Spam Prevention using Maia Mailguard

Tanner Lovelace
North Carolina System Administrators

9/May/2005

The Spam Problem

- Spam seems to be growing at an exponential rate
- Running without some sort of spam filter is not an option anymore
- However, one size doesn't fit all.
  - Users need to adjust their own settings

Assumptions

- You know or already have a mail server setup
- You've heard of (or at least can lookup) amavisd-new, spamassassin, and various virus filters.

What is amavisd-new?

- Framework for mail filtering
  - Virus scanning
  - Spam filtering
  - Banning dangerous attachments
  - Handling invalid mail headers
- Filtering policies
- Quarantine and notification

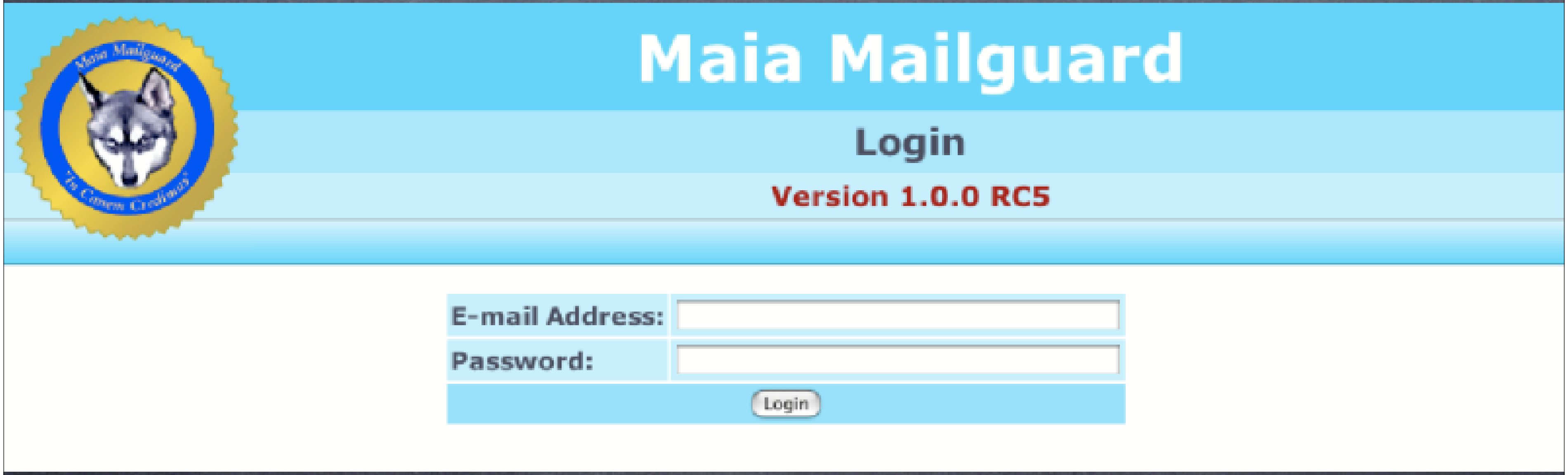
What is SpamAssassin?

- Spam Filtering
  - Feature recognition
  - Lookups
  - Collaborative reporting networks
  - Bayesian learning mechanisms

Maia Mailguard

- Began as simple web interface to amavisd-new
- Expanded over time to become complete system
  - PHP, SQL and Perl scripts
  - Database (MySQL or PostgreSQL)
  - amavisd-new, SpamAssassin, and virus scanners

