EUROPOL EC3 European Cybercrime Centre

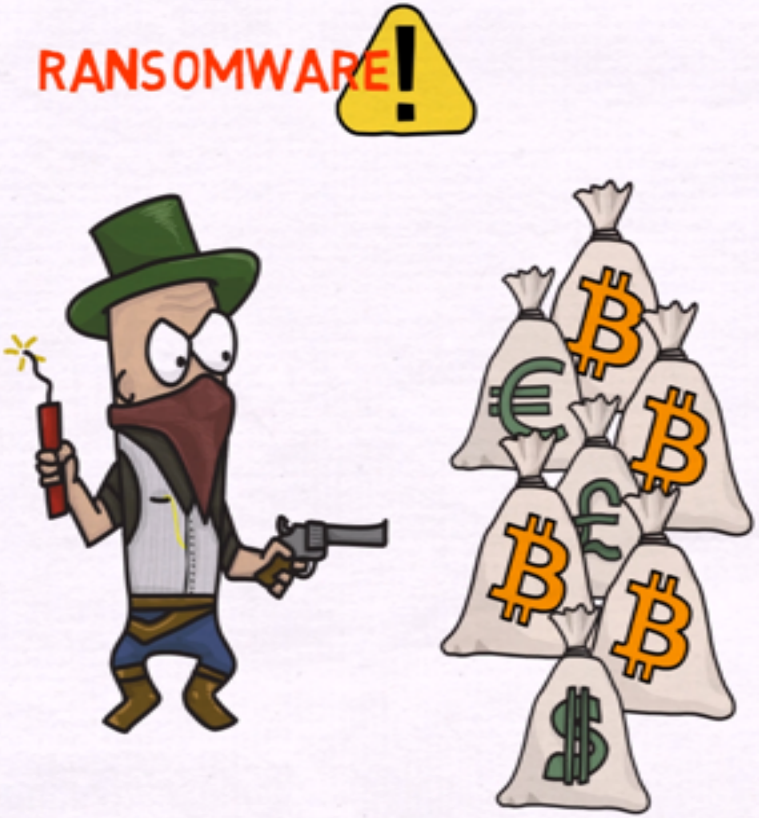
@EC3Europol

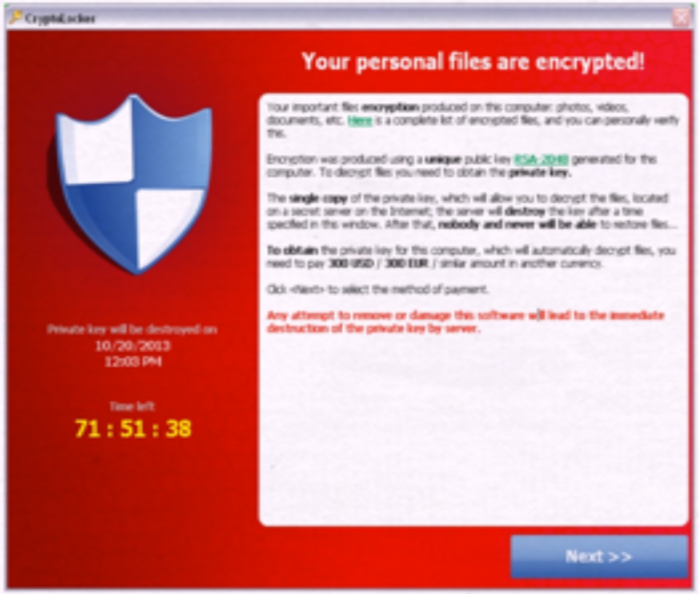
IP Resource Announcement
The Law enforcement perspective

Gregory Mounier
European Cybercrime Centre EC3
Outreach and Support

EUROPOL EC3 European Cybercrime Centre

A new crypto-ransomware is diffusing around Europe





Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

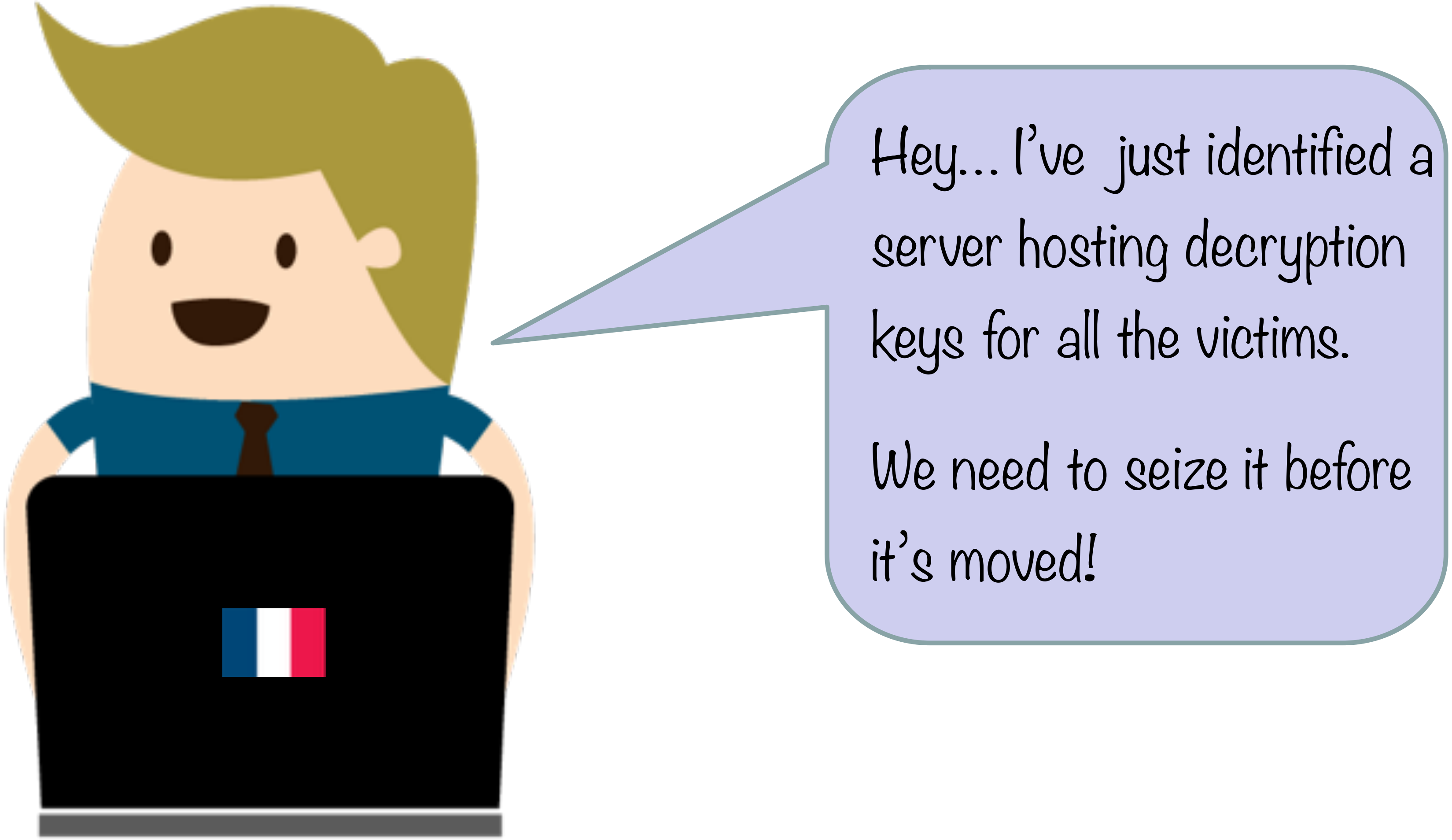
Click <Next> to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/20/2013
12:03 PM

