Whois/RDS and GDPR

ICANN 60
31 October 2017

Agenda

- Developments since ICANN59
  - RDS Use Cases Matrix
  - ICANN Org. Outreach
  - Community Discussions
  - Legal Analyses
- Significance to the Public Interest
  - Impact on Law Enforcement
  - Impact on Cybersecurity
  - Impact on Consumer Protection and the Public
  - Impact on Business Interests
- Next Steps
  - Issue for GAC/ICANN Board Meeting
  - Draft GAC Advice
  - Contribution to solutions

Whois is Important for Public Safety

- Civil and criminal law enforcement authorities rely on Whois as a first step for investigating and combatting illegal conduct
- Public relies on Whois when websites do not contain contact information

Whois is Important for Public Safety

- Law Enforcement Case Examples
  - Criminal
  - Civil/Consumer Protection
  - Privacy
- Uses by the public
  - Due Diligence for purchases or transmitting sensitive $ or health information
  - Resolve disputes
  - Report complaints

EUROPOL

EC3 | European Cybercrime Centre

@EC3Europol

USE OF WHOIS
CYBER INVESTIGATORS

Grégory Mounier

Europol

Role of WHOIS in cyber investigations

EUROPOL EC3 European Cybercrime Centre

- WHOIS information is mainly used for two purposes:
  1. to identify a **contact point** for a domain name
  2. to gather **investigative leads** related to the owner/purchaser of the domain.
- WHOIS can help crime attribution
- WHOIS is one cyber investigative tool among many others
- WHOIS is not a silver bullet
- WHOIS help establish patterns or help identification of an individual

