

# Inside the SCAM Jungle :

## A Closer Look at 419 Scam Email Operations



Olivier Thonard

Jelena Isacenkova

Andrei Costin  
Aurelien Francillon  
Davide Balzarotti



# Nigerian Scam Trap



**Subject:** BUSINESS PROPOSAL

**Date:** Tue, 26 Jun 2001 22:13:10 -0700 (PDT)

**From:** [emmanuel udo <emmanuel\\_udo@yahoo.com>](mailto:emmanuel_udo@yahoo.com)

**To:** [tim.richardson@senecac.on.ca](mailto:tim.richardson@senecac.on.ca)

FROM: DR, EMMANUEL UDO.

TEL: 234 1 759 1549; FAX: 234 1 759 0379.

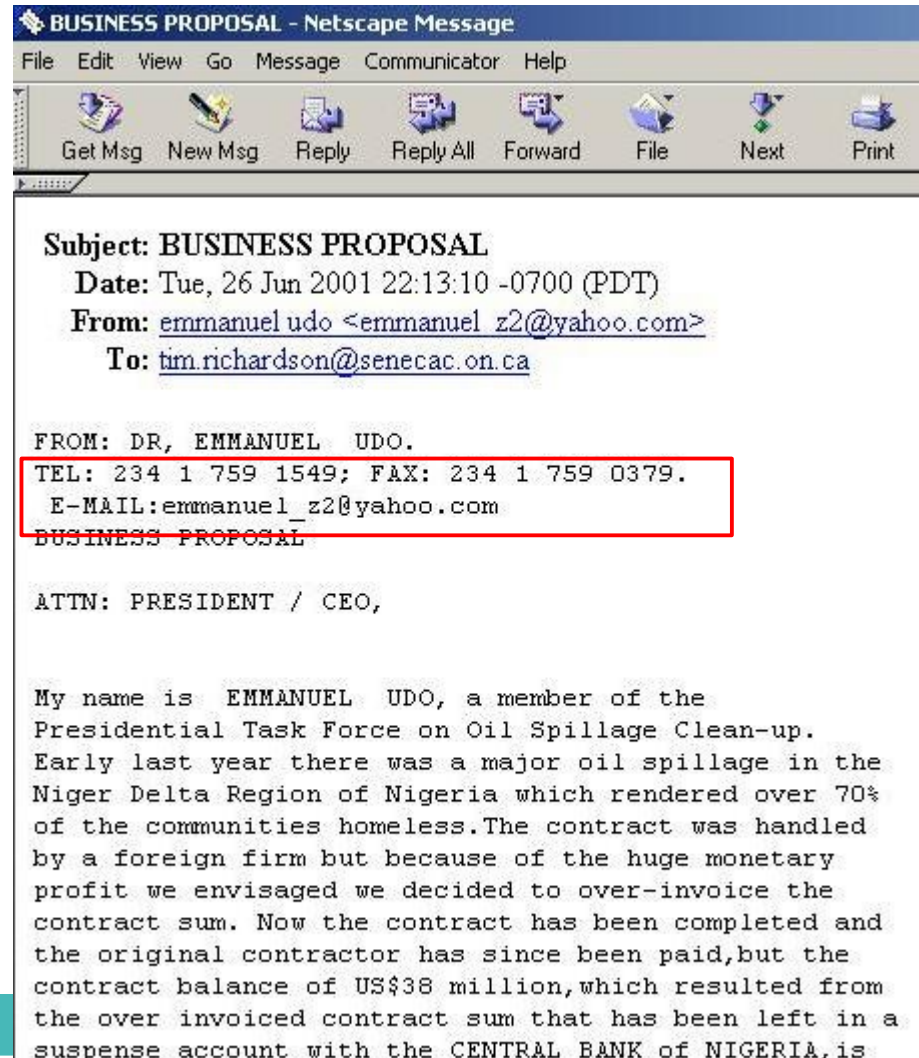
E-MAIL: [emmanuel\\_udo@yahoo.com](mailto:emmanuel_udo@yahoo.com)

BUSINESS PROPOSAL

ATTN: PRESIDENT / CEO,

My name is EMMANUEL UDO, a member of the Presidential Task Force on Oil Spillage Clean-up. Early last year there was a major oil spillage in the Niger Delta Region of Nigeria which rendered over 70% of the communities homeless. The contract was handled by a foreign firm but because of the huge monetary profit we envisaged we decided to over-invoice the contract sum. Now the contract has been completed and the original contractor has since been paid, but the contract balance of US\$38 million, which resulted from the over invoiced contract sum that has been left in a suspense account with the CENTRAL BANK of NIGERIA, is

# Nigerian Scam Trap




# Spam vs. 419 Scam

# SPAM

- High-volume
- Highly dynamic infrastructure
- Automated sending
- Trap victims through engineering effort
- Contact with victims over URLs



## 419 SCAM

- Low-volume
  - Hide behind webmail accounts
  - Manual sending
  - Trap with social engineering techniques
  - Contact with victims via emails and/or phone numbers
- 
- A rolled-up US dollar bill is held by a wooden clothespin. The bill is partially unrolled, showing the green color and some of the design. The clothespin is made of light-colored wood and is clamped onto the bill.



# Why we study campaigns

- The goal :
  - identify and characterize 419 scam campaigns
  - find predictive scam email features
- Our assumptions :
  - Scam is likely sent in campaigns, like Spam
  - Emails and phone numbers are personal scammer assets (Costin et al., PST'13) => linking features

# Outline

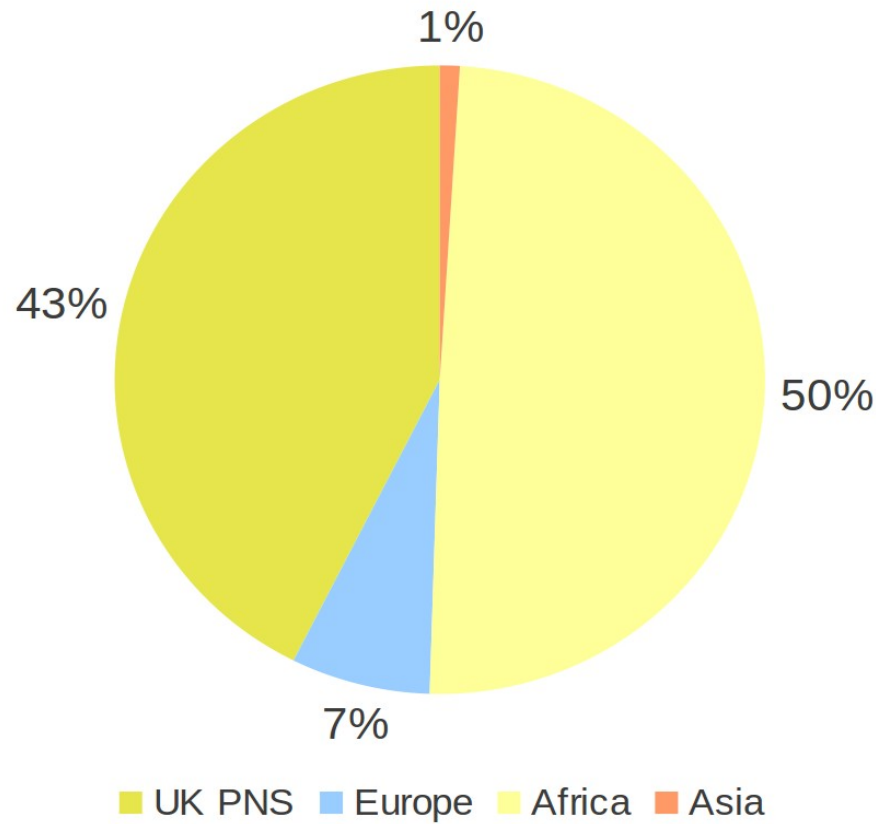
- Dataset
- Methodology
- Experimental results
- Conclusions

