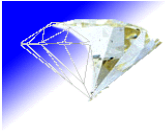


## GUUG Frühjahrsfachgespräch

---

# GREETDELAY, a new approach to fight Spam from BotNets

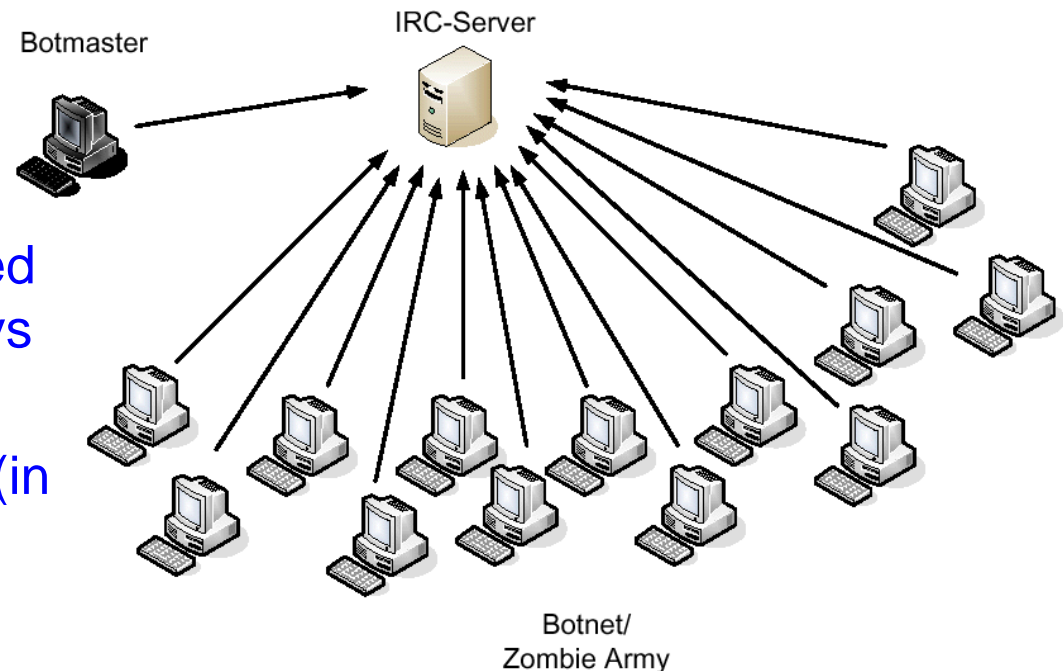
**Dr. Erwin Hoffmann**  
**March 2007**



## Four Source Hypothesis ....

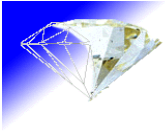
- Main source: BotNet PCs
- 2nd source: Through-Away Domains
- 3rd source: Unqualified operated and configured E-Mail Gateways (Open Relays)
- 4th source: On-purpose MTAs (in particular .ru)

*BotNets are build "industrial" to serve criminal purposes and are marketed as such. A BotNet consists typically of about 20,000 PCs. It is guessed, that worldwide 50 mio PCs are available through BotNets*



*Today, BotNets are controlled centrally by means of the IRC protocol.*

*Source: "Threat Update: Botnets" by Lukas Feiler*



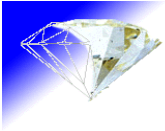
## Current Filter Approaches (1) ....

---



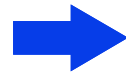
*Sample: port-87-234-35-12.static.qsc.de; p50805008.dip.t-dialin.net*

- Rejection during TCP connection phase; in particular DNS lookups:
  - Legitimate senders have to have a A-Record  
maybe bad for dial-in users
  - Legitimate senders have to have a MX Record for the domain  
common practice for most of the cable net provider
  - Qualified senders have additional DomainKeys/SPF in place  
still not common; only for big players; a lot of overhead
  - RBL and OpenRelay lookups (bye, bye ORDB)  
may be poison (requires additional whitelists)  
more-or-less static IPs only
- ↪ Since BotNet PCs connect typically through cable nets/DSL (see above: QSC, t-online) those means don't help much



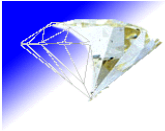
## Current Filter Approaches (2) ....

