



Instituto  
Nacional  
de Ecología

# ***SpamAssassin para Qmail,***

***una herramienta de SL  
para el bloqueo de SPAM***

**Ing. Alejandro Escalante  
25 Noviembre 2004**

# ***Probablemente ha recibido una enorme cantidad de correo basura.....***

## **Cansado de borrar por dominio**



espacioterapeutico.com  
Flashmail.com  
unicum.de  
chat.ru  
mallku.net  
free-online.net  
mail-online.dk  
reply.pmO.net  
reply.mb0O.net  
amh.com.ve ...

## **Cansado de borrar por titulo**



Your password!  
Re: Your password!  
Vacaciones en Orlando  
ingles, hablemosingles  
GANESE  
Tusegurointernacional  
Live videos  
Gangbang ...

## ***Quizá es el momento de hacer algo en su institución. ¿Desea continuar recibiendo Spam?***

- ¿Existe algo más sencillo que definir reglas para cada mensaje?
- ¿Hay algún mecanismo que detecte Via gra, v1a gra vi@gr@?
- No dispongo de recursos necesarios \$\$\$ ¿Qué puedo hacer?
- ¿Es posible filtrar para todos mis usuarios?
- ¿Se puede rotular cada mensaje, mover a otra carpeta o borrar?
- Suena bien, pero ¿Cuál es su nivel de efectividad?, ¿Fácil de operar?
- Deberá de operar en tiempo cuasi-real

## ***¡Introducción a SpamAssassin!***

SpamAssassin™ es una herramienta que surge en el 2001 como una opción para el filtrado de correo SPAM, consiste en un mecanismo heurístico basado en reglas y ponderaciones predefinidas incorporados en un algoritmo bayesiano. Es una integración de elementos que combinan varias técnicas para la detección de SPAM. Originalmente Registrado por DeerSoft, posteriormente adquirido por Network Associates, actualmente opera bajo la Licencia Apache Software Foundation



**Sistema para el filtrado de correo SPAM**

## *Estadísticas globales en la detección de SPAM*

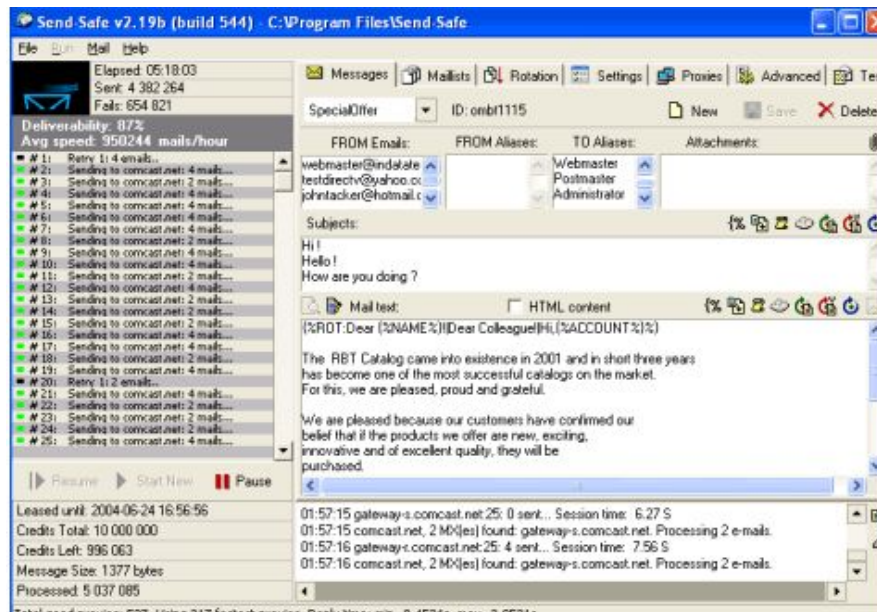
	DNSBLs	Comparación Frases	Heurístico (SA)	Estadístico
<b>Exactitud</b>	0 - 60%	80%	95%	99%+
<b>Falsos Positivos</b>	10%	2%	0.5%	0.1%



