

CERTuy

 **AGESIC**



Correo **NO**** Solicitado**

Mauricio Campiglia
mauricio@[nospam]campiglia.org
mauricio (en) campiglia (dot) org

MontevideoLibre

- Proyecto de creación de red comunitaria
- Grupo de interesados en tecnologías inalámbricas
- Laboratorio y campo de aprendizaje y pruebas
- Grupo de amigos

UYLug

- **Grupo de Usuarios de GNU/Linux**
- **Apoyo para empezar**
- **Contrapartes para discutir, aprender y crecer**
- **Listas de correo**
- **Eventos técnicos y de los otros**
- **Fiestas de instalación**

Técnicas

- **Agresivas**
 - Fake MX, Greylisting, Throttling, ...
- **Normales**
 - Contenidos, Reputación, Apego a RFC
- **En declive o inútiles**
 - Listas (blancas, negras),
- **En proceso de adopción**
 - Vacunas, SPF, Colaborativas, ...

Listas Blancas

- Lista de invitados
- Inefectivas debido a la fácil **falsificación**
- De ayuda como filtro previo de otras técnicas
 - Remitentes o dominios conocidos ****y**** confiables
 - Usado en **conjunto** (de ahí lo de previo)
 - Bypass de verificación
 - Disminución de puntaje
 - Verificaciones más laxas (permisivas)

Listas Negras

- Declaración de persona **non grata**
- Inefectivas debido a la fácil falsificación
- Al igual que las listas blancas...
 - Usado en **conjunto** con otras técnicas
 - Aumento de puntaje
 - Verificaciones más estrictas
 - Más verificaciones

Confirmación de contacto

- Señooooora, ¿y si el nene no quiere tomar la sopa?
- Alta en lista de contactos previo a envío
 - Automatizado
- Ej. ¿montevideo.com?
- A decir de mis amigos:
 - La única técnica 100% efectiva

Greylisting

- **El cartero llama dos veces ;-)**
 - Y ****no****, no es **mezcla** de listas blancas y negras
- **Una capa adicional de protección**
 - Que se lleva el 50% del problema
- **Requiere interacción con el MTA**
- **Permite listas blancas**

Greylisting, cómo

Listas Marrones

- **Esto ya parece broma... ;-)**
- **Mezclas de listas negras y mecanismos p2p**
 - Listas negras colaborativas
- **Concepto ya existente, nuevo nombre**
 - BSD + sendmail + ...
- **Adopción no generalizada**

Apego al Estándar

● La letra chica del contrato

```
#### Checks to remove badly formed email
*smtpd_helo_required = yes
*strict_rfc821_envelopes = yes
*disable_vrfy_command = yes
*unknown_address_reject_code = 554
*unknown_hostname_reject_code = 554
*unknown_client_reject_code = 554
*smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname, regexp:/etc/postfix/helo.regexp, permit
#### When changing sender_checks, this file must be regenerated using postmap <file>, to generate a Berkeley DB
*smtpd_recipient_restrictions =
  * check_client_access hash:/etc/postfix/helo_client_exceptions
  * check_sender_access hash:/etc/postfix/sender_checks,
  * reject_invalid_hostname,
#### Can cause issues with Auth SMTP, so be weary!
  * reject_non_fqdn_hostname,
#####
  * reject_non_fqdn_sender,
  * reject_non_fqdn_recipient,
  * reject_unknown_sender_domain,
  * reject_unknown_recipient_domain,
  * permit_mynetworks,
  * reject_unauth_destination,
  .
# Add RBL exceptions here, when changing rbl_client_exceptions, this
#file must be regenerated using postmap <file>, to generate a
#Berkeley DB
  * check_client_access hash:/etc/postfix/rbl_client_exceptions,
  * reject_rbl_client cbl.abuseat.org,
  * reject_rbl_client sbl-xbl.spamhaus.org,
  * reject_rbl_client bl.spamcop.net,
  * reject_rhsbl_sender dsn.rfc-ignorant.org,
  * check_policy_service inet:127.0.0.1:60000
  * permit
```