Web Interface

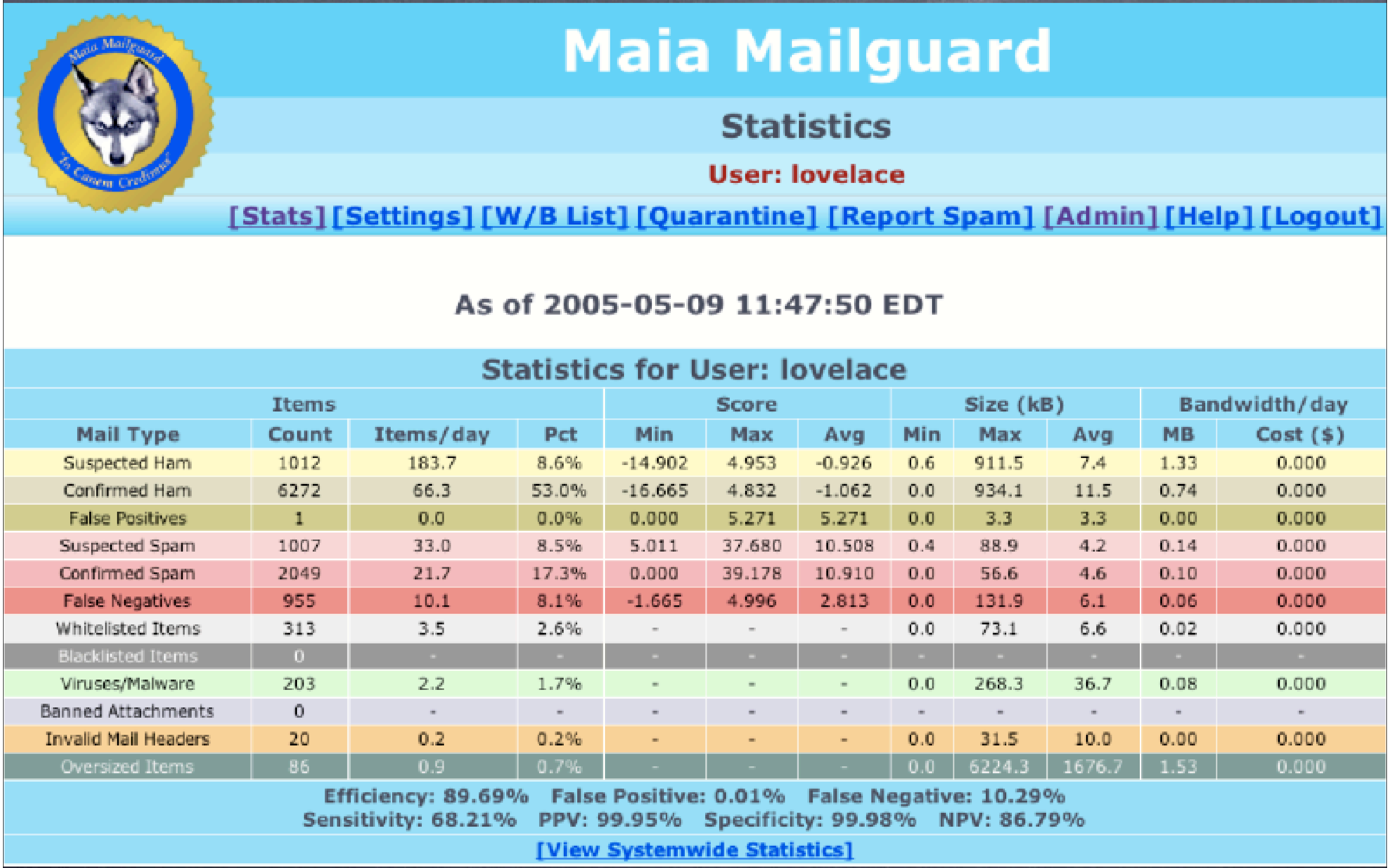


Maia Mailguard

Login

Version 1.0.0 RC5

E-mail Address:	
Password:	



