Multi-Instance Support in Postfix / postscreen

Ralf Hildebrandt

Charité Universitätsmedizin Berlin

OpenSource Trends Days 2010 – Steinfurt, 23. September

Multi-instance Support gibt es seit Postfix 2.6
nutzt aber keiner. . .

- monolithisch– man kann alles in einer Instanz machen - wird aber schnell unübersichtlich
  - `master.cf` Änderungen
  - `receive_override_options`
  - `smtpd_restriction_classes`
  - Viele `smtpd` Prozesse mit verschiedenen Optionen
  - Viele `cleanup` Prozesse mit verschiedenen Optionen
  - ...
- multi-instance– jede Instanz hat eine eigene `master.cf`, `main.cf` und Queue
- Binaries werden gemeinsam genutzt

- eine Instanz pro Kunden-IP
  Wo die Mail reinkommt, soll sie auch wieder rauskommen. . .
- Realisierung eines `smtp_fallback_relay`
  Es nimmt Mails auf, die nicht sofort zustellbar sind
- Sender-basiertes Routing
  . . . dem Hörensagen nach!

- auf einem Clusterknoten, beim Mounten des `queue_directory` des ausgefallenen Knotens
- ...

- nullclient
  für lokale generierte Mail: `cron`, `logcheck` etc.
- postfix-out
  nimmt die Mail vom `content_filter` an und schickt sie weiter
- postfix-in
  nimmt die Mail aus dem Netz an und füttert den `content_filter`

Die “normale” `/etc/postfix/main.cf` wird unsere nullclient Instanz - gleichzeitig das Muster für alle weiteren Instanzen:

```
master_service_disable = inet
mydestination =
local_transport = error:5.1.1 Mailbox unavailable

# Send everything to the internal mailhub
relayhost = [mailhub.example.com]
```

Multi-instance Support aktivieren:

```
# postmulti -e init
```

Erste zusätzliche Instanz `postfix-out` hinzufügen:

```
# postmulti -I postfix-out -G mta -e create
```

- `-I postfix-out` der Name der Instanz
- `-G mta` die Gruppe, der die Instanz angehört
- `-e create` Instanz erzeugen

/etc/postfix-out/main.cf

```
multi_instance_name = postfix-out
queue_directory = /var/spool/postfix-out
data_directory = /var/lib/postfix-out
```

Jetzt muß nur noch konfiguriert werden!

/etc/postfix-out/master.cf

```
# Replace default port 25 entry with one listening on port 10026.
127.0.0.1:10026    inet  n       -       n       -       -  smtpd
```

`main.cf` weiter ergänzen!

/etc/postfix-out/main.cf

```
inet_interfaces = loopback-only
smtpd_authorized_xforward_hosts = $mynetworks
local_header_rewrite_clients =
smtpd_recipient_restrictions = permit_mynetworks, reject
relay_domains = example.com, .example.com
```

/etc/postfix-out/main.cf

- `anvil` deaktivieren
- `local_header_rewrite_clients` leeren
- Zustellung durch `local` abstellen

Aktivierung

```
postmulti -i postfix-out -e enable
postmulti -i postfix-out -p start
```

Zweite zusätzliche Instanz `postfix-in` hinzufügen:

```
# postmulti -I postfix-in -G mta -e create
```

- `-I postfix-in` der Name der Instanz
- `-G mta` die Gruppe, der die Instanz angehört
- `-e create` Instanz erzeugen

/etc/postfix-in/main.cf

```
multi_instance_name = postfix-in
queue_directory = /var/spool/postfix-in
data_directory = /var/lib/postfix-in
```

Jetzt muß nur noch konfiguriert werden!

