EUROPEAN CYBERCRIME CENTRE

EC3 EUROPOL

GAC – PSWG
Inter-sessional meeting - Brussels

Use of DNS and IP WHOIS for cyber investigations

Case examples

European Cybercrime Centre
EC3 Europol

28 October 2015

Europol Unclassified - Europol Public Information

EC3 Operations

Cyber Intelligence

Cyber Data Fusion

FP Terminal

Transnational Payment Fraud

FP Cyborg

Cyber Intrusion

FP Twins

Child Sexual Expolitation

Role of WHOIS in cyber investigations

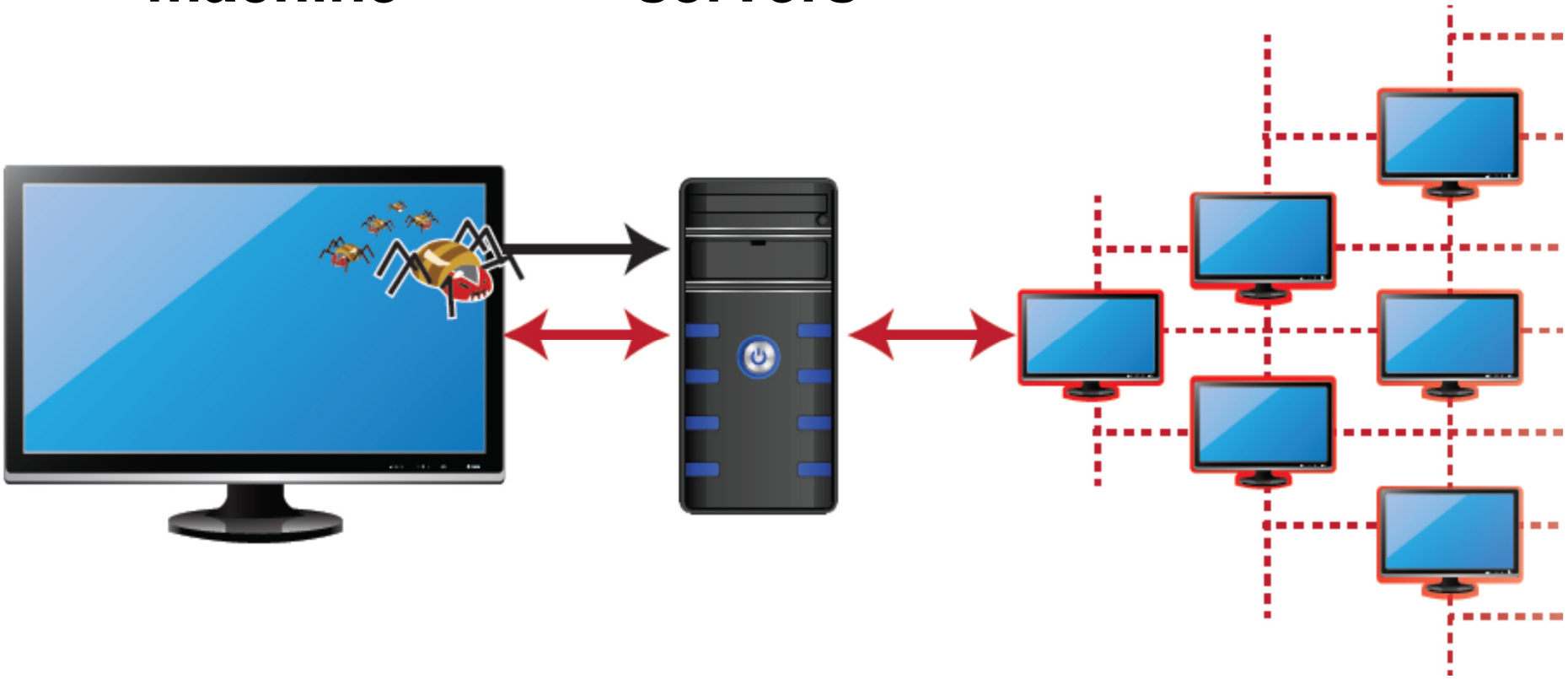
- WHOIS can help crime attribution
- WHOIS is one cyber investigative tool among many others
- WHOIS is not a silver bullet
- Accurate WHOIS makes life of criminals more difficult