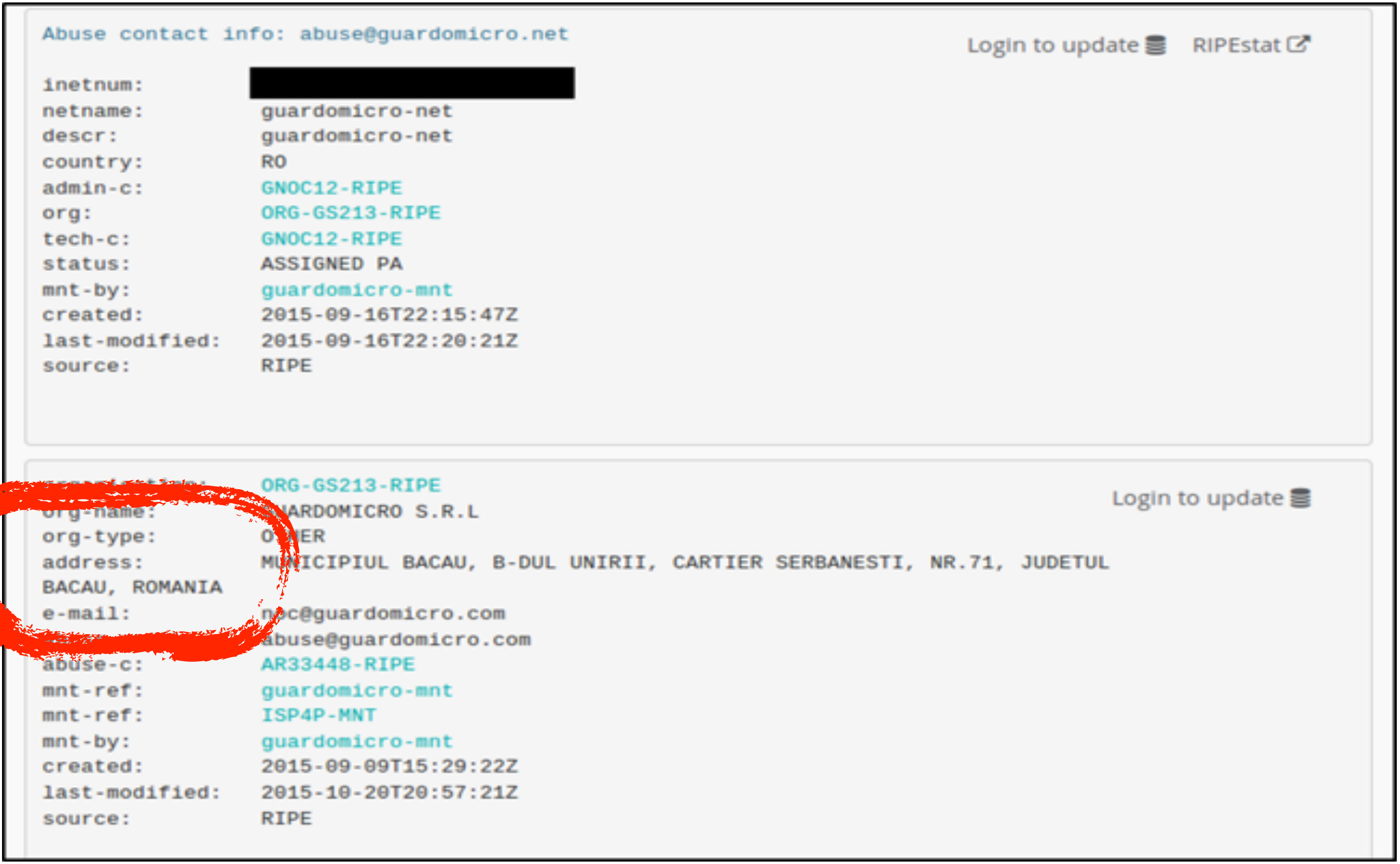
Time left
71 : 51 : 38

JEAN is a French Cyber Investigator working on the responsible botnet


Hey… I've just identified a server hosting decryption keys for all the victims.

We need to seize it before it's moved!

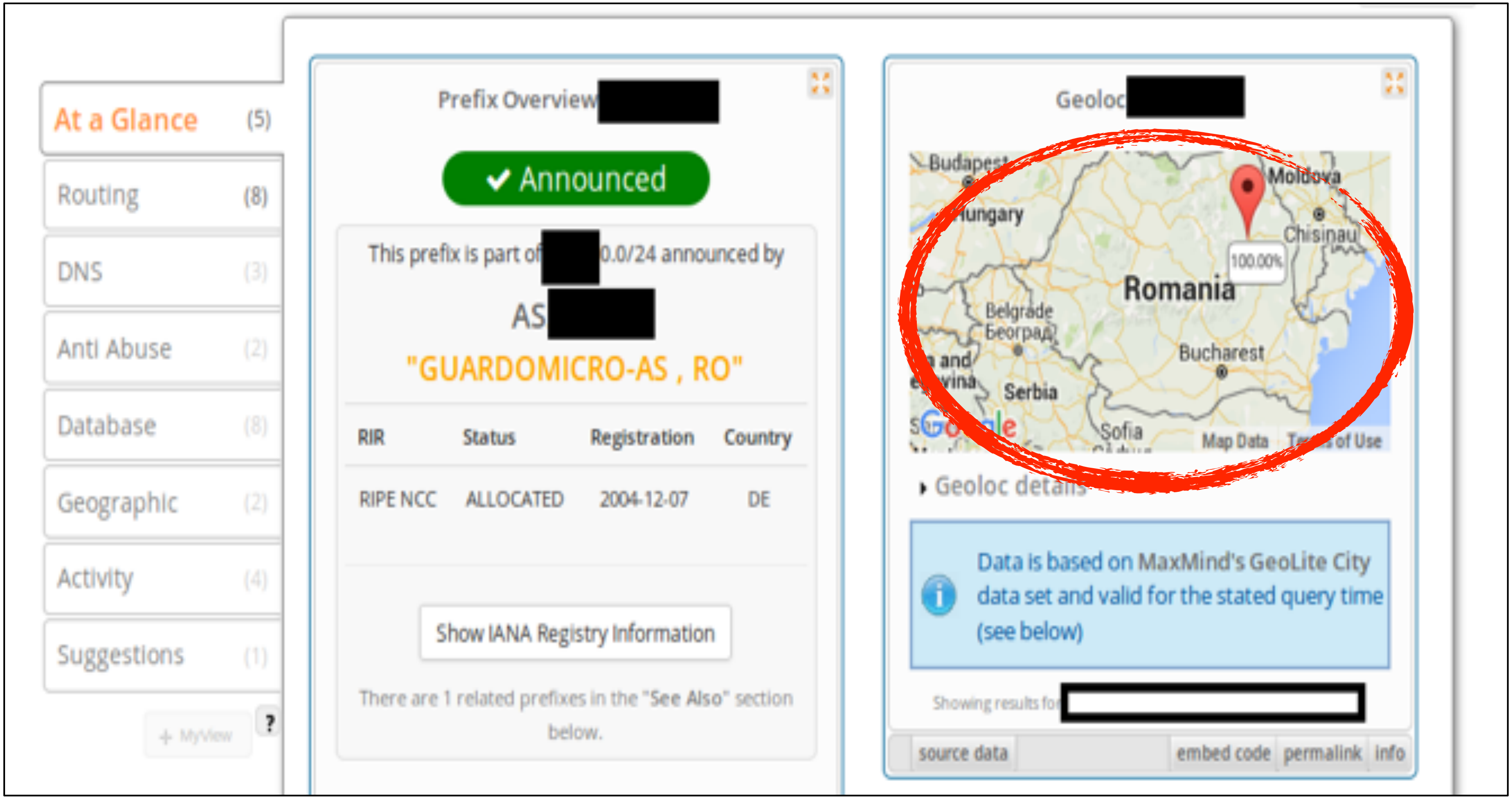
First Step: Let's check RIPE Whois Database…



```
Abuse contact info: abuse@guardomicro.net

inetnum:        [redacted]
netname:        guardomicro-net
descr:          guardomicro-net
country:        RO
admin-c:        GNOC12-RIPE
org:            ORG-GS213-RIPE
tech-c:         GNOC12-RIPE
status:         ASSIGNED PA
mnt-by:         guardomicro-mnt
created:        2015-09-16T22:15:47Z
last-modified:  2015-09-16T22:20:21Z
source:         RIPE
```

```
organisation:   ORG-GS213-RIPE
org-name:       GUARDOMICRO S.R.L
org-type:       OWNER
address:        MUNICIPIUL BACAU, B-DUL UNIRII, CARTIER SERBANESTI, NR.71, JUDETUL
BACAU, ROMANIA
e-mail:         noc@guardomicro.com
[illegible]     abuse@guardomicro.com
abuse-c:        AR33448-RIPE
mnt-ref:        guardomicro-mnt
mnt-ref:        ISP4P-MNT
mnt-by:         guardomicro-mnt
created:        2015-09-09T15:29:22Z
last-modified:  2015-10-20T20:57:21Z
source:         RIPE
```

Second step: Additional check on stat.ripe.net



Prefix Overview [redacted]

✓ Announced

This prefix is part of [redacted]0.0/24 announced by

AS [redacted]

"GUARDOMICRO-AS , RO"

RIR	Status	Registration	Country
RIPE NCC	ALLOCATED	2004-12-07	DE

Show IANA Registry Information

There are 1 related prefixes in the "See Also" section below.

