

Security in practice: Vulnerability Disclosure and Phishing

Giovane C. M.Moura

SIDN Labs and TU Delft

Bachelor CSE – CSE3220 – Guest Lecture

Delft, The Netherlands

2025-02-26



What you will learn today:

Coordinated Vulnerability Disclosure

1. Explain its importance
2. Simulate a disclosure
3. Explain different vendor's behavior in practice
4. Be able to make informed choices when doing a CVD

Reference: CCR2023 [2]

Phishing attacks at scale

1. Explain phishing and economics
2. Evaluate the attacker mindset
3. Explain attacker's choices
4. Explain what type of mitigations exist

Reference: CCS2024 [1]

What you will learn today:

Coordinated Vulnerability Disclosure

1. Explain its importance
2. Simulate a disclosure
3. Explain different vendor's behavior in practice
4. Be able to make informed choices when doing a CVD

Reference: CCR2023 [2]

Phishing attacks at scale

1. Explain phishing and economics
2. Evaluate the attacker mindset
3. Explain attacker's choices
4. Explain what type of mitigations exist

Reference: CCS2024 [1]

Outline

Background

Vulnerability Disclosure

Phishing Attacks at Scale

Impersonated companies

Comparing companies among ccTLDs

Phishing mitigation

Call for Action

- Data Scientist at [SIDN Labs](#)
 - research team of SIDN, .nl registry
- Assistant Professor at [TU Delft](#)
 - PhD University of Twente (2013)
 - Msc Computer Science UFRGS, Brazil (2008)

(Slides will be online, content in [red](#) is a clickable link)



SIDN and SIDN Labs

- SIDN is the .nl registry and operator
- private company with a public mission
- Part of the Netherlands digital critical infrastructure (under **RDI .nl** oversight)
- €23M in revenue, 6% (€1.5M)for research (SIDN Labs)
- 107 employees, 15 in Labs
- Labs mission: open research for the public good, for a more secure and robust Internet in the Netherlands and elsewhere
- We do **paid internships**: <https://sidnlabs.nl/en/graduating>

Outline

Background

Vulnerability Disclosure

Phishing Attacks at Scale

Impersonated companies

Comparing companies among ccTLDs

Phishing mitigation

Call for Action

Vulnerability Disclosure

First, a quiz:

1. What is a software vulnerability?
2. It is important? Why?
3. Difference between a software **bug** and **vulnerability**?
4. Has anyone here found a software bug? And a vulnerability?
5. Who's fault is the software vulnerability?
6. Can we fully prevent software vulnerabilities?

Vulnerability Disclosure

First, a quiz:

1. What is a software vulnerability?
2. It is important? Why?
3. Difference between a software **bug** and **vulnerability**?
4. Has anyone here found a software bug? And a vulnerability?
5. Who's fault is the software vulnerability?
6. Can we fully prevent software vulnerabilities?

Vulnerability Disclosure

First, a quiz:

1. What is a software vulnerability?
2. It is important? Why?
3. Difference between a software **bug** and **vulnerability**?
4. Has anyone here found a software bug? And a vulnerability?
5. Who's fault is the software vulnerability?
6. Can we fully prevent software vulnerabilities?

Vulnerability Disclosure

First, a quiz:

1. What is a software vulnerability?
2. It is important? Why?
3. Difference between a software **bug** and **vulnerability**?
4. Has anyone here found a software bug? And a vulnerability?
5. Who's fault is the software vulnerability?
6. Can we fully prevent software vulnerabilities?

Vulnerability Disclosure

First, a quiz:

1. What is a software vulnerability?
2. It is important? Why?
3. Difference between a software **bug** and **vulnerability**?
4. Has anyone here found a software bug? And a vulnerability?
5. Who's fault is the software vulnerability?
6. Can we fully prevent software vulnerabilities?

Vulnerability Disclosure

First, a quiz:

1. What is a software vulnerability?
2. It is important? Why?
3. Difference between a software **bug** and **vulnerability**?
4. Has anyone here found a software bug? And a vulnerability?
5. Who's fault is the software vulnerability?
6. Can we fully prevent software vulnerabilities?

What would YOU do if you'd find a vulnerability?



You have three options

1. Keep it private

- It does not get fixed

2. Sell it (See HackerOne)

- US \$ 1M USD for 0-day IOS bugs
- This one will not fix the issue
- Can empower attackers elsewhere
- Ethically dubious

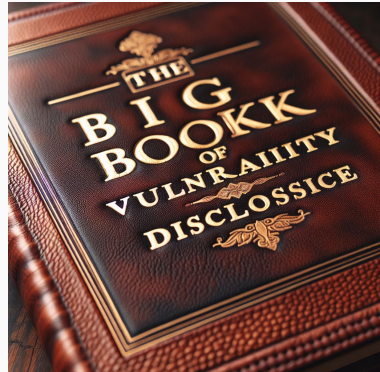
3. Disclose it

- the most ethical choice
- the one that most likely get it fixed, benefiting the public



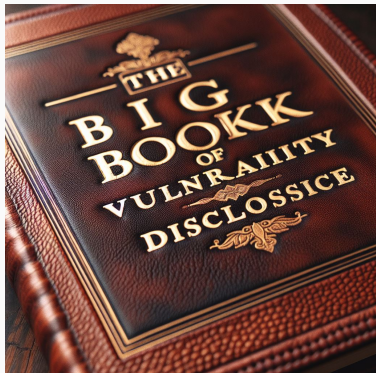
Say you decided to do disclose it

- How to do it?
- That is where the problems start:
 - There is no consensus in the community
 - There is consensus even in the terminology



