Bekjempelse av spam med OSS

Torkel Hasle
Bibliotek-Systemer AS
torkel@bibsyst.no

NUUG 17. mars 2005


NO BANANA UNION
NO SOFTWARE PATENTS


www.spass24.com

Spam er en pest og en plage!

- Stjeler tid
- Stjeler plass
- Stjeler båndbredde
- Totalt unyttig
- Totalt ute av kontroll

Økende problem

	2001	2003	2004	2005	2006
EU	7%		50%		
BRIGHTMAIL		40%	60%		
POSTINI			78%	92%	
SPAMHAUS				75%	95%

Spamhaus forecast

Spam, now at 75% of all email traffic arriving at most ISPs mail servers, is set to increase still further thanks to new features in proxy hijacking software released by spammers. Many major email services report a large increase in spam coming directly from the major mail relays of other ISPs. Spamhaus sees this change and the increase in spam as a threat to be taken seriously, as unchecked, at the current pace spam levels could reach 95% of all email traffic by mid-2006.

Spamhaus 2

Spamhaus predicts that by mid-2006 spam could reach 95% of all email traffic and we would at that stage see visible signs of the beginning of a slow meltdown of email delivery systems caused by overloaded email queues and stressed spam filters.

Kostnader

25 mrd $ pr. år!

Hovedpunkter

- Hvem, hva, hvorfor?
- Spam-teknikker
- Bekjempelse
- RFC2821 (smtp)
- Postfix
- Postgrey
- Spamassassin

Hvorfor?

- **$$$$$$$$$$$$$$**
- De store talls lov: hvis 1% av 10 mill utsendinger resulterer i positivt svar, som gir en fortjeneste på 10$, blir det totalt en fortjeneste på 1mill. $!
- Det finnes minst 1% idioter, jfr T5PC og World Games
- 1 in 5 British Consumers Buy Software from Spam!!!

Hvem?

www.spamhaus.org/rokso:

Alan Ralsky United States

Albert Ahdoot and Alyx Sachs - Net Global Marketing United States

Alex Zhardanovsky / Azoogle Canada

Alexey Panov - ckync.com Russia

Amadeo Belmonte / Data One Marketing / I Net Values Inc. United States

America Find Inc. United States

Andrew Amend / US Health Laboratories United States

Andrew Westmoreland United States

Angelo Tirico United States

Anthony ''Tony'' M. Banks United States

Australian Porn Mafia Australia

Batch1 / Adam Vitale / g00dfellas.com United States

Bernard Balan "Merlin" Canada

Bill Stanley / telekomeurope.com United States

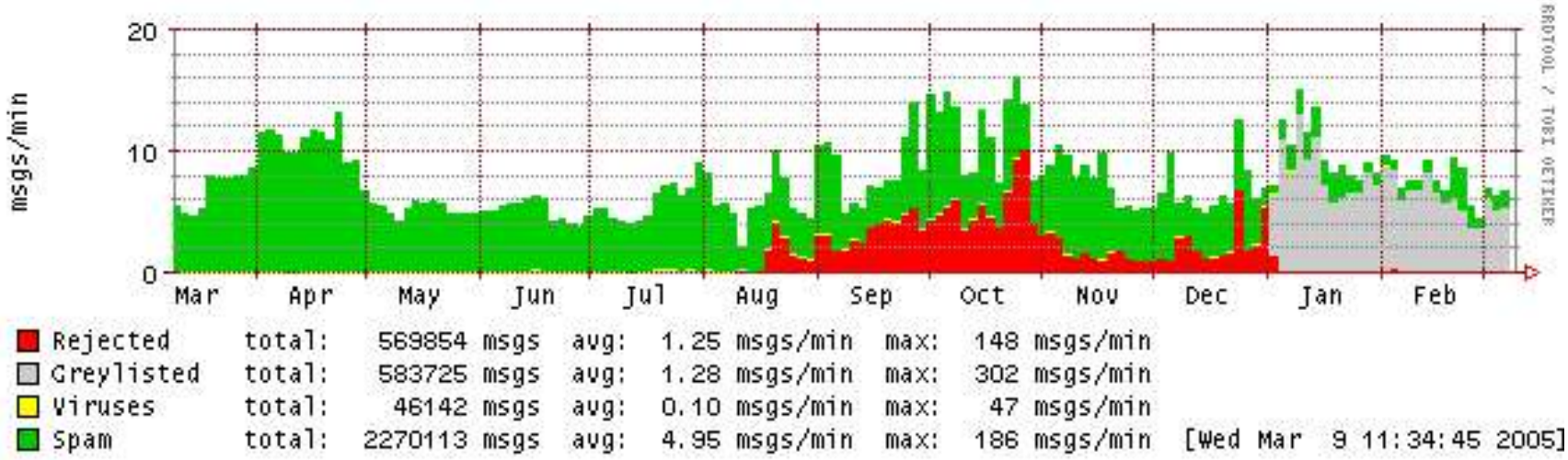
Hvem?