/etc/postfix-in/main.cf

```
default_transport = smtp:[127.0.0.1]:10025
relay_transport = $default_transport
virtual_transport = $default_transport
transport_maps =
```

Alles geht an den `content_filter` auf 127.0.0.1:10025

/etc/postfix-in/main.cf

```
smtp_send_xforward_command = yes
smtp_destination_recipient_limit = 1000
# Tolerate occasional high latency in the content filter.
smtp_data_done_timeout = 1200s
```

.. und was man sonst so braucht (Antispam usw.)

Aktivierung

```
postmulti -i postfix-in -e enable
postmulti -i postfix-in -p start
```

Steuerung

- `postfix start` bzw. `postfix stop`
  starten/stoppen alle Instanzen
- `postmulti -i postfix-out -p flush`
  `postfix flush` der “postfix-out” Instanz
- `postmulti -i postfix-in -p reload`
  `postfix reload` der “postfix-in” Instanz
- `postmulti -i - -p stop`
  `postfix stop` der primären Instanz (die mit Konfiguration in `/etc/postfix`)
- `postmulti -g mta -p status`
  `postfix status` für alle Mitglieder der Gruppe “mta”


AND NOW FOR SOMETHING
COMPLETELY
DIFFERENT.

- “Botnets now produce 95% of spam” `http://sanjose.bizjournals.com/sanjose/stories/2010/08/23/daily29.html`
- . . . figure bumped up from 84 % in April.
- In August, the most spammed industry sector with a spam rate of 94.8 % was the Automotive sector.
- Spam levels for the Education sector were 92.9 %,
- 92.8 % for Retail,
- 92.7 % for IT Services,
- 92.6 % for the Chemical & Pharmaceutical sector,
- 91.7 % for Public Sector and
- 91.2 % for Finance.

Effiziente Behandlung von Clients aus Botnetzen wäre sinnvoll!

Spezifische Gegenmaßnahmen

- DNSBLs
  - Gibt es, ist aber ineffizient!
- Greet delays
  - Gibt es, aber auch ineffizient!
- Greylisting
  - Gibt es :-)
- Erkennung von “Earlytalkern”
  - Gibt es noch gar nicht!
- Erkennung von anderem “abnormen” Verhalten
  - Gibt es noch gar nicht!

Aktuelle Entwicklung in Postfix

Postscreen ist der Codename für einen neuen Daemon der vor Postfixs `smtpd` sitzt und Verbindungen ausfiltert.

Aktuelle Entwicklung in Postfix

service “smtpd” has reached its process limit “100”: new smtpd clients may experience noticeable delays to avoid this condition, increase the process count in master.cf or reduce the service time per client

Aktuelle Entwicklung in Postfix II

Ziele:

- Zombies von Postfixs `smtpd` fernhalten
- Erhöhung der Skalierbarkeit. . .
  indem zeitintensive Operationen wie DNSBL Abfragen und SMTP Protokollcheck aus dem `smtpd` ausgelagert werden

Angriff der Zombiehorden

Angriff der Zombiehorden II

- Der Kernel queued Verbindungen
- Postfix arbeitet “nur” 100 Verbindungen (genauer `default_process_limit`) simultan ab

-> Serverüberlastung

Symptome einer Serverüberlastung

- Clients erfahren eine extreme Verzögerung bevor Postfix antwortet
  - Clients geben auf bevor Postfix antwortet
- Postfix loggt viele “`lost connection`” Einträge
- Postfix ab Version 2.3 loggen “`all server ports busy`”-Warnungen

postscreen - master.cf

Aus

```
smtp      inet  n       -       -       -       -       smtpd
```

wird

```
smtp      inet  n       -       -       -       1       postscreen
smtpd     pass  -       -       -       -       -       smtpd
```

Man beachte das Process Limit von 1 – `postscreen` ist wirklich nur ein einzelner Daemon.

postscreen - `main.cf`

```
postscreen_dnsbl_sites = zen.spamhaus.org
postscreen_dnsbl_action = enforce

postscreen_greet_action = enforce
postscreen_hangup_action = drop

postscreen_whitelist_networks = 141.42.0.0/16

postscreen_blacklist_networks = 64.20.227.135/32
postscreen_blacklist_action = drop
```

```
Aug 29 14:29:32 mail postfix/postscreen[23289]: \
PASS OLD 66.221.63.75
```

