Inside the SCAM Jungle :

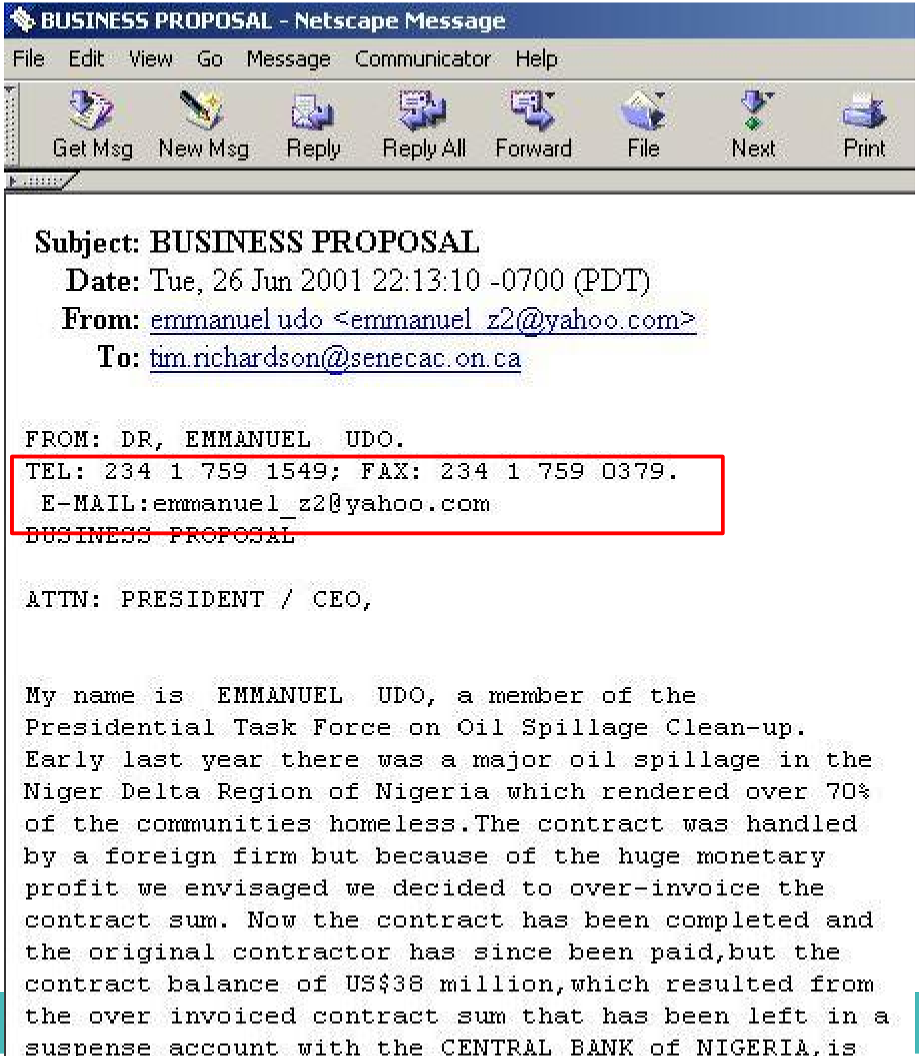
A Closer Look at 419 Scam Email Operations

Olivier Thonard

Jelena Isacenkova

Andrei Costin
Aurelien Francillon
Davide Balzarotti

Nigerian Scam Trap


BUSINESS PROPOSAL - Netscape Message
File Edit View Go Message Communicator Help
Get Msg
New Msg
Reply
Reply All
Forward
File
Next
Print

Subject: BUSINESS PROPOSAL
Date: Tue, 26 Jun 2001 22:13:10 -0700 (PDT)
From: emmanuel udo <emmanuel_z2@yahoo.com>
To: tim.richardson@senecac.on.ca

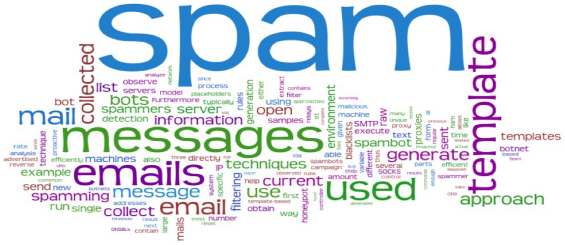
FROM: DR, EMMANUEL UDO.
TEL: 234 1 759 1549; FAX: 234 1 759 0379.
E-MAIL:emmanuel_z2@yahoo.com
BUSINESS PROPOSAL

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

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

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

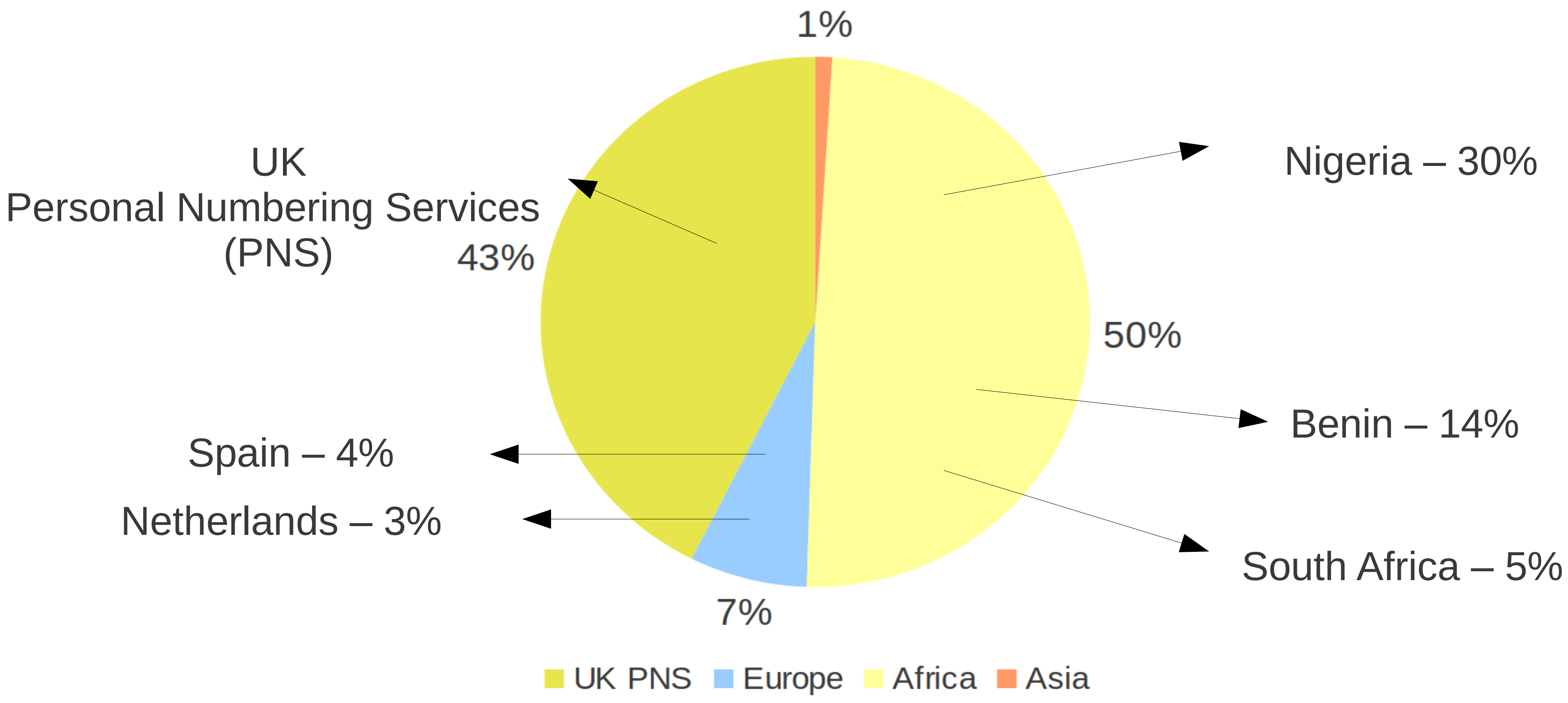
- Dataset
- Methodology
- Experimental results
- Conclusions