Maia Mailguard

Statistics

User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

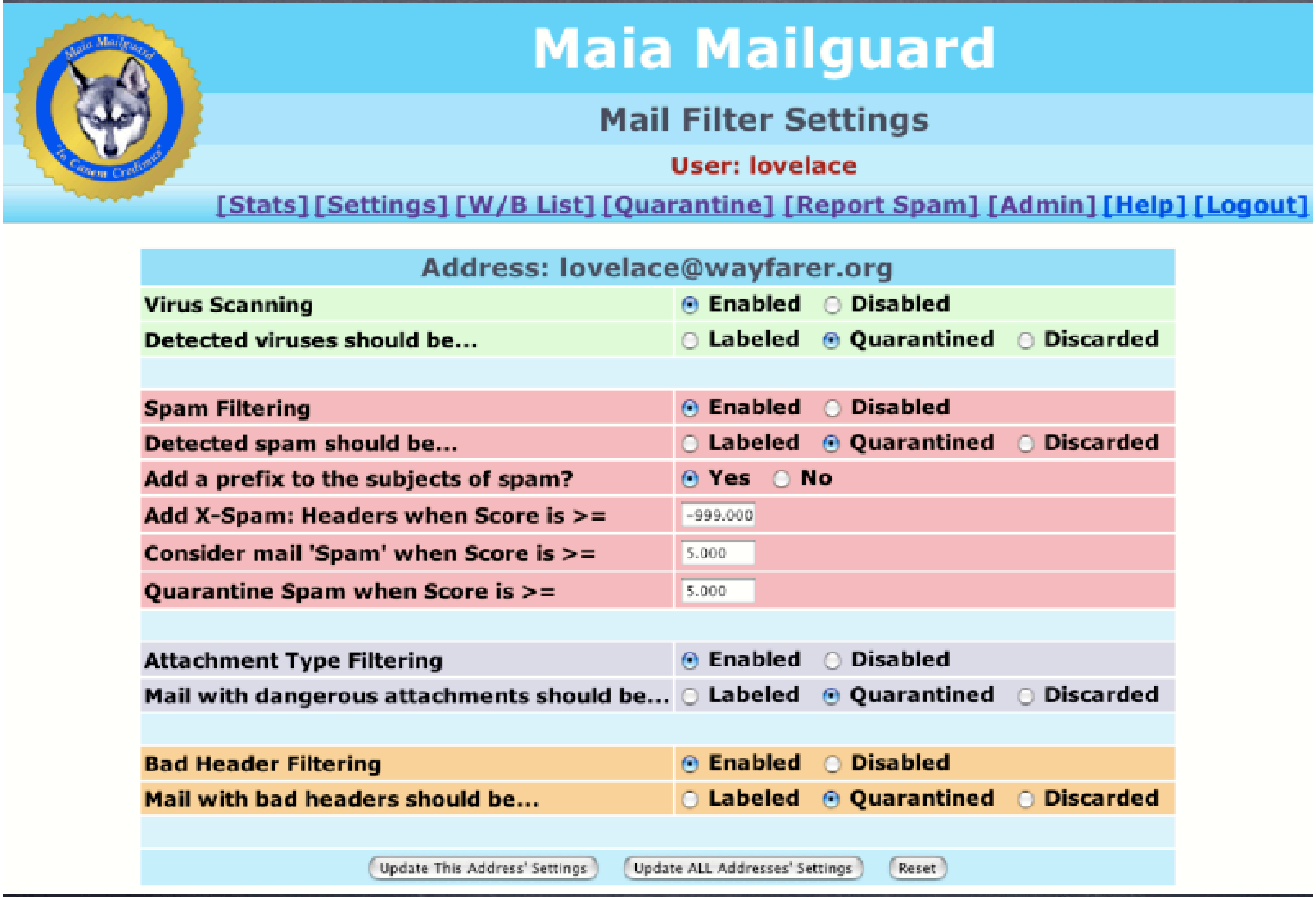
As of 2005-05-09 11:47:50 EDT

Statistics for User: lovelace

	Items			Score			Size (kB)			Bandwidth/day	
Mail Type	Count	Items/day	Pct	Min	Max	Avg	Min	Max	Avg	MB	Cost ($)
Suspected Ham	1012	183.7	8.6%	-14.902	4.953	-0.926	0.6	911.5	7.4	1.33	0.000
Confirmed Ham	6272	66.3	53.0%	-16.665	4.832	-1.062	0.0	934.1	11.5	0.74	0.000
False Positives	1	0.0	0.0%	0.000	5.271	5.271	0.0	3.3	3.3	0.00	0.000
Suspected Spam	1007	33.0	8.5%	5.011	37.680	10.508	0.4	88.9	4.2	0.14	0.000
Confirmed Spam	2049	21.7	17.3%	0.000	39.178	10.910	0.0	56.6	4.6	0.10	0.000
False Negatives	955	10.1	8.1%	-1.665	4.996	2.813	0.0	131.9	6.1	0.06	0.000
Whitelisted Items	313	3.5	2.6%	-	-	-	0.0	73.1	6.6	0.02	0.000
Blacklisted Items	0	-	-	-	-	-	-	-	-	-	-
Viruses/Malware	203	2.2	1.7%	-	-	-	0.0	268.3	36.7	0.08	0.000
Banned Attachments	0	-	-	-	-	-	-	-	-	-	-
Invalid Mail Headers	20	0.2	0.2%	-	-	-	0.0	31.5	10.0	0.00	0.000
Oversized Items	86	0.9	0.7%	-	-	-	0.0	6224.3	1676.7	1.53	0.000

Efficiency: 89.69% False Positive: 0.01% False Negative: 10.29%
Sensitivity: 68.21% PPV: 99.95% Specificity: 99.98% NPV: 86.79%

[View Systemwide Statistics]



Maia Mailguard

Mail Filter Settings

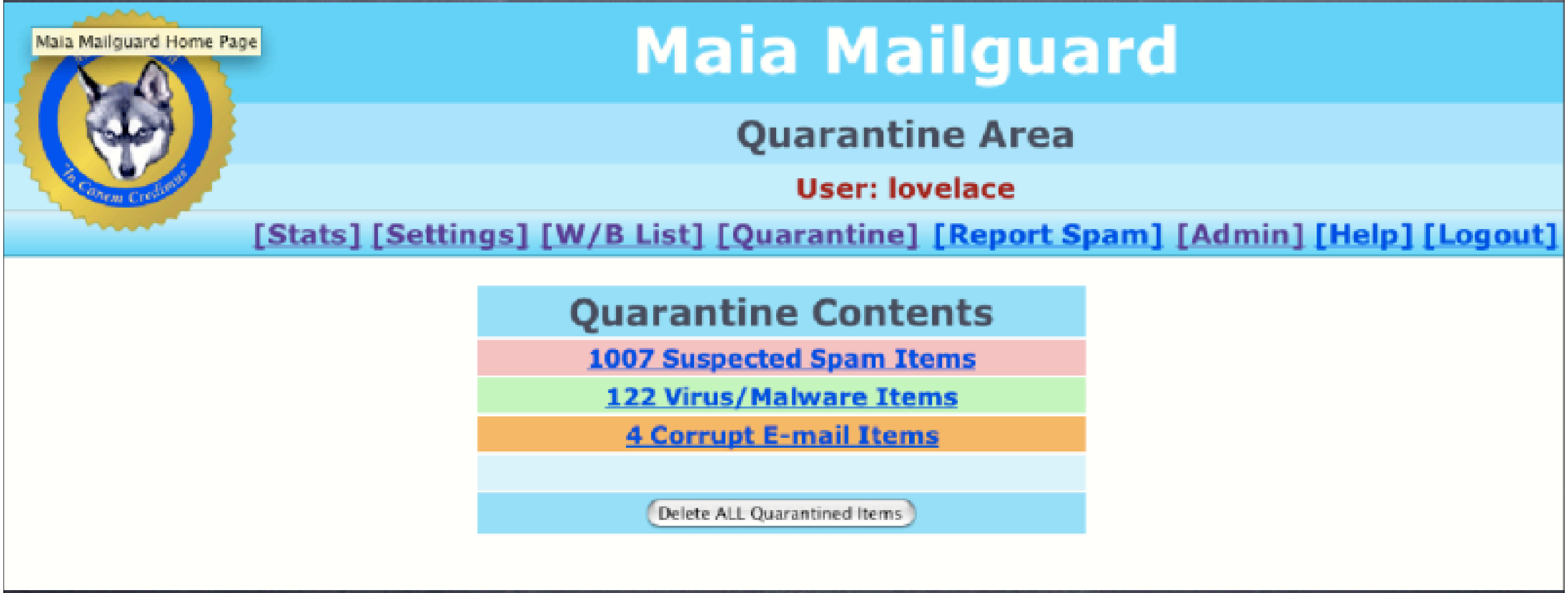
User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

Address: lovelace@wayfarer.org

Virus Scanning	● Enabled ○ Disabled
Detected viruses should be...	○ Labeled ● Quarantined ○ Discarded
Spam Filtering	● Enabled ○ Disabled
Detected spam should be...	○ Labeled ● Quarantined ○ Discarded
Add a prefix to the subjects of spam?	● Yes ○ No
Add X-Spam: Headers when Score is >=	-999.000
Consider mail 'Spam' when Score is >=	5.000
Quarantine Spam when Score is >=	5.000
Attachment Type Filtering	● Enabled ○ Disabled
Mail with dangerous attachments should be...	○ Labeled ● Quarantined ○ Discarded
Bad Header Filtering	● Enabled ○ Disabled
Mail with bad headers should be...	○ Labeled ● Quarantined ○ Discarded

