

Characterizing and Mitigating Phishing Attacks at ccTLD Scale

Giovane C. M. Moura^{1,2}, **Thomas Daniels**^{3,4}, Maarten Bosteels³,
Sebastian Castro⁵, Moritz Müller^{1,6}, Thymen Wabeke¹,
Thijs van den Hout¹, Maciej Korczyński⁷, Georgios Smaragdakis²

1: SIDN Labs 2: TU Delft 3: DNS Belgium 4: KU Leuven

5: .IE Registry 6: University of Twente 7: University of Grenoble Alps

2024-10-29

RIPE 89, Prague, Czechia



Outline

Introduction

Impersonated companies

Comparing companies among ccTLDs

Phishing mitigation

Call for Action

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 deceives users to provide private data



Phishing-as-a-Service: LabHost

B B C

Home News Sport Business Innovation Culture Travel Earth Video Live

Police bust global cyber gang accused of industrial-scale fraud

18 April 2024

Share ↵

Tom Symonds

Home Affairs correspondent



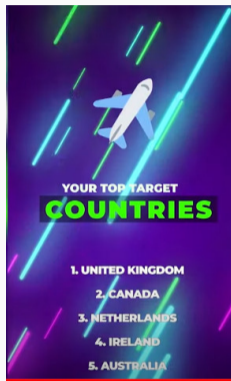
<https://www.bbc.com/news/uk-68838977>

Phishing-as-a-Service: LabHost

LabHost stats:

- Subscription model: €300 per month
- 40,000 domains linked to LabHost
- 10,000 users worldwide
- 170 brand templates
- Hosting infrastructure

Takeaway: **Professional criminals scamming vulnerable people**



Labhost top countries
Source: [The Telegraph](#)

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` (**DNS Belgium**)
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` (**DNS Belgium**)

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 blacklist



.nl



.ie



.be

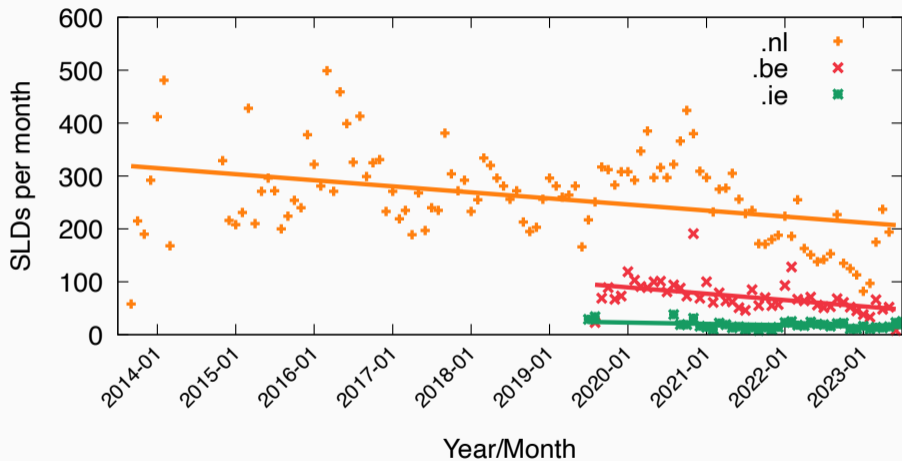
Domains	25,389	555	2,810
Period	~10 years	~4 years	~4 years
Years	2013–2023	2019–2023	2019–2023

Table 2: Netcraft phishing blacklist dataset

We triangulate the blacklist dataset with ccTLDs' private datasets:

- Historical registration database
- Web measurements
- DNS measurements

Phishing domains per month



SLD: Second-level domain ([example.nl](#))

Outline

Introduction

Impersonated companies

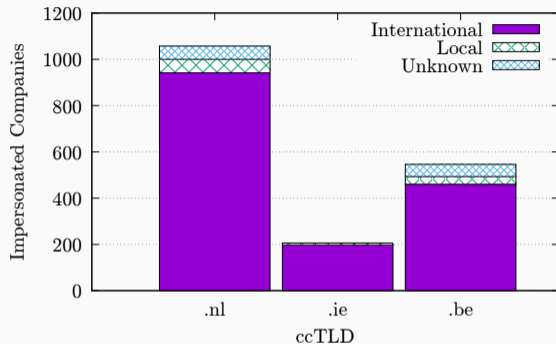
Comparing companies among ccTLDs

Phishing mitigation

Call for Action

Do they target mostly national companies?