Say you decided to do disclose it

- How to do it?
- That is where the problems start:
 - There is no consensus in the community
 - There is consensus even in the terminology



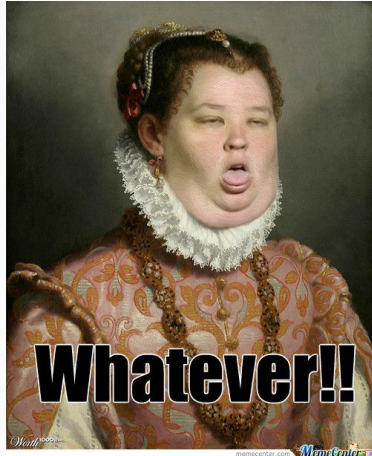
There is not even terminology consensus

What's the different between:

1. Private Disclosure
2. Public Disclosure
3. Full Disclosure
4. Responsible Disclosure
5. Coordinated Vulnerability Disclosure

Private Disclosure

- You tell only the vendor
- They decide to do whatever they want
- Commonly used in the past
- Outcomes:
 - Being ignored
 - Legal threats [3]



Full Disclosure

- The opposite of private disclosure:
 - You tell everyone, everything
- Only way to bring public scrutiny to vulnerabilities[3]
- It removes the veil of secrecy



In between both: “Responsible” or Coordinated Disclosure

- This is simply Full disclosure with an embargo:
- You give a vendor some time to fix it
 - US Cert suggests: 45 days
 - Google Project Zero: 90 days
- After it, you are “free” do disclose it
 - But WOULD you?
 - Imagine you vs one of the Big Tech companies?



Evolving terminology: use Coordinated, phase out Responsible

- “Responsible” disclosure implies a moral duty on whoever found the bug
- The responsible is the vendor! They created the bug
- Coordinated Vulnerability Disclosure (CVD) is the preferred term
- It removes the onus on the researcher and has not moralistic label

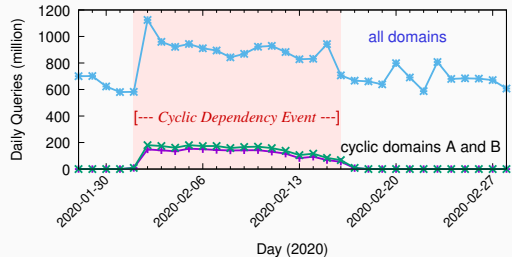


The screenshot shows the top of a webpage from the Nationaal Cyber Security Centrum (NCSC). The header includes the NCSC logo and the text "Nationaal Cyber Security Centrum" and "Ministerie van Justitie en Veiligheid". Below the header is a green navigation bar with the text "Kwetsbaarheid melden (CVD) >". The main content area features the heading "CVD-meldingen formulier" followed by a paragraph explaining that technical vulnerabilities found in government systems can be reported to the NCSC, and that such reports are called Coordinated Vulnerability Disclosure (CVD). A link to "CVD-beleid" is provided for more information.

CVD is used by the NCSC-NL

So we found one vulnerability

- It affected Google Public DNS
- It caused 50% traffic increase on New Zealand's .nz DNS server
- Important:
 - Third-parties were the victims, not GDNS
- What to do?
 - There were not many papers telling 1st hand experience
 - Uncharted territory



Vulnerability Disclosure

- “In practice, the theory is different”



(my Electricity and Magnetism
professor at college)

TsuNAME Vulnerability

- Clients or resolvers would loop
- It could overwhelm authoritative DNS servers
- Google has far more capacity than most operators
- An attacker could aim GDNS at DNS servers

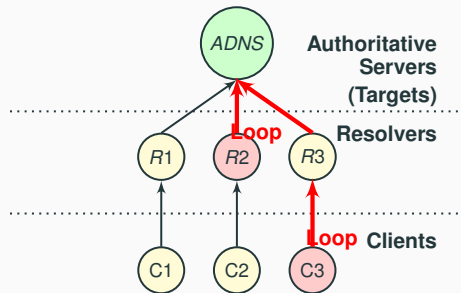
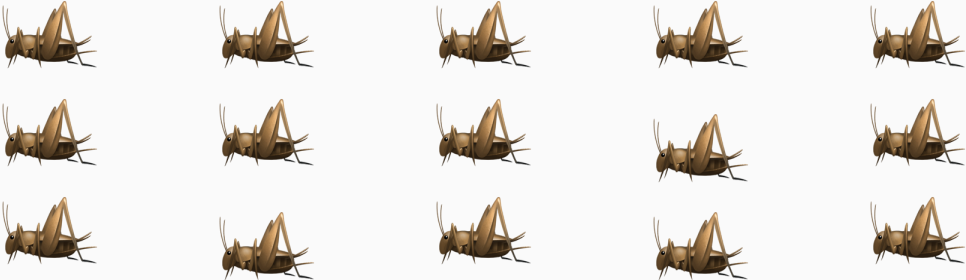


Figure 1: TsuNAME attack.

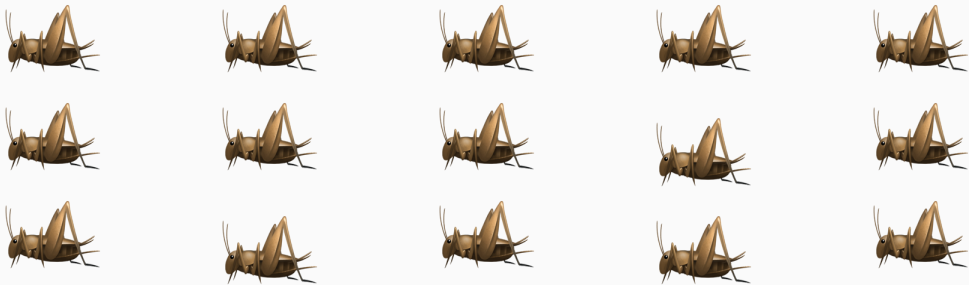
So what did we do?