Quarantine Area



Maia Mailguard Home Page
"In Canem Credimus"

Maia Mailguard

Quarantine Area

User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

Quarantine Contents

1007 Suspected Spam Items

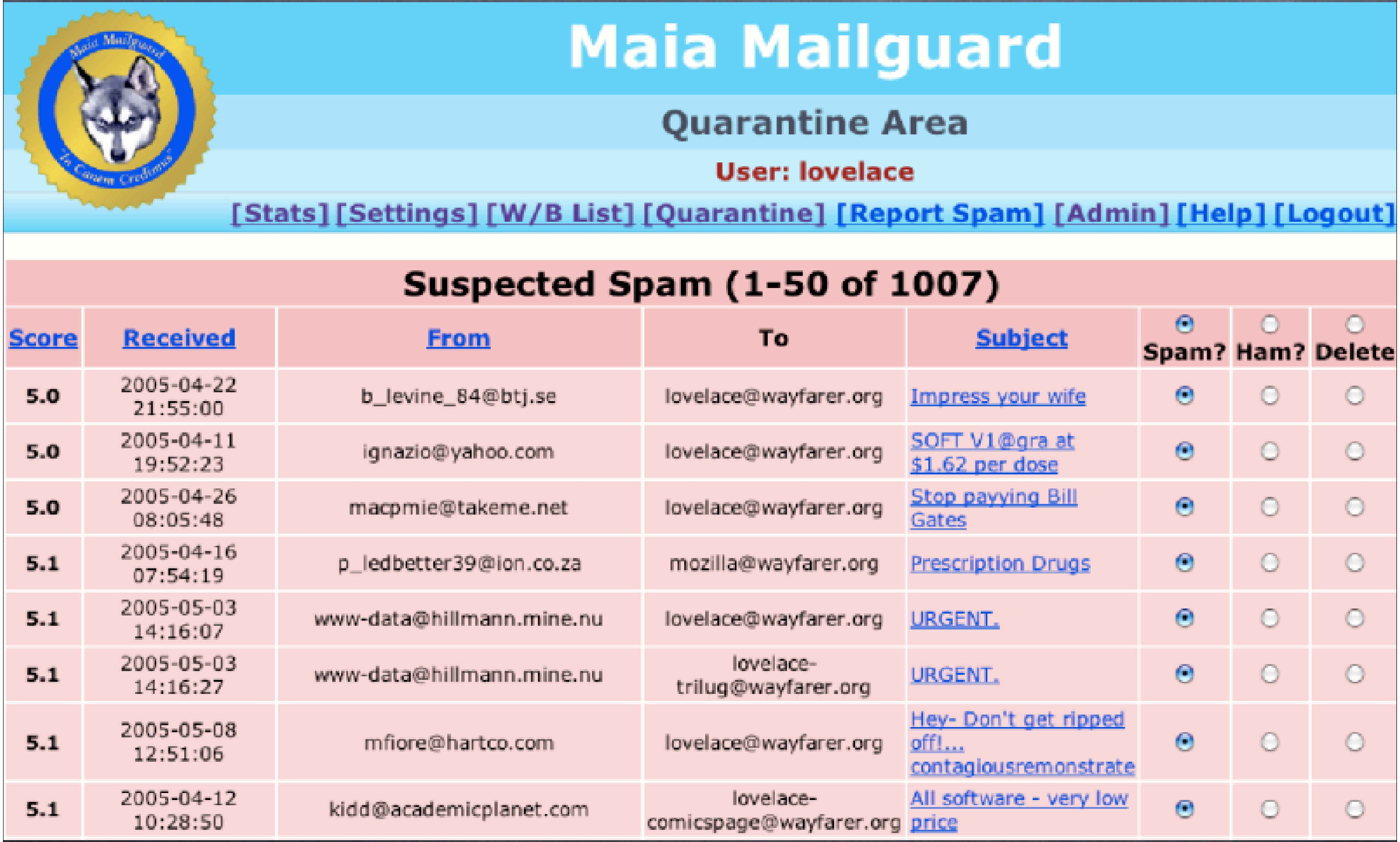
122 Virus/Malware Items

4 Corrupt E-mail Items

Delete ALL Quarantined Items

Spam Quarantine

- Users can manage their own quarantine area
  - Rescue (redeliver) e-mails
  - Confirm as spam
  - Delete
- Users can also report false negatives