Hier wurde ein “guter” Client im Cache gefunden

postscreen - das Log

```
Sep 12 12:51:14 mail postfix/dnsblog[26460]: addr 113.160.111.50
blocked by domain zen.spamhaus.org as 127.0.0.11
Sep 12 12:51:14 mail postfix/dnsblog[26460]: addr 113.160.111.50
blocked by domain zen.spamhaus.org as 127.0.0.4
Sep 12 12:51:15 mail postfix/postscreen[25489]: PREGREET 20 after
0.41 from 113.160.111.50: HELO static.vdc.vn??
Sep 12 12:51:21 mail postfix/postscreen[25489]: DNSBL rank 1 for
113.160.111.50
Sep 12 12:51:22 mail postfix/postscreen[25489]: NOQUEUE: reject:
RCPT from [113.160.111.50]: 550 5.7.1 Service unavailable; client
[113.160.111.50] blocked using zen.spamhaus.org;
from=<Jacquelyn@static.vdc.vn>, to=<recipient@charite.de>,
proto=SMTP, helo=<static.vdc.vn>
Sep 12 12:51:23 mail postfix/postscreen[25489]: NON-SMTP COMMAND
from 113.160.111.50 Received:
```

Hier wurde ein “schlechter” Client in genau einer der `postscreen_dnsbl_sites` gefunden.
Die in `postscreen` eingebaute SMTP-Engine konnte envelope sender, recipient und HELO bestimmen

bare newline detection

- bare newline detection

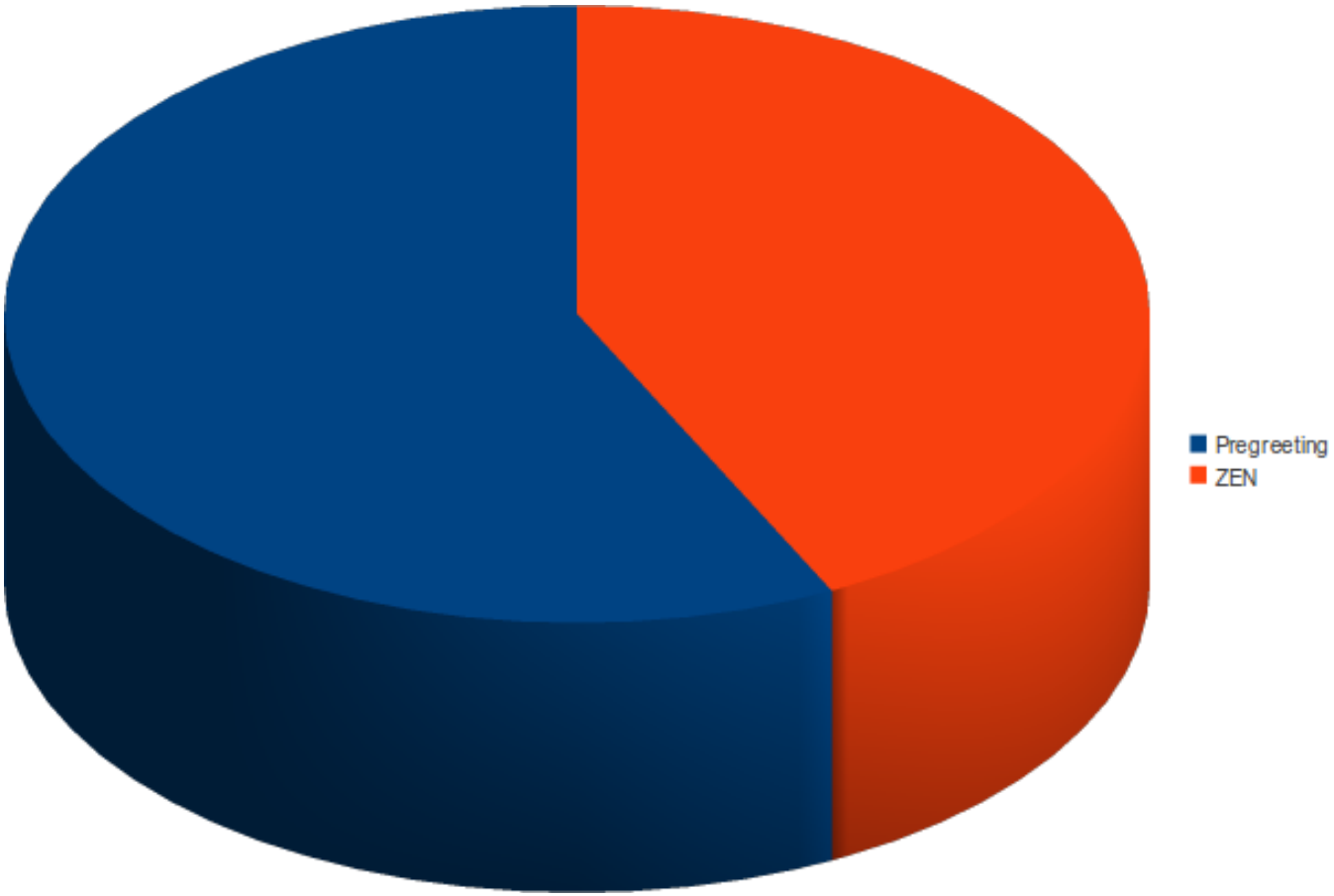
  Real spambots don't make this mistake anymore, but poorly-written software still does.

```
Sep 18 22:07:14 mail postfix/postscreen[1821]: BARE NEWLINE from 88.75.36.251
```