- We knew some folks at GDNS
- So we notified them personally
- (Private disclosure)

So what happened?



So what happened?



But why?

Security = People

We made lots of mistakes

- So we wrote a paper about it [2]
- 1st hand experience
- And lessons learned



TsuNAME disclosure timeline

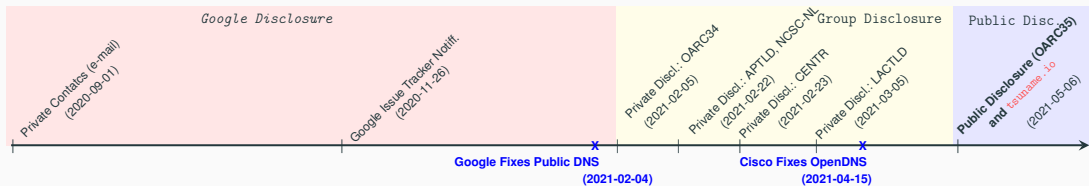


Figure 2: TsuNAME disclosure timeline

Lesson 1: Full disclosure improves security for everyone

- .nz has 50% traffic increase on TsuNAME
- We wonder why there had been no public reports on it
 - given it had a big damage potential
- We decide to disclose it
- It was ultimately fixed
- Improved security for everyone



Lesson 2: Disclosure has ethical implications

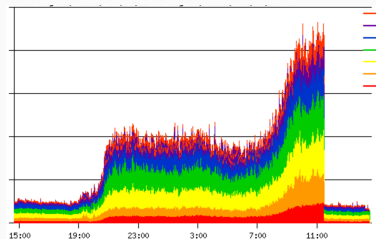
- Don't disclose and others can become victims
- Our initial private disclosure only to Google did not work
 - it was our mistake
- We first notified all vendors in the group disclosure phase
 - they all release reports on the vulnerability

Lesson 3: ask help to reduce burden

- We disclosed it in many venues, in 4 languages
- It took lots of time and energy
- US-CERT has a vulnerability disclosure coordinator to help
 - so you don't have to do it yourself
 - they take away all emotional/legal burden

Lesson 4: You don't have the complete picture

- During our Q&A at OARC34 group disclosure, two ccTLD operators told us they had been victims of it before
- .nz had 50% traffic increase, an european ccTLD had 1000%.
- The other said it had tried private disclosure many times
 - we could not verify it
 - but is an example of why private disclosure does not work



Lesson 5: Prepare for stressful reactions

You can't make everyone happy

- Positive reactions: Google, BIND, Cisco OpenDNS, Unbound
- Negative: one operator said it was fear-mongering, other said it was a known problem
 - it was partially known, but not at this scale
 - there's a IETF draft now that covers it
- The primary goal is not to please everyone but to fix the problem

Improving the disclosure process

1. Clarify vendor roles and timeframes:

- Most guidelines don't cover roles
- Vendors can sit on a disclosure
- Their bug system is also vague timeline wise:
 - TsuNAME on Google: "P2 issues need to be addressed on a reasonable timescale"

2. Update and endorse CVD guidelines

- We need guidelines that protect individuals who disclosure
- With clear timeframes
- And concise

How to do do disclosure then (step-by-step):

1. Report directly to the vendor
 - some even pay you, big bounty programs
2. Wait for vendor initial assessment
3. If vendor is unresponsive or refuse to fix it, give them a ultimatum
 - 45 days for public disclosure
 - if vendor ask extra time, grant it, if it's hard to fix it
4. Public disclose it after agreed date
 - Beware of stress that may come with it
 - or ask help if you don't wanna deal with this

Disclosure simulation: role play

- Play in pairs: vendor and researcher
- Researcher:
 - Goal: get vendor to fix the vulnerability
- Vendor:
 - Goal: be reluctant, given it will cost time and money
- One minute discussing it
- Discussion after it

Recap: What you will learn today:

Coordinated Vulnerability Disclosure

1. Explain its importance
2. Simulate a disclosure
3. Explain different vendor's behavior in practice
4. Be able to make informed choices when doing a CVD

Reference: CCR2023 [2]

Outline

Background

Vulnerability Disclosure

Phishing Attacks at Scale

Impersonated companies

Comparing companies among ccTLDs

Phishing mitigation

Call for Action

Phishing quiz

1. What is phishing attack?
2. How serious is it?
3. What types of phishing attacks exist?
4. Has anyone here been victim of a phishing attack?



Phishing quiz

1. What is phishing attack?
2. How serious is it?
3. What types of phishing attacks exist?
4. Has anyone here been victim of a phishing attack?



Phishing quiz

1. What is phishing attack?
2. How serious is it?
3. What types of phishing attacks exist?
4. Has anyone here been victim of a phishing attack?



Phishing quiz

1. What is phishing attack?
2. How serious is it?
3. What types of phishing attacks exist?
4. Has anyone here been victim of a phishing attack?



Phishing quiz

1. What is phishing attack?
2. How serious is it?
3. What types of phishing attacks exist?
4. Has anyone here been victim of a phishing attack?