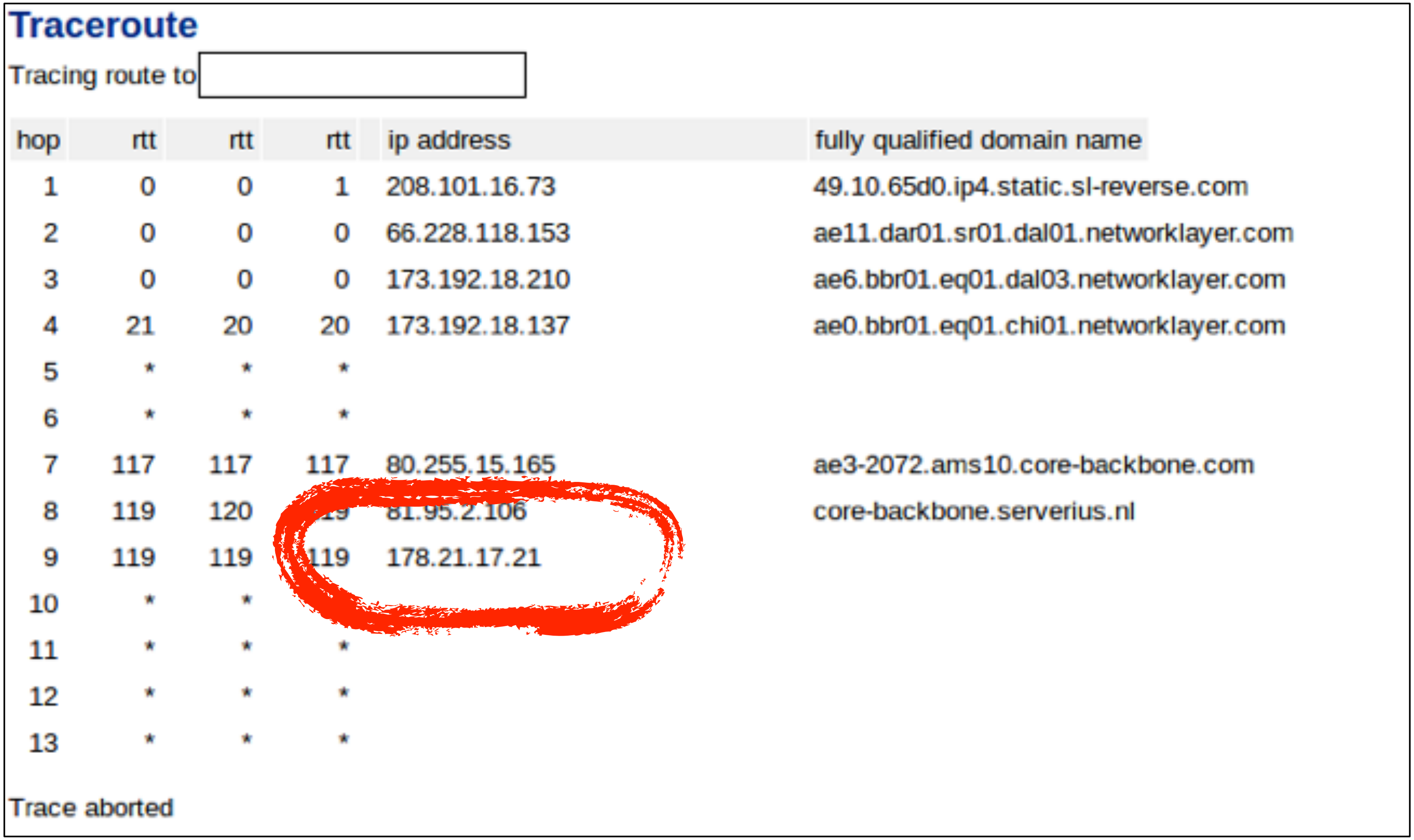
Geoloc [redacted]

▸ Geoloc details

Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for [redacted]

Third Step: Traceroute...



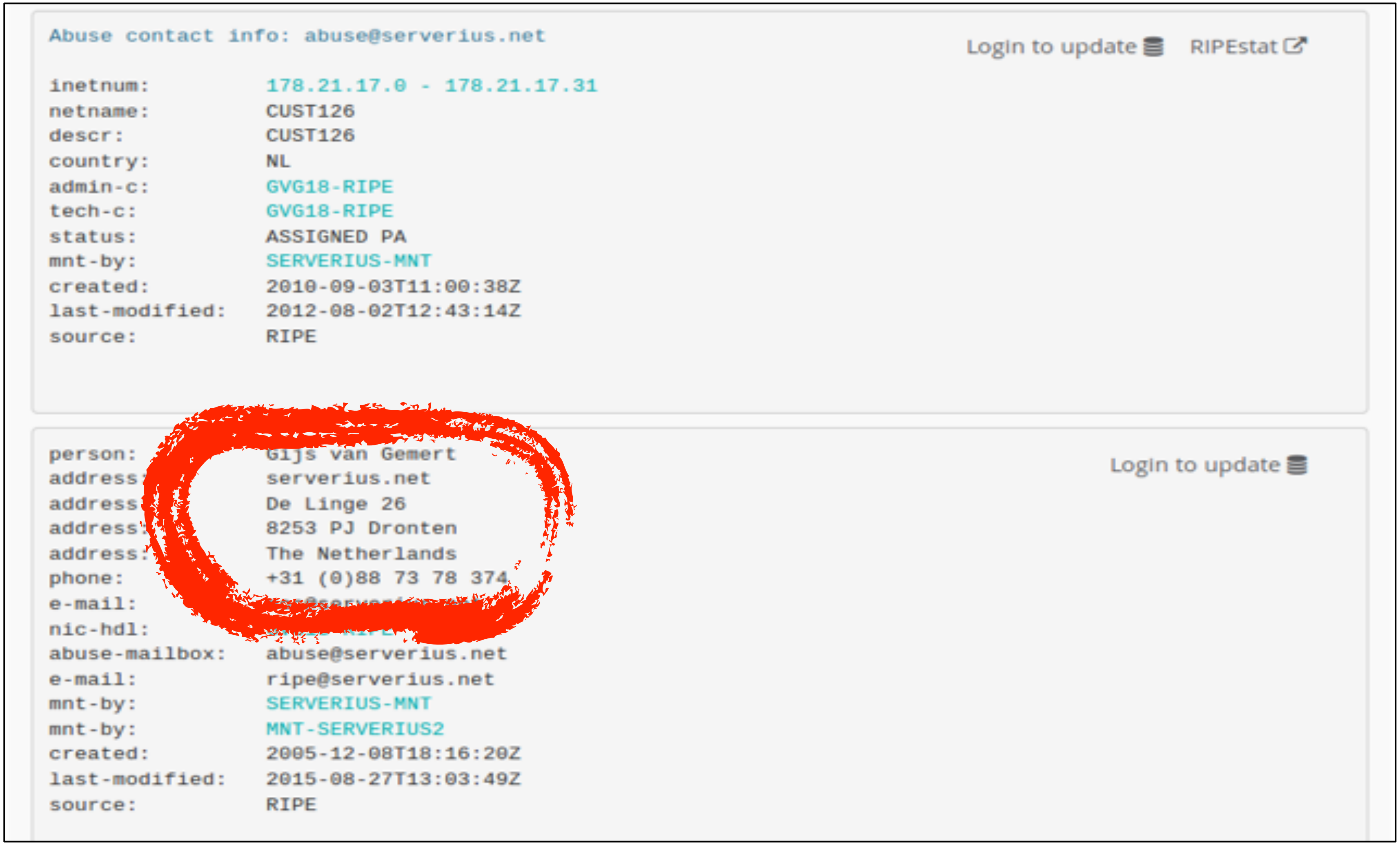
Traceroute

Tracing route to

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	0	0	1	208.101.16.73	49.10.65d0.ip4.static.sl-reverse.com
2	0	0	0	66.228.118.153	ae11.dar01.sr01.dal01.networklayer.com
3	0	0	0	173.192.18.210	ae6.bbr01.eq01.dal03.networklayer.com
4	21	20	20	173.192.18.137	ae0.bbr01.eq01.chi01.networklayer.com
5	*	*	*		
6	*	*	*		
7	117	117	117	80.255.15.165	ae3-2072.ams10.core-backbone.com
8	119	120	119	81.95.2.106	core-backbone.serverius.nl
9	119	119	119	178.21.17.21	
10	*	*			
11	*	*	*		
12	*	*	*		
13	*	*	*		

