Characterizing and Mitigating Phishing Attacks at ccTLD Scale

Giovane C. M. Moura[1,2], Thomas Daniels[3,4], Maarten Bosteels[3], Sebastian Castro[5], Moritz Müller[1,6], Thymen Wabeke[1], Thijs van den Hout[1], Maciej Korczyński[7], Georgios Smaragdakis[2]

1: SIDN Labs **2**: TU Delft **3**: DNS Belgium **4**: KU Leuven
5: .IE Registry **6**: University of Twente **7**: University of Grenoble Alps

2024-10-25
Alice and Eve, Leiden, The Netherlands

Outline

Paper presented last week at ACM CCS 2024

Wild bison in Utah, US

Paper PDF:

$whoami

- Data Scientist at SIDN Labs
- Assistant Prof. at TU Delft (Cyber Security/EWI)
- PhD UTwente (2013)

- SIDN Labs?
- Research in Industry?
- Not selling anything?
- Who funds us?
- (we're a bit of an outlier)
- We do bunch of things:
  - academic papers
  - open source software
  - internet standards (IETF)
  - future internet
  - we take internships
  - https:/sidnlabs.nl/en

Phishing is a major threat on the Internet

- FBI: 300k complaints, US$160 million in losses in 2022 [1]
- One of most important cyber threats for national security – EU ENISA, US CISA [2, 3]
- Phishing deceive users to provide private data

Phishing at Three ccTLDs

1. First time 3 ccTLDs come together to analyze phishing:
   - The Netherlands' `.nl` (SIDN)
   - Ireland's `.ie` (.IE Registry)
   - Belgium's `.be` (DNSBelgium)
2. Longitudinal study (10 years)
3. Complete view of the zones
   - ccTLD registries are responsible for running their countries' zone

Expanding phishing characterization with full zone view:

	Previous Works	Ours
Time	1 year	4–10 years
Companies	10	1233
Domains	1.4k	28.7k

Phishing at Three ccTLDs

1. First time 3 ccTLDs come together to analyze phishing:
   - The Netherlands' `.nl` (SIDN)
   - Ireland's `.ie` (.IE Registry)
   - Belgium's `.be` (DNSBelgium)
2. Longitudinal study (10 years)
3. Complete view of the zones
   - ccTLD registries are responsible for running their countries' zone

Expanding phishing characterization with full zone view:

	Previous Works	**Ours**
Time	1 year	4–10 years
Companies	10	1233
Domains	1.4k	28.7k

ccTLDs compared

ccTLD	.nl	.ie	.be
# Domains	6.1M	330.1k	1.7M
Reg. Policy	Open	Restricted	Open
Country Population	17.5M	4.9M	11.5M

Table 1: ccTLDs overview.

- Restricted registration: check Irish ID, passport, or business in Ireland
- Open registration ( ): anyone can register a domain

Datasets: Phishing blocklist

	.nl	.ie	.be
Domains	25,389	555	2,810
Period	∼10 years	∼4 years	∼4 years
Years	2013–2023	2019–2023	2019–2023

Table 2: Netcraft phishing blocklist dataset

We triangulate the blocklist dataset with ccTLDs' private datasets:

- historical registration database
- Web measurements
- DNS measurements

Datasets: Phishing blocklist

	.nl	.ie	.be
Domains	25,389	555	2,810
Period	∼10 years	∼4 years	∼4 years
Years	2013–2023	2019–2023	2019–2023

Table 2: Netcraft phishing blocklist dataset

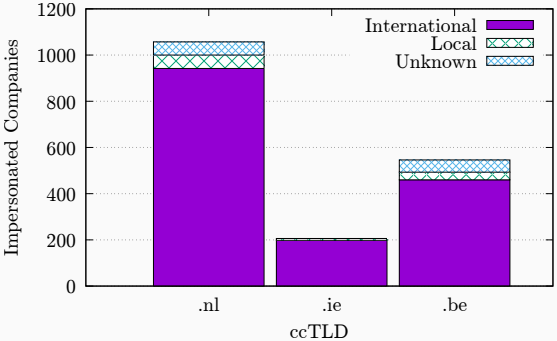
We triangulate the blocklist dataset with ccTLDs' private datasets:

- historical registration database
- Web measurements
- DNS measurements

Outline

Do they target mostly national companies?