Phishing is a major threat on the Internet

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



BBC

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



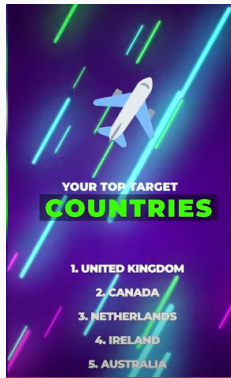
<https://www.bbc.com/news/uk-68838977>

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](#)

NOS Nieuws • Donderdag 18 april, 08:00



Internationaal phishing-netwerk opgerold, vijf arrestaties in Nederland

De politie heeft in verschillende landen een groot phishing-netwerk opgerold dat nep-websites van bijvoorbeeld banken en overheidsinstanties verkocht aan andere criminelen, die er op hun beurt mensen mee probeerden op te lichten. Zo zijn 500.000 creditcardgegevens buitgemaakt en 1,2 miljoen wachtwoorden gestolen.

Ook invallen in Nederland

In totaal waren er achttien landen betrokken bij het onderzoek. In Nederland werkte onder meer het team Digitale Criminaliteit Midden-Nederland eraan mee. Er zijn zes Nederlandse woningen doorzocht en daarbij werden onder andere 57 gegevensdragers, ruim honderd simkaarten en vijf vuurwapens in beslag genomen.

De vijf Nederlandse arrestanten komen uit Leeuwarden, Papendrecht, Woudenberg en Vleuten en zijn tussen de 21 en 36 jaar oud. Naast die aanhoudingen heeft de politie ook twee 'stopgesprekken' gevoerd met gebruikers van de site. De politie sluit meer acties niet uit.

Phishing cooking recipe (do not do it)

Ingredients:

- 1 domain name
 - You could register one
 - Or you could hack one
 - Question: what's the pros and cons of each?
- 1 look-alike website
 - You could dev one
 - You could buy a phishing kit
- If you reg a new domain, you'll need a hosting provider
- Dissemination: spam? social networking?

Phishing cooking recipe (do not do it)

Ingredients:

- 1 domain name
 - You could register one
 - Or you could hack one
 - Question: what's the pros and cons of each?
- 1 look-alike website
 - You could dev one
 - You could buy a phishing kit
- If you reg a new domain, you'll need a hosting provider
- Dissemination: spam? social networking?

Can you name some phishing defense methods?

Phishing blocklist

- Vendors sell real-time phishing blocklists
- Different detection methods, their “secret sauce”
- We (SIDN) buy from one of them, and use it for mitigation
- But no one had look into it as a researcher
- So that’s what we did



Phishing blocklist

- Vendors sell real-time phishing blocklists
- Different detection methods, their “secret sauce”
- We (SIDN) buy from one of them, and use it for mitigation
- But no one had look into it as a researcher
- So that’s what we did



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
Comp.	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
Comp.	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

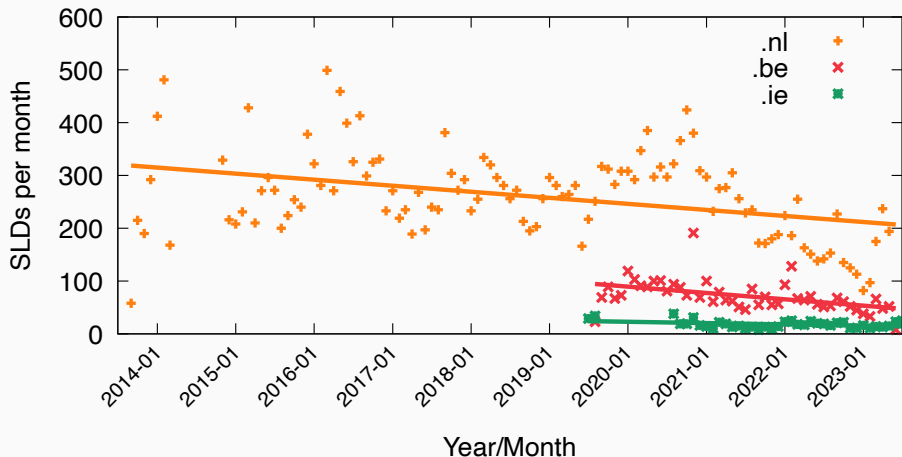
Domains	25,389	555	2,810
Period	~10 years	~4 years	~4 years
Years	2013–2023	2019–2023	2019–2023

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

Background

Vulnerability Disclosure

Phishing Attacks at Scale

Impersonated companies

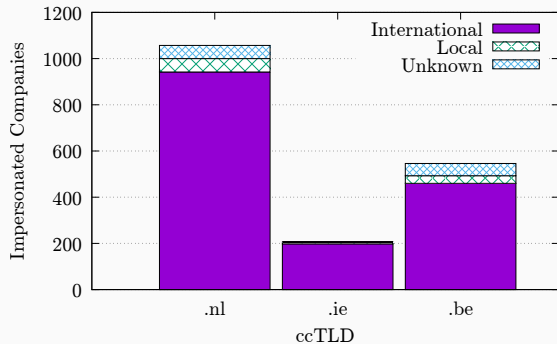
Comparing companies among ccTLDs

Phishing mitigation

Call for Action

Do they target mostly national companies?

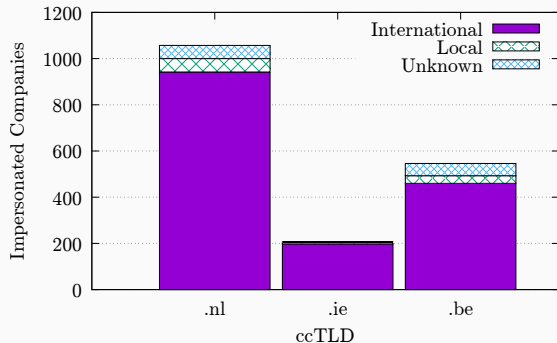
- Citizens have trust in their ccTLDs
 - Govs use it
- Do attackers exploit this trust for phishing?



