Abuse monitoring policies and procedures @ EURid

Brussels, 28 Jan 2016

Giovanni Seppia, External Relations manager

Author: EURid Asbl/vzw
Status of document/presentation:
CONFIDENTIAL

Agenda

- Roles
- Abuses + actions
- LEA cooperation
- WHOIS Q plan
- APEWS

Roles of key players in the domain industry

Registry	Registrar
Manager of the TLD at the root level	In the registry-registrar-registrant model, it manages the possible other services linked to a domain name (e.g. hosting)
Domain name	Website, email, FTP
Currently around 1800 registries, including both cc and gTLDs	Much over 10 000 around the world

Your European Identity

Abuses (either via complaints or own assessment)

Content related (website)
- Copyright infringement (streaming, peer to peer, …)
- Online pharmacies
- Online gambling
- Counterfeit
- …

Email related
- Spam
- Phishing
- Scam
- …

Technical / infrastructure related
- DDOS, etc.
- Botnets, malware distribution, clickfraud

Actions

Authority of EURid is limited to verification of **registration data**

According to the **EC Regulations (733/2002 and 874/2004)** and T&C EURid may take action in case of abuse, but:

- *At own risk (damage claims if wrong action)*
- *Assessment of "abuse": only court!*

When content related, cooperation with/redirect to the registrar

Correctness of registration data:

- Cross-checks with third parties if address exists
- Notification to registrar and/or registrant with the request to correct data within 14 calendar days
- If no satisfactory reaction, the domain is suspended (6 months)
- The domain is withdrawn (1 month)
- The domain is released (available for registration - first come first served)
- **Fast track for special cases**

.eu Your European Identity

LEA cooperation (Belgian level)

CERT-EU (Memorandum of Understanding since three years)
First hand notifications of spam/phishing/

Cybersquad (Belgian customs special cybercrime unit)
Very good cooperation on counterfeit.
In most cases, they don't want to take down a domain, but to collect evidence of website content because they need verification of registration data and want to arrest people on the spot.

FOD Economie (Belgian Ministry of Economic Affairs)
Very good cooperation on copyright infringement (peer to peer).
In most cases, the need verification of registration data and want to arrest people on the spot or they request action via Public Prosecutor.

Public Prosecutor
Request for seizure of domain(s) and/or redirection to specific website or IP address (in most cases based on global cooperation with FBI / EUROPOL) (art. 39bis Criminal Code).

Whois Quality Plan

- Fully deployed in early 2014
- Extensive consultation with our registrar community
- Extensive check of actions developed by our industry peers
- Currently great cooperation with most of the registrars (including those working with large resellers network)
- Clear impact on growth in exchange of a more sound and clean WHOIS database

Whois Quality Plan
Statistics 2015

- Domain names

  - Suspended: 14 710 (holder still has the domain and it is shown in WHOIS)

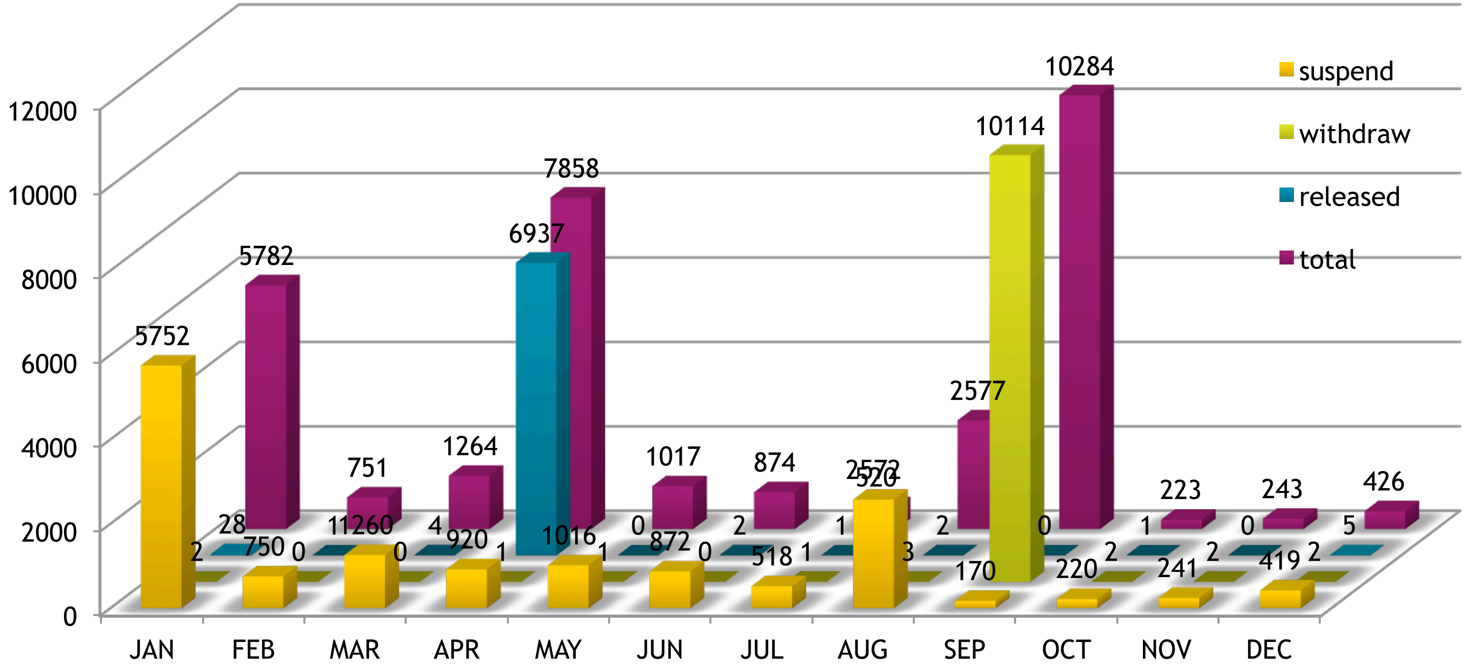
  - Withdrawn: 10 128 (holder no longer has the domain but it is not shown in WHOIS)

  - Released: 6 981 (domains are available on first come first served basis)

Total = **31 819** domain names were deleted as a result of data verification (at EURid's own initiative)

.eu
Your European Identity

WHOIS Quality Plan
Statistics 2015



.eu
Your European Identity

A.P.E.W.S

Abuse Prevention & Early Warning System

.eu

Your European Identity

In the pipeline

- **Suspension (**see previous slides**)**
- **Withdrawal / revocation (**see previous slides**)**

COMING SOON

- **Delayed delegation**: registrations that are marked by APEWS as potentially being abusive will be delegated later

Research on predicting abuse

- **Scope:** Focusing on certain kinds of abuses such as C&C for botnets, spam and phishing domains, malware domains (distribution and control)
- Output of abusive prediction system will be used for delayed delegation

Research on predicting abuse

- 2015: project with iMinds, KU Leuven to investigate the possibility of creating a predictive model and/or method to predict abuse

- The model is first and foremost based on the registration data and not DNS query data. Registration data includes:
  - Registrant data,
  - Registrar “reputation”,
  - Name server data,
  - #registration per registrar per registrant per unit of time
  - …

Preliminary results - 2015

- Based on feeds from Spamhaus, Google SafeSearch as input parameters
- It is possible to predict with a relatively high certainty that a domain name is likely used for malicious purposes
- Prediction techniques are in the refinement process as well as the development of a working prototype

Thank you!

giovannis@eurid.eu

.eu
Your European Identity