Dataset

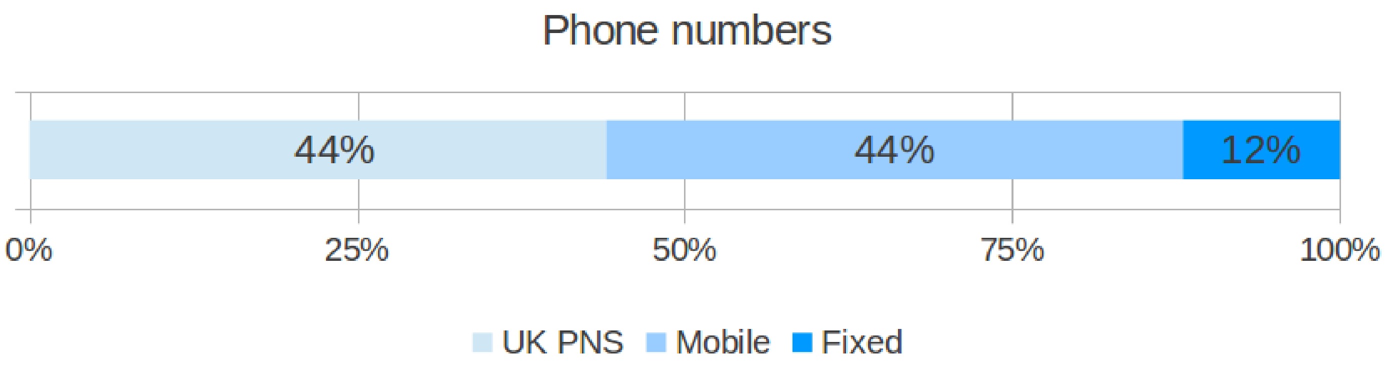
Dataset

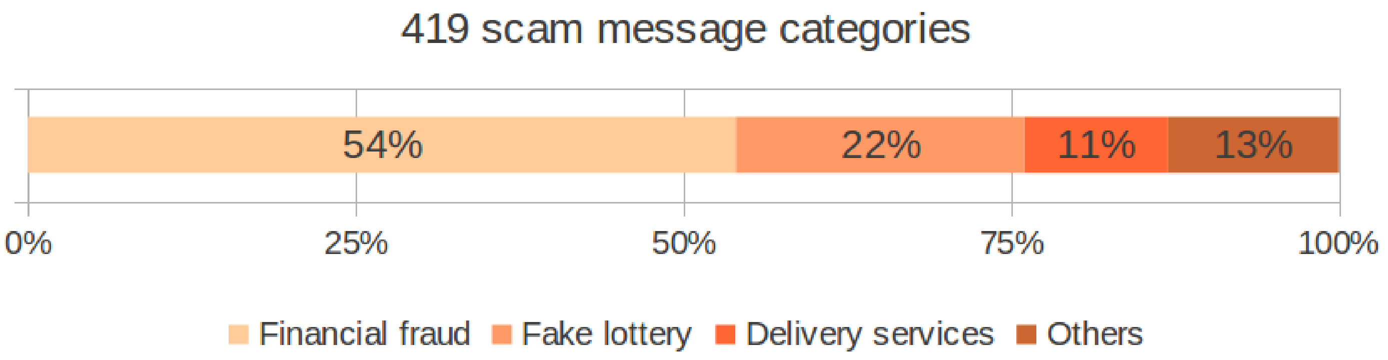
- Public data from `419scam.org`
- From January 2009 till August 2012
- 36,761 scam messages
- 12 countries (Europe, Africa and Asia)
- 34,723 unique email addresses
- 11,738 unique phone numbers