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

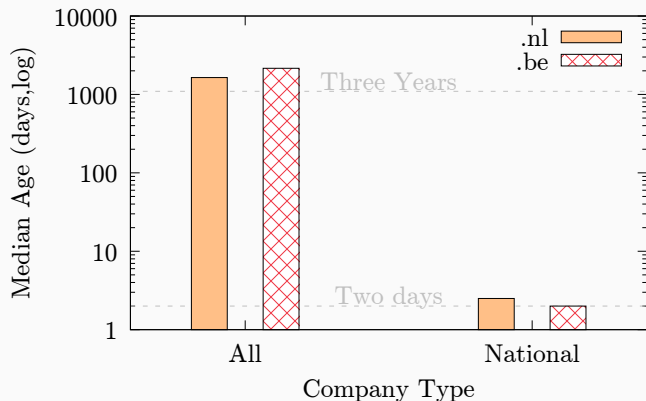
Do they target mostly national companies?

- 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?**

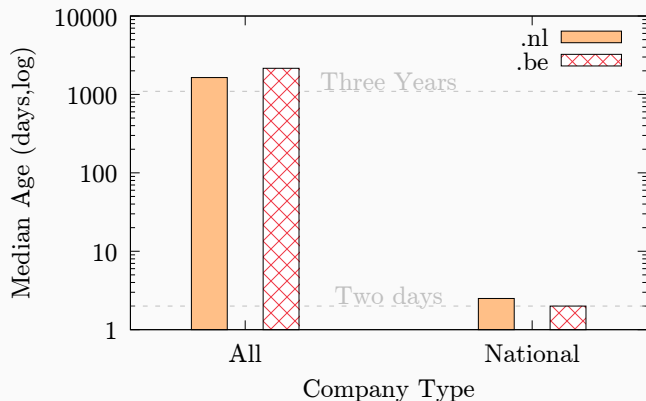
National companies vs international companies



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

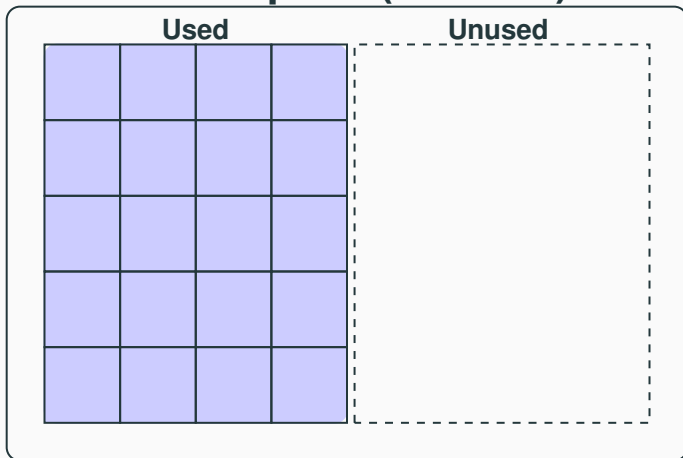
		
Target	National companies	International companies
Type	New domains	Old domains
Ratio Domains	20%	80%

Table 3: Two attack strategies

Why this difference?

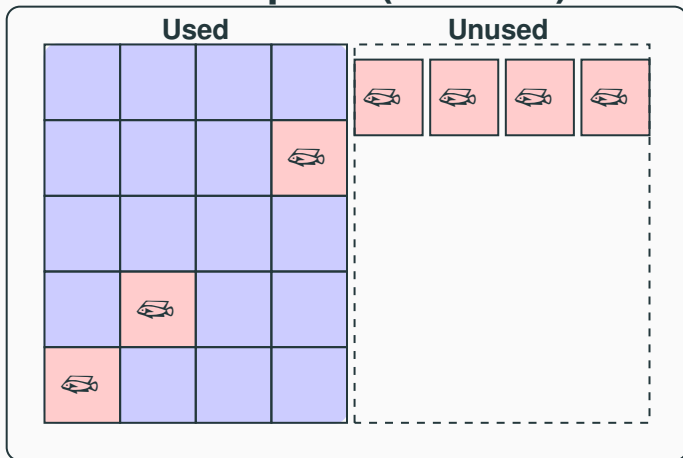
Two attack strategies

Namespace (.nl zone)



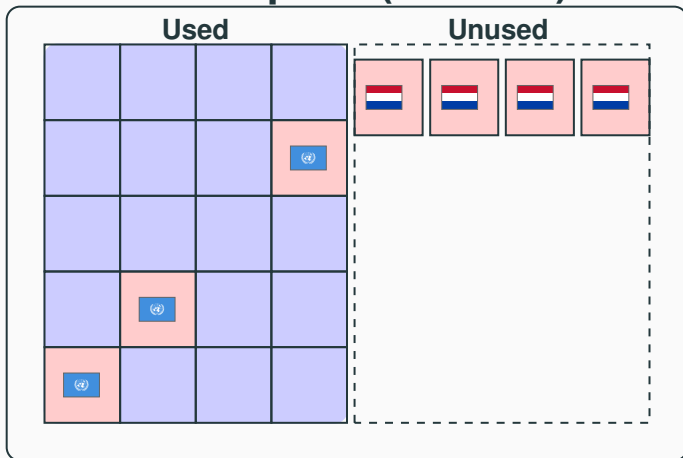
Two attack strategies

Namespace (.nl zone)

