Fraud detection at EURid, an overview

ccNSO TechDay
2021.06.14
Jordi Iparraguirre

Why is EURid into this?

We strive for a trusted **.eu** space

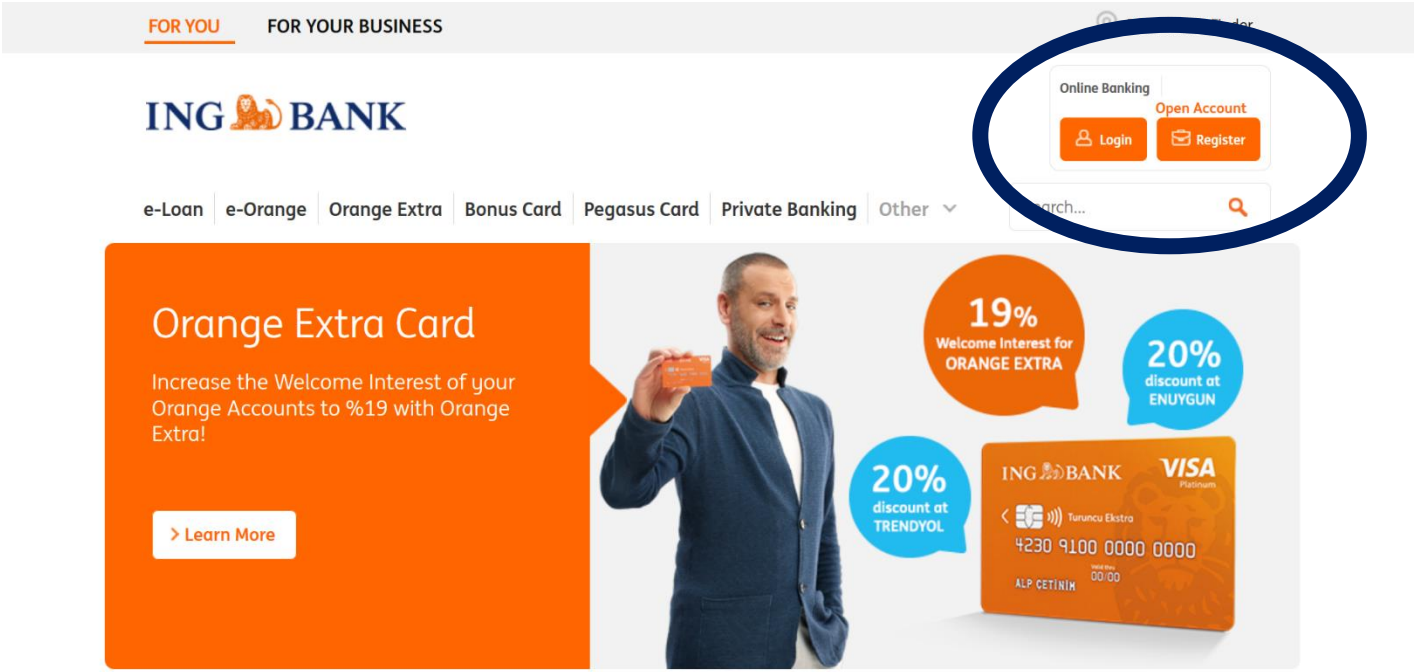
for users, businesses & consumers

Basic framework

- We do not host content
- We do not want to be the resource used for causing harm
- We are not the police/judge of the Internet
- We verify registrant’s Whois data
- But, can we walk an extra mile? → Prevent and mitigate abuse

If we are not the police/judge of the Internet, how can we prevent abuse?

What is abuse?



