LinuxFocus article number 279
http://linuxfocus.org

Het gevecht tegen Spam-Mail

door Katja en Guido Socher

<katja/at/linuxfocusorg
guido/at/linuxfocus.org>

Over de auteur:

Katja is redactrice van de duitse versie van LinuxFocus. Ze houdt van Tux, film & fotografie en de zee. Je kunt haar homepage hier vinden.

Guido is al lange tijd Linux fan en hij waardeert Linux omdat het keuzemogelijkheden biedt en vrijheid geeft. Je kunt naar eigen believen oplossingen kiezen en ontwikkelen.

Kort:

Spam tussen je mail!? Spam E-mail groeit met schrikbarende snelheid en is voor bijna iedereen een serieus probleem. In dit artikel zullen we uitleggen wat je tegen deze plaag kunt beginnen.

Vertaald naar het Nederlands door:
Christ Verschuuren
<cjmversch/at/netscape.net>

Wat is spam-mail?

Spam-mail heeft vele namen. Sommigen noemen het UCE (Ongevraagde commerciële email) anderen noemen het Ongewenste E-mail, maar al deze namen verklaren niet echt wat het eigenlijk is. Als je

(nog) geen spam ontvangt kijk dan eens naar deze collectie spam-mail (spam_samples.html). Het is een willekeurige selectie uit de over een paar dagen ontvangen spam-mail. Lees eens door de berichten en je zult snel begrijpen dat dit niets te maken heeft met commercie of zakendoen. Deze spammers zijn criminelen. Geen enkele zichzelf respecterende zakenman/vrouw zou miljoenen mensen zo irriteren en beledigen om enkele "argelozen" te vinden die in hun trucjes trappen.

Het is een wijd verbreid misverstand onder mensen die weinig ervaring met het Internet hebben om te geloven dat deze manier van reclame maken vergelijkbaar is met de aanbiedingen die ze bij tijd en wijle van hun supermarkt ontvangen. Producten die verkocht worden middels spam-mails zijn vaak illegaal en vaak is er helemaal geen product. Het zijn trucjes om je geld af te troggelen.

Hoe veel?

Spammers halen je e-mail adressen van webpagina's, nieuwsgroepen of uit domeinregistraties (als je je eigen domein hebt). Er zijn individuen die robots gebruiken om de adressen te verzamelen, branden deze op CD's en verkopen ze voor weinig geld aan andere Spammers. Als je je e-mail adres vandaag de dag in klare taal op je homepage plaatst, kunnen dergelijke programma's dit herkennen, vervolgens heb je in enkele maanden tijd een serieus probleem dat niet meer te stoppen is. Het probleem wordt met de dag groter!

In 1998 was het percentage spam mail verzonden naar LinuxFocus minder dan 10%. In November 2002 zijn de statistieken als volgt:

Onze server krijgt ongeveer 4075 mailberichten per week. 3273 zijn spam-mails!
=> **80% van alle mailverkeer is Spam.**

Dat wil zeggen dat 80% van de capaciteit van de mail server en 80% van de netwerkcapaciteit wordt gebruikt voor iets dat niemand wil.

Van deze 3273 spam mails is ongeveer 40% afkomstig uit Amerika (vooral Canada, US, Mexico) en ongeveer 30% uit Azië (vooral Korea, China en Taiwan).

Wat doen we met Spam

Als je naar de spam-mails kijkt zul je zien dat ze nagenoeg allemaal een mogelijkheid bieden om verwijderd te worden uit de e-mail lijst. Doe dat niet! Je hebt te maken met criminelen. Geen enkele spammer zou iets bereiken als hij een behoorlijke verwijderlijst zou hanteren. Waarom bieden ze dan nog steeds deze mogelijkheid? Het antwoord is eenvoudig. Het maakt een veel betere indruk op de lezer en het is een statistisch hulpmiddel bij uitstek. De spammer kan onmiddelijk controleren dat zijn berichten aankomen. Met andere woorden **je bevestigd de ontvangst van zijn bericht!**

Er is ook een simpel technisch probleem met het concept van de verwijderlijst. LinuxFocus is geen grote site, maar we zouden een full time kracht nodig hebben om ons af te melden voor alle 3273 Spam berichten die we per week ontvangen en deze persoon dat afmelden dan in een minuut moeten kunnen doen. Elke spammer gebruikt een andere methode, het zou een belachelijke opdracht zijn en het kan niet werken. Verwijderlijsten zijn onzin en helpen alleen de spammers.