Trace aborted

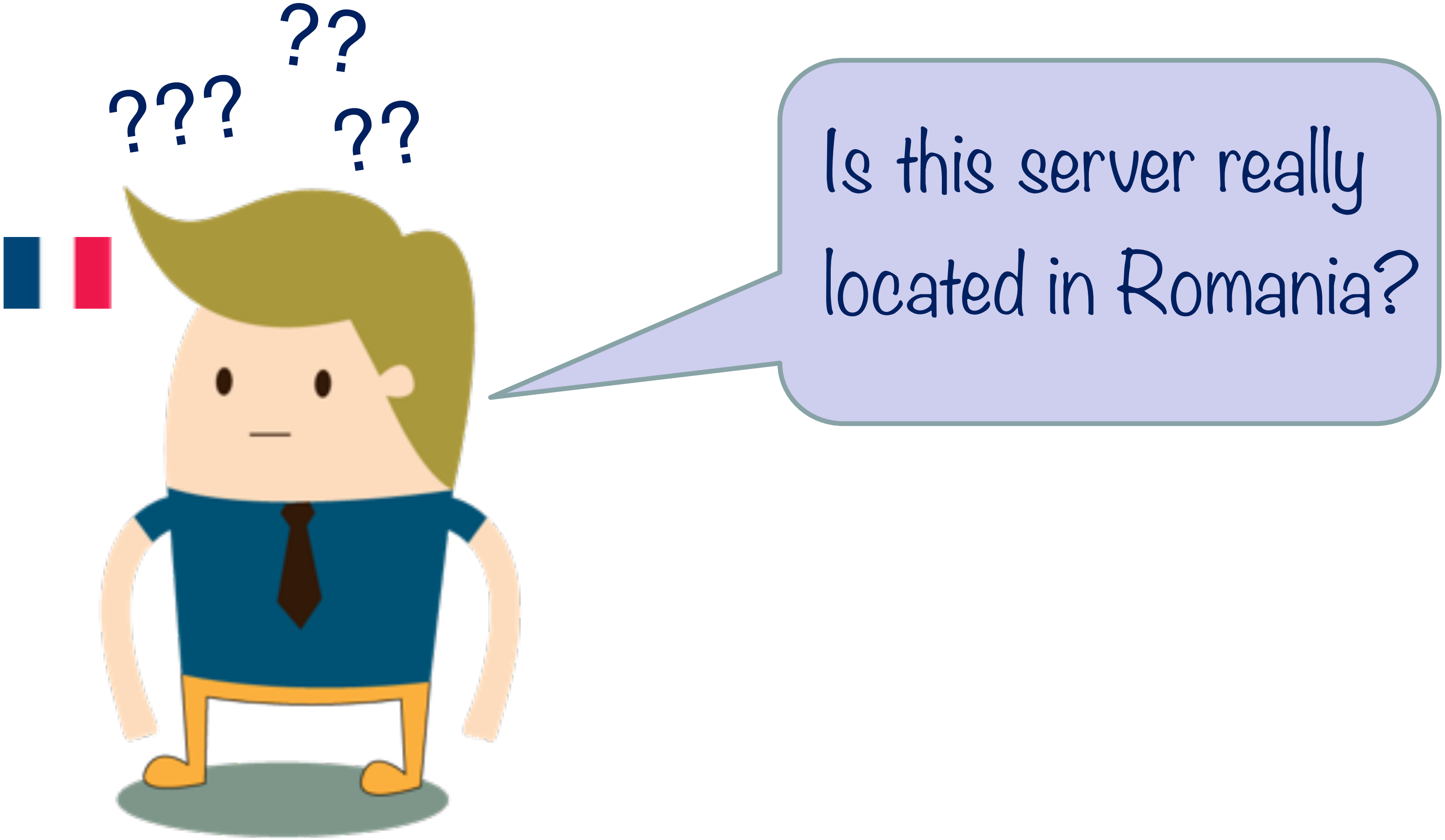
...but ends up in The Netherlands



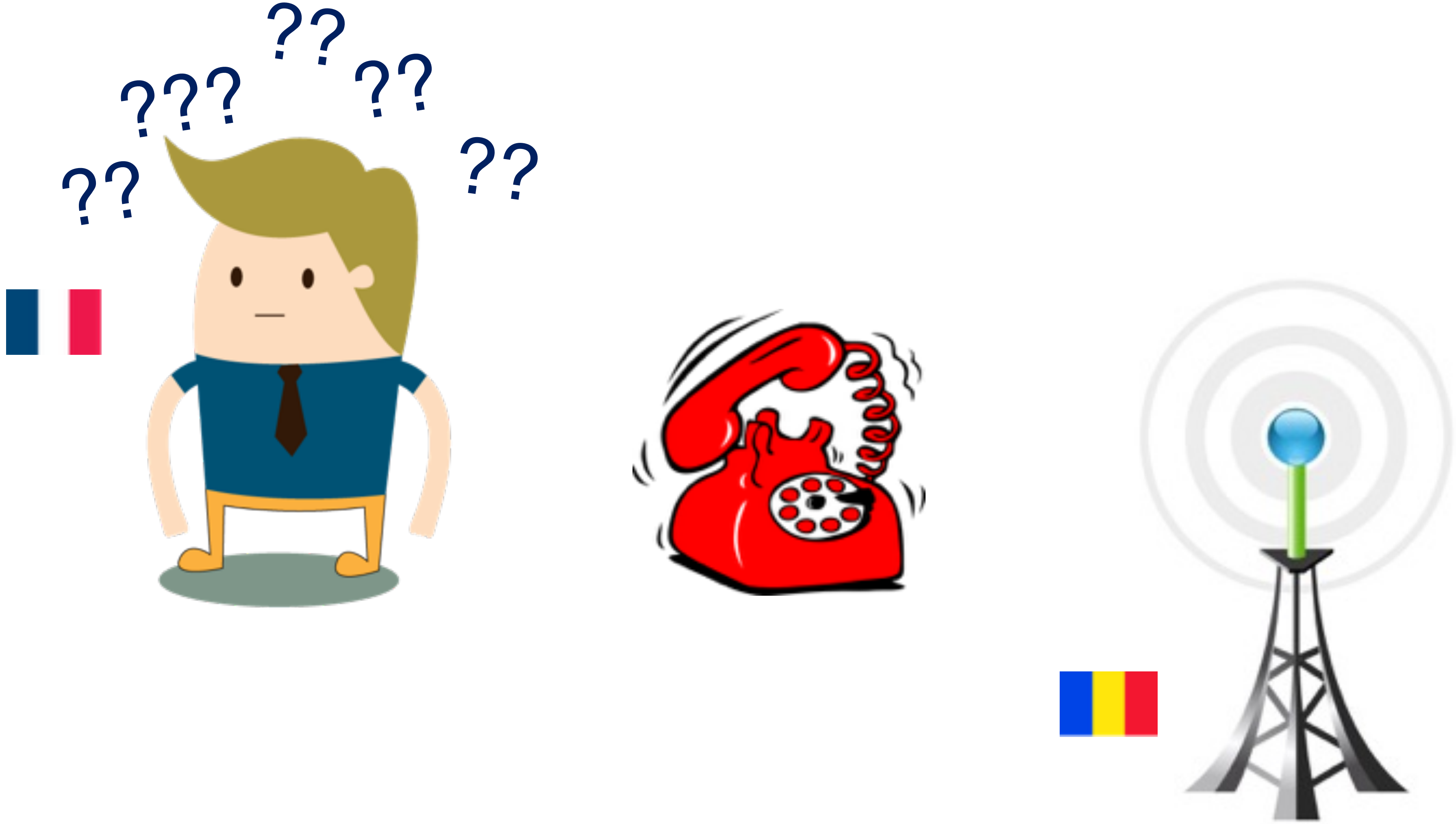
```
Abuse contact info: abuse@serverius.net                         Login to update   RIPEstat

inetnum:        178.21.17.0 - 178.21.17.31
netname:        CUST126
descr:          CUST126
country:        NL
admin-c:        GVG18-RIPE
tech-c:         GVG18-RIPE
status:         ASSIGNED PA
mnt-by:         SERVERIUS-MNT
created:        2010-09-03T11:00:38Z
last-modified:  2012-08-02T12:43:14Z
source:         RIPE
```

```
person:         Gijs van Gemert                                 Login to update
address:        serverius.net
address:        De Linge 26
address:        8253 PJ Dronten
address:        The Netherlands
phone:          +31 (0)88 73 78 374
e-mail:         [redacted]
nic-hdl:        [redacted]
abuse-mailbox:  abuse@serverius.net
e-mail:         ripe@serverius.net
mnt-by:         SERVERIUS-MNT
mnt-by:         MNT-SERVERIUS2
created:        2005-12-08T18:16:20Z
last-modified:  2015-08-27T13:03:49Z
source:         RIPE
```