impots.gouv.fr
un site de la Direction générale des Finances publiques

Votre espace particulier

Votre espace professionnel

Accueil > Particulier > Formulaire de remboursement électronique - N 0062405129

Confirmer vos informations

Nom complet

Prénom

Nom

Date de Naissance

Jour | Mois | Année

Adresse

Adresse

Code Postal

Téléphone

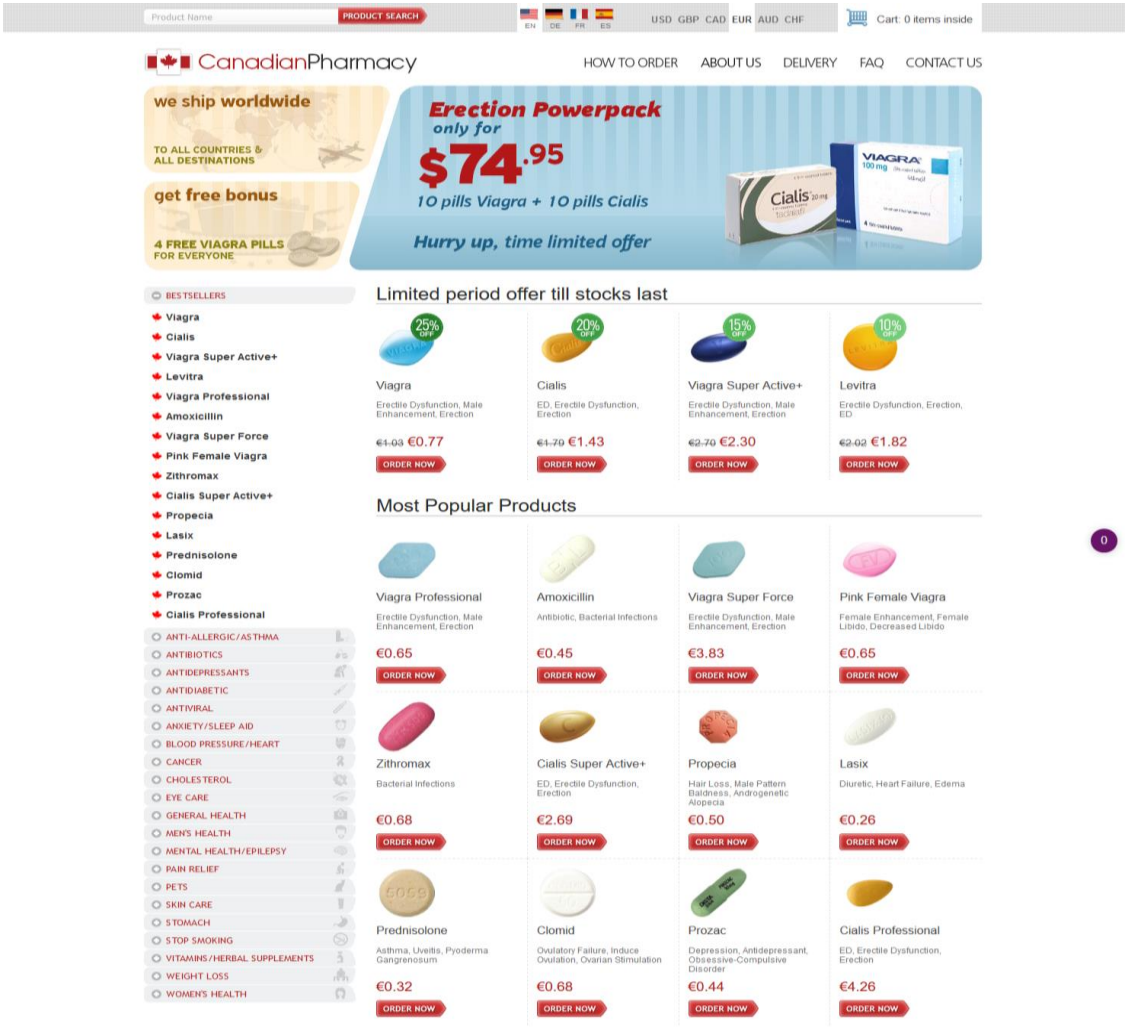
Mobile

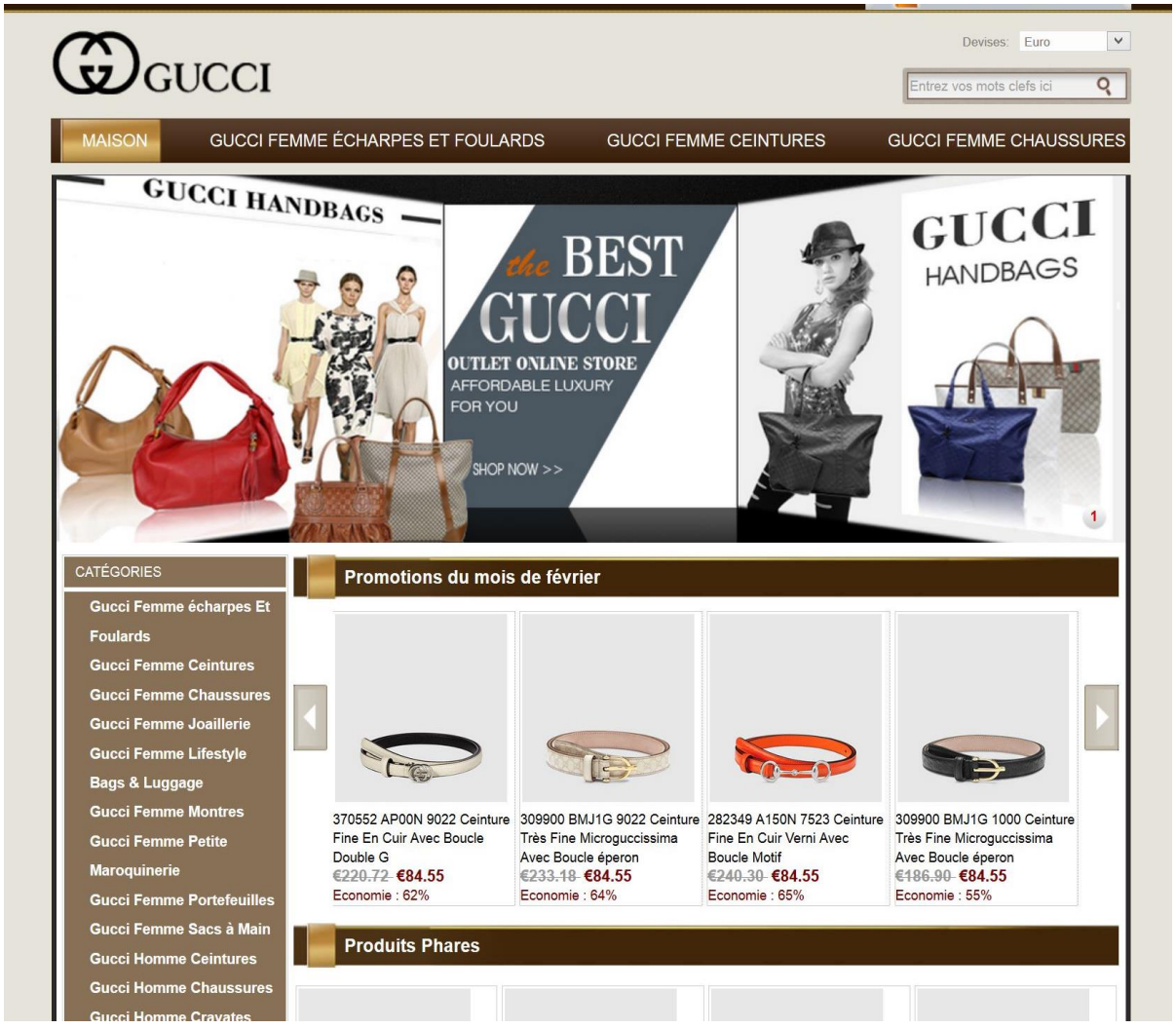
Vos coordonnées bancaire

Votre banque : Choisissez votre banque

Valider

Un site de la direction générale des Finances publiques



