The fight against SPAM

An Internet Number Resources Management Perspective

By

Amreesh D. Phokeer

04/12/2015

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Overview

1. Background
2. Statistics
3. Spam sources
4. Role of an RIR
5. Recommendations

AFRINIC 23

POINTE NOIRE

28 NOVEMBER - 4 DECEMBER

BACKGROUND

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Origin

spam – noun:
a canned meat product made mainly from ham

Meaning

spam – noun:

irrelevant or inappropriate messages sent on the Internet to a large number of recipients

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Well-known issue

- Multidimensional issue
- Started long time back
- ISOC, ITU, M3AAWG, IETF involved
- Many research initiatives
- Role of Regional Internet Registries (RIR)?

AFRINIC 23

POINTE NOIRE

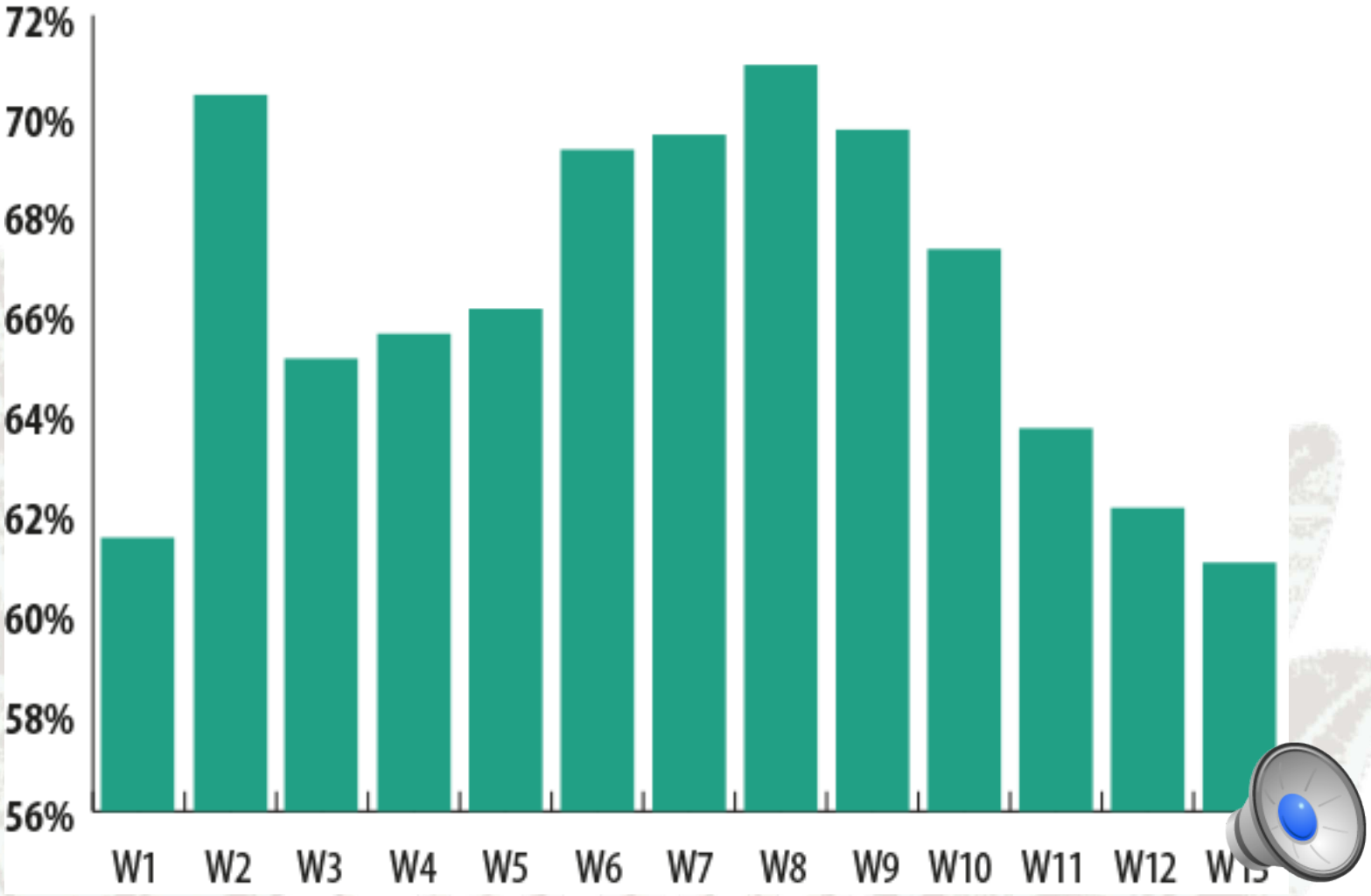
28 NOVEMBER - 4 DECEMBER

STATISTICS

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Spam and Phishing statistics Report Q1-2014

