

# Characterizing and Mitigating Phishing Attacks at ccTLD Scale

---

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

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

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

28<sup>th</sup> October 2024

DNS-OARC Workshop 43, Prague, Czechia



# Outline

Introduction

Impersonated Companies

DNS Measurements

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



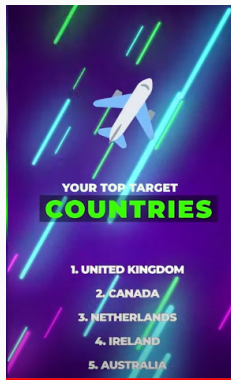
<https://www.bbc.com/news/uk-68838977>

# 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 (4, 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 (4, 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 ID and relationship to the country
- 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

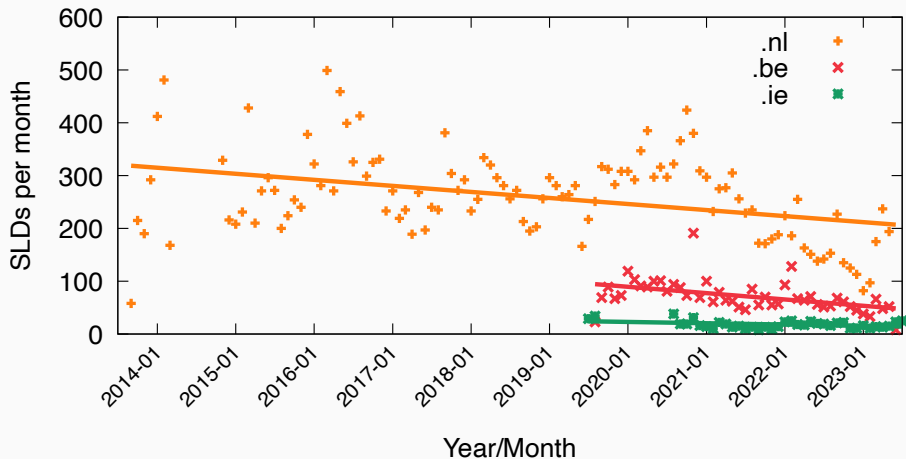
Domains	25,389	555	2,810
Period	~10 years	~4 years	~4 years
Years	2013–2023	2019–2023	2019–2023

**Table 2:** Netcraft phishing blocklist dataset

We triangulate the blocklist dataset with ccTLDs' private datasets:

- Historical registration database
- Web measurements
- DNS measurements

# Phishing domains per month



SLD: Second-level domain (**example.nl**)

# Outline

Introduction

Impersonated Companies

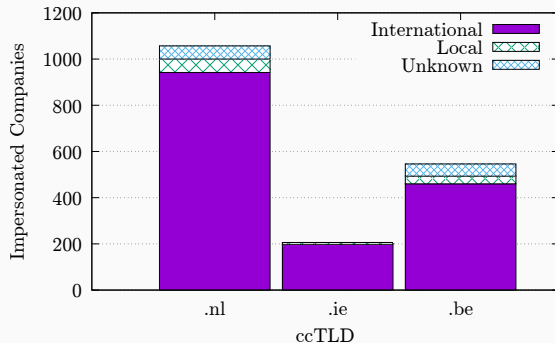
DNS Measurements

Phishing mitigation

Call for Action

# Do they target mostly national companies?

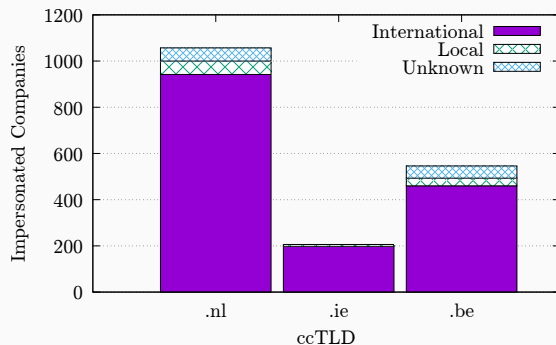
- Citizens have trust in their ccTLDs
  - Govs use it
- Do attackers exploit this trust for phishing?