# Dataset

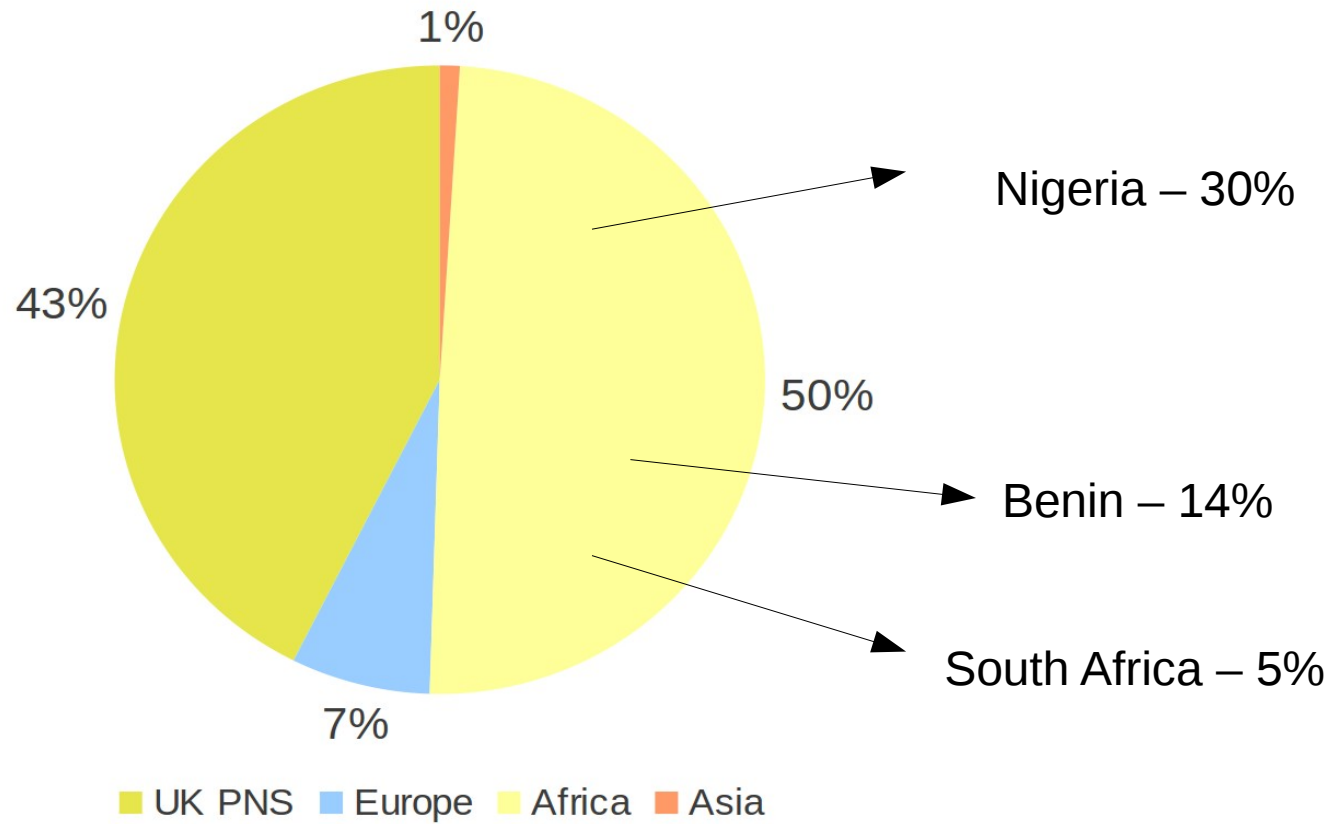
# Dataset

- Public data from `419scam.org`
- From January 2009 till August 2012
- 36,761 scam messages
- 12 countries (Europe, Africa and Asia)
- 34,723 unique email addresses
- 11,738 unique phone numbers