Justin Mason  
Creador de SA

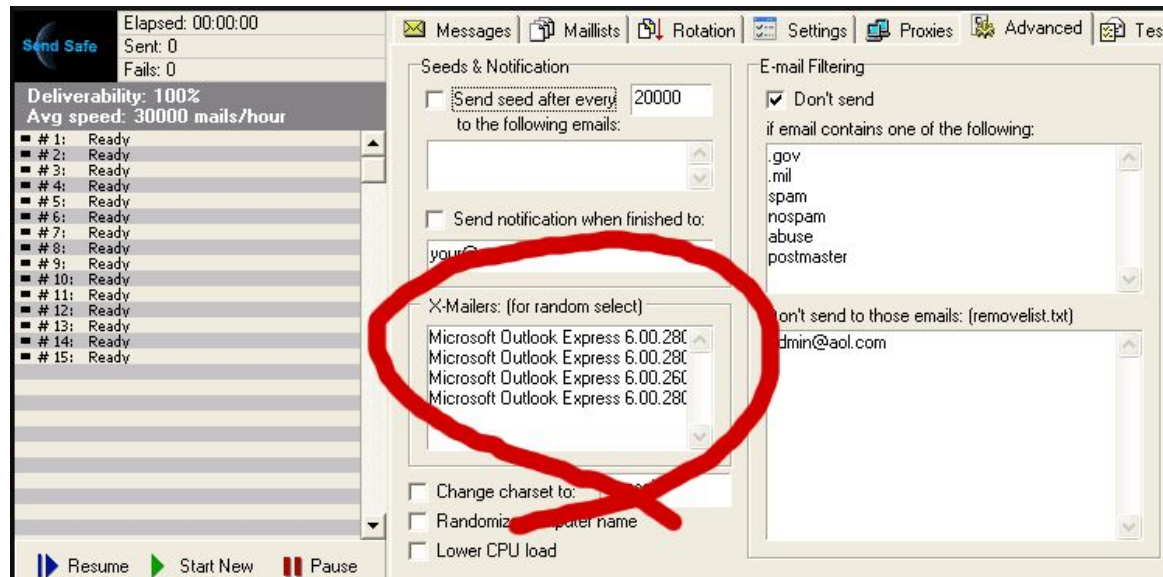
## Arquitectura de Spam Assassin

SA realiza un análisis de cada mensaje, aplicando una serie de **reglas predefinidas**, las cuales en conjunto son el corazón del sistema de detección. Aprovecha estas reglas rápidas para identificar el 95% de los mensajes y dado que la gran mayoría de los spammers no escriben su propio código y utilizan algún sistema abierto que adiciona encabezados, es relativamente sencillo identificar cuando se altera un mensaje



## Consideraciones iniciales, Spam Assassin

La reacción de algunos spammers ante el surgimiento de SA fue empezar a utilizar encabezados que simulaban ser legítimos durante el envío masivo de mensajes, por ejemplo desde Outlook Express



## *Las primeras reglas de filtrado*

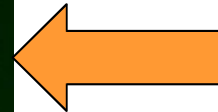
SA realiza un análisis en los encabezados o el cuerpo del mensaje para identificar coincidencias de patrones, (por ejemplo: Haga dinero fácil...), búsquedas de resolución de DNS (por ejemplo: sco.com, 127.0.0.1, etc) o también una verificación (checksum) del mensaje. Sin embargo aún en encabezados modificados, un mensaje correcto contiene un identificador válido único.

```
Message-ID: <00e601c4926f$468d5870$. . . .  
Message-ID: <008901c48e89$3efc91a0$. . . .  
Message-ID: <0b5301c49704$2741bee0$. . . .  
Message-ID: <006d01c493f3$c570da60$. . . .  
Message-ID: <002801c32fd1$5f6598f0$. . . .
```

## *Las primeras reglas de filtrado*

Aun Outlook Express incluye en forma automática un identificador para la fecha en el identificador de cada mensaje

```
Message-ID: <00e601c4926f$468d5870$. . . .  
Message-ID: <008901c48e89$3efc91a0$. . . .  
Message-ID: <0b5301c49704$2741bee0$. . . .  
Message-ID: <006d01c493f3$c570da60$. . . .  
Message-ID: <002801c32fd1$5f6598f0$. . . .
```

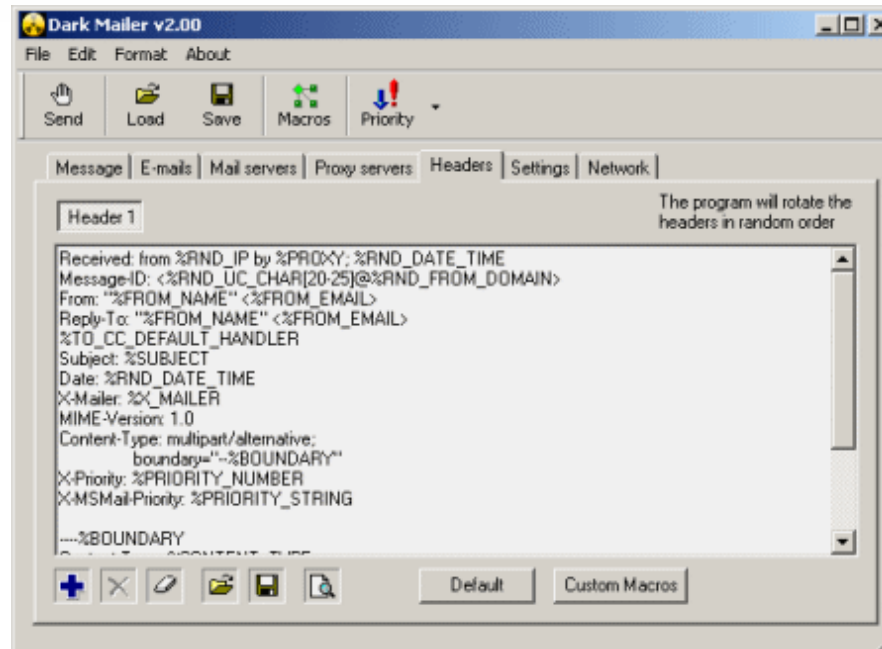


```
Message-ID: <0b5301c49704$2741bee0$. . . .
```

Se genera el identificador del mensaje y se compara, permite incorporar la regla **MSGID\_OUTLOOK\_INVALID** la cual detecta un 25% del spam.