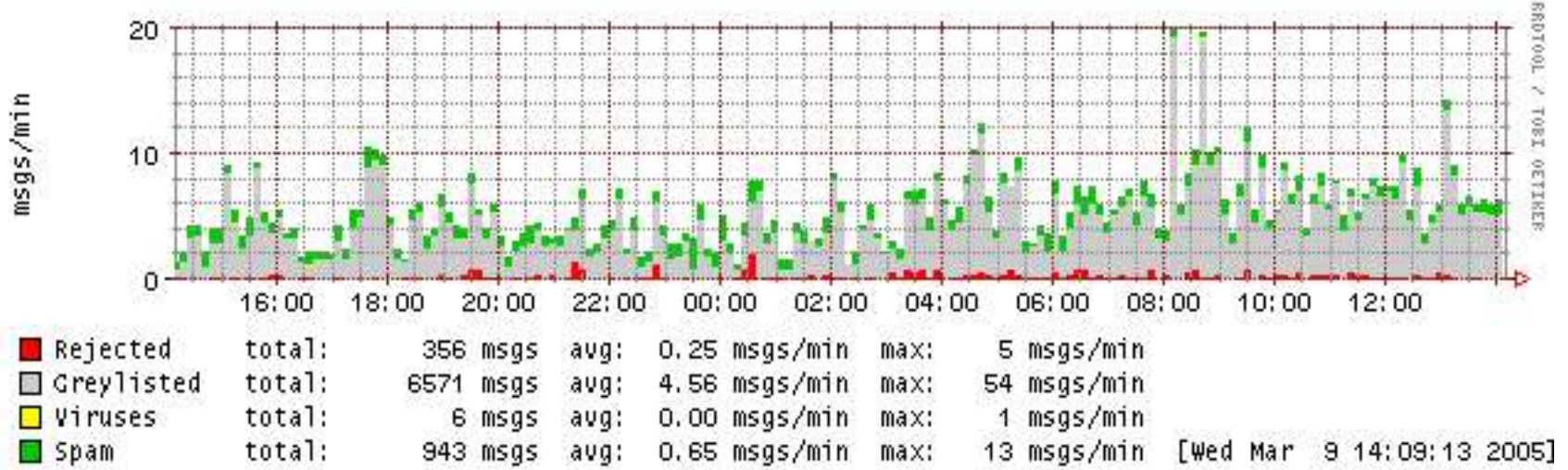
		Andel %	Akk % - USA
1	United States	42,1	
2	South Korea	13,4	13,4
3	China	8,4	21,9
4	Canada	5,7	27,6
5	Brazil	3,3	30,9
6	Japan	2,6	33,5
7	France	1,4	34,9
8	Spain	1,2	36,0
9	United Kingdom	1,1	37,2
10	Germany	1,0	38,2
11	Taiwan	1,0	39,2
12	Mexico	0,9	40,1

De største kjeltringene

- Ruslan Ibragimov, author of the 'Send-Safe' proxy spamware (nå blokkert fra MCI)
- Alexey Panov, author of the equally illegal Direct Mail Sender ("DMS") proxy spamware

Litt statistikk





Hvordan?

- Høste epostadresser fra web-sider, newgrupper osv.
- Selge/kjøpe epostlister
- Sende ut via epostroboter
- Sende ut via virusinfiserte zombie-pcer
- Falske avsenderadresser og domener

IT-avisen 2. juni 2003

Antispam-strateg Ryan Hamlin, Micro$oft:

Problemet er løst om to år, vil koste 18 milliarder (hva??)

Men før det vil ting bli mye verre

Det blir som med virus, som et irritasjonsmoment, men ikke et stort hinder.

Kommentar: Jeg er spent, bare 3 mnd. igjen til problemet er løst!!!!

Bill Gates 22. nov 2004

told media that SPAM could be history within two more years

M$ is working in the field with their Sender-ID technology

Vi må vente helt til slutten av 2006!

Spam teknikker

- Predatert
- HTML
- «Gappy» V-l_A+G-R_A
- «Web bugs» (remote images)
- Invisible ink (usynlig «god» tekst)
- Vertikale tabeller
- Sender ut til randomiserte epostadresser: asdfasd@hasle.com (brute force)

Botnets

- Zombie PC-er som benyttes for relay av spam
- Infisert av SoBig/Spyware osv.
- Tilvekst: 80-100.000 pr. uke!!!
- http://project.honeynet.org/papers/bots/

WEB-bugs

- Kalles også Lazy HTML
- `<img height="1" width="1" src="http://campaigns.emailserver2.com/MBDT/EmailOpenListener.aspx?xe=sMilE4d9satWWzMlYPb5vKys">`
- `<bgsound >`
- `<embed >`
- «Autoklikk link»
- Thunderbird kan blokkere disse

Bekjempelse

- Lovgivning (Can-Spam, EU)
- Teknologi (RBL, Greylisting, SPF)
- Hindre spam å sendes (ISP)
- Få folk til å slutte å klikke (håpløst)
- Spam/virus smelter sammen: stopper du virus, stopper du spam

Lovgivning

- Internasjonalt problem: lovgivningen helt utilstrekkelig over landegrensene
- Opt-in/Opt-out?
- USA: Can Spam = Yes, you can spam!
- EU: strengere regler, men ikke nok!
- Australia en av de få land med lovgivning som virker
- Norge: Ot.prop. 92/2003-04
- Ikke veien å gå:-(

Teknologi

- Blacklists (MTA)
- ip-filtre (iptables)
- Spamtraps/Honeypots
- Innholdsfiltre (Spamassassin, Popfile)
- Signaturer (Brightmail)
- SPF (Sender Policy Framework)
- M$ kryptert delay (bad idea!)
- M$ Sender-ID (patentsøkt fiasko)
- Domains keys (Yahoo)
- Greylisting

Viktig!