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

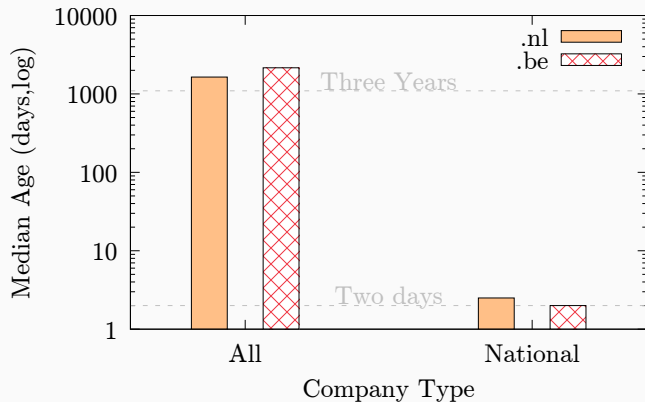
# Do they target mostly national companies?

- 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?

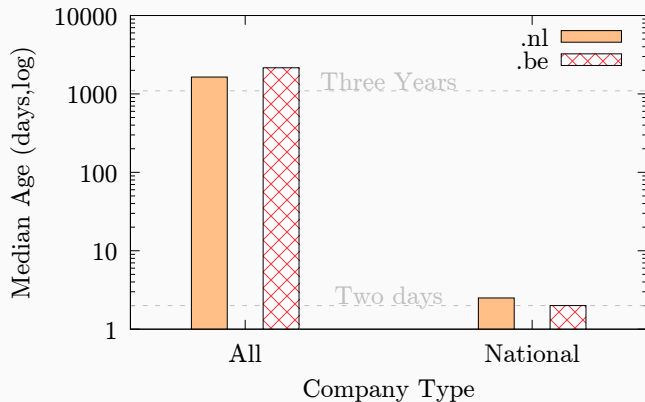
# National companies vs international companies



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

		
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%

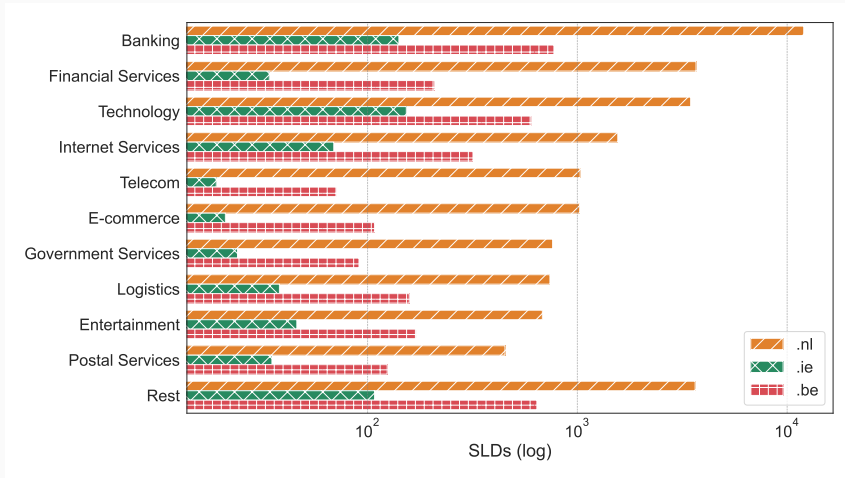
**Table 4:** Local and International attack strategies

# 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
- But they try:
  - Batches of new registrations using forged documents
  - Target low price specials at registrars