De enige juiste actie is: verwijder het bericht!

Software om spam te beheersen

Er zijn een aantal mogelijkheden op spam berichten uit te filteren en dit is een goede zaak, omdat het daardoor moeilijker wordt voor spammers om hun boodschap te verspreiden. Het blijft echter een worsteling. De hulpmiddelen om spam te filteren worden steeds geavanceerder, maar de spammers verbeteren hun methoden ook.

Er zijn 2 typen filters:

1. Controles die zijn ingebouwd in de MTA (Message Transfer Agent=Mail server). Hier kun je meestal het bericht weigeren. Dat wil zeggen: de e-mail wordt niet eens opgeslagen. Er wordt een foutcode teruggestuurd zodra tijdens de ontvangst van het bericht wordt herkend dat het om een spambericht gaat. Typische voorbeelden van deze hulpmiddelen zijn IP gebaseerde blokkadelijsten en controles op berichtkoppen. Als je zelf geen mail server hebt, dan zou je ISP er een moeten installeren.

2. Filteren na ontvangst van het bericht. In dit geval is de e-mail succesvol afgeleverd en wordt hij pas later uitgefilterd.

We zullen nu de verschillen mogelijkheden meer in detail bespreken. Ze hebben allemaal voor- en nadelen. De beste oplossing om van spam af te komen is om meerdere hulpmiddelen te gebruiken.

E-mail direct bij de MTA weigeren

Als je je e-mail direct bij ontvangst door de mail server weigert, kan de spammer een foutmelding terugontvangen en weet hij dat dit adres niet geldig is. Als het een van de "CD-makers" is kan hij je adres uit de lijst verwijderen. Het bespaart een hoop bandbreedte, omdat je niet het hele bericht hoeft te ontvangen. Je kunt een foutmelding zenden, zodra je ontdekt dat het spam betreft.

Om dit te doen heb je een goede en flexibele MTA nodig. Helaas zijn de twee meest gebruikte servers, Sendmail en degene van Bill Gates niet geschikt voor deze taak. Twee erg goede alternatieven zijn Postfix en Exim. Als niet kunt veranderen van mail server kun je altijd nog een smtp proxy als messagewall voor de server (smtp = Simple Mail Transfer Protocol, het Internet mail protocol) plaatsen.

We zullen nu de werking van enkele veelvoorkomende filtertechnieken bespreken. We zullen niet beschrijven hoe ze geconfigureerd moeten worden in elk van de MTA’s. Dat zou het artikel te lang maken. In plaats daarvan stellen we voor de documentatie van je geïnstalleerde MTA te lezen. Postfix en Exim zijn goed gedocumenteerd.

- Realtime Block lists:
  Dit zijn DNS gebaseerde lijsten. Je controleert het IP adres van de mailserver dat een bericht naar je wil zenden met een zwarte lijst van bekende spammers. Algemene lijsten zijn www.spamhaus.org of ordb.org. Er is ook een tool, blq genaamd (zie referenties) om handmatig

zulke blokkadelijsten te bevragen en na te gaan of een bepaald IP adres in de lijst is opgenomen. Wordt hier echter niet te enthousiast over en zoek zorgvuldig de te gebruiken blokkadelijst, omdat er ook tussen zitten die volledige IP reeksen blokkeren om de eenvoudige reden dat een spammer ooit een inbelverbinding had bij de betreffende ISP. Persoonlijk zou ik in ieder geval ordb.org gebruiken om post van slecht beheerde servers buiten te houden.
Ervaring leert dat deze blokkade lijsten ongeveer 1%-3% van de spam mail ondervangen.

- 8 bit karakters in de onderwerp tekst:
  Ongeveer 30% van de spam is vandaag de dag afkomstig uit China, Taiwan of een ander oosters land. Als je echt geen chinees kunt lezen, dan kun je berichten weigeren die veel 8 bit karakters (geen ASCII) in de onderwerp tekst hebben. Sommige MTA's hebben hier een separate configuratie optie voor, maar je kunt ook een normale tekstvergelijking (reguliere expressie) op de berichtkop gebruiken:

  /^Subject:.*[^ -~][^ -~][^ -~][^ -~]/

  Dit zal alle e-mail weigeren die meer dan 4 opeenvolgende karakters in de onderwerp tekst heeft die geen deel uitmaken van de ASCII range spatie tot tilde. Als je niet bekend bent met tekstvergelijkingen is het aan te bevelen je hierin te verdiepen, je zult ze nodig hebben (zie LinuxFocus artikel 53). Zowel exim als postfix kunnen gecompileerd worden met ondersteuning voor perl tekstvergelijking (zie www.pcre.org). Perl heeft de krachtigste tekstvergelijkingsopties. Deze methode is vrij goed en houdt circa 20-30% van de spam-mail buiten.

