EUROPOL

EC3 European Cybercrime Centre

@EC3Europol

CARRIER GRADE NAT (CGN)

AND CRIME ATTRIBUTION ONLINE

RIPE 74
BUDAPEST, HUNGARY
8 – 12 May 2017

Gregory Mounier
EUROPOL - EC3

Europol Unclassified - Basic Protection level

CGN and online crime attribution – LEA perspective

1. CGN / LSNAT : the law enforcement perspective
   - Problem of attribution
   - Scale of the problem
   - Case examples

2. Possible short-term and long term solutions

3. European Network of Law Enforcement Specialists on CGN

4. <u>Discussion</u>: How can RIPE community help?

Investigating crime online: traces on the Internet

- First traces at the start of investigations
  - E-mail (headers)
  - Connection to websites / Posts on social media platforms
  - Chat nicknames / channel names
  - Log files on attacked computer systems
- Further steps: requests for information
  - Internet Content Providers (hosters, webmail servers) => IPv4 + time
  - Internet Access Providers (access to Internet): identification / localization
- Start of traditional investigation methods
  - Interrogations / house searches

IPv4 - IPv6 transition

- **End-to-end principle of Internet**
  - – One unique IP address per connected device
  - – Until 2011 IPv4 identification was OK

- **IPv4 exhaustion – transition to IPv6**
  - – As of 2011 Pool of IPv4 (4.3 billion) started to deplete
  - – IPv4 exhausted in 4 regions and Africa in 2018
  - – Mobile/GSM providers – explosive growth – more address needed
  - – IoT – 20 billions by 2020

- **IPv6 adoption is not fast enough**
  - – IPv6 (3.4 x 10^{38} = 340 trillion trillion trillion)
  - – IPv6 adoption worldwide ~ 16% worldwide.
  - – In Europe: Belgium: 49%, SP, LT, LV, IT < 1%

EUROPOL EC3 European Cybercrime Centre

Interim work-around: CGN

Carrier grade NAT (Network Address Translation)

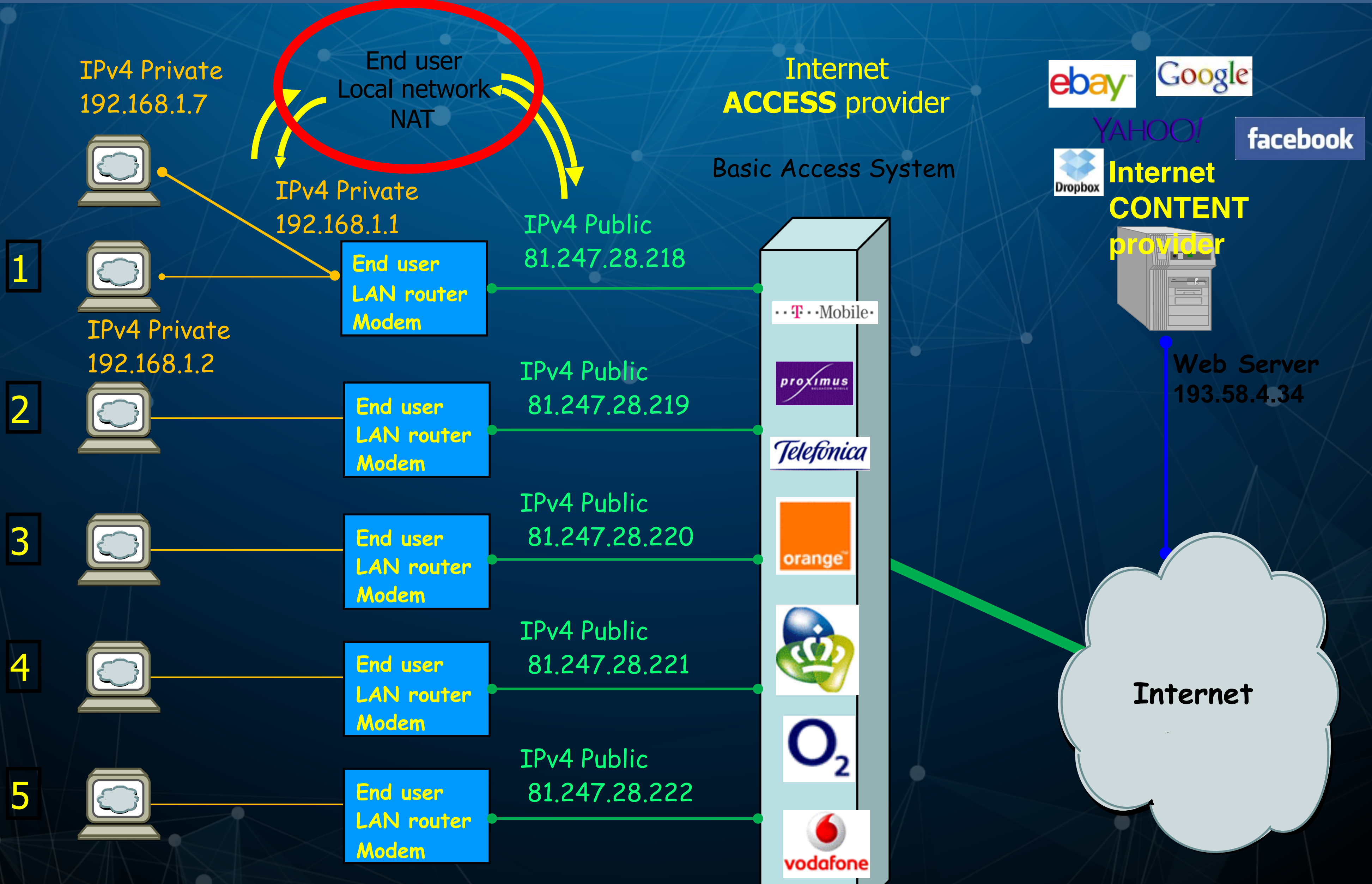
- <u>CGN concept:</u>
  - Old technology (LAN and private network)
  - 1 IPv4 address is shared simultaneously by multiple subscribers/end-users
  - Only difference btw subscribers : **source port number**
  - In the absence of source port = IP address cannot be traced back to subscriber.
- <u>Interim solution</u> to address shortage of IPv4
- Millions of $ invested in CGN technologies each year Could be invested in IPv6 transition
- Path dependency / irrational behaviour / no-exit strategy / tragedy of the commons?