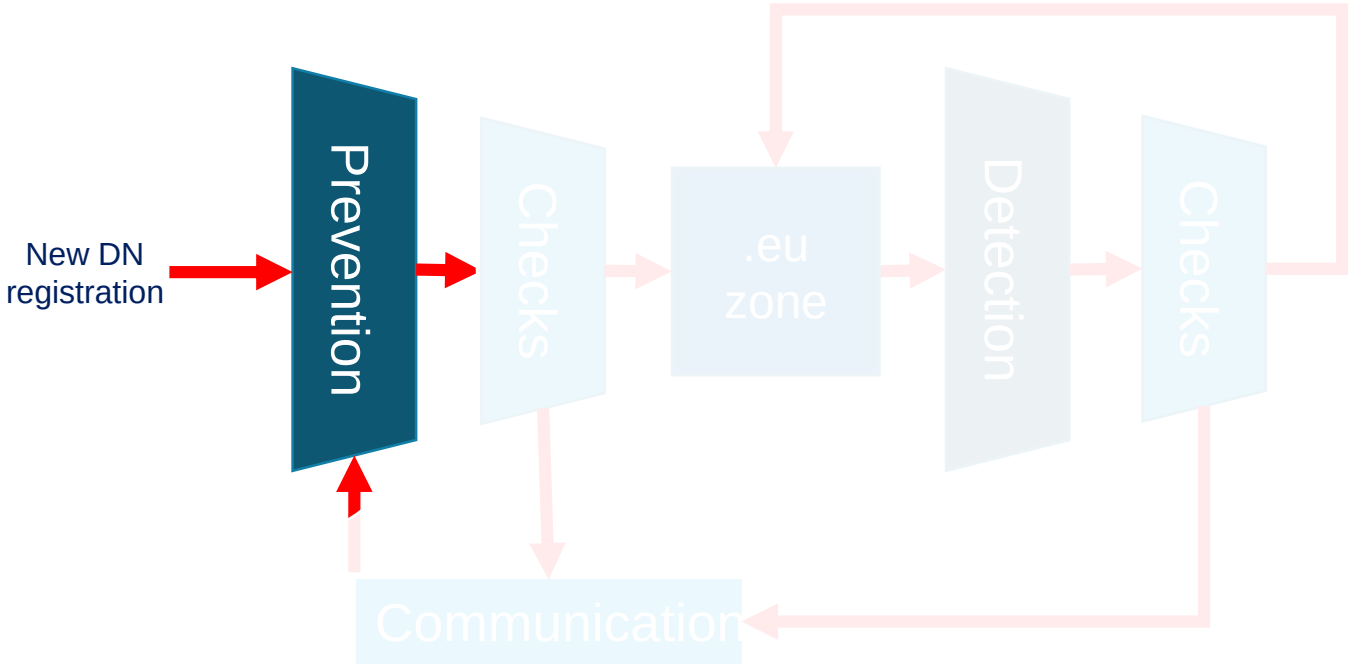


Prevent and mitigate abuse

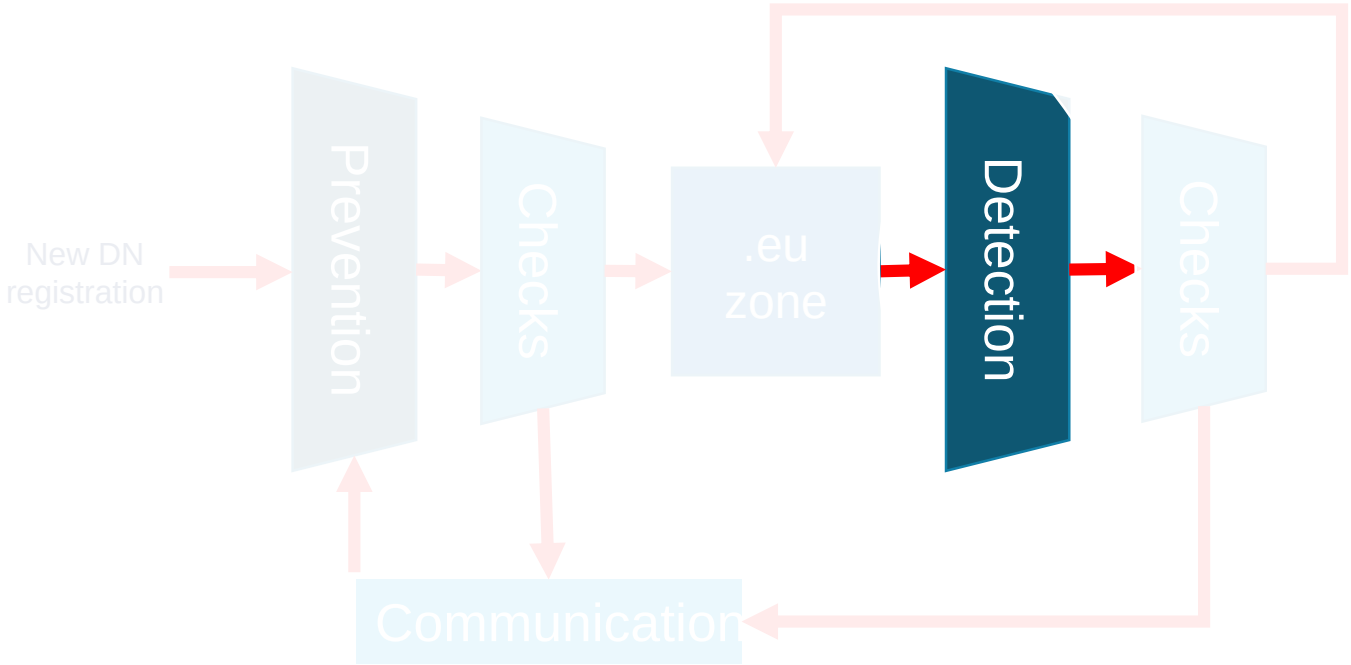
Concept

We act at different levels

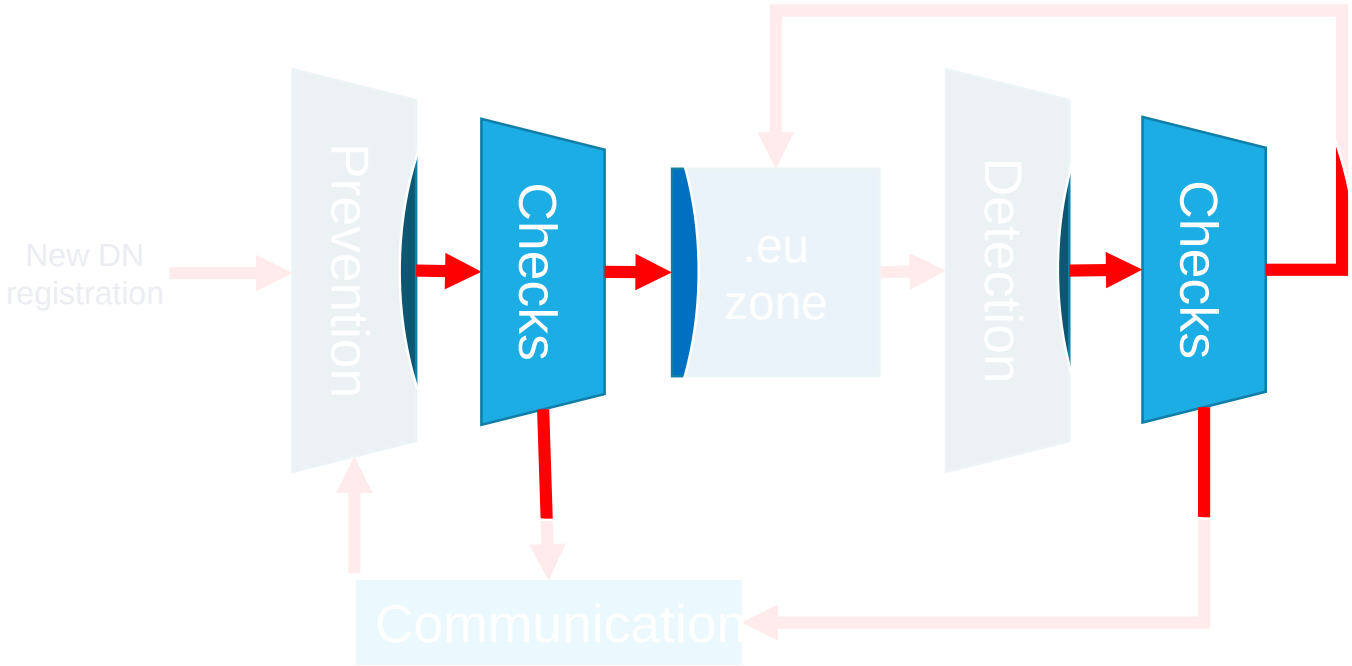
1. **Prevention**: APEWS



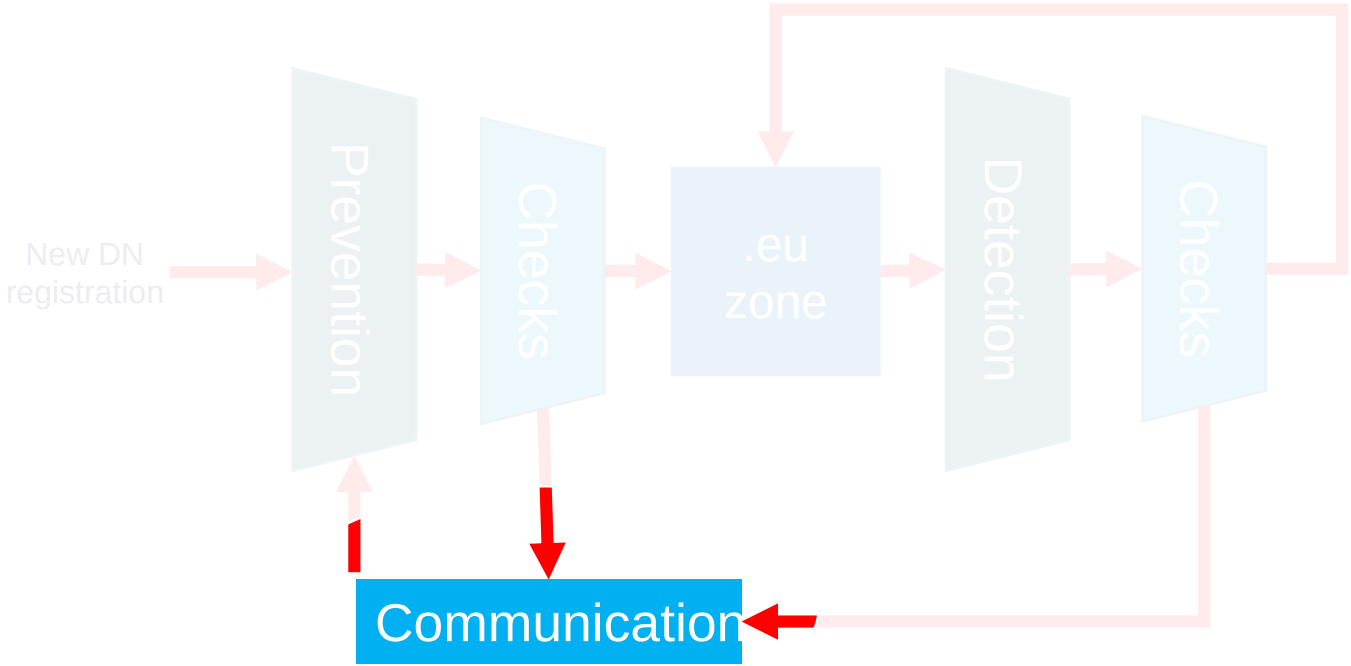
2. **Detection**: Post delegation



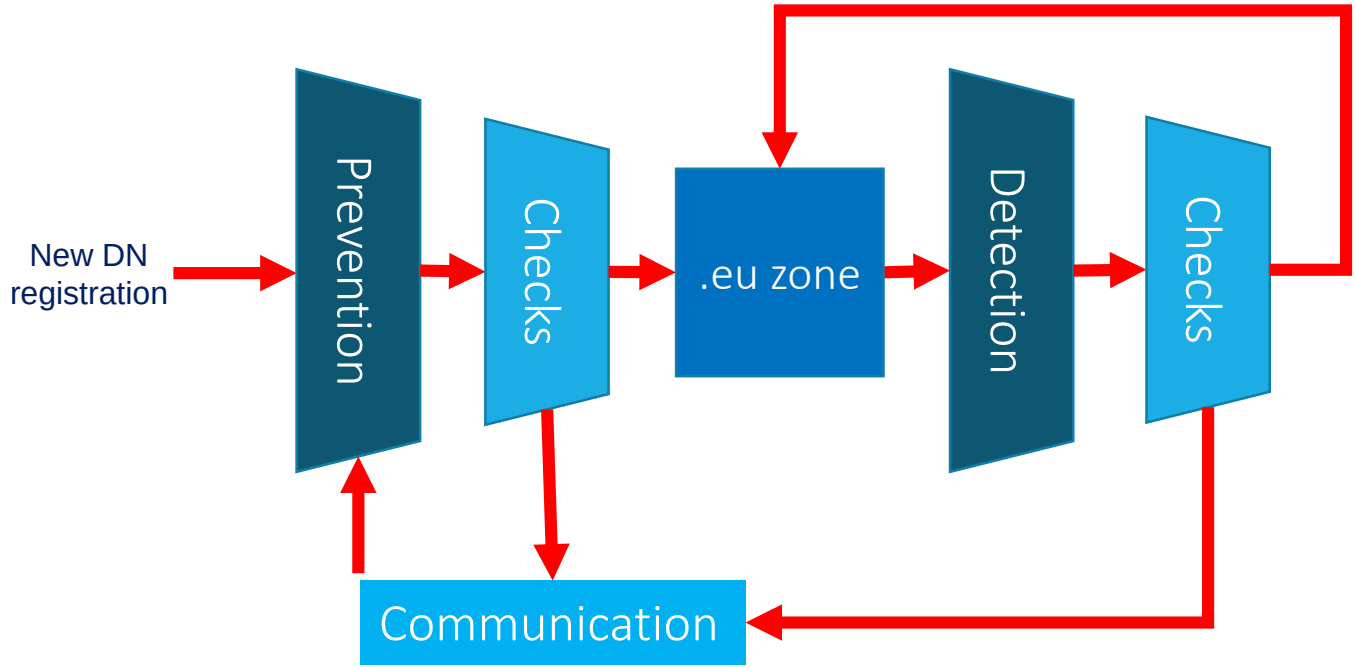
3. **Checks**: WhoisQuality & KYC



4. **Communication**: Share findings



We act at different levels



Prevent and mitigate abuse

Practice

1. APEWS

Abuse **P**rediction and **E**arly **W**arning **S**ystem