---



*Reject::SNDR::DNS\_Helo: P:ESMTP  
S:82.127.162.206:alille-151-1-4-206.w82-127.abo.wanadoo.fr  
H:yuowe5 F:lordblack@muonline.dibunet.com*

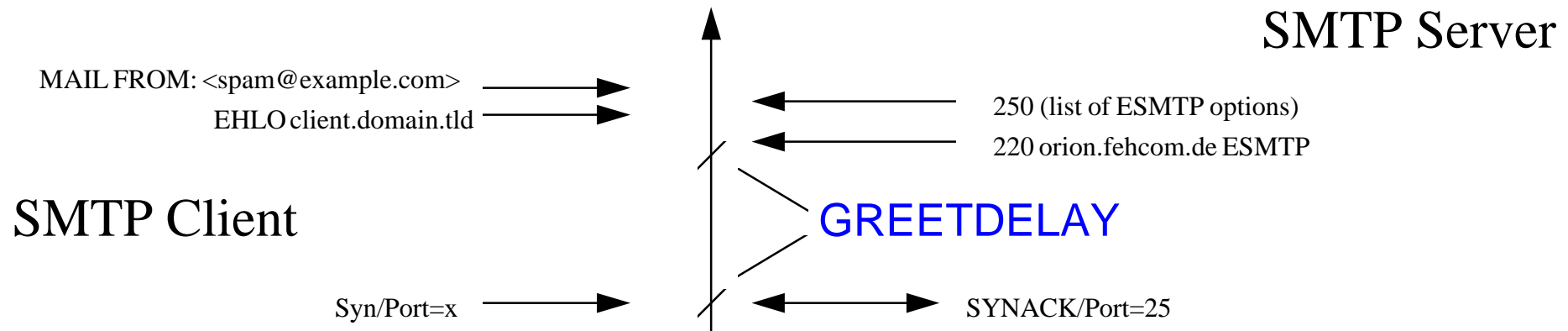
- Rejection during SMTP session:
  - Reverse MX Lookup of 'Mail From:' address  
almost useless these days
  - DNS A/MX lookup of the provided 'Helo/Ehlo' name  
useful, but what about Thunderbird's [a.b.c.d] ?
  - Greylisting, ie. initial temporary rejection of mail (while later accept)  
common today; requires additional whitelisting & expiration  
mechanism; puts queueing burden on all other MTAs
  - Analysis of mail content (SpamAssassin) and rejection above a  
certain Spam score  
very practical, but rather resource intensive
- ↪ Danger of 'false' positives; Greylisting is inferior with rapid delivery of  
emails

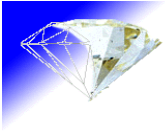


## GREETDELAY: The new approach ...

---

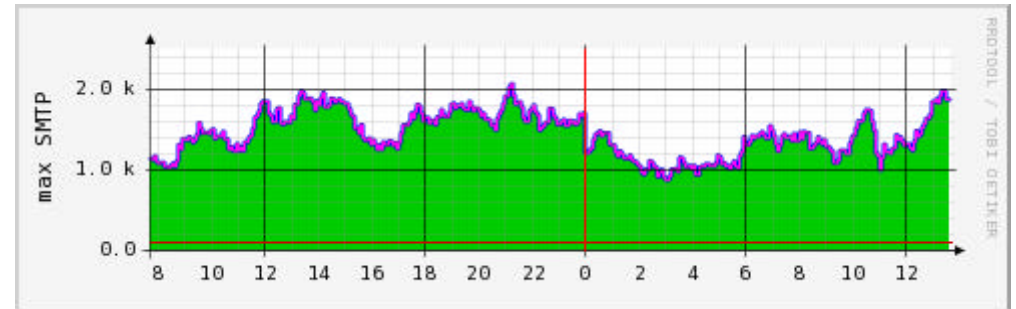
- The idea of GREETDELAY is simple:
  - After the TCP connection of port 25 has been established, the server waits GREETDELAY seconds before he send his EHLO greeting to the client.
  - In case the SMTP clients sustaines that time, the SMTP session is established and continues in the usual way.
  - RFC (2)821 allows a 360 second delay between SMTP transactions.