Apego al Estándar

- ¿Cuál?
 - RFC2821 (RFC821)
- Hecho con el propio **MTA**
 - Solo configuración
- **Fácil, Bonito, Barato** ;-)
- Y ya que estamos agregamos **buen comportamiento**

Apego al Estándar

- HELO requerido
- HELO FQDN
- Sender FQDN
- Espera por el 200 OK
- Sobres RFC821 estrictos

Y ya que estamos

- **No habilitar relay externo**
 - Puede usarse vistas por ej.
- **No habilitar usuarios no existentes**
 - Ayuda contra Backscatter
- **Verificación de nombre reverso**
 - Y revisamos que el nuestro esté bien
- **Límite de envíos**
 - Cuidado, requiere **planificación**

Registro MX falso

- **Agregar un registro MX sin MTA asociado**
 - **Prioridad** baja y/o muy alta
 - Servidor inexistente (o puertos filtrados)
 - Por favor en **rango propio** de direcciones
- **Ayuda contra bots automáticos**
- **El reintento puede demorar**
 - Aumento de latencia

Retroverificación

- **Reverse DNS**
 - Via verificación de encabezados
- **Fake sending**
 - Simulo un envío y genero error
 - Como Greylisting pero al verres... ;-)
- **Consumo de recursos**
 - Propios
 - Ajenos (de los “amigos”)

Listas de Reputación

- **RBL, DNSBL y otras bls...**
- **En declive**
 - Uso de botnets
- **Reputación de contenido**
 - Hashes de contenido distintivo o significativo
 - No tan en declive
 - Razor, Pyzor, Clearinghouse

Filtrado por contenido

- **Hacia adonde apuntan las directivas**
- **Al...**
 - O cómo hacer que un humano piense como máquina
- **Reglas**
- **Estadísticas**

Filtrado por contenido, reglas

- **Conjunto de patrones**
 - Similar al antivirus
- **Reactivo**
- **Reglas escritas por otros (repositorios)**
 - Bueno, también podemos escribirlas nosotros
- **¿En declive? (ver declaración en Sare Ninjas)**

Filtrado por contenido, estadística

- **Acá está la parte interesante de la cosa**
 - AI
- **Bayes**
 - Spamassassin
- **Discriminadores Markovianos**
 - CRM114 <---(injusto)
- **Ji cuadrado**
 - Bogofilter

Técnicas de Autenticación de correo

- **SPF**
 - Registro TXT en DNS
- **DKIM**
 - Firmado por la organización remitente
- **Querido pero odiado**
 - Yahoo no implementa
 - Hotmail es demasiado permisivo
 - La delgada línea roja

Vacunación

- **Técnica entre pares**
 - Si a mí me pasó que no te toque a tí
- **Lenta adopción**
- **Queda por ver la velocidad de propagación**
- **Requiere entramado de confianza**
 - Recordar, conocido != confiable

Tarpit

- **El dulce sabor de la venganza**
- **Hacer el envío insoportablemente lento**
 - Incluso para un bot
- **Atrapar al bot**
 - Tamaño de ventana cero
 - Lentitud al responder
- **Requiere cuidado, planificación y cuidado**

Honeypot

- a.k.a. Spampots
- **Recursos disponibles solo para los spammers ;-)**
 - Dominios truchos
 - MTAs sin MX
 - Direcciones preparadas para recolectores
 - Direcciones de dirección inválida
- **Valiosísimo para aprendizaje (ver trampas)**

Trampas

- **Direcciones falzas**
- **Elementos amigables a los recolectores**
- **MTAs sin MX asociado**
 - Esto cae en el punto anterior... ;-)
- **Normalmente usados para alimentar conocimiento**
 - Alimento estadístico o para anticuerpos ;-)

¿Qué hacer en lo personal?