IPv4 Life Support

CGN
Chattanooga Times Free Press Bennett

Courtesy
©Jan Zorz

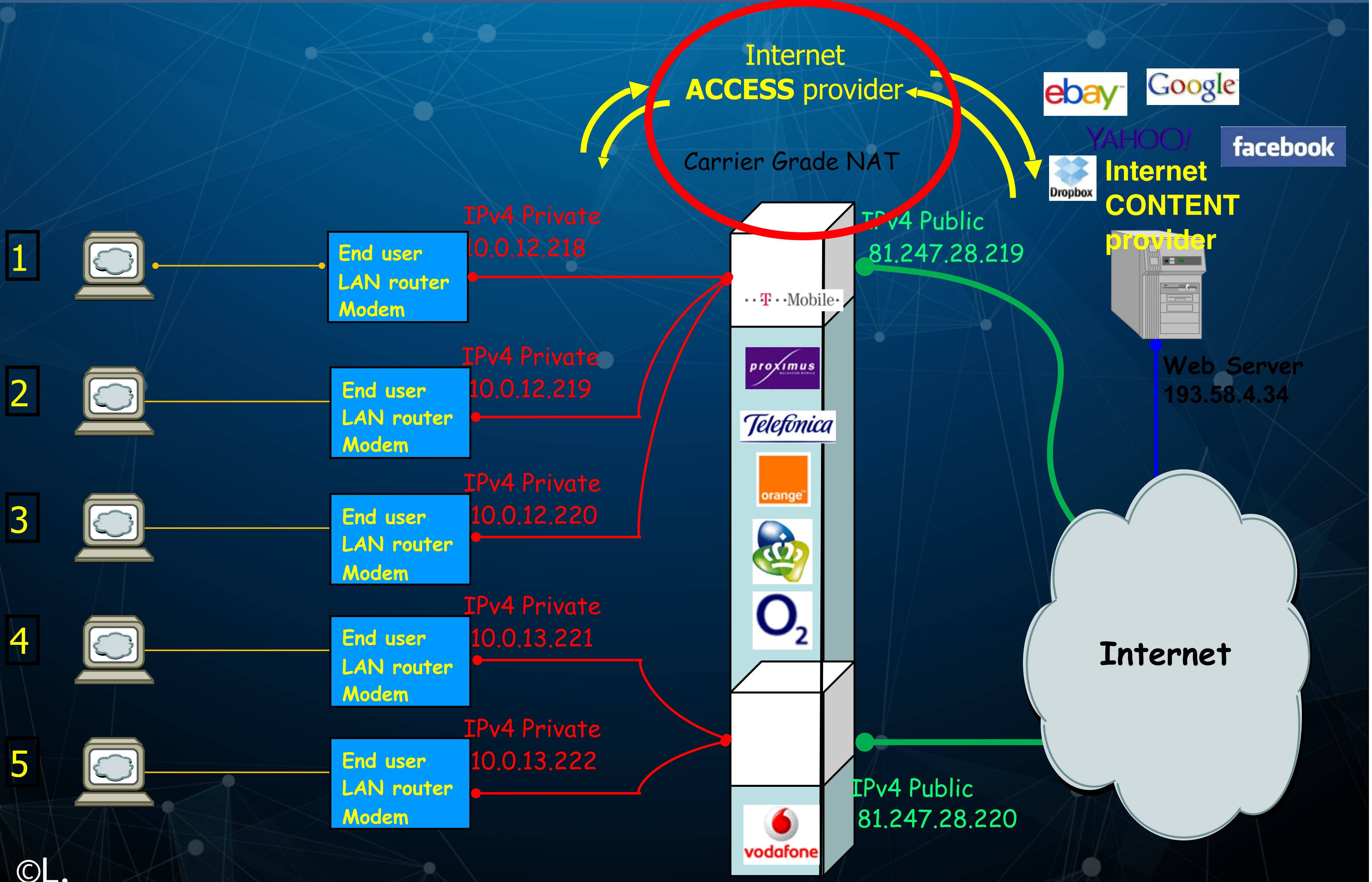
IPv4-address attribution without CGN



©L. Beirens

EUROPOL EC3 European Cybercrime Centre

IPv4-address attribution with CGN



©L. Beirens

EUROPOL
EC3 European Cybercrime Centre

Impact on law enforcement

NO ATTRIBUTION

- No ability to trace back an IP address to an individual subscriber.
- Need to determine which one of the hundreds/thousands of subscribers associated with a public IP address is the suspect.

Non-compliance with existing legislations

- Most EU MS have legislation requiring Electronic Service Providers to **identify end-user subscriber information** when served with legal order

  UK – Part 3 Counter Terrorism and Security Act 2015 + DRIPA 2014

  FR – art.6 Loi du 21 juin 2004 paragraph II

- **Budapest convention: art. 18.3 – Production Order**

  “Each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (…) any information (…) held by a service provider (…) ***which can establish the subscriber’s identity****”*

Scale of the problem

EC3 survey – August 2016

- All EU MS LEA/judiciary are affected
- In some countries : 50% of investigations = Mobile IP involved and 90% of these cases Mobile IP is behind an CGN
- Majority of IAPs are unable to provide subscriber information when served with a legal order and an IP address
- Criminal investigations are dropped or delayed

Academic research 2016: CGN use by IAPs:

- **95%** of GSM providers (mobile network operators)
- **50%** (32% + 12%) of traditional Fixed Line Internet Access Providers (cable, fibre and ADSL)

A Multi-perspective Analysis of Carrier-Grade NAT Deployment¸ ACM IMC 2016

http://www.icir.org/christian/publications/2016-imc-cgnat.pdf

Short-term solution to identify subscribers?

Internet Engineering Task Force (IETF) RFC 6302 - June 2011

https://tools.ietf.org/html/rfc6302

IETF recommends that Internet-facing servers (service providers) logging **incoming IP addresses** also log:

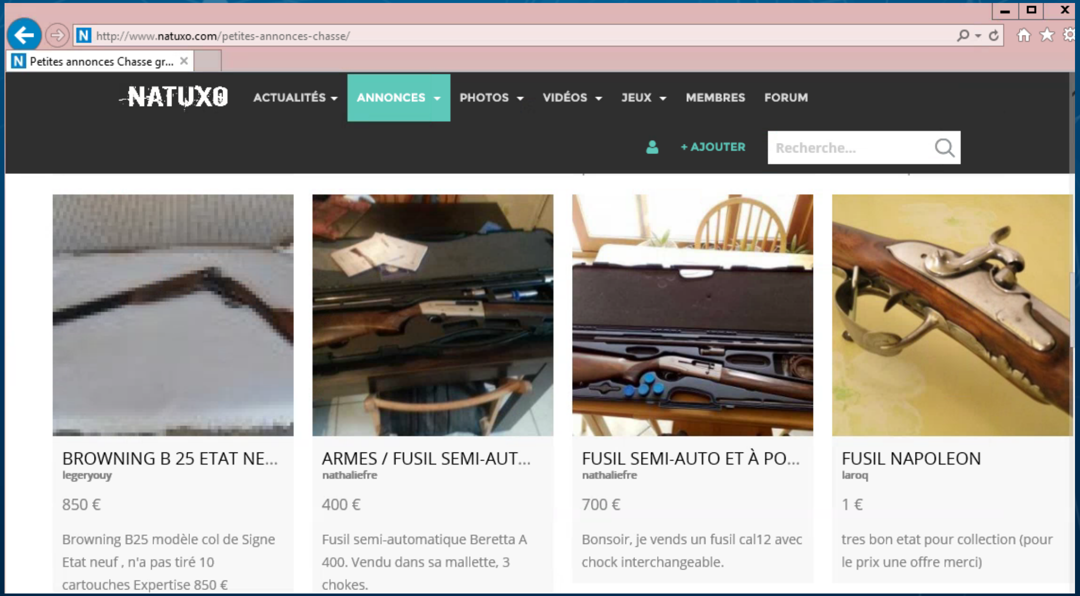
- **Source port number**
- Timestamp (exact time of the connection)
- Transport protocol

To identify unique subscriber behind a CGN, LEA/Judiciary should provide Access Providers:

- **IPv4 address**
- **Time stamp**
- **Source port number**

CASE EXAMPLE (1)

Prohibited assault rifle sold on www.natuxo.com


http://www.natuxo.com/petites-annonces-chasse/
Petites annonces Chasse gr...
NATUXO
ACTUALITÉS
ANNONCES
PHOTOS
VIDÉOS
JEUX
MEMBRES
FORUM
+ AJOUTER
Recherche...

BROWNING B 25 ETAT NE...
legeryouy
850 €
Browning B25 modèle col de Signe Etat neuf , n'a pas tiré 10 cartouches Expertise 850 €

ARMES / FUSIL SEMI-AUT...
nathaliefre
400 €
Fusil semi-automatique Beretta A 400. Vendu dans sa mallette, 3 chokes.

FUSIL SEMI-AUTO ET À PO...
nathaliefre
700 €
Bonsoir, je vends un fusil cal12 avec chock interchangeable.

FUSIL NAPOLEON
laroq
1 €
tres bon etat pour collection (pour le prix une offre merci)

- AK 47 assault riffle sold on www.natuxo.com FR-speaking ad website for hunting gears.
- IP logs => Mobile IP Swiss Mobile provider
- SIENA request to Swiss authorities
- CH => Cannot identify subscriber because No source port number.
- Case is closed.

CASE EXAMPLE (2)

Distribution of Child Abuse Material (CAM) - 2016 -FR

- CAM stored on a cloud storage service
- Investigators request and receive logs of connection (IP + timestamp) from hosting company.
- But <u>no source port</u>.
- Investigators provide IP + timestamp to IAP and ask identification of unique subscriber = **50 individuals** using the same IP address.
- Every 50 individuals were investigated.
- **<u>Case delayed by several months + privacy of 49 innocent violated</u>**

CASE EXAMPLE (3)

Counter Terrorism investigation: individuals supporting ISIS from Europe - 2015 - DE

- Public Prosecutor need to identify active and inactive members of a chat forum suspected of providing support to ISIS
- Request log files to hosting provider => different IP addresses logged but no source ports
- IAP cannot identify unique subscribers because CGN and no source port
- Criminal prosecution of suspected users not possible.
- Public Prosecutor unable to pursue this line of enquiry.

CASE EXAMPLE (4)

Large scale tax reclaim fraud - UK

- HMRC are investigating large scale fraud perpetrated through abuse of their online portal for tax reclaims.
- Fraudsters have performed bulk claims for overpaid tax, costing the British tax payer significant sums.
- HMRC identifies IP addresses involved in the attacks.
- However these are mobile IP addresses (GSM therefore 95% behind CGN) = Leads are frustrated from the outset.
- Inability to resolve IPs back to a suspect, thereby closing the line of enquiry to identify those responsible.