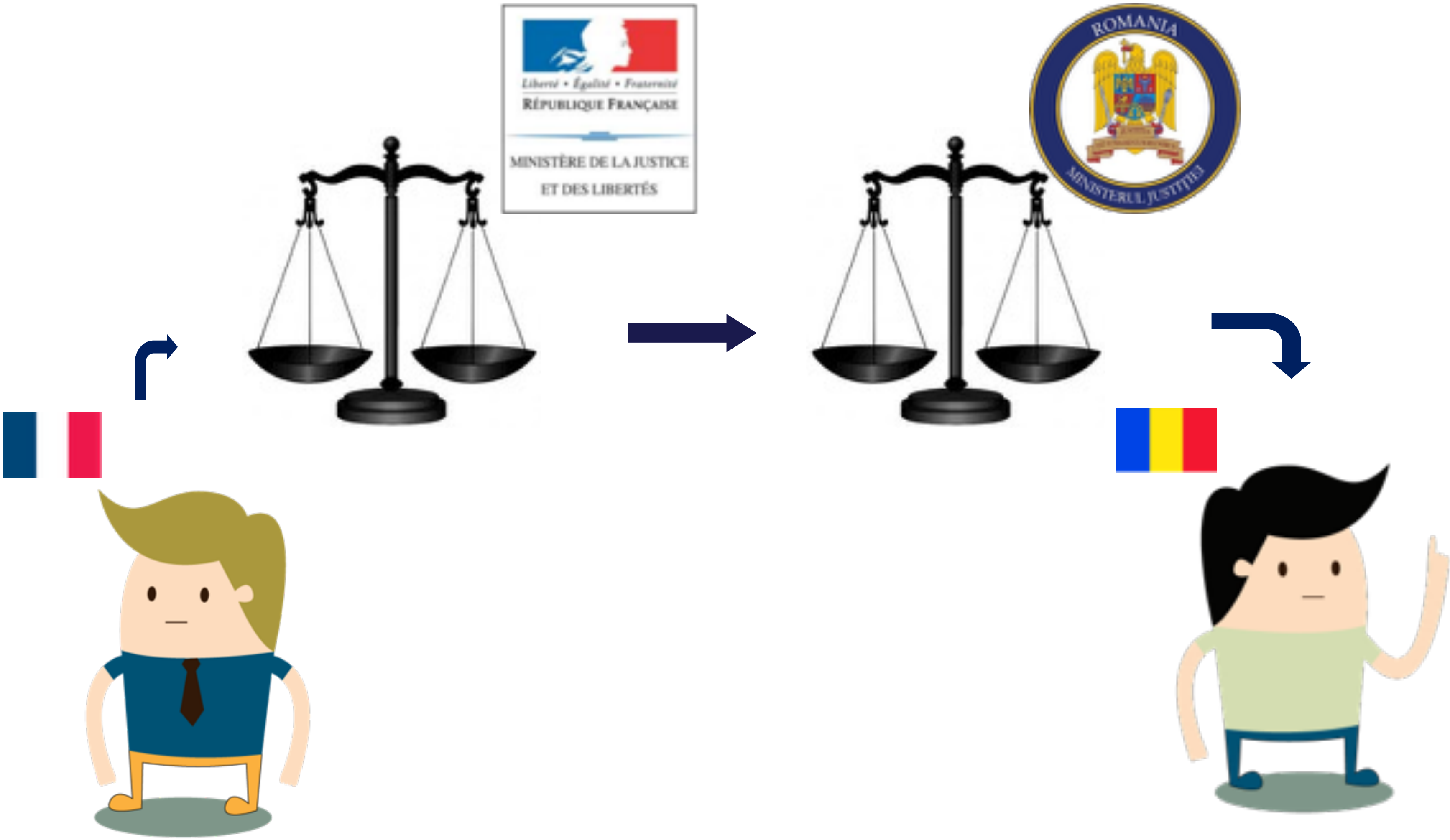
This is not very useful...



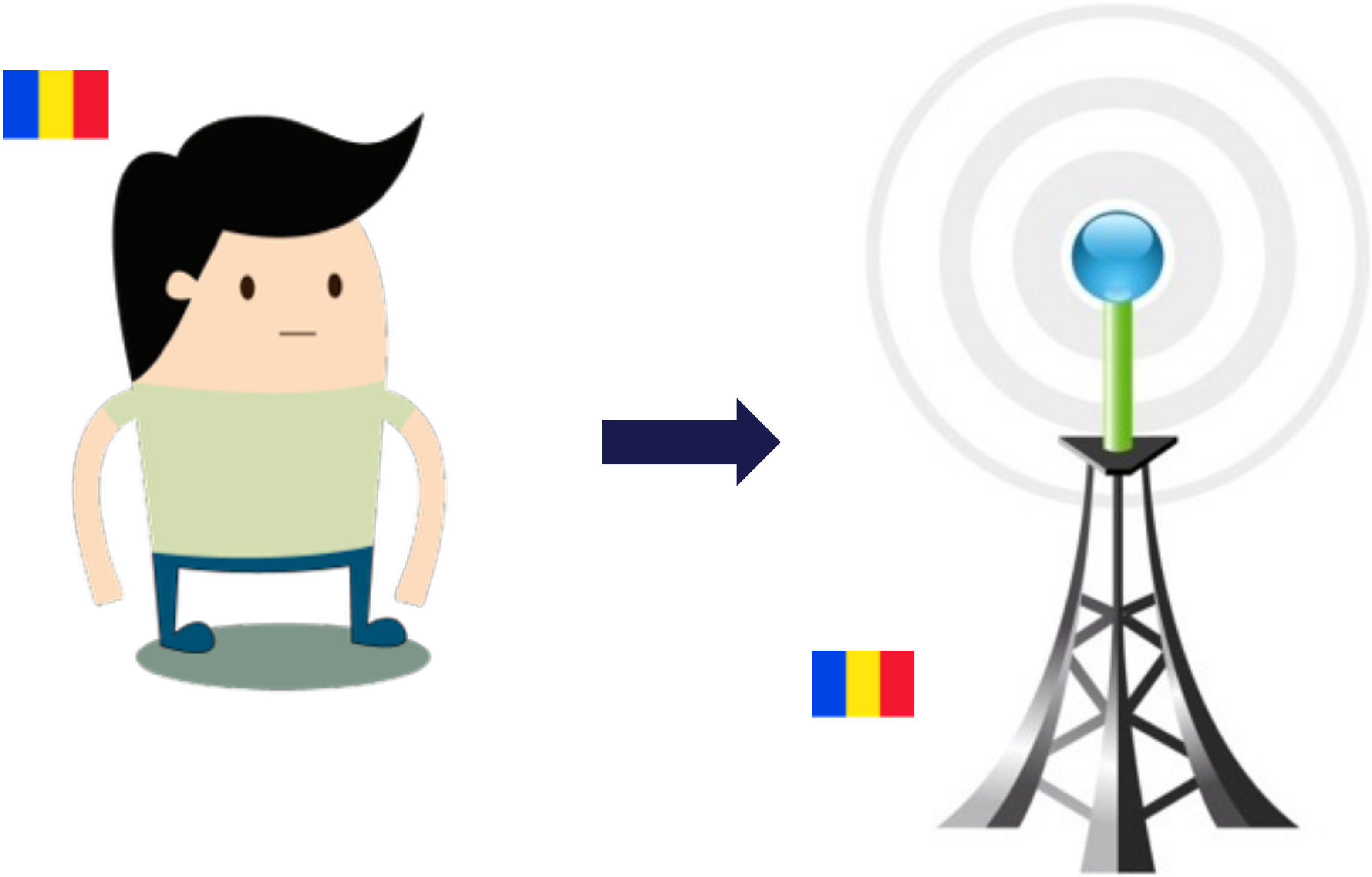
Jean **informally contact** the Romanian provider - No success