- Lijsten met "Van" adressen van bekende spammers:
  Vergeet het maar. Dit werkte misschien nog in 1997. Spammers gebruiken tegenwoordig fictieve adressen of adressen van onschuldige personen.

- Weigeren niet FQDN (Fully Qualified Domain Name) afzenders en onbekende afzender domeinen:
  Sommige spammers gebruiken niet-bestaande adressen in het "from:" veld. Het is niet mogelijk om complete adressen te controleren, maar je kunt het domeindeel van het adres (achter @) wel controleren met behulp van controle tegen een DNS server.
  Dat houdt ongeveer 10-15% van de spam tegen en je wilt deze e-mails toch niet ontvangen,omdat je toch niet zou kunnen reageren op het bericht zelfs als het geen spam was.

- IP adres heeft geen PTR record in het DNS:
  Dit controleert of het IP adres vanwaar je het bericht hebt ontvangen vertaald kan worden in een domein naam. Dit is een erg krachtige optie en houdt veel berichten tegen. We willen deze mogelijkheid niet aanbevelen! Dit test niet of de systeembeheerder van de mail server goed werk gedaan heeft, maar of hij een goede backbone provider heeft. ISP's kopen IP adressen van hun backbone providers en deze kopen weer in bij grotere backbone providers. Alle betrokken backbone providers en ISP's moeten hun DNS juist configureren om de hele keten te laten werken. Als iemand ergens in de keten een fout maakt of zijn DNS niet wil configureren,dan werkt het niet. Het zegt niets over de individuele mail server aan het eind van de keten.

- Vereist HELO commando:
  Als 2 MTAs (mail servers) met elkaar praten (via smtp) dan zeggen ze eerst wie ze zijn (bijv. mail.linuxfocus.org). Sommige spam software doet dat niet. Dit houdt 1-5% van de spam buiten.

- Vereist HELO commando en weigert onbekende servers:
  Je gebruikt de naam die je krijgt uit het HELO commando en ga dan naar een DNS om te controleren of dit een juist geregistreerde server is. Dit is een erg goede methode omdat een spammer die tijdelijk een inbelverbinding gebruikt er meestal geen geldig DNS record voor zal configureren.
  Dit blokkeert ongeveer 70-80% van alle spam maar weigert ook legitieme berichten afkomstig van sites met meerdere mail servers waar een slordige systembeheerder heeft verzuimd om alle hostnamen van alle servers in DNS plaatsen.

Sommige MTA's hebben nog meer opties maar de bovenstaande zijn gewoonlijk aanwezig in een goede MTA. Het voordeel van de bovenstaande controles is dat ze geen zware belasting van de CPU veroorzaken. Over het algemeen hoef je je mailserver hardware niet te upgraden voor deze controles.

Filteren van reeds ontvangen mail

De hierna volgende technieken worden gewoonlijk toegepast op het gehele reeds ontvangen bericht en de zendende mail server wordt gewaar dat het bericht niet bezorgd kon worden. Dat betekent dat ook een te goeder trouw zijn zender geen foutrapportage krijgt. Het bericht verdwijnt gewoon.
Dit gezegd hebbende moeten we gelijk opmerken dat niet helemaal waar is omdat dat afhangt van de filtermogelijkheden van de mail server. Exim is erg flexibel en laat je toe om maatwerk filters te schrijven voor berichten.

- SpamAssassin (http://spamassassin.org/):
  Dit is een in perl geschreven spam filter. Het gebruikt zorgvuldig handgeschreven regels en kent punten toe aan typische spam teksten als "strong buy", "you receive this mail because", "Viagra", "limited time offer".... Als het aantal punten boven een bepaald niveau komt wordt het bericht aangemerkt als spam. Het probleem van dit filter is dat erg veeleisend op het gebied van geheugen en cpu snelheid. Je zult waarschijnlijk je mail server hardware moeten upgraden, zeker als je server hardware al 2-3 jaar oud is. We adviseren niet om het rechtstreeks op de mail server te gebruiken. Spamassassin levert tevens een spamd programma (spamd=spam daemon + spamc=client om met de daemon te verbinden) dat de starttijd van spamassasin terugbrengt en de cpu belasting vermindert, maar het blijft een applicatie die veel rekenkracht vraagt.