Alternative solution?
Belgian model – Voluntary Code of Conduct

WHEN? - 2012

WHO?

- Belgium Federal Police + Telecom regulator BIPT-IBPT + Council of Prosecutors-general + Ministry Economical affairs
- BE IAP association + 4 big BE IAPs

WHAT ?

- CGN Code of Conduct: 2 page informal code:
  - a) Voluntary restrict number of users behind IPv4 : max 16.
  - b) Voluntary limit the use of CGN
  - c) Start adopting IPv6 asap

Belgian model – voluntary Code of Conduct

Goals

- Guarantee the identification of subscribers when timestamp + IP + source port available.
- Reduce risk of “no unique identification” if IP+ timestamp available but NOT the source port
- Create conditions allowing LEA to make cross-check analysis of different responses in case LEA can find several IPs + timestamps for the suspect

EUROPOL EC3 European Cybercrime Centre

Belgian model – voluntary Code of Conduct

Conclusions:

- In 2017 most Belgium-based network operators respect **16 max user limit**
- 1 fixed BE IAP implemented even a lower limit : 8 users
- Average users per mobile IP received by BE police : on average 4
- Biggest IAPs are quickly moving towards IPv6 because no financial interest to invest in CGN anymore.
- In 2017 BE = highest IPv6 adoption rate in the world = 49%.
- In comparison: UK, FR=14%, SP, LT, LV, IT < 1%

POSSIBLE POLICY SOLUTIONS

1. Long-term: Increase IPv6 adoption by IAPs and ICPs

- Trillions of IPv6 addresses available = **No need for CGN**
- European-wide IPv6 promotion campaign – financial incentives – European Digital Single Market?

2. Short-term: European Internet Access Providers:

- Voluntary Code of Conduct with main European IAPs?
  a) Voluntary restrict number of users behind IPv4
  b) Voluntary limit the use of CGN
- Previous experience: EU Internet Forum - Voluntary Code of Conduct Commission - GAFAs for to remove illegal hate speech – May 2016.

- **Aim:**
  - Reduce risk of “crime non-attribution”
  - Gradually reduce and limit the use of CGN
  - Create favourable market conditions for IPv6 investments