Award winning machine learning system

Domain name is registered but NOT (yet) delegated

Pre-delegation Machine-Learning checks

Suggests, before delegation, allegedly abusive domains

- Using domain registration data
- Mixed with external intelligence (experts' confirmed abuse lists)

1. APEWS

Domain name delegation is stopped

- We ask registrant for evidence of correct registration data
- We do human review of each case
- Now, with KYC (eIDAS and MRZ), we automate it and increase certitude

APEWS development started in 2016 after negotiation with the EC

In production since January 2020

1. APEWS

APEWS uses different ML algorithms

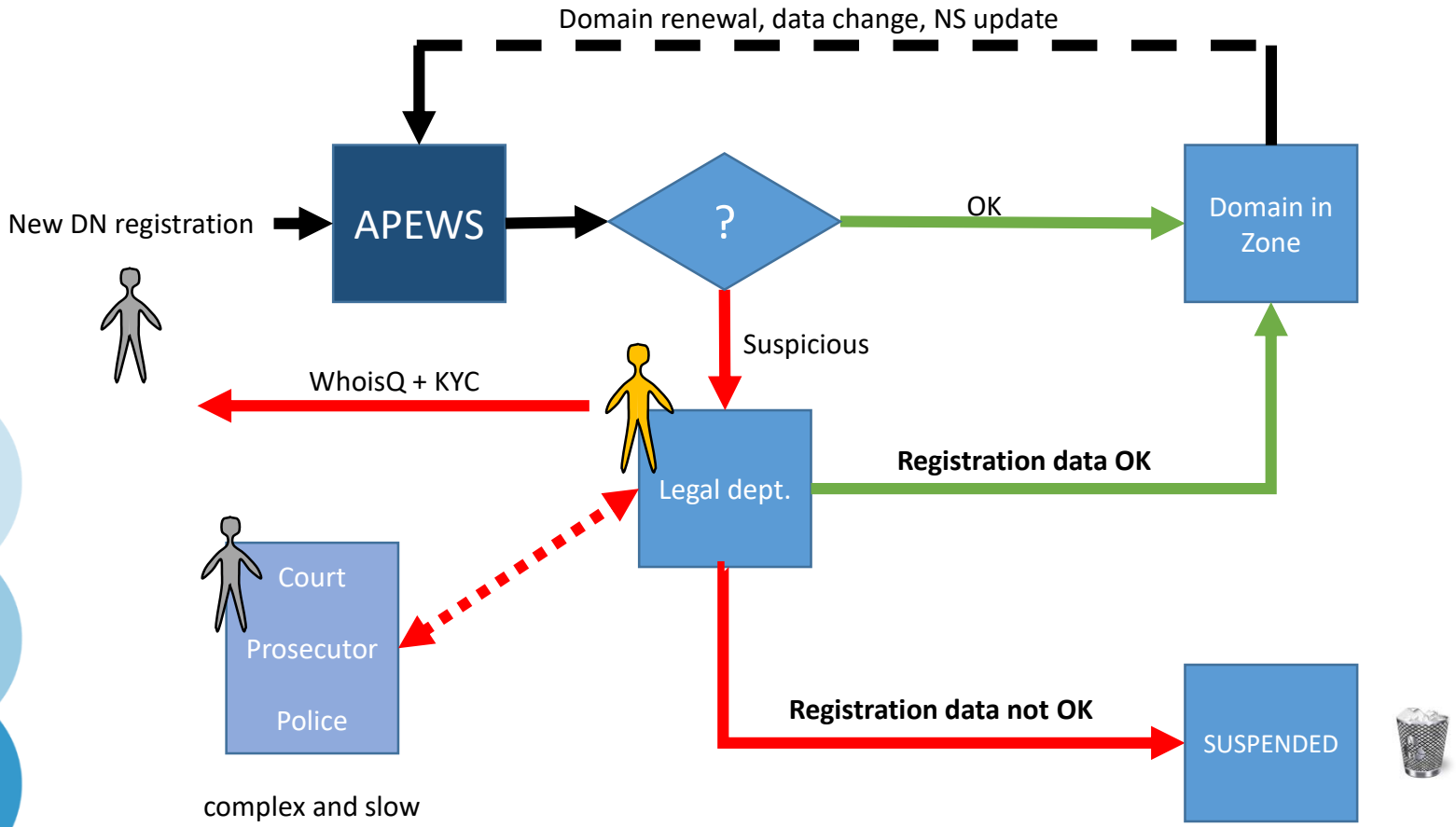
APEWS re-trains itself regularly

Academic papers:

https://eurid.eu/en/news/identification-of-malicious-dns/

Combined with a rule-based system

- Eg. Stop COVID19 related domains (EC request)



2. Post-delegation checks

Domain name is registered AND delegated

Looks for allegedly abusive domains

- DNs delegated in the last 24h
- DNs delegated a few weeks ago
- Ad-hoc list of domains, at any time