# Outline

Introduction

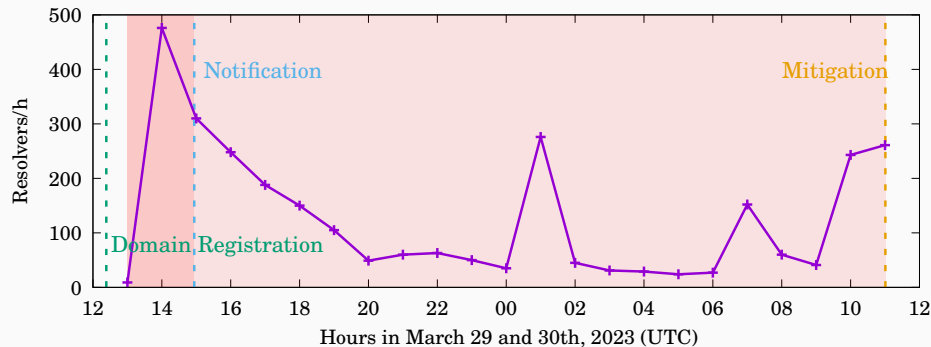
Impersonated Companies

DNS Measurements

Phishing mitigation

Call for Action

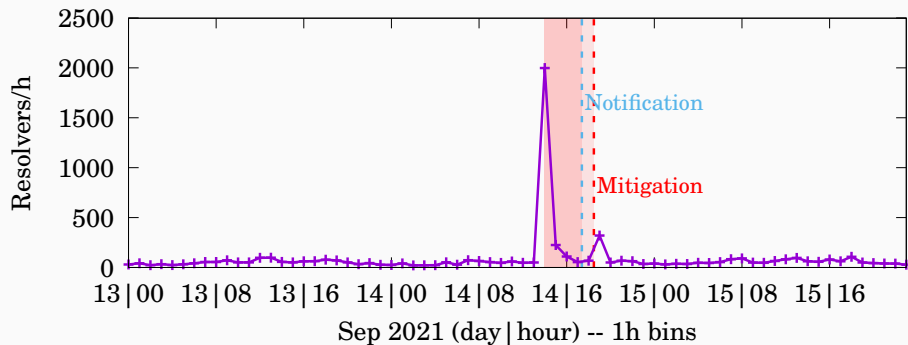
# DNS Activity: Malicious registered domain



**Figure 1:** Maliciously registered: 1 day old

- Name especially chosen for the attack

# DNS Activity: Compromised domain example



**Figure 2:** Compromised domain: 21 years old

- Legitimate business which got hacked



# Outline

Introduction

Impersonated Companies

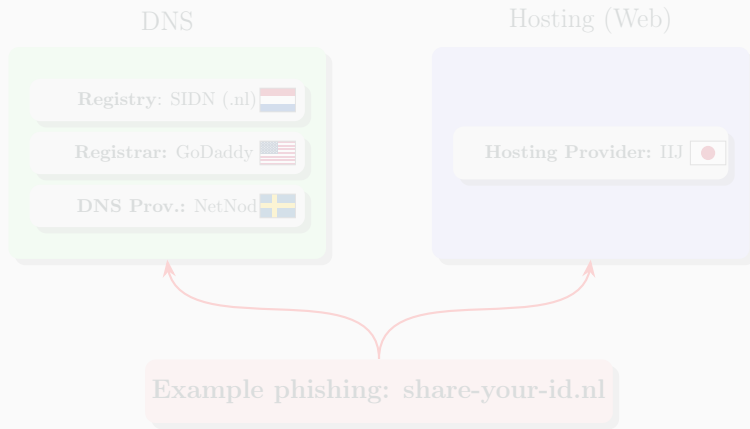
DNS Measurements

Phishing mitigation

Call for Action

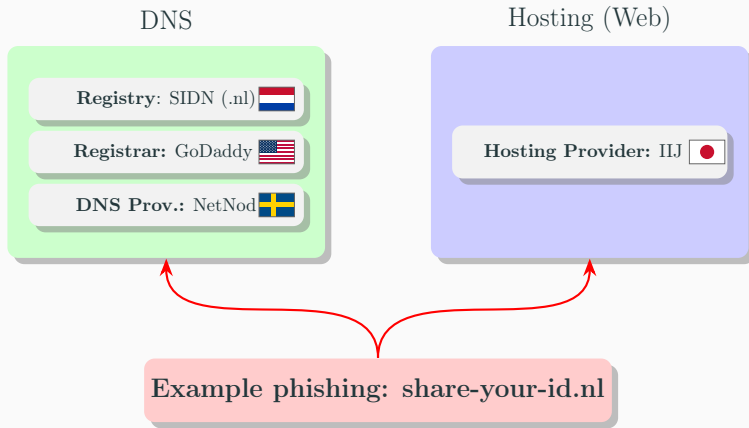
# From characterization to mitigation

- 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
- Upon notification:
  - .nl alerts the registrar
  - .be suspends the domain
  - .ie allows Netcraft to alert the registrar directly

	 .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.

