E-MAIL-SICHERHEIT MADE IN GERMANY

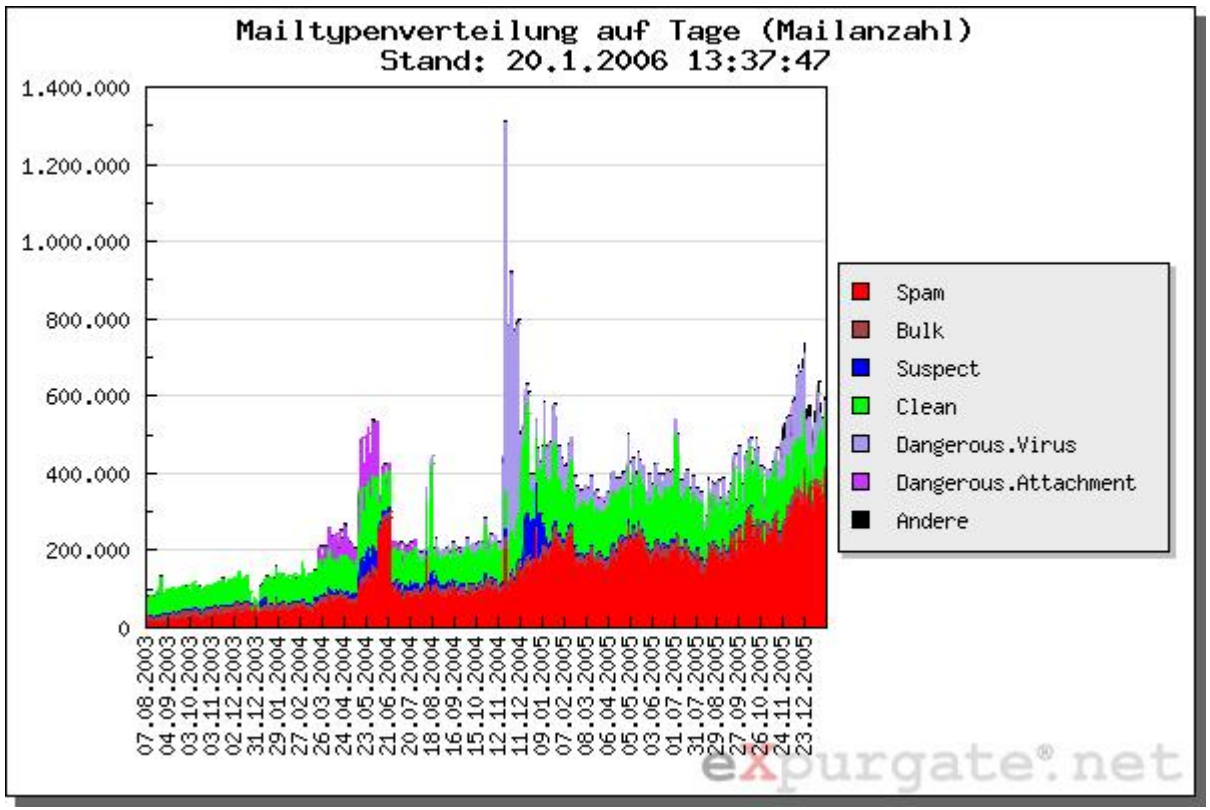
Raymond Gannon ISP Account Manager

The company

- eleven GmbH, established in 2001 in Berlin, Germany
- E-Mail security services & solutions
- Primary products
  - eXpurgate
    - Spamfilter & email categorization service
  - enSurance
    - Email Firewall for ISP and large enterprise
- Serving more than 20 000 business worldwide
- 350 Million Mails per day!

