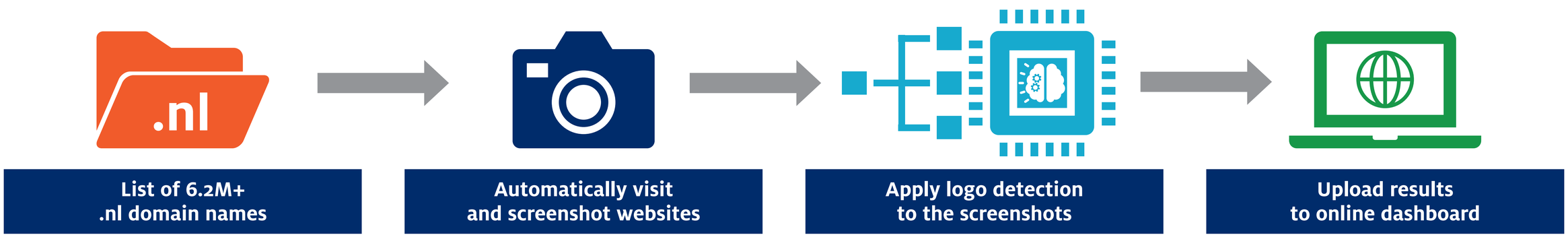
LogoMotive: identifying online scams through logo detection on .nl websites

Thijs van den Hout – thijs.vandenhout@sidn.nl & Thymen Wabeke – thymen.wabeke@sidn.nl

Summary

- Scammers trick people into using their malicious websites by abusing the familiarity and trust that wellknown logos instil.
- LogoMotive enables organisations to find malicious .nl websites based on logo misuse; it detects logos by using the YOLO deep-learning object detection model.
- We tested whether logo detection can increase the safety of .nl by applying our system to all 6.2M+ .nl domains in two successful pilots with the Dutch national government and the Thuiswinkel.org trustmark.
- Abuse analysts manually evaluated 20k+ domain names whose website used a government or Thuiswinkel logo.



Insight 1 - Logo detection reveals malicious websites

- We found 6 phishes that abuse the Dutch national government's logo and 208 webshops that misuse Thuiswinkel's trustmark.
- Malicious websites were often not reported on other abuse feeds and were discovered quickly.

Insight 2 - Logo detection reveals suspicious redirects and dormant risks

- We found 82 suspicious redirects to legitimate government domain names, which may later be used to host malicious content, including spear-phishing.
- Logo detection can be used to proactively gain an edge over scammers and keep an eye on suspicious domain names.

Insight 3 - Logo detection gives organisations more insight into their domain name portfolio

- A complete overview prevents unwanted cancellation and enables monitoring of security standards.
- We discovered 318 legitimate government domains not present in their domain name register and 54 domains belonging to legitimate Thuiswinkel.org members.

Future work

- Implementation in SIDN BrandGuard.
- Automatic prioritization of results.
- Detecting logos on more than just the homepage.
- Code & full paper: logomotive.sidnlabs.nl.

Table 1: Pilot results with the Dutch national government

Label	Full .nl-zone	Newly-registered
Total	12862	53
Without gov. logo (FP)	1164 (9.05%)	0 (0%)
With gov. logo (TP)	11698 (**90.95%**)	53 (100%)
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 (satire, etc.)	75 (0.58%)	5 (9.43%)
Government domains	952 (7.40%)	4 (7.55%)
In portfolio	636 (4.94%)	2 (3.77%)
Not in portfolio	316 (2.46%)	2 (3.77%)

Table 2: Pilot results with Thuiswinkel.org's webshop trustmark

Label	Domains	Unique URLs
Total	10669	3890
Without trust mark (FP)	83 (0.78%)	64 (1.65%)
With trust mark (TP)	10586 (**99.22%**)	3826 (98.35%)
Benign	10324 (96.77%)	3691 (94.88%)
Trustmark abuse	208 (1.95%)	106 (2.72%)
Discovered	54 (0.51%)	29 (0.75%)

Table 3: Implementation of security standards

Government domains	In domain name register	Not in domain name register
Implements DNSSEC	98%	74%
Implements DMARC	92%	41%

SIDN Labs

Rijksoverheid

Thuiswinkel.org