

Bots im Kontext von Spam

Need Captcha Entry Team by urigarin 22.09.08

Posted in [Data Entry](#), [Data Processing](#)

eco AK Sicherheit
Februar 2009

Hello, I need captcha Entry team for various captchas site. I can pay \$.75-1/1k. If you can do more than huge captchas per day. please bid if you are interested system is much faster all time. ... (Budget: \$30-250, Jobs: Data Entry, Data Processing)

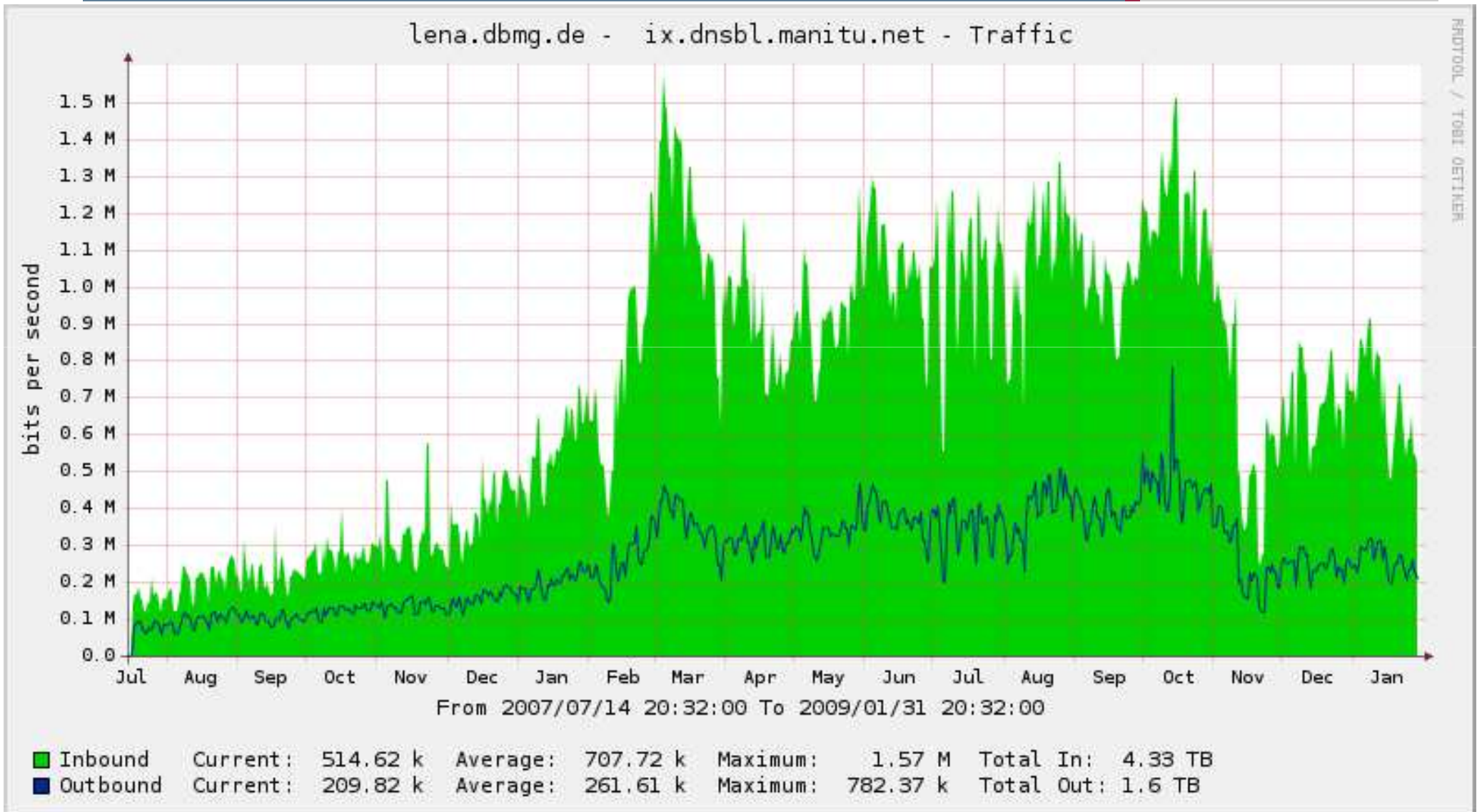
Christian J. Dietrich
dietrich [at] internet-sicherheit . de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
FH Gelsenkirchen

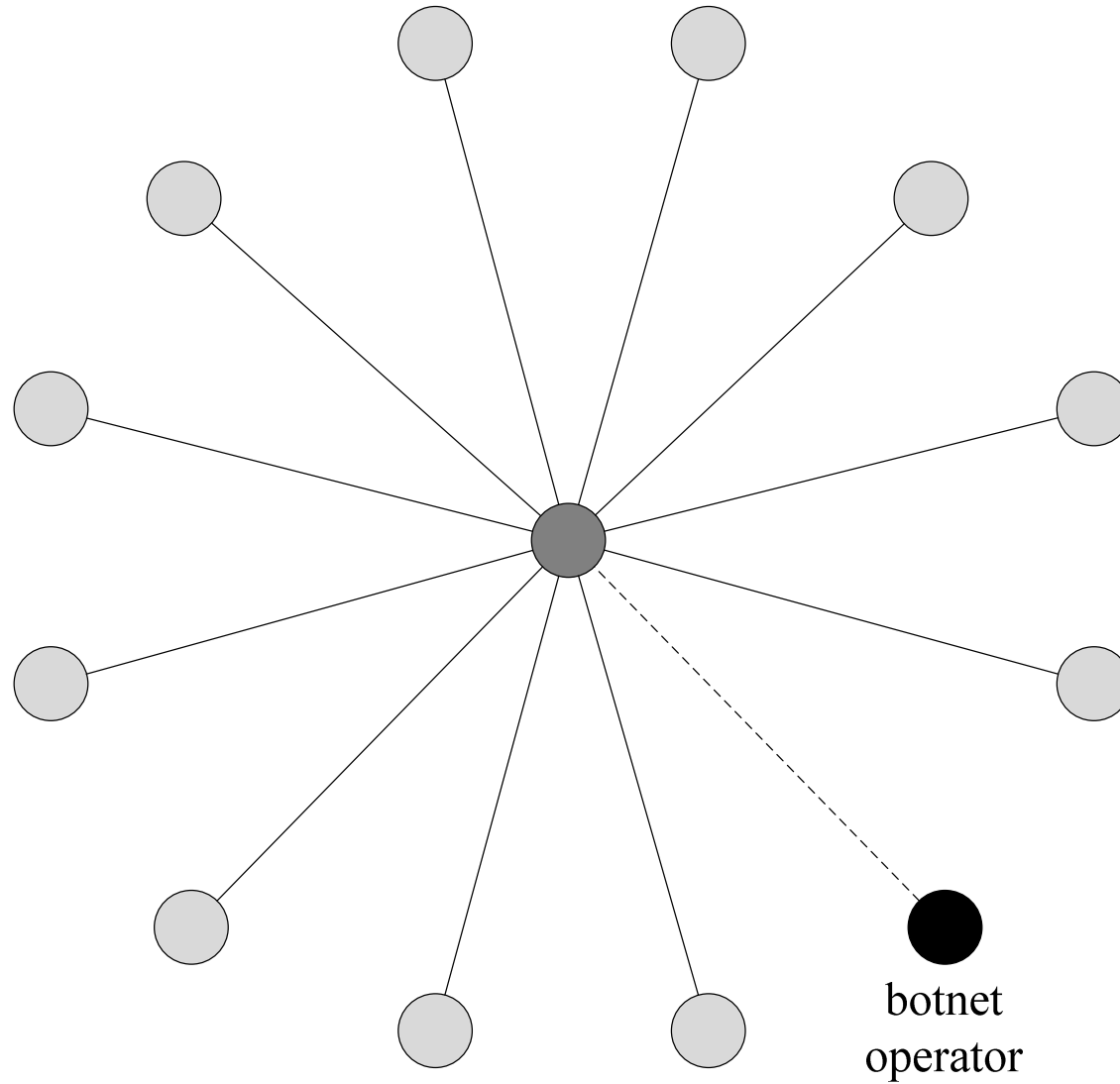


- Einleitung
- **Aktuelle Spam-Entwicklung im Detail**
- Die Tools der Spammer
„Make money fast – the spammer’s way“
- Botnet Security Mechanisms
- Fazit