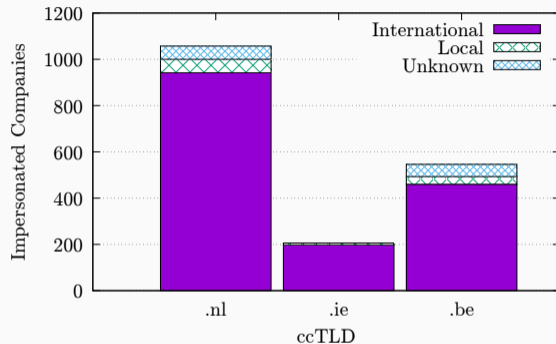
- Citizens have trust in their ccTLDs
 - Govs use it
- Do attackers exploit this trust for phishing?



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

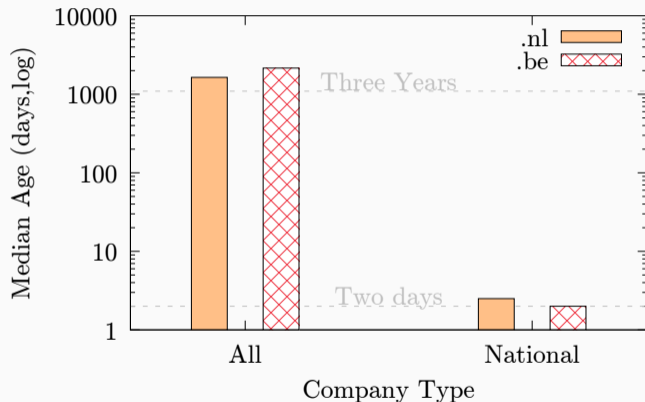
Do they target mostly national companies?

- 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?**

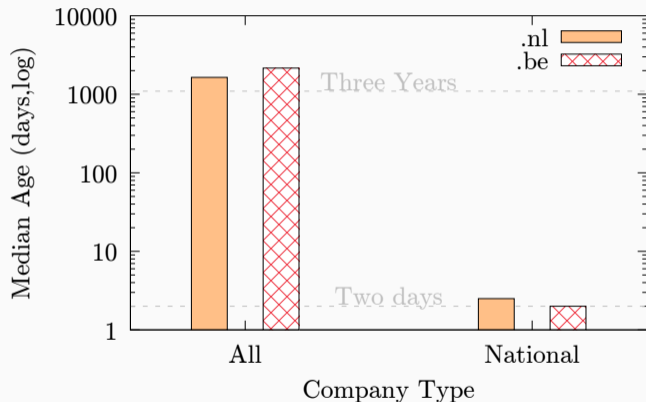
National companies vs international companies



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

Finding: two attack strategies

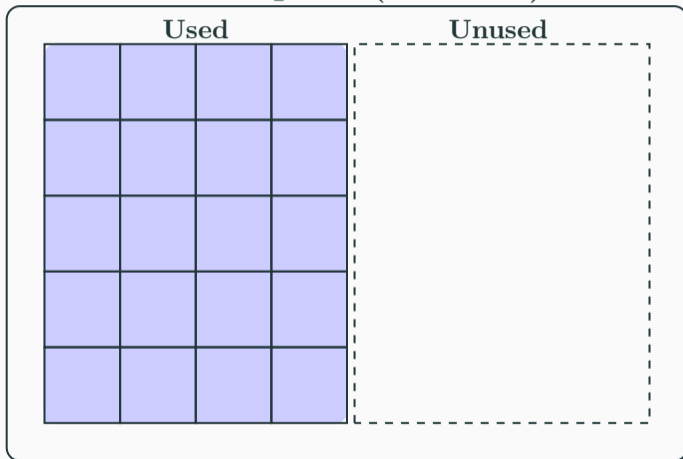
		
Target	National companies	International companies
Type	New domains	Old domains
Ratio Domains	20%	80%

Table 3: Two attack strategies

Why this difference?