## Características - Aleatorio

Existen programas que permiten utilizar una plantilla para el envío masivo de mensajes, incluyen mecanismos que toman algún valor del entorno



La regla **PERCENT\_RANDOM** permite identificar un 17% del spam

## Características – Verificación (Checksum)

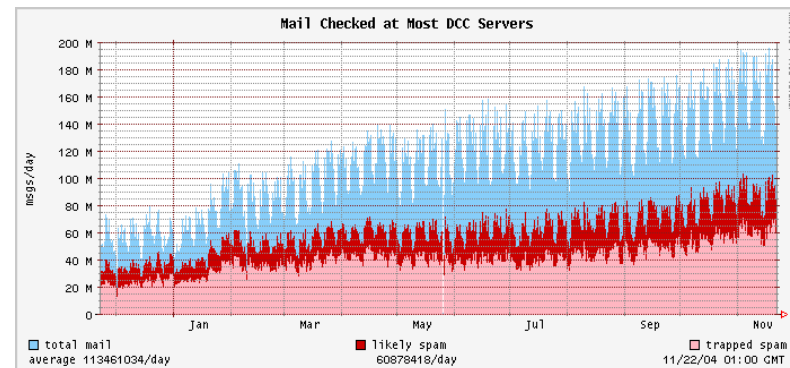
### Vipul Razor , Pyzor, DCC

Permiten revisar cuando un mismo mensaje se envía a una gran cantidad de sistemas o destinatarios, permite su detección al adicionar un encabezado o firma y compararlo con alguno de estos sistemas que manejan listas válidas (*Whitelists*). Se puede configurar SA para reportar a estos sistemas el envío de Spam.

Razor está escrito en Perl, mientras que Pyzor utiliza Python

**VIPUL'S  
Razor**

<http://razor.sf.net>.



Distribute Checksum Clearinghouse  
<http://www.dcc-servers.net/dcc/>

## **Características – Verificación (Checksum)**

### **...y si logran alterar las tablas de Hash?**

Esto se realiza al adicionar en forma aleatoria una cadena dentro del cuerpo del mensaje.

```
rtezkaehjx twyi  
OUR US DOCTORS WILL WRITE YOU A PRESCR1PTION FOR FREE!  
ddvtab eztua  
http://www.jtgxsezyk.com@www.oiadjdjist.biz/cf634/
```

## Características - Reglas

Se cuenta con una serie de reglas predefinidas que nos permitirán iniciar la ponderación del mensaje, por ejemplo:

- ★ *20\_porn.cf* indicadores de encabezados porno
- ★ *20\_dnsbl\_tests.cf* para las pruebas de Listas Negras DNS
- ★ *20\_phrases.cf* identifica frases para ser removido

Un mayor detalle en el título en mayúsculas, evaluando la función:

Encabezado	SUBJ_ALL_CAPS	eval:subject_is_all_caps( )
Descripción	SUBJ_ALL_CAPS	
Título en mayúsculas	score SUBJ_ALL_CAPS	0.550 0.567 0 0

## *Otras características*

Ninguna Regla, por si sola, puede marcar un mensaje como spam

SA también adiciona la posibilidad de aprender a clasificar mensajes en base a un grupo de carpetas en donde el usuario previamente han incluido **sus** mensajes basura (spam) y mensajes validos (ham). Esta operación le permite a SpamAssassin “**Aprender**” a identificar cada correo

Verdaderos Negativos (HAM)

Son aquellos mensajes en que el usuario y SA están de acuerdo en que no son spam. Adiciona el encabezado **X-Spam-Status** con la leyenda **NO** y **X-Spam-Checker-Version** con la versión utilizada por SA

Verdaderos Positivos (SPAM)

Son aquellos mensajes en que el usuario y SA están de acuerdo en que es spam, como mínimo adiciona los encabezados **X-Spam-Level**, **X-Spam-Status**, y **X-Spam-Flag**. Si se habilita la opción **rewrite\_subject** se adiciona en el titulo del mensaje **\*\*\*\*\*SPAM\*\*\*\*\***.