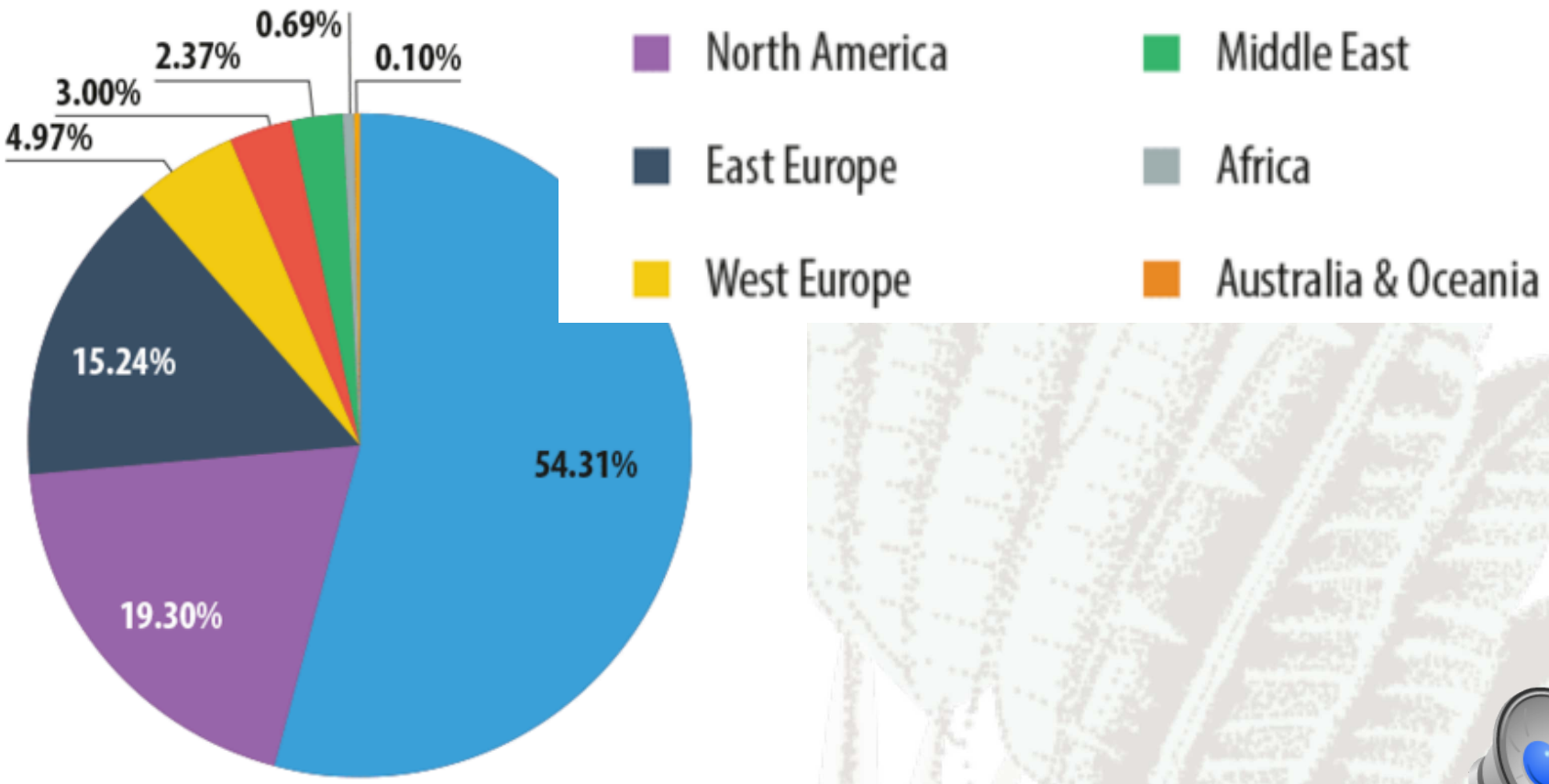
KASPERSKY lab



AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Global Spam Statistics

Statistic: Sources of Spam by Region

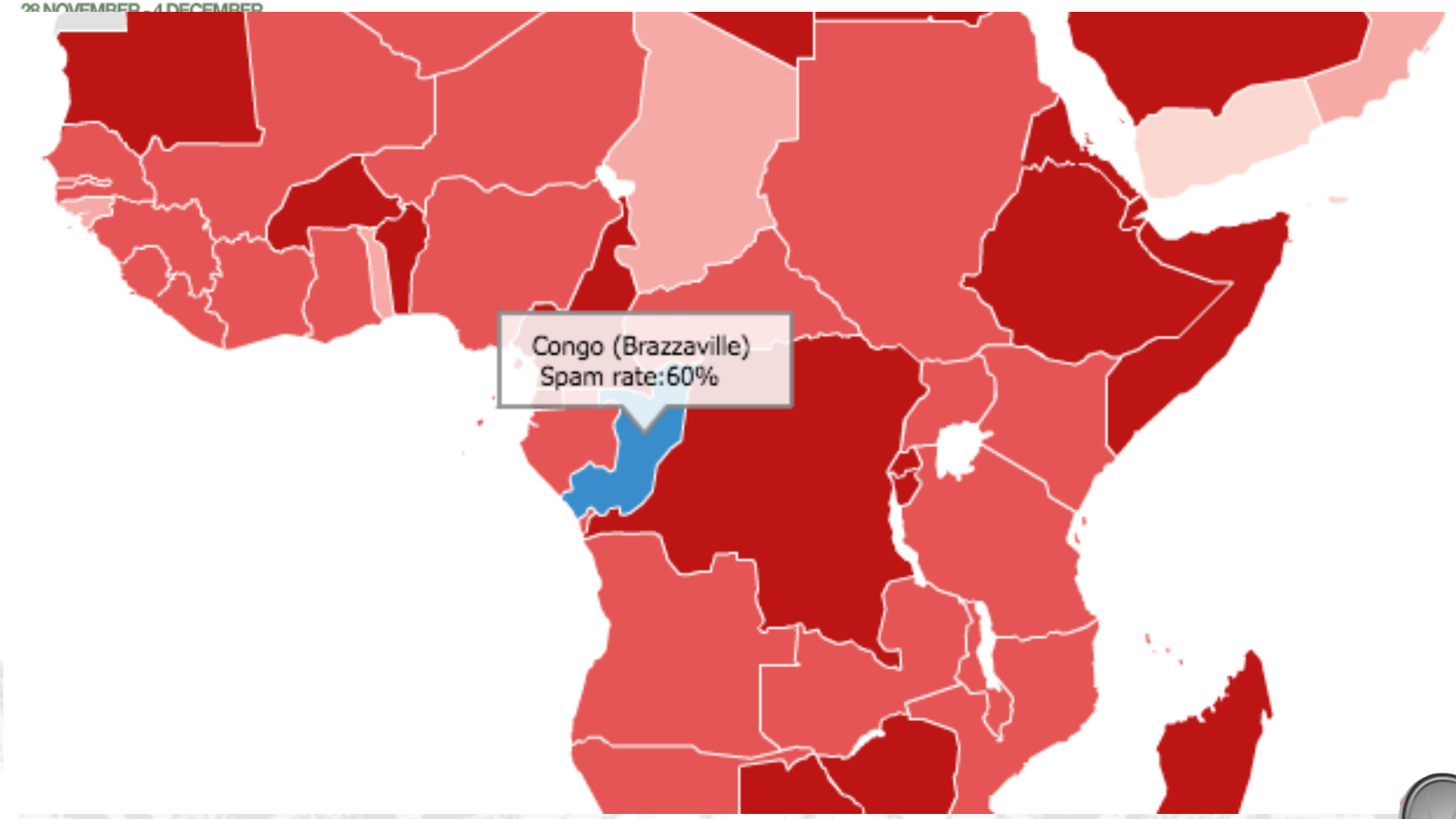


http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-20

AFRINIC 23 congo POINTE NOIRE

28 NOVEMBER - 4 DECEMBER

In the Republic of Congo



http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Some alarming figures

- 7 billion of mobile devices

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Some alarming figures

- 7 billion of mobile devices
- 3 billion of Internet users

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Some alarming figures

- 7 billion of mobile devices
- 3 billion of Internet users
- 115 billion emails per day

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Some alarming figures

- 7 billion of mobile devices
- 3 billion of Internet users
- 115 billion emails per day

90%+ of spam

AFRINIC 23 congo POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Top 20 worst countries by Infected networks