# Phishing against a French bank (.nl domain name)

Crédit Mutuel

Rechercher

DEVENIR CLIENT

ESPACE CLIENT

Espace client : Connexion

Identifiant / Mot de passe

Certificat Electronique

SAFETRANS

Tout savoir sur internet et la sécurité

Utilisez tous nos conseils pour un comportement adapté et sécurisé lors de toutes vos transactions sur internet.

[Lire la suite](#)

Identifiant

Mot de passe

Se connecter

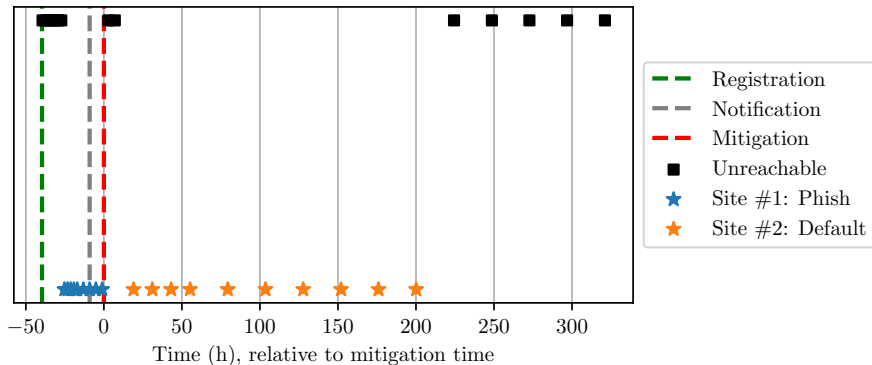
[Codes d'accès oubliés](#) [Infos sécurité](#)

Le Crédit Mutuel, coopérative, appartient à ses 8,3 millions de clients-sociétaires.

Caisse Fédérale de Crédit Mutuel et caisses affiliées, société coopérative à forme de société anonyme au capital de 5 458 531 000 €, 4 rue Frédéric-Guillaume Raiffeisen, 67000 Strasbourg, RCS Strasbourg B 556 505 354, régie par les articles L 571-1 et suivants du code monétaire et financier. Pour les opérations effectuées en qualité d'intermédiaires en opérations d'assurances inscrits au registre national sous le numéro unique d'identification 07 003 758 (immatriculations consultables sous [www.ortas.fr](#)), contrats d'assurances de ACM VIE SA et ACM SASD SA, entreprises régies par le code des assurances et MTRL, Mutuelle Nationale relevant du Livre I du code de la mutualité.

Mentions légales · Guides et informations réglementaires · Site institutionnel · Trouver une caisse ou un distributeur · Gestion des cookies · Protection des données · ↑

# Phishing against a French bank (.nl domain name)



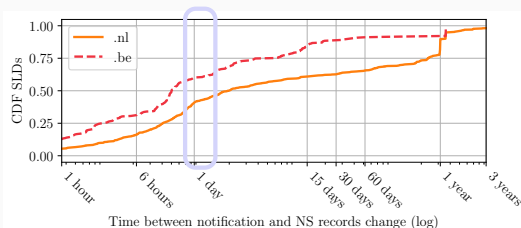
- Web mitigation example
- Hosting provider mitigated it – domain was not deleted

# DNS vs Web mitigation speed

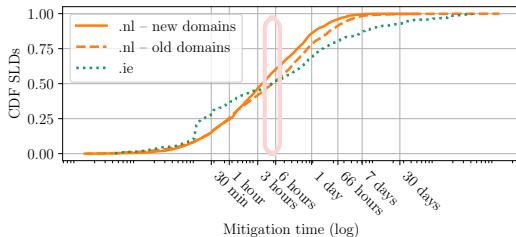
Web mitigation is faster than DNS mitigation