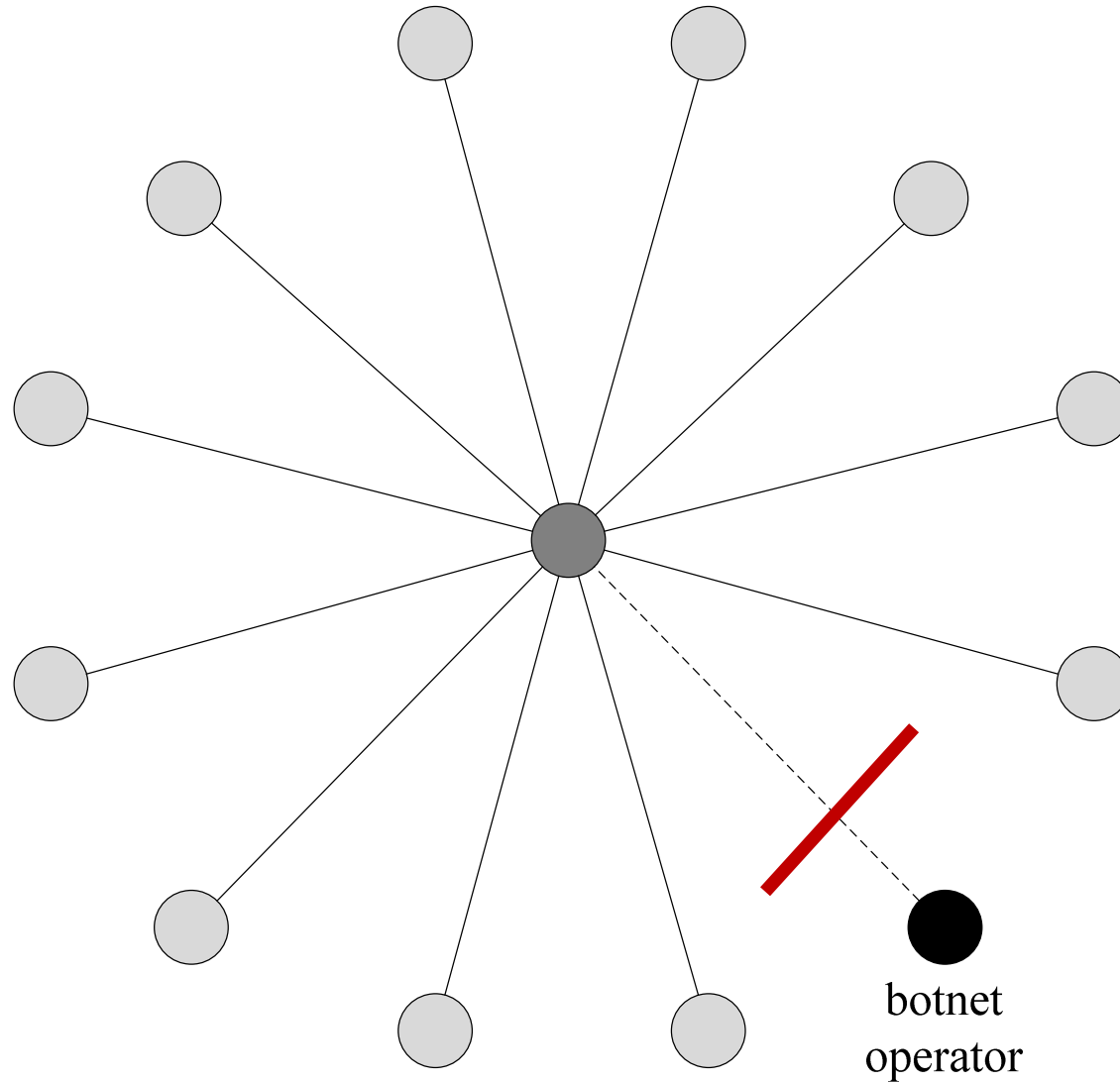
Spam? Wo ist das Problem?