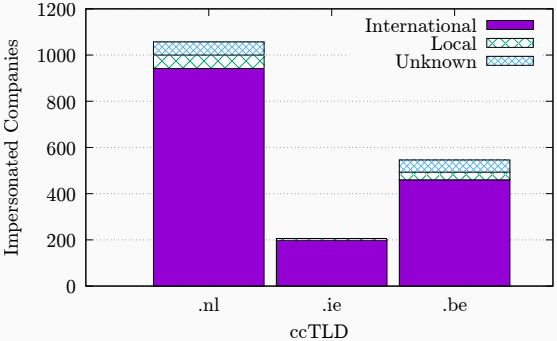
- Citizens have trust in their ccTLDs
  - Govs use it
- Do attackers exploit this trust for phishing?



- Most impersonated companies are **International**
- So most attackers **do not seem to care which TLD they use**.
  - Is it really so?

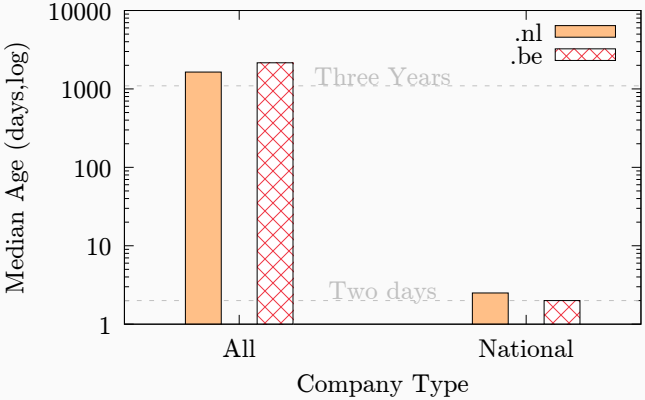
Do they target mostly national companies?

- Citizens have trust in their ccTLDs
  - Govs use it
- Do attackers exploit this trust for phishing?



- Most impersonated companies are **International**
- So most attackers **do not seem to care which TLD they use**.
  - Is it really so?

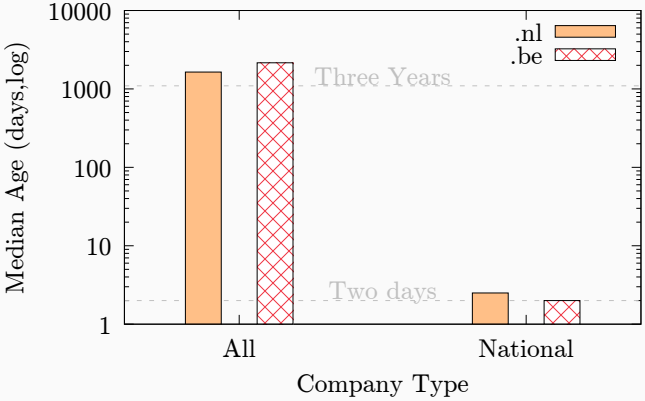
National companies vs International Companies



We see a pattern:

1. **International** companies impersonated with old domains
2. **National** companies impersonated with new domains

