IST-Africa 2016 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2016
ISBN: 978-1-905824-55-7

A Survey of Anti-Spam Mechanisms and Their Usage from a Regional Internet Registry's Perspective

Amreesh PHOKEER[1], Alain AINA[2]
[1]*AFRINIC, Research and Innovation, 11th Floor Raffles Tower, Ebene, Mauritius*
Tel: +230 403 51 00, Fax: + 230 466 67 58, Email: amreesh@afrinic.net
[2]*TRSTECH, 867 Avenue du Calais, Nyekonakpoe, Lome, Togo*
Tel: +228 22 21 92 24, Fax: +228 22 21 92 24, Email: aalain@trstech.net

Abstract: This paper specifically deals with the different policies and technical frameworks at a Regional Internet Registry (RIR) level in terms of anti-spam measures. It also exposes the issue of spam from an Internet registry perspective, as an important element of the Internet technical infrastructure. We found out that, an RIR itself is not mandated to fight spam but it maintains a registry that is of paramount importance for traceability of Internet Number Resources ownership information. The paper starts with describing the challenges faced by operators followed by the different sources of spam. It then exposes the different mechanisms deployed by RIRs but importantly, this paper shows how those mechanisms either technical or policy-oriented are mostly underutilised, although they are operational. The latter is achieved by taking AFRINIC, the African RIR as case study.

Keywords: Spam, RIR, prefix hijacking, WHOIS, Reverse DNS, RPKI, policy

1. Objectives

The objectives of this paper are:

- Give the reader an overview of the different sources of spams
- Explain the importance of a Regional Internet Registry (RIR) as a provider of Internet-critical information and custodian of data.
- Expose the different mechanisms with regards to Internet number resources policy framework and other technical means available.
- Provide statistics about usage of those mechanisms by taking as case study the AFRINIC WHOIS database.

2. Introduction

The concept of 'spam' on the Internet is virtually known to every Internet user. The fight against spam is actually a worldwide issue as it has a negative effect on the Internet causing both technical and operational problems to network operators and users. It is therefore a nuisance and is also regularly used in criminal activities such as phishing and other types of fraud. Spamming started back in the days where email actually started and it initially took the form of chain letters [31]. Spamming techniques and medium have greatly evolved with the advent of cloud-based email and social media platforms. A study from Symantec on the state of spam shows that spam made up of more that 92% of all email messages [1]. This goes to show the severity of the issue.

This is why, after so many years, the fight against spam still remains a topic of great interest for both the technical community and policy-makers. Many stakeholders in the digital sphere have pulled hands together and came with joint-effort to fight spam, name ITU and ISOC [21]. The private sector also came up with the M3AAWG (Messaging Malware Mobile Anti-Abuse Working Group) [25]. The aim of this Working Group is to focus on operational issues of Internet abuse to fight botnets, malware, spam, viruses, DoS attacks through technology, industry collaboration and public policy.

2.1 – What is an RIR?

As a registry of Internet resources, an RIR operates at the network layer of the OSI model or more commonly at the Internet layer of the TCP/IP model. By virtue of its function, which is the allocation of Internet resources (IP addresses and AS number) at regional levels, RIRs have a direct link to operators at the network-level, which are the LIRs (Local Internet Registries) or End-users [34]. They all operate a network and can therefore potentially be a source of spam, as well as, victim of spammers.

2.2 – Defining a Spam

The exact definition of spam is something that has been subject to endless debates on many forums. Some feel that the implicit right to freedom of speech allows them to send any mails they wish. This however must be weighed up against the rights of the recipients. RFC2635 defines Spam as "transmission of bulk unsolicited emails"[2].