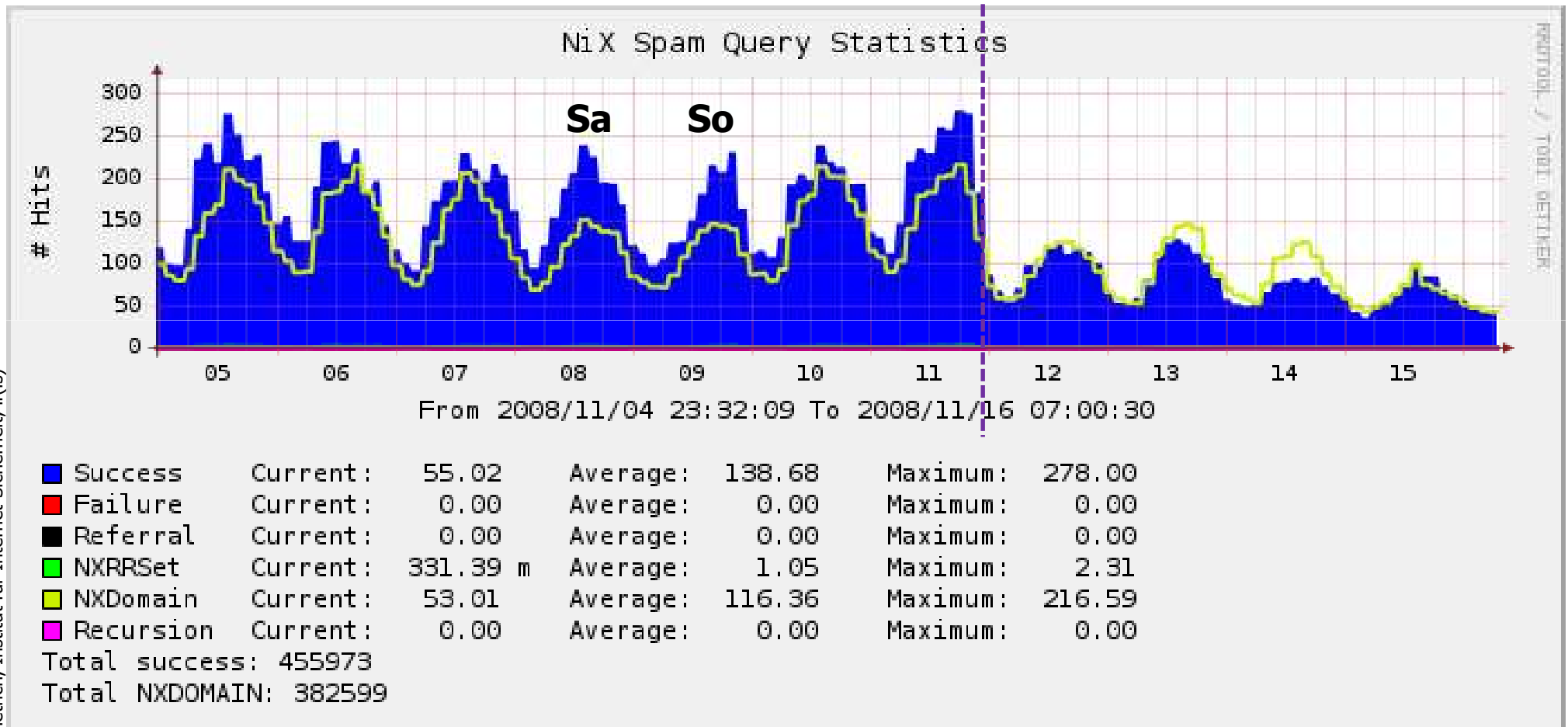
Botnet-Infrastruktur



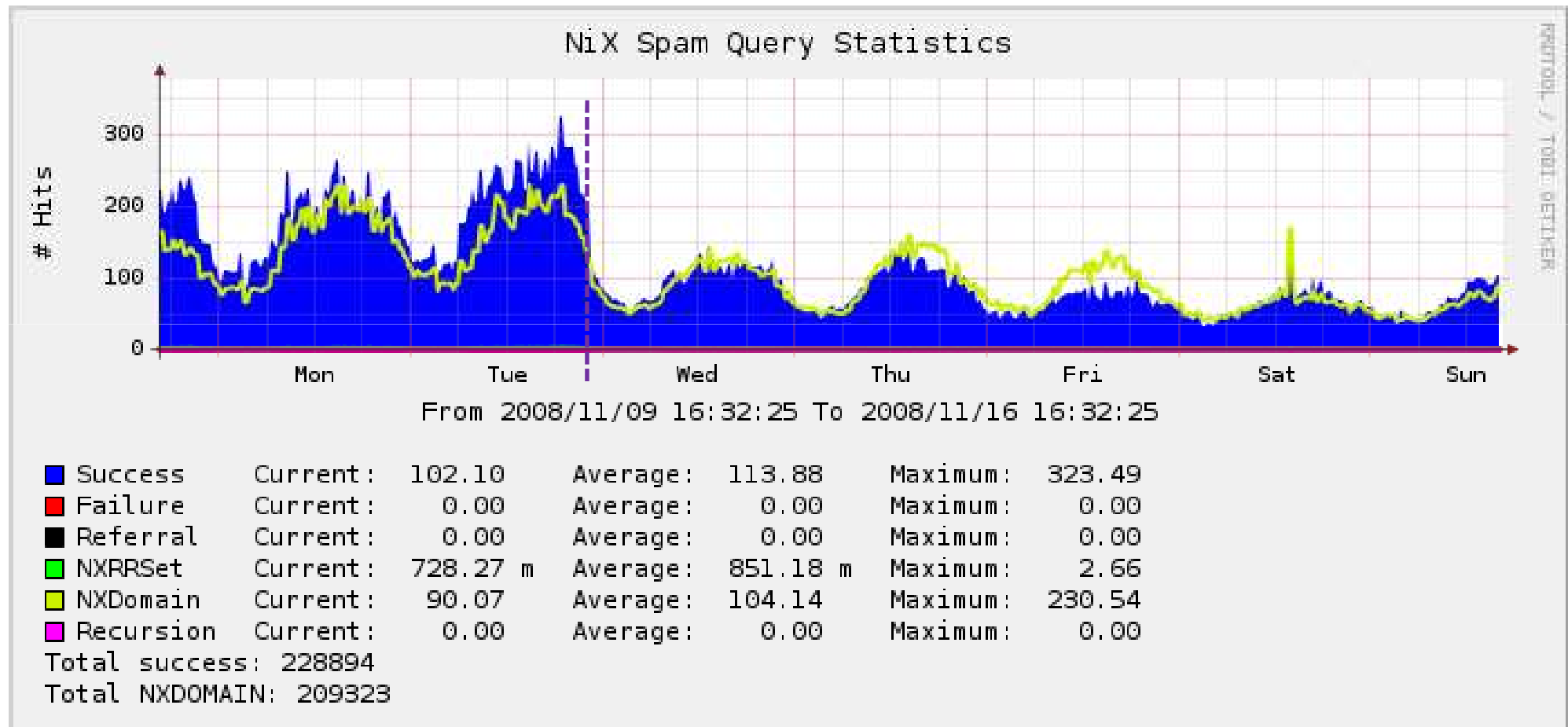
Botnet C&C abgeschnitten



McColo (US ISP) taken offline 11/11/2008

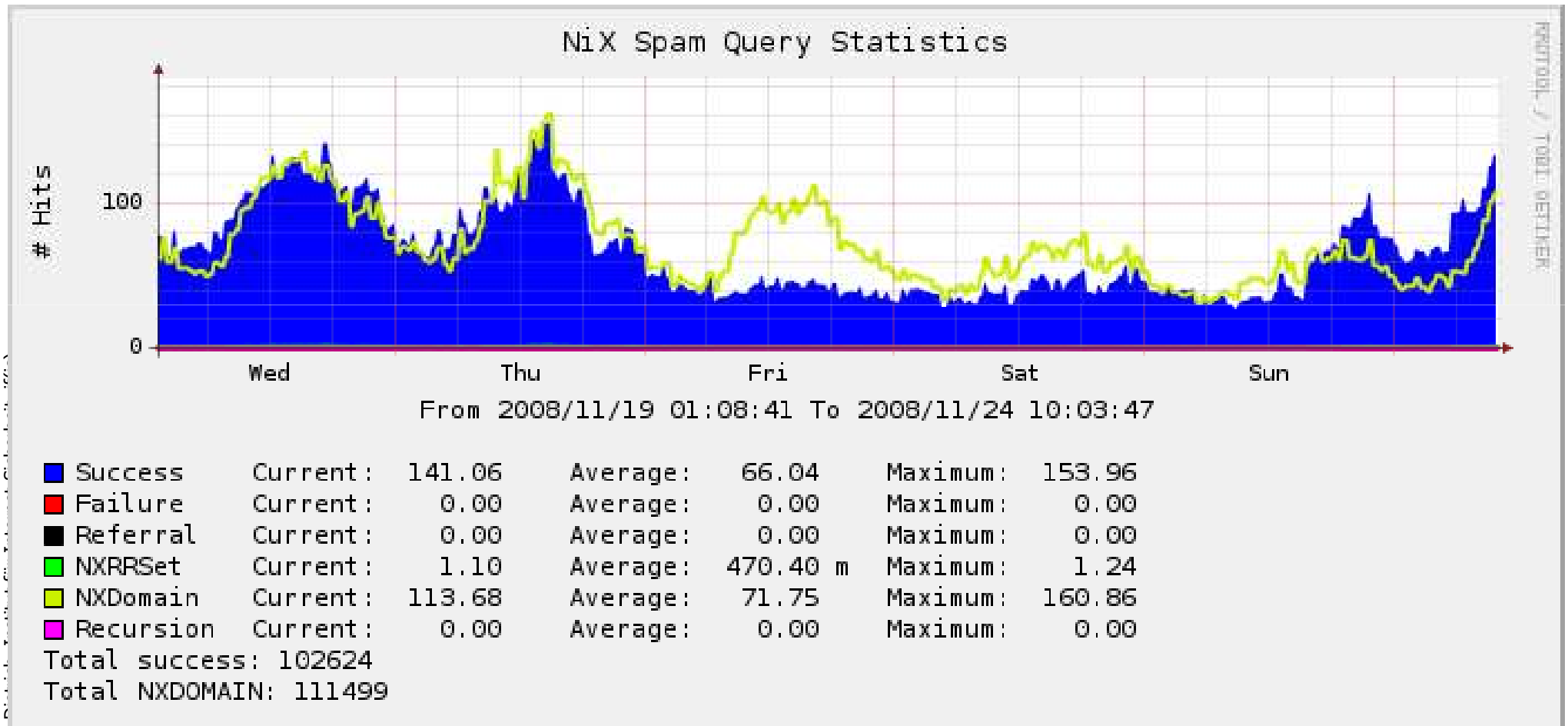


McColo (US ISP) taken offline 11/11/2008



DDoS on InternetX (Schlund NS)

21/11/2008



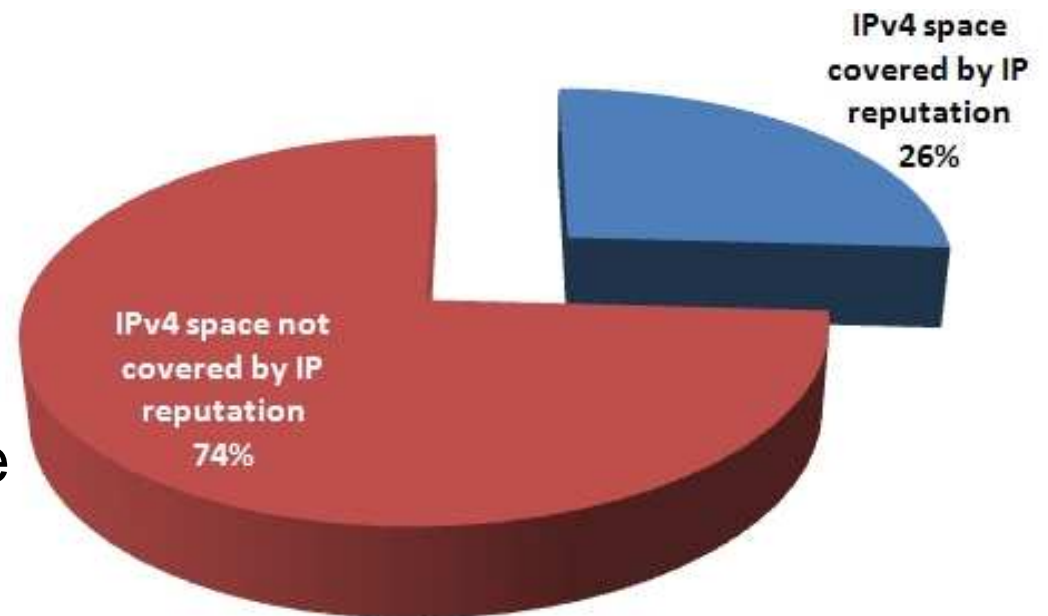
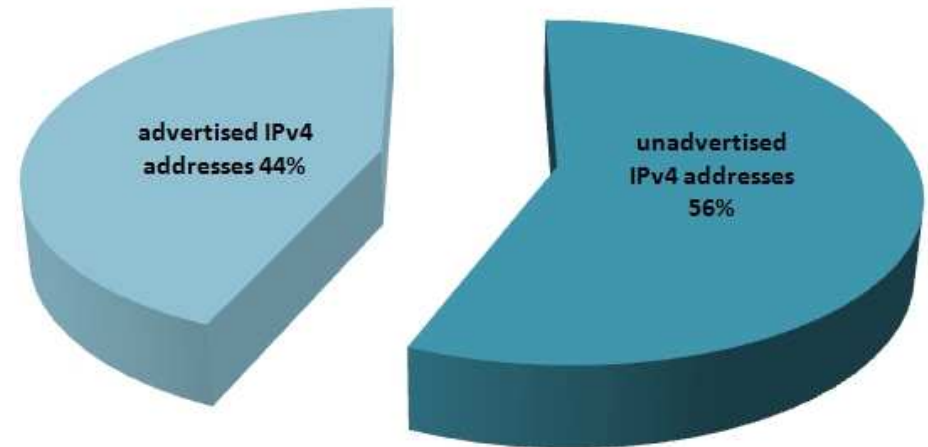
Reputation von IP-Adressen