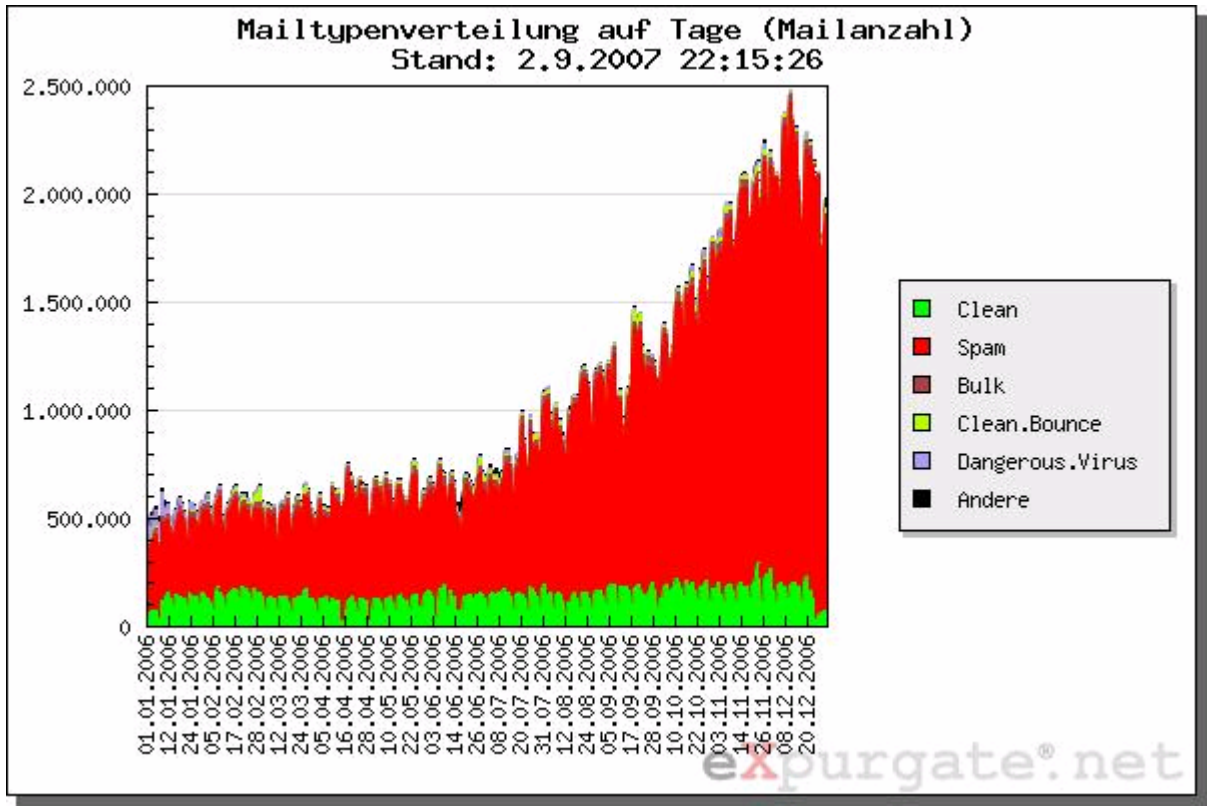
Some references

E-mail traffic development 08/03 - 12/05
(typical German blue chip / 100 000 accounts)



E-mail traffic development 2006

(typical German blue chip / 100 000 accounts)

