.eu, .ευ & .ею and DNS Abuse

Peter Janssen
General Manager, EURid vzw

ICANN77 Washington D.C.
14/06/2023
Registration & delegation process

1. Registrant → Registrar
2. Registrar → EPP → Domain Name Delegation → Primary NS
3. Registrar → Web portal → EPP → Domain Name Delegation → Primary NS
4. Registrar → EPP → Domain Name Delegation → Primary NS
Delayed delegation

At "delegation time"
- Evaluate the registration
- Flagged as "potential malicious"
  - Yes: Delay delegation
    - Start validation process
  - No: Delegate

14/06/2023 Washington D.C. – ICANN77 – Public
Decision engine (APEWS)

• **Abuse Prediction and Early Warning System**

• **Goal:**
  - At time of registration of a domain name
  - Predict if the domain name is registered with malicious/abusive intent

• **Domain name “attributes”**
  - Registrant data (name, address, email, ...)
  - Registrar
  - Domain name “randomness”
  - DNS info (name servers)

• **Machine learning models**
Predictive model

For each new registration, the system predicts if the domain name was registered with malicious intent.
Prediction results

Blacklist ratio per month

Jan 2019 Jan 2020 Jan 2021 Jan 2022 Jan 2023
Prediction model

• Tuning
  • Recall (how many were found)
    vs.
  • Precision (how many of those that were found were correct)

• During the time predictions were made but no delayed delegation
  • Recall > 80%
  • Precision > 80%

• False positive (predicted as malicious but really benign)
  • Registrant has to do a little extra effort (validate the registrant data)
Deployment

• Post registration – Pre delegation

• Pre registration
  • Prediction needs to be fast enough
    (as registrar is waiting for response from registration request)

• Post registration – Post delegation
  • Other information is available (content of websites, security feeds, ...)

• Cross TLD/registry
  • Similar abusive patterns exist across different TLDs
  • Anonymisation of registrant data (one way hashing)
    • “peterjanssen” -> “c103ce1de8dfcfaa705fb18487a7c602”