■ Theorie

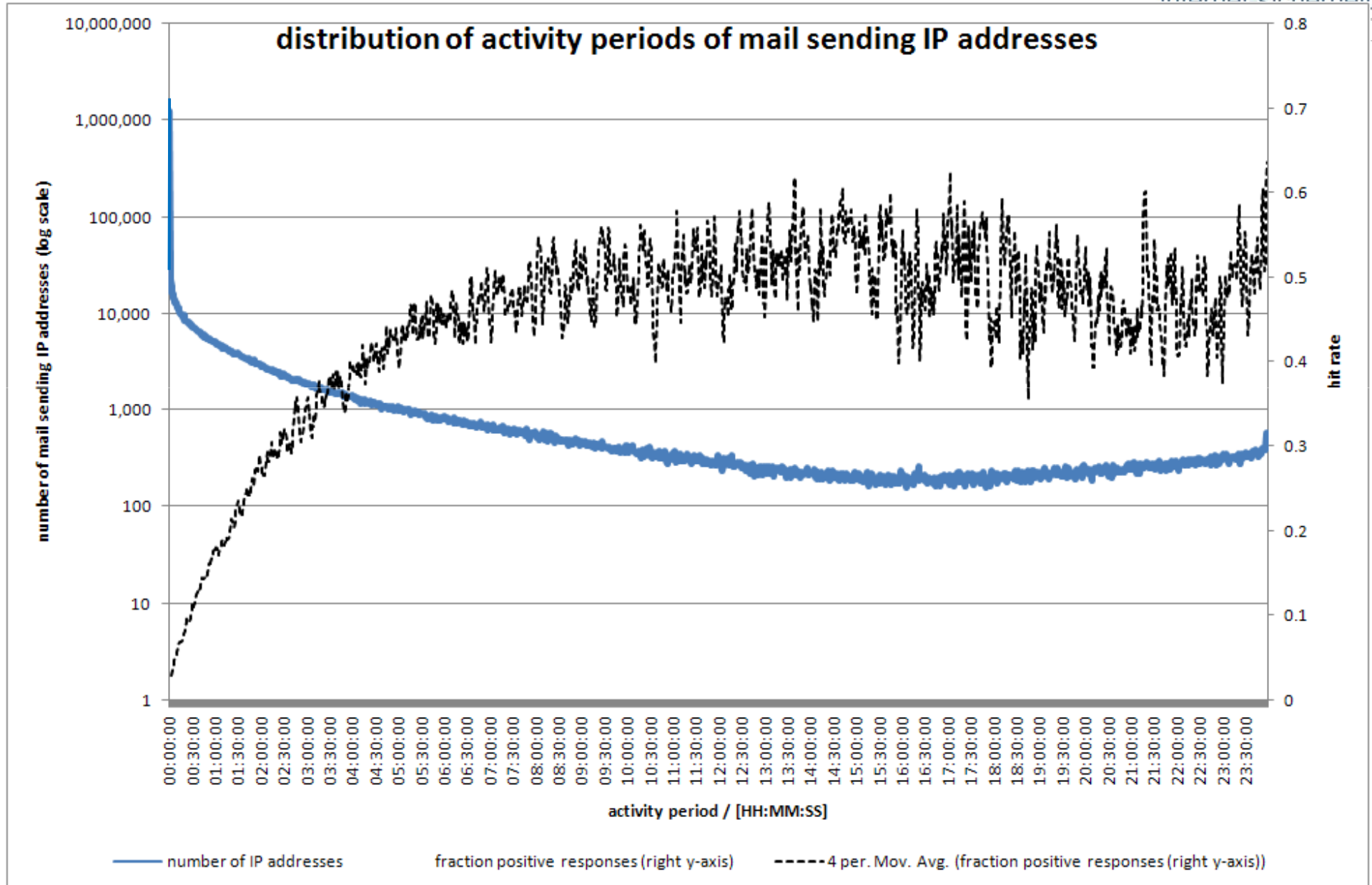
- $2^{32} = 4,2$ Mrd. IPv4-Adressen

■ Praxis

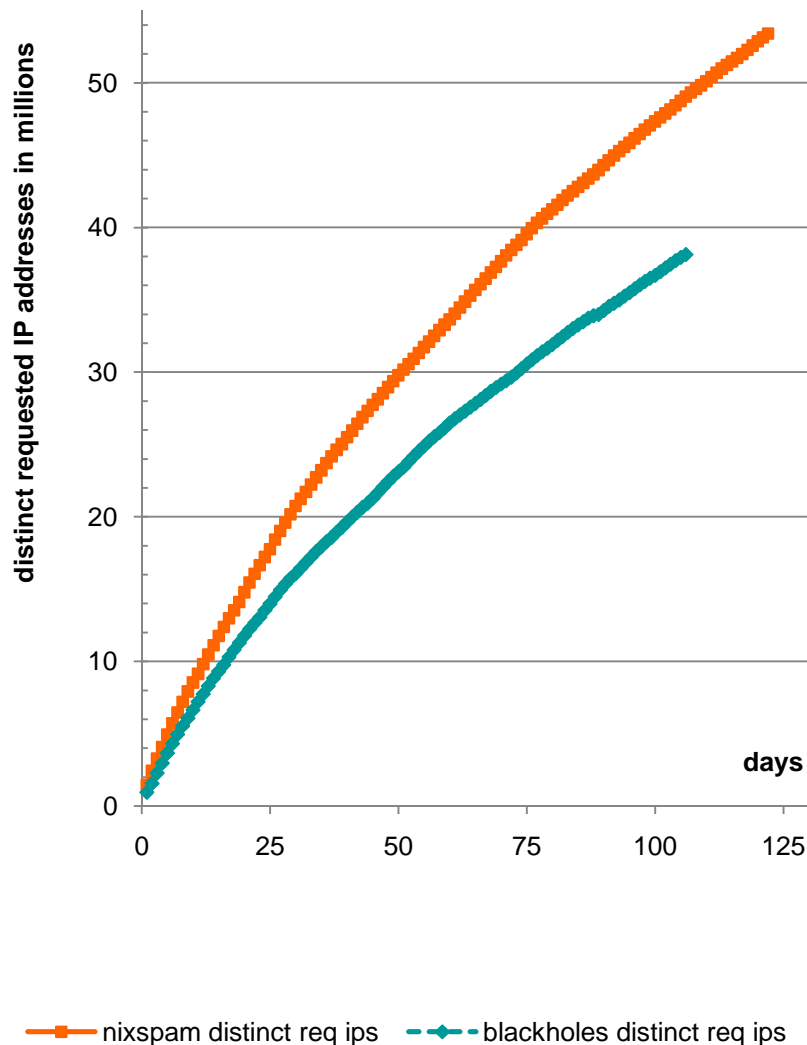
- **1,872 Mrd. IPv4-Adressen advertised (Routing)**
- **~75%** der advertised IPv4-Adressen sind **ohne Reputation!**
- Statistisch: Nur jede 4. advertised IP-Adresse ist „bekannt“



Verteilung der Aktivitätszeiträume von E-Mail-Quellen

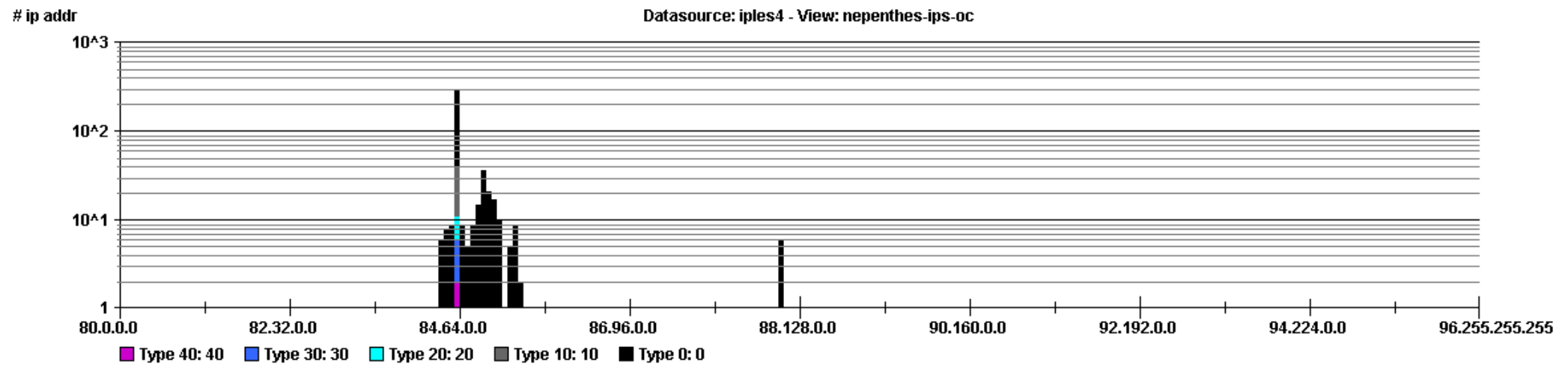
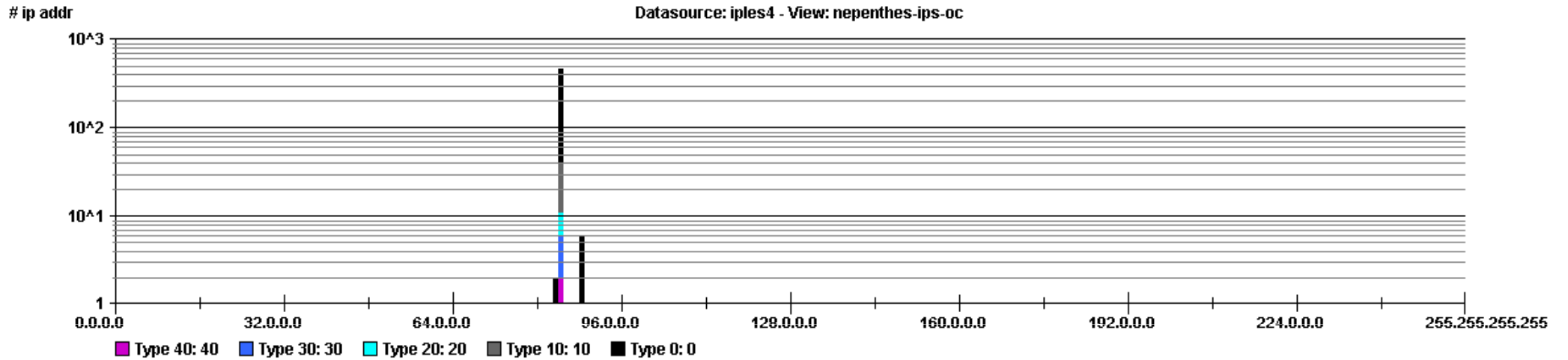


