Fake web shops: detect them before they do harm

Thymen Wabeke - thymen.wabeke@sidn.nl / Sascha de Cocq - dcocq@icscards.nl

Summary

- Fake web shops do not deliver, deliver counterfeit products or commit credit card fraud.
- An estimated 20% of all web shops is fake[1] and these shops form a increasing problem for our online society.
- Our research aims at developing and evaluating an operational fake web shop detector that is adaptive, accurate and proactive.
- A pilot by SIDN Labs and ICS resulted in the detection of 893 fake web shops in the .nl-zone.

Future work

- How to adapt models such that they are robust against changing tactics?
- How to automatically improve the detection method using expert evaluation (active learning)?
- How to get the detector in production and add relevant datasets of other stakeholders in the web shop value chain?
- How to collaborate with other TLDs?

Pilot by SIDN Labs & ICS

Goal

Train and evaluate a classifier that discriminates suspicious from trustworthy web shops. This step towards an operational detector mainly focuses on the accuracy requirement.

Approach

- Train a classifier using 231 shops that are reported by ICS
- Apply the model to all domains in the .nl-zone
- ICS analysts evaluate the suspicious shops
- ICS starts Notice and Take Down (NTD) procedure for the true positives

Insights

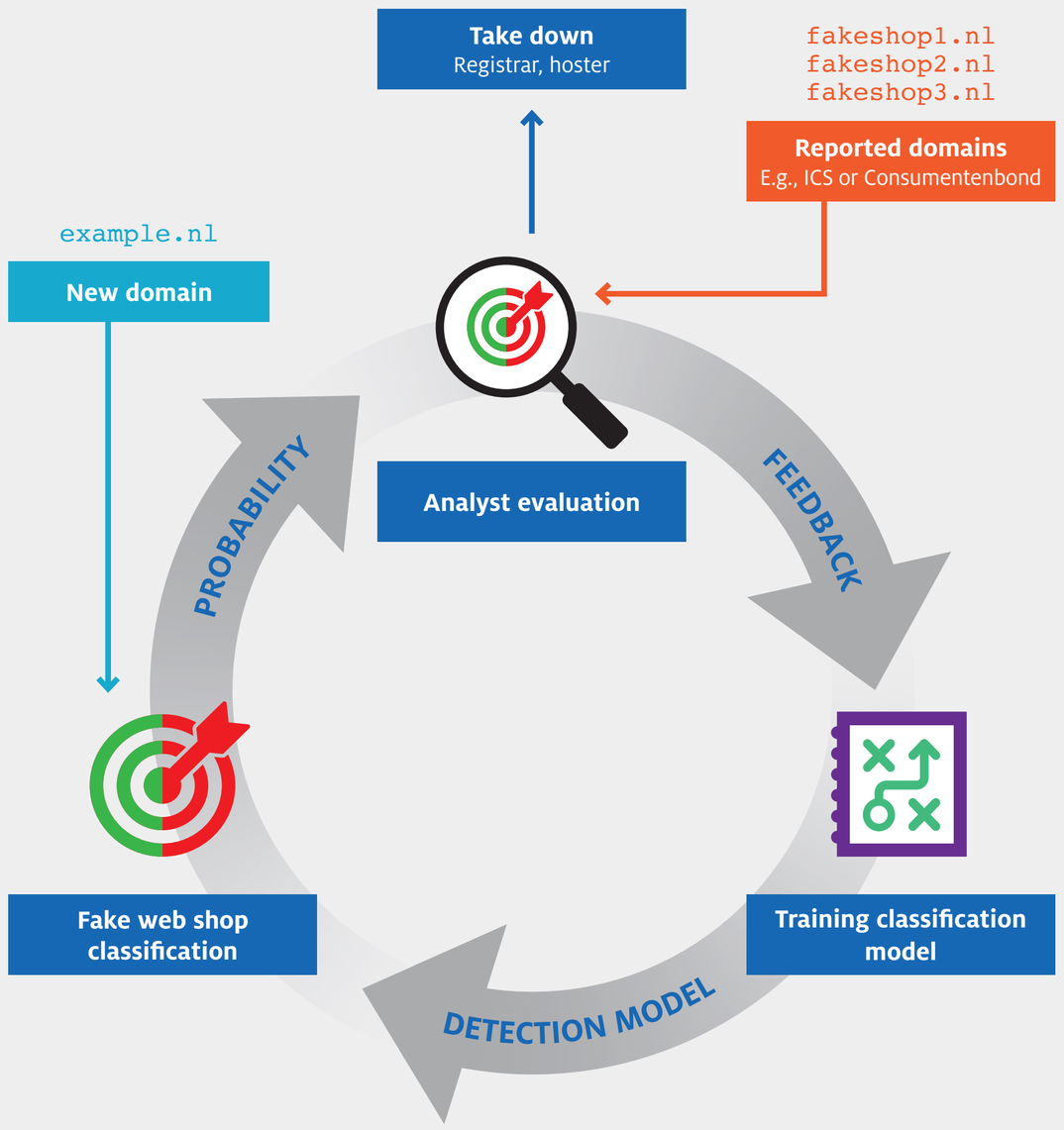
- We proactively found 893 fake web shops using this first version of the classifier.
- Expert evaluations are valuable feedback to improve and update the detection model.
- The fake web shops reported by ICS are similar to the ones found by SIDN, Consumentenbond and others in the past.
- The NTD procedure is time consuming.

Classifier evaluation

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

Feature examples

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



Requirement	Implication
Adaptive	• Keep updating models to adapt to changing tactic of adversaries
Accurate	• Multiple inputs and heterogeneous data sources • Analyst evaluate suspicious shops • Use their feedback to improve the detection model
Proactive	• Early detection • Efficient takedown process

[1] *https://nos.nl/artikel/2230087-waar-komen-al-die-nep-webshops-toch-vandaan.htm*