- **Stopp dritten i døra!**
- Dvs:
  - ip-filtre, greylisting, RBL
  - behandling på envelope-nivå, dvs før selve mailen overføres
- Filtre på MUA (Popfile, Spamassassin) ikke så bra, men brukbar som siste skanse
- Bayesisk filtrering ikke tilstrekkelig alene, men i kombinasjon med andre teknikker
- Alle ISP bør filtrere utgående epost for virus
- Alle ISP bør blokkere SMTP fra dynamiske adresser

Hvorfor blokkere dial-up og dynamiske adresser?

- Fordi det ikke er mulig for mottaker å verfisere avsender
- Fordi alle dynamiske adresser kan (og bør) sende via ISP's smtp-server
- Zombier sender som regel direkte, lettere å stoppe med greylisting

Stopp virus

- Bi-effekt: stop virus gratis:

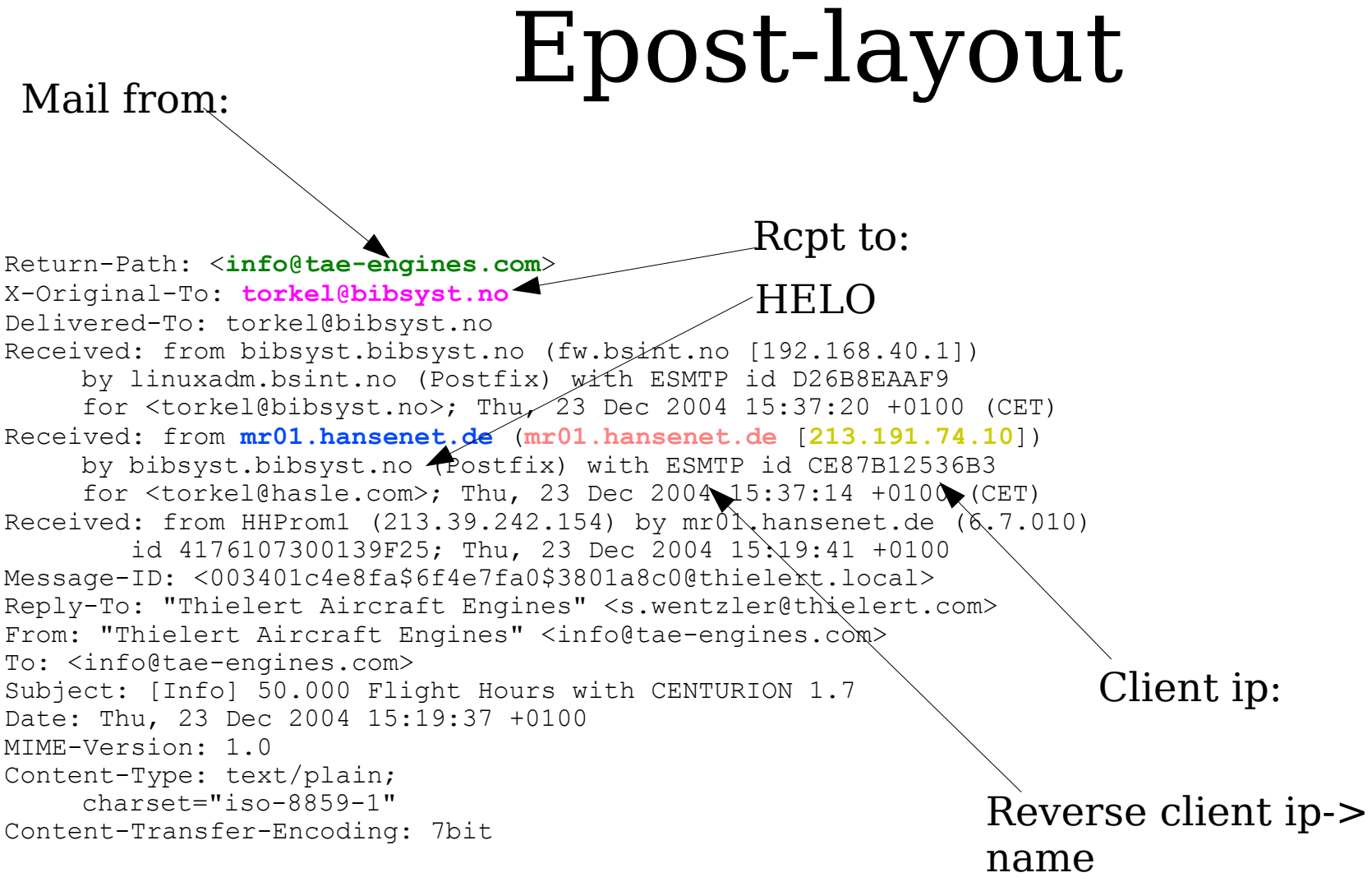
```
/Content-.*name=\"?[^"]*\.(vbs|vbe|jse|css|wsh|sct|hta|vxd|
exe|dot|hlp|pak|pif|pps|com|cmd|ocx|shs|cla|au|dll|scr|chm|
bat|lnk|src|zip|rar)\"?$/ DISCARD Content header filtering
(possible virus)
```