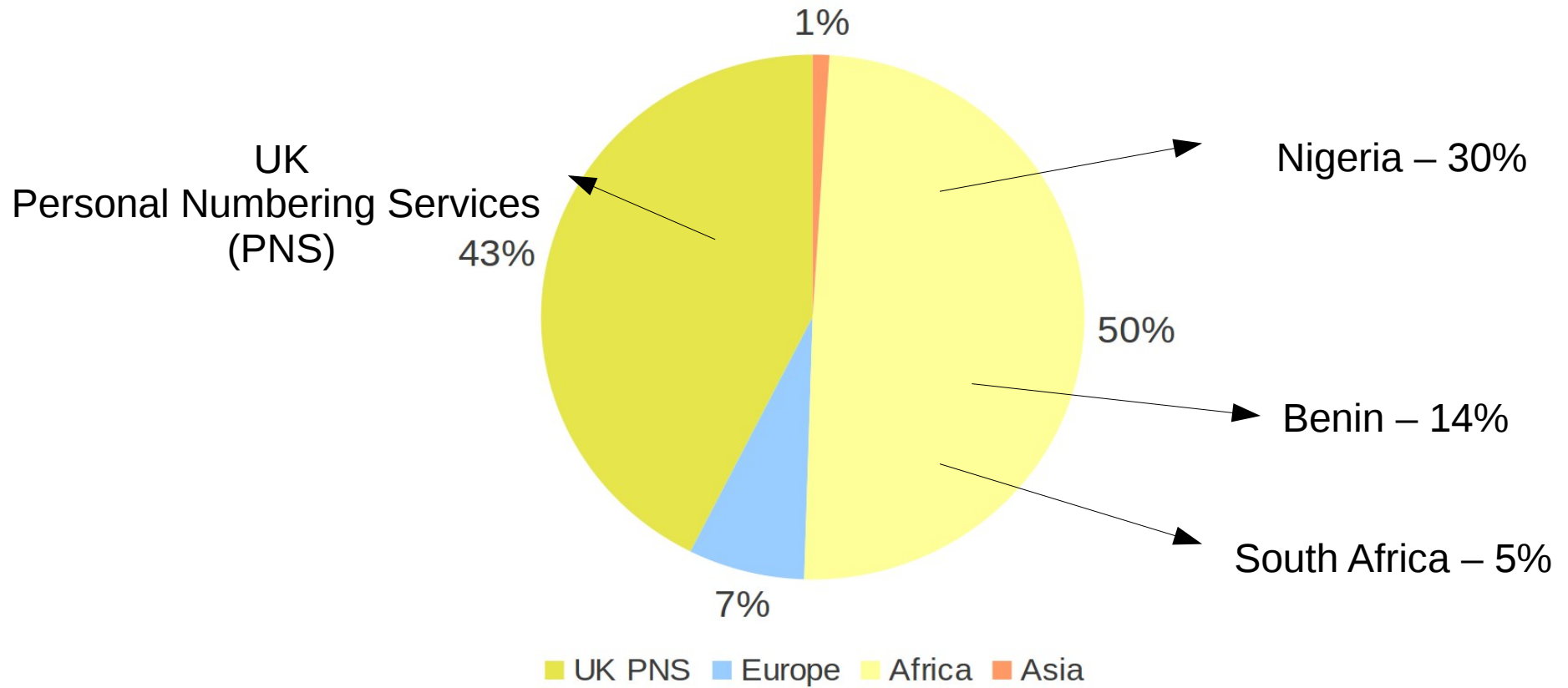
# Scam origins by phone numbers



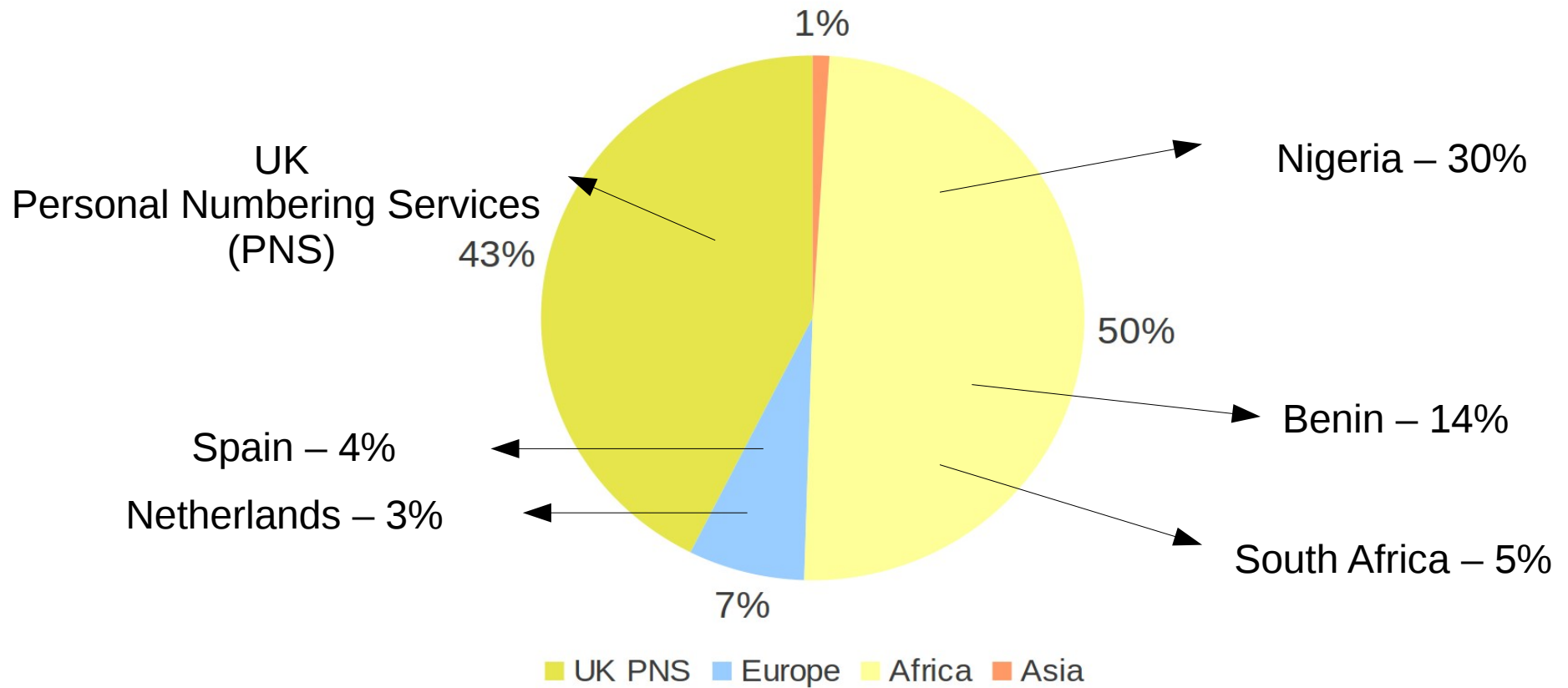
# Scam origins by phone numbers



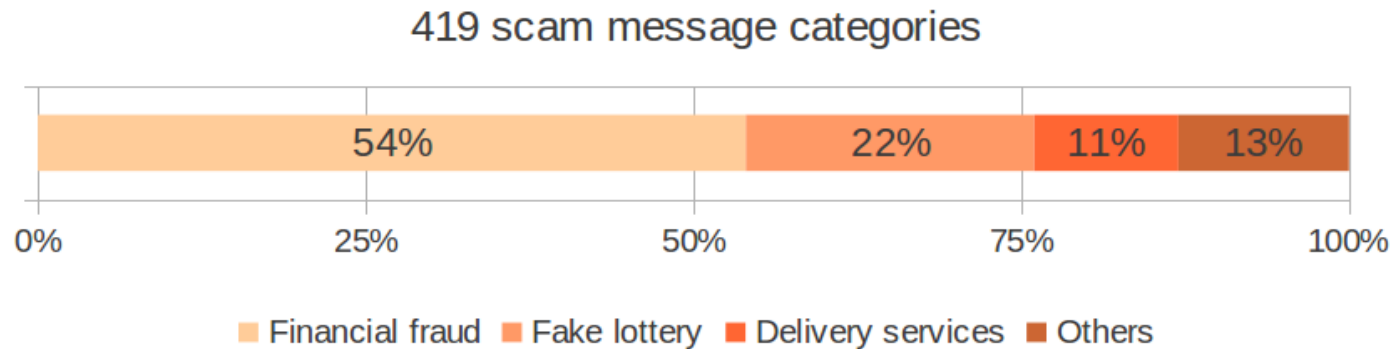
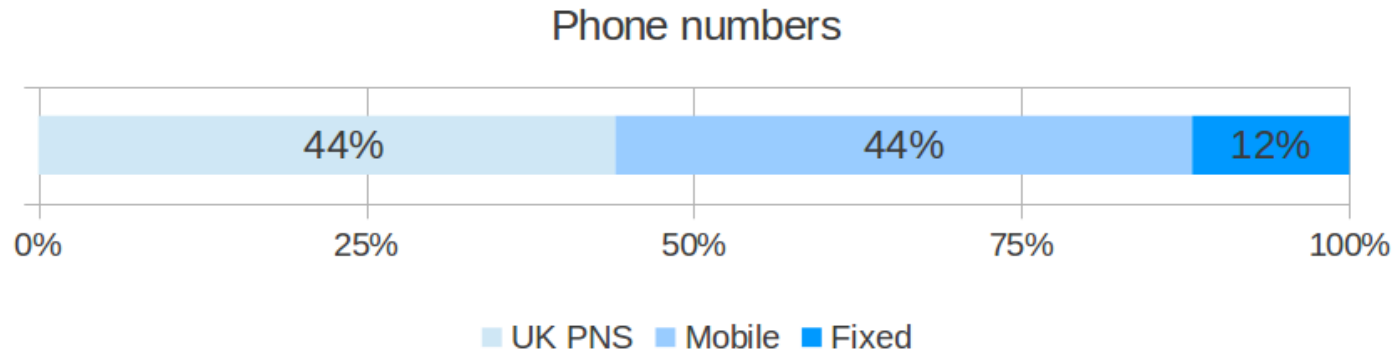
# Scam origins by phone numbers