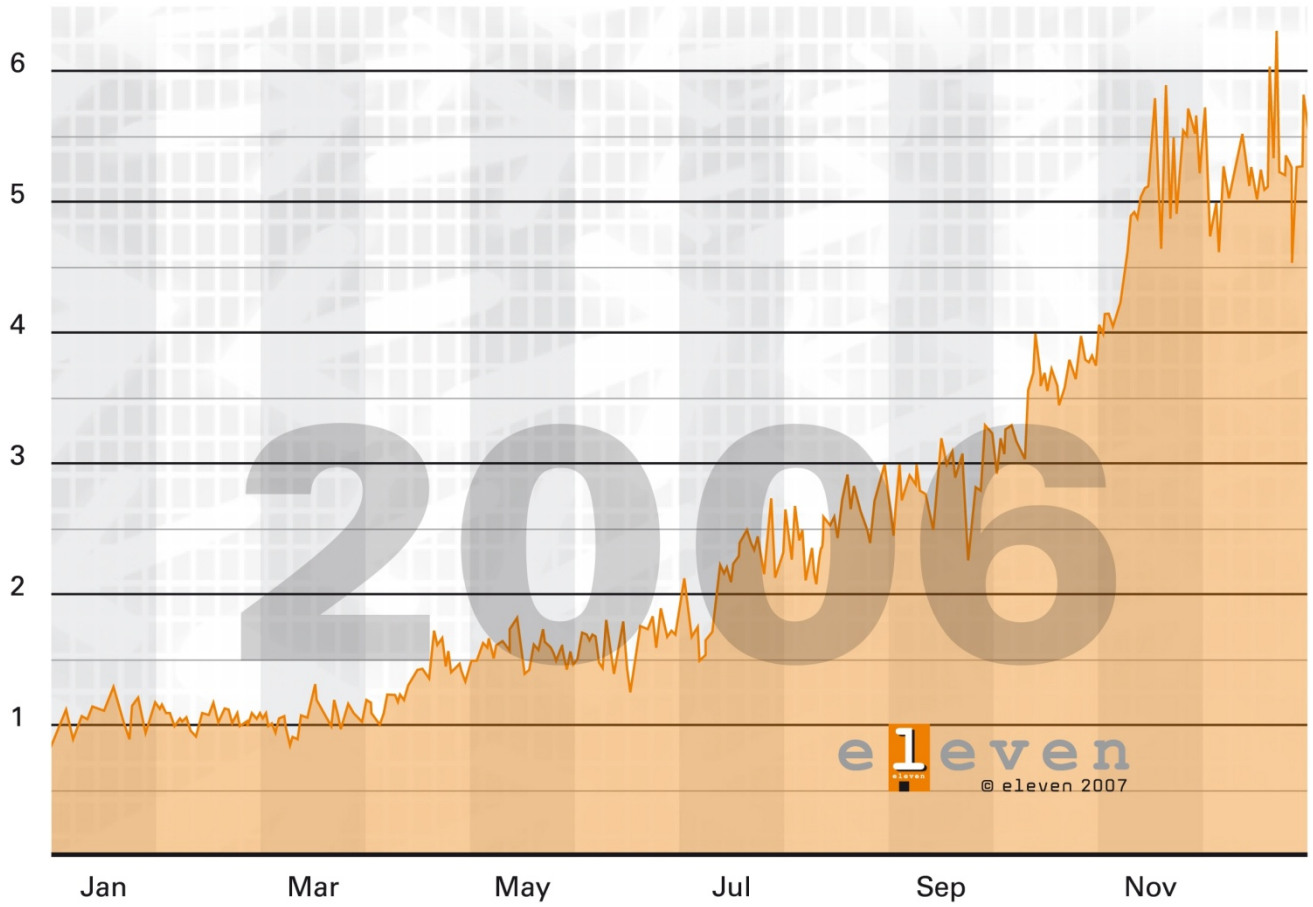


RR1 wie hat sich der clean anteil von 2003 bis ende 2006 im vergleich zum spam-anteil entwickelt