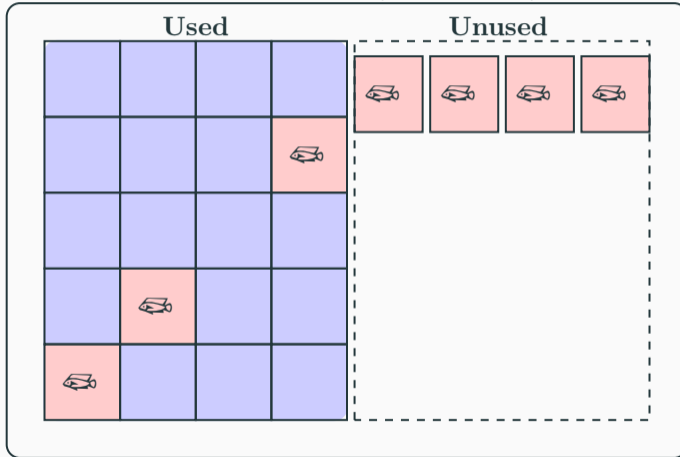
Two attack strategies

Namespace (.nl zone)



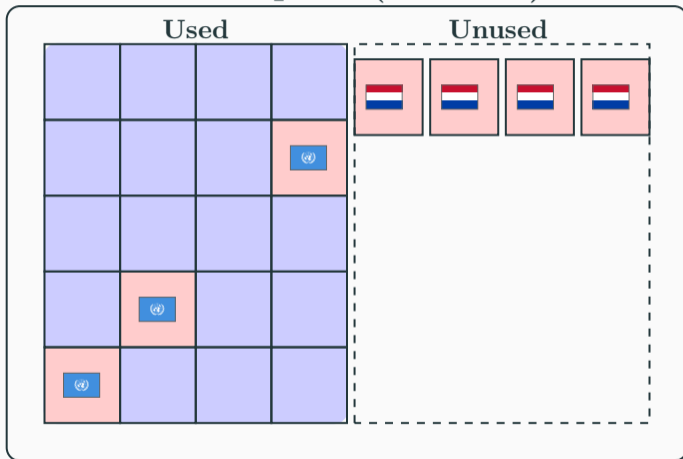
Two attack strategies

Namespace (.nl zone)



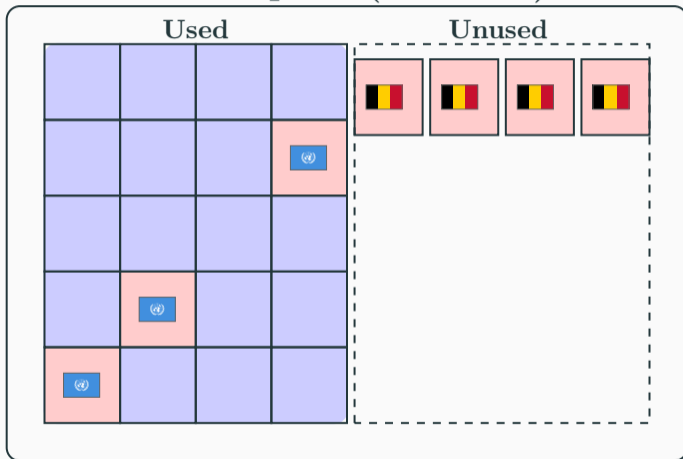
Two attack strategies

Namespace (.nl zone)



Same for .be

Namespace (.be zone)







Two attack strategies

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

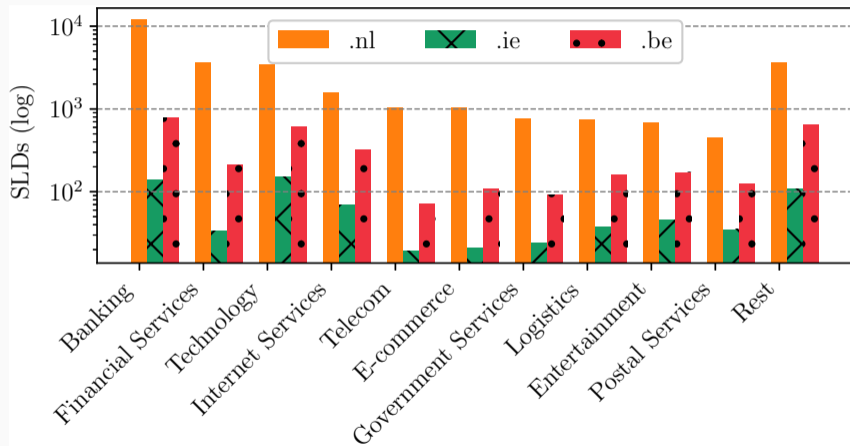
Table 4: Local and International attack strategies