- ¡NO, **NO** pinche aquí para removerse!
 - Corolario: No, no mande al spammer a la <piiiiiiiip>
- Cuidado con el **perfil** en línea
 - Ofusque, haga anónimo, use descartables...
- Mantenga su máquina **limpia**
 - Esto es en beneficio social, no personal, créame.
- Utilice palabras como llaves con su círculo
- Reporte

Soluciones Comerciales

- Ver (go to) Soluciones Comerciales

; -)

Soluciones Libres (para el MTA)

- **Spamassassin**
 - La vedette
 - Bayes, Reglas, etc.
- **Bogofilter**
 - Usable en el cliente de correo
 - Ji Cuadrado

Soluciones Libres (para el MTA)

- **Dspam**
 - Estadística variada
- **CRM114**
 - Estadística variada

Casos reales, estadísticas

- ¿Qué quieren decir los porcentajes?
 - 95%
 - 1 de cada 20
 - 99%
 - 1 de cada 100
 - 99,5%
 - 1 de cada 200
 - 99,95%
 - 1 de cada 2000

Casos reales, estadísticas

- **Porcentajes vistos de otro modo:**
- **De cada 1,000 correos recibidos son basura...**
 - 50 con efectividad 95%
 - 10 con efectividad 99%
 - 1 con efectividad 99.9%
 - 0 (bueno, $\frac{1}{2}$) con efectividad 99.99%
- **¿Cuántos correos recibe su MTA por día?**

Casos reales, estadísticas

- **Greylist se comía el 80% a 90%**
 - Hoy se lleva cerca del 50%
- **El área con mayor actividad es estadística**
 - CRM114 efectividad superior al 99%
 - Dspam, efectividad superior al 99% (enchulado)

Casos reales, aprendizaje

- **Infraestructura de aprendizaje es muy necesaria**
- **Automatizar lo más posible**
- **Requiere planificación y cuidado**
 - No es difícil, no es trivial
- **Centralizado vs. por usuario**
- **Consideraciones de almacenamiento**
 - En particular con técnicas estadísticas modernas

Casos reales, trampas

- ¿Lo **requiero**?
- ¿Que **tipo** de trampas?
- No trivial de implementar ****Y**** requieren atención
- Teniendo alternativas relativamente sencillas, son una buena forma de alimentar estadísticas
- Verificación **humana** en etapas iniciales

Casos reales, lecciones aprendidas

- **No hay bala de plata**
 - Estrategia combinada es la mejor estrategia
- **Perdimos RBLs por el camino**
 - Y probablemente sigamos perdiendo
- **Perdimos repositorios de reglas de filtrado**
 - Y probablemente sigamos perdiendo

Casos reales, lecciones aprendidas

- **Filtrado estadístico es muy, muy efectivo...**
 - ... si se lo enseña
- **CRM114 aprende rapidísimo...**
 - ... pero penaliza con el uso de almacenamiento
- **Mayor perfil en línea >>> Usuario más afectado**
 - Trabajar en ofuscar la información de los sitios
 - Entrenar, concienciar...

Referencias

- **A plan for spam**
 - Paul Graham
- **Ending Spam**
 - Zdziarski, No Starch Press
- **Spamassassin**
 - Schwartz, O'Reilly

Referencias

- <http://spamassassin.apache.org>
- <http://bogofilter.sourceforge.net>
- <http://dspam.nuclearelephant.com/>
- <http://crm114.sourceforge.net/>
-
- <http://ietf.org>
- <http://www.linuxjournal.com/article/6467>
- <http://wikipedia.org>

Referencias

- <http://razor.sourceforge.net/>
- <http://www.rhyolite.com/anti-spam/dcc/>
- <http://pyzor.sourceforge.net/>
- <http://www.rulesemporium.com/>
- <http://spamlinks.net/>

¿Preguntas?

- Esperamos tus comentarios, aportes y sugerencias.

capacitacion (en) agesic (dot) gub (dot) uy

¡Muchas gracias!

www.agesic.gub.uy

Preguntas?

Esperamos tus comentarios, aportes y sugerencias.

capacitacion@agesic.gub.uy

Muchas gracias !!

www.agesic.gub.uy