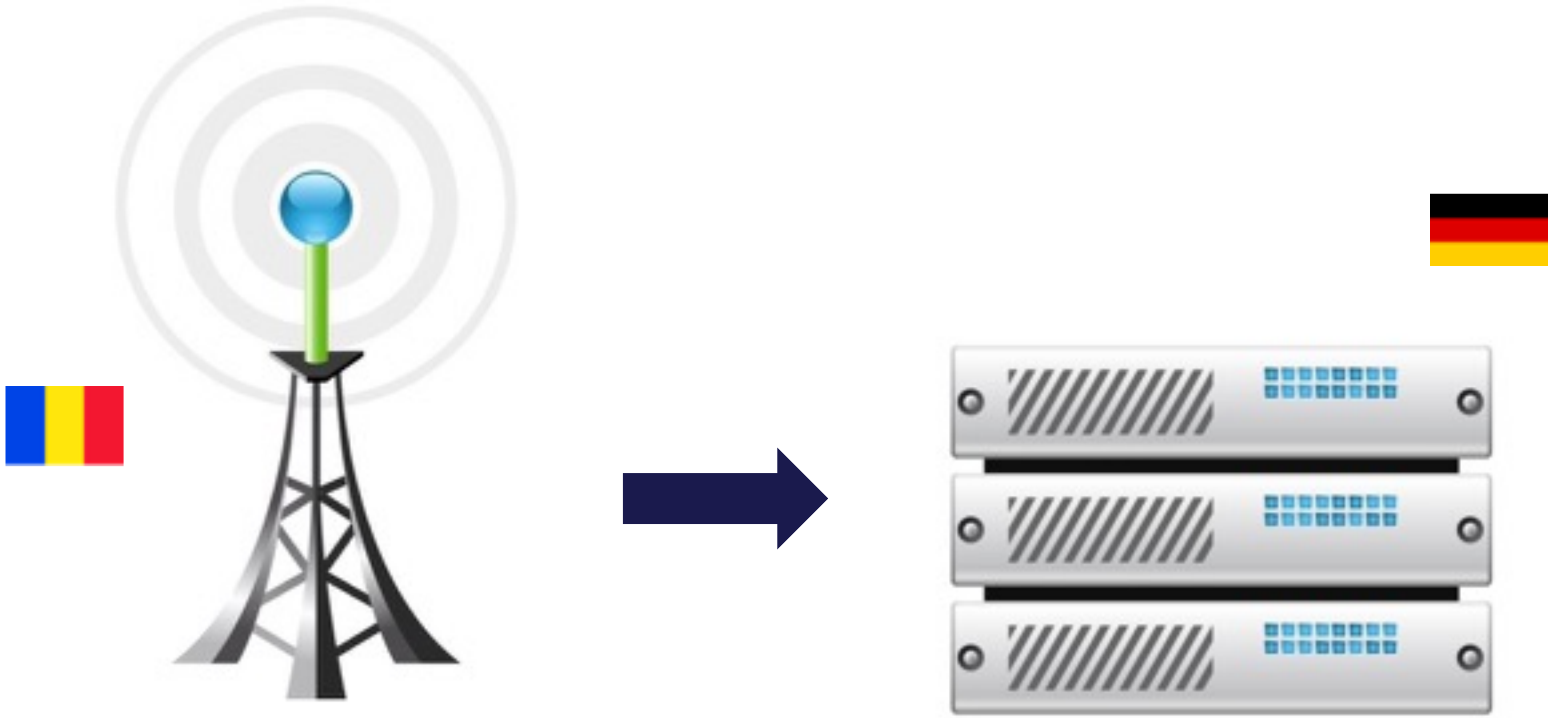
MLAT from France to Romania…


Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA JUSTICE ET DES LIBERTÉS
ROMANIA
MINISTERUL JUSTIŢIEI

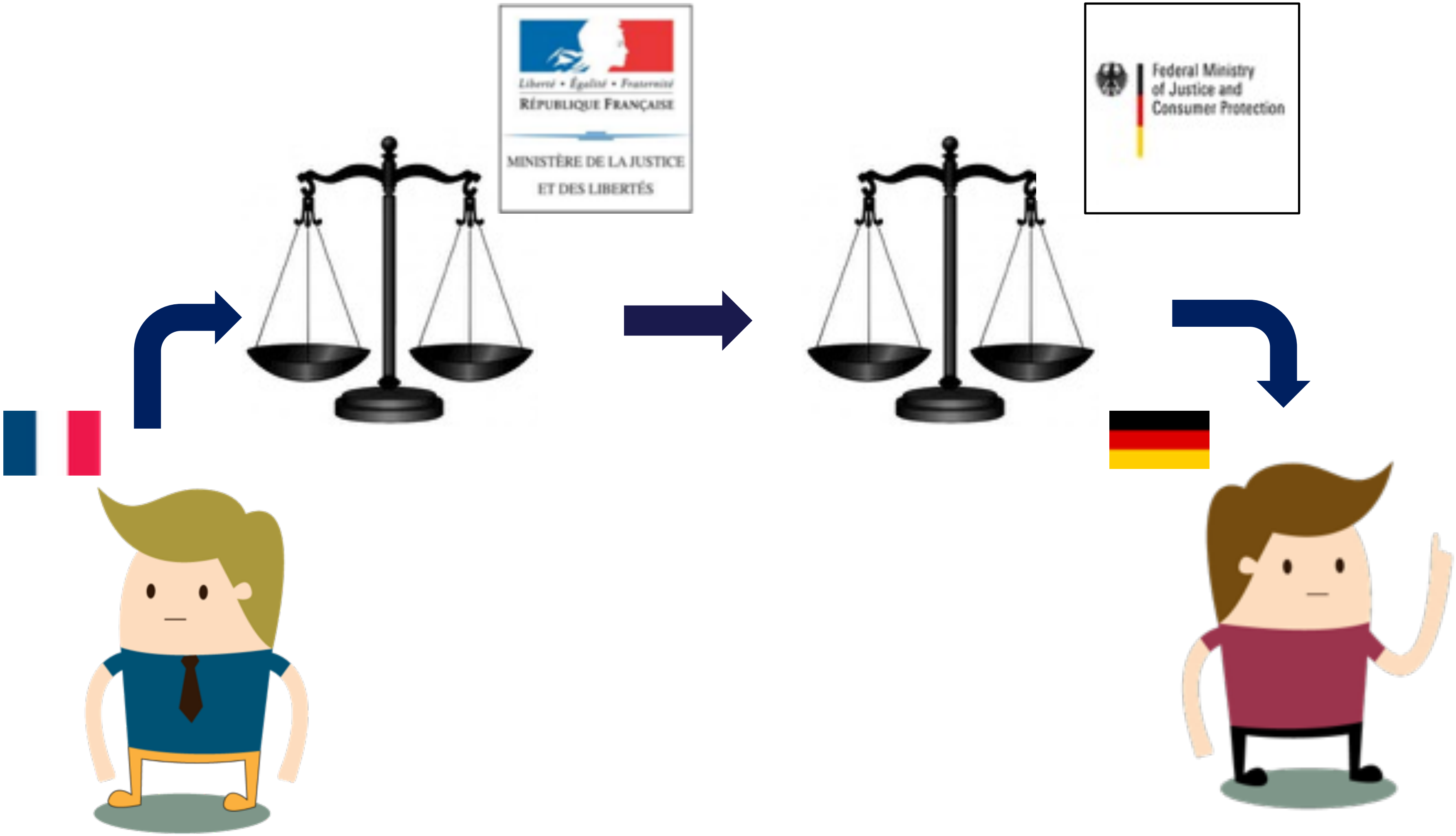
1 month later: Romanian LE goes to the indicated company