Scam origins by phone numbers



Data categories


Phone numbers

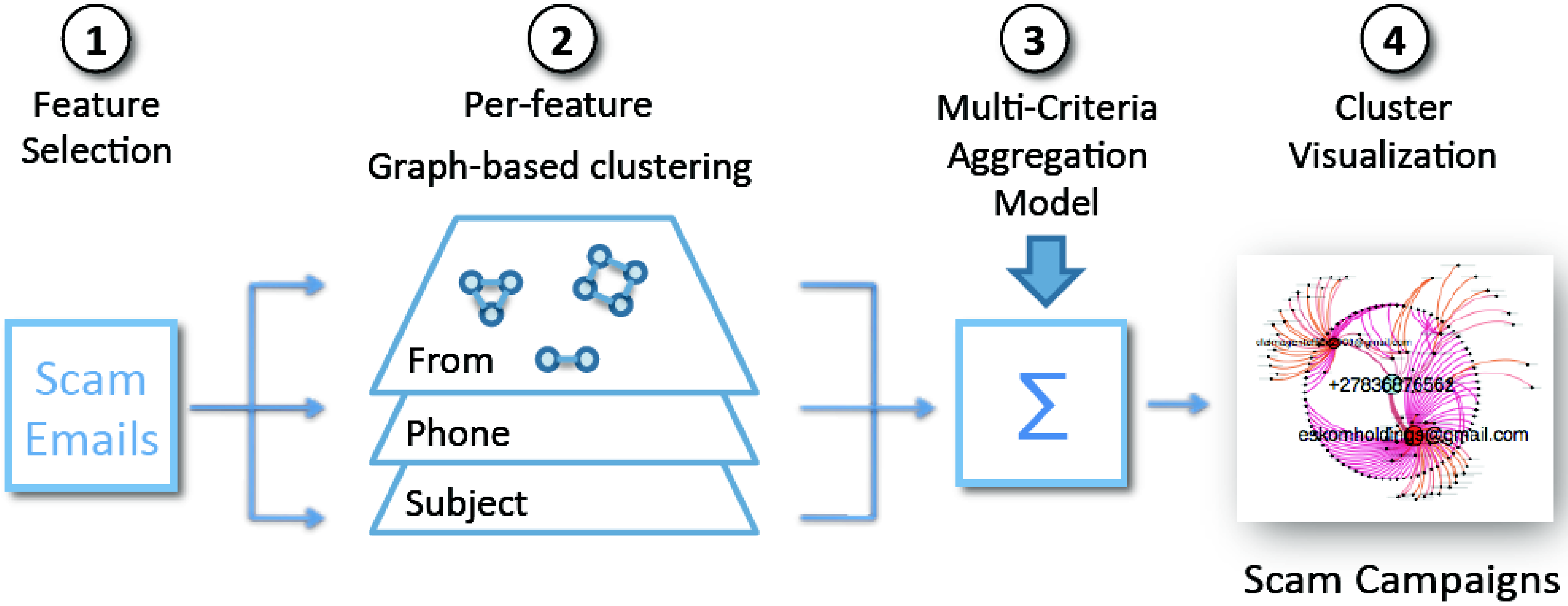

419 scam message categories

Methodology

TRIAGE

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

TRIAGE, part 2



1 Feature Selection

2 Per-feature Graph-based clustering

3 Multi-Criteria Aggregation Model

4 Cluster Visualization

Scam Emails

From

Phone

Subject

Σ

Scam Campaigns

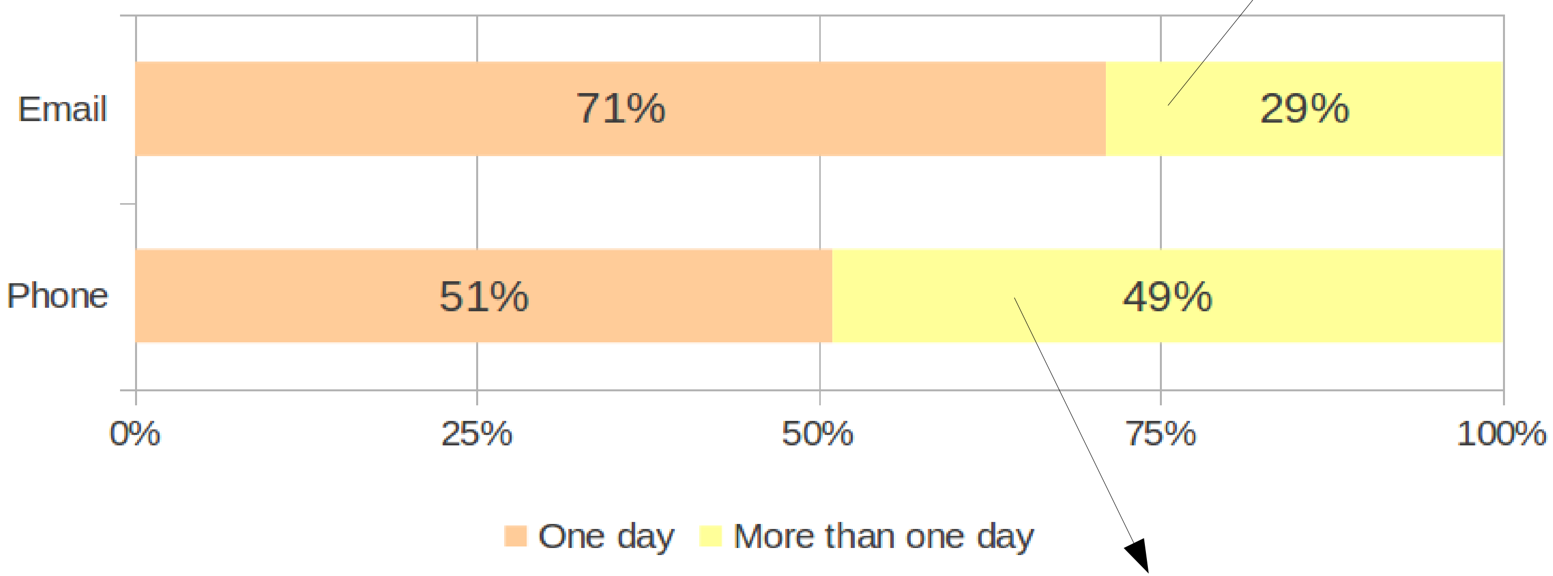
Experimental results

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

Being re-used on average 2,5 months



Being re-used on average 6 months

Examples

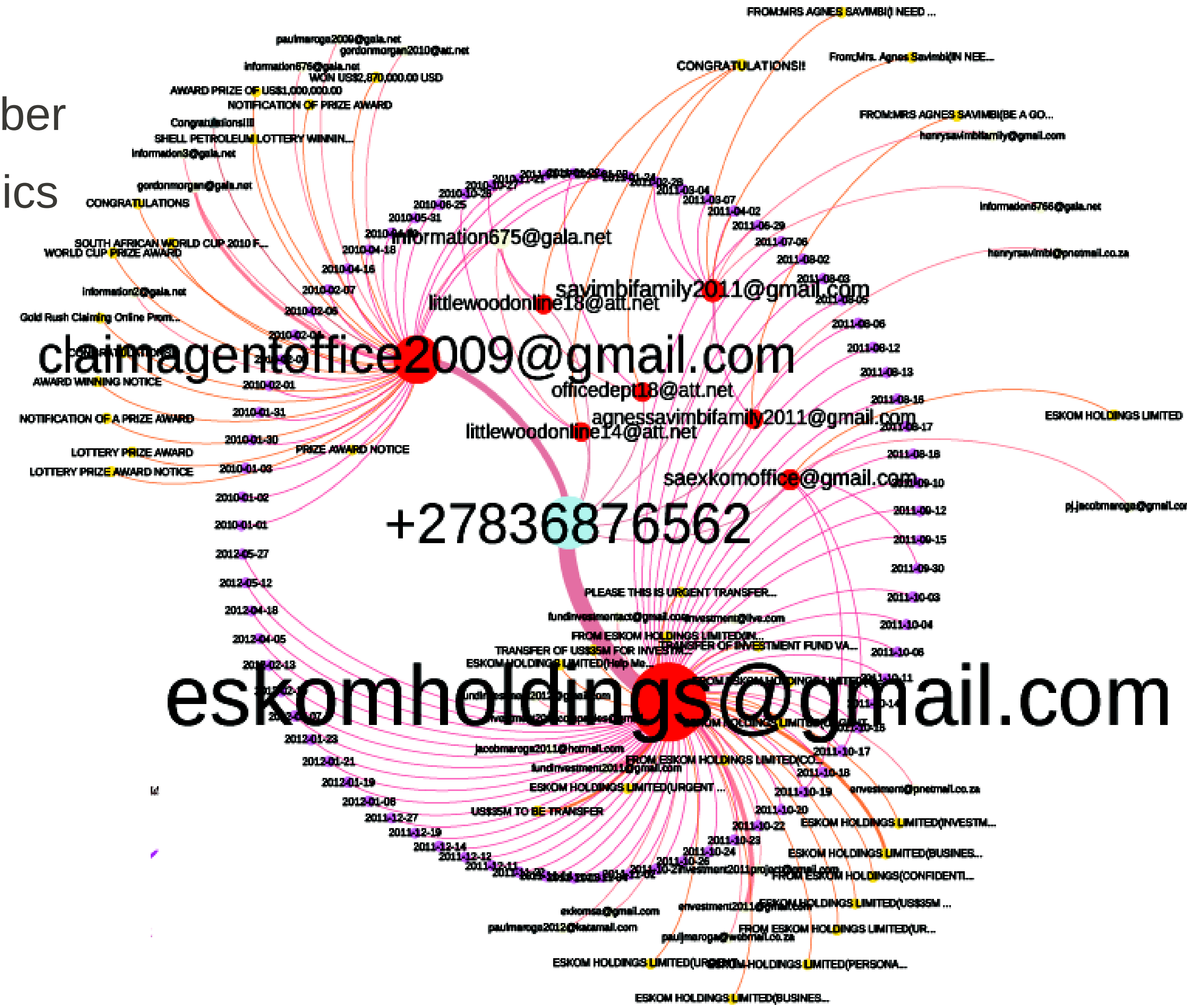
Main traits:

Single phone number

Two campaign topics

Long lived

83 emails


claimagentoffice2009@gmail.com
eskomholdings@gmail.com
+27836876562
information675@gala.net
littlewoodonline18@att.net
savimbifamily2011@gmail.com
officedept18@att.net
agnessavimbifamily2011@gmail.com
littlewoodonline14@att.net
saexkomoffice@gmail.com
paulmaroga2009@gala.net
gordonmorgan2010@att.net
information676@gala.net
WON US$2,870,000.00 USD
AWARD PRIZE OF US$1,000,000.00
NOTIFICATION OF PRIZE AWARD
Congratulations!!!
SHELL PETROLEUM LOTTERY WINNIN...
information3@gala.net
gordonmorgan@gala.net
CONGRATULATIONS
SOUTH AFRICAN WORLD CUP 2010 F...
WORLD CUP PRIZE AWARD
information2@gala.net
Gold Rush Claiming Online Prom...
AWARD WINNING NOTICE
NOTIFICATION OF A PRIZE AWARD
LOTTERY PRIZE AWARD
LOTTERY PRIZE AWARD NOTICE
PRIZE AWARD NOTICE
FROM:MRS AGNES SAVIMBI() NEED ...
CONGRATULATIONS!!
From;Mrs. Agnes Savimbi(IN NEE...
FROM:MRS AGNES SAVIMBI(BE A GO...
henrysavimbifamily@gmail.com
information6766@gala.net
henrysavimbi@pnetmail.co.za
ESKOM HOLDINGS LIMITED
pj.jacobmaroga@gmail.com
PLEASE THIS IS URGENT TRANSFER...
fundinvestmentact@gmail.com
investment@live.com
FROM ESKOM HOLDINGS LIMITED(IN...
TRANSFER OF INVESTMENT FUND VA...
TRANSFER OF US$35M FOR INVESTM...
ESKOM HOLDINGS LIMITED(Help Me...
jacobmaroga2011@hotmail.com
FROM ESKOM HOLDINGS LIMITED(CO...
fundinvestment2011@gmail.com
ESKOM HOLDINGS LIMITED(URGENT ...
US$35M TO BE TRANSFER
envestment@pnetmail.co.za
ESKOM HOLDINGS LIMITED(INVESTM...
ESKOM HOLDINGS LIMITED(BUSINES...
investment2011project@gmail.com
FROM ESKOM HOLDINGS(CONFIDENTI...
eskomsa@gmail.com
envestment2011@gmail.com
ESKOM HOLDINGS LIMITED(US$35M ...
paulmaroga2012@katamail.com
FROM ESKOM HOLDINGS LIMITED(UR...
pauljmaroga@webmail.co.za
ESKOM HOLDINGS LIMITED(URGENT...
ESKOM HOLDINGS LIMITED(PERSONA...
ESKOM HOLDINGS LIMITED(BUSINES...
2010-01-01
2010-01-02
2010-01-08
2010-01-30
2010-01-31
2010-02-01
2010-02-06
2010-02-07
2010-04-16
2010-04-18
2010-05-31
2010-06-25
2010-10-28
2010-10-27
2010-11-21
2011-02-28
2011-03-04
2011-03-07
2011-04-02
2011-06-29
2011-07-06
2011-08-02
2011-08-03
2011-08-06
2011-08-12
2011-08-13
2011-08-16
2011-08-17
2011-08-18
2011-09-10
2011-09-12
2011-09-15
2011-09-30
2011-10-03
2011-10-04
2011-10-06
2011-10-11
2011-10-14
2011-10-16
2011-10-17
2011-10-18
2011-10-19
2011-10-20
2011-10-22
2011-10-23
2011-10-24
2011-10-26
2011-12-11
2011-12-12
2011-12-14
2011-12-19
2011-12-27
2012-01-08
2012-01-19
2012-01-21
2012-01-23
2012-02-13
2012-04-05
2012-04-18
2012-05-12
2012-05-27