The definition of spam should largely be considered from the point of view of the recipient. Any mail that a recipient does not wish to receive can in many cases be considered as spam but there are some generally accepted characteristics of spam:

- Bulk volumes of messages sent to thousands of users who have never requested to be sent them.
- Messages that raise security concerns: Mail Bombing, Viruses, Phishing, Scams, ID Theft.
- Messages that negatively affect the operation of the networks in the methods that they are delivered.
- Mostly consisting of commercial, offensive or harmful content
- Sending of messages that are difficult to trace back to a sender

2.3 Challenges for Network Service Providers

Most of the challenges that service providers face with regards to spam are the same around the world. Security concerns, bandwidth consumption, overloading of computing resources, dissatisfied customers are all problems that are affecting networks across the globe [32]. Resource-constrained networks do sometimes feel the effect of these more strongly due to the bandwidth, computing and financial resource constraints on the continent and thus there is a requirement to be somewhat more careful with the approach to dealing with spam [33].

3. Sources of Spam

There is a wide variety of spamming techniques ranging from botnets using infected computers, the exploitation of unsecured networks, spamming through social network platforms or exploiting open relays and proxies [19]. In this section we will provide some information on two specific spamming sources, which more or less relate to the function of a Regional Internet Registry.

Table 1: Some Sources of Spam

Spam Source	Description
Botnets and Zombies	It is believed that the majority of the spam today comes from botnets or infected computers connected to the Internet. Those could be either servers at the operator level but importantly, they are typically computers found in home networks. Examples of botnets are Bobax, Grum or Pushdo [3]. The fact that they are usually located within the ISP's customer subnets, RIRs are usually used as an important source of information for abuse contact.
Direct spamming "419 scam"	One example of direct spamming is scam. Africa is well known for the "419 Scam" also called the "Nigerian Scam", where you receive an email saying that you won a lottery or you inherited a massive amount of money [4]. They usually request an up-front payment before releasing the sum. "419 Scams" not only use spoofed email addresses but make use of phishing techniques to lure people to fake website that would collect credit card information or bank login details.
IP Address hijacking	IP space hijacking is not a new phenomenon and has been a recurring issue over the years. Spammers can hijack spaces that have not yet been allocated (still in IANA pool) or they can use free/reserved space from an RIR pool. Unallocated spaces not registered in an RIR database and being advertised in the global routing are referred as *bogon* space [5]. Some spam filters will use *Bogons* database to fight spam but it is not always very efficient. The problem is that sometimes mail headers legitimately contain *Bogon* IPs for example, in case internal mail servers use public IPs in a private fashion. The history of the Internet is full of cases of IP hijacking, one very well known in the RIR community is the Pakistan Telecom-YouTube hijack [6]. Although the objective was not to do spamming but to rather blackhole traffic, the principle used was the same. The hijack was successful partly because of poor outbound BGP filtering but also because there were no hard security mechanisms deployed at a wide scale. Another aspect to consider is the fact that Internet routing is done "by rumour", meaning that hijacked spaces can easily find their way on the global routing tables.

4. Accurate Internet Number Resources Management

Anti-spam techniques can broadly be classified in two categories: either Content-based [16] or Reputation-based [17]. Examples of Content-based techniques are heuristic filtering, fingerprint based filtering or machine learning techniques. On the other hand, Reputation-based approaches would rather focus on parameters such as email origin, traffic flow and volume [18]. Depending on which side an email administrator is (End-user, sender or server side), different spam mitigation techniques apply.

It is important to understand that as a registry, an RIR has the obligatory duty to maintain an up-to-date database of information. As per the ICP-2 document on the criteria for the establishment of new RIRs from ICANN, RIRs must keep proper records of all registry activities [7]. As such, RIRs do not specifically operate any anti-spam mechanism but maintains a set of frameworks (either technical or policy based) that can be used as mitigating factors. Those are for example the Abuse Contact Information policy [8], the Reverse DNS service and related policies, the Internet Routing Registry (IRR) [10] and the Resource Certification framework (RPKI) [11].