Address lookup

canonical name **lemonde.fr.**

aliases

addresses **93.184.220.20**

Domain Whois record

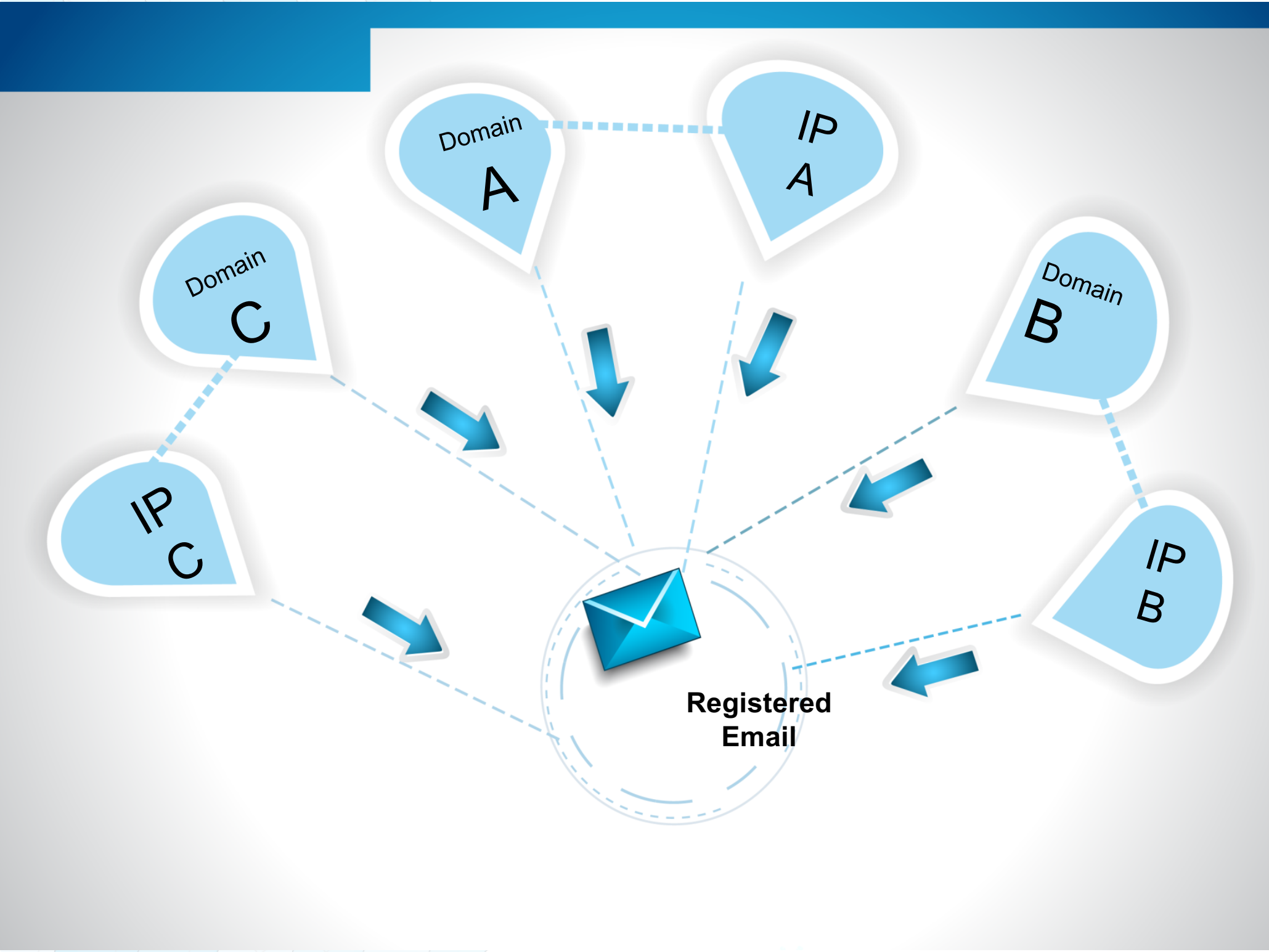
Queried **whois.nic.fr** with "**-n lemonde.fr**"...

```
domain:       lemonde.fr
status:       ACTIVE
hold:         NO
holder-c:     SEDM43-FRNIC
admin-c:      DA15208-FRNIC
tech-c:       NH3559-FRNIC
zone-c:       NFC1-FRNIC
nsl id:       NSL106501-FRNIC
registrar:    Ascio Technologies Inc. Danmark - filial af Ascio Technologies Inc. USA
Expiry Date:  11/02/2018
created:      02/08/2005
last-update:  11/02/2017
source:       FRNIC

ns-list:      NSL106501-FRNIC
nserver:      ns1.ascio.net
nserver:      ns2.ascio.net
nserver:      ns4.ascio.net
source:       FRNIC

registrar:    Ascio Technologies Inc. Danmark - filial af Ascio Technologies Inc. USA
type:         Isp Option 1
address:      Islands Brygge 55
address:      DK-2300 COPENHAGUE S
country:      DK
phone:        +44 2070159328
fax-no:       +45 33 88 61 01
e-mail:       nicrelations@ascio.com
website:      http://www.ascio.com
anonymous:    NO
registered:   18/01/2001
```

```
nic-hdl:      SEDM43-FRNIC
type:         ORGANIZATION
contact:      SOCIETE EDITRICE DU MONDE
address:      80, boulevard Auguste Blanqui
address:      75707 Paris Cedex 13
country:      FR
phone:        +33 1 57 28 20 00
fax-no:       +33 1 57 28 21 21
e-mail:       domain_names@lemonde.fr
registrar:    Ascio Technologies Inc. Danmark - filial af Ascio Technologies Inc. USA
changed:      04/09/2012 nic@nic.fr
anonymous:    NO
obsoleted:    NO
eligstatus:   ok
eligdate:     04/09/2012 09:34:28
source:       FRNIC

nic-hdl:      DA15208-FRNIC
type:         PERSON
contact:      Domain Administrator
address:      SOCIETE EDITRICE DU MONDE
address:      80, boulevard Auguste Blanqui
address:      75707 Paris
country:      FR
phone:        +33 1 57 28 20 00
e-mail:       domain_names@lemonde.fr
registrar:    Ascio Technologies Inc. Danmark - filial af Ascio Technologies Inc. USA
changed:      04/08/2016 nic@nic.fr
anonymous:    NO
obsoleted:    NO
eligstatus:   ok
eligdate:     04/08/2016 17:45:52
reachmedia:   email
reachstatus:  ok
reachsource:  REGISTRAR
reachdate:    04/08/2016 17:45:52
source:       FRNIC
```

BOTNET

- EC3 identified a suspect with **WHOIS data**
- **WHOIS lookup** on the **domain** => **email address**
- **Reverse WHOIS lookup** => other domains registered with same email
- Domain => **Old private website**
- Successful arrest and conviction


Domain
A
IP
A
Domain
C
Domain
B
IP
C
IP
B
Registered
Email

Conclusion

- **Accurate and easily accessible WHOIS data:**
  - ✓ Helps law enforcement to attribute crime
  - ✓ Saves precious time (victims)
  - ✓ Security researchers, CERT teams, first responders
  - ✓ Makes life of criminals more difficult

Agenda

- Developments since ICANN59
  - RDS Use Cases Matrix
  - ICANN Org. Outreach
  - Community Discussions
  - Legal Analyses
- Significance to the Public Interest
  - Impact on Law Enforcement
  - Impact on Cybersecurity
  - Impact on Consumer Protection and the Public
  - Impact on Business Interests
- Next Steps
  - Issue for GAC/ICANN Board Meeting
  - Draft GAC Advice
  - Contribution to solutions

Possible GAC Advice

1. 2007 GAC Whois Principles remain applicable and should be respected

2. Keep Whois accessible to the public to combat abuse and fraud, and engage in due diligence for online transactions and communications

3. Keep Whois accessible and effective for consumer protection and law enforcement investigations and crime prevention efforts

4. Encourage ICANN to practice transparency in its GDPR activities and provide opportunity for timely and meaningful GAC input

5. Encourage ICANN to engage with the European Commission to facilitate discussions regarding the GDPR compliance process