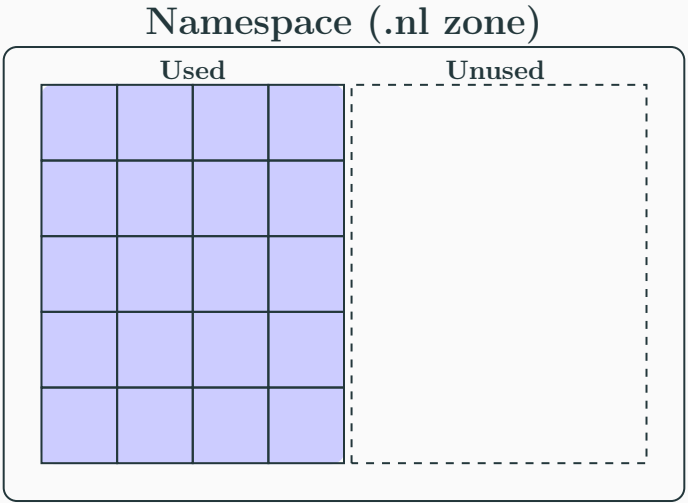
National companies vs International Companies



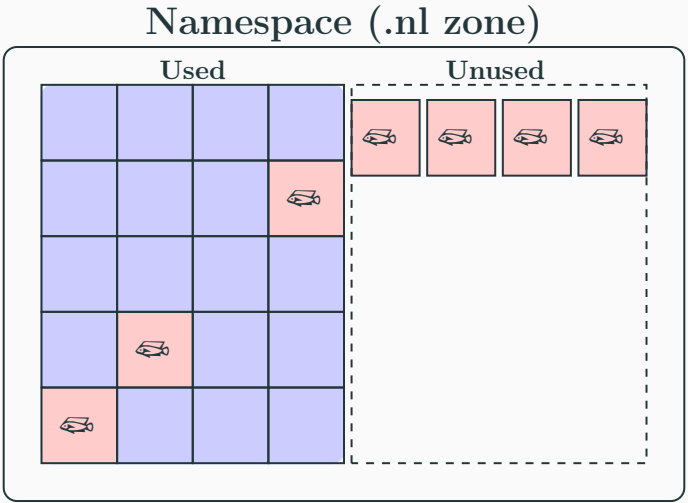
We see a pattern:

1. **International** companies impersonated with old domains
2. **National** companies impersonated with new domains