4.1 Importance of the WHOIS Database

RIRs maintain a public database of Internet number allocation (Provider 'Aggregatable') and end-user assignments (Provider Independent) spaces. Local Internet Registries, for e.g. Internet Service Providers (ISP), also need to declare their sub-allocation and customer assignments in their respective RIR's WHOIS database. Besides Internet Numbers, which consist of IPv4, IPv6 and Autonomous Systems (AS) numbers, the WHOIS database holds many other data objects required for the operations of a network. Below are a list of the main objects from the AFRINIC WHOIS database.

Table 2: List of WHOIS Objects

Object	Description
inetnum	Object contains information on allocations and assignments of IPv4 address space.
inet6num	Object contains information on allocations and assignments of IPv4 address space.
aut-num	A database representation of an Autonomous System (AS)
domain	Domain name as specified in RFC 1034
mntner	Objects in the AFRINIC Database may be protected using mntner (pronounced "maintainer") objects.
irt	An irt object is used to define a Computer Security Incident Response Team (CSIRT).
organisation	The organisation class provides information identifying an organisation such as a company, charity or university, that is a holder of a network resource whose data is stored in the whois database.
Role	The role class is similar to the person class. However, instead of describing a human being, it describes a role performed by one or more human beings.
person	Contains information about technical or administrative contact responsible for the object where it is referenced.

As such, each object in the WHOIS database has a contact information in the form of either a PERSON object, a notify email address, a maintainer object and if the object is tied to an organisation, the “org” attribute.

```
aut-num:        AS37708
as-name:        AFRINIC-MAIN
descr:          AFRINIC MAIN AS
admin-c:        CA15-AFRINIC
tech-c:         IT7-AFRINIC
org:            ORG-AFNC1-AFRINIC
mnt-by:         AFRINIC-HM-MNT
mnt-lower:      AFRINIC-IT-MNT
mnt-routes:     AFRINIC-IT-MNT
mnt-irt:        IRT-AFRINIC-IT
source:         AFRINIC
```

Fig 1: Example of an Autonomous System (AS) Number

4.2 *Importance of Registering Customer Assignments*

Spam filters are built on information received from different sources such as Spamhaus [23]. Sometimes when a host or several hosts on a network are found to be spamming, the network gets blacklisted. The WHOIS database is used to retrieve information on those subnets, which are usually customer assignments. However, if an LIR fails to register its customer assignments in the RIR's WHOIS database, the only next information available would be the LIR network itself.

As a matter of best practice, it is therefore recommended for LIRs to register their end-user assignments, the reason being if a host in a non-registered subnet (for e.g. a /28) is blocked because it is involved in spamming activities, the whole subnet of the parent (for e.g. a /19) can be denied access.

It is therefore highly recommended for an ISP to register their customer assignments. In Africa, there was a policy proposal through the AFRINIC Policy Development Process to make the registration of customer assignments mandatory [30]. However, LIRs sometimes refrain from providing information on customer assignments, even though the address spaces are in use, as a matter of privacy.

4.3 Importance of Registering Reverse DNS

4.3.1 Reverse DNS Service

RIRs manage reverse DNS for the IANA delegated zones which are the *.in-addr.arpa for IPv4 and *.ip6.arpa for IPv6. For example, if a member was assigned a 196.1.5.0/24 network on which a mail server is running, the member needs to do the delegation of the 5.1.196.in-addr.arpa zone from its RIR, who manages the parent 196.in-addr.arpa zone.

> *IN-ADDR.ARPA Maintenance*
>
> *The regional registries will be responsible for maintaining IN-ADDR.ARPA records only on the parent blocks of IP addresses issued directly to the ISPs or those CIDR blocks of less than /16. Local IRs/ISPs with a prefix length of /16 or shorter will be responsible for maintaining all IN-ADDR.ARPA resource records for its customers. IN-ADDR.ARPA resource records for networks not associated with a specific provider will continue to be maintained by the regional registry.*

Fig 2: Section 5 of RFC2050

4.3.2 Importance of PTR Records

As a matter of best practice, even though RFC1033 and RFC1912 specify that "Every Internet-reachable host should have a name", rDNS has never become a protocol requirement for the operation of the DNS. Therefore, rDNS has always been considered as optional, explaining why not every host on the Internet today is mappable to a domain name. However, this technique is widely used by email servers to fight spam.