## ***Características para uso a gran escala, Uso de Spamd***

Interfaz Cliente-Servidor para SpamAssassin

Precarga, mucho mas rápido para grandes volúmenes

Puede cargar preferencias de usuario de una base de datos SQL

Puede hacer balanceo de carga

Utilizado en muchas organizaciones e ISP, Stanford Univ, SourceForge

## ¿Cómo se vé?

spam			
	De	Asunto	Recibido Tamaño
Fecha: Hoy			
✉	Cynthia	*****SPAM***** if you want real vicodin read this	Lunes 22/11... 4 KB
✉	-X@Ñ	*****SPAM***** u·Qa%4'D	Lunes 22/11... 5 KB
✉	Benita B...	*****SPAM***** oxycccontttin no script needeed	Lunes 22/11... 2 KB
✉	@ bay18-d...	*****SPAM*****	Lunes 22/11... 2 KB
✉	Joni Po...	*****SPAM*****	Lunes 22/11... 2 KB
✉	Therese...	*****SPAM***** Movies Still In Theaters, Mature Movies, Software, DVD, Music, X Box B	Lunes 22/11... 3 KB
✉	close-up	*****SPAM***** Dana has an amazing butt.	Lunes 22/11... 3 KB
✉	@ escaboy...	*****SPAM***** Deliver Mail (alex@insp.mx)	Lunes 22/11... 3 KB
✉	Thermo...	*****SPAM***** Pierda 10 kg por mes	Lunes 22/11... 4 KB
✉	@ noreply...	*****SPAM***** Thank you!	Lunes 22/11... 2 KB
✉	Carmen ...	*****SPAM***** Herald tribune article on pain relief ...	Lunes 22/11... 4 KB
✉	Camille ...	*****SPAM***** Beat The Market Today,.....Hot Pick!	Lunes 22/11... 18 KB
✉	Nathani...	*****SPAM***** how is my son needs hurting ' drink ...	Lunes 22/11... 3 KB
✉	hot girls	*****SPAM***** She loves milk squirting from her pu...	Lunes 22/11... 3 KB
✉	Josue Ri...	*****SPAM***** assist your daughter with her suffer...	Lunes 22/11... 3 KB
✉	Griffiths...	*****SPAM***** your girlfriend needs to cope with th...	Lunes 22/11... 2 KB
✉	¶W@ó¶U	*****SPAM***** ¢Ñ°Ú!!!\$AÁÚ; AÃ°°ªÁB¥d¶A¶Ú?	Lunes 22/11... 4 KB
✉	LA CERT...	*****SPAM***** 1ER JORNADA DE PROFESIONISTAS D...	Lunes 22/11... 11 KB
✉	@ webmas...	*****SPAM***** Re: mail delivery system <Esmtp:86...	Lunes 22/11... 78 KB
✉	@ conteni...	*****SPAM***** Status (alex@insp.mx)	Lunes 22/11... 2 KB
✉	Melissa	*****SPAM***** if you want real vicodin read this	Lunes 22/11... 4 KB
✉	ATM»È!;...	*****SPAM***** 24x¶@É¶U'Ú:£¥'L--À°±z¾ã;X-t¶...	Lunes 22/11... 8 KB
✉	???	*****SPAM***** e¥@¥Nª°\$AÁÚ:£· ³]-p°ó-¶¶Ú¶¶°°N...	Lunes 22/11... 3 KB
✉	Miles Al...	*****SPAM***** C.oa.deiane dirrrrrt cheap	Lunes 22/11... 2 KB
✉	@ la_brujit...	*****SPAM***** hi	Lunes 22/11... 2 KB
✉	@ pkt_sup...	*****SPAM***** Document	Lunes 22/11... 2 KB
✉	@ vicodinE	*****SPAM***** Re: important information	Lunes 22/11... 2 KB

\*\*\*\*\* SPAM\*\*\*\*\* if you want real vicodin read this

✉ Cynthia [prrrfect49@uronramp.net]

Para:

Save Over 50% On Your Prescription Drugs

If you are tired of spending a ton of money on your prescription medicine then you have found the right place. From our site you can

1. Order name brand right to your door
3. Save over 50% on your medicine that you buy from your local pharmacy now
4. No prior prescription is required to order from us

If saving money on something you need sounds good to you then [Click Here](#) to view our site. We offer over 100 of the prescription drugs you need so we will have what you want.

