- MAAWG – Messaging Anti-Abuse Working Group
- Celebrado los días 10,11 y 12 de Junio en Heidelberg (DE).
- Conferencias y grupos de trabajo sobre abusos de correo electrónico, principalmente.
- Algunos de los asistentes:

  - AT&T
  - AOL
  - Cisco
  - Comcast
  - Yahoo
  - Spamhaus
  - Symantec
  - McAfee
  - Microsoft
  - Telefónica
  - Hostalia
  - RedIris
  - Euskaltel
  - La Caixa
  - Spamina

Alvaro Marín Illera <alvaro@hostalia.com>

- **ISP Close Colloquium**
  - Evento dirigido únicamente a ISPs
  - Mitigación de bots y diferentes medidas a usar:
    - Educación del usuario final
    - Detección rápida de bots
    - Alertas a usuarios afectados
    - Recomendaciones (Best Practices)
    - Abuse Help Desk efectivo
    - Walled gardens, como medidas de cuarentena
- **Métricas y tendencias** *(Symantec,IronPort)*
  - Incremento de spam : con URLs y de EEUU
  - Spam europeo a la baja
  - Web de SenderBase y sus funcionalidades
  - Abuso web2.0 (creación de cuentas, posts masivos...)
  - Reactor Mailer para el envío de spam
  - España, 30% de PCs que visitan malware => infectados

- **Reactor Mailer** *(IronPort)*
  - Demo de Reactor Mailer, software de la RBN.
  - Usa PCs infectados con *Srizbi*
  - 60% de IronPort recibido es generado por R.M.
  - TCP:3579 para web y TCP:4099 para gestión del bot
  - Web con templates, GD/Freetype...
  - Detección:
    - Tráfico hacia 208.72.168.0/23
    - HTTP sobre TCP:4099 (el mismo que AOL messenger)
    - GET y POST contienen *bot-serials* únicos
    - GET /g/[14 digitos para el *bot-serial*]-[4 dígitos para el *bot-version*]
    - Ya existen reglas en SpamAssassin
      - Cabecera Message-ID siempre empieza por 000
      - Diferencia entre versiones de OE en el mensaje
      - Hora siempre a UTC +000
    - Diferencias en HELO, espacios en comandos...etc entre OE y Srizbi
    - La pila TCP/IP tiene un *fingerprint* único

- **Prácticas actuales en la UE** *(1&1,Telenet,GmbH)*

  - 1&1 Imposibilidad de parar el 100% de spam saliente
    - → Necesidad de notificaciones de otros ISPs
    - → Cortar de raíz => parar intrusiones web

  - Telenet.be, 10 años filtrando puerto 25
    - → Clientes con malware multados
    - → Ratios a mensajes salientes

  - GmbH bloquea cuenta de PC *zombie* y redirigen a una web con información y utilidades para su desinfección.
    - → Servicio de aviso telefónico + honeypots para conseguir malware y estudiarlo.

- **Reputación** *(Bbiw.net, AOL y ReturnPath)*
  - Tendencia general para evitar spam
  - Basada en valores binarios para cálculo total
  - Recoger datos + fórmula + umbrales => acción
  - División a usuarios por grupos dependiendo de su lenguaje, tolerancia a spam, feedback...etc.

- **Prevención de altas fraudulentas** *(AT&T)*
  - Hosting => altas fraudulentas para *phishing* y spam
  - Chequeos CVV2 de tarjetas de crédito
  - GeoIP para detectar anomalías
  - Comprobar si dominio o IP origen en RBL o URIBL

- **DNSBL** *(ReturnPath)*
  - Comienzo en 1997. Hoy +700 listas públicas
  - Individualmente => 80%, Conjuntamente => 90/95%
  - Varias clasificaciones
    - Basadas en IP o dominio
    - Se obtiene “bueno” o “malo” o informativas
    - Subjetivas (“demasiado”) u objetivas (“malware”)
  - Lo más importante:
    - Publicar la política de la lista
    - Métodos para darse de baja fácilmente
  - El responsible es el administrador que la usa, no el creador de la lista.

- **Soporte de entrega de email** *(AOL,MS y KPN)*
  - KPN está haciendo pilotos con ARF para reportes a otros ISPs
  - AOL mostró su portal *postmaster.aol.com*
    - Docs, blog, Best Practices, Whitelisting, FBL, códigos de rechazo, callcenter...
  - MS (350mill de usuarios y 2'8mill de Ips/diarias) mostró *postmaster.msn.com*
    - JMRP para emisores masivos (12mil users)
    - SNDS para reputación de IPs (180mill de IPs)
    - SenderID
    - Bounces con códigos y descripciones mejoradas

- **Gestión de conexiones SMTP** *(AOL, MailChannels)*
  - Reducir costes de hardware
  - Filtrado en base a información histórica
  - Tiempo de espera de spammers menor (tiempo=$$)
    - → Realentizar tráfico SMTP haciendo pausas
    - → Conexiones establecidas crecen enormemente(20x)
      - Retardar por rangos, según país origen...
  - Configuración de políticas típicas:
    - → RBLs para con quien “no se quiere hablar”
    - → Rate Limit para “los amigos”
    - → 4xx o *traffic shaping* para clientes con pasado “dudoso”
  - Retroalimentaciones entre todos los sistemas