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

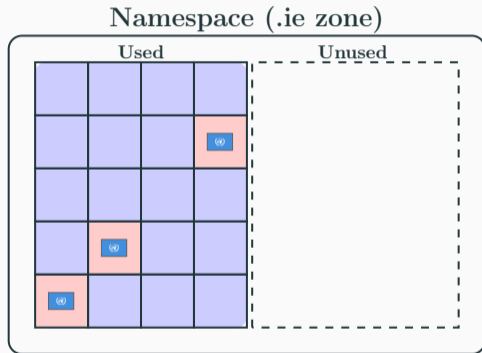


But what about Ireland?



Only two new phishing domains

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



Outline

Introduction

Impersonated companies

Comparing companies among ccTLDs

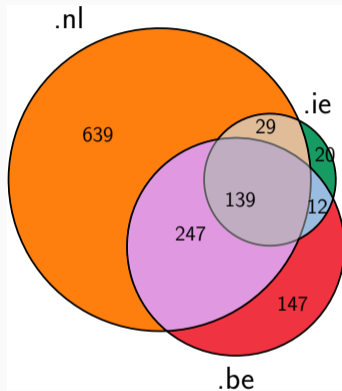
Phishing mitigation

Call for Action

Impersonated companies per ccTLD

139 companies found in the 3 ccTLDs

- Microsoft 🇺🇸
- Apple 🇺🇸
- Google 🇺🇸
- FedEx 🇺🇸
- Banco Santander 🇪🇸
- Maersk 🇩🇰
- Full list in [4]
 - Extended version of the paper

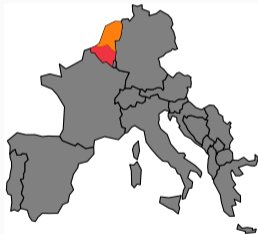


Venn diagram of impersonated companies.

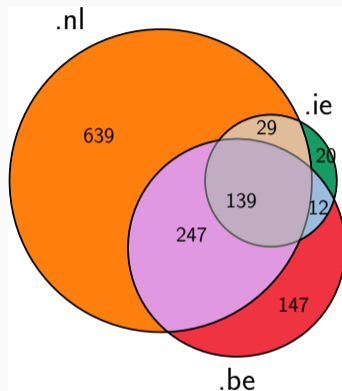
Impersonated companies per ccTLD

247 companies found in .nl and .be

- Many companies operate in both countries
- Cultural, language, and economic ties



- Rest intersections in paper

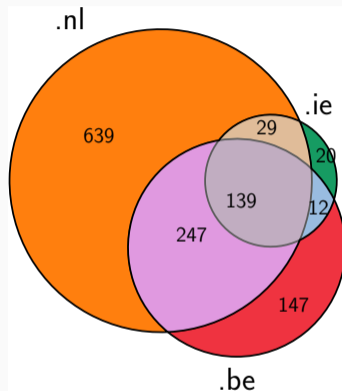


Venn diagram of impersonated companies.

Impersonated companies per ccTLD

Remaining seem to be a function of attack surface

- .nl has larger domain name space (6.1M domains)
- 10 years of data



Venn diagram of impersonated companies.