----133154929571896824--



## Mensaje 1

```
Return-Path: <benitabassettjx@asklinx.dircon.co.uk>
Delivered-To: alex@insp.mx
Received: (qmail 12802 invoked from network); 23 Nov 2004 04:59:42 -0000
Received: from unknown (HELO mcafee) (192.168.10.73)
  by correo.insp.mx with SMTP; 23 Nov 2004 04:59:42 -0000
Received: From ccowzb.de ([213.204.163.122]) by mcafee (webshield SMTP v4.5 MR1a
P0803.345);
  id 1101184986203; Mon, 22 Nov 2004 22:43:06 -0600
Message-ID: <OJGBDIOKEEPCKBKFADMNIEOCAA.benitabassettjx@asklinx.dircon.co.uk>
From: "Benita Bassett" <benitabassettjx@asklinx.dircon.co.uk>
To: acamarena@insp.mx,acruz@insp.mx,alantu@insp.mx,alex@insp.mx,btelle@insp.mx,
cenids@insp.mx
Subject: *****SPAM***** oxycccontttin no script needed
Date: Thu, 31 Jul 2003 06:49:50 +0000
MIME-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: base64
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on correo.insp.mx
X-Spam-Level: *****
X-Spam-Status: Yes, hits=5.5 required=3.0 tests=BAYES_44,DATE_IN_PAST_96_XX,
  HTML_50_60,HTML_MESSAGE,MIME_BASE64_TEXT,MIME_HTML_NO_CHARSET,
  MIME_HTML_ONLY,PORN_4 autolearn=no version=2.63
X-Spam-Report:
  * -0.0 BAYES_44 BODY: Bayesian spam probability is 44 to 50%
  * [score: 0.4985]
  * 0.1 HTML_MESSAGE BODY: HTML included in message
  * 0.3 MIME_HTML_ONLY BODY: Message only has text/html MIME parts
  * 0.1 HTML_50_60 BODY: Message is 50% to 60% HTML
  * 1.0 MIME_BASE64_TEXT RAW: Message text disguised using base64 encoding
  * 0.6 MIME_HTML_NO_CHARSET RAW: Message text in HTML without charset
  * 1.9 PORN_4 URI: URL uses words/phrases which indicate porn
  * 1.5 DATE_IN_PAST_96_XX Date: is 96 hours or more before Received: date
```



## Mensaje 2

```
Return-Path: <fortaleza172-sol@yahoo.com.br>
Delivered-To: alex@insp.mx
Received: (qmail 6442 invoked from network); 23 Nov 2004 01:31:26 -0000
Received: from unknown (HELO mcafee) (192.168.10.73)
  by correo.insp.mx with SMTP; 23 Nov 2004 01:31:26 -0000
Received: From locaweb.com.br ([201.1.136.133]) by mcafee (webshield SMTP v4.5 MR1a P0803.345);
  id 1101172478312; Mon, 22 Nov 2004 19:14:38 -0600
From: "Thermogreen" <fortaleza172-sol@yahoo.com.br>
To: Para la persona mas importante del mundo: usted
Subject: *****SPAM***** Pierda 10 kg por mes
MIME-Version: 1.0
Content-Type: text/html
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on correo.insp.mx
X-Spam-Level: ***
X-Spam-Status: Yes, hits=3.6 required=3.0 tests=BAYES_20,DATE_MISSING,
  HTML_70_80,HTML_FONTCOLOR_BLUE,HTML_FONT_BIG,HTML_IMAGE_ONLY_04,
  HTML_MESSAGE,MIME_HTML_NO_CHARSET,MIME_HTML_ONLY,TO_MALFORMED
  autolearn=no version=2.63
X-Spam-Report:
* 1.9 DATE_MISSING Missing Date: header
* 0.6 TO_MALFORMED To: has a malformed address
* 0.1 HTML_FONTCOLOR_BLUE BODY: HTML font color is blue
* 0.1 HTML_MESSAGE BODY: HTML included in message
* 0.3 HTML_FONT_BIG BODY: HTML has a big font
* 0.1 HTML_70_80 BODY: Message is 70% to 80% HTML
* 0.3 MIME_HTML_ONLY BODY: Message only has text/html MIME parts
* 1.0 HTML_IMAGE_ONLY_04 BODY: HTML: images with 200-400 bytes of words
* -1.4 BAYES_20 BODY: Bayesian spam probability is 20 to 30%
  [score: 0.2262]
* 0.6 MIME_HTML_NO_CHARSET RAW: Message text in HTML without charset
```

## Mensaje 3

```
Return-Path: <noreply@paypal.com>
Delivered-To: alex@insp.mx
Received: (qmail 27782 invoked from network); 23 Nov 2004 00:35:50 -0000
Received: from unknown (HELO mcafee) (192.168.10.73)
  by correo.insp.mx with SMTP; 23 Nov 2004 00:35:50 -0000
Received: From insp.mx ([200.23.251.86]) by mcafee (webshield SMTP v4.5 MR1a P0803.345);
  id 1101169154609; Mon, 22 Nov 2004 18:19:14 -0600
From: noreply@paypal.com
To: alex@insp.mx
Subject: *****SPAM***** Thank you!
Date: Mon, 22 Nov 2004 16:13:57 -0800
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary="-----_NextPart_000_0016-----_NextPart_000_0016"
X-Priority: 3
X-MSMail-Priority: Normal
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on correo.insp.mx
X-Spam-Level: ****
X-Spam-Status: Yes, hits=4.4 required=3.0 tests=BAYES_10,MIME_BOUND_NEXTPART,
  MIME_MISSING_BOUNDARY,MISSING_MIMEOLE,NO_REAL_NAME,PRIORITY_NO_NAME
  autolearn=no version=2.63
X-Spam-Report:
  * 0.2 NO_REAL_NAME From: does not include a real name
  * -0.9 BAYES_10 BODY: Bayesian spam probability is 10 to 20%
  * [score: 0.1131]
  * 1.8 MIME_MISSING_BOUNDARY RAW: MIME section missing boundary
  * 1.6 MISSING_MIMEOLE Message has X-MSMail-Priority, but no X-MimeOLE
  * 0.5 MIME_BOUND_NEXTPART Spam tool pattern in MIME boundary
  * 1.2 PRIORITY_NO_NAME Message has priority setting, but no X-Mailer
```