- DISCARD innebærer at mail mottas og kvitteres som OK; men droppes i stillhet (ingen backscatter mail).
- Lettvekstløsning, mye enklere enn å sjekke signaturer (jfr. Regjeringens 19-timers emailserver downtime)

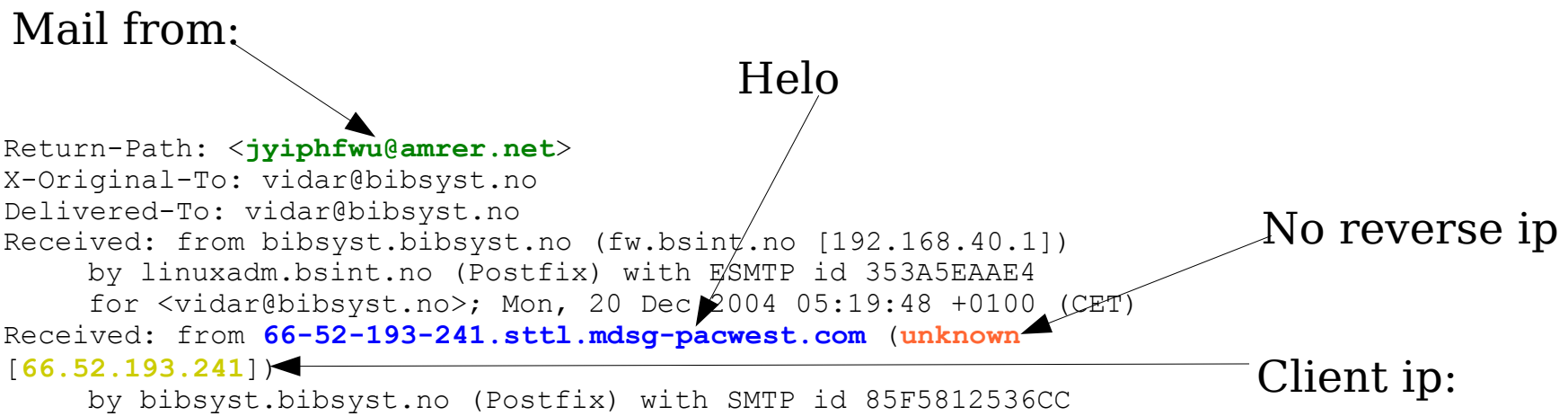
RFC 2821

```
telnet localhost 25
220 OK mail.my.domain ESMPT
HELO foo.domain.tld
250 mail.my.domain
MAIL FROM: john.doe@my.domain
250 OK
RCPT FROM: doo.dee@other.tld
250 OK
DATA
354 End data with <CR><LF>.<CR><LF>
.....
.
250 Ok: queued as 4265F6BE748
```

Epost-layout



Spam-layout




```
Return-Path: <jyiphfwu@amrer.net>
X-Original-To: vidar@bibsyst.no
Delivered-To: vidar@bibsyst.no
Received: from bibsyst.bibsyst.no (fw.bsint.no [192.168.40.1])
     by linuxadm.bsint.no (Postfix) with ESMTP id 353A5EAAE4
     for <vidar@bibsyst.no>; Mon, 20 Dec 2004 05:19:48 +0100 (CET)
Received: from 66-52-193-241.sttl.mdsg-pacwest.com (unknown
[66.52.193.241])
     by bibsyst.bibsyst.no (Postfix) with SMTP id 85F5812536CC
     for <vidar@bibsyst.no>; Mon, 20 Dec 2004 05:19:39 +0100 (CET)
X-Message-Info: AZM/tmm+45+l/E+269/432047248502
Received: from smtp-agreeable.sensuous.djyiphfwu@amrer.net
([66.52.193.241])
 by db31-hd97.djyiphfwu@amrer.net with Microsoft SMTPSVC
(5.0.0651.6646);
      Tue, 21 Dec 2004 05:19:21 +0400
X-Message-Info: CQDV+%ND_LC_CHAR[1-3]402+wiu+Q+90/62456353103944
Received: (qmail 84354 invoked by uid 1); Tue, 21 Dec 2004 03:20:21
+0200
Date: Mon, 20 Dec 2004 18:17:21 -0700
Message-Id: <3107092659.60442@djyiphfwu@amrer.net>
From: Support disseminate <djyiphfwu@amrer.net>
To: Vidar <vidar@bibsyst.no>
Subject: ****SPAM(31.7)**** CHEAPEST D*R-U-G-S ON THE WEB freeze
MIME-Version: 1.0 (produced by decisionalwearied 3.3)
```

Korrekt mailoppsett er viktig

```
  Mar 16 13:12:59 fw postfix/cleanup[7020]:
1314012536CC: reject: header To: stein.lier@akershus-
f.kommune.no, sigurd.nesse@nes-
ak.kommune.no,??birger.areklett@nes-ak.kommune.no,
ingrid.salt@volda.vgs.no,??inger.tomte@nottkom.no,
bjarne.brandt@oppegaard.vgs.no,??merete.rek from unknown
[213.184.199.233]; from=<Martin.Hauge@mrfylke.no>
to=<torkel@bibsyst.no> proto=ESMTP
helo=<your.hostname.domainname>: Wrong To:-header
```

OSS Verktøy

- Postfix MTA
- Postgrey
- SpamAssassin
- Amavisd-new
- Clam-Av virus-filter
- Spamtrap