DNS: 50–60% first 24h

Web: 50–60% first 6h



(a) DNS mitigation: Domain suspension



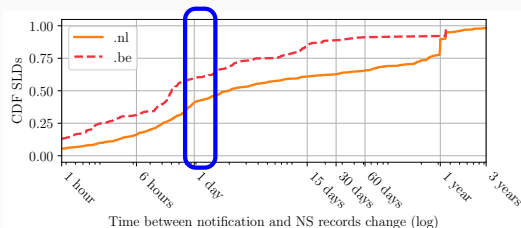
(b) Web mitigation

# DNS vs Web mitigation speed

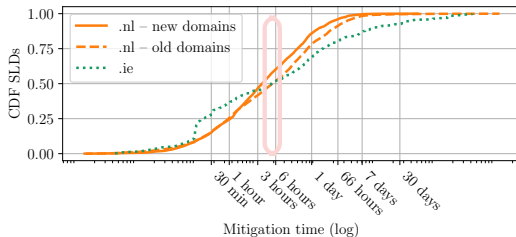
Web mitigation is faster than DNS mitigation

DNS: 50–60% first 24h

Web: 50–60% first 6h



(c) DNS mitigation: Domain suspension



(d) Web mitigation

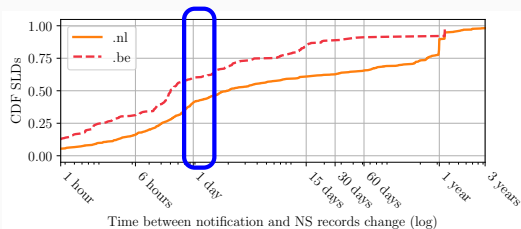


# DNS vs Web mitigation speed

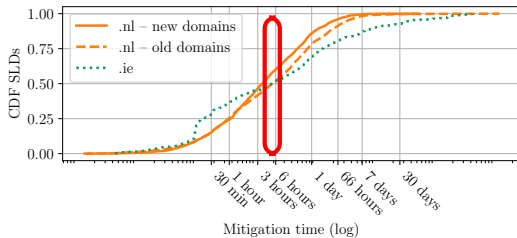
Web mitigation is faster than DNS mitigation

**DNS: 50–60% first 24h**

**Web: 50–60% first 6h**

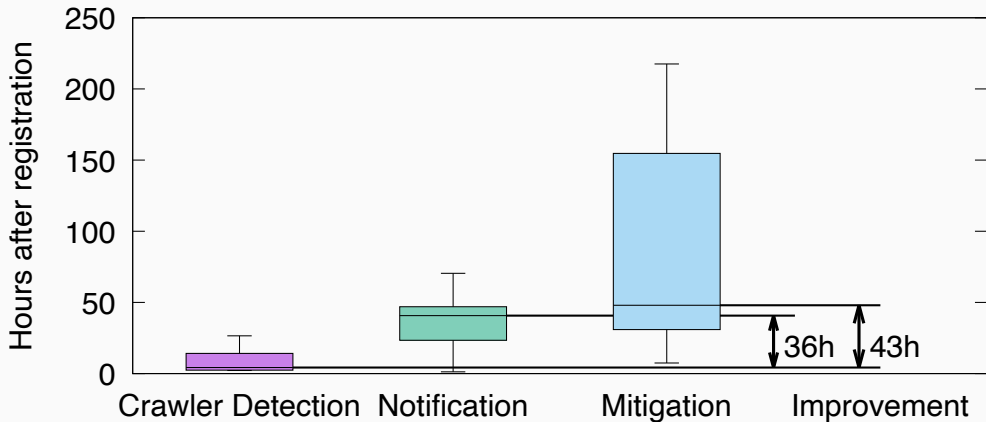


(e) DNS mitigation: Domain suspension



(f) Web mitigation

# Web mitigation: reducing detection time is possible



**Figure 3:** Phishing detection, notification, and mitigation

# Outline

Introduction



Impersonated Companies

DNS Measurements

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
3. Join the study if you can



# 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](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:](https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023)

[//www.enisa.europa.eu/publications/enisa-threat-landscape-2023](https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023),  
2024.