# Scam origins by phone numbers



# Data categories



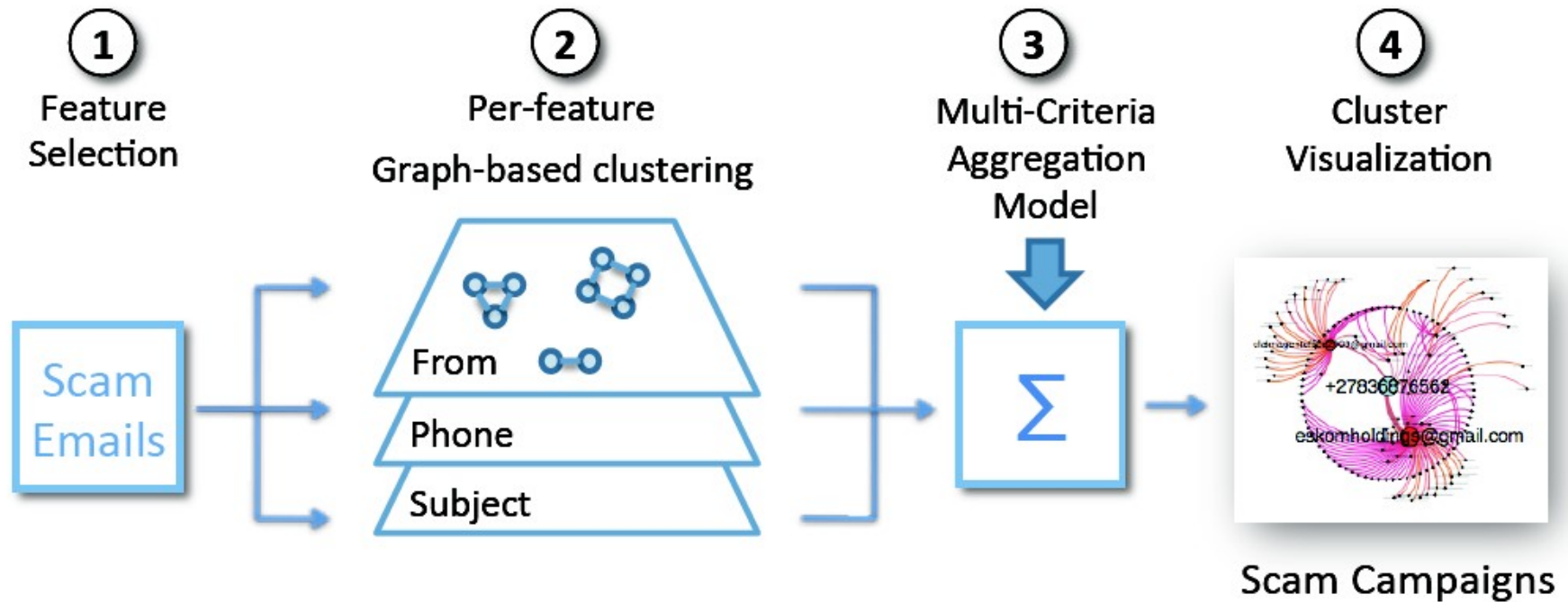


# Methodology

# TRIAGE

- Security data mining framework (Thonnard et al. at RAID'10, CEAS'11, RAID'12)
- Multi-dimensional clustering
- Links common elements together forming clusters/campaigns