2. Post-delegation checks

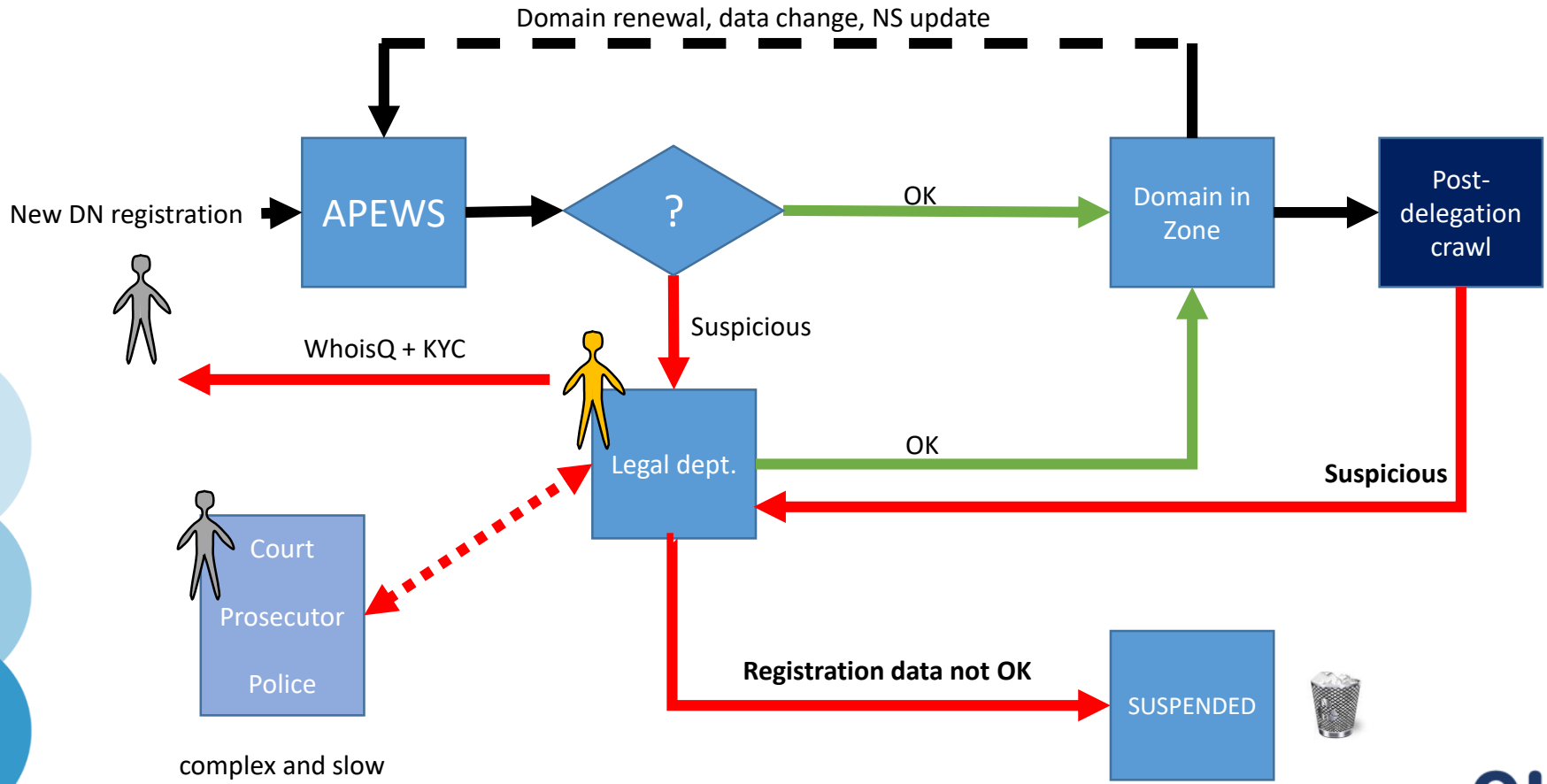
Analyze DN itself (look for certain brands, keywords, …)

Crawl all DNs

Analyze HTML content

- web shop? → selling well-known brands?
- bank clone?
- etc (we easily create and add new modules)

Analyze registration data and metadata


Domain renewal, data change, NS update
New DN registration
APEWS
?
OK
Domain in Zone
Post-delegation crawl
Suspicious
WhoisQ + KYC
Legal dept.
OK
Suspicious
Court
Prosecutor
Police
Registration data not OK
SUSPENDED
complex and slow