Country	Rate
Laos	6.60%
Mauritania	5.40%
Yemen	4.50%
Iraq	4.10%
Macedonia	4%
Myanmar	3.30%
Vietnam	3.20%
Somalia	3%
Congo	3%
India	3%
Togo	3%
Guinea	2.90%
British Indian Ocean Territory	2.90%
Libya	2.90%
Cape Verde	2.80%
Nigeria	2.80%
Turks and Caicos Islands	2.70%
Serbia	2.60%
Iran	2.40%
Armenia	2.40%

http://www.abuseat.org/nas.html

AFRINIC 23 Congo POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Top 20 worst countries
Spam Per Capita

Country	/capita
Monaco	1.24
Guam	0.846
Bermuda	0.755
Dominica	0.675
Djibouti	0.556
United States	0.446
Belize	0.376
Russian Federation	0.296
Armenia	0.276
Botswana	0.243
Canada	0.239
Mongolia	0.19
Montenegro	0.185
Suriname	0.183
Kyrgyzstan	0.173
Ukraine	0.166
Serbia	0.163
Bahamas	0.161
Romania	0.15

http://www.abuseat.org/nas.html

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Challenges

- Security threats
- Resources intensive
- Risk of being blacklisted

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

SPAM SOURCES

Sources of spam

- Open relays and proxies
- Insecure networks and hosts
- Botnets and zombies
- Direct spammers
- Hijacked prefixes
  - Spamhaus: 3.5 % of blacklists subnets are from AFRINIC

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

ROLE OF AN RIR

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Maintain a proper and up-to-date registry

- inetnum
- inet6num
- as-block
- aut-num
- as-set
- route
- route6
- route-set
- inet-rtr

- filter-set
- peering-set
- rtr-set
- domain
- mntner
- irt
- key-cert
- organisation
- role
- person

Registration of ASSIGNED PA

inetnum:	**197.157.255.0 - 197.157.255.255**
netname:	**CT-CORPORATE-BZV**
descr:	**Clients corporate Brazzaville**
country:	**CG**
admin-c:	**AT19-AFRINIC**
tech-c:	**AT19-AFRINIC**
status:	**ASSIGNED PA**
mnt-by:	**CongoTelecom-mnt**
changed:	**aymar.tsibayis@congotelecom.cg 20151201**
source:	**AFRINIC**
parent:	**197.157.252.0 - 197.157.255.255**

- Very important to keep information up-to-date
- Spam filters not to black list the parent space

AFRINIC 23 Congo POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Registration of ASSIGNED PA

- In Republic of Congo:
  - –11 LIRs with a “Allocated PA” space

AFRINIC 23 Congo POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Registration of ASSIGNED PA

- In Republic of Congo:
  - 11 LIR with a “Allocated PA” space
  - Only 3 LIRs have properly registered assignments, even if subnets are advertised

Abuse contact policy

- Earlier no standard way to add Abuse information
  - email attribute
  - notify attribute

- IRT object
  - Single object can be used referenced in inetnum(6) and aut-num objects

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Abuse contact policy

- Earlier no standard way to add Abuse information
  - email attribute
  - notify attribute

- IRT object

POLICY IS OPTIONAL

Reverse DNS(SEC)

- AFRINIC managed IANA delegated zones:
  - {196, 197, 154, 41, 102, 105}.in-addr.arpa
  - {0.c.2, 2.4.1.0.0.2, 3.4.1.0.0.2}.ip6.arpa
  - we register /24 and /16 reverse DNS from members
- PTR records are used by mail servers
- Register reverse DNS
- Enforced security
  - Signed your reverse DNS and publish DS records

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Route Hijacking

- Route hijacking: mechanism used by spammers
- Use reserved or un-allocated space (BOGON)
- How to protect your routes:
  - Keep BGP filters up-to-date using IRR
  - Start using RPKI and ROA and activate BGP filters based on route validation

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

RECOMMENDATIONS

AFRINIC 23
POINTE NOIRE
28 NOVEMBER - 4 DECEMBER

Conclusion

- Keeping records up-to-date
- Register customer ASSIGNMENTS
- Register Reverse DNS
- Use DNSSEC to protect zones
- Keep BGP filters up-to-date by registering your route objects
- Implement security mechanisms against route hijacking

AFRINIC 23

POINTE NOIRE

28 NOVEMBER - 4 DECEMBER

Thank you for your Attention

Questions?

twitter.com/ afrinic

flickr.com/ afrinic

facebook.com/ afrinic

linkedin.com/company/ afrinic

youtube.com/ afrinic media

www. afrinic .net