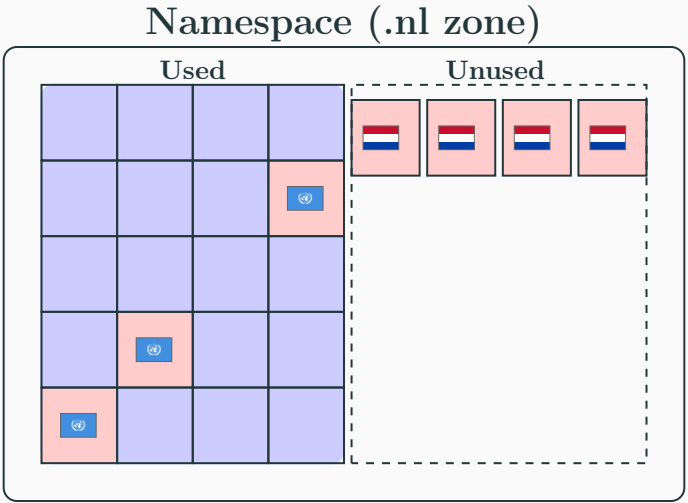
Two Attack Strategies



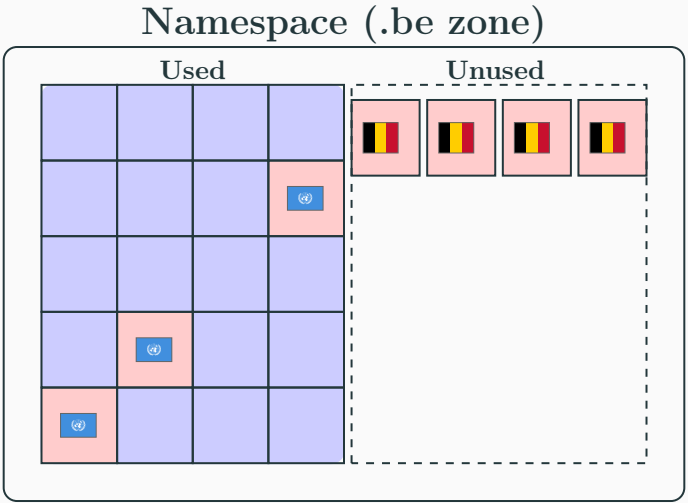
Two Attack Strategies



Two Attack Strategies



Same for .be



Two Attack Strategies

Target	ING bank	Apple
Domain	`activate-creditcard.nl`	`pastries-AMS.nl`
Domain Type	New	Old (compromised)
Costs	✓ Reg, DNS, Hosting	✗ Free
Likely attacker	"Local"	"International"
Share	20%	80%

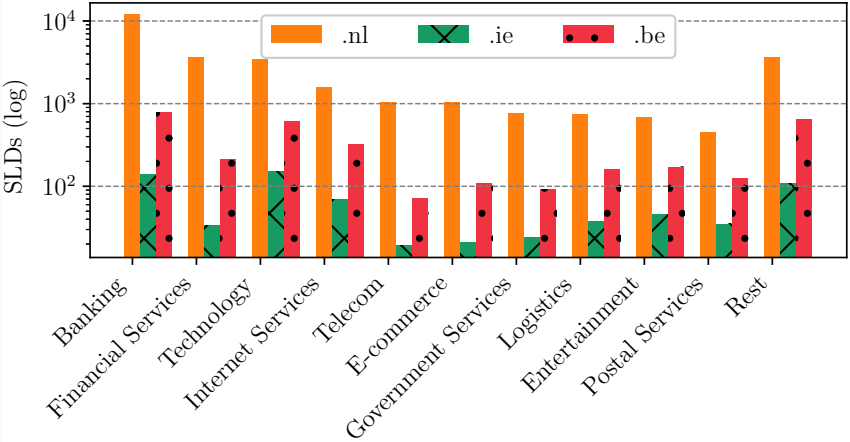
Table 3: Local and International attack strategies

Top 10 impersonated companies (`.nl` zone)

Rank	Company	Domains	Median Age (days)
1	Microsoft	2,319	2,251
2	PayPal	2,134	1,751
3	ING	1,815	1
4	ICS	1,410	2
5	Apple	1,276	1,775
6	ABN AMRO	1,259	1
7	Google	1,236	1,416
8	Rabobank	1,222	1
9	Webmail Users	1,054	2,247
10	Netflix	756	1,653

Top 10 impersonated companies in phishing attacks on the `.nl` zone ( ).

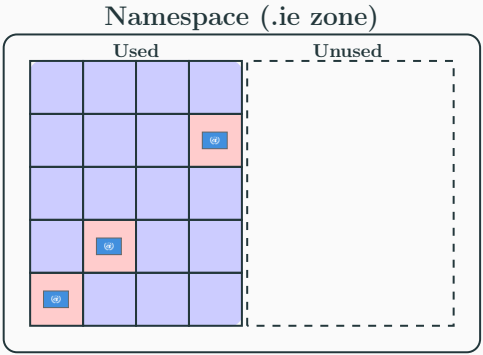
Most Popular Market Segments



But what about Ireland?