European Network of LEA specialists on CGN

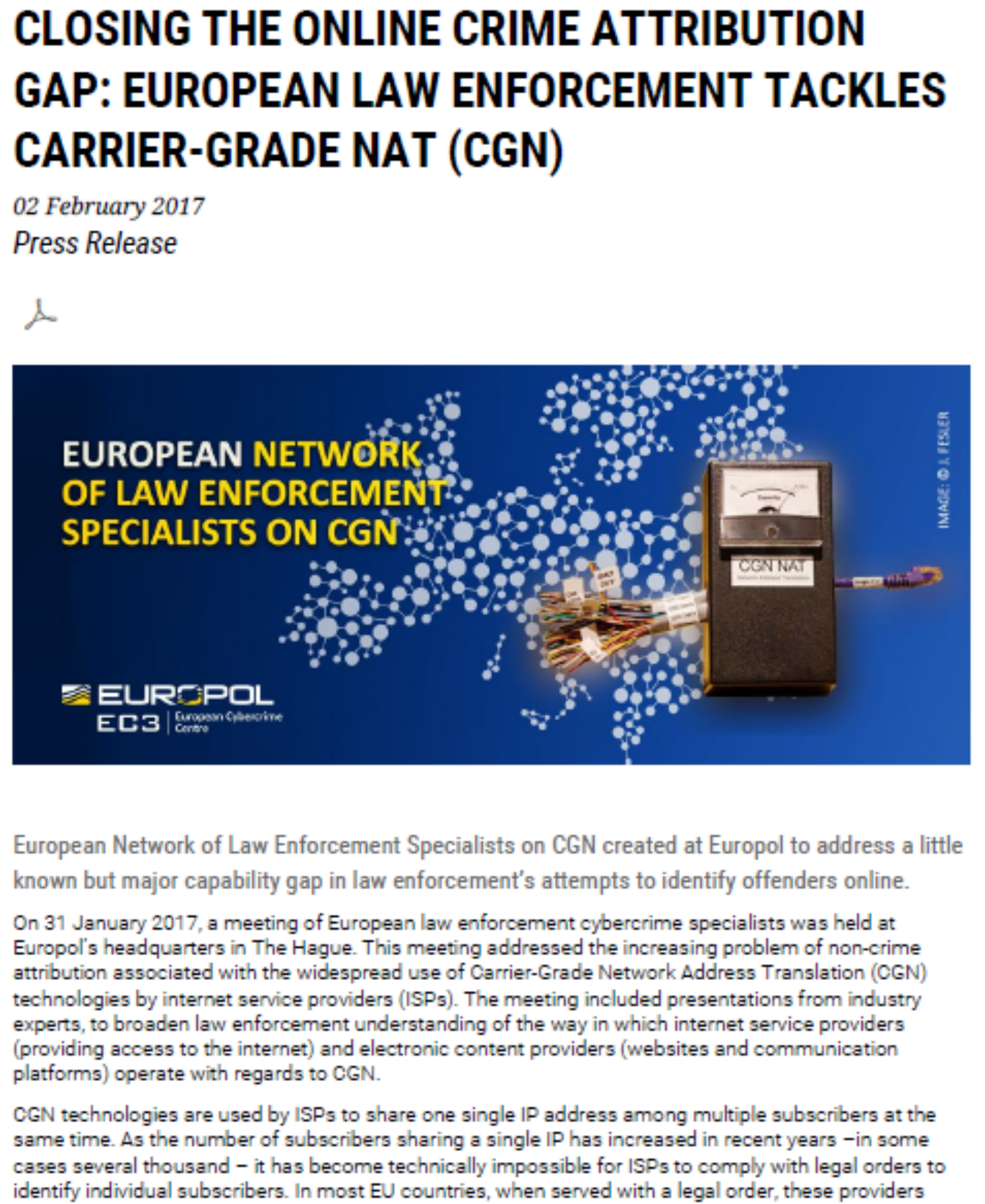
EUROPEAN NETWORK OF LAW ENFORCEMENT SPECIALISTS ON CGN
EUROPOL
EC3 European Cybercrime Centre
CGN NAT
Network Address Translation
Capacity
BAD GUY
1000 Users
Single IPv4
IMAGE: © J. FESLER

European Network of LEA specialists on CGN

Develop knowledge and expertise at EU level

- Document cases of non-attribution CGN + Repository of cases.
- Document best practices to overcome CGN-related attribution problems
- Engage with IAPs and policy-makers

European Network of LEA specialists on CGN



CLOSING THE ONLINE CRIME ATTRIBUTION GAP: EUROPEAN LAW ENFORCEMENT TACKLES CARRIER-GRADE NAT (CGN)