Key

○ Phone Nr

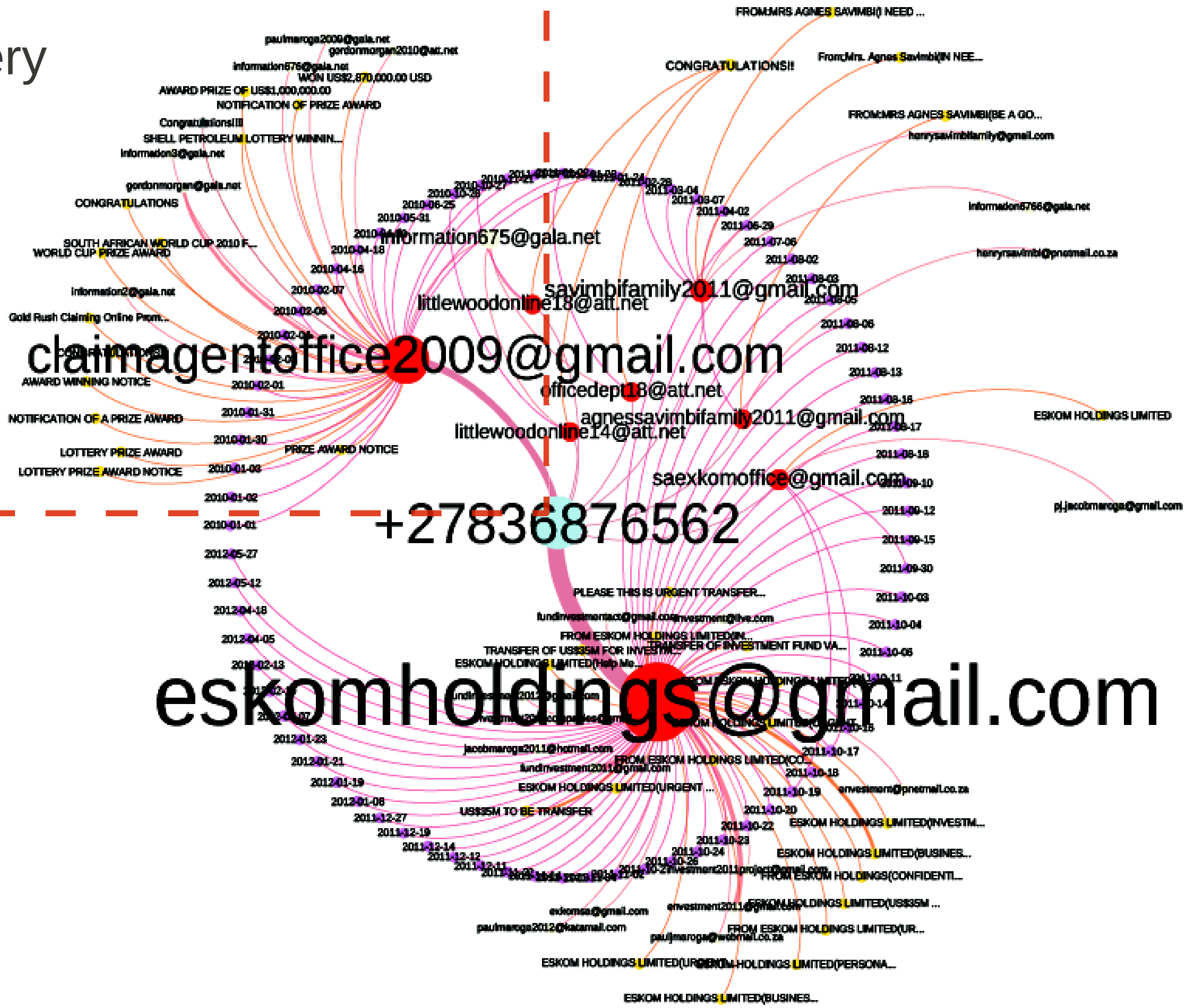
● Subject

● From addr.

○ Reply addr.

● Dates

Fake lottery
1 year


paulmaroga2009@gala.net
gordonmorgan2010@att.net
information676@gala.net
WON US$2,870,000.00 USD
AWARD PRIZE OF US$1,000,000.00
NOTIFICATION OF PRIZE AWARD
Congratulations!!!
SHELL PETROLEUM LOTTERY WINNIN...
information3@gala.net
gordonmorgan@gala.net
CONGRATULATIONS
SOUTH AFRICAN WORLD CUP 2010 F...
WORLD CUP PRIZE AWARD
information2@gala.net
Gold Rush Claiming Online Prom...
CONGRATULATIONS!!
AWARD WINNING NOTICE
NOTIFICATION OF A PRIZE AWARD
LOTTERY PRIZE AWARD
LOTTERY PRIZE AWARD NOTICE
PRIZE AWARD NOTICE
claimagentoffice2009@gmail.com
information675@gala.net
littlewoodonline18@att.net
savimbifamily2011@gmail.com
officedept18@att.net
agnessavimbifamily2011@gmail.com
littlewoodonline14@att.net
saexkomoffice@gmail.com
+27836876562
eskomholdings@gmail.com
2010-01-01
2010-01-02
2010-01-08
2010-01-30
2010-01-31
2010-02-01
2010-02-04
2010-02-06
2010-02-07
2010-04-16
2010-04-18
2010-05-31
2010-06-25
2010-10-28
2010-10-27
2010-12-21
2011-02-28
2011-03-04
2011-03-07
2011-04-02
2011-06-29
2011-07-06
2011-08-02
2011-08-03
2011-08-05
2011-08-06
2011-08-12
2011-08-13
2011-08-16
2011-08-17
2011-08-18
2011-09-10
2011-09-12
2011-09-15
2011-09-30
2011-10-03
2011-10-04
2011-10-06
2011-10-11
2011-10-14
2011-10-16
2011-10-17
2011-10-18
2011-10-19
2011-10-20
2011-10-22
2011-10-23
2011-10-24
2011-10-26
2011-12-11
2011-12-12
2011-12-14
2011-12-19
2011-12-27
2012-01-08
2012-01-19
2012-01-21
2012-01-23
2012-02-13
2012-04-05
2012-04-18
2012-05-12
2012-05-27
FROM:MRS AGNES SAVIMBI() NEED ...
CONGRATULATIONS!!
From:Mrs. Agnes Savimbi(IN NEE...
FROM:MRS AGNES SAVIMBI(BE A GO...
henrysavimbifamily@gmail.com
information6766@gala.net
henrysavimbi@pnetmail.co.za
ESKOM HOLDINGS LIMITED
pj.jacobmaroga@gmail.com
PLEASE THIS IS URGENT TRANSFER...
fundinvestmentact@gmail.com
investment@live.com
FROM ESKOM HOLDINGS LIMITED(IN...
TRANSFER OF INVESTMENT FUND VA...
TRANSFER OF US$35M FOR INVESTM...
ESKOM HOLDINGS LIMITED(Help Me...
FROM ESKOM HOLDINGS LIMITED(...
ESKOM HOLDINGS LIMITED(URGENT...
jacobmaroga2011@hotmail.com
FROM ESKOM HOLDINGS LIMITED(CO...
fundinvestment2011@gmail.com
ESKOM HOLDINGS LIMITED(URGENT ...
US$35M TO BE TRANSFER
envesiment@pnetmail.co.za
ESKOM HOLDINGS LIMITED(INVESTM...
ESKOM HOLDINGS LIMITED(BUSINES...
investment2011project@gmail.com
FROM ESKOM HOLDINGS(CONFIDENTI...
eskomsa@gmail.com
envestment2011@gmail.com
ESKOM HOLDINGS LIMITED(US$35M ...
paulmaroga2012@katamail.com
FROM ESKOM HOLDINGS LIMITED(UR...
pauljmaroga@webmail.co.za
ESKOM HOLDINGS LIMITED(URGENT...
ESKOM HOLDINGS LIMITED(PERSONA...
ESKOM HOLDINGS LIMITED(BUSINES...