Eindeutigkeit von E-Mail-Quellen

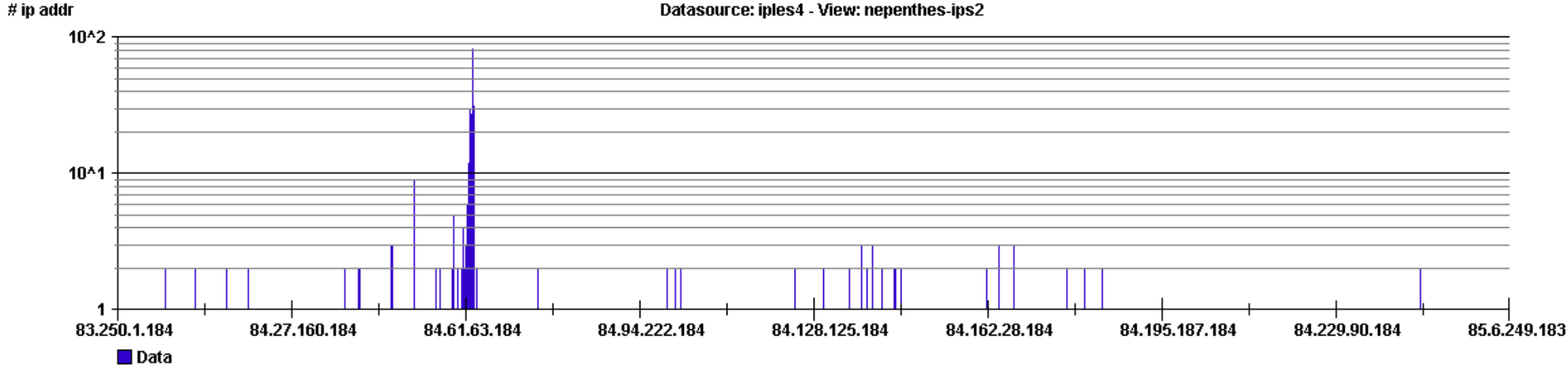
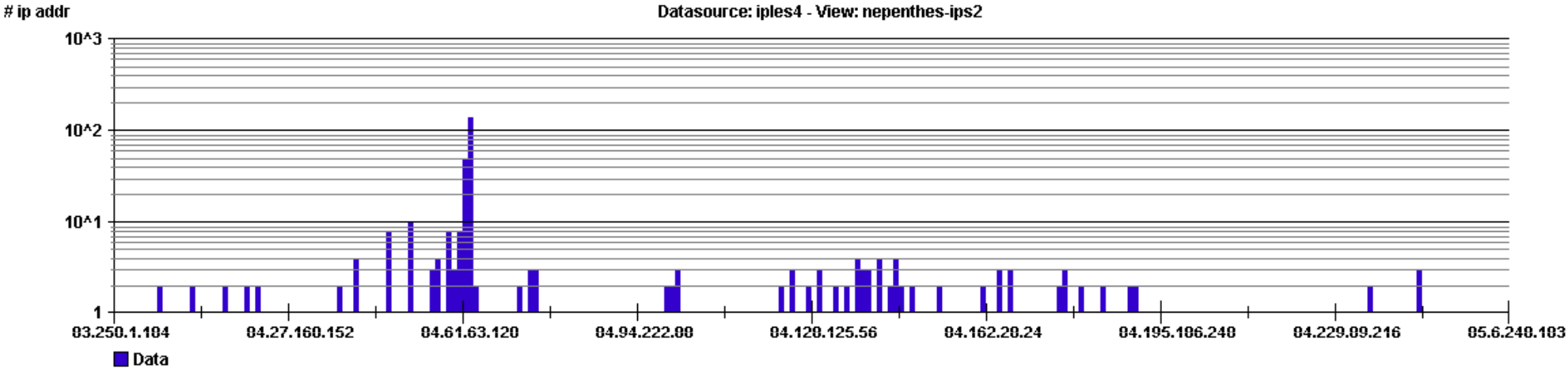


- 125-Tage-Zeitraum zeigt die „Einmaligkeit“ von IP-Adressen
- Mehr als **55 Mio. verschiedene IP-Adressen** von E-Mail-Quellen in 125 Tagen
- **12 Jahre** bis alle 1,8 Mrd. advertised IP-Adressen mind. 1 Mal genutzt wurden
- Orange line = Primärsensor
- Blue line = Sekundärsensor

Infektionsquellen



Infektionsquellen



- Einleitung
- Aktuelle Spam-Entwicklung im Detail
- **Die Tools der Spammer**
„Make money fast – the spammer’s way“
- Botnet Security Mechanisms
- Fazit



Send-Safe Mailer 2.5 (build 940) - C:\Program Files\Send-Safe Mailer

File Help

Master Settings

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign

General

Mailing Options:

Connection timeout (mS):

Send/Receive timeout (mS):

Emails per SMTP session: randomize

Sessions per connection: randomize

Number of threads:

Number of send attempts:

Bulk Features:

Add session emails to:

- Add random to FROM
- Random headers
- MIME-encoded content
- High email priority
- Randomize body HTML
- Morph embedded images

Miscellaneous:

- Log server protocol
- Don't Send, Test mode

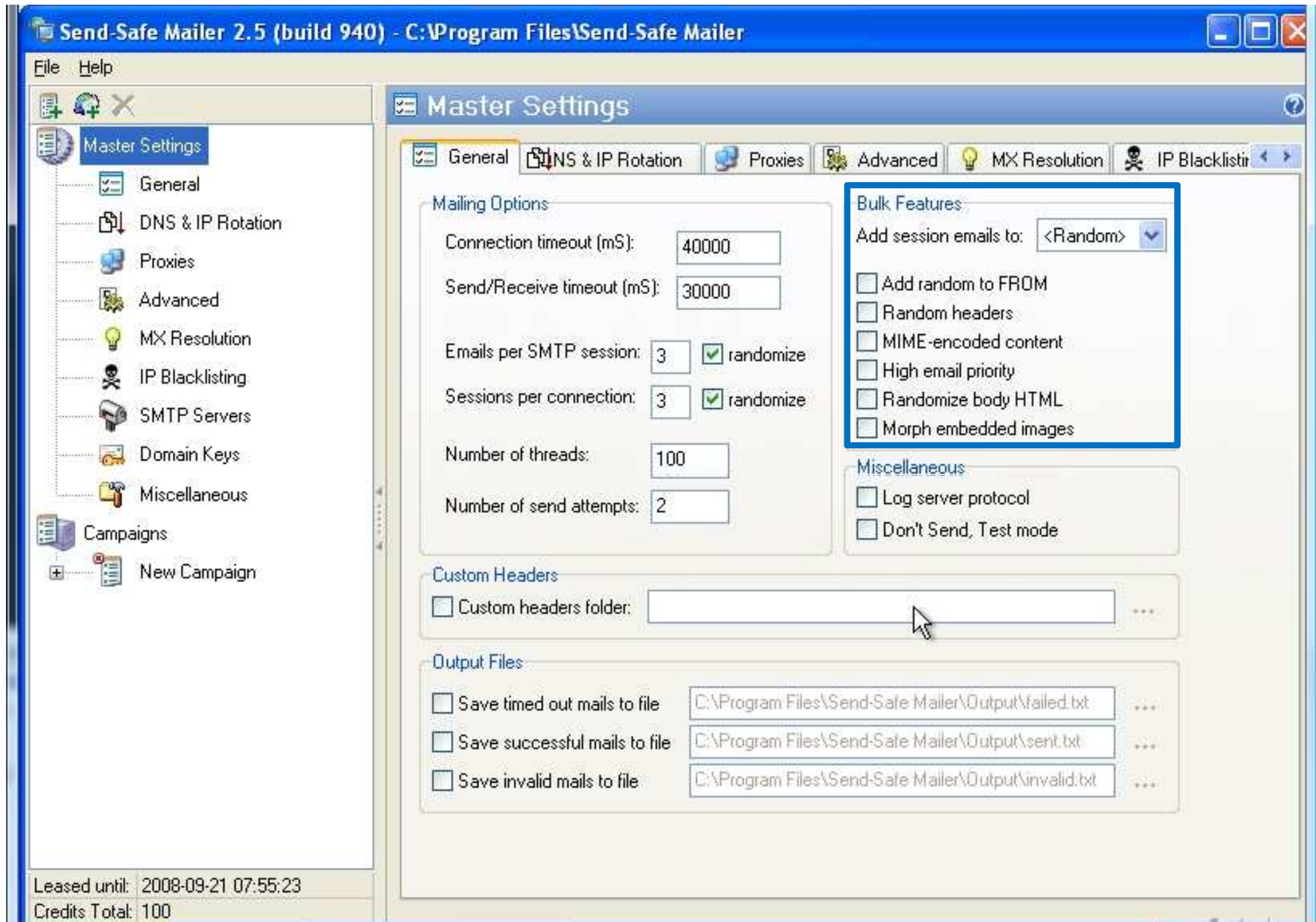
Custom Headers:

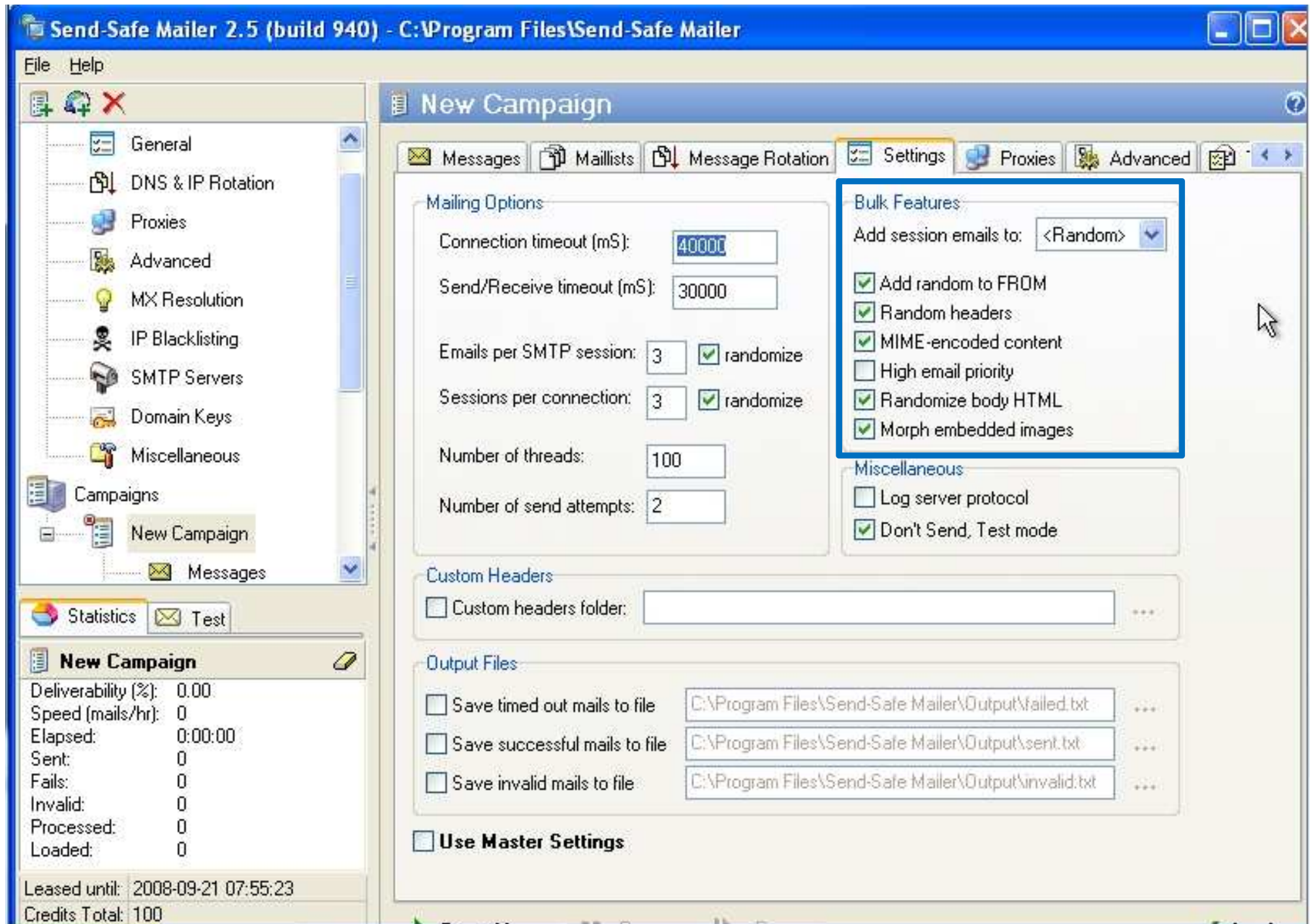
Custom headers folder: ...

Output Files:

- Save timed out mails to file ...
- Save successful mails to file ...
- Save invalid mails to file ...

Leased until: 2008-09-21 07:55:23
Credits Total: 100





Send-Safe Mailer 2.5 (build 940) - C:\Program Files\Send-Safe Mailer

File Help

Lowest Price Guarantee & Fast Delivery

Viagra	only \$2.00
Cialis	only \$2.00
Ambien	only \$2.00
Xanax	only \$2.00

Save up to 80%

Do not click, just type **<http://www.RXGPS.org>**
in the address bar of your browser, then press the enter key

Settings Proxies Advanced

Bulk Features

Add session emails to: <Random>

- Add random to FROM
- Random headers
- MIME-encoded content
- High email priority
- Randomize body HTML
- Morph embedded images

Miscellaneous

- Log server protocol
- Don't Send, Test mode

Messages

Statistics Test

New Campaign

Deliverability (%)	0.00
Speed (mails/hr)	0
Elapsed	0:00:00
Sent	0
Fails	0
Invalid	0
Processed	0
Loaded	0

Leased until: 2008-09-21 07:55:23
Credits Total: 100

Custom Headers

- Custom headers folder: []

Output Files

- Save timed out mails to file: C:\Program Files\Send-Safe Mailer\Output\failed.txt
- Save successful mails to file: C:\Program Files\Send-Safe Mailer\Output\sent.txt
- Save invalid mails to file: C:\Program Files\Send-Safe Mailer\Output\invalid.txt

Use Master Settings

Lowest Price Guarantee & Fast Delivery

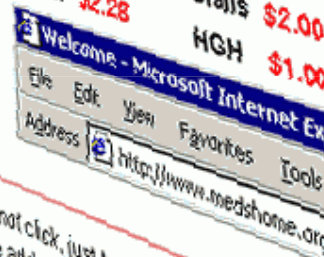
Viagra	only \$2.00
Cialis	only \$2.00
Ambien	only \$2.00
Xanax	only \$2.00

Save up to

Do not click, just type **http://**
in the address bar of your browser,

Discount Pharmacy Online

Viagra	\$2.00	Cialis	\$2.00
Ultram	\$2.28	HGH	\$1.00



Do not click, just type **www.MedsHome.org**
in the address bar of your browser, then press the Enter Key

Bulk Features

Add session emails to: <Random>

Add random to FROM

Random headers

Messages

Statistics Test

New Campaign

Deliverability (%): 0.00
 Speed (mails/hr): 0
 Elapsed: 0:00:00
 Sent: 0
 Fails: 0
 Invalid: 0
 Processed: 0
 Loaded: 0

Leased until: 2008-09-21 07:55:23

Credits Total: 100

Use Master Settings

Save invalid mails to file
 C:\Program Files\Send-Safe Mailer\Output\invalid.txt

Master Settings

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous

Campaigns

- New Campaign

Master Settings

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklistir

Seeds and Notification

Send seed after every 20000 to the following emails:

[Empty list box]

X-Mailers: (for random select)

- Microsoft Outlook Express 5.00.29
- Microsoft Outlook Express 5.00.29
- Microsoft Outlook Express 5.50.45
- Microsoft Outlook Express 5.50.48
- Microsoft Outlook Express 5.50.49
- Microsoft Outlook Express 6.00.24
- Microsoft Outlook Express 6.00.26
- Microsoft Outlook Express 6.00.28
- Microsoft Outlook Express 6.00.28

E-mail Filtering

Don't send

if email contains one of the following:

[Empty list box]

Don't send to those emails:

[Empty text box]

Change charset to: us-ascii

Use EHLO instead of HELO.

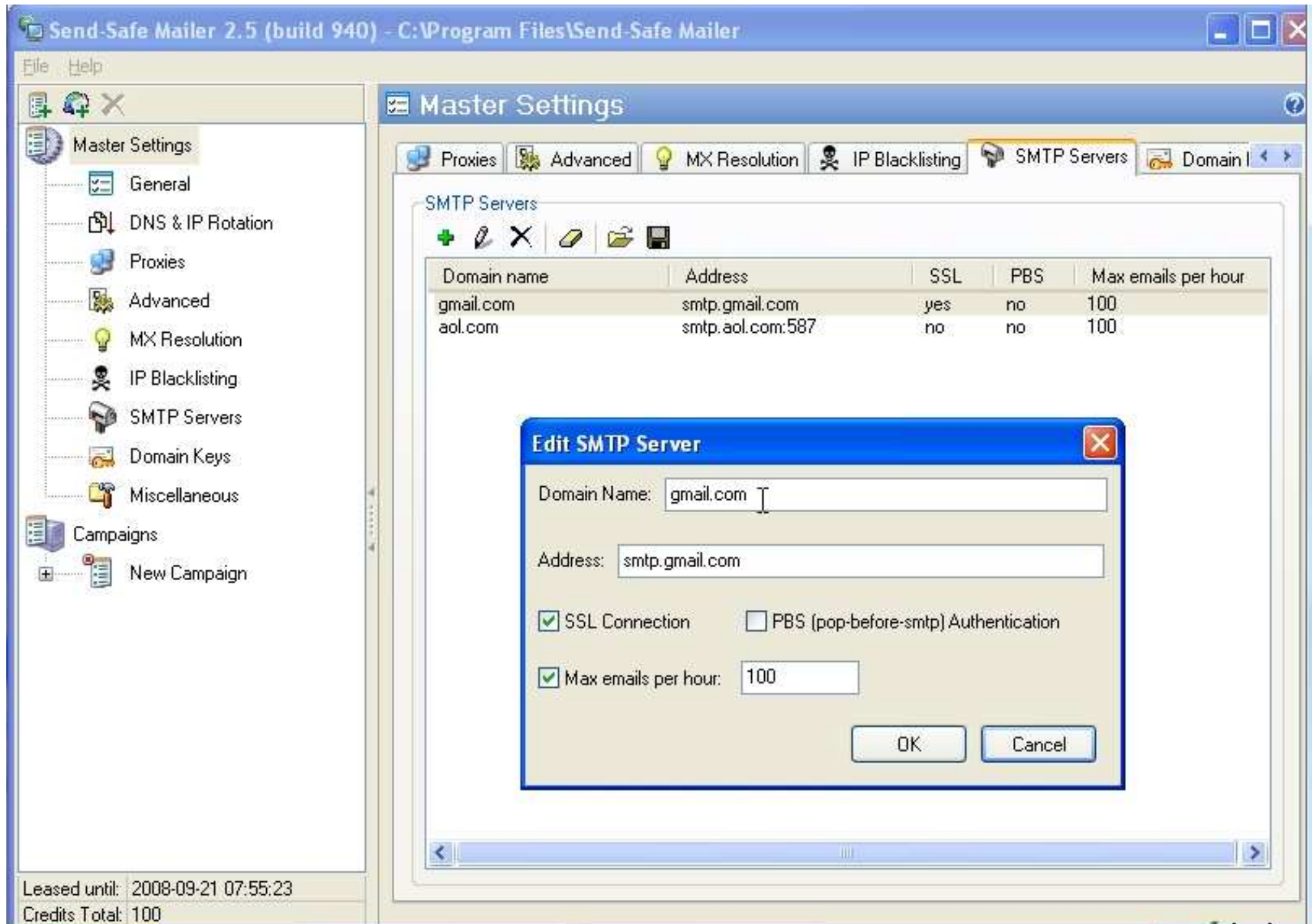
MIME-encoded subjects, charsets (comma separated): US-ASCII, windows-1252, ISO-8859-1