Weitere Entwicklungen

- Greylisting
  nach Implementierung der SMTP-Engine nur eine kleine Erweiterung des Cache

Analysen vom 1.9.2010 bis 7.9.2010:

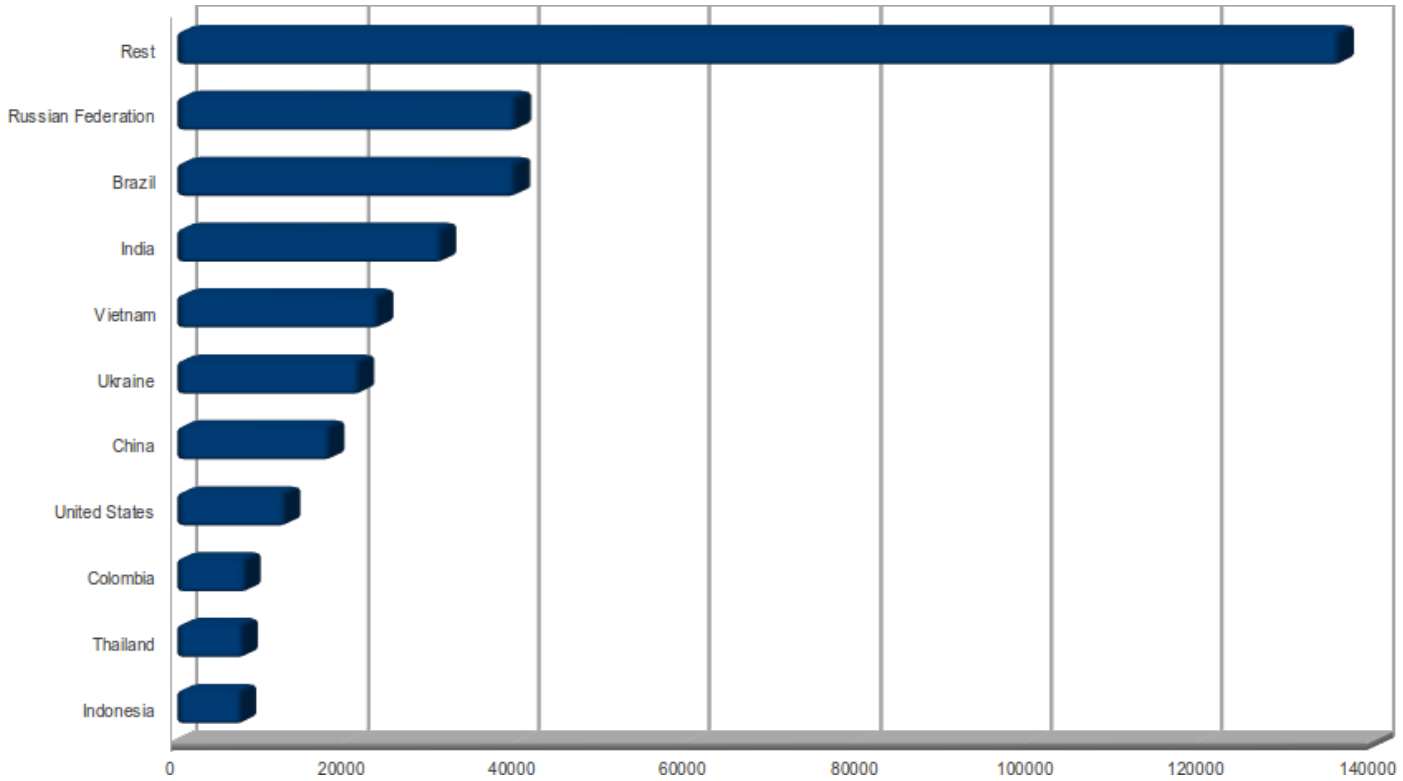


Analysen vom 1.9.2010 bis 7.9.2010 II:

- 605.391 Abweisungen durch postscreen (100%)
- 347.100 durch Pregreeting detection (ca. 57,3%)
- 258.291 durch DNSBL (`zen.spamhaus.org`) (ca. 42,7%)

Das zeigt m.E. das Potential der SMTP-Engine in postscreen – denn diese Werte stammen aus der Zeit wo nur Pregreeting erkannt werden konnte!