Om praksis

- For vitenskapen er praksis et uinteressant spesialtilfelle

Når båten er lekk

- Bruker du **bøtta** først, fordi den tar unna mest vann, selv om du ikke er garantert å få vekk alt vannet
- Tar resten med **øsekaret**, evt. en **klut**

Postfix 2.1(www.postfix.org)

- Sendmail klone skrevet av Wietse Wenema, IBM
- Sikker
- Håndterer store volumer (> 5 mill mail pr. dag)
- Gode mekanismer mot spam/UCE
- Innebygget oppslag mot RBL
- Kan filtrere på envelope/header/body
- Kan knyttes opp mot eksterne filtre for spam/virus
- (Relativt) lett å konfigurere

RFC 2821

- Sjekk på klient (navn -> addr -> navn)
- Sjekk på HELO (navn -> addr -> navn)
- Sjekk på MAIL TO: (mottaker)
- Sjekk på RCPT FROM: (domain)
- Gyldig syntaks

Globale variable

Perameter	Verdi	Kommentar
Disable_vrfy_command	Yes	Spammere kan ikke sjekke gyldige epostadresser
smtpd_error_sleep_time	30	Sekunder før svar ved feil (tarpit)
smtpd_soft_error_limit	1	Antall feil før sleep_time inntrer
smtpd_hard_error_limit	10	Etter 10 feil kobler vi ned
smtp_banner	$myhostname ESMTP	Ikke si mer enn nødvendig
header_checks	regexp:header_checks	Vi sjekker header for virus
body_checks	regexp:body_checks	Filtrerer web-bugs

smtpd_sender_restrictions

Parameter	Verdi	Kommentar
permit_mynetworks		Selvsagt
check_sender_access	hash:access_sender	Whitelist
reject_non_fqdn_sender		Vi krever full avsenderadresse
reject_unknown_sender_domain		Finnes avsenderdomenet?

smtpd_recipient_restrictions

Parameter	Verdi	Kommentar
permit_my_networks		Selvsagt
check_etrn_access		Hvem som kan koble opp med ETRN (revers smtp)
reject_rbl_client		Se egen liste
reject_non_fqdn_recipient		Full epostadresse for mottaker
permit_mx_backup		Mail til sekundære MX domener
reject_unauth_destination		Stopper relay
check_sender_access	regexp:access	Whitelist
check_recipient_access	regexp:access_recipient	Whitelist mottakere
check_unknown_client		Revers ip (skummel, frarådes)
reject_invalid_hostname		HELO uten syntaksfeil
reject_non_fqdn_hostname		Fullt kvalifisert domenenavn
reject_unknown_hostname		Sjekk at HELO resolver til A eller MX (frarådes)

Bruk av sekundær MX

- Frarådes, med mindre du har full kontroll med filtreringen
- Mottar stort sett utelukkende spam
- Bedre: sørg for at din primære MX har gode oppetider

Hvorfor følge standard?

- Det meste av virusmail har ikke FDQN i HELO-streng
- Mange spammere sender fra servere uten revers navneoppslag
- Mange spammere bruker fingerte avsenderdomener som ikke finnes

Hvorfor ikke?

- Mange falske positiver fordi mailservere mangler reversoppslag (ca. 30%)
- Mange falske positiver fordi Outlook [Express] ikke sender FDQN i Helo-streng, men Netbios-navn!!??

Blacklists (DNSBL)

- Sjekker mot klientens ip-adresse eller navn
- Bruker DNS:
  - sjekk mot ip-adresse 200.1.2.3:
    ```
    host 3.2.1.200.bl.bibsyst.no
    3.2.1.200.bl.bibsyst.no. has address 127.0.0.2
    ```
  - ```
    host -t TXT 3.2.1.200.bl.bibsyst.no
    3.2.1.200.bl.bibsyst.no. text "Blocked" "-"
    "filtered"
    ```
- Lettvektsprotokoll – cacher svaret
- Defacto standard
- NB! logger må følges nøye!
    ```

Blacklists - 2

- http://www.dnsstuff.com/
- http://openrbl.org
- http://moensted.dk/spam/
- http://www.declude.com/junkmail/support/ip4r.htm
- http://blackholes.us/
- http://www.spamcop.net/
- http://www.spamhaus.org/
- ...

Gode blacklists

```
 4855   sbl-xbl.spamhaus.org;
 2899   korea.services.net;
  821   combined.njabl.org;
  733   bl.spamcop.net;
  610   list.dsbl.org;
  426   cn-kr.blackholes.us;
  403   t1.dnsbl.net.au;
  341   bl.bibsyst.no;
   88   japan.blackholes.us;
   44   no-more-funn.moensted.dk;
   29   dsn.rfc-ignorant.org;
   22   russia.blackholes.us;
   21   unconfirmed.dsbl.org;
   16   multihop.dsbl.org;
   12   dul.dnsbl.sorbs.net;
    9   hongkong.blackholes.us;
    6   malaysia.blackholes.us;
    4   cbl.abuseat.org;
    3   turkey.blackholes.us;
    3   thailand.blackholes.us;
    3   psbl.surriel.com;
    1   porn.rhs.mailpolice.com;
    1   dnsbl.sorbs.net;
    1   bulk.rhs.mailpolice.com;