IP addresses assigned by an RIR are public IP address that will be used statically. Email operators that have used these static IPs need to properly configure the rDNS entries to make the match between the IP address and the domain name of the server. This also applies to home (dialup) users who are usually assigned dynamic IPs by their respective LIRs. Below are examples of PTR records to "whois.afrinic.net" domain name.

```
20.2.216.196.in-addr.arpa domain name pointer whois.afrinic.net.
0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.2.0.0.0.0.0.0.d.2.4.1.0.0.2.ip6.arp
a domain name pointer whois.afrinic.net.
```

Fig 2: Example of PTR Records

4.3.3 rDNS Check by Mail Servers

Reverse DNS (rDNS) is a mechanism used by mail servers to make the connection back the sender's PTR record if it has one. When an email server sends an email to another server, the receiver will check whether the IP of the domain name in the SMTP Banner has a corresponding PTR record. The receiving server will use this IP to check that the sender has a reverse DNS entry [12].

The downfall is that is that not all email service administrators will configure rDNS for their server. Legitimate emails coming from those servers might get rejected if the receiver has activated rDNS check [13].

4.4 Implementation of an Abuse Contact Policy (Case Study of AFRINIC)

Some RIRs, namely AFRINIC and the RIPE NCC have implemented an Abuse Contact Information policy. The policy stipulates that there must be a dedicated object in the WHOIS database to cater for abuse contact information.

Network owners increasingly operate dedicated abuse handling departments, distinct from the basic operations department. More and more network owners and other institutions are also starting to exchange data about abusive behaviour with each other, to more quickly allow networks to identify internal abuse, external abuse, and other security problems. Earlier, the abuse reports were sent to e-mail address specified in the e-mail field. These addresses were used because the RIR WHOIS Database currently did not have any specialised contact object for abuse departments. Instead, all abuse reports were sent to contacts that usually have broader responsibilities or different responsibilities.

If an IP address is found to be spamming, abuse reports are sent to e-mail address specified in the e-mail field of the object holding the prefix information. RIRs have therefore implemented a new object type called "irt" for Incidence Response Team. IRT objects provide information about a CSIRT (Computer Security Incident Response Team), which is basically a group of individuals responsible for handling network security incidents and reports for any given organization or entity.

The issue however, is that the "mnt-irt" is not mandatory. For instance at AFRINIC, the policy does not force its members to register an IRT object in their inetnum, inet6num and aut-num objects. The table below shows the number of IRT objects per object type in the AFRINIC WHOIS database (August 2015):

	Abuse contact information (e.g. remarks: Please send abuse to abuse@example.com)				**IRT object usage (e.g. mnt-irt: IRT-AFRINIC-IT)**	
Object Type	**Total in database**	**Number of objects with any abuse information**	**% over total in database**		**Number of objects with mnt-irt attribute**	**% over total in database**
IPv4	113111	12668	11.2		10	0.00
IPv6	1057	120	11.3		1	0.09
AS Number	1474	48	3.25		5	0.34
Total	115642	12836	11		16	**0.01**

Table 3: Statistics on Abuse Contact Information on AFRINIC WHOIS Objects

4.5 Resource Certification against Route Hijacking

Route hijacking is a complex issue that has been the headache of network operators for a long time. As mentioned earlier, routing on the Internet today is based on trust and mutual relationships between BGP peers. So far there has not been any largely accepted mechanism that uses hard security principles like digital signatures in order to make routing on the Internet more robust. RPKI (Resource Public key Infrastructure), together with BGPSEC [27] (still under development), are the frameworks being currently investigated as a global solution to secure the Internet Routing.