Outline

Introduction

Impersonated companies

Comparing companies among ccTLDs

Phishing mitigation

Call for Action

Maliciously registered domain example

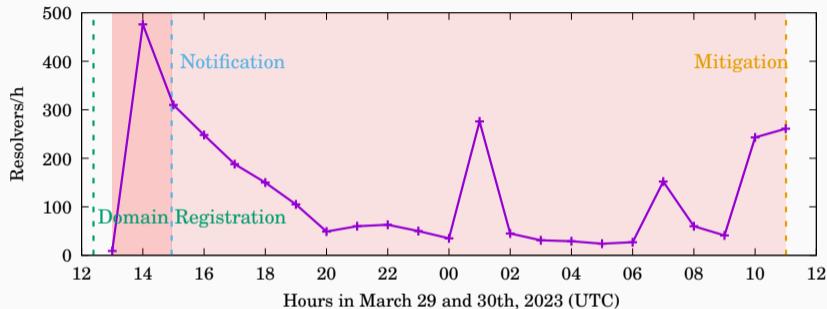


Figure 1: Maliciously registered: 1 day old

- Name especially chosen for the attack
- Mitigation at DNS level

Compromised domain example

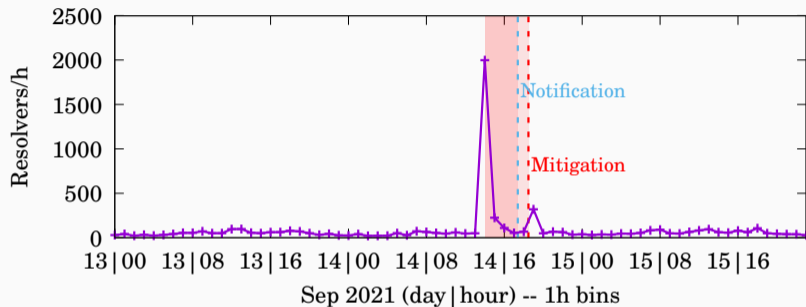
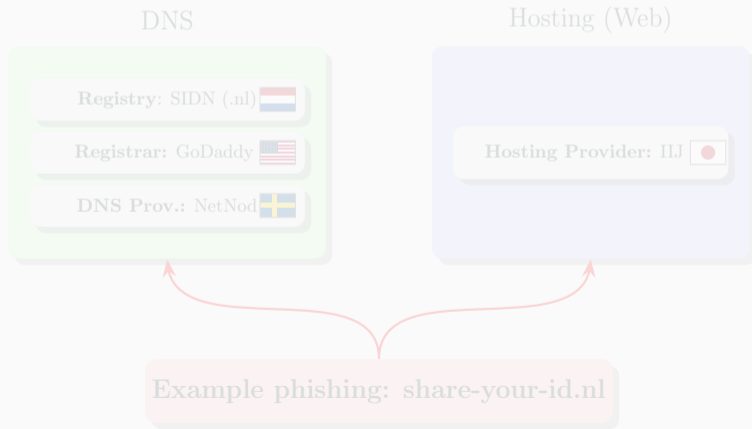


Figure 2: Compromised domain: 21 years old

- Legitimate business which got hacked
- Mitigation only at hosting provider level

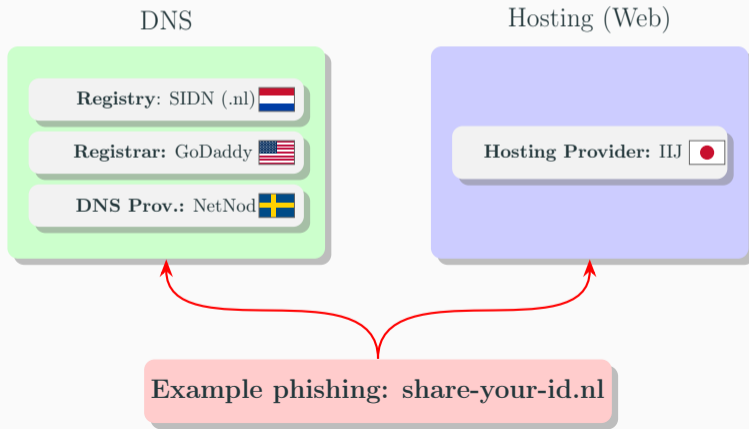
From characterization to mitigation

- 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)



ccTLD mitigation policy

- ccTLDs can perform 3 operations at the DNS level
- Each of them have its own policy (§B in [4])



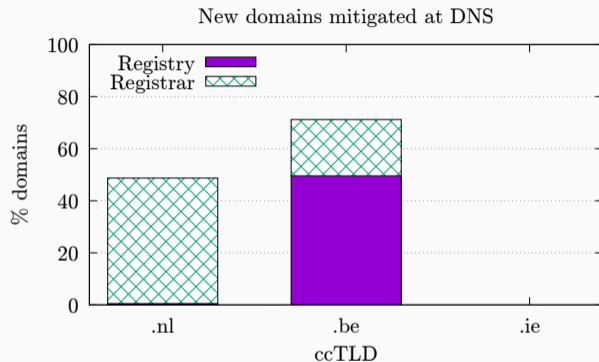
	 .nl	 .ie	 .be
Suspend domain	✓ After 66h	✓ After 30 days	✓ ASAP
Delete domain	✓	✓ After two weeks	✓
Change NS records	—	—	✓