Sun Dec 26 23:55:08 CET 2004
```

Effektivitet

Rejected %	#	Blocklist
65.54	56,529	t1.dnsbl.net.au
50.23	43,324	blackholes.five-ten-sg.com
49.19	42,424	sbl-xbl.spamhaus.org
44.67	38,529	xbl.spamhaus.org
44.26	38,175	cbl.abuseat.org
41.87	36,114	dnsbl.sorbs.net
38.80	33,465	rbl-plus.mail-abuse.org
35.60	30,710	bl.spamcop.net
32.21	27,784	unconfirmed.dsbl.org
31.83	27,457	list.dsbl.org
31.17	26,885	dsbl.dnsbl.net.au
24.60	21,216	no-more-funn.moensted.dk
16.94	14,612	bl.csma.biz
12.48	10,765	combined-hib.dnsiplists.completewhois.com
12.04	10,381	dnsbl.njabl.org
7.89	6,806	l1.spews.dnsbl.sorbs.net

Falske positiver

Table 2
MX hosts of Actual Correspondents
(lower numbers are better)

Listed %	MX hosts #	list name
3.18	169	unconfirmed.dsbl.org
1.32	70	blackholes.five-ten-sg.com
0.81	43	bl.csma.biz
0.62	33	no-more-funn.moensted.dk
0.55	29	l1.spews.dnsbl.sorbs.net
0.53	28	t1.dnsbl.net.au
0.38	20	rbl-plus.mail-abuse.org
0.30	16	dnsbl.sorbs.net
0.24	13	combined-hib.dnsiplists.completewhois.com
0.23	12	dnsbl.njabl.org
0.04	2	list.dsbl.org
0.04	2	dsbl.dnsbl.net.au
0.02	1	sbl-xbl.spamhaus.org
0.00	0	cbl.abuseat.org
0.00	0	bl.spamcop.net

Ikke bruk disse DNSBL

(aggressive/for mange falske positiver)

- block.blars.org
- dnsbl.JAMMConsulting.com
- ipwhois.rfc-ignorant.org
- misc.spam.blackholes.five-ten-sg.com

Nyttige linker

- www.dnsstuff.com
  sjekker ip-adresse mot flere hundre RBL
- www.dnsreport.com
  sjekker oppsett av DNS
- http://www.norid.no/domenenavnbaser/zonecheck/NORID's sonesjekk
- http://bind8nt.meiway.com/itsaDNSmess.cfm
  Is my DNS a mess?
- http://www.trusontechnologies.com/services/spam_tester.php
  Relay tester
- http://www.whois.sc/1.2.3.4
  Whois database oppslag

Ulemper ved bruk av RBL

- FP
- Rammer vidt
- Overhead
- ...

Falske positiver (FP)

Oppgitte avsendere for avvist epost:

Ant.	Type	Adresse
1	(Spam)	tanya_hicks_bg@alphasystem.no
1	(Virus: .zip)	mk@brimer.no
1	(Spam)	rjhasle@online.no
1	(Virus: .scr)	ben@ssb.no
1	(Virus: .pif)	9exxe@9.5
1	(Spam)	mslaterhv@altendorfer.at
6	(Spam)	cartermathers@bestadultsites.biz
9	(Spam)	wayorschambers@zipmail.com.br
1	(Spam)	warnerrm@cim.mcgill.ca
1	(Spam)	josie_ramseyun@astarte.ch
3	(Spam)	apache@alumnos.ceat.cl

Bayesian filtering

- Analysere spam/ham for kombinasjoner av ord
- Beregner sannsynlighet for spam
- Mozilla/Thunderbird har dette
- Popfile
- Bogofilter
- For lite presisjon alene, kan brukes sammen med andre teknikker (SpamAssassin)

Sender Policy Framework (SPF)

- Autentisere avsender domene:
- `host -t TXT bibsyst.no`

  ```
  bibsyst.no text "v=spf1 mx mx:hasle.com mx:kogstad.org
  mx:morkemo.com -all"
  ```

  `host -t MX bibsyst.no`