Robert Rothe, 04/09/2007

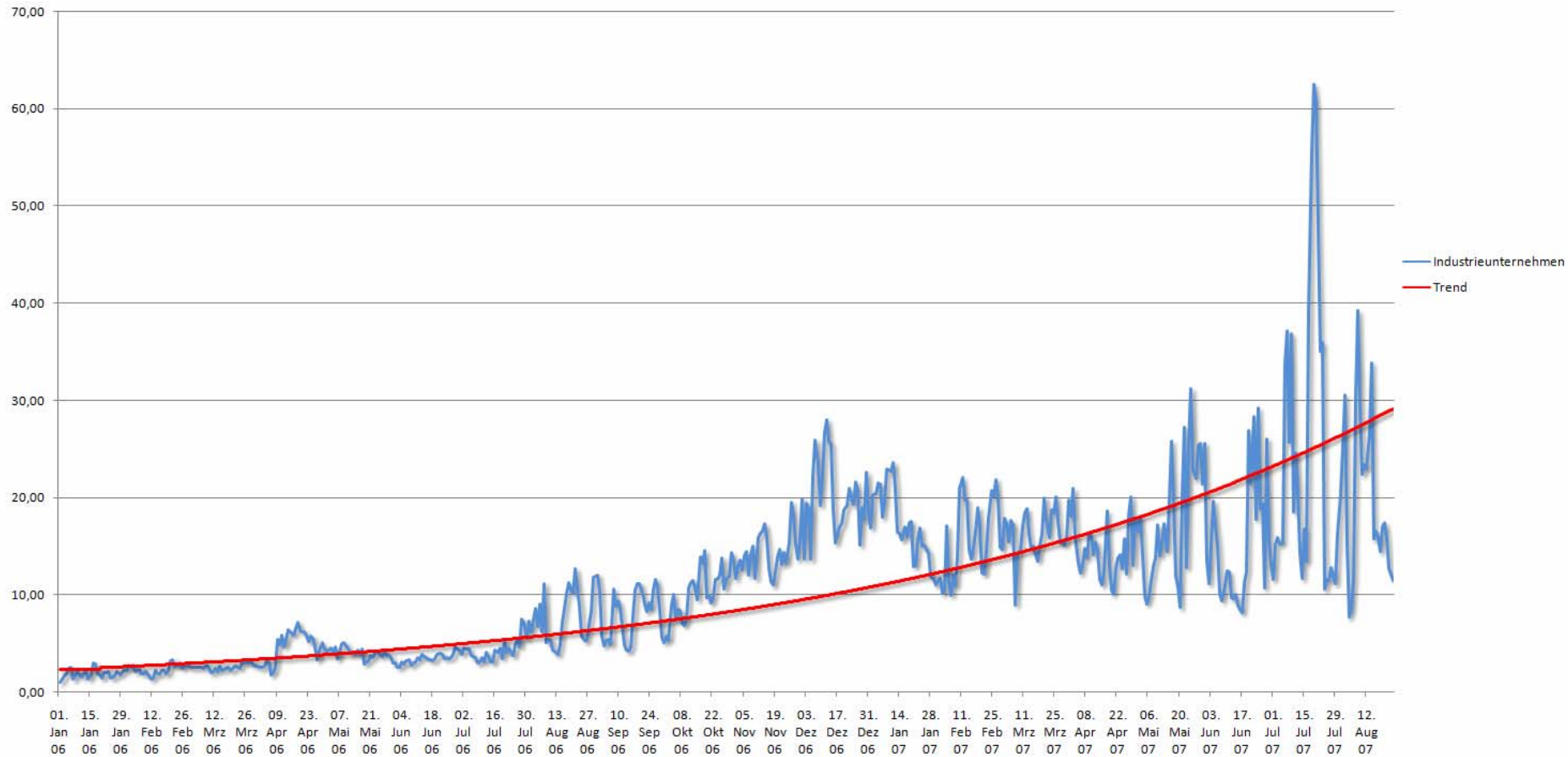
Increase of Spam 2006

entire eXpurgate traffic, 01.01.2006 – 31.12.2006



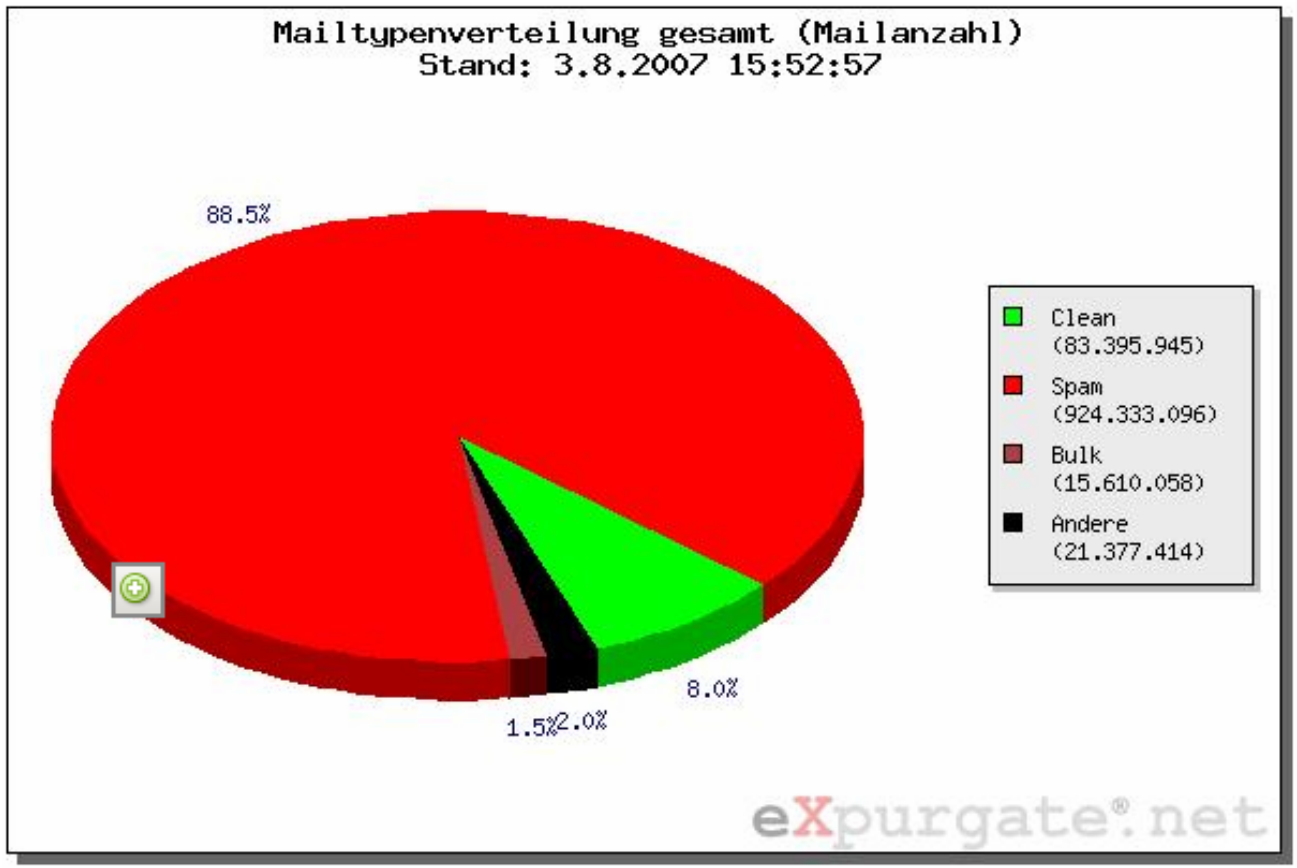
Up to 63 GB E-Mail trash daily

blue chip company, 01.01.2006 - 12.08.2007



Actual Spam Proportion: 89 % Spam

Large Enterprise 08/07



Technical characteristics of spam filters

- Recognition rate
  - How many spam mails are detected as spam?
- False Positive Rate
  - How many “clean” e-mails are sorted out erroneously?
- Speed/performance
  - How many mails/sec. per server?
- Privacy
  - What data is transmitted by the filter?
- Administration
  - How much maintenance is needed to keep the filter up-and-running?

New Spam variations

- 2004 — spam containing text and images
- mid 2005 — increase of "image spam" (inline)
- end 2005 — start of randomized image Spam
- April 2006 — peak of sliced images
- June 2007 — new: container spam I (PDF)
- July 2007 — new: container spam II (ZIP, etc.)
- October 2007 — new: mp3 spam

Latest spam trend: container

- First container format: PDF
- 1st occurence: June, 2007
- PDF container can carry:
  - images, graphics, drawings
  - text
  - combinations of the above
- Distributed primarily via Botnets
- Peaking at up to 30% of the entire botnet traffic
- Powerful format !