Botnets infrastructure

Malware & infected machine

Command & Control servers

Botnet



Europol Unclassified - Basic Protection level

EUROPEAN CYBERCRIME CENTRE

EC3 EUROPOL

Botnets and DNS abuse

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

ISP operating at global level

IP of server used as botnet C&C → IP Database: ISP in country A → NO

↓

Alternative searching tools → Country B: Subsidary ISP company in B → MLAT

RIRs, LIRs and ISPs should all maintain accurate WHOIS data on IP end users

Investigative time wasted to alternatively localize the IPs

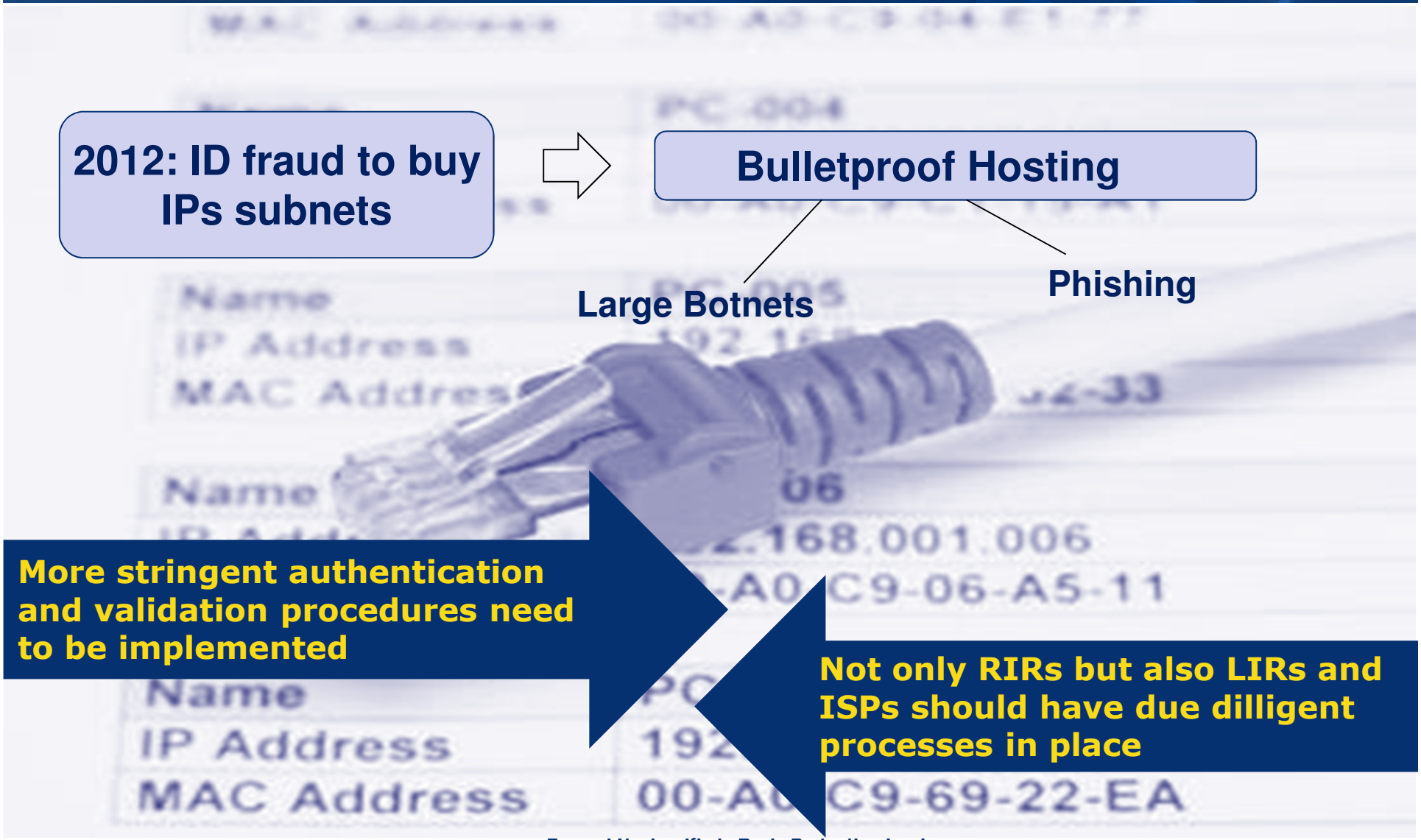
Bulletproof Hosting

2012: ID fraud to buy IPs subnets

Bulletproof Hosting

Large Botnets

Phishing



More stringent authentication and validation procedures need to be implemented

Not only RIRs but also LIRs and ISPs should have due dilligent processes in place

Conclusion 1

- **Accurate and reliable DNS and IP WHOIS data:**
  - ✓ **Helps crime attribution**
  - ✓ **Saves precious investigation time**
  - ✓ **Makes life of criminals more difficult**

Europol Unclassified - Basic Protection level

Conclusion 2

- Improved compliance
- Improved due diligence
- Stringent authentication and validation procedures
- Contractual requirement for all actors involved in DNS and IP market to update WHOIS information

Europol Unclassified - Basic Protection level

Europol Unclassified - Europol Public Information