MIME-encoded froms, charsets (comma separated): US-ASCII, windows-1252, ISO-8859-1

Log MessageIDs with destination emails

Leased until: 2008-09-21 07:55:23

Credits Total: 100



- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
 - Messages

Statistics Test

New Campaign

Deliverability (%):	0.00
Speed (mails/hr):	0
Elapsed:	0:00:00
Sent:	0
Fails:	0
Invalid:	0
Processed:	0
Loaded:	0

Leased until: 2008-09-21 07:55:23
Credits Total: 100

New Campaign

Messages Maillists Message Rotation Settings Proxies Advanced

Rename New Message ID: ir2uneqs

Message Body Subjects FROMs and Attachments Message Source

Message text: HTML Content

{% %#

```
{%ROT:HelloHi!Hi,%}

You don't have to reply, this is a test.
I have a new site: somewhereonweb.com

You are welcome!
```

Preview

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
 - Messages

Statistics Test

New Campaign	
Deliverability (%):	0.00
Speed (mails/hr):	0
Elapsed:	0:00:00
Sent:	0
Fails:	0
Invalid:	0
Processed:	0
Loaded:	0
Leased until: 2008-09-21 07:55:23	
Credits Total: 100	

New Campaign

Messages Maillists Message Rotation Settings Proxies Advanced

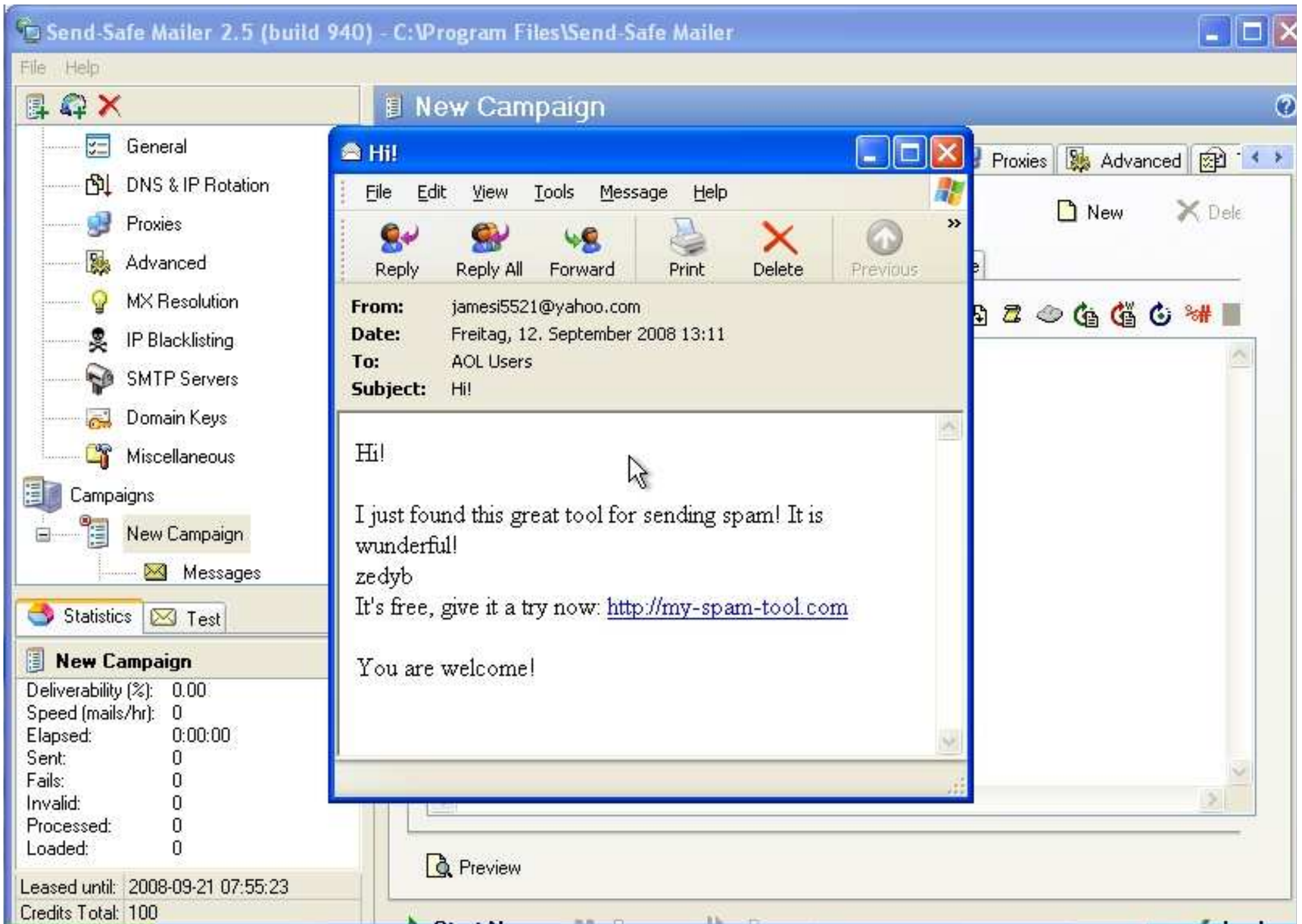
Rename New Message ID: ir2uneqs New Delete

Message Body Subjects FROMs and Attachments Message Source

Message text: HTML Content

{%ROT:HelloHiHiHi,%}
I just found this great tool for sending spam! It is wunderfull!
{%RND:<110>%}
It's free, give it a try now: <http://my-spam-tool.com>
You are welcome!

Preview



New Campaign

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
- Messages

Statistics Test

New Campaign

Deliverability (%): 0.00
 Speed (mails/hr): 0
 Elapsed: 0:00:00
 Sent: 0
 Fails: 0
 Invalid: 0
 Processed: 0
 Loaded: 0

Leased until: 2008-09-21 07:55:23
 Credits Total: 100

Hi!

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

From: info@tri-finance.com
Date: Freitag, 12. September 2008 13:11
To: AOL Users
Subject: Hi!

Hello

I just found this great tool for sending spam! It is wonderful!

olon

It's free, give it a try now: <http://my-spam-tool.com>

You are welcome!

New Delete

Refresh Stop Back Forward Home %#

Preview

New Campaign

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
- Messages

Statistics Test

New Campaign

Deliverability (%): 0.00
Speed (mails/hr): 0
Elapsed: 0:00:00
Sent: 0
Fails: 0
Invalid: 0
Processed: 0
Loaded: 0

Leased until: 2008-09-21 07:55:23
Credits Total: 100

Hi!

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

From: vakoop3@yahoo.com
Date: Freitag, 12. September 2008 13:15
To: AOL Users
Subject: Hi!

Hi,

I just found this great tool for sending spam! It is wonderful!
ucyemezq
It's free, give it a try now: <http://my-spam-tool.com>

You are welcome!