Key

○ Phone Nr

● Subject

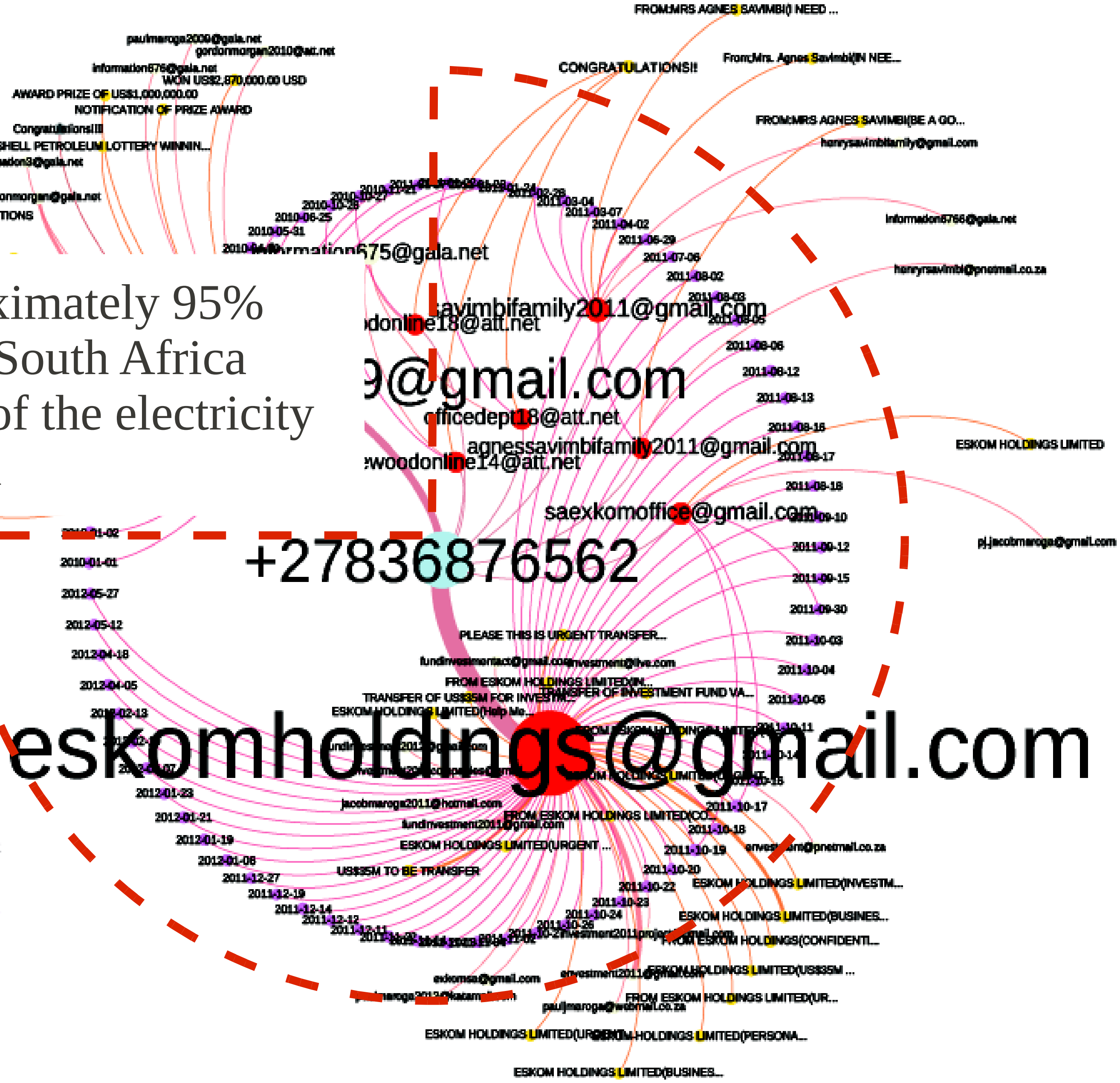
● From addr.

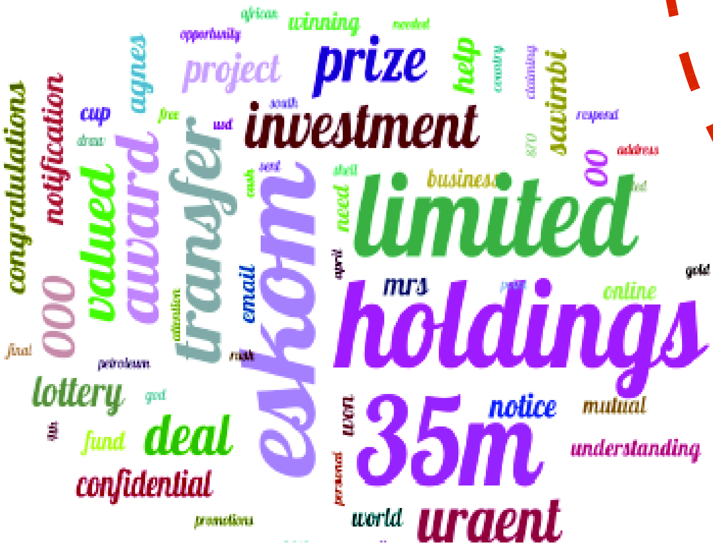
○ Reply addr.

● Dates

Eskom

“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

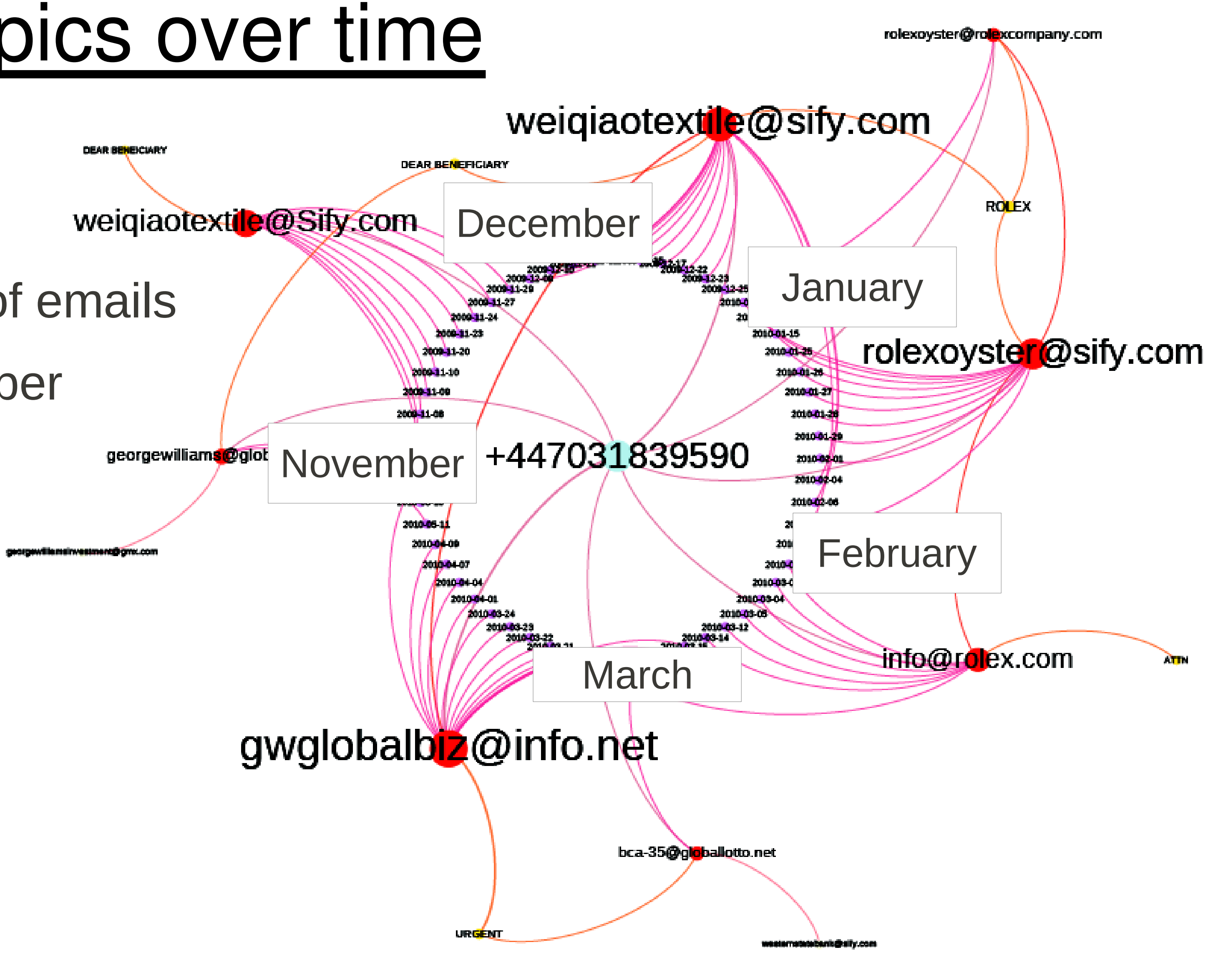
Main traits:

Topics change

Monthly package of emails

Single phone number

58 emails



Key

○ Phone Nr

● Subject

● From addr.

