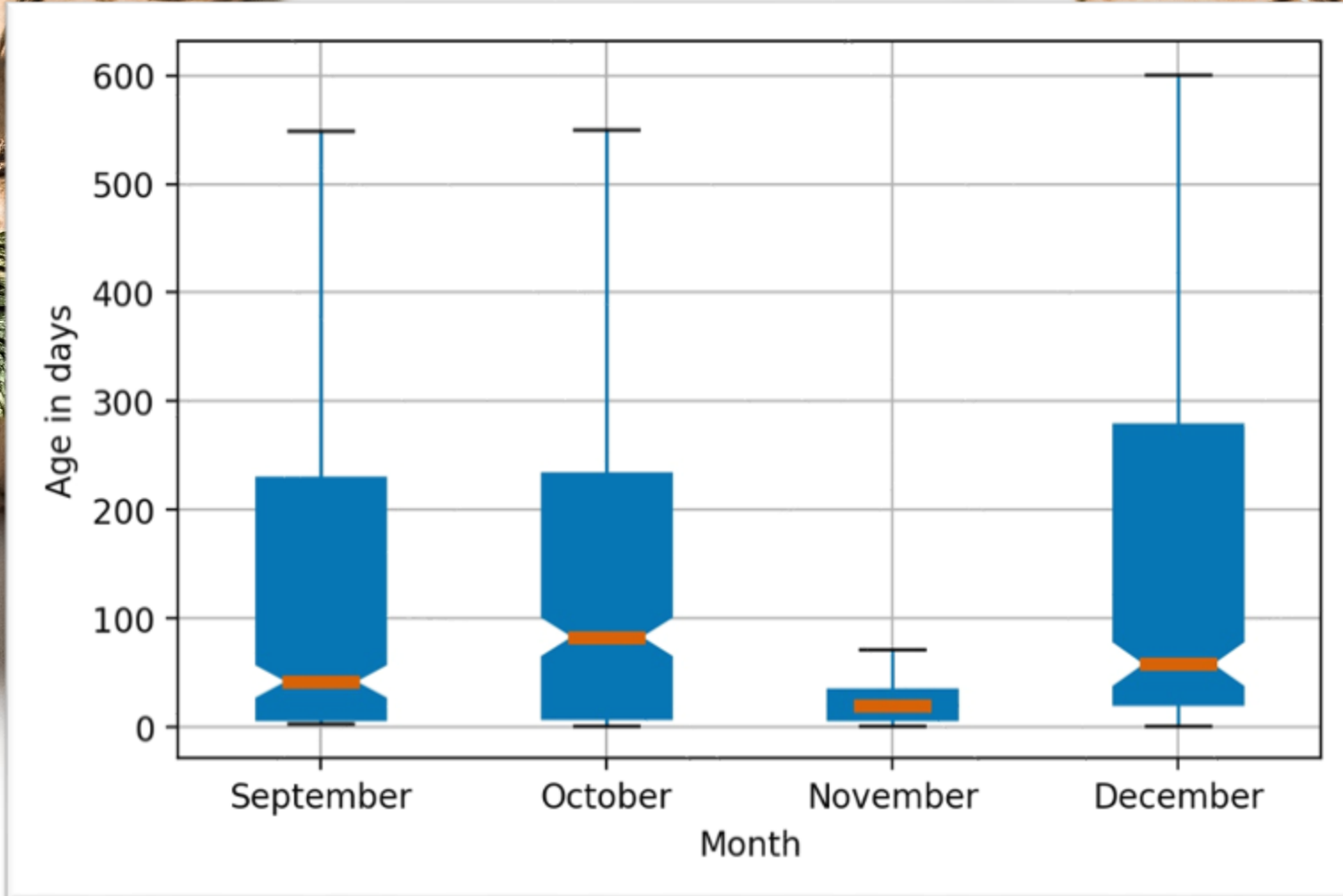
Learn from feedback





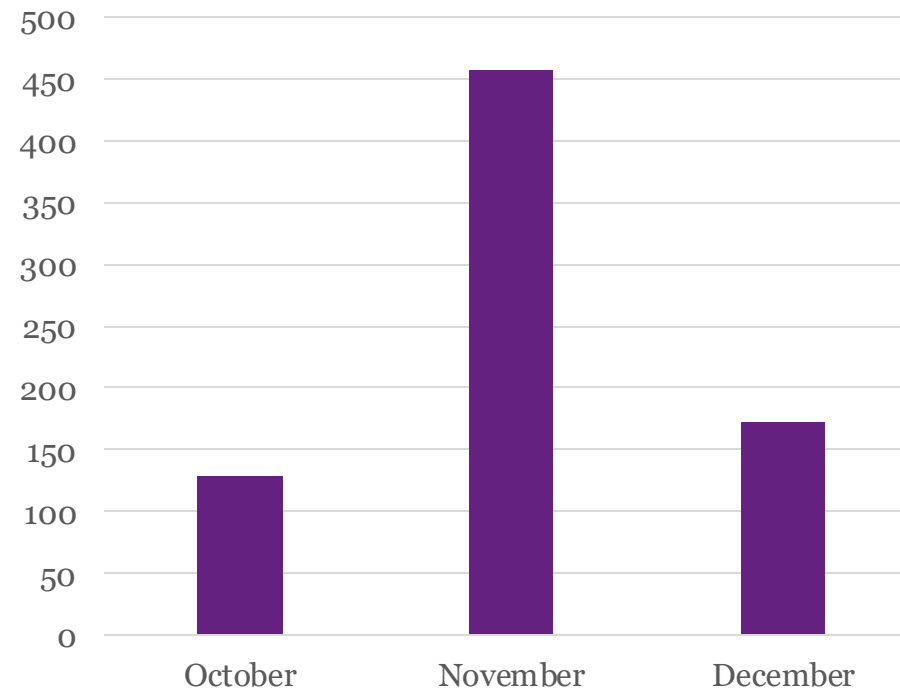
	Notified	Registrars	Removed by registrar	Art 16 by SIDN
Dec '19	2091	3	2088	3

November peak: scam season



November peak: better model

- 458 found in November, overlooked in October
- 173 found in December, overlooked in November