## Mensaje 4

```
Return-Path: <mjftxbjwq@excite.com>
Delivered-To: alex@insp.mx
Received: (qmail 11411 invoked from network); 22 Nov 2004 22:54:56 -0000
Received: from unknown (HELO mcafee) (192.168.10.73)
  by correo.insp.mx with SMTP; 22 Nov 2004 22:54:56 -0000
Received: From dsl-201-128-47-221.prod-infinitum.com.mx ([201.128.47.221]) by mcafee (webshield SMTP
v4.5 MR1a P0803.345);
  id 1101163100203; Mon, 22 Nov 2004 16:38:20 -0600
Received: from 140.12.162.128 by 201.128.47.221; Mon, 22 Nov 2004 23:37:41 +0100
Message-ID: <BJSETVOQSDBNMIMHLUJPPPF@mailexcite.com>
From: "hot girls " <mjftxbjwq@excite.com>
Reply-To: "hot girls " <mjftxbjwq@excite.com>
To: abperez@insp.mx, alex@insp.mx, btelle@insp.mx, calvarado@insp.mx, cenids@insp.mx, crics@insp.mx
Subject: *****SPAM***** She loves milk squirting from her pussy.
Date: Mon, 22 Nov 2004 20:43:41 -0200
X-Mailer: Microsoft Outlook, Build 10.0.2616
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="--477449194551957214"
X-Priority: 3
X-MSMail-Priority: Normal
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on correo.insp.mx
X-Spam-Level: *****
X-Spam-Status: Yes, hits=10.2 required=3.0 tests=BAYES_60,FORGED_MUA_OUTLOOK,
  FORGED_OUTLOOK_TAGS,HTML_60_70,HTML_IMAGE_ONLY_02,HTML_MESSAGE,
  MIME_HTML_NO_CHARSET,MIME_HTML_ONLY,MIME_HTML_ONLY_MULTI,
  MISSING_MIMEOLE autolearn=no version=2.63
X-Spam-Report:
* 0.1 HTML_60_70 BODY: Message is 60% to 70% HTML
* 1.6 BAYES_60 BODY: Bayesian spam probability is 60 to 70%
* [score: 0.6282]
* 0.1 HTML_MESSAGE BODY: HTML included in message
* 0.3 MIME_HTML_ONLY BODY: Message only has text/html MIME parts
* 1.2 HTML_IMAGE_ONLY_02 BODY: HTML: images with 0-200 bytes of words
* 0.6 MIME_HTML_NO_CHARSET RAW: Message text in HTML without charset
* 1.6 MISSING_MIMEOLE Message has X-MSMail-Priority, but no X-MimeOLE
* 1.0 FORGED_OUTLOOK_TAGS Outlook can't send HTML in this format
* 1.1 MIME_HTML_ONLY_MULTI Multipart message only has text/html MIME parts
* 2.6 FORGED_MUA_OUTLOOK Forged mail pretending to be from MS outlook
```

## ***Instalación***

**SA** se escribió para entornos basados en Unix que incluyan Perl, de preferencia 5.6.1 o recientes. Se requieren los módulos *ExtUtils::MakeMaker*, *File::Spec*, *Pod::Usage*, *HTML::Parser*, *Sys::Syslog*, *DB\_File*, *Digest::SHA1*, y *Net::DNS*. Se pueden consultar tres sitios de referencia *Vipul's Razor* (<http://razor.sourceforge.net>), *Pyzor* (<http://pyzor.sourceforge.net>), y *DCC* (<http://www.rhyolite.com/anti-spam/dcc/>)

```
# perl -MCPAN -e shell
cpan> o conf prerequisites_policy ask
cpan> install Mail::SpamAssassin
```

Se puede descargar y configurar manualmente de <http://www.spamassassin.org>

```
$ gunzip -c Mail-SpamAssassin-3.0.1.tar.gz | tar xf -
$ cd Mail-SpamAssassin-3.0.1
$ perl Makefile.PL
$ make
# make install
```

## ***Instalación - Continuación***

Para los usuarios de Debian, Gentoo o compatibles con apt-get

```
# apt-get install spamassassin
```

Otra opción es descargar y compilar el fuente RPM

```
# rpm -Uvh spamassassin-3.0.1.src.rpm
```

```
# cd /usr/src/redhat/SPECS
```

```
# rpm -bb spamassassin.spec
```

```
# cd ../RPMS/i386
```

```
# perl-Mail-SpamAssassin-3.0.1.i386.rpm spamassassin-tools-3.0.1.i386.rpm
```

```
# rpm -Uvh Perl-Mail-Spam*rpm spamassassin*3.0.1*.rpm
```