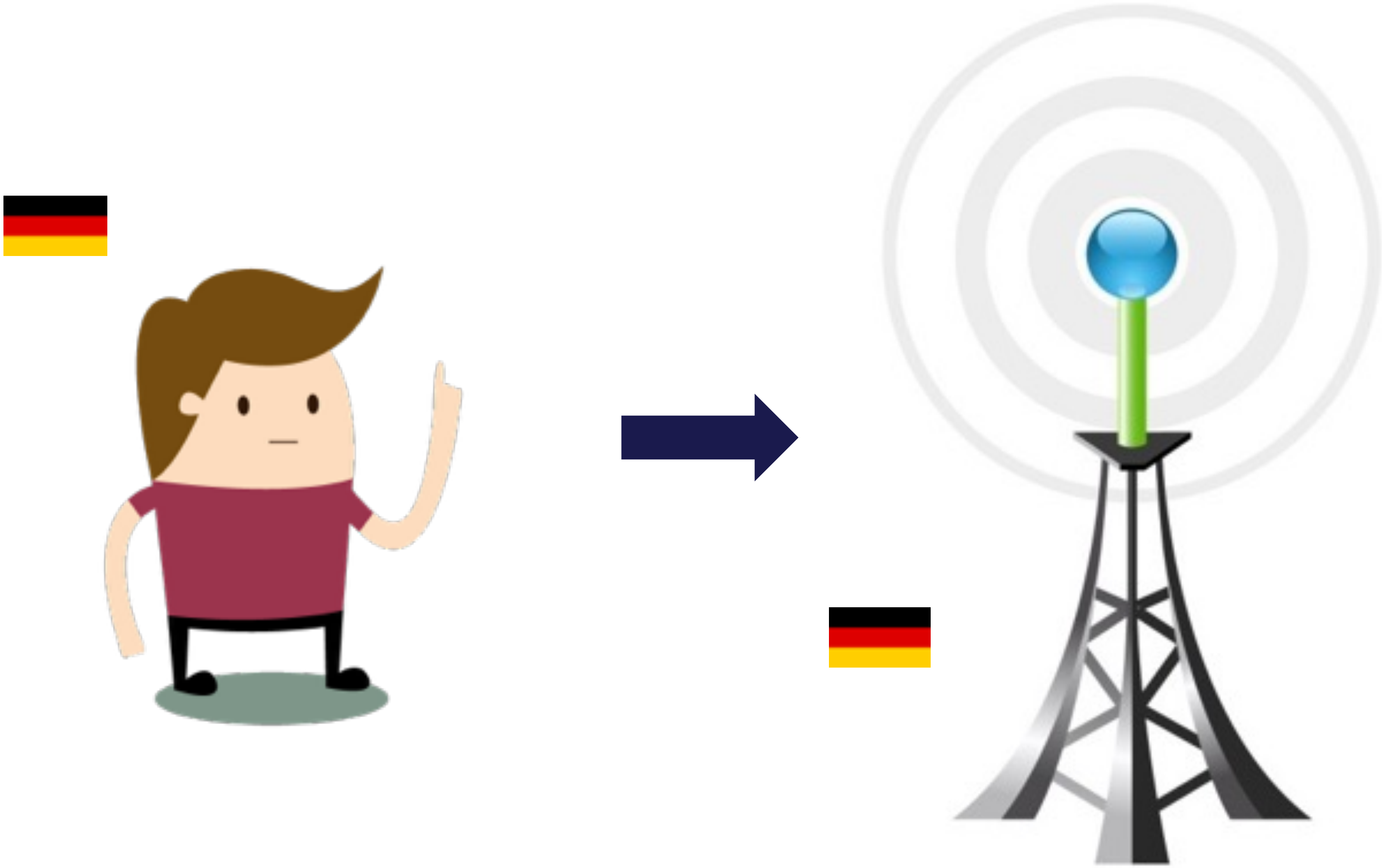
Scenario 1: Romanian company cooperate



Second MLAT from France to Germany

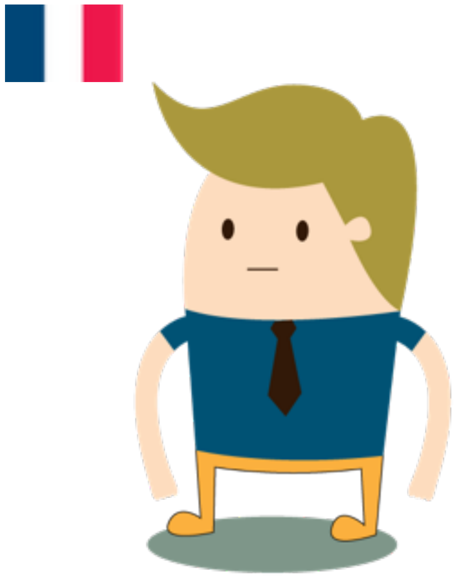


1 month later: German LE goes to seize the server



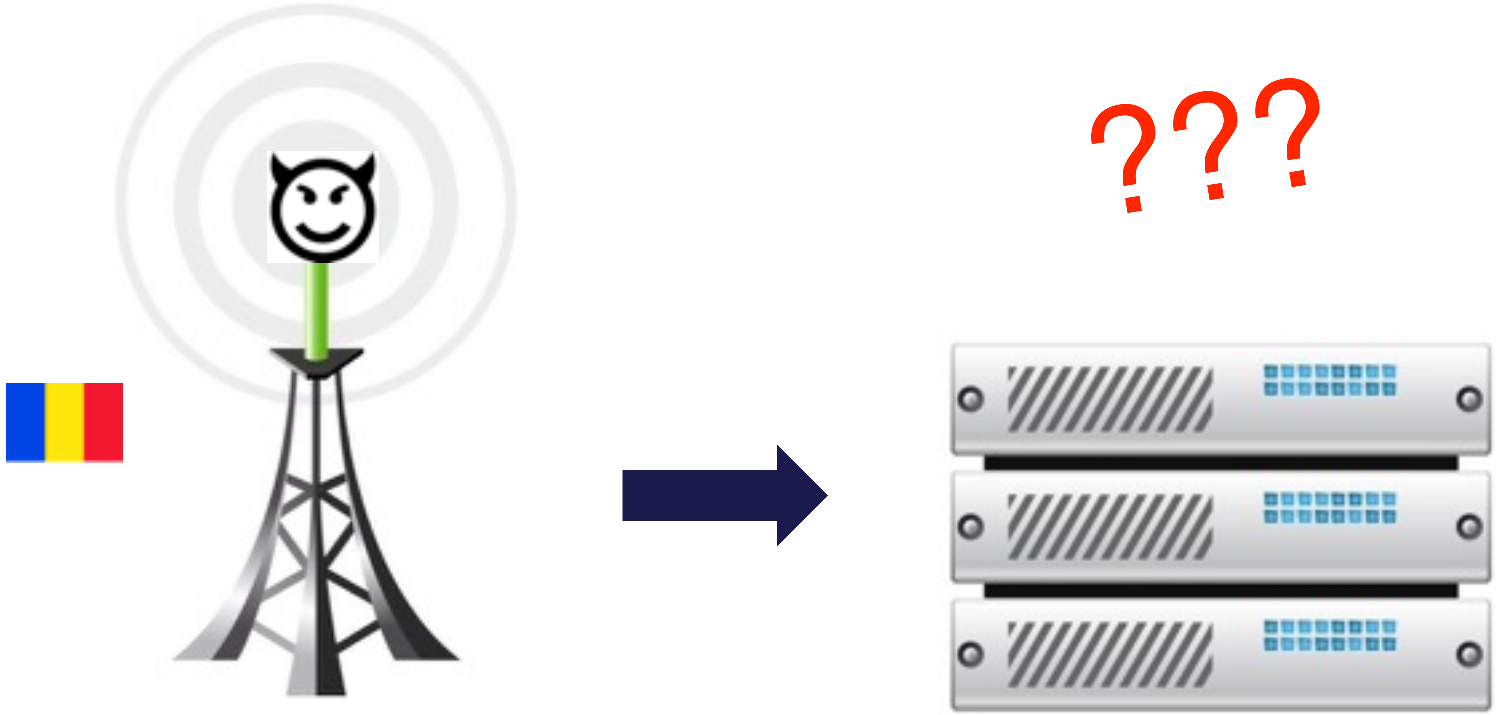
Too late!

Decryption keys have been moved to another server…



Scenario 2

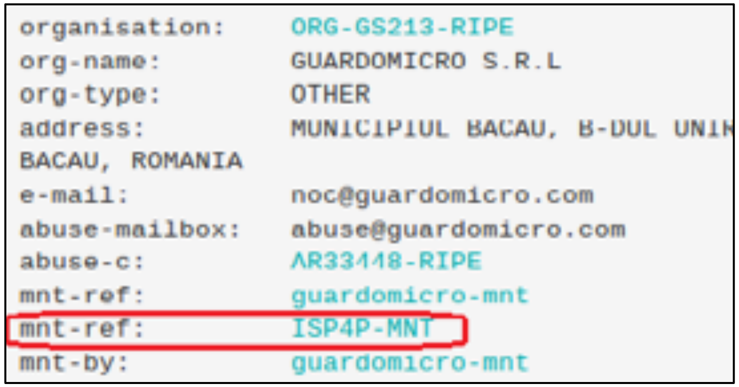
Romanian company uncooperative / victim of ID theft



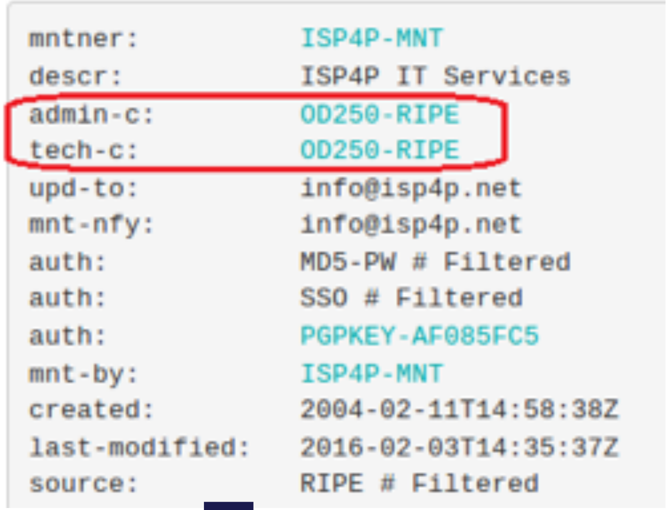
What can Jean do now?

Only link to Germany in RIPE Whois Database:

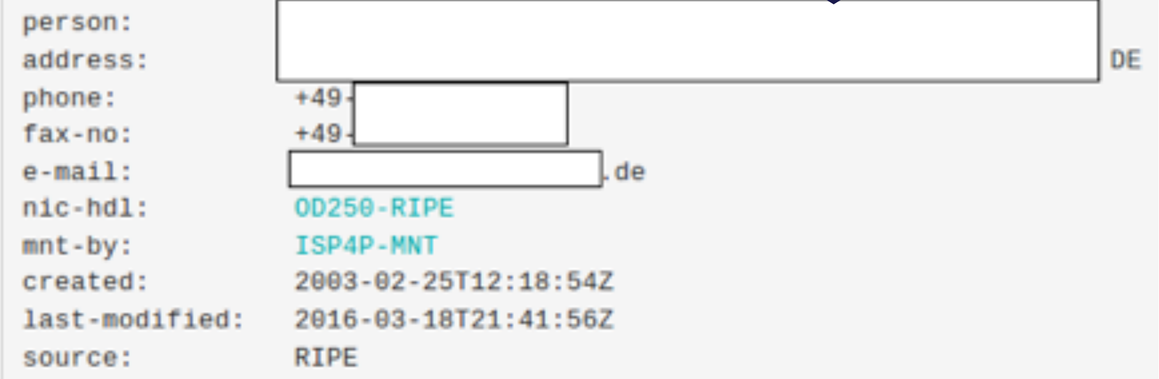
The maintainer



```
organisation:     ORG-GS213-RIPE
org-name:         GUARDOMICRO S.R.L
org-type:         OTHER
address:          MUNICIPIUL BACAU, B-DUL UNIR
BACAU, ROMANIA
e-mail:           noc@guardomicro.com
abuse-mailbox:    abuse@guardomicro.com
abuse-c:          AR33448-RIPE
mnt-ref:          guardomicro-mnt
mnt-ref:          ISP4P-MNT
mnt-by:           guardomicro-mnt
```