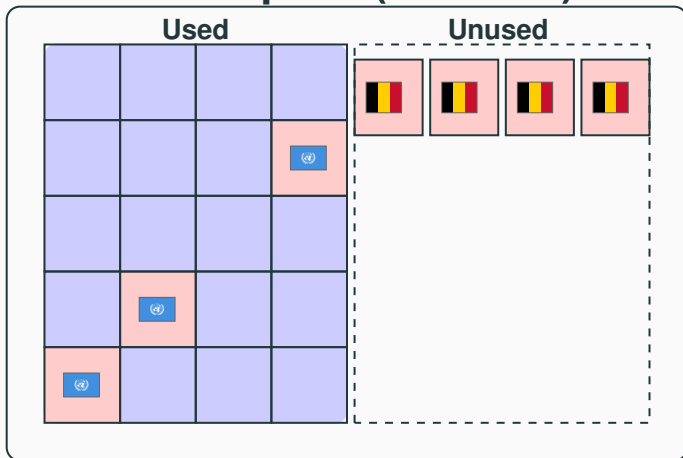


Two attack strategies

Namespace (.nl zone)



Namespace (.be zone)



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%

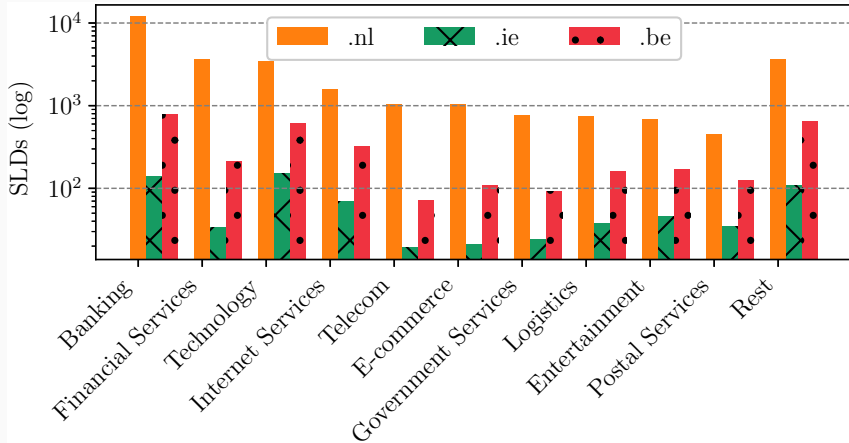
Table 4: Local and International attack strategies

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 ()

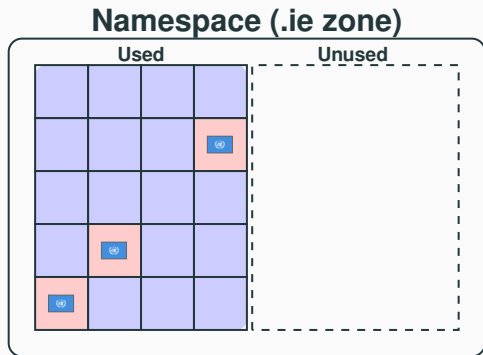
Most popular market segments



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



Outline

Background

Vulnerability Disclosure

Phishing Attacks at Scale

Impersonated companies

Comparing companies among ccTLDs

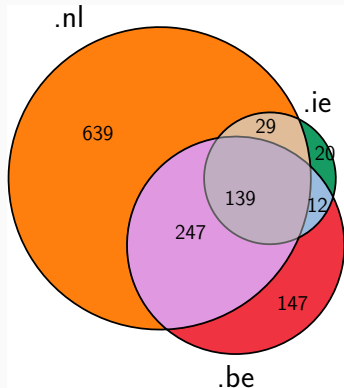
Phishing mitigation

Call for Action

Impersonated companies per ccTLD

139 companies found in the 3 ccTLDs

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

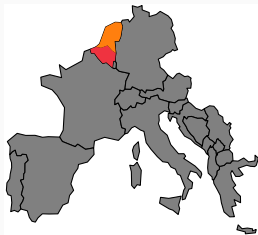


Venn diagram of impersonated companies.

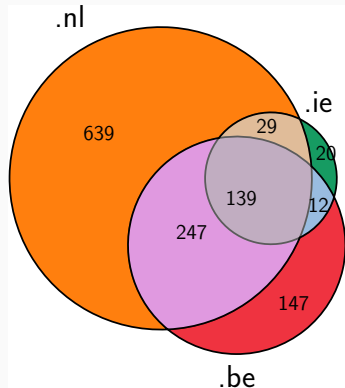
Impersonated companies per ccTLD

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.