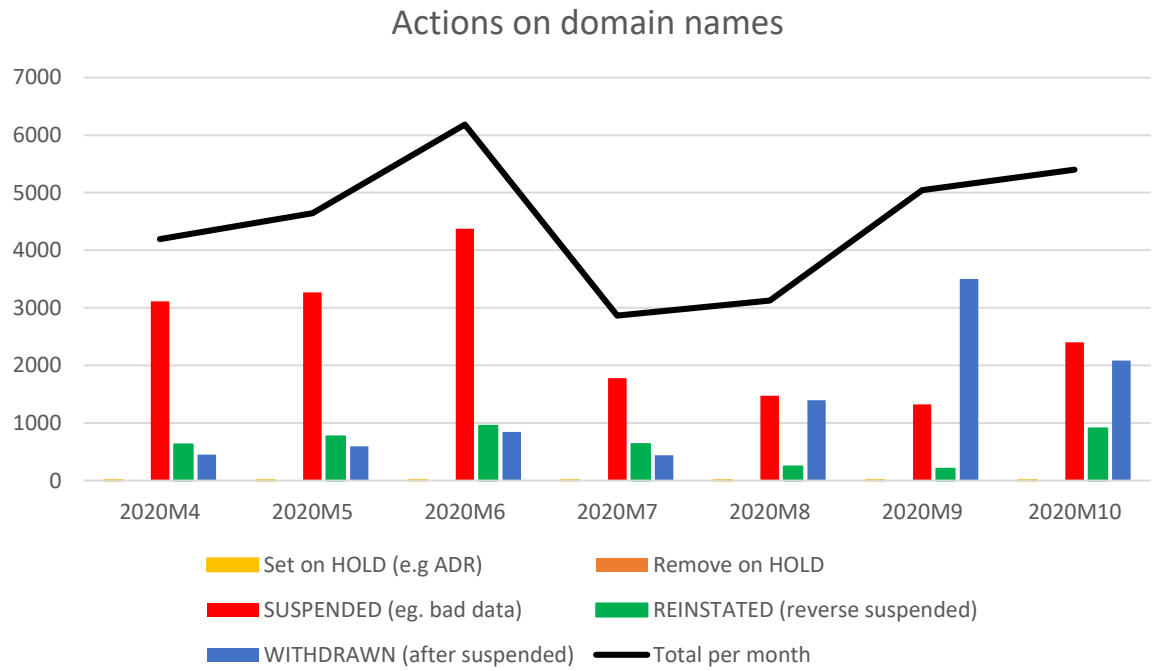
3. Check: Review of suspicious cases

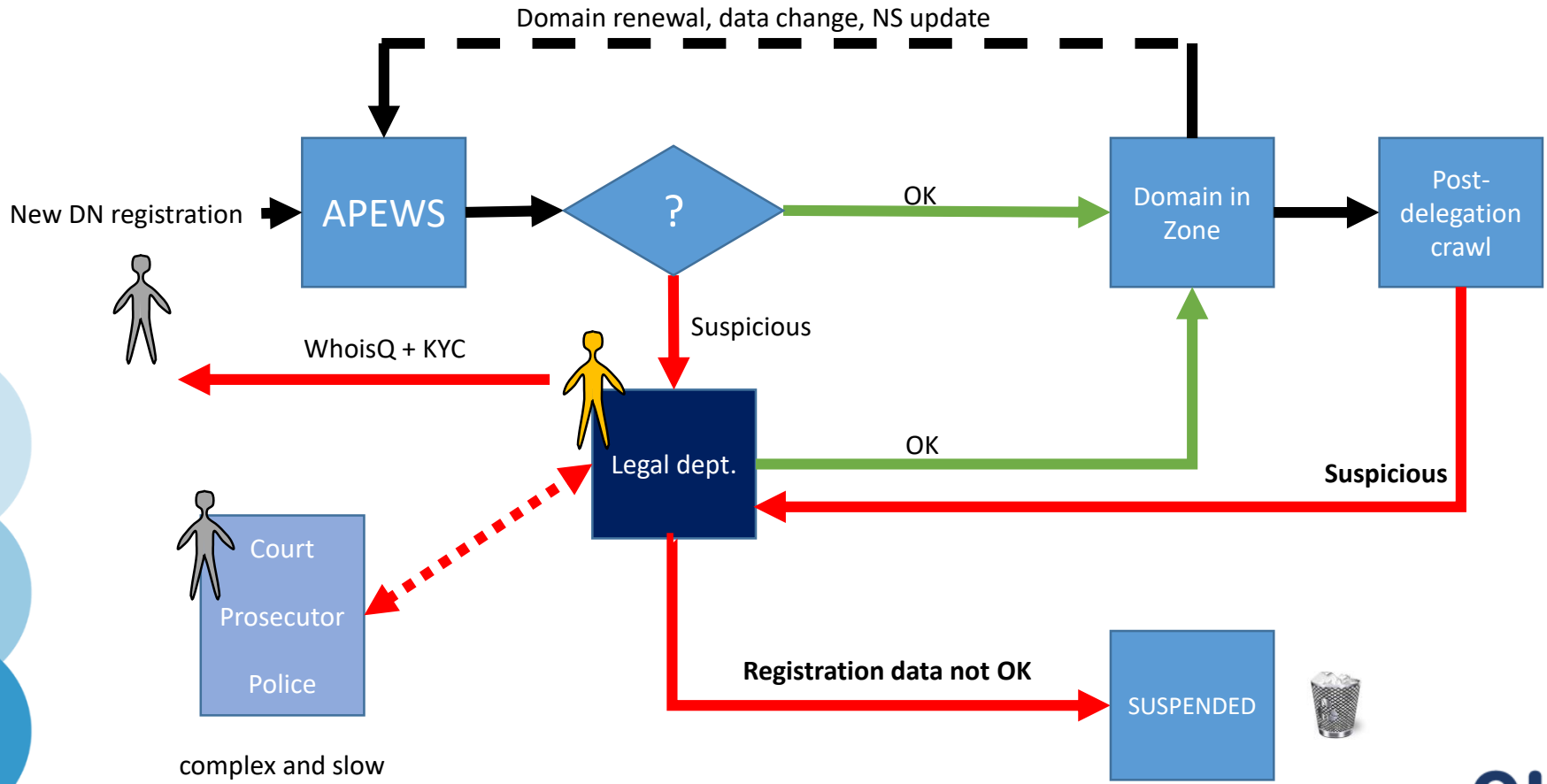
Human revision by EURid's **Legal** department

- Whois Quality check: ask registrant to prove its whois data
  - Email exchange (calls)
  - Suspicions of receiving forged/*photoshoped* bills/ID documents
  - Now, **KYC** → much more difficult to lie

- We cannot suspend based on our opinion on web content
- So we share our suspicions with experts

3. Review of suspicious cases




Domain renewal, data change, NS update
New DN registration
APEWS
?
OK
Domain in Zone
Post-delegation crawl
Suspicious
WhoisQ + KYC
Legal dept.
OK
Suspicious
Court
Prosecutor
Police
Registration data not OK
SUSPENDED
complex and slow