Internet Routing Registries (IRR) can also be used to mitigate the risk of route hijacking, though not really considered as a sustainable solution. There are around 30

Routing registries in the world [28], some of them operated by RIRs, others by private entities. Network operators can publish their routing policies online allowing other BGP speakers to create filters based on those policies. Currently, there is no way to validate the information on IRRs making the system a bit brittle. That is why eyeballs are currently on the RPKI framework as the next big step in routing security.

Resource Certification [11] is a security framework with makes use of a Public Key Infrastructure to certify resources that have been assigned to a member, through the delivery of a Resource Certificate. It adds a verifiable form of resource holdership. A Resource Certificate is based on the X.509 certificate format (RFC 5280), extended by RFC3779 to include Internet number resources (IPv4, IPv6 and AS number).

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
    Signature Algorithm:
sha256WithRSAEncryption
Issuer:
CN=AFRINIC/serialNumber=90A020F44F15B89D6FB15B5060D21067E43C0C0B
        Validity
            Not Before: May 15 06:59:27 2015GMT
            Not After : Mar 31 00:00:00 2016GMT
Subject:
CN=F365CA10AF/serialNumber=B883D77155F7D67BA69663FE59AB8FCE04300394
...
...
        sbgp-ipAddrBlock:critical
                IPv4:
                  196.1.0.0/24
                IPv6:
```

Fig 3: Example of an RPKI Certificate with Internet Resources

With a Resource Certificate, network operators can create cryptographic objects called Route Origin Authorization (ROA), which are signed by the certificate to bind a prefix to an Origin AS. ROAs become therefore the mechanism “par excellence” to prevent route hijacking as only prefix owners can verifiably say which AS is allowed to advertise its network.