○ Reply addr.

● Dates

iPhone campaign

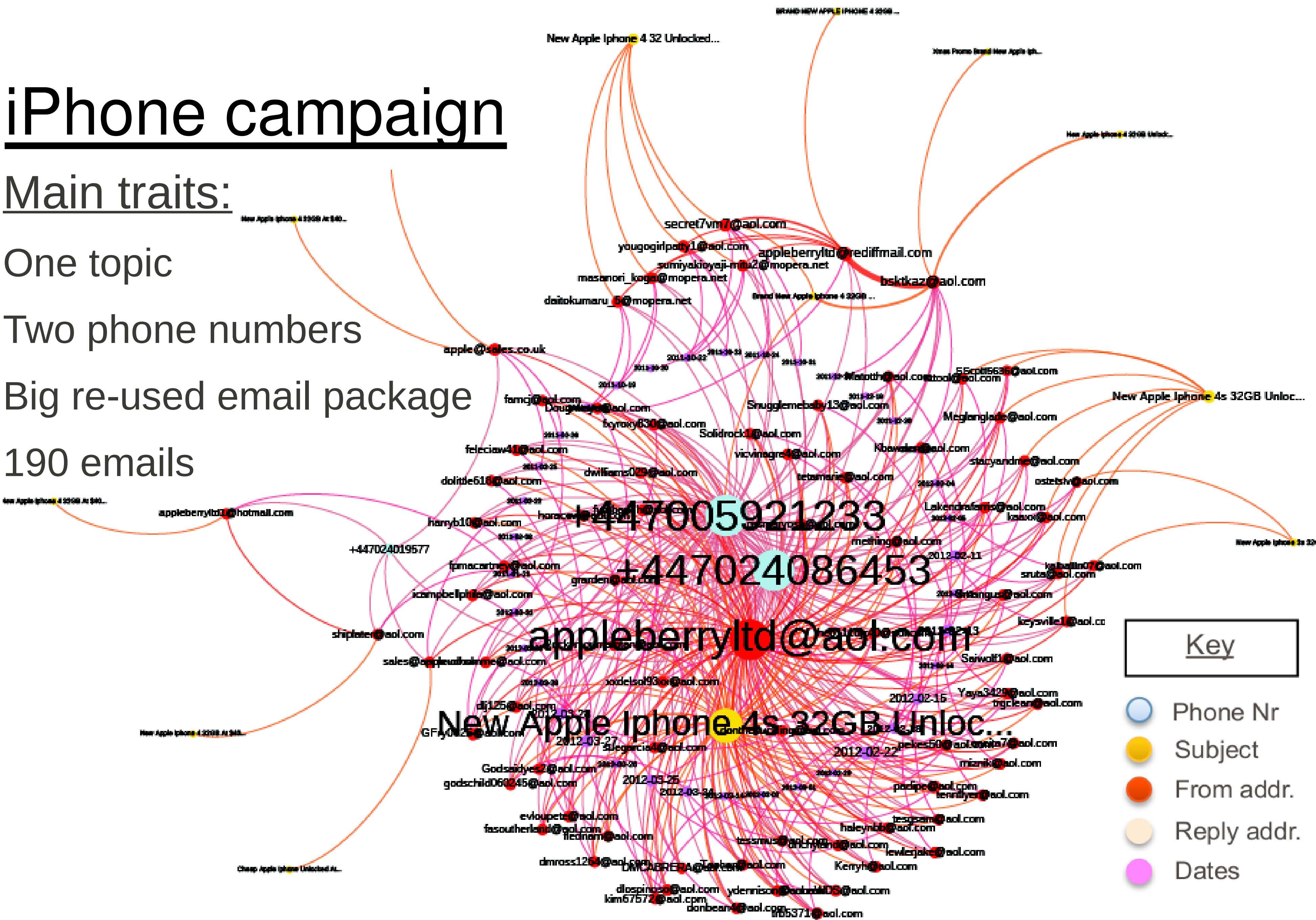
Main traits:

One topic

Two phone numbers

Big re-used email package

190 emails



Key

● Phone Nr

● Subject

● From addr.

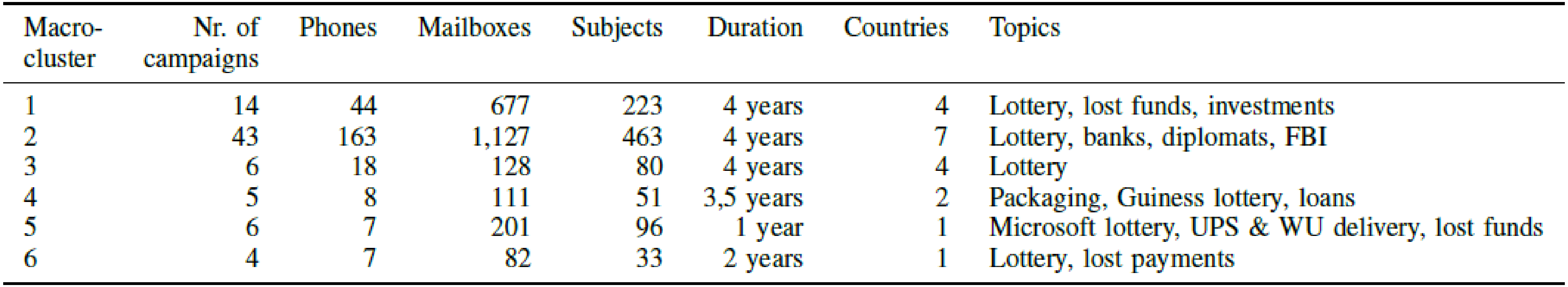
● Reply addr.