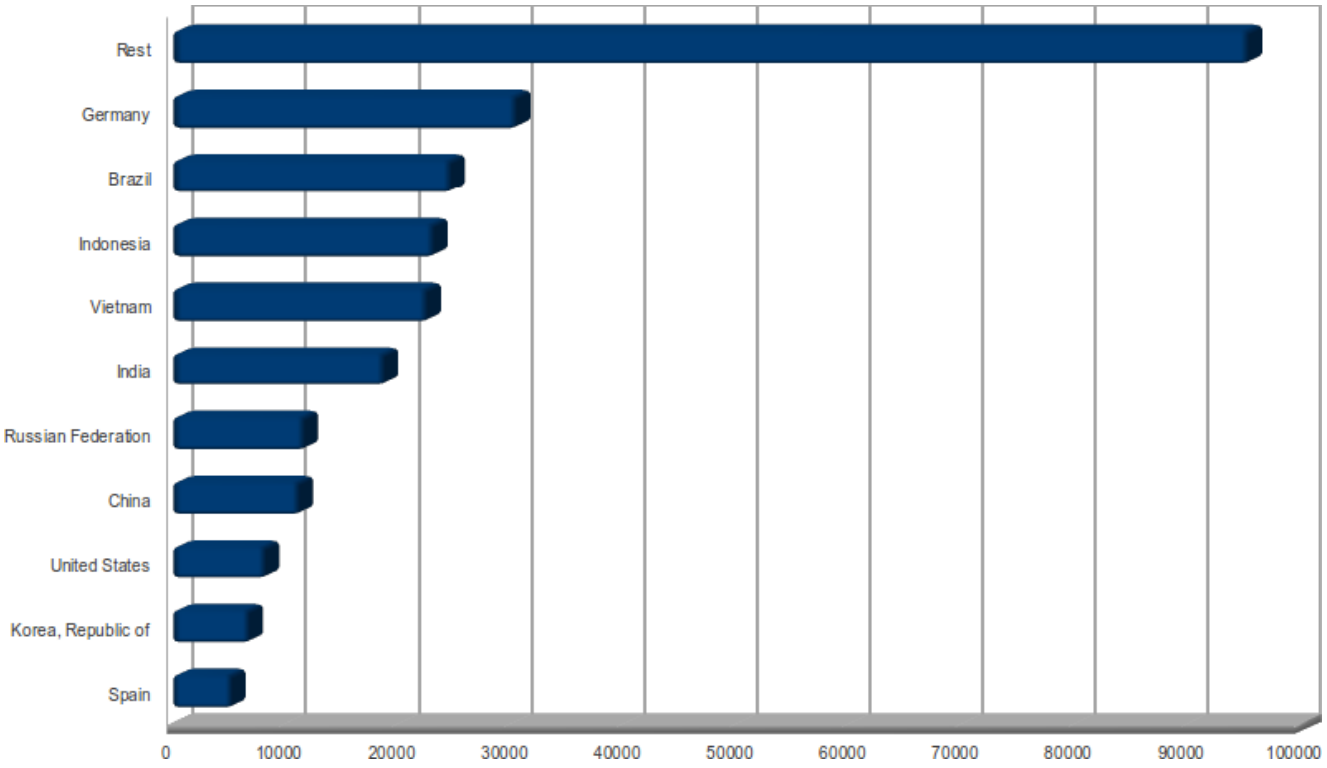
Pregreeter nach Ländern:



Pregreeter nach Ländern II:

- 39879 RU, Russian Federation (11,4%)
- 39799 BR, Brazil (11,4%)
- 31134 IN, India (8,9%)
- 23746 VN, Vietnam (6,8%)
- 21530 UA, Ukraine (6,2%)
- 18035 CN, China (5,1%)
- 12868 US, United States (3,7%)
- 8234 CO, Colombia
- 7898 TH, Thailand
- 7722 ID, Indonesia

DNSBL nach Ländern:



DNSBL nach Ländern II:

- 30505 DE, Germany (11,8%)
- 24689 BR, Brazil (9,5%)
- 23164 ID, Indonesia (8,9%)
- 22566 VN, Vietnam (8,7%)
- 18788 IN, India (7,2%)
- 11686 RU, Russian Federation (4,5%)
- 11233 CN, China (4,3%)
- 8229 US, United States (3,1%)
- 6794 KR, Korea, Republic of
- 5239 ES, Spain