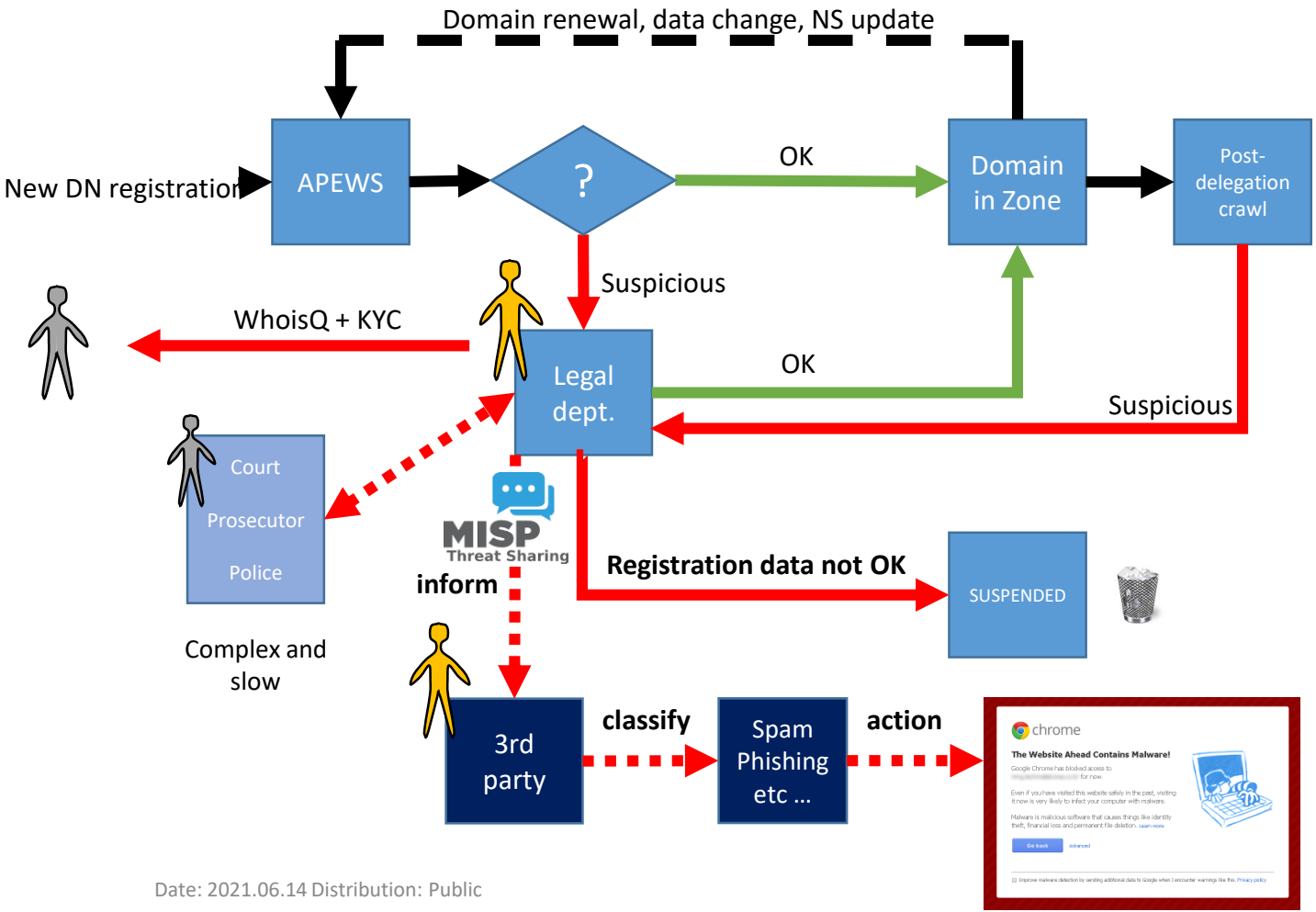
4. Share intelligence

Sharing allegedly suspicious DNs with 3rd party experts
(depending on alleged “type of abuse”)

- EUROPOL
- CERT.be + CCB (Centre for Cybersecurity Belgium)
- FOD Economy (Belgian customs)
- ASOP (Alliance for Safe Online Pharmacy)
- APWG.eu (Anti Phishing Working Group)
- eCommerce Foundation
- Global Cyber Alliance
- …

4. Share intelligence

We (daily) share our findings in parallel to our own checks (WhoisQ + KYC)



Aantal namaakwebsites daalt: proactieve aanpak werkt!

Online namaakverkoop en piraterij op het internet blijven hoge toppen scheren. Toch worden er minder namaakwebsites opgericht, blijkt uit het aantal afgesloten websites in België. Dit is het resultaat van de internationale campagne In Our Sites en de proactieve samenwerking met EURid, DNS Belgium en de douane. België scoort hiermee goeie punten en is op dat vlak wereldwijd één van de koplopers.

Vorig jaar sloten de Economische Inspectie en de douane 990 namaakwebsites af. Dit jaar is dat aantal lichtjes gestegen tot 1.016. Op het eerste gezicht lijkt er niet veel veranderd, maar niets is minder waar. Sinds de coronacrisis steeg het aantal online aankopen immers gevoelig. Toch steeg het aantal afgesloten namaakwebsites op .be en .eu niet evenredig. Dat is te danken aan de samenwerking van de FOD Economie met EURid, DNS Belgium en de douane in het kader van de internationale Europol-actie In Our Sites. Die zet in op een proactieve aanpak. EURid en DNS Belgium sluiten verdachte websites die eindigen op .be of .eu meteen bij de bron af. Hoewel de online verkoop in 2020 een boost kende, steeg het aantal geblokkeerde namaakwebsites met .be en .eu niet. Deze manier van werken maakt van België zelfs één van de koplopers op wereldwijd vlak.

Number of fake websites decreases: proactive approach works!

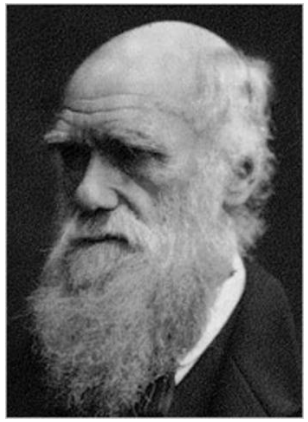
Online counterfeiting and Internet piracy continue to soar. Yet fewer fake websites are being set up, according to the number of closed websites in Belgium. This is the result of the international In Our Sites campaign and the proactive collaboration with **EURid**, DNS Belgium and customs. Belgium scores good points with this and is one of the leaders worldwide in this area.

https://news.**economie.fgov.be**/193665-aantal-namaakwebsites-daalt-proactieve-aanpak-werkt

But… This is a Darwinian marathon

We push

They **adapt** to bypass detection or go away



We **adapt** or fail

They change

And…

- We do see **changes in behaviours**

- Eg. pushing abusers to send “valid” but useless data
  - Some issues clearly disappeared
  - Invented and plausible registration data
  - There are repositories of fake-valid ID data in github
  - Anonymizer services (no need in EU due to GDPR, but…)
  - **KYC** to the rescue!

Thanks! Questions?

Jordi.iparraguirre@eurid.eu

.eu .ею .ευ

Powered by EURid