## ***En suma - ¿Qué se instaló?***

- Módulos de Perl
- Conjunto de reglas básicas
- Archivo de configuración local
- spamassassin
- spamd (demonio residente memoria)
- spamc (cliente)
- sa-learn (sistema aprendizaje)

## ***Integración – Sistemas de Correo***

Se diseño pensando en su flexibilidad e integración con varios Agentes de Transferencia de Correo MTA (Sendmail, Qmail, Exim, Postfix, Microsoft Exchange)

Integración dentro de plugins para scanner de virus (MIMEDefang, amavisd)

Proxies y clientes IMAP/POP3

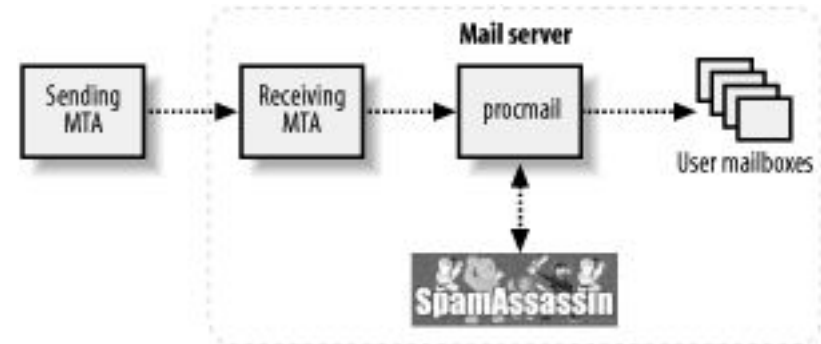
Plugins comerciales para clientes de Windows (Eudora, MS Outlook)

WebMail (Horde, Openwebmail, etc.) y mas que no conozco!

## Invocando SA con - Procmail

Procmail es sistema de procesamiento que acepta mensajes como entrada estándar y aplica una serie de reglas o acciones para la entrega de mensajes

```
/etc/procmailrc  
DROPPRIVS=yes  
PATH=/bin:/usr/bin:/usr/local/bin  
SHELL=/bin/sh  
# Spamassassin  
:0fw  
<300000  
|/usr/bin/spamassassin
```



*Integrando SA con Procmail*



## ***Integrando SA con - Qmail***

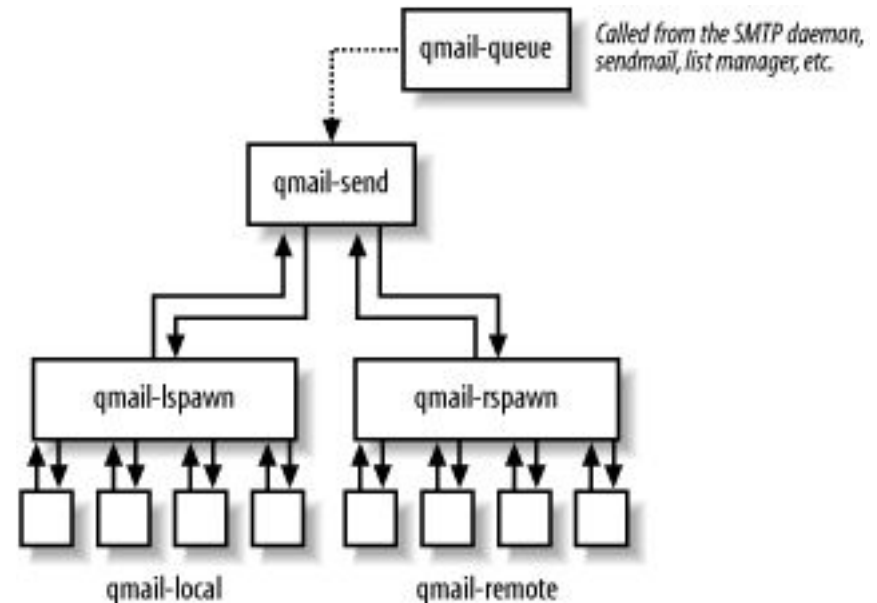
Qmail es un agente de transporte de correo escrito por el investigador en criptografía Dan Bernstein y diseñado para proveer un sistema de correo de alta seguridad. Consiste en varios componentes, cada uno de ellos corre con el mínimo de privilegios.

Qmail incluye una cantidad compleja de componentes, esta presentación no cubre la configuración, operación y seguridad de Qmail. Aspectos referentes al manejo de seguridad se pueden consultar en el sitio de David Sill's, Mi vida con Qmail, <http://www.lifewithqmail.org>, el libro de consulta de Qmail, Ed. Apress o Qmail de John Levine , Ed. O'Reilly

## Operación - Qmail

A cada componente de Qmail le corresponden diferentes roles en la recepción de mensajes desde Internet. Los mensajes típicamente entran vía el demonio **qmail-smtpd**, el cual escucha el puerto 25 y conduce la transacción SMTP con el remitente remoto. **Qmail-smtpd** pasa el mensaje al programa **qmail-queue**, quién lo almacena en una cola de salida para un procesamiento futuro.