```
version: 0
as_id: 37301
prefixes:
  146.64.10.0/24-24
signing certificate:
  serial:   7 (0x7)
  not before:   2015-06-11T08:42:09
  not after:    2015-06-26T08:42:09
  subject:  CN=557949f1-a786
  ski:      2e4427450ad7ecf6ad6b3b257a29b6547adb79c2
  g_ski:    LkQnRQrX7Patazsleim2VHrbecI
  sia:
    signedObject:
rsync://rpki.afrinic.net/repository/member_repository/F3634D22/24294C
20FADD11E49BBA825D3BB695CA/CA8EB9AE101511E5B100220DD949923A.roa
  issuer:   CN=F3634D22AR,
SN=FAFEBCF83FC94DF547DDAE1DF56495BDBCD2C192
  aki:      fafebcf83fc94df547ddae1df56495bdbcd2c192
  g_aki:    -v68-D_JTfVH3a4d9WSVvbzSwZI
```

Fig 4: Example of a Route Origin Authorization (ROA) Object

Relying party BGP speakers that are RPKI enabled, will create filters based on data received from RPKI Cache validator [15]. Then the router will tag every route announcement in its RIB as *valid*, *unknown* or *invalid*. An announcement is:

- **Valid** when it is covered by at least one ROA. (i.e AS in ROA matches Originating AS and prefix in ROA covers prefix announced)
- **Unknown** when no covering ROA has been found for the announcement.
- **Invalid** when a ROA covers the prefix announcement but the Originating AS does not match AS in ROA.

Below are some statistics about RPKI globally:

RIR	Total no. of route announcements	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	15370 (100%)	237 (1.54%)	5 (0.03%)	15128 (98.43%)	97.93%	1.57%
APNIC	156613 (100%)	3138 (2%)	1168 (0.75%)	152307 (97.25%)	72.88%	2.75%
ARIN	219008 (100%)	1785 (0.82%)	341 (0.16%)	216882 (99.03%)	83.96%	0.97%
LACNIC	76962 (100%)	14235 (18.5%)	673 (0.87%)	62054 (80.63%)	95.49%	19.37%
RIPE NCC	158548 (100%)	16550 (10.44%)	1168 (0.74%)	140830 (88.82%)	93.41%	11.18%

Table 4: RPKI Deployment in the AFRINIC Region

Furthermore, Spamhaus [29] maintains an "Extented/Don't Route Or Peer Lists" aka EDROP and DROP lists [23]. Those lists are advisory list of "hijacked networks" and being used by spammers or other cyber criminal to do illicit operations. These lists are mainly used by firewalls and routing equipments to drop traffic.

We used to EDROP list [24] to extract the number of subnets (/24) that are from AFRINIC region.

RIR	# of subnets in EDROP list (/24)	%	Referenced IRT objects	Subnets (/24) Covered by ROA
AFRINIC	94	3.5	0	None
APNIC	2486	92.5	-	None
ARIN	14	0.5	-	None
LACNIC	3	0.1	-	1
RIPE	100	3.7	-	2
Total	**2697**			

Table 5: Statistics from Spamhaus

The table above shows that 3.5% of hijacked space (in the EDROP list) is from AFRINIC. None of the space tagged as "hijacked" by Spamhaus have an IRT object referenced and none are covered by ROAs.

5. Conclusion

This paper gave an overview of the how RIRs contribute to the fight against spam globally. As mentioned, spam is a multidimensional problem that cannot be tackled from one perspective only. The policy measures and technical frameworks made available to the Internet community are only part of a global endeavour to combat spam. Many international institutions are also involved in this battle like the Internet Engineering Task Force (IETF) [20], the International Telecommunication Union (ITU) [21] and the Internet Society (ISOC) [22].

ISPs and network service providers need to correctly document their networks and publish their information in the WHOIS Database. RIR members must be made aware of the purpose of the data that is stored in the WHOIS database and the importance of its accuracy. Often when large blocks of IPs are blacklisted this is as a result of a failure to resolve the network abuse with the designated owner of the IP block. Network operators need to be made aware of their responsibilities for managing abuse of their networks by spammers (and other abusers). The consequences of failing to manage abuse of their networks can include blacklisting of their own and others networks and they should take responsibility for when they negatively affect users.

Apart from policy measures, RIRs maintain and manage different technical frameworks that are the Reverse DNS service, the Internet Routing Registry (IRR) and the Resource Certification (RPKI) system. While those frameworks should not be considered as the "ultimate anti-spam solutions", they must be viewed as mitigating measures. Altogether, those frameworks help build a more robust Internet infrastructure and therefore contributed to reduce the attack surface of spammers.