Preview

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
 - Messages

Statistics Test

New Campaign

Deliverability (%): 0.00
 Speed (mails/hr): 0
 Elapsed: 0:00:00
 Sent: 0
 Fails: 0
 Invalid: 0
 Processed: 0
 Loaded: 0

Leased until: 2008-09-21 07:55:23
 Credits Total: 100

New Campaign

Messages Maillists Message Rotation Settings Proxies Advanced

Rename New Message ID: ir2uneqs New Dele

Message Body Subjects **FROMs and Attachments** Message Source

FROM Emails FROM Aliases: TO Aliases:

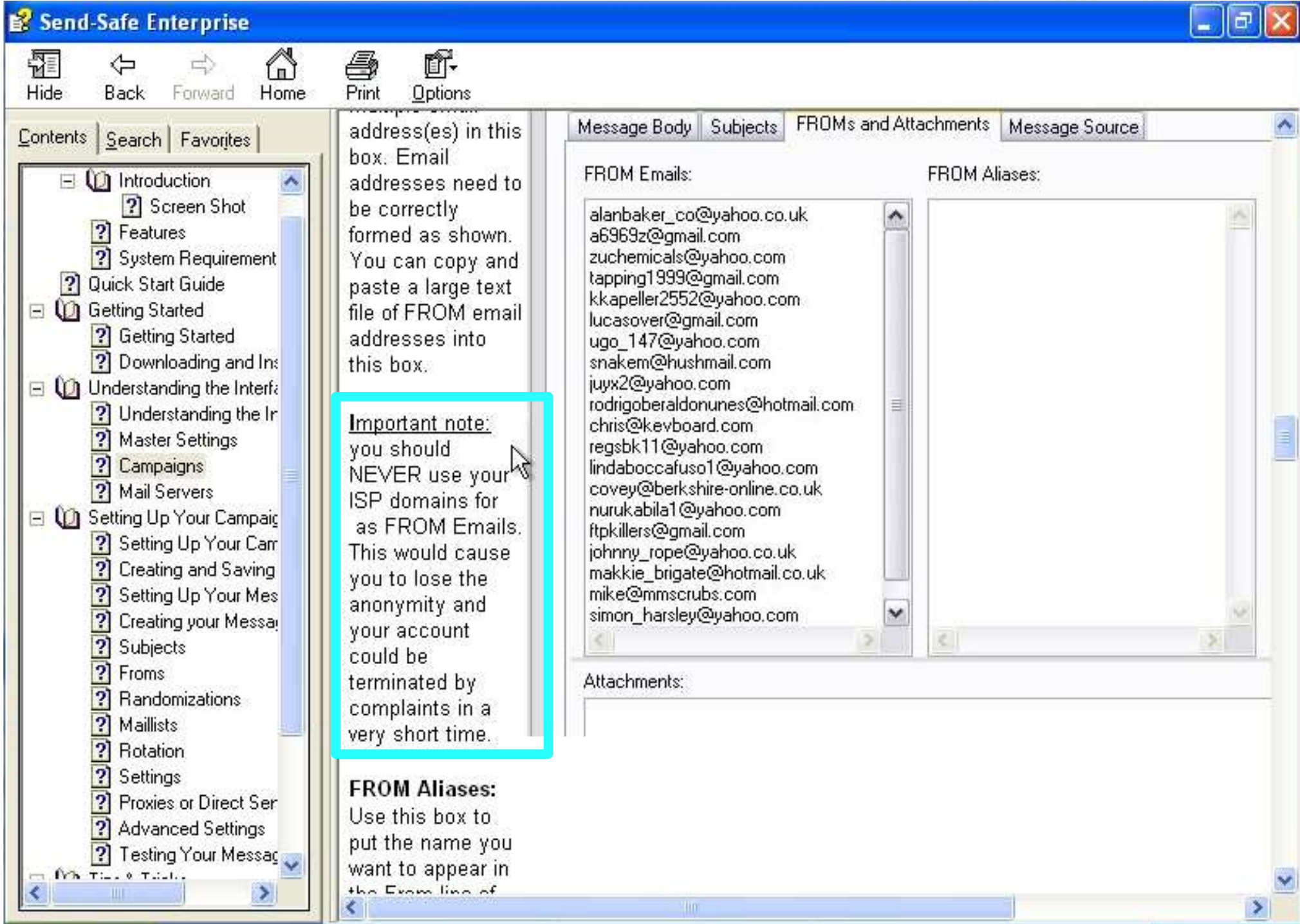
email@domain.com

connect@atechonline.net
 jamesi5521@yahoo.com
 jchavali@gmail.com
 martynsenior@mail.com
 davidsnow11@yahoo.com
 richmortal@yahoo.com
 vakoop3@yahoo.com
 basilIndenkala@yahoo.com
 globalbox02@yahoo.com
 izeoku99@hotmail.com
 info@tri-finance.com
 bdw229@aol.com

AOL Users
 Webmaster
 Postmaster
 Administrator

Attachments:

Preview



address(es) in this box. Email addresses need to be correctly formed as shown. You can copy and paste a large text file of FROM email addresses into this box.

Important note: you should NEVER use your ISP domains for as FROM Emails. This would cause you to lose the anonymity and your account could be terminated by complaints in a very short time.

Message Body Subjects FROMs and Attachments Message Source

FROM Emails:

- alanbaker_co@yahoo.co.uk
- a6969z@gmail.com
- zuchemicals@yahoo.com
- tapping1999@gmail.com
- kkapeller2552@yahoo.com
- lucasover@gmail.com
- ugo_147@yahoo.com
- snakem@hushmail.com
- juyx2@yahoo.com
- rodrigoberaldonunes@hotmail.com
- chris@keyboard.com
- regsbk11@yahoo.com
- lindaboccafuso1@yahoo.com
- covey@berkshire-online.co.uk
- nurukabila1@yahoo.com
- ftpkillers@gmail.com
- johnny_rope@yahoo.co.uk
- makkie_brigate@hotmail.co.uk
- mike@mmscrubs.com
- simon_harsley@yahoo.com

FROM Aliases:

-

Attachments:

New Campaign

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
- Messages


Statistics Test

New Campaign	
Deliverability (%):	0.00
Speed (mails/hr):	0
Elapsed:	0:00:00
Sent:	0
Fails:	0
Invalid:	0
Processed:	0
Loaded:	0


Leased until: 2008-09-21 07:55:23
 Credits Total: 100

Open

Look in: My Pictures



girl



Sample Pictures

File name: girl

Files of type: Image Files (*.bmp;*.gif;*.jpg;*.jpeg)

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
 - Messages

Statistics Test

New Campaign

Deliverability (%):	0.00
Speed (mails/hr):	0
Elapsed:	0:00:00
Sent:	0
Fails:	0
Invalid:	0
Processed:	0
Loaded:	0

Leased until: 2008-09-21 07:55:23
Credits Total: 100

New Campaign

Messages Maillists Message Rotation Settings Proxies Advanced

Rename New Message ID: ir2uneqs New Delete

Message Body Subjects FROMs and Attachments **Message Source**

Custom Message Source (advanced users only)

```
{%RANDOMHEADERS%}
Message-ID: {%MSGID%}
{%NOT_OUTLOOK%}Date: {%DATE%}
{%RANDOMLY%}Reply-To: {%FROM%}
From: {%FROM%}
{%NOT_OUTLOOK%}{%USERAGENT_HEADER%}
{%NOT_OUTLOOK%}{%RANDOMLY%}X-Accept-Language: en-us
{%NOT_OUTLOOK%}MIME-Version: 1.0
{%TOCC_HEADERS%}
Subject: {%SUBJECT%}
{%OUTLOOK%}Date: {%DATE%}
{%OUTLOOK%}MIME-Version: 1.0
Content-Type: multipart/related;
{%OUTLOOK%} type="multipart/alternative";
           boundary="{%BOUNDARY1%}"
{%OUTLOOK%}{%RANDOMLY%}X-Priority: 3
{%OUTLOOK%}X-MSMail-Priority: Normal
{%OUTLOOK%}{%MAILER_HEADER%}
{%OUTLOOK%}X-MimeOLE: Produced By Microsoft MimeOLE V{%OUTLOOK_VERSION%}

{%OUTLOOK%}This is a multi-part message in MIME format.
```

Preview

- General
- DNS & IP Rotation
- Proxies
- Advanced
- MX Resolution
- IP Blacklisting
- SMTP Servers
- Domain Keys
- Miscellaneous
- Campaigns
 - New Campaign
 - Messages

Statistics Test

New Campaign

Deliverability (%): 0.00
 Speed (mails/hr): 0
 Elapsed: 0:00:00
 Sent: 0
 Fails: 0
 Invalid: 0
 Processed: 0
 Loaded: 0

Leased until: 2008-09-21 07:55:23
 Credits Total: 100

New Campaign

- Maillists
- Message Rotation
- Settings
- Proxies
- Advanced
- Test
- Mailing

Send test messages

Email to: ✉ Send email

Send test messages directly (without proxies)

Number of emails to

Test the message against SpamAssassin

```
X-Spam-Checker-Version: SpamAssassin 3.0.0 (2004-09-13) on j
X-Spam-Status: No, score=-2.1 required=5.0 tests=ALL_TRUSTED
FROM_ENDS_IN_NUMS,NO_REAL_NAME autolearn=ham version:
| |
```

✔ Test

Content analysis details: (-2.1 points, 5.0 required)

pts	rule name	description
0.1	NO_REAL_NAME	From: does not include a real n:
0.2	FROM_ENDS_IN_NUMS	From: ends in numbers
-2.4	ALL_TRUSTED	Did not pass through any untrust

- Einleitung
- Aktuelle Spam-Entwicklung im Detail
- Die Tools der Spammer
„Make money fast – the spammer’s way“
- **Fazit**

- Spam als (grober) Indikator für Botnetz-Aktivität
- „Professionalisierung“
 - Aufgaben (Captcha-Brechen)
 - Tools (Spamtools)
- Missbrauch legitimer Infrastruktur zum Spam-Versand
- Viel „Kreativität“
- Hybride Kommunikation der Bots (zentral und P2P)

E-Mail Sicherheit – aktuelle Entwicklungen und Trends

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Christian J. Dietrich
dietrich [at] internet-sicherheit . de

Institut für Internet-Sicherheit
<https://www.internet-sicherheit.de>
FH Gelsenkirchen