[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

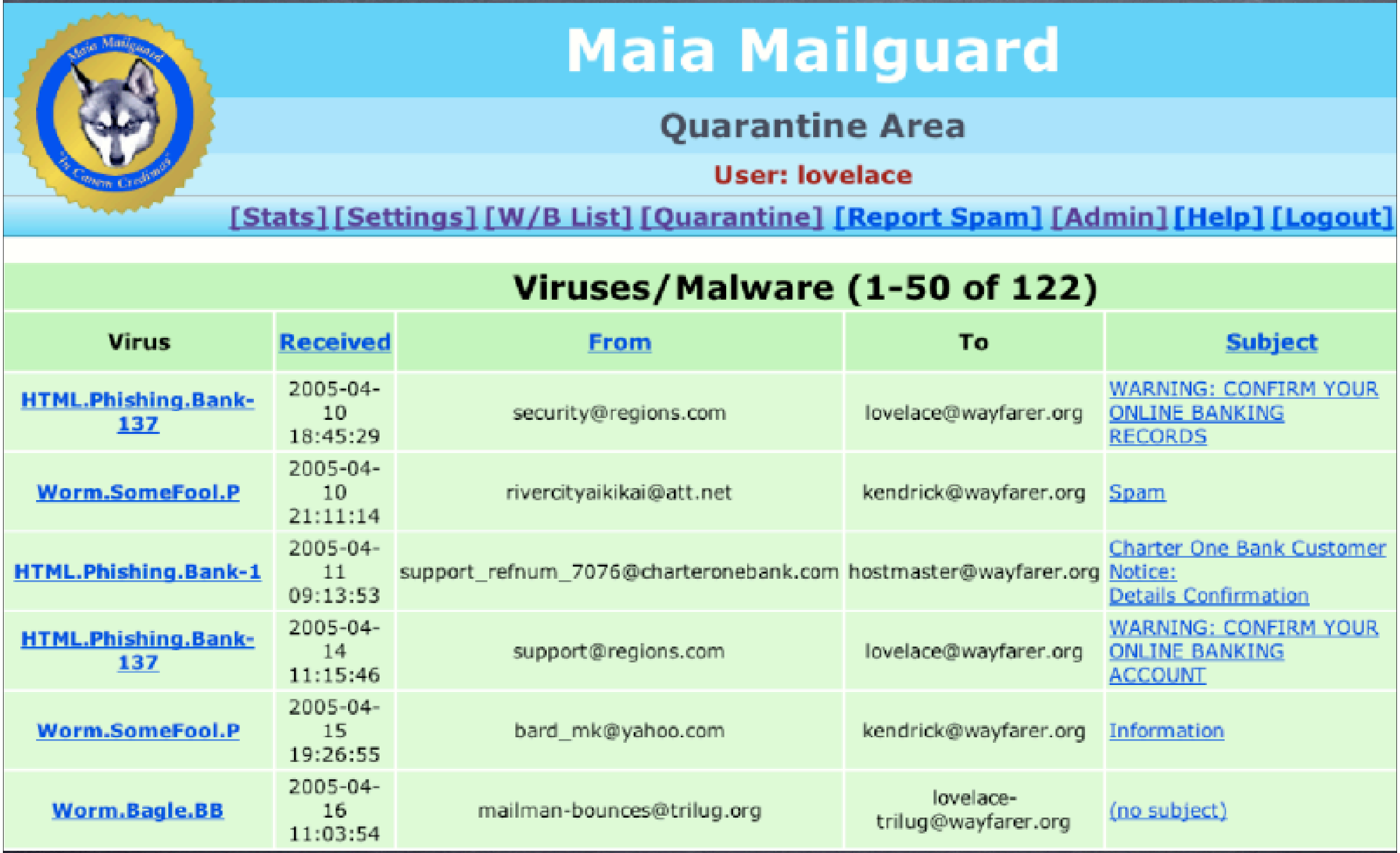
Maia Mailguard

Quarantine Area

User: lovelace

Suspected Spam (1-50 of 1007)

Score	Received	From	To	Subject	● Spam?	○ Ham?	○ Delete
5.0	2005-04-22 21:55:00	b_levine_84@btj.se	lovelace@wayfarer.org	Impress your wife	●	○	○
5.0	2005-04-11 19:52:23	ignazio@yahoo.com	lovelace@wayfarer.org	SOFT V1@gra at $1.62 per dose	●	○	○
5.0	2005-04-26 08:05:48	macpmie@takeme.net	lovelace@wayfarer.org	Stop payying Bill Gates	●	○	○
5.1	2005-04-16 07:54:19	p_ledbetter39@ion.co.za	mozilla@wayfarer.org	Prescription Drugs	●	○	○
5.1	2005-05-03 14:16:07	www-data@hillmann.mine.nu	lovelace@wayfarer.org	URGENT.	●	○	○
5.1	2005-05-03 14:16:27	www-data@hillmann.mine.nu	lovelace-trilug@wayfarer.org	URGENT.	●	○	○
5.1	2005-05-08 12:51:06	mfiore@hartco.com	lovelace@wayfarer.org	Hey- Don't get ripped off!... contagiousremonstrate	●	○	○
5.1	2005-04-12 10:28:50	kidd@academicplanet.com	lovelace-comicspage@wayfarer.org	All software - very low price	●	○	○