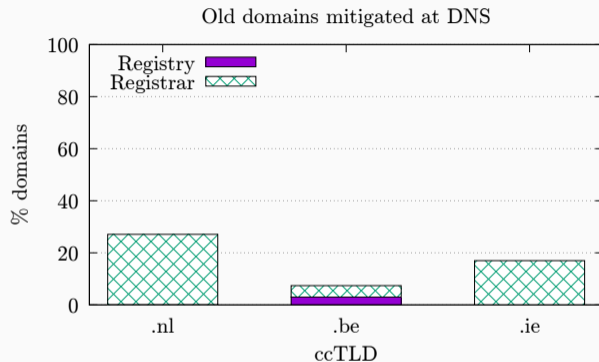
Table 5: ccTLDs phishing detection and mitigation procedure.

DNS mitigation and ccTLD policy: new domains



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

Phishing mitigation at DNS: old domains



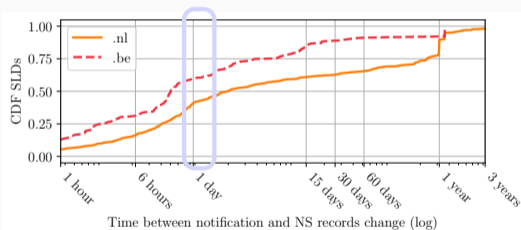
- Most old domains are compromised
 - Web mitigation is preferred
- Exceptions: aged domains

DNS vs Web mitigation speed

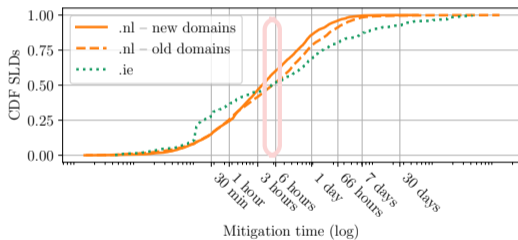
Web mitigation is faster than DNS mitigation

DNS: 50–60% first 24h

Web: 50–60% first 6h



(a) DNS mitigation: Domain suspension



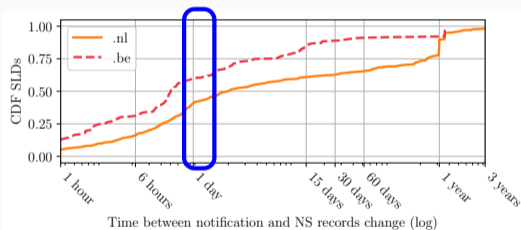
(b) Web mitigation

DNS vs Web mitigation speed

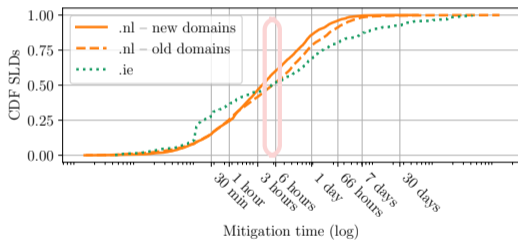
Web mitigation is faster than DNS mitigation

DNS: 50–60% first 24h

Web: 50–60% first 6h



(c) DNS mitigation: Domain suspension



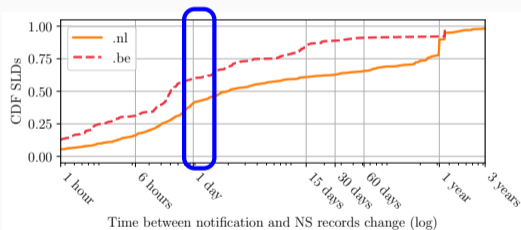
(d) Web mitigation

DNS vs Web mitigation speed

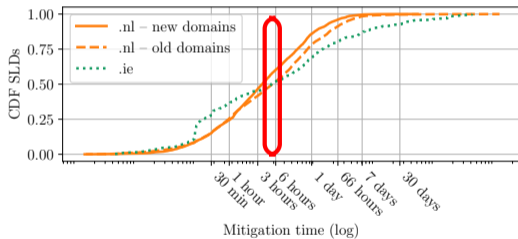
Web mitigation is faster than DNS mitigation