  Om de berichten te filteren moet je een .procmailrc bestand maken (alsmede een .forward bestand) vergelijkbaar met het volgende:

```
# The condition line ensures that only messages smaller than 50 kB
# (50 * 1024 = 56000 bytes) are processed by SpamAssassin. Most spam
# isn't bigger than a few k and working with big messages can bring
# SpamAssassin to its knees. If you want to run SpamAssassin without
# the spamc/spamd programs then replace spamc by spamassassin.
:0fW:
* < 56000
| /usr/bin/spamc
# All mail tagged as spam (e.g. with a score higher than the set threshold)
# is moved to the file "spam-mail" (replace with /dev/null to discard all
# spam mail).
:0:
* ^X-Spam-Status: Yes
spam-mail
```

Het installeren is eenvoudig en spamassassin filtert meer dan 90% van de spam uit.

- procmail (http://www.procmail.org):
  Procmail is in zichzelf geen spam filter maar je kunt het gebruiken om er een te schrijven. procmail heeft ook een geringe belasting zolang je het aantal regels beperkt houdt tot het redelijke (bijv. minder dan 10). Om het te gebruiken maak je een .forward bestand in je home-directory en voegt de volgende regel toe:

  ```
  "| exec /usr/bin/procmail"
  ```

  Sommige mensen adviseren het gebruik van
  "|IFS=' ' && exec /usr/bin/procmail"
  maar dit leidt tot nieuwe problemen met een extra proces dat wordt opgestart en niet meer werkt onder controle van de mail server. Beveiligde mail servers als postfix of exim zullen geen probleem hebben met het bovengenoemde .forward bestand.

  Procmail is bijzonder geschikt voor een omgeving waarin je normaliter communiceert in een gesloten groep. Bijv. voor mensen in een bedrijf waar de meeste berichten afkomstig zullen zijn van de collega's en enkele vrienden. Hier is een voorbeeld voor "mycompany.com":

  ```
  # .procmailrc file.
  # search on header for friends:
  :0 H:
  * ^From.*(joe|paul|dina)
  /var/spool/mail/guido

  # search on header for mails which are not coming from
  # inside mycompany.com and save them to maybespam
  :0 H:
  * !^From.*(@[^\@]*mycompany\.com)
  /home/guido/maybespam

  # explicit default rule
  :0:
  /var/spool/mail/guido
  ```

  Dit maakt het veel eenvoudiger om spam te verwijderen en je vindt de lelijke spam niet meer tussen je normale berichten.

  Procmail is erg flexibel en kan ook voor andere taken gebruikt worden. Hier is een ander voorbeeld:
  Procmail bevat een "reply to sender" programma formail genaamd. Dit kan bijvoorbeeld gebruikt worden om een bericht terug te zenden naar degene die je een bericht stuurt. Een serieuze plaag zijn e-mails met ingesloten MS-Word documenten. Als je als Linux ontwikkelaar e-mail gebruikt om informatie over je projecten of Linux in het algemeen uit te wisselen ben je hoogstwaarschijnlijk niet geïnteresseerd in mensen die teksten in Word schrijven en dan insluiten bij mails. Virussen kunnen op die manier gemakkelijk verspreid worden. Over het algemeen infecteren ze Linux niet,maar het is in het algemeen een slecht idee om MS-word teksten naar andere mensen te sturen omdat dezelfde versie van MS-word nodig hebben om het bericht te kunnen lezen. Er zijn open formaten als RTF of HTML die geen virussen verspreiden, op

meerdere platforms worden gebruikt en die geen versie problemen hebben.

```
# Promail script to
# reject Word documents. Reject the mail, but do not reply to
# error messages "From MAILER-DAEMON"
# If you use ":0 Bc" instead of ":0 B" then you will still get the mail
:0 H
* !^From.*DAEMON
{
  # The mime messages with word documents look like this in the body
  # of the message:
  #------=_NextPart_000_000C_01C291BE.83569AE0
  #Content-Type: application/msword;
  #        name="some file.doc"
  #Content-Transfer-Encoding: base64
  #Content-Disposition: attachment;
  #        filename="real file.doc"
  :0 B
  * ^Content-Type:.*msword
  | (formail -r ; cat /home/guido/reject-text-msword ) | $SENDMAIL -t
}

# explicit default rule
:0:
/var/spool/mail/guido
```

Het tekst bestand /home/guido/reject-text-msword moet een tekst bevatten die verklaard dat msword documenten virussen kunnen verspreiden en vraagt de zender om het document opnieuw te versturen in bijvoorbeeld RTF formaat.