● Dates

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



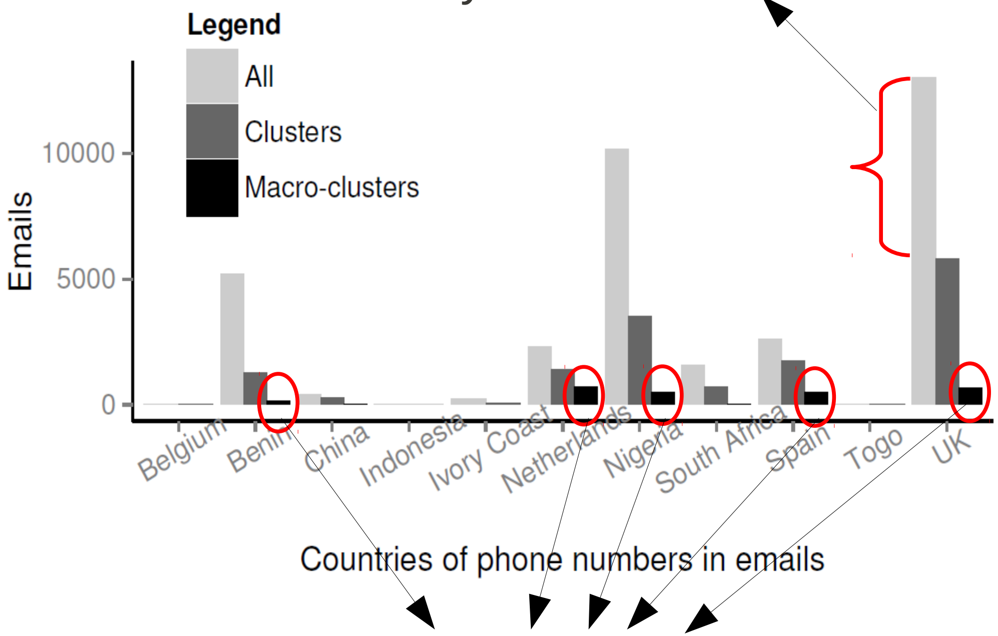
Macro-cluster	Nr. of campaigns	Phones	Mailboxes	Subjects	Duration	Countries	Topics
1	14	44	677	223	4 years	4	Lottery, lost funds, investments
2	43	163	1,127	463	4 years	7	Lottery, banks, diplomats, FBI
3	6	18	128	80	4 years	4	Lottery
4	5	8	111	51	3,5 years	2	Packaging, Guiness lottery, loans
5	6	7	201	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

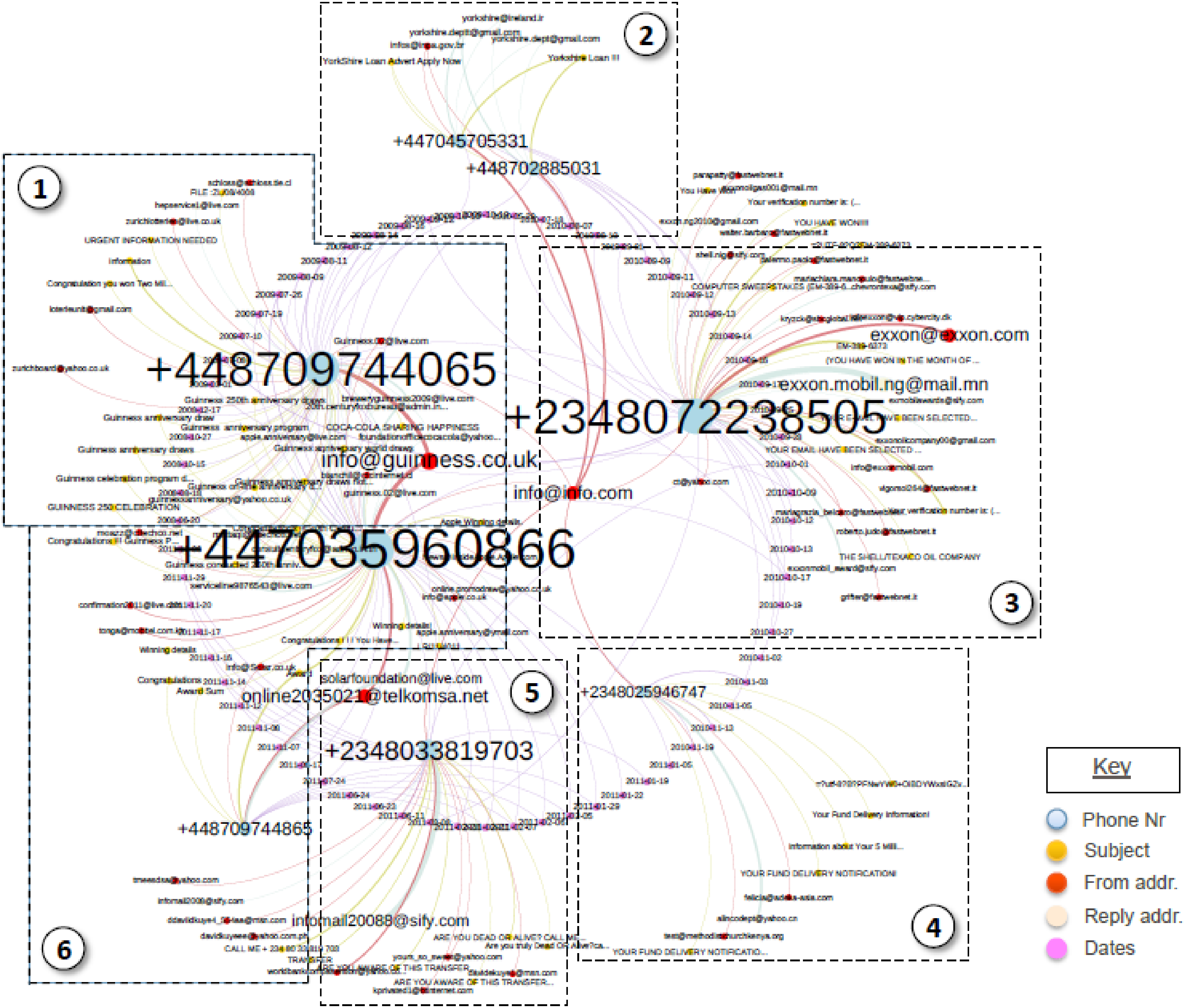
Clusters by countries

Unclustered:
stealthy or isolated scammers



Organized

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


1
2
3
4
5
6
+447045705331
+448702885031
+448709744065
+447035960866
+2348072238505
+2348025946747
+2348033819703
+448709744865
info@guinness.co.uk
info@info.com
exxon@exxon.com
exxon.mobil.ng@mail.mn
solarfoundation@live.com
online2035021@telkomsa.net
infomail20088@sify.com
yorkshire@ireland.ir
yorkshire.deptt@gmail.com
yorkshire.dept@gmail.com
YorkShire Loan Advert Apply Now
Yorkshire Loan !!!
URGENT INFORMATION NEEDED
Congratulation you won Two Mil...
Guinness 250th anniversary draws
Guinness anniversary draw
Guinness anniversary program
COCA-COLA SHARING HAPPINESS
Guinness anniversary draws
Guinness celebration program d...
GUINNESS 250 CELEBRATION
Apple Winning details
Winning details
COMPUTER SWEEPSTAKES
(YOU HAVE WON IN THE MONTH OF ...
YOUR EMAIL HAVE BEEN SELECTED ...
THE SHELL/TEXACO OIL COMPANY
YOU HAVE WON!!!
Your Fund Delivery Information!
Information about Your 5 Mill...
YOUR FUND DELIVERY NOTIFICATION
YOUR FUND DELIVERY NOTIFICATIO...
ARE YOU DEAD OR ALIVE? CALL ME...
Are you truly Dead Or Alive?ca...
ARE YOU AWARE OF THIS TRANSFER
ARE YOU AWARE OF THIS TRANSFER...
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?