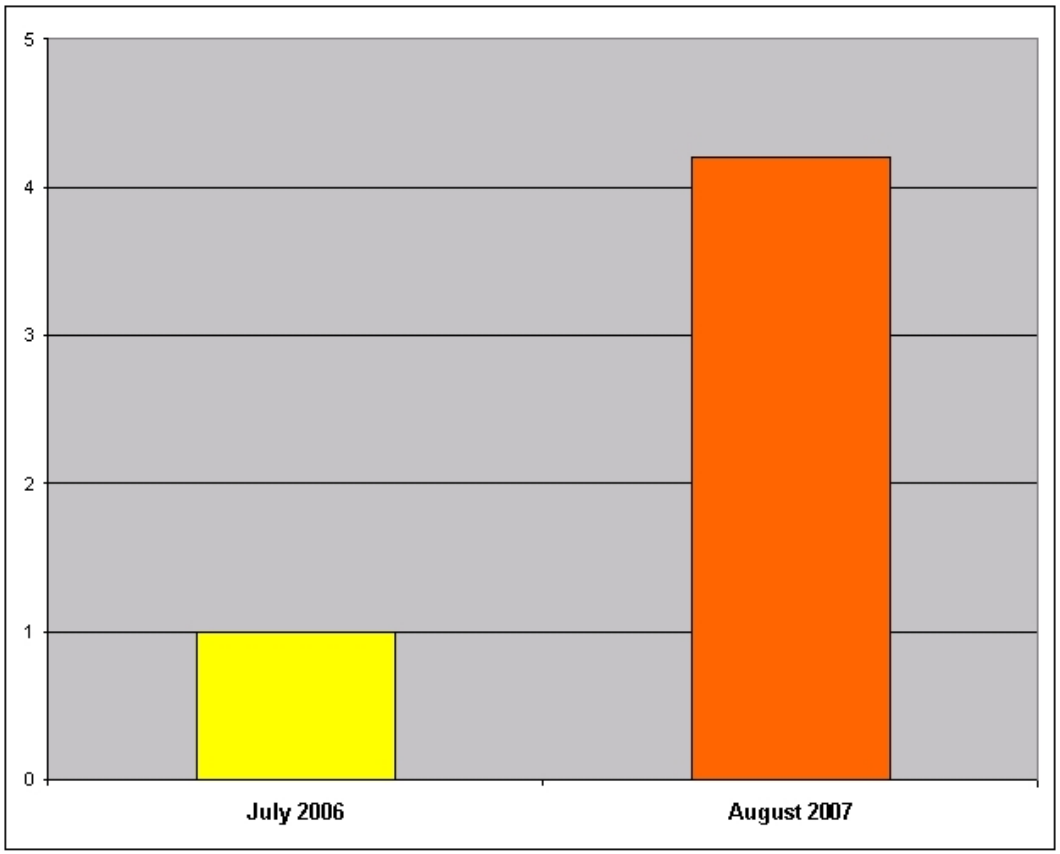
Container spam II / zip-Spam

- Next container format: ZIP
- 1st occurence July, 2007
- zip container can include any document:
  - pdf, txt, xls (sometimes used as container itself)

- Lasted not even three weeks ("too many clicks")
- Similar containers were tried ("arj", "rar", ..)

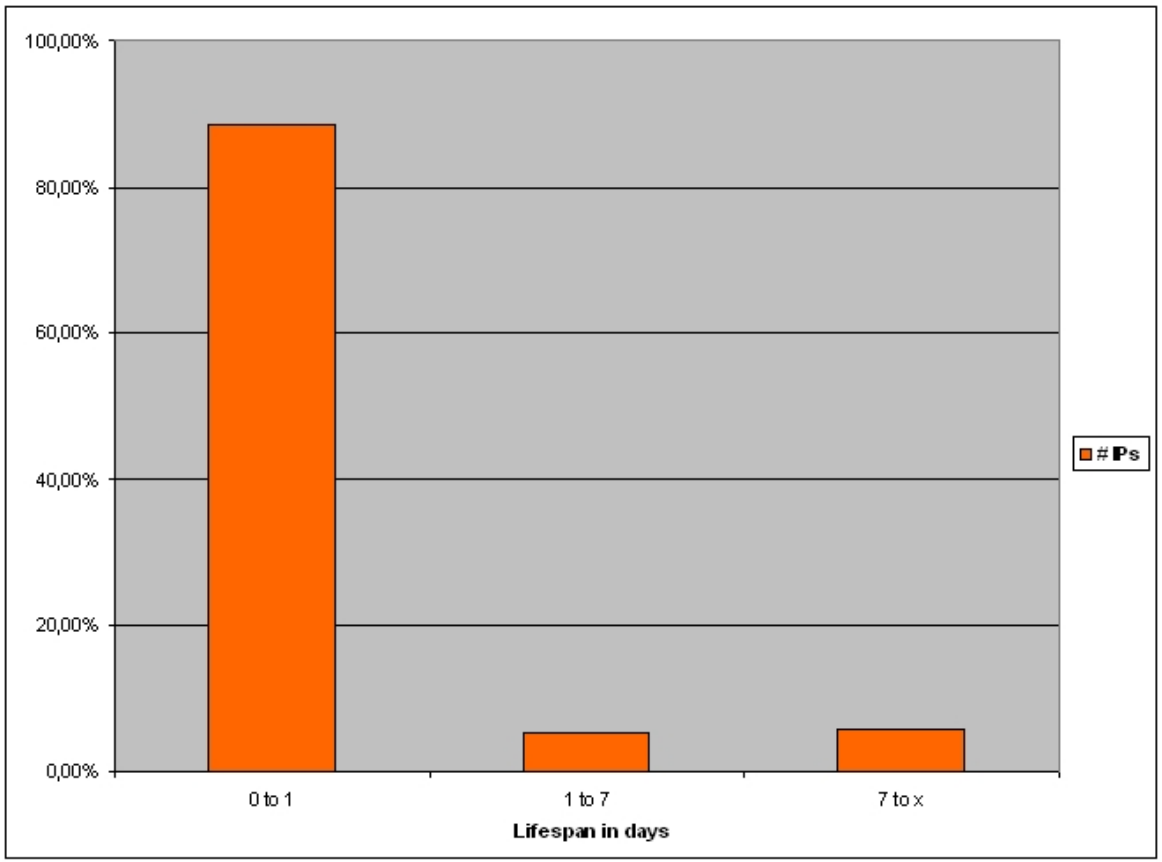
Number of different sender by IP

Comparison July 2006 vs. August 2007



Lifespan of sender IP (August 2007)