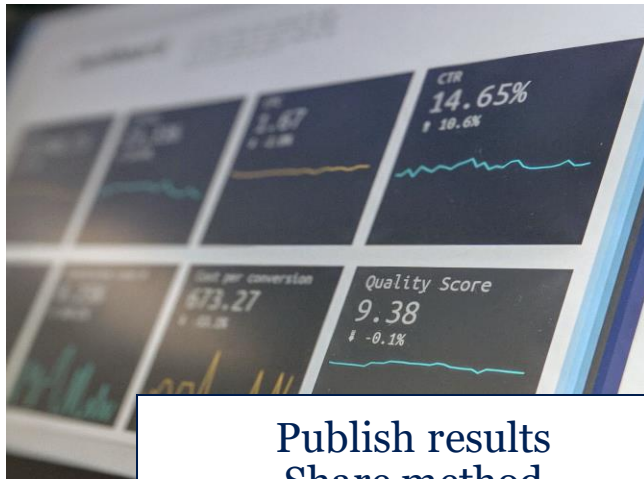
Next steps



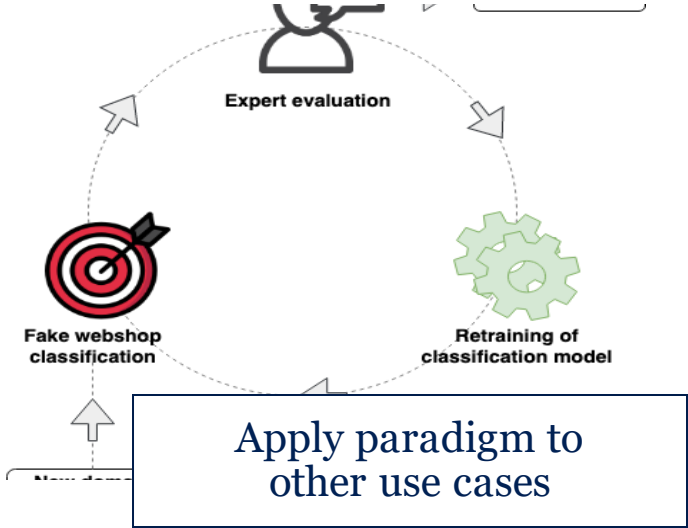
Better evaluation
Keep up-to-date



Identify campaigns
Follow the money
Effective interventions



Publish results
Share method



Photos: Roman Synkevych, Stephen Dawson and Michael Longmire on Unsplash