Outline

Background

Vulnerability Disclosure

Phishing Attacks at Scale

Impersonated companies

Comparing companies among ccTLDs

Phishing mitigation

Call for Action

Maliciously registered domain example

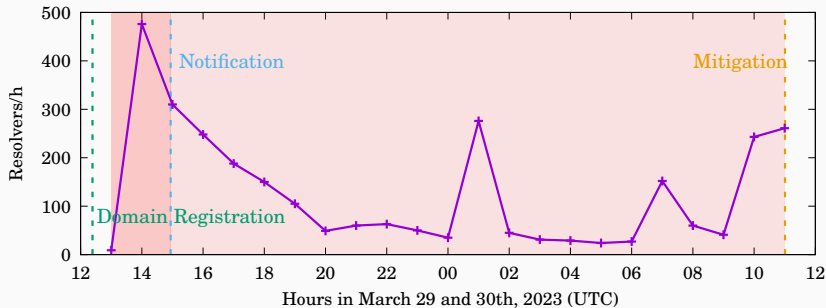


Figure 3: Maliciously registered: 1 day old

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

Compromised domain example

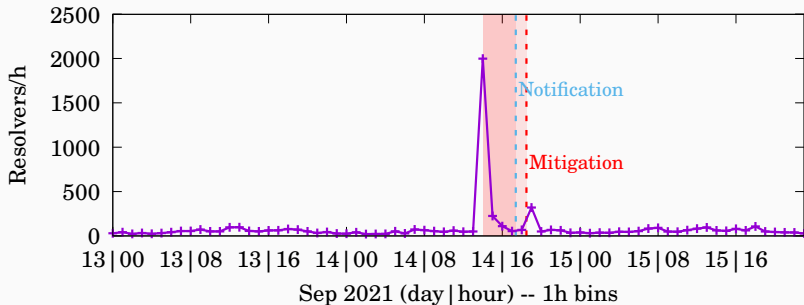
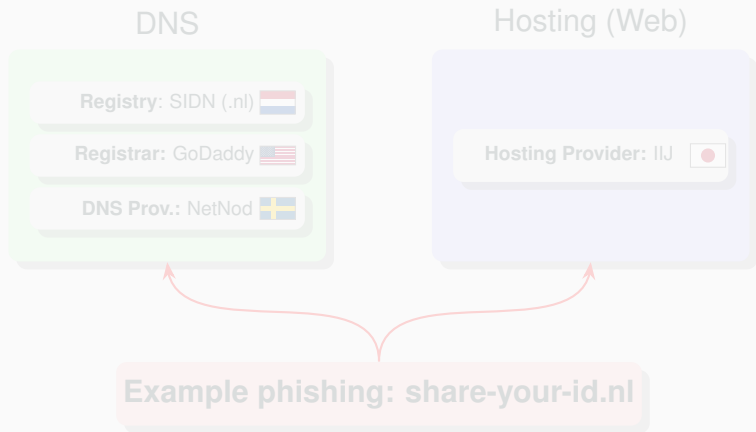


Figure 4: Compromised domain: 21 years old

- 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 [?])



.nl



.ie

Suspend domain

✓ After 66h

✓ After 30 days

✓

Delete domain

✓

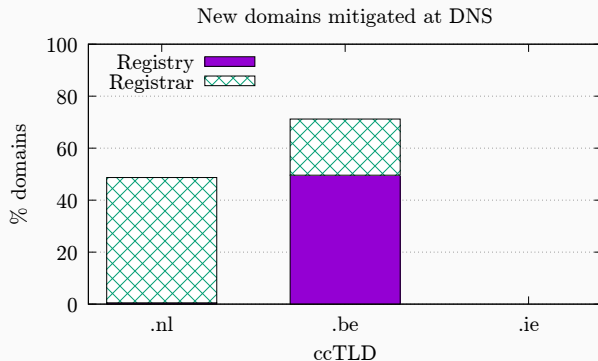
✓ After two weeks

Change NS records

—

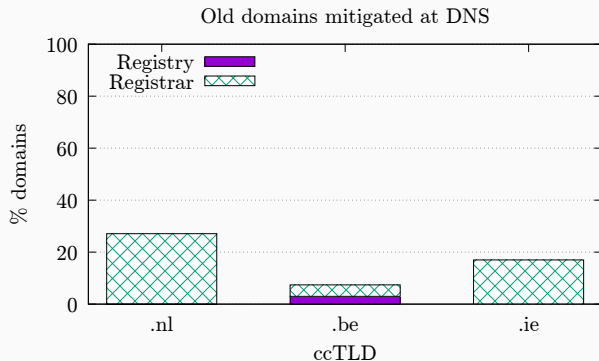
—

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



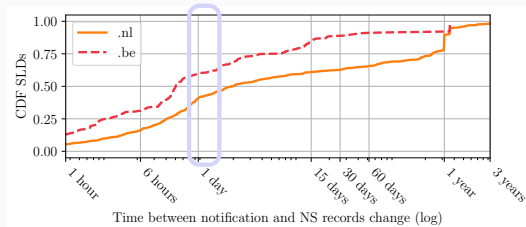
- Most old domains are compromised
 - Web mitigation is preferred
- Exceptions: aged domains

DNS vs Web mitigation speed

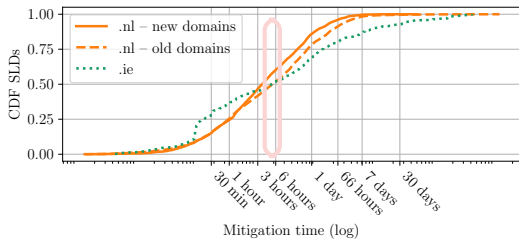
Web mitigation is faster than DNS mitigation

DNS: 50–60% first
24h

Web: 50–60% first 6h



(a) DNS mitigation: Domain suspension



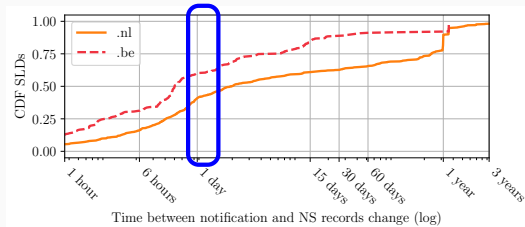
(b) Web mitigation

DNS vs Web mitigation speed

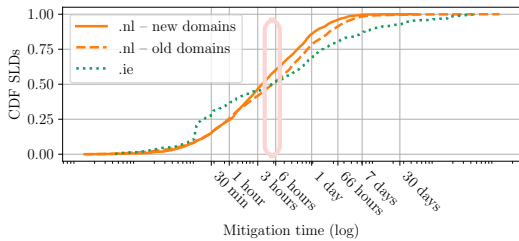
Web mitigation is faster than DNS mitigation