DNS: 50–60% first 24h

Web: 50–60% first 6h



(e) DNS mitigation: Domain suspension



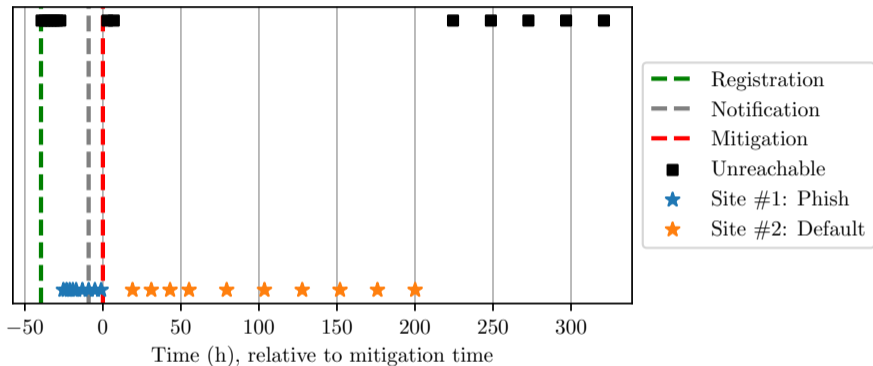
(f) Web mitigation

Phishing against a French bank (.nl domain name)

The screenshot displays a phishing website designed to mimic the Crédit Mutuel client portal. At the top left, the Crédit Mutuel logo is visible. A search bar with the placeholder text 'Rechercher' is located at the top center. On the top right, there are two buttons: 'DEVENIR CLIENT' with a recycling icon and 'ESPACE CLIENT' with a house icon. Below the navigation, the page title reads 'Espace client : Connexion'. The main content area is divided into two columns. The left column contains a login form with fields for 'Identifiant / Mot de passe', 'Certificat Electronique', and 'SAFETRANS'. Below the form is a small image of a hand holding a smartphone displaying a lock icon, followed by a section titled 'Tout savoir sur Internet et la sécurité' with a link to 'Lire la suite'. The right column features a larger login form with 'Identifiant' and 'Mot de passe' fields, a 'Se connecter' button, and links for 'Codes d'accès oubliés' and 'Infos sécurité'. At the bottom of the page, there is a footer with the text 'Le Cr dit Mutuel, coop rative, appartient   ses 8,3 millions de clients-soci taires.' and a detailed paragraph about the bank's legal status and services. The footer also includes a navigation menu with links for 'Mentions l gales', 'Outils et informations r glementaires', 'Site institutionnel', 'Trouver une caisse ou un distributeur', 'Gestion des cookies', and 'Protection des donn es', along with an upward-pointing arrow icon.

Screenshot captured with DMap, in-house scraper

Phishing against a French bank (.nl domain name)



- Web mitigation example
- Hosting provider mitigated it – domain was not deleted

Outline

Introduction

Impersonated companies

Comparing companies among ccTLDs

Phishing mitigation

Call for Action

Phishing attack strategies compared



Target		
Type	New domains	Old domains
Share SLDs	20%	80%
Share Companies	<5%	>95%
Leverage ccTLD Trust	✓	✗
TLD Restricted Reg.	Inhibits ✓	Does not inhibit ✗
Mitigation	DNS, Web	Mostly Web

Table 6: Phishing attack strategies

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



Paper: <https://gsmaragd.github.io/publications/CCS2024/CCS2024.pdf>

- [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.

- [3] European Union Agency for Cybersecurity.
Malware, Phishing, and Ransomware.
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>,
2024.
- [4] Giovane C. M. Moura, Thomas Daniels, Maarten Bosteels, Sebastian Castro, Moritz Müller, Thymen Wabeke, Thijs van den Hout, Maciej Korczyński, and G. Smaragdakis.
Characterizing and Mitigating Phishing Attacks at ccTLD Scale (extended), volume **EWI-TR-2024-1**.

Delft University of Technology, Faculteit Elektrotechniek, Wiskunde en Informatica, 2024.