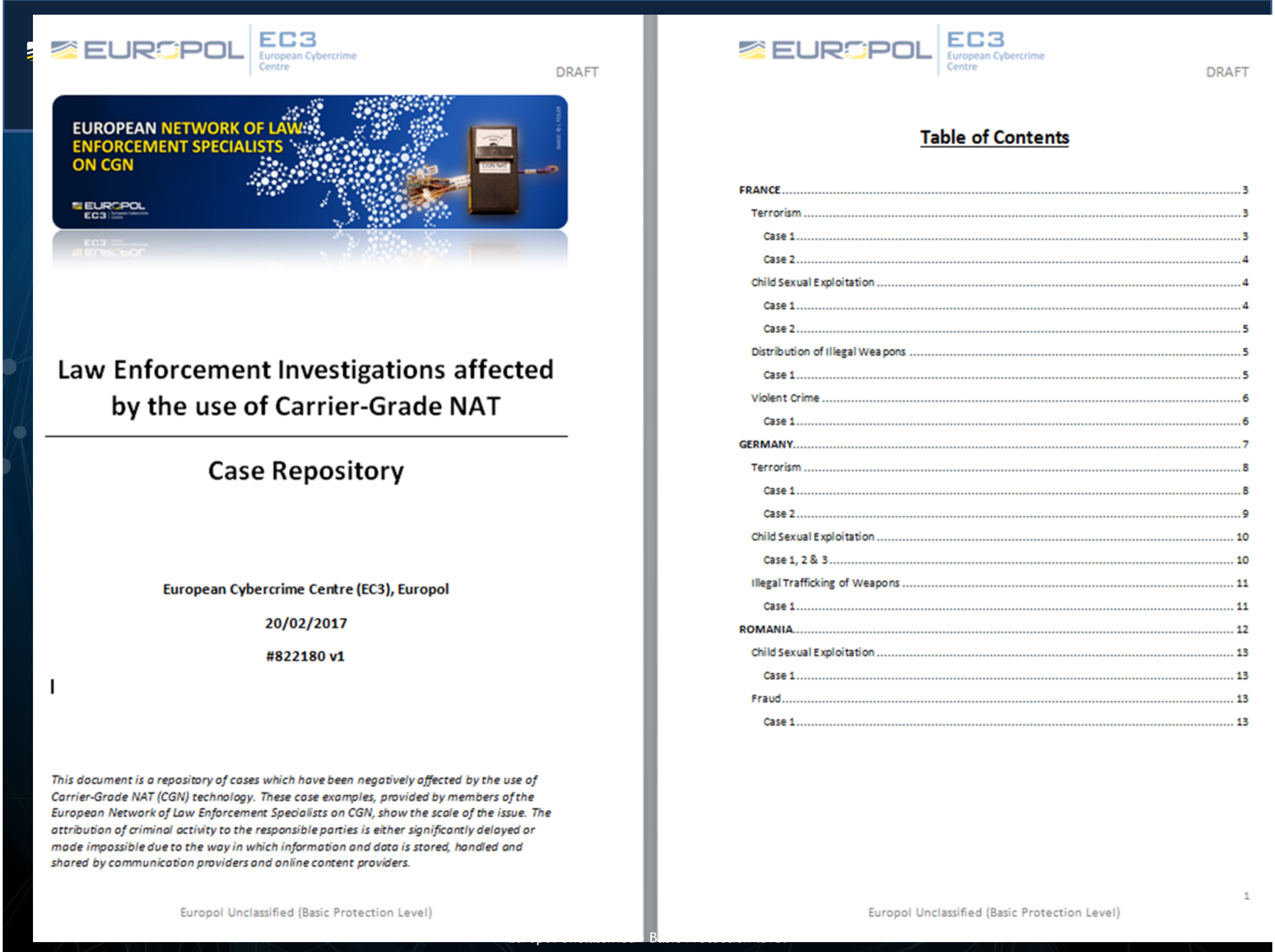
02 February 2017

Press Release

European Network of Law Enforcement Specialists on CGN created at Europol to address a little known but major capability gap in law enforcement's attempts to identify offenders online.

On 31 January 2017, a meeting of European law enforcement cybercrime specialists was held at Europol's headquarters in The Hague. This meeting addressed the increasing problem of non-crime attribution associated with the widespread use of Carrier-Grade Network Address Translation (CGN) technologies by internet service providers (ISPs). The meeting included presentations from industry experts, to broaden law enforcement understanding of the way in which internet service providers (providing access to the internet) and electronic content providers (websites and communication platforms) operate with regards to CGN.

CGN technologies are used by ISPs to share one single IP address among multiple subscribers at the same time. As the number of subscribers sharing a single IP has increased in recent years –in some cases several thousand – it has become technically impossible for ISPs to comply with legal orders to identify individual subscribers. In most EU countries, when served with a legal order, these providers



EUROPOL EC3 European Cybercrime Centre

DRAFT

EUROPEAN NETWORK OF LAW ENFORCEMENT SPECIALISTS ON CGN

Law Enforcement Investigations affected by the use of Carrier-Grade NAT

Case Repository

European Cybercrime Centre (EC3), Europol

20/02/2017

#822180 v1

This document is a repository of cases which have been negatively affected by the use of Carrier-Grade NAT (CGN) technology. These case examples, provided by members of the European Network of Law Enforcement Specialists on CGN, show the scale of the issue. The attribution of criminal activity to the responsible parties is either significantly delayed or made impossible due to the way in which information and data is stored, handled and shared by communication providers and online content providers.

Europol Unclassified (Basic Protection Level)

EUROPOL EC3 European Cybercrime Centre

DRAFT

Table of Contents

1

Europol Unclassified (Basic Protection Level)

Way forward?

- Europol and European Commission are looking at possible way forwards:
  - Coordinated EU dialogue with IAPs to gradually phase out/limit the use of CGN
  - Promote IPv6 adoption by BOTH IAPs and ICPs
- Discussion: How can RIPE community help?

Thank you!

gregory.mounier@europol.europa.eu