

# ARF – Abuse Reporting Format

- FeedBack Loops (FBLs) como método de aviso/queja desde ISPs u organizaciones receptoras de mensajes no deseados.
- Avisos por mal uso del correo electrónico (abusos).
- Generalmente dirigidos a:
  - ♦ ISP del usuario originario del mensaje
  - ♦ El propio usuario final (como JMRP de MSN)
- Beneficios:
  - ♦ Emisor: borrado de suscriptores, reputación IPs...
  - ♦ ISPs: robo de contraseñas, fallos web, mailings...
  - ♦ Usuarios: como forma de desuscripción automática

# ARF – Abuse Reporting Format

- Algunos servicios FeedBack Loops (FBLs):
  - ◆ AOL
  - ◆ MSN
  - ◆ SpamCop
  - ◆ Yahoo? (ReturnPath)
  - ◆ Comcast

- Ejemplo:

*Email: 4105891794@reports.spamcop.net*

*[ SpamCop V4.5.0.102 ] This message is brief for your comfort. Please use links below for details. Email from 82.194.X.X / 4 May 2009 10:29:27 +0200*

*<http://www.spamcop.net/w3m?>*

*i=z4105891794z28bad177cf5cdf62b36d9025ee21862z 82.194.X.X is open proxy, see: <http://www.spamcop.net/mky-proxies.html> [ Offending message ]*

## ■ ARF – Abuse Reporting Format

- ♦ Intención de estandarizar el formato de los FBLs
  - <http://mipassoc.org/arf/>
- ♦ Yakov Shafranovich primer *draft* en Abril 2005
- ♦ AOL, ha sido uno de los principales impulsores y de los primeros en adoptarlo
- ♦ Diseñado para soportar reportes por diferentes propósitos (de usuarios a sistema antispam, abusos...)
- ♦ El mensaje original se incluye como adjunto MIME
- ♦ Dividido en 3 partes:
  - Parte para lectura “humana”
  - Parte para lectura automática
  - Parte con el mensaje original
- ♦ En vez de todo el mensaje, se pueden incluir solo las cabeceras (recomendado no modificar el destinatario)

- Último *draft* publicado el 17 Abril 2009. Características:
  - ♦ MIME tipo "*multipart/report*" con *report-type="feedback-report"*
    - Primera parte "*text/plain*" con texto explicativos
    - Segunda parte "*message/feedback-report*"
    - Tercera parte "*message/rfc822*" o "*text/rfc822-headers*"
  - ♦ El asunto debe ser el del original o con "FW:" por delante
  - ♦ "*feedback-report*" como nuevo Content-Type y para definir una serie de campos:
    - Obligatorios:
      - Feedback-Type: por ej, "abuse"
      - User-Agent: programa y versión que hace los envíos
      - Version: versión de la especificación usada (0.1 → 1)
      - DKIM-Failure: tipo de verificación fallida
    - Opcionales:
      - Original-Envelope-Id, Original-Mail-From, Original-Mail-From, Reporting-MTA, Source-IP...

# ARF – Abuse Reporting Format

## ■ Ejemplo:

*Content-Type: multipart/report; boundary="\_-----=\_1241410897244100"; report-type="feedback-report"*  
*Date: Mon, 4 May 2009 06:21:37 +0200*  
*Subject: Abuse Report for IP 124.112.42.44: The Life changing experience Accai Berry*  
*From: Postmaster Hostalia <no-reply@hostalia.com>*  
*To: x@x*

*This is a multi-part message in MIME format.*

*-- \_-----=\_1241410897244100*  
*Content-Disposition: inline*  
*Content-Transfer-Encoding: 7bit*  
*Content-Type: text/plain*

*Dear Abuse Team,*

*You are receiving this e-mail because this account is the whois contact of 124.112.42.44.*

*This report is in Abuse Reporting Format; to see more about this (ARF), please read:*

*<http://www.mipassoc.org/arf/>*

*-- \_-----=\_1241410897244100*

# ARF – Abuse Reporting Format

*Content-Disposition: inline  
Content-Transfer-Encoding: 7bit  
Content-Type: message/feedback-report*

*Feedback-Type: abuse  
Version: 0.1  
Source-IP: 124.112.42.44  
Feedback-Agent: HOSTALIA ARF-AbuseReporter v0.1  
Received-Date: Mon, 4 May 2009 09:12:46 +0800*

*--\_-----=\_1241410897244100  
Content-Disposition: inline  
Content-Length: 677  
Content-Transfer-Encoding: binary  
Content-Type: message/rfc822*

*Received: from 44.42.112.124.broad.dynamic.hf.ah.cndata.com (unknown [124.112.42.44])  
Date: Mon, 4 May 2009 09:12:46 +0800  
From: "Rico Cates" <because55@albatross-voyages.com>  
Subject: The Life changing experience Accai Berry  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180  
X-Mailer: Microsoft Outlook Express 6.00.2900.2180*

*--\_-----=\_1241410897244100--*

# ARF – Abuse Reporting Format

Fecha	IPs listadas	Reportados	IPs delistadas
23-04-2009	6190	5330	89
24-04-2009	5961	4815	61
25-04-2009	6842	5656	2
26-04-2009	6342	5498	11
27-04-2009	7848	6665	40
28-04-2009	7653	6408	28
29-04-2009	9349	7858	43
30-04-2009	7608	5968	20
01-05-2009	9985	7078	11
02-05-2009	18798	13573	13
03-05-2009	14053	11254	15

## ■ Recursos:

- ♦ Web:
  - <http://mipassoc.org/arf/index.html>
  -
- ♦ Drafts:
  - <http://www.shaftek.org/publications/drafts/abuse-report/>
- ♦ Perl:
  - <http://wordtothewise.com/resources/ARF.pm.txt>
  - Email::ARF::Report