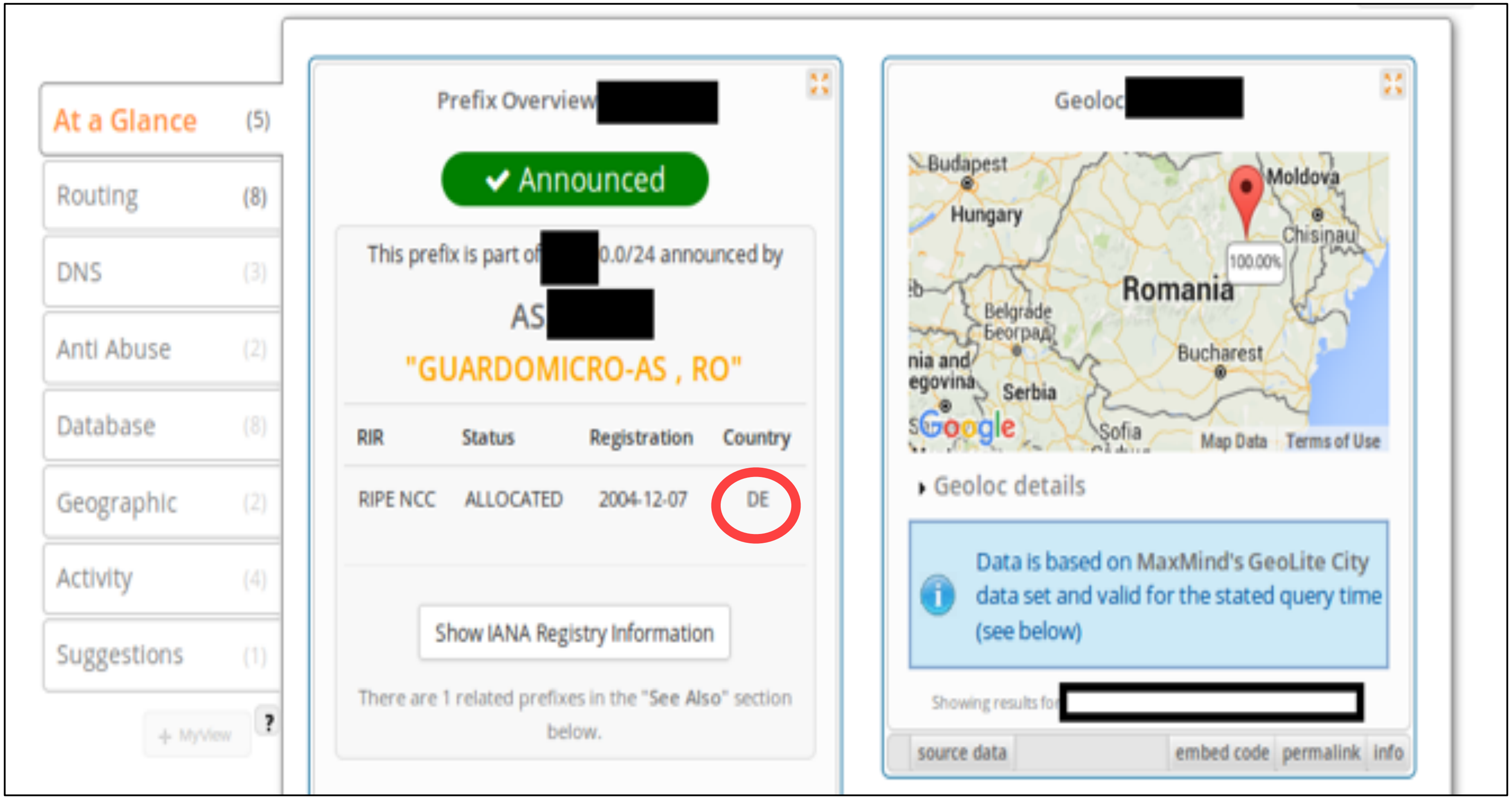


```
mntner:           ISP4P-MNT
descr:            ISP4P IT Services
admin-c:          OD250-RIPE
tech-c:           OD250-RIPE
upd-to:           info@isp4p.net
mnt-nfy:          info@isp4p.net
auth:             MD5-PW # Filtered
auth:             SSO # Filtered
auth:             PGPKEY-AF085FC5
mnt-by:           ISP4P-MNT
created:          2004-02-11T14:58:38Z
last-modified:    2016-02-03T14:35:37Z
source:           RIPE # Filtered
```



```
person:           [redacted]
address:                                             DE
phone:            +49 [redacted]
fax-no:           +49 [redacted]
e-mail:           [redacted].de
nic-hdl:          OD250-RIPE
mnt-by:           ISP4P-MNT
created:          2003-02-25T12:18:54Z
last-modified:    2016-03-18T21:41:56Z
source:           RIPE
```

Scenario 2



Prefix Overview [redacted]

✓ Announced

This prefix is part of [redacted]0.0/24 announced by

AS[redacted]

"GUARDOMICRO-AS , RO"

RIR	Status	Registration	Country
RIPE NCC	ALLOCATED	2004-12-07	DE

Show IANA Registry Information

There are 1 related prefixes in the "See Also" section below.

Geoloc[redacted]

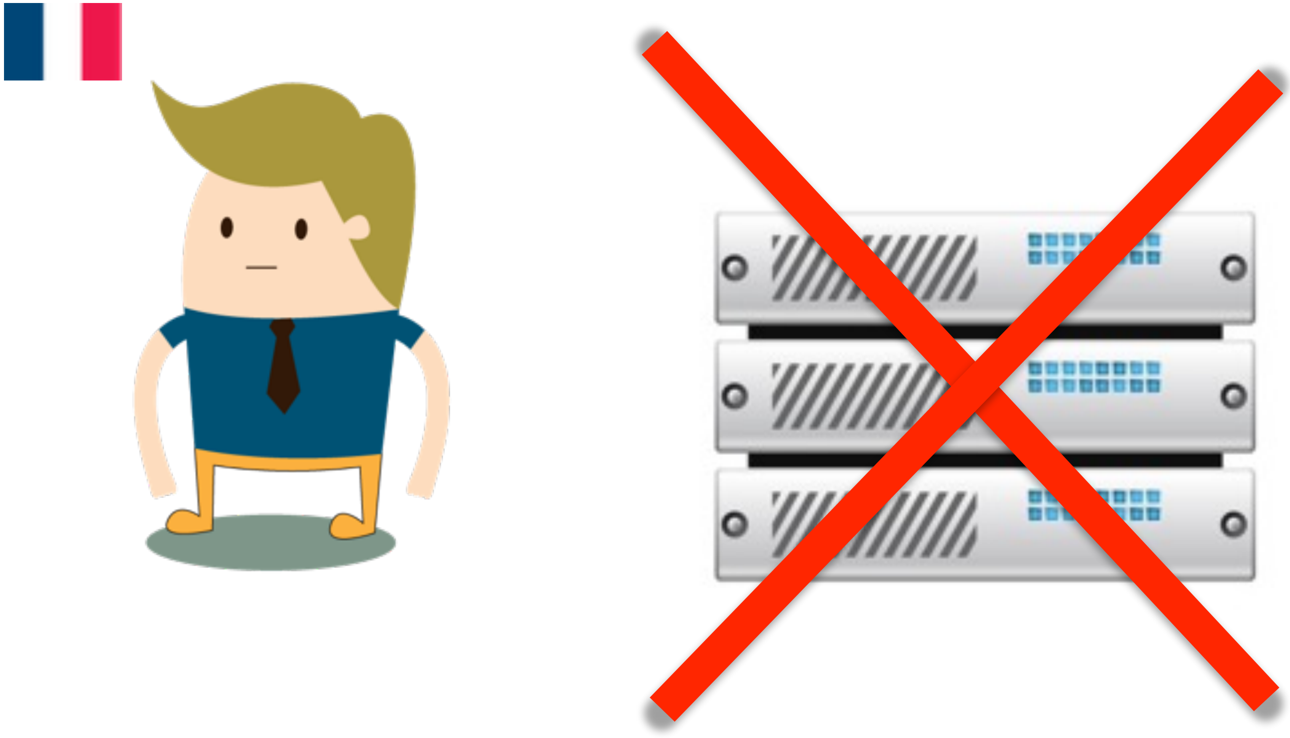
Geoloc details

Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for [redacted]

Too late!

Decryption keys have been moved to another server…



Conclusion

- ➢ How can we ensure that IP addresses are announced in the country where they are actually registered?
- ➢ Can the RIPE database reflect the location of an ISP handling an IP address?

Thank you!

gregory.mounier@europol.europa.eu