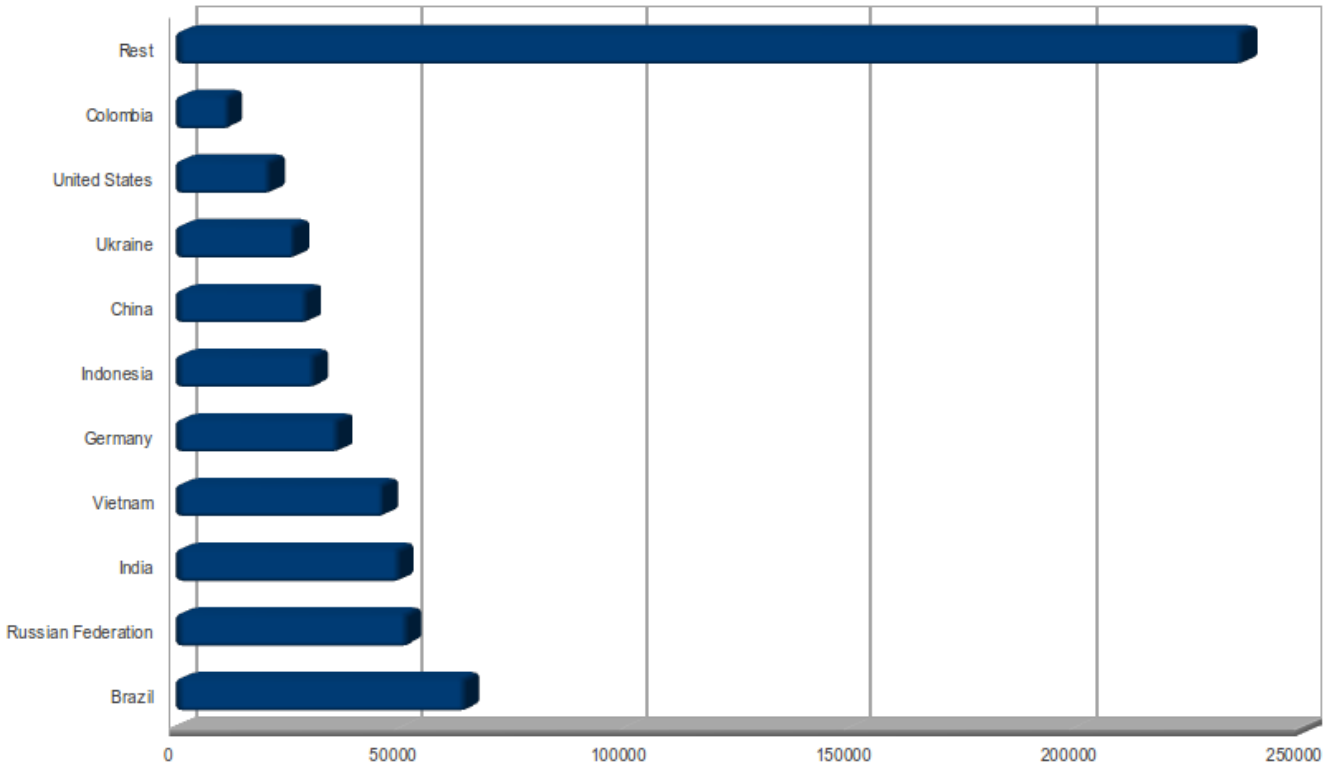
Pregreeter nach Städten:

- 4735 TW, Taipei
- 5258 PE, Lima
- 5786 VN, N/A
- 5945 TH, Bangkok
- 6487 RU, Moscow
- 6645 BR, N/A
- 6842 BR, Sao Paulo
- 6921 CN, Changchun (1,9%)
- 10297 VN, Hanoi (2,9%)
- 11106 UA, Kiev (3,1%)

DNSBL nach Städten:

- 2865 UA, Kiev
- 3047 VN, Ho Chi Minh City
- 3556 RU, Moscow
- 3573 BR, N/A
- 4765 KR, Seoul (1.8%)
- 5786 DE, N/A
- 5862 VN, N/A
- 6424 ID, Jakarta (2.4%)
- 9444 VN, Hanoi (3.6%)
- 18116 DE, Nürnberg (7.0%)

Gesamt nach Ländern:



Gesamt nach Ländern II:

- 11736 CO, Colombia
- 21097 US, United States
- 26590 UA, Ukraine
- 29268 CN, China
- 30886 ID, Indonesia (5,1%)
- 36237 DE, Germany (5,9%)
- 46312 VN, Vietnam (7,6%)
- 49922 IN, India (8,2%)
- 51565 RU, Russian Federation (8,5%)
- 64488 BR, Brazil (10,6%)

Gesamt nach Städten:

- 8102 TH, Bangkok
- 8136 CN, Changchun
- 8953 ID, Jakarta
- 9297 BR, Sao Paulo
- 10043 RU, Moscow
- 10218 BR, N/A
- 11648 VN, N/A
- 13971 UA, Kiev
- 18118 DE, Nürnberg
- 19741 VN, Hanoi

Fragen?