Maia Mailguard

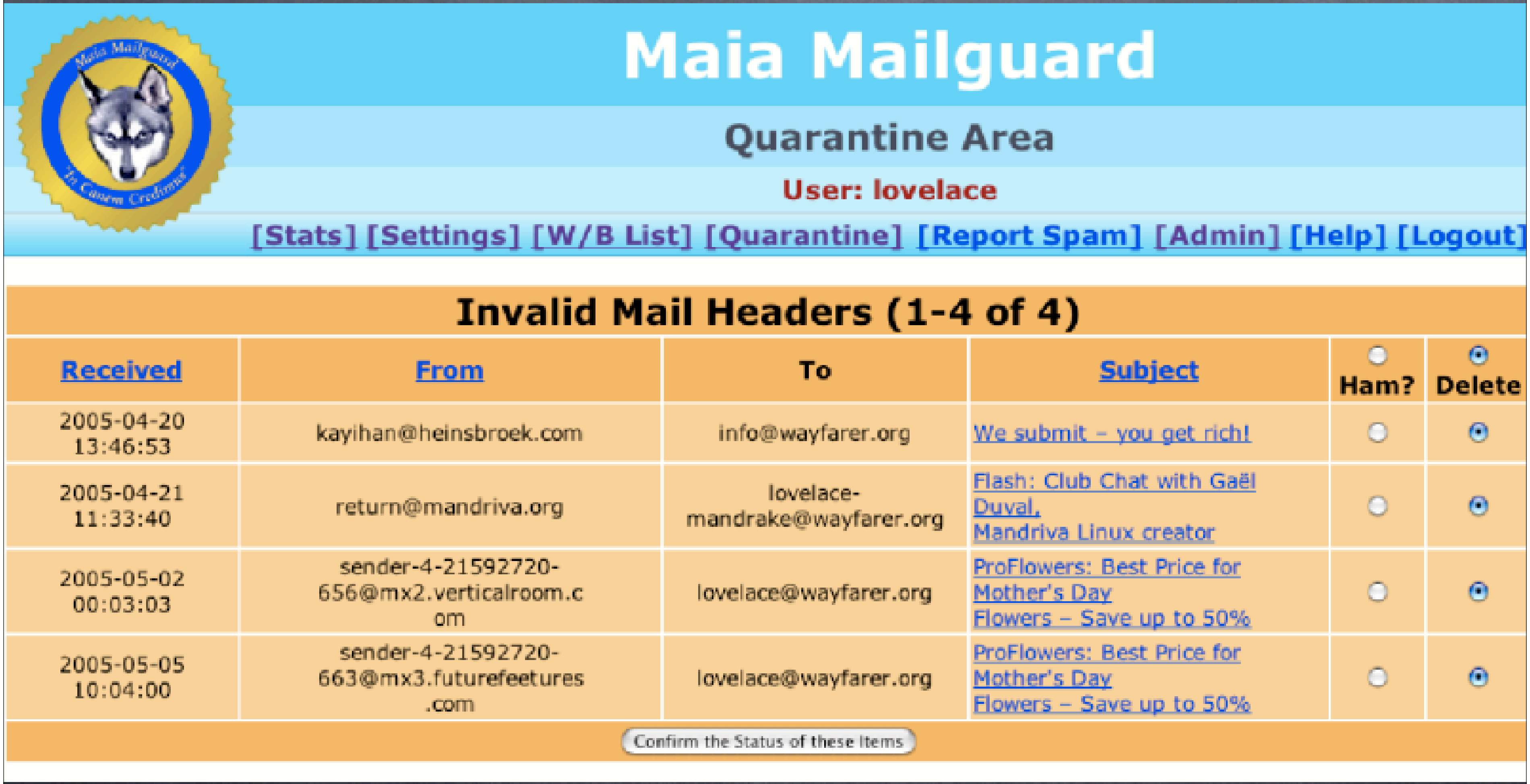
Quarantine Area

User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

Viruses/Malware (1-50 of 122)

Virus	Received	From	To	Subject
HTML.Phishing.Bank-137	2005-04-10 18:45:29	security@regions.com	lovelace@wayfarer.org	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS
Worm.SomeFool.P	2005-04-10 21:11:14	rivercityaikikai@att.net	kendrick@wayfarer.org	Spam
HTML.Phishing.Bank-1	2005-04-11 09:13:53	support_refnum_7076@charteronebank.com	hostmaster@wayfarer.org	Charter One Bank Customer Notice: Details Confirmation
HTML.Phishing.Bank-137	2005-04-14 11:15:46	support@regions.com	lovelace@wayfarer.org	WARNING: CONFIRM YOUR ONLINE BANKING ACCOUNT
Worm.SomeFool.P	2005-04-15 19:26:55	bard_mk@yahoo.com	kendrick@wayfarer.org	Information
Worm.Bagle.BB	2005-04-16 11:03:54	mailman-bounces@trilug.org	lovelace-trilug@wayfarer.org	(no subject)



Maia Mailguard

Quarantine Area

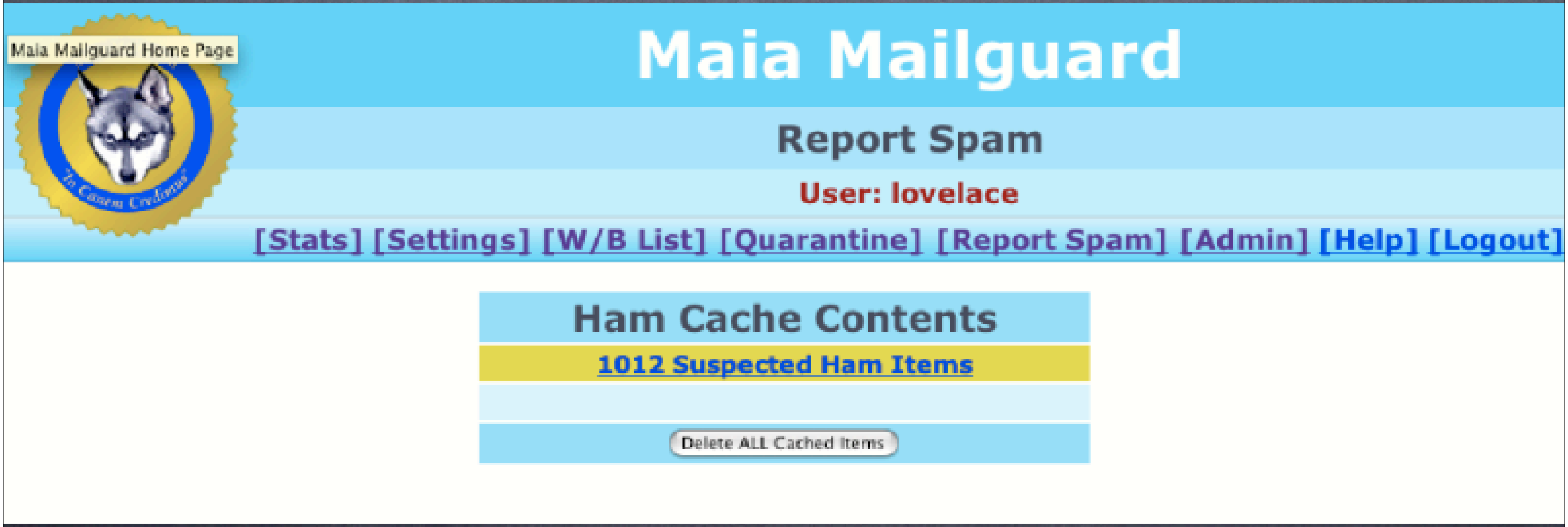
User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