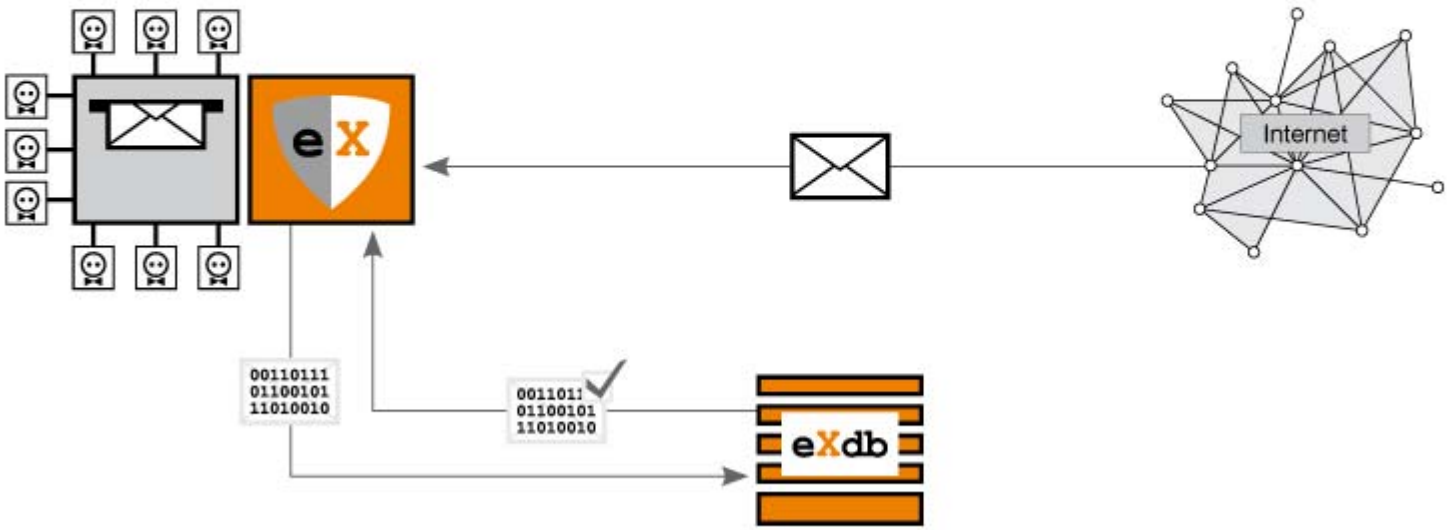
90 % of all sender IP-addresses are active for less than a day !