**DNS: 50–60% first
24h**

Web: 50–60% first 6h



(c) DNS mitigation: Domain suspension



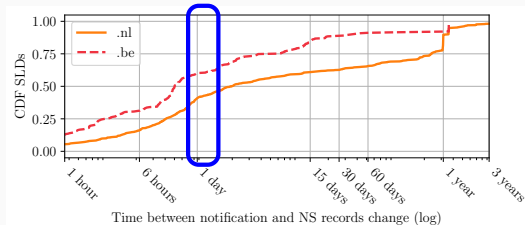
(d) Web mitigation

DNS vs Web mitigation speed

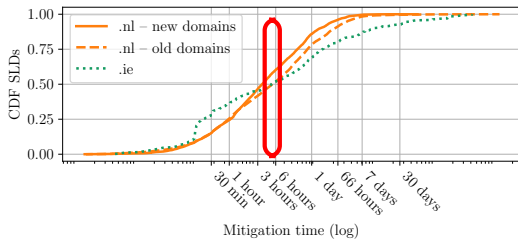
Web mitigation is faster than DNS mitigation

**DNS: 50–60% first
24h**

Web: 50–60% first 6h



(e) DNS mitigation: Domain suspension



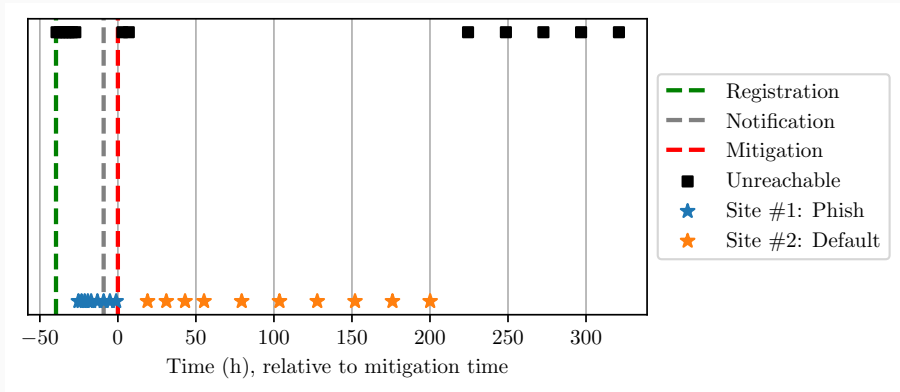
(f) Web mitigation

Phishing against a French bank (.nl domain name)

The screenshot displays a phishing website designed to look like the legitimate Crédit Mutuel client portal. At the top, the 'Crédit Mutuel' logo is on the left, and a search bar with the placeholder 'Rechercher' is on the right. Further right are two menu items: 'DEVENIR CLIENT' with a recycling icon and 'ESPACE CLIENT' with a house icon. Below the header, the main content area is titled 'Espace client : Connexion'. On the left, there are three vertical menu items: 'Identifiant / Mot de passe', 'Certificat Electronique', and 'SAFETRANS'. Below these is a small image of a hand holding a smartphone with a lock icon, followed by the heading 'Tout savoir sur Internet et la sécurité' and a short paragraph of text with a 'Lire la suite' link. The central focus is a login form with two input fields labeled 'Identifiant' and 'Mot de passe', a 'Se connecter' button, and two links below: 'Codes d'accès oubliés' and 'Infos sécurité'. At the bottom of the page, there is a footer with several small links: 'Mentions légales', 'Guides et informations réglementaires', 'Site institutionnel', 'Trouver une caisse ou un distributeur', 'Gestion des cookies', and 'Protection des données'. The footer also includes a small logo for 'ABS' and the 'TU Delft' logo.

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

Background

Vulnerability Disclosure

Phishing Attacks at Scale

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



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

Recap:What you will learn today:

Coordinated Vulnerability Disclosure

1. Explain its importance
2. Simulate a disclosure
3. Explain different vendor's behavior in practice
4. Be able to make informed choices when doing a CVD

Reference: CCR2023 [2]

Phishing attacks at scale

1. Explain phishing and economics
2. Evaluate the attacker mindset
3. Explain attacker's choices
4. Explain what type of mitigations exist

Reference: CCS2024 [1]

Recap:What you will learn today:

Coordinated Vulnerability Disclosure

1. Explain its importance
2. Simulate a disclosure
3. Explain different vendor's behavior in practice
4. Be able to make informed choices when doing a CVD

Reference: CCR2023 [2]

Phishing attacks at scale

1. Explain phishing and economics
2. Evaluate the attacker mindset
3. Explain attacker's choices
4. Explain what type of mitigations exist

Reference: CCS2024 [1]

Conclusion

- Hope you enjoyed it
- Contact: giovane.moura@sidn.nl , giovane.moura@tudelft.nl

- [1] MOURA, G. C. M., DANIELS, T., BOSTEELS, M., CASTRO, S., MÜLLER, M., WABEKE, T., VAN DEN HOUT, T., KORCZYŃSKI, M., AND SMARAGDAKIS, G.

Characterizing and mitigating phishing attacks at cctld scale.

In Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security (New York, NY, USA, 2024), CCS '24, Association for Computing Machinery, p. 2147–2161.

- [2] MOURA, G. C. M., AND HEIDEMANN, J.

Vulnerability disclosure considered stressful.

SIGCOMM Comput. Commun. Rev. 53, 2 (jul 2023), 2–10.

[3] SCHNEIER, B.

Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea', 2007.