Invalid Mail Headers (1-4 of 4)

Received	From	To	Subject	○ Ham?	● Delete
2005-04-20 13:46:53	kayihan@heinsbroek.com	info@wayfarer.org	We submit - you get rich!	○	●
2005-04-21 11:33:40	return@mandriva.org	lovelace-mandrake@wayfarer.org	Flash: Club Chat with Gaël Duval, Mandriva Linux creator	○	●
2005-05-02 00:03:03	sender-4-21592720-656@mx2.verticalroom.com	lovelace@wayfarer.org	ProFlowers: Best Price for Mother's Day Flowers - Save up to 50%	○	●
2005-05-05 10:04:00	sender-4-21592720-663@mx3.futurefeetures.com	lovelace@wayfarer.org	ProFlowers: Best Price for Mother's Day Flowers - Save up to 50%	○	●

Spam Reporting



Maia Mailguard Home Page
In Canem Credimus

Maia Mailguard

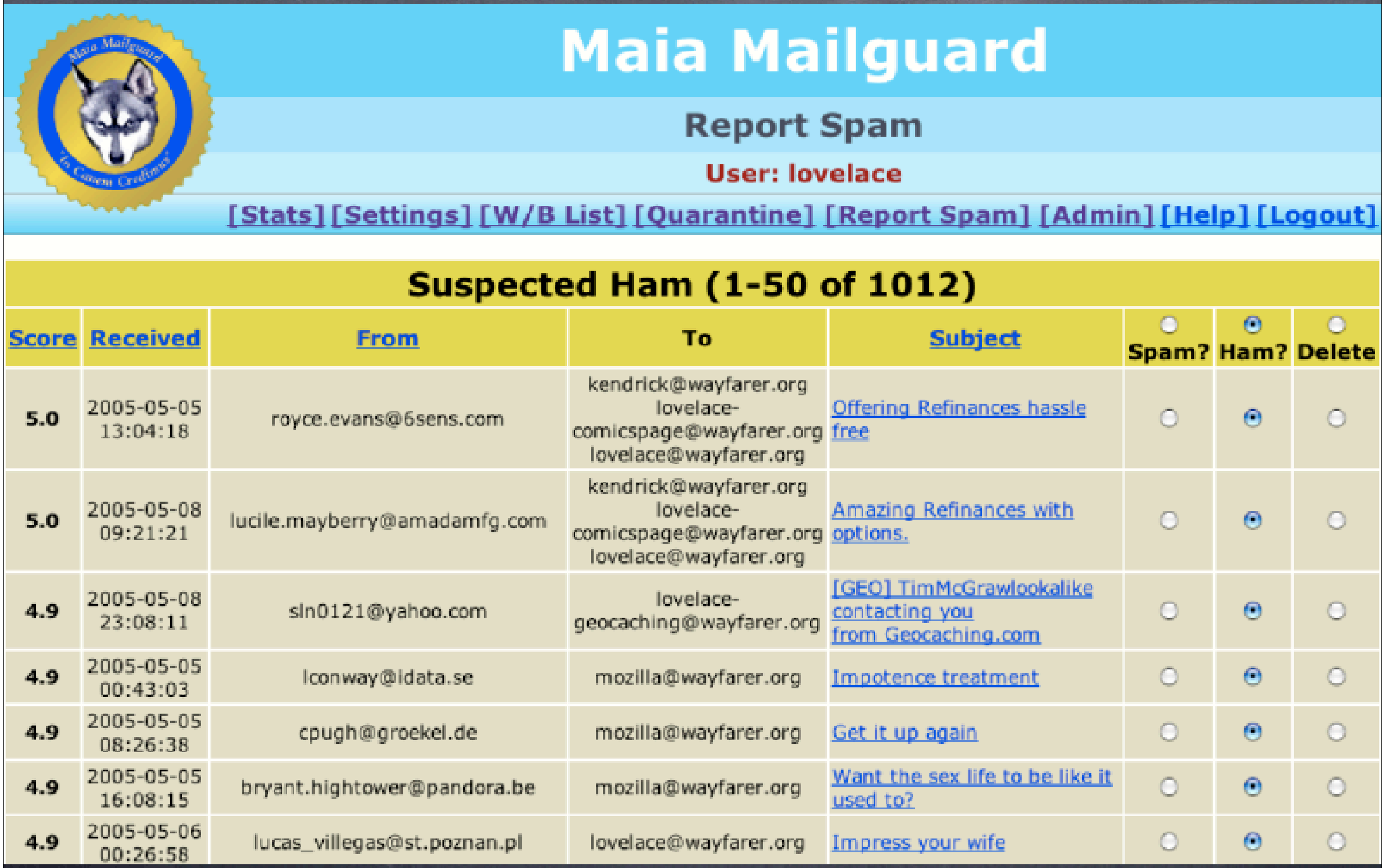
Report Spam

User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

Ham Cache Contents

1012 Suspected Ham Items



Maia Mailguard

Report Spam

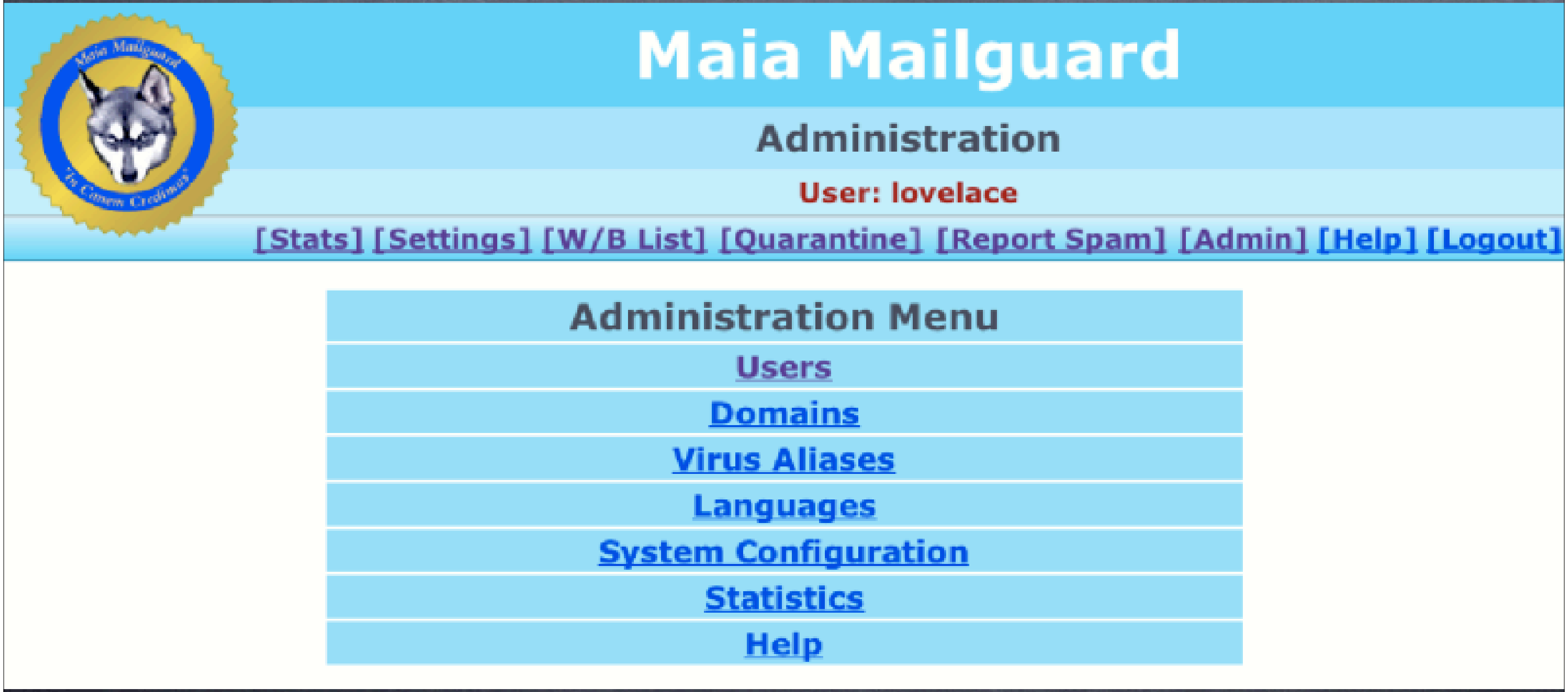
User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

Suspected Ham (1-50 of 1012)

Score	Received	From	To	Subject	○ Spam?	● Ham?	○ Delete
5.0	2005-05-05 13:04:18	royce.evans@6sens.com	kendrick@wayfarer.org lovelace-comicspage@wayfarer.org lovelace@wayfarer.org	Offering Refinances hassle free	○	●	○
5.0	2005-05-08 09:21:21	lucile.mayberry@amadamfg.com	kendrick@wayfarer.org lovelace-comicspage@wayfarer.org lovelace@wayfarer.org	Amazing Refinances with options.	○	●	○
4.9	2005-05-08 23:08:11	sln0121@yahoo.com	lovelace-geocaching@wayfarer.org	[GEO] TimMcGrawlookalike contacting you from Geocaching.com	○	●	○
4.9	2005-05-05 00:43:03	lconway@idata.se	mozilla@wayfarer.org	Impotence treatment	○	●	○