# TRIAGE, part 2



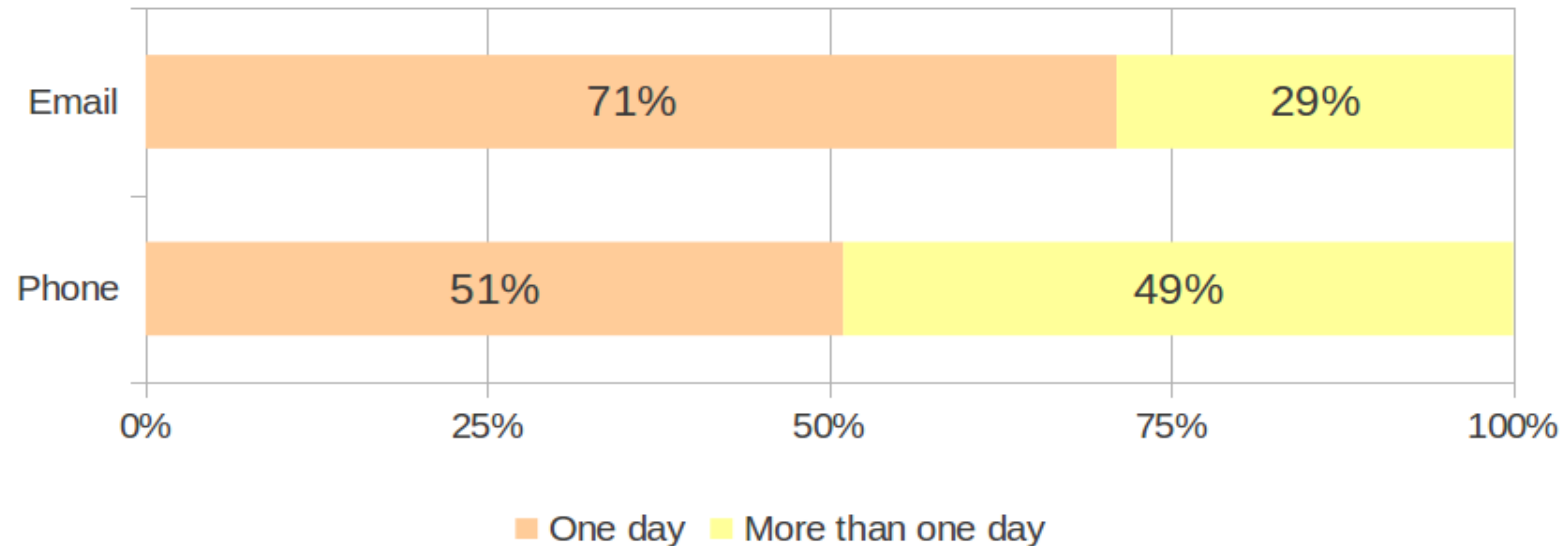


# Experimental results

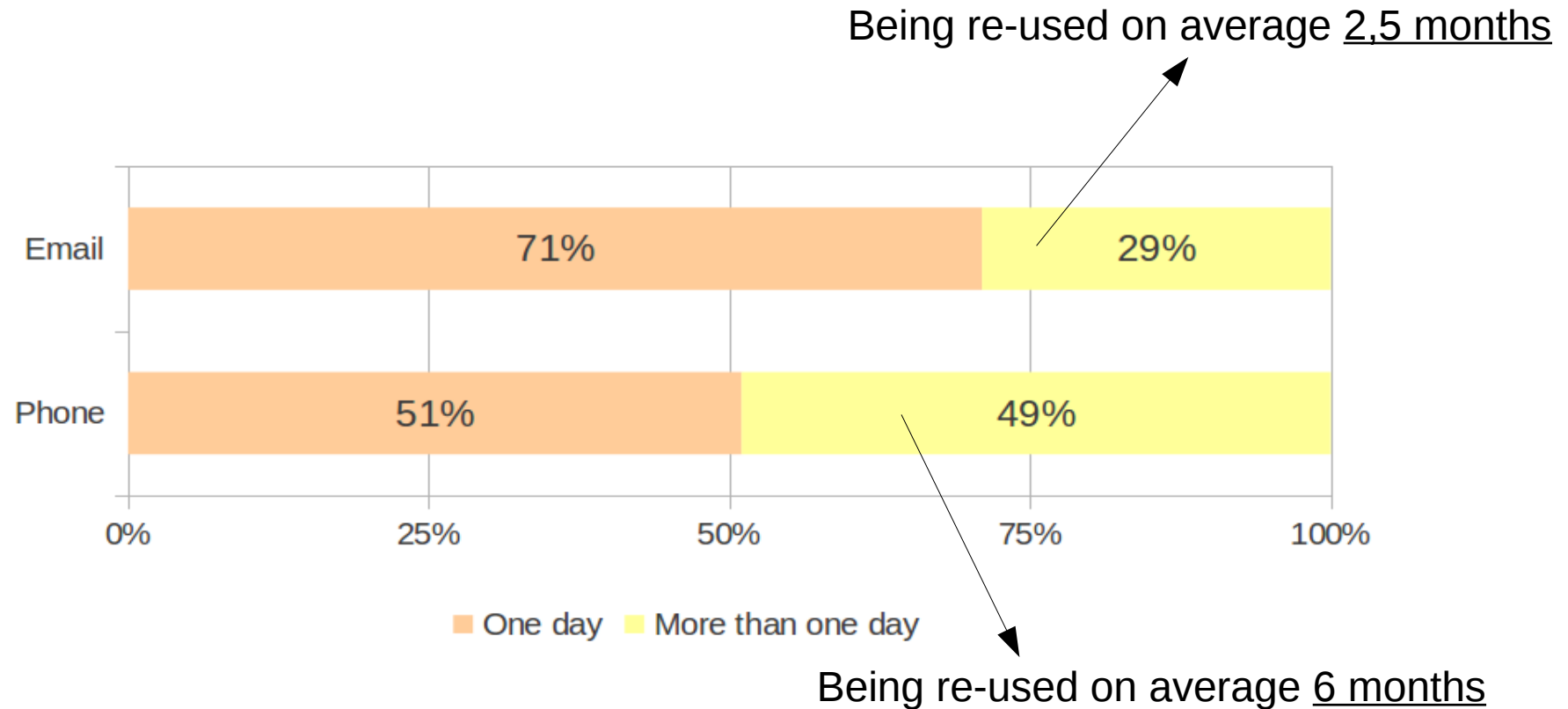
# Campaigns

- 1,040 campaigns identified, with at least 5 messages each
- Top 250 campaigns on average :
  - Long and scarce : last for **one year** and have only **28 active days**
  - Small (38 emails) : **keep low-volume**, could be unorganized
  - Use **2 phone numbers**
  - Use **6 Reply-To** email addresses
  - Use **14 From** email addresses

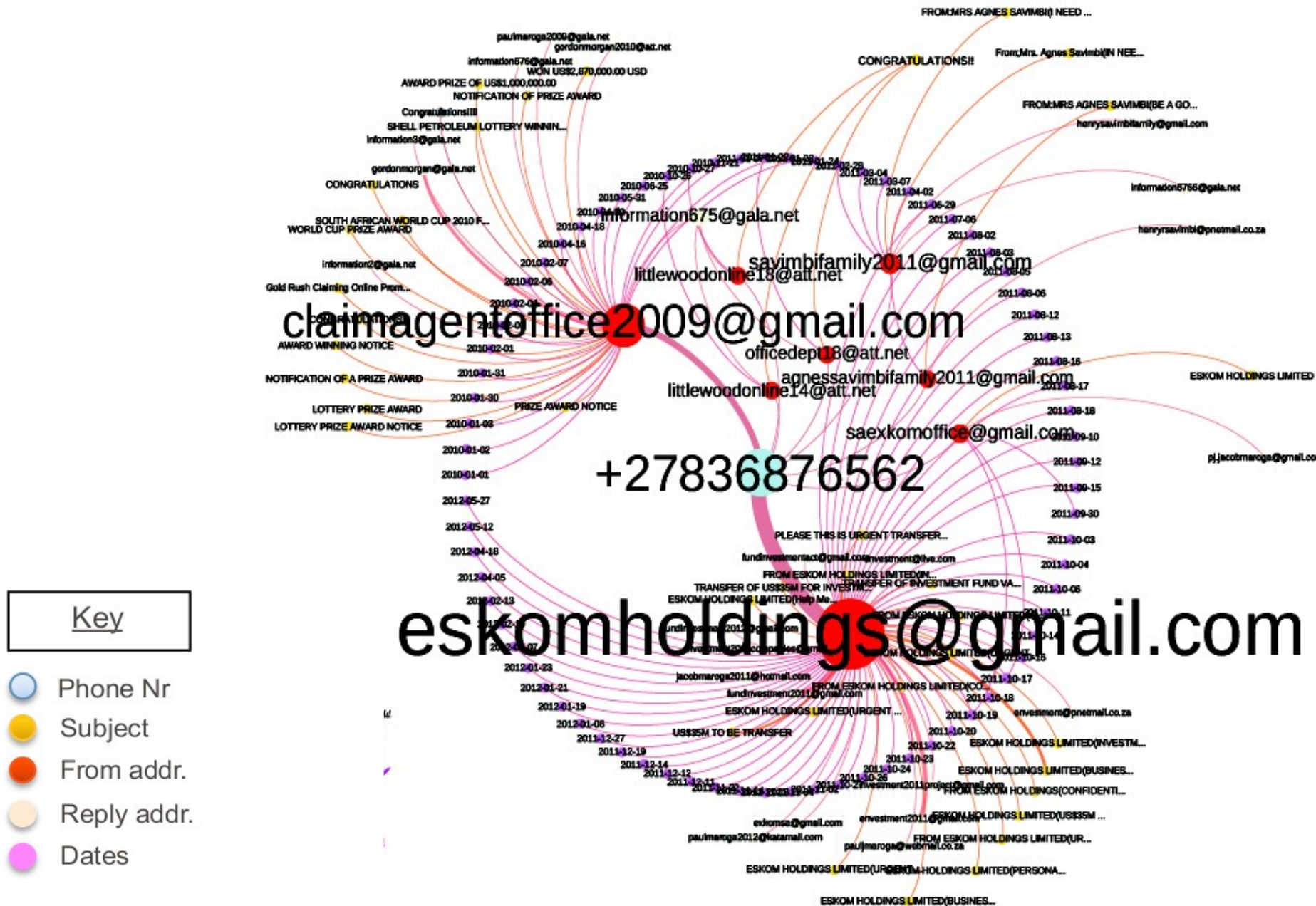
# Re-use of emails and phones



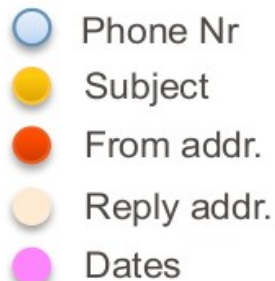
# Re-use of emails and phones



# Examples



# 83 emails



[illegible]

- Phone Nr
- Subject
- From addr.
- Reply addr.
- Dates



“Eskom generates approximately 95% of the electricity used in South Africa and approximately 45% of the electricity used in Africa.”, - Escom