Only two new phishing domains

- `.ie` = restricted registration policy
- Restricted policy prevents part of the phishing attacks
  - But cannot prevent compromised domain names



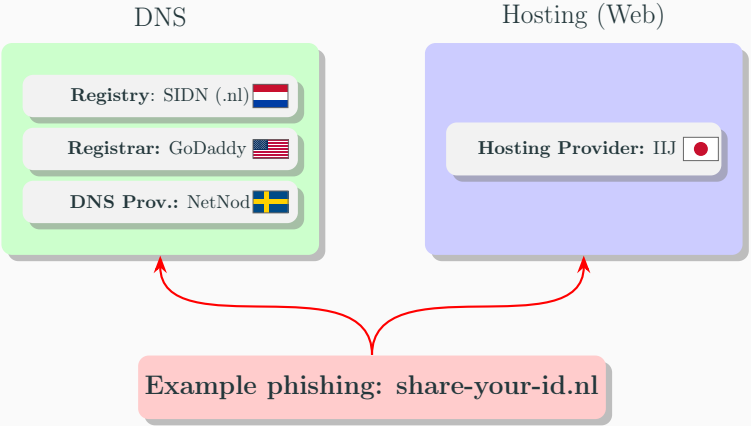
Outline

From characterization to Mitigation

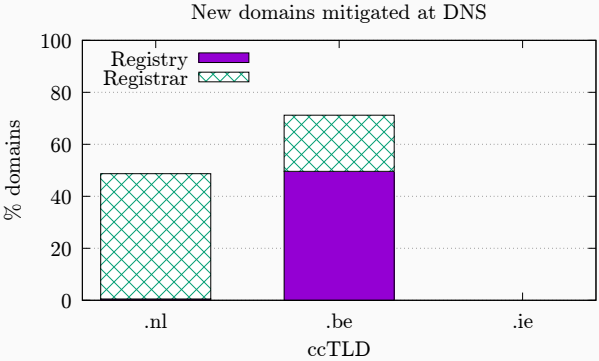
- Phishing mitigation ***is not*** a single event
- Different parties can mitigate it independently
  - registrant (example.nl) → Registrar (GoDaddy) → Registry (SIDN)

From characterization to Mitigation

- Phishing mitigation ***is not*** a single event
- Different parties can mitigate it independently
  - registrant (example.nl) → Registrar (GoDaddy) → Registry (SIDN)

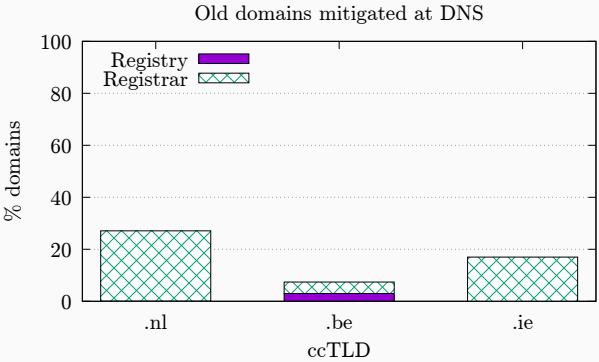


DNS mitigation and ccTLD policy: new domains



- `.be` suspend new domains ASAP
- `.nl` notifies registrars, hosting who take action
- Rest is mitigated at Web level

Phishing Mitigation at DNS: Old Domains



- Most old domains are compromised
  - Web mitigation is preferred
- Exceptions: aged domains

Outline

Call for Action

1. More research on compromised domains
   - Most phishing is compromised (80%)
   - Most research focuses on new domains
2. Revisit registration and abuse policies for registries
   - Registries discussing results internally

Summary

Three EU ccTLDs on the largest phishing characterization study

1. Two main attacker types:
   - National companies → new domains
   - Intl' → old, compromised domains
2. Policy impact on mitigation:
   - `.ie`'s restricted registration prevents new phishing domains
   - `.be` registry does most of DNS mitigation.
   - `.nl`'s registrars do most of DNS mitigation
3. Call for action on compromised domains

Real phishing victims in the Netherlands go on the record

Source: NOS.nl

References i

[1] US Federal Bureau of Investigation, Internet Crime Complaint Center.
Internet Crimer Report.
https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, 2023.

[2] European Union Agency for Cybersecurity.
ENISA Threat Landscape 2023.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, 2023.

References ii

[3] European Union Agency for Cybersecurity.
Malware, Phishing, and Ransomware.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, 2024.