4.9	2005-05-05 08:26:38	cpugh@groekel.de	mozilla@wayfarer.org	Get it up again	○	●	○
4.9	2005-05-05 16:08:15	bryant.hightower@pandora.be	mozilla@wayfarer.org	Want the sex life to be like it used to?	○	●	○
4.9	2005-05-06 00:26:58	lucas_villegas@st.poznan.pl	lovelace@wayfarer.org	Impress your wife	○	●	○

Administration Demo



Maia Mailguard

Administration

User: lovelace

[Stats] [Settings] [W/B List] [Quarantine] [Report Spam] [Admin] [Help] [Logout]

Administration Menu

Users

Domains

Virus Aliases

Languages

System Configuration

Statistics

Help

Maia Mailguard Setup

- Main script is amavisd-new patched to save e-mails to database
- The patched script replaces amavisd-new
  - Run the exact same way as amavisd-new

Behind the Scenes

- Front end is PHP but backend is Perl scripts run by cron.
  - process-quarantine.pl (hourly)
  - expire-quarantine-cache.pl (daily)
  - send-quarantine-reminders.pl (weekly)
  - load-sa-rules.pl (upon SA rule changes)
  - stats-snapshot.pl (hourly at top of hour)

Important things to consider

- Lots of database usage
  - Default MySQL tables lock entire table on writes.
  - Use InnoDB tables instead (row-level locking)

What I'd like to see addressed in the future

- Better e-mail alias management
- Better domain management
- Better documentation on getting good performance
- Mail client integration

Conclusion

- Maia Mailguard is an easy, effective spam/virus management system.
- Users can handle their own policies, training, and quarantine areas.
- Easy to use web interface.

Useful links

- Maia Mailguard home
  - http://www.renaissoft.com/maia/
- Linux Journal article
  - http://www.linuxjournal.com/article/7820