El demonio **qmail-send** lee los mensajes en la cola de salida e intenta entregarlos utilizando el demonio **qmail-lspawn** (que pasa el mensaje a **qmail-local** para envíos locales) o el demonio **qmail-rspawn** (que pasa el mensaje a **qmail-remote** para envíos a servidores remotos)



## Revisión de Spam- Entrega Local

La forma mas sencilla de integrar Qmail con SpamAssassin consiste en redirigir los mensajes a través de SA durante el proceso de entrega local. Las ventajas que se obtienen son:

- Fácil integración
- Se puede correr **spamd** y procesar rápidamente con **spamc**
- Permite utilizar preferencias de usuario, listas personales, y reglas almacenadas en SQL.

Sin embargo su principal desventaja es que solamente tiene alcance en las entregas locales.

Si se desea filtrar la entrega local bastará con modificar el archivo **/var/qmail/control/defaultdelivery**, el cual especifica si se entrega cada mensaje en un directorio (./Maildir/ ) o a un archivo (.Mailbox), por la línea:

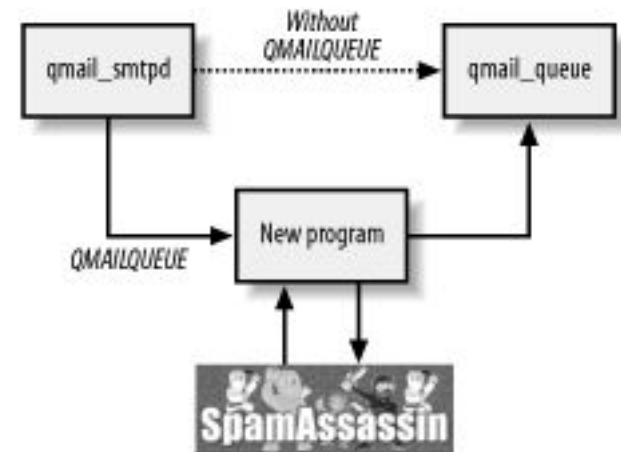
```
| /usr/bin/spamc | maildir ./Maildir/
```

## Revisión de Spam- todo el correo entrante

Si se desea configurar un mecanismo para revisar todos los recipientes tanto locales como remotos, se necesita realizar una verificación cuando el correo es recibido y antes de la entrega final. Qmail provee esta capacidad a través de un parche en **qmailqueue**, el cual es incluido en la distribución de qmail.

Para verificar si se cuenta con el parche

```
# cd /var/qmail/bin  
# strings qmail-smtpd | grep QMAILQUEUE  
QMAILQUEUE
```

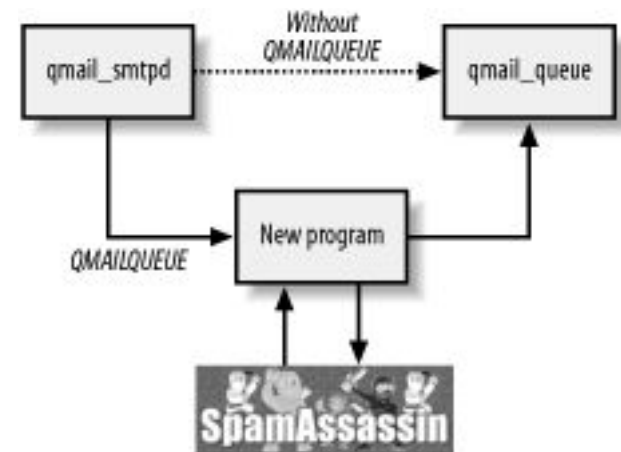


## Revisión de Spam- todo el correo entrante

Si no se cuenta con el parche de QMAILQUEUE, entonces se puede realizar lo siguiente:

Se puede emular QMAILQUEUE, al renombrar **qmail-queue** a **qmail-queue.orig** y escribiendo un nuevo script para **qmail-queue** que redireccione el mensaje a través de SpamAssassin y luego al archivo **qmail-queue.orig**.

```
#!/bin/sh  
PATH=/var/qmail/bin:$PATH  
| spamc | qmail-queue.orig
```



## ***Personalice SpamAssassin***

Adicionalmente a las reglas básicas iniciales, sin embargo se pueden contemplar otras más específicas o recientes:

### **BigEvil**

<http://www.rulesemporium.com/rules/bigevil.cf>

### **70 SARE Adult**

[http://www.rulesemporium.com/rules/70\\_sare\\_adult.cf](http://www.rulesemporium.com/rules/70_sare_adult.cf)

# *Agradecimientos*

A mi esposa Margarita, por tener la paciencia y el cariño necesario para apoyarme en cada nuevo proyecto.

## *Gracias!*

**Ing. Alejandro Escalante**  
**Dirección de Recursos**  
**Informáticos**  
**aescalan@ine.gob.mx**