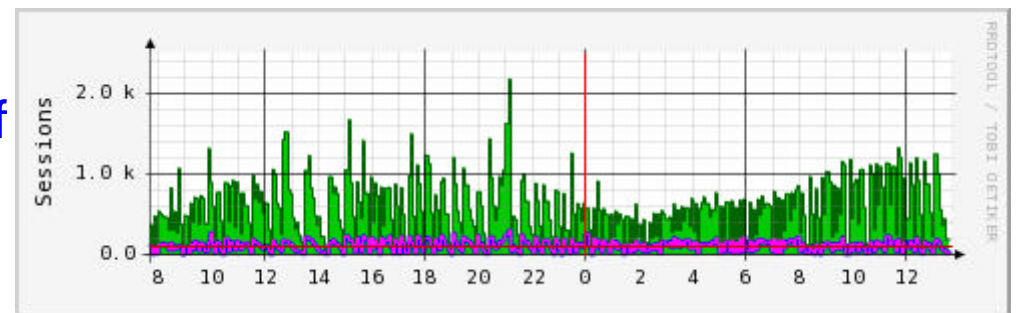


## Why is GREETDELAY so efficient ...

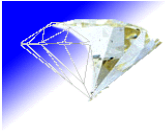
- SMTP engines on BotNet PCs do not have a 'mail queue'; rather
  - they are build such to immediately get rid of the message (irrespectively of success/failure) and
  - move to the next victim.
- A GREETDELAY of 50 - 60 secs will (currently) reduce the amount of spam by 50% - 70%.
- GREETDELAY does not have a significant impact on regular SMTP clients (MTA).



*Incoming TCP connections on port 25*



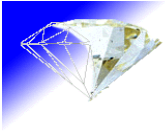
*Accepted SMTP sessions (green) after a GREETDELAY of 30 secs; additionally filtered emails in magenta*



## Pros about GREETDELAY...

---

- *Easy to implement and supported almost everywhere:*
  - Qmail: <http://www.fehcom.de/qmail.html>
  - Exim: <http://slett.net/spam-filtering-for-mx/exim-smtpdelays.html>
  - Postfix: <http://slett.net/spam-filtering-for-mx/techniques.html#smtpdelays>
  - Sendmail: <http://jc.ngo.org.uk/blog/2007/02/10/sendmail-8140-logging-the-greetpause-firing-time/>
- *No administration required:*
  - Can be set-up in splitt-horizion manner
  - Additional whitelisting possible
- *(Almost) No impact on regular email traffic*
- *Since the GREETDELAYing MTA keeps the spam sender in a TCP connection, the overall amount of spam is reduced (less sending slots)*

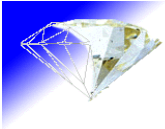


## Cons against GREETDELAY ...

---

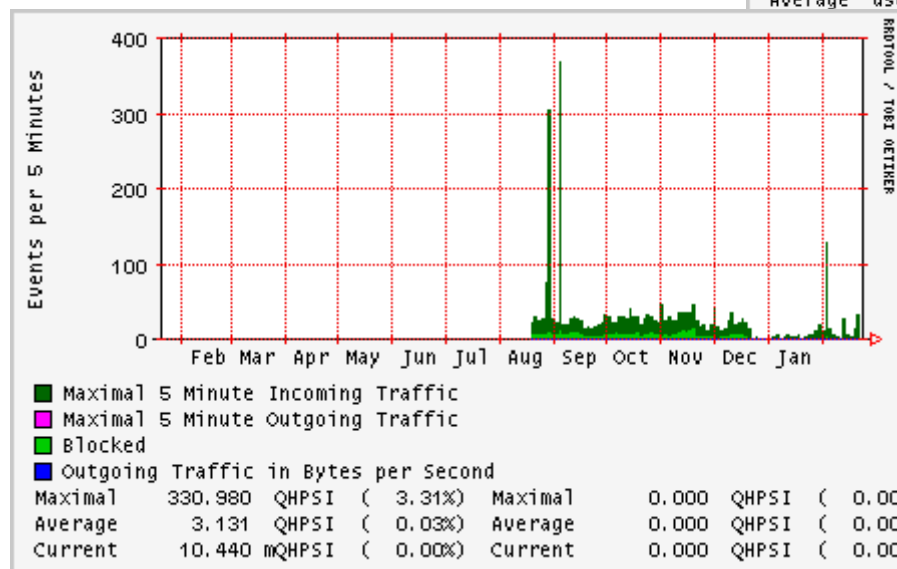