Hoe procmail gebruikt moet worden en wat alle vreemde tekens in het configuratiebestand betekenen wordt uitstekend uitgelegd in de "procmailrc" man pagina’s.

- bogofilter (http://www.tuxedo.org/~esr/bogofilter):
  Bogofilter is een Bayesian spam filter. Het is volledig geschreven in C en het is erg snel (vergeleken met SpamAssassin). Een Bayesian filter is een statistisch filter dat je eerst moet leren wat spam is en wat geen spam is. Je hebt ongeveer 100 training berichten nodig (gesorteerd in spam en geen spam) voordat het filter efficiënt kan werken op nieuwe berichten.

  Bogofilter is snel maar het werkt niet van start af aan, zoals SpamAssassin dat doet. Na een tijdje is het net zo efficiënt als SpamAssassin en filtert het meer dan 90% van de spam uit.

- razor (http://razor.sf.net/):
  Dit is een gedistribueerd, samenwerkend spam herkennings systeem. Checksums van bekende spam berichten worden opgeslagen in een database. Als je een nieuw bericht krijgt, bereken je de checksum en vergelijkt deze met de checksums in de centrale database. Als de checksum overeenkomt dat kun je het bericht verwijderen als spam. razor werkt vanwege speciale e-mails accounts die zijn verspreid over het Internet met de bedoeling om in de adreslijsten van de spammers te komen. Deze accounts ontvangen alleen spam en geen normale berichten. In aanvulling hierop kunnen mensen berichten naar razor zenden om deze te laten aanmerken als spam berichten. Er is een gerede kans dat de berichten al bekend als spam nog voordat ze in je mailbox aankomen. Dit systeem ondervangt circa 80% van de spam. razor heeft een karakteristiek

die geen van de andere filter technieken heeft: razor ontdekt bijna geen onterechte berichten. Dat wil zeggen: het aantal berichten die geen spam zijn en toch worden aangemerkt als spam is erg laag bij razor.

Er zijn vele oplossingen mogelijk om spam te bestrijden. We denken dat het bovenstaande de belangrijkst hiervan behandeld.

De beste oplossing is om controles in de MTA te gebruiken als eerste verdedigingslinie en de resterende spam te verwijderen met een filter methode.

HTML mail

Een bijzonder gevaarlijke vorm van e-mail xijn spam mails in HTML formaat.

De meeste spammers gebruiken de "afmeld mogelijkheid" om te zien hoeveel van hun berichten aankomen. HTML geformateerde berichten bieden een veel betere vorm van feedback: Afbeeldingen. Je kunt dit systeem vergelijken met de bezoekerstellers die je op sommige webpagina's aantreft. De spammer kan precies zien wanneer en hoeveel van zijn berichten zijn gelezen. Als je de Spam berichten zorgvuldig bestudeert zul je zien dat in sommige gevallen het URL voor de inbegrepen afbeeldingen een volgnummer bevat: De spammer kan precies zien wie naar zijn berichten kijkt en op welke tijd. Een onvoorstelbaar beveiligingslek.

Moderne e-mail programma's zullen afbeeldingen die zomaar ergens van een URL worden opgehaald niet tonen. Echter er zijn nauwelijks moderne en veilige HTML leesprogramm's. Kmail en de nieuwste versie van mozilla mail bieden de mogelijkheid om afbeeldingen van externe bronnen te blokkeren. De meeste andere programma's genereren mooie statistieken voor de spammer.

De oplossing? Gebruik geen mailprogramma dat html mail kan verwerken of download de berichten eerst, verbreek dan de verbinding met het Internet en lees dan pas je mail.

Waar komt spam vandaan?

Vertrouw nooit het zenderadres in het "From" veld van spam berichten! Het zijn of niet bestaande of onschuldige gebruikers. Het komt slechts zelden voor dat dit het mailadres van de spammer is. Als je wilt weten waar de mail vandaan komt moet je naar de volledige berichtkop kijken:

```
...

Received: from msn.com (dsl-200-67-219-28.prodigy.net.mx [200.67.219.28])
        by mailserver.of.your.isp (8.12.1) with SMTP id gB2BYuYs006793;
        Mon, 2 Dec 2002 12:35:06 +0100 (MET)
Received: from unknown (HELO rly-xl05.dohuya.com) (120.210.149.87)
        by symail.kustanai.co.kr with QMQP; Mon, 02 Dec 2002 04:34:43
```

In dit geval zend een onbekende host met IP adres 120.210.149.87 die beweert rly-xl05.dohuya.com te zijn de mail door naar symail.kustanai.co.kr. symail.kustanai.co.kr zend het bericht vervolgens weer door.
De spammer verbergt zich ergens achter 120.210.149.87 dat waarschijnlijk een eenvoudig

inbelverbinding is.