# Different topics over time

## Main traits:

Topics change

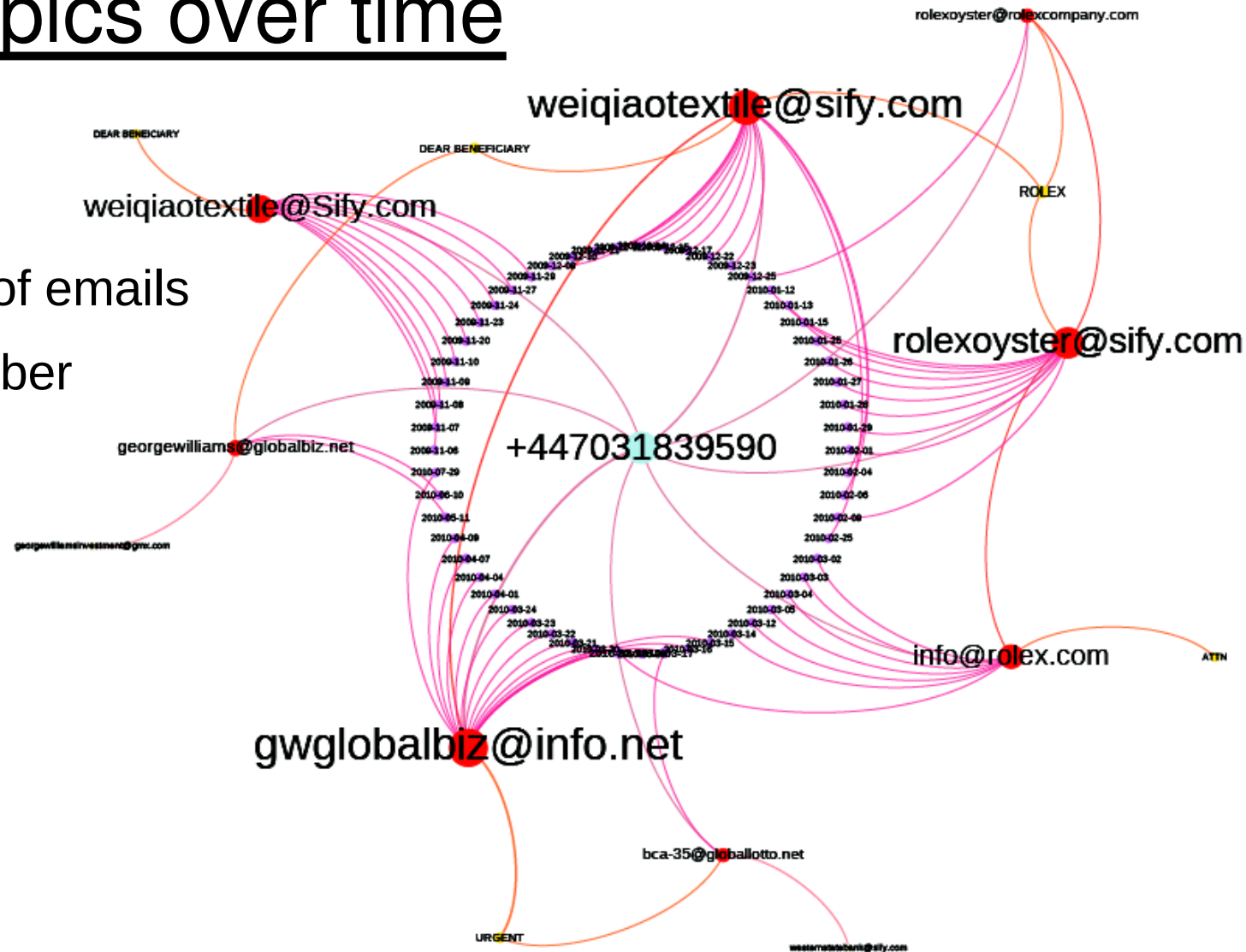
Monthly package of emails

Single phone number

58 emails



- Phone Nr
- Subject
- From addr.
- Reply addr.
- Dates



# Different topics over time

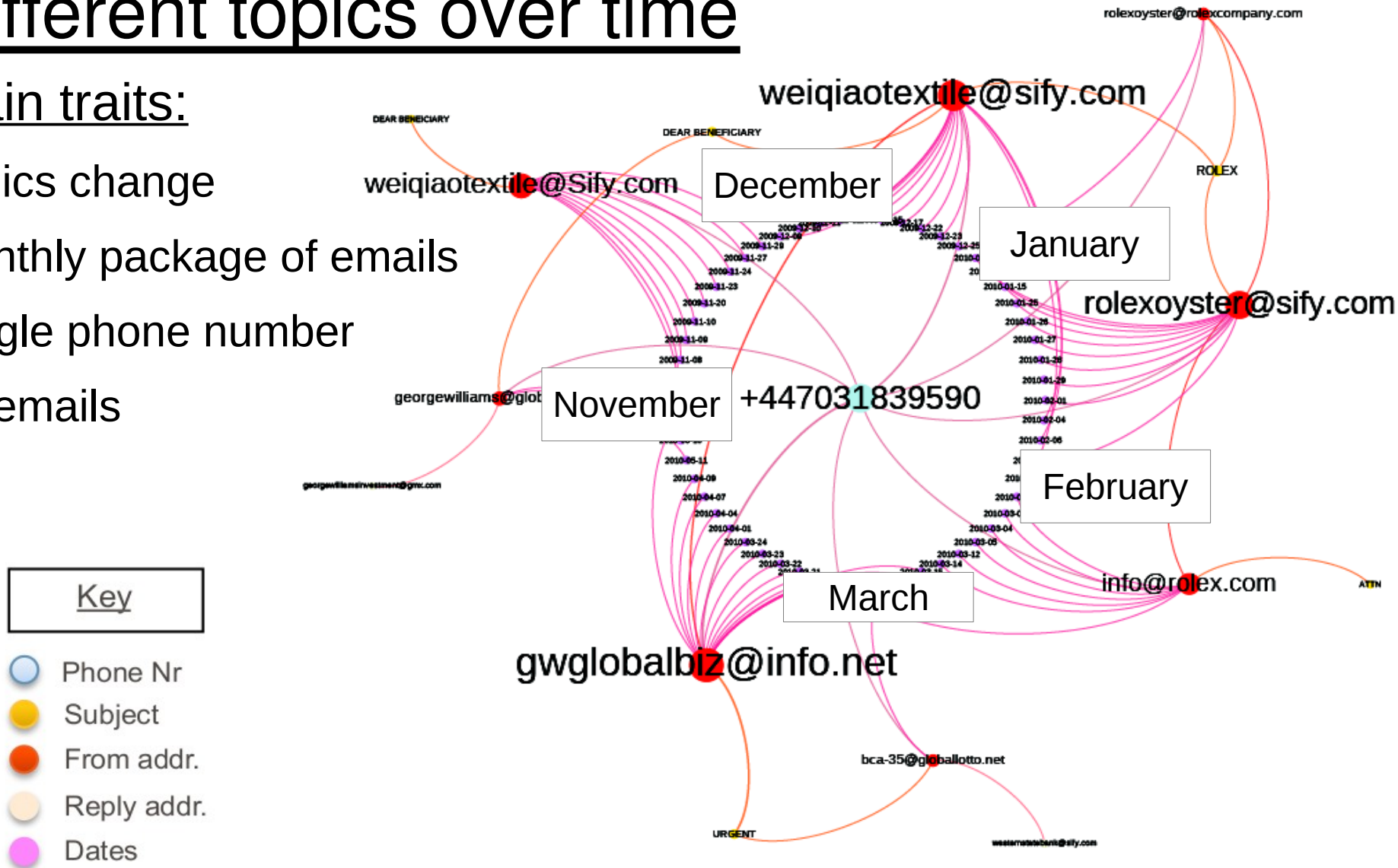
## Main traits:

Topics change

Monthly package of emails

Single phone number

58 emails



# iPhone campaign

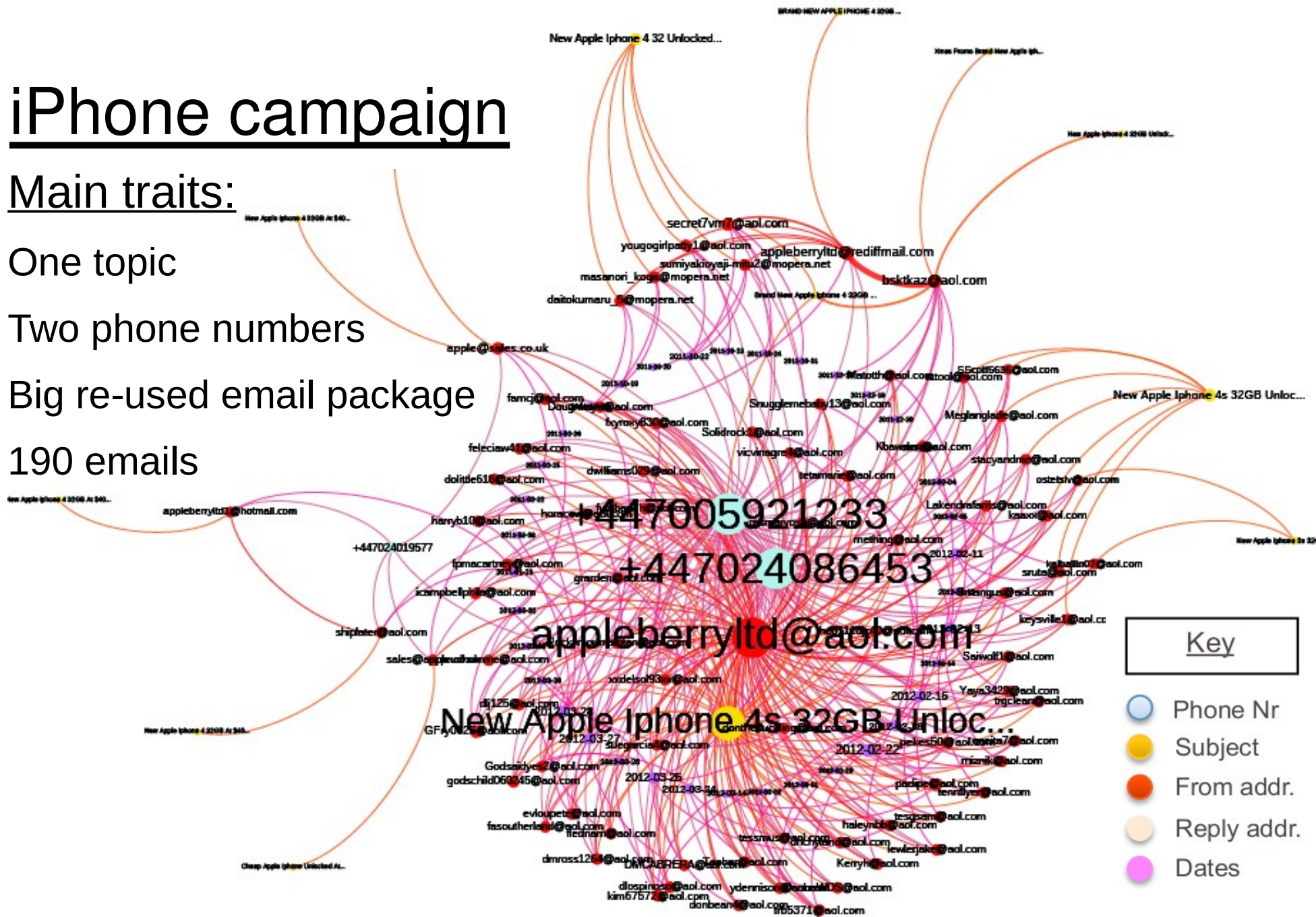
## Main traits:

One topic

Two phone numbers

Big re-used email package

190 emails



# Macro-clusters

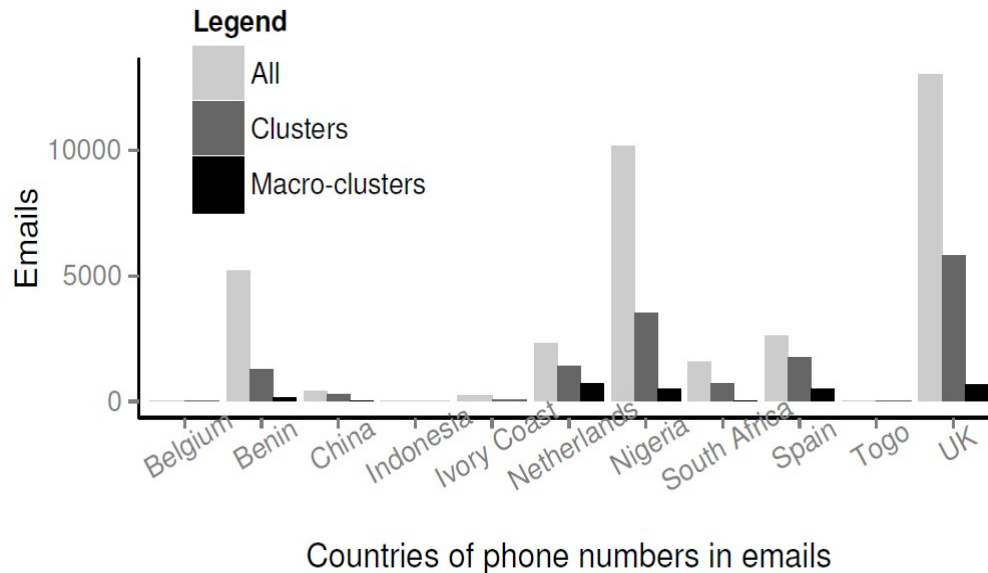
- Link strongly connected clusters into loosely connected
- Linked through emails and/or phone numbers
- 62 macro-clusters, 195 inter-connected clusters

# Top macro-clusters

Macro-cluster	Nr. of campaigns	Phones	Mailboxes	Subjects	Duration	Countries	Topics
1	14	44	677	223	4 years	4	Lottery, lost funds, investments
2	43	163	1,127	463	4 years	7	Lottery, banks, diplomats, FBI
3	6	18	128	80	4 years	4	Lottery
4	5	8	111	51	3,5 years	2	Packaging, Guinness lottery, loans
5	6	7	201	96	1 year	1	Microsoft lottery, UPS & WU delivery, lost funds
6	4	7	82	33	2 years	1	Lottery, lost payments

- Some are organized groups operating on international scale
- **Fake lottery** scam is primarily run by scammers located in Europe that are connected with African scammer groups

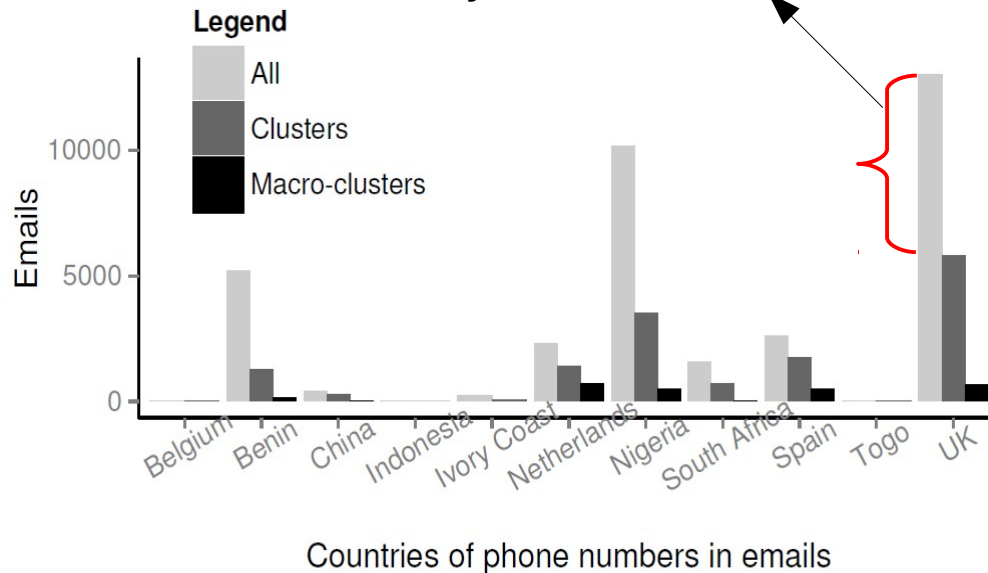
# Clusters by countries



- Majority of **unclustered** data present **isolated African actors** => unorganized
- **Macro-clusters** cover African and many European actors => bigger **organized** groups covering **Western markets**