Some of the statistics available on usage shows that the systems in place are mostly under-utilised. Much effort has to be gathered to encourage members register their end-user assignments and create the corresponding abuse contact information objects, keep their objects up-to-date, register and sign their reverse DNS and to prevent prefix hijacking, start making use of the IRR and RPKI systems.

References

[1] Anon, (2016). [online] Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_09-2010.en-us.pdf [Accessed 8 Jan. 2016].

[2] J. Rosenberg, C. Jennings, Cisco, RFC5039, The Session Initiation Protocol (SIP) and Spam, January 2008.

[3] Z. Zorz, Help Net Security, [online] Available at: http://www.net-security.org/secworld.php?id=8599, [Accessed 8 Jan. 2016].

[4]Federal Bureau of Investigation, Common Fraud Schemes, [online] Available at: https://www.fbi.gov/scams-safety/fraud [Accessed 8 Jan. 2016].

[5] N. Feamster, J. Jung, H. Balakrishnan, MIT Computer Science and AI Laboratory, An Empirical Study of "Bogon" Route Advertisements, January 2005.

[6] M. Brown, Dyn Research, Pakistan hijacks YouTube, [online] Available at: http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/, [Accessed 8 Jan. 2016].

[7] ICANN, Criteria for Establishment of New Regional Internet Registries, June 2001. [online] Available at:
https://www.icann.org/resources/pages/new-rirs-criteria-2012-02-25-en, [Accessed 8 Jan. 2016].

[8] T. Knecht, AFRINIC Abuse contact Information Policy, May 2012. [online] Available at https://afrinic.net/en/library/policies/698-afpub-2010-gen-006, [Accessed 8 Jan. 2016].

[10] A. Toonk, How Accurate are the Internet Routing Registries, March 2009, [online] Available at http://www.bgpmon.net/how-accurate-are-the-internet-route-registries-irr/ [Accessed 8 Jan. 2016].

[11] M. Lepinski, S.Kent, IETF RFC6480, An Infrastructure to support Secure Internet Routing, February 2012.

[12] P. Srikanthan, CS Department, George Mason University, An overview of Spam Handling Techniques, 2003

[13] Spamhaus, Why should I worry about reverse DNS(rDNS), [online] Available at: http://www.spamhaus.org/faq/section/ISP%2520Spam%2520Issues#128, , [Accessed 8 Jan. 2016].

[15] R. Bush, R. Austein, IEFT RFC6810, The Resource Public Key Infrastructure (RPKI) to Router Protocol, January 2013

[16] W. Bin, P Wen-feng, Institute of Computing Technology, Chinese Academy of Sciences, A survey of Content-based Anti-spam Email Filtering, May 2005

[17] A. Ramachandran, N. Feamster, S. Vempala, Georgia Tech, ACM CCS 07, Filtering spam with behavioural blacklisting, 2007

[18] H.S. Alkahtani, P. Gardner-Stephen, R. Goodwin, King Faisal University, Saudi Arabia, Flinders University, Australia. A Taxonomy of Email Spam Filters, 2011

[19] Anon, (2016). [online] Open mail relay, WIKIPEDIA, Available at: https://en.wikipedia.org/wiki/Open_mail_relay, [Accessed 8 Jan. 2016].

[20] G. Lindberg, Chalmers University of Technology, IETF RFC2505, Anti-Spam Recommendations for SMTP MTAs, February 1999.

[21] Anon, (2016). [online] Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/SPAM.aspx [Accessed 8 Jan. 2016].

[22] The Internet Society, Combating Spam Project, [online] Available at: http://www.internetsociety.org/combating-spam-project, [Accessed 8 Jan. 2016].

[23] Spamhaus Don't Route or Peer Lists, [online] Available at: http://www.spamhaus.org/drop/ [Accessed 8 Jan. 2016].

[24] Spamhaus EDROP List, The Spamhaus Project. [online] Available at: http://www.spamhaus.org/drop/edrop.txt [Accessed 8 Jan. 2016].

[25] Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG). (online) Available at: https://www.m3aawg.org/ [Accessed 8 Jan. 2016].

[27] S. Bellovin, R. Bush, IETF RFC7353, Security Requirements for BGP Path Validation, August 2014.

[28] Merit, List of Routing registries, [online] Available at: http://www.irr.net/docs/list.html [Accessed 8 Jan. 2016].

[29] The Spamhaus Project, [online] Available at: http://www.spamhaus.org/ [Accessed 8 Jan. 2016].

[30] J.R. Houtomey, AFRINIC Policy, Mandatory requirements for registering assignments and sub-allocations, September 2014. [online] Available at: http://afrinic.net/fr/library/policies/archive/withdrawn-proposals/1215-mandatory-requirements-for-registering-assignments-and-sub-allocations [Accessed 8 Jan. 2016].

[31] Schwartz, Alan, Simson Garfinkel, and Debby Russell. Stopping spam. O'Reilly & Associates, Inc., 1998.

[32] Lyman, Jay. "Spam costs $20 billion each year in lost productivity." E-Commerce Times 29 (2003).

[33] Beverly, R. and Sollins, K., 2008. Exploiting transport-level characteristics of spam.

[34] Karrenberg, D., Gerard Ross, A.P.N.I.C., Paul Wilson, A.P.N.I.C. and Nobile, L., Regional Internet Registry.