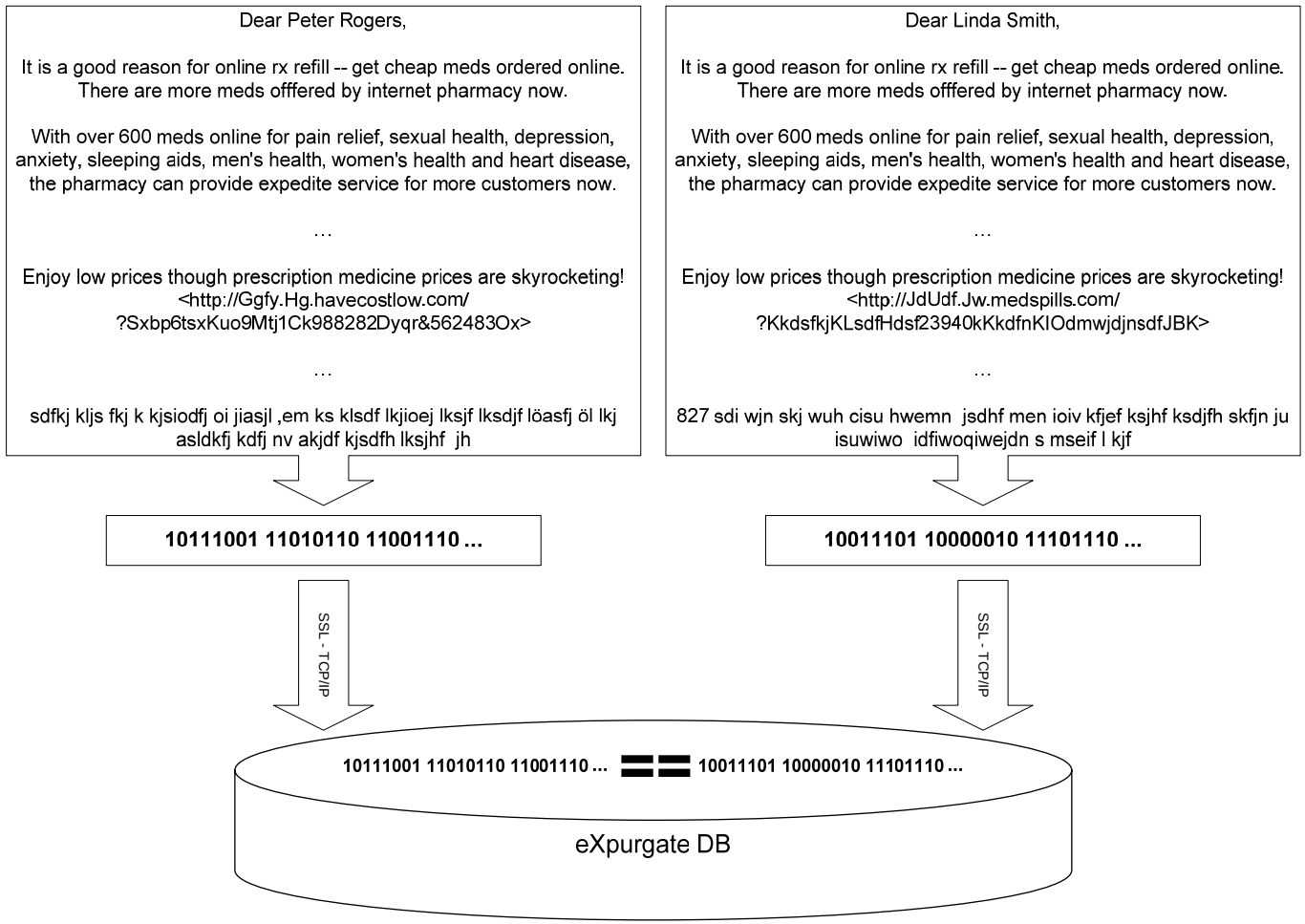
eXpurgate®

Spam filter and e-mail categorisation service

eXpurgate®.Inhouse



The eXpurgate checksum



enSurance

- Dynamic, load-depending control of the e-mail flow
- In high load situations, e-mails from known communication partners are fast tracked – "Frequent Partner" list
- Availability even in the case of an attack (DoS) or extreme load peaks
- Unknown communication partners are temporarily rejected
- Quick processing and reception of e-mails is guaranteed
- The "Frequent Partner" list is dynamically and automatically updated and extended

enSurance

- No blacklisting
  - Permanent blocking of "bad" IP addresses
  - False Positives
  - No reliable sources
  - Slow & complex
- No greylisting
  - This approach is outdated
  - Delaying of legitimate e-mails
- No whitelist
  - Does not tell you anything about the "type" of the e-mail
  - whitelisting is extremely error-prone
  - always incomplete

enSurance

- Protects the whole installation base
- Statistics can be performed across all eXpurgate installations and servers
- Supports loop protection and mail bomb protection

eXpurgate®

- Categorisation of all incoming e-mails
- Important (individual) e-mails are distinguished from lower-ranking messages (e.g. newsletters) and unsolicited or even dangerous e-mails
- **Spam recognition rate > 98,4%**
- Individual messages won't be wrongly classified as spam (**no "false positives"**)
- Detection of potentially dangerous e-mail contents or attachments
- Can be combined with virus scanning and **Virus Outbreak Detection**
- After initial installation and configuration, **no further administrative effort** is needed
- Little or no system load
- Suitable for enterprises of all sizes and large ISPs

Thank you very much for your attention!

E-MAIL-SICHERHEIT MADE IN GERMANY