Met andere woorden de politie zou deze persoon kunnen vinden als ze naar de eigenaar van kustanai.co.kr gaan en vragen om de server logs en een afdruk van de verbindingen van de lokale telefoonmaatschappij. Jij hebt weinig kans uit te vinden wie dat was.

Het kan ook zijn dat het eerste deel van de berichtkop vals is en dat de spammer zich in het echt achter dsl-200-67-219-28.prodigy.net.mx bevind. Dit is erg waarschijnlijk omdat er geen goede reden voor symail.kustanai.co.kr is om het bericht naar msn.com te zenden via de dsl verbinding (dsl-200-67-219-28.prodigy.net.mx). De mailserver.of.your.isp (symbolische naam) is de server van jouw Internet Service Provider en is het enige deel van de "Received:" regel dat echt betrouwbaar is.

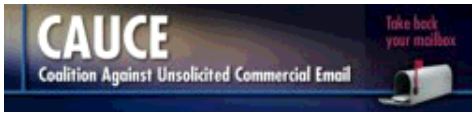
Het is mogelijk de spammer te vinden, maar daarvoor heb je internationaal onderzoek en de lokale politie nodig om prodigy.net.mx te bezoeken.

Conclusie

Als spam in het huidige tempo blijft toenemen dan zal het Internet spoeding veel meer Spam transporteren dan echte e-mail. Spam wordt vervoerd op kosten van de ontvanger. Er is meer bandbreedte benodigd en vaak moeten de mail systemen worden opgewaardeerd om de Spam stroom te kunnen beheersen.
De wetgeving in veel landen is gericht op het bechermen van burgers tegen misdadige spammers. In feite zijn er landen die wetten hebben waardoor eerlijke burgers worden beperkt (digital rights management etc...) en de criminelen worden geholpen (bijv. door leuke statistieken te krijgen over hun spam-mail).

Sluit je aan bij de Coalition Against UCE!

http://www.euro.cauce.org/en/



http://www.cauce.org/

Internet Service Providers zouden hun mail systemen moeten controleren. Ongeautoriseerde toegang tot mail servers moet voorkomen worden en het aantal berichten dat een gebruiker per minuut kan verzenden moet beperkt worden.

Referenties

- http://spamassassin.org/: spamassassin homepage
- http://www.procmail.org/: procmail homepage
- http://www.spambouncer.org/: spambouncer: een op procmail gebaseerd spam filter
- http://www.postfix.org/: homepage van de postfix MTA
- http://www.exim.org/: homepage van de exim MTA
- http://messagewall.org/: homepage van de messagewall smtp proxy
- http://www.unicom.com/sw/blq/: het blq perl script om een query uit te voeren op DNS

gebaseerde blokkadelijsten

- http://www.ordb.org/: DNS gebaseerde open relay blokkadelijst
- http://www.spamhaus.org: DNS gebaseerde blokkadelijst
- http://www.samspade.org/: Waar komt spam vandaan?
- http://www.dnsstuff.com/: gevarieerde blokkadelijsten en DNS gebaseerde hulpmiddelen
- http://www.geektools.com/cgi-bin/proxy.cgi: geektools Whois proxy
- http://www.tuxedo.org/~esr/bogofilter/bogofilter mail filter
- http://razor.sf.net/: razor
- http://pyzor.sourceforge.net: razor, geïmplementeerd in python
- http://lwn.net/Articles/9460/: Linux weekly nieuws artikel met een vergelijking van bogofilter en spamassassin.

Site onderhouden door het LinuxFocus editors team	Vertaling info:
© Katja en Guido Socher	en --> -- : Katja en Guido Socher <katja/at/linuxfocusorg guido/at/linuxfocus.org>
"some rights reserved" see linuxfocus.org/license/	en --> nl: Christ Verschuuren <cjmversch/at/netscape.net>
http://www.LinuxFocus.org	

2005-01-14, generated by lfparser_pdf version 2.51