AFRISPAM WORKING GROUP
Report
06/01/2008
afrispam@afrinic.net

Jean Robert HOUNTOMEY
Chair
hrobert@iservices.tg
Graham BENEKE
Co-Chair
graham-ml@apolix.co.za

Status of the document : DRAFT

Report

Context

On 2nd May 2007 at the AfriNIC-6 meeting in Abuja Nigeria, anti-spam BOF (birds of a feather) meetings aimed at addressing specific issues relating to spam on African networks.

Around July 2007 while blocking a source of spam, the whole netblock of 196.207.0.0/16 was blacklisted by UCEPROTECT Level 3. This affected several different entities in different geographical locations managing & administering smaller subnets within this range.

The urgent need for an action in the developing countries against spam was pointed out during the Internet governance and WSIS discussions.

Several regions are taking bigs steps and leaving Africa far behind.

The ITU is leading several meetings and discussions around the subject of "Countering spam"

The Interpol has set up an African Regional Working Party to look on issue related to Information Technology Crime point and they point out serveral actions.

Taking into consideration that African users and Network operators are already facing several problems including issues like bandwidth, access and education. Meanwhile there seems to be a lack of anti-spam initiatives in the AfriNic Service Region.

The AFRISPAM Working Group decided at the AfriNic 07 meeting in Durban has been charted:

1 - to identify the problems related to spam and fighting spams in the AfriNIC service Region

2 - to produce a report to AfriNic community at the AfriNic08 meeting

I. Background

The concept of 'spam' on the Internet is known to virtually every internet user. The fight against spam is a

worldwide issue.

Spam has a broad negative affect on the Internet causing technical and operational problems to network operators and users. It is a nuisance and is also regularly used in criminal activities such as phising and other fraud.

Spam is a huge consumer of both bandwidth and computational resources.
As a result it has a direct financial impact on the costs involved in running an Internet network.

Parts of the AfriNIC region have gained a bad reputation within the international community for being the source of a large amout of spam and fraudulant emails and have become permanently blacklisted.

Current statistics gathered from mail servers show that more than 80% of all SMTP message deliveries are spam. New trends for this to spread to other messaging platforms such as mobile devices and instant messengers are also evident.

No longer simply a mere nuisance, spam has become a serious problem for individuals and businesses alike as the clogging of networks and spreading of fraudulent schemes is having a direct financial impact on the economy.

I.1 What is 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.

The definition of spam should largly 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

I.2. Challenges for African Network operators

Most of the challenges that network operators face with regards to spam are the same around the world. Security concerns, bandwidth consuption, overloading of computing resources, disatisfied customers are all problems that are affecting networks across the globe.

African 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.

The biggest challenge that African network operators face is a lack of knowledge. The methods of sending spam are continuously evolving and changing and the only way to combat this is to be continuously updating the spam fighting techniques. The knowledge about these techniques needs to be effectively shared between operators to ensure that their networks are able to continue to function and it is in their best interests to be collaborating with other operators within each country and across the continent.

II- Recommendations.

While we agree that Spam is a much more serious issue in AfriNIC service region as it is a heavy drain on resources that are scarcer and costlier than elsewhere, we submit the following overview of recommendations :

II.1. Dealing with spam from an AfriNIC perspective:

One of the most common use of the AfriNIC whois database is in the tracking down of network abusers - primarilly senders of spam. ISPs and Network operators need to correctly document their networks and publish their information in the AfriNic Database.

AfriNIC 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 and others networks and they should take responsibility for when they negatively affect users.

II.2. Education initiatives:

Defining best practices for network operators, ISP and users. By defining what is considered to be acceptable behavior for Internet users within the region it becomes easier to identify when users fail to meet those requirements.

ISP Personnel need to be coming together to share experiences and techniques with each other. No training courses exist to teach operators how to deal with spam and the only way to gain this knowledge is through sharing and collaboration.

II.3. Responding to Abuse.

Formation of CSIRTs and CERTs - Computer Security and Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs). Operators must recognise the need to have staff

available and skilled in dealing with network abuse and these same staff should be in communication with similar staff at other organisations in order to effeciently deal with incidents when they arise.

II.4. Legal and collaboration issues

As the usage of the Internet in the region grows - so does the abuse of the Internet. Network operators must have Acceptable Usage Policies (AUPs) in place the require users to not abuse the Internet access services that they are purchasing. Operators need to make sure that users are aware of these AUPs and be educated about how they affect a users usage of the Internet.

Law makers within each country should be lobbied to implement laws that will make the acts of abusing the Internet and spamming into criminal offences. This provides the operators with a firm basis for dictating what users may use the networks for and should provide the network operators protection in enforcing these rules.

Co-operation at all levels - government, public sectors, private sectors, businesses. Spam is something that is now affecting many sections of society and all effected parties must be working together towards a common goal if they hope to ever overcome the issue. ISPs, ISP associations and associations of computer users should be leading this as they are in the best position to properly understand the issues.

II.5. User interaction

Organisations should be striving towards providing easily understandable educational material about spam for users. This should include issues such as identifying spam, tools and techniques for reducing the spam received and methods for users to complain about spams that are received.

Centralised spam reporting systems can make this process more user friendly and ISP asscosiations and consumer rights groups should consider how they can provide and effective channel for average users to resolve their complaints about spam received.

These considerations could be resumed in to 3 perspectives :

- Registry perspective
- Operational perspective
- Policies makers perspective