# Clusters by countries

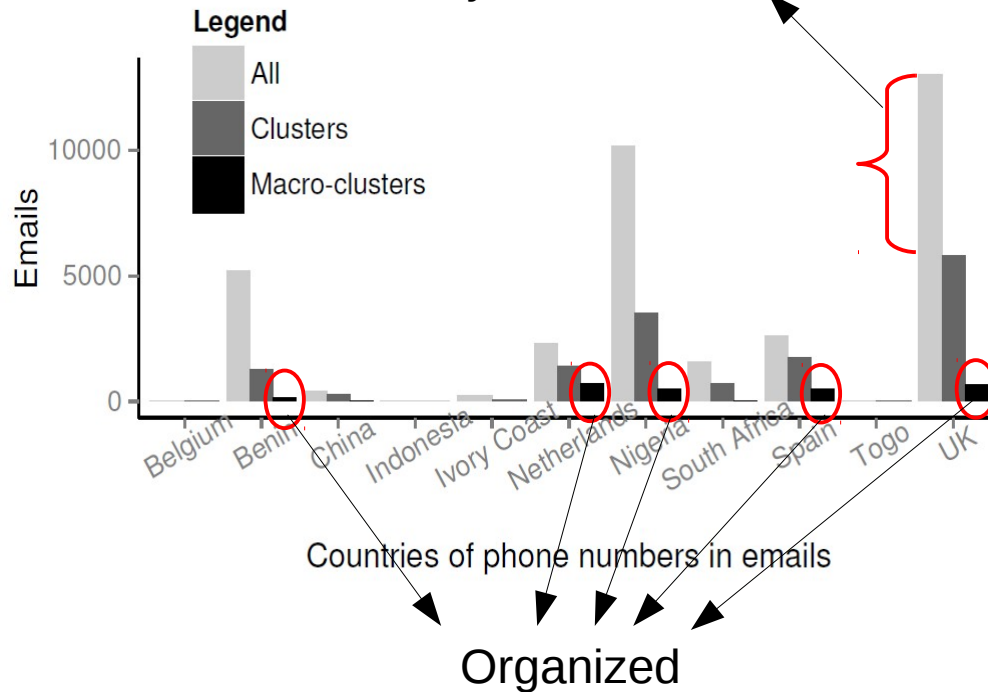
Unclustered:  
stealthy or isolated scammers



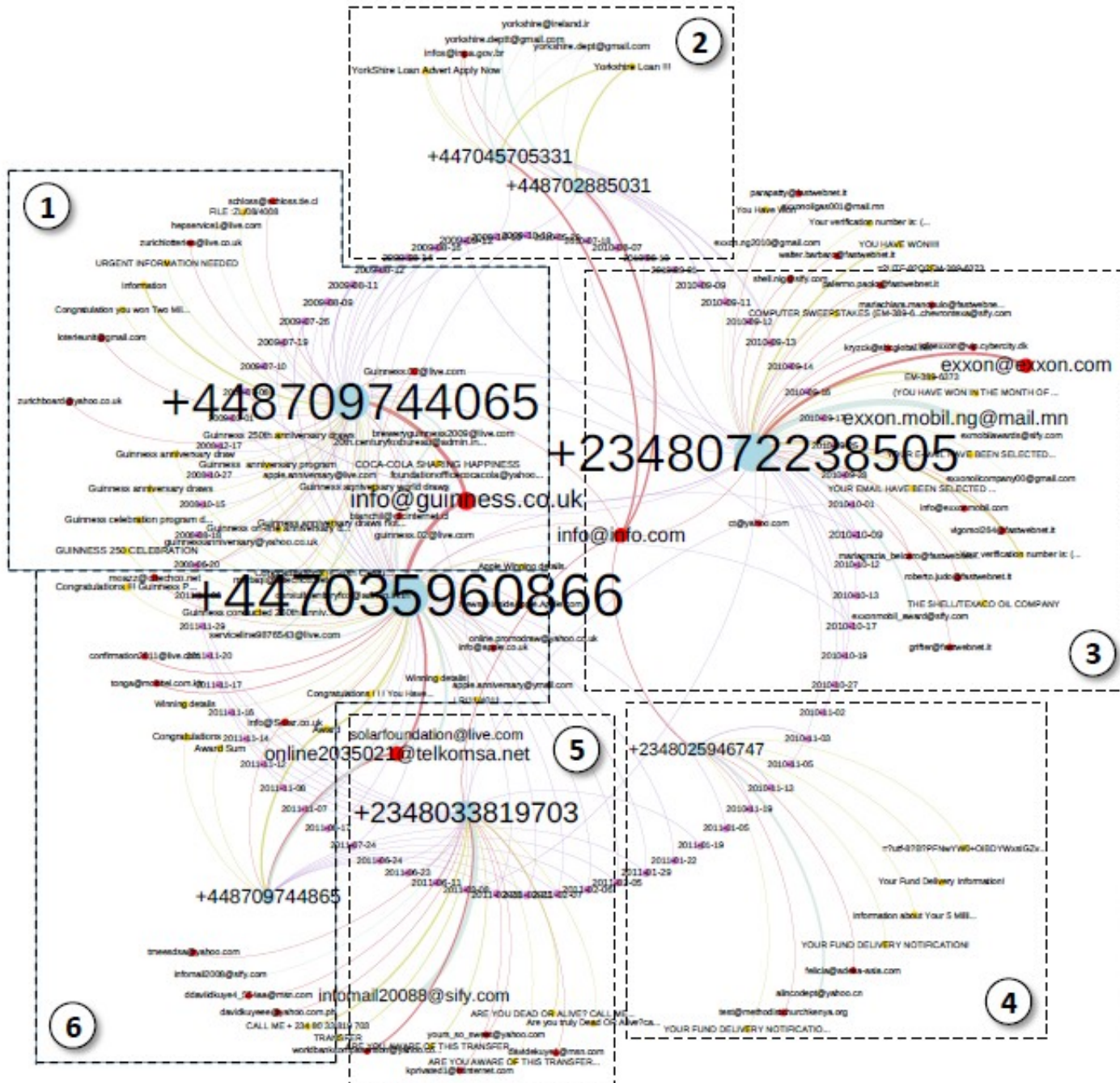
- Majority of **unclustered** data present **isolated African actors** => unorganized
- **Macro-clusters** cover African and many European actors => bigger **organized** groups covering **Western markets**

# Clusters by countries

Unclustered:  
stealthy or isolated scammers



- Majority of **unclustered** data present **isolated African actors** => unorganized
- **Macro-clusters** cover African and many European actors => bigger **organized** groups covering **Western markets**



# Key

- Phone Nr
- Subject
- From addr.
- Reply addr.
- Dates

# Conclusions

**Emails** and **phone numbers** play a **crucial role** in Nigerian email scam

- Campaigns are long and scarce
- Scammers hide behind webmail and forwarded phones
- Scam campaigns differ in their infrastructure, orchestration and modus operandi
- Different scammers probably compete for trendy topics, thus changing topics over time

# Questions?