  ```
  bibsyst.no mail is handled by 5 bibsyst.bibsyst.no.
  ```

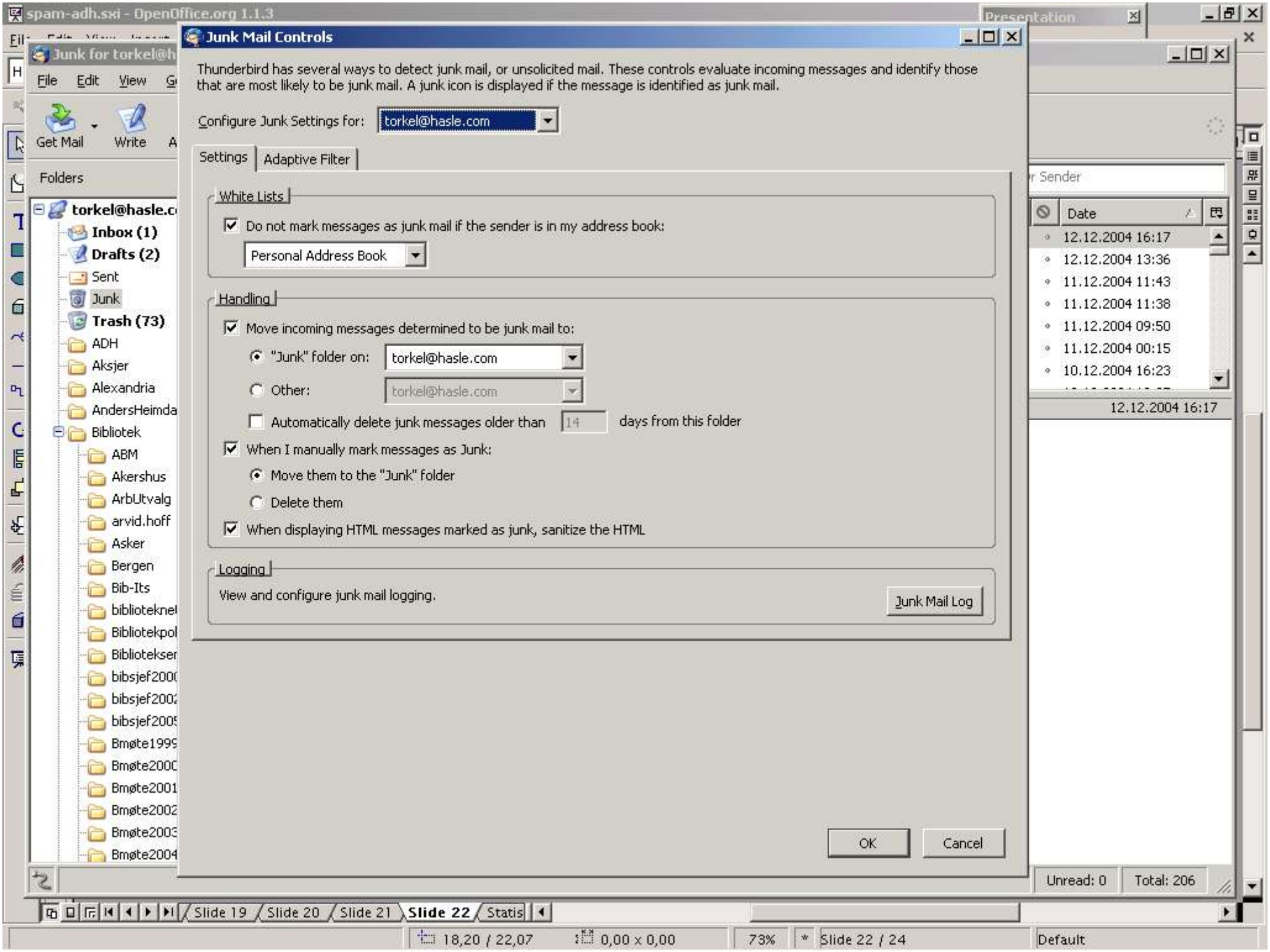
  `host -t A bibsyst.bibsyst.no`

  ```
  bibsyst.bibsyst.no has address 193.90.32.70
  ```

- NB! Håndterer ikke forwarding

Spamassassin 3.0

```
X-Spam-Prev-Subject: CHEAPEST D*R-U-G-S ON THE WEB freeze
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.0.0 (2004-09-13) on linuxadm.bsint.no
X-Spam-Level: **********************************
X-Spam-Status: Yes, score=31.7 required=5.0 tests=BAYES_50,GAPPY_SUBJECT,
    HELO_DYNAMIC_IPADDR2,LONGWORDS,MIME_BOUND_DD_DIGITS,RATWARE_RCVD_AT,
    UNRESOLVED_TEMPLATE,URIBL_OB_SURBL,URIBL_SBL,URIBL_SC_SURBL,
    URIBL_WS_SURBL,X_MESSAGE_INFO autolearn=no version=3.0.0
X-Spam-Report:
    *  2.9 UNRESOLVED_TEMPLATE Headers contain an unresolved template
    *  4.1 MIME_BOUND_DD_DIGITS Spam tool pattern in MIME boundary
    *  1.3 GAPPY_SUBJECT Subject: contains G.a.p.p.y-T.e.x.t
    *  3.5 HELO_DYNAMIC_IPADDR2 Relay HELO'd using suspicious hostname (IP addr 2
    *  4.2 X_MESSAGE_INFO Bulk email fingerprint (X-Message-Info) found
    *  3.4 RATWARE_RCVD_AT Bulk email fingerprint (Received @) found
    *  0.0 BAYES_50 BODY: Bayesian spam probability is 40 to 60%
    *      [score: 0.5000]
    *  1.0 URIBL_SBL Contains an URL listed in the SBL+XBL blocklist
    *      [URIs: getthatpills.com]
    *  1.5 URIBL_WS_SURBL Contains an URL listed in the WS SURBL blocklist
    *      [URIs: getthatpills.com]
    *  3.2 URIBL_OB_SURBL Contains an URL listed in the OB SURBL blocklist
    *      [URIs: getthatpills.com]
    *  4.3 URIBL_SC_SURBL Contains an URL listed in the SC SURBL blocklist
    *      [URIs: getthatpills.com]
    *  2.3 LONGWORDS Long string of long words
```


spam-adh.sxi - OpenOffice.org 1.1.3
Junk for torkel@h
File Edit View
Get Mail
Write
Folders
torkel@hasle.c
Inbox (1)
Drafts (2)
Sent
Junk
Trash (73)
ADH
Aksjer
Alexandria
AndersHeimda
Bibliotek
ABM
Akershus
ArbUtvalg
arvid.hoff
Asker
Bergen
Bib-Its
Bmøte1999
Bmøte2000
Bmøte2001
Bmøte2002
Bmøte2003
Bmøte2004
Junk Mail Controls
Thunderbird has several ways to detect junk mail, or unsolicited mail. These controls evaluate incoming messages and identify those that are most likely to be junk mail. A junk icon is displayed if the message is identified as junk mail.
Configure Junk Settings for:
torkel@hasle.com
Settings
Adaptive Filter
White Lists
Do not mark messages as junk mail if the sender is in my address book:
Personal Address Book
Handling
Move incoming messages determined to be junk mail to:
"Junk" folder on:
torkel@hasle.com
Other:
torkel@hasle.com
Automatically delete junk messages older than
14
days from this folder
When I manually mark messages as Junk:
Move them to the "Junk" folder
Delete them
When displaying HTML messages marked as junk, sanitize the HTML
Logging
View and configure junk mail logging.
Junk Mail Log
OK
Cancel
Presentation
Sender
Date
12.12.2004 16:17
12.12.2004 13:36
11.12.2004 11:43
11.12.2004 11:38
11.12.2004 09:50
11.12.2004 00:15
10.12.2004 16:23
12.12.2004 16:17
Unread: 0
Total: 206
Slide 19
Slide 20
Slide 21
Slide 22
Statis
18,20 / 22,07
0,00 x 0,00
73%
Slide 22 / 24
Default

Spamtrap

- 99% av post til secondary MX er spam!
- Smtptrapd benytter dette for å «fange» spam
- Ip-adressene kan danne grunnlag for RBL
- ftp://ftp.mfi.com/pub/sysadmin/2004/aug2004supplement.zip

Hvordan sette opp RBL

Definere en egen sone i DNS:

```
// blacklists
zone "bl.bibsyst.no" {
    type master;
    file "db.virus";
};
```

- Sonefilen (db.virus):

```
*.200   IN      A       127.0.0.2
*.200   IN      TXT     Blocked - filtered
*.201   IN      A       127.0.0.2
*.201   IN      TXT     Blocked - filtered
```

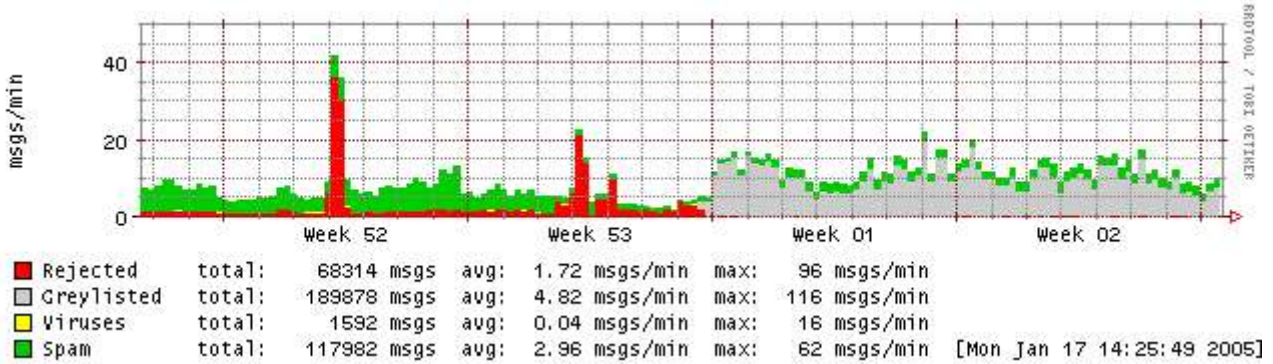
Greylisting

- Ved første oppkobling fra en ny server: gi 450-feilmelding (try again), og tillat oppkobling igjen etter 5-60 minutter
- Spammere (og virus) gir opp etter ett forsøk?
- www.greylisting.org
- +++ enkelt, effektivt, lite FP
- (-) forsinker leveranse av mail

Greylisting -2

- Ikke bruk standardversjonen som følger med Postfix
- Bruk istedet Postgrey http://isg.ee.ethz.ch/tools/postgrey/
- Default action: DEFER_IF_PERMIT
- Bedre: 451
- Ikke bruk DEFER (feil!!)

Før/etter greylisting



Originale forslag

- http://www.feedbackarchive.com/spamvampire/
- http://it.slashdot.org/article.pl?sid=04/12/09/1918205&tid=111
- Zucchini method

Statistikk uke 50/2003

Mottatt:	138 000
Blokkert (oppkoblinger):	132 000
SUM:	270 000
Virus:	254
Stoppet:	185 000

Andel spam:	**68%**
Effekt:	**99,968%**
FP:	**0,009%**

Tips:

- Legg aldri epostadresse på web-sider
- Bruk aldri mailto-link
- Bruk heller kontaktside med forms
- Bruk forskjellige epostadresser for hver gang du registrerer deg hos en leverandør
- Hvis du absolutt må legge ut mailadressen, bruk f.eks.
  - torkel at hasle dot com
  - torkel%40hasle%2Ecom
  - torkel@hasle.com
  - eller bruk Javascript

Konklusjon

- Det nytter å stoppe spam!
- Still høye krav til konfigurasjon av egen mailserver
- Bruk teknologien så langt som mulig
- OpenSource verktøy er mer enn gode nok!
- Ingen menneskerett å sende {exe,zip}-filer som vedlegg til mail
- Hvis ikke vi gjør **NOK nå,** vil nettet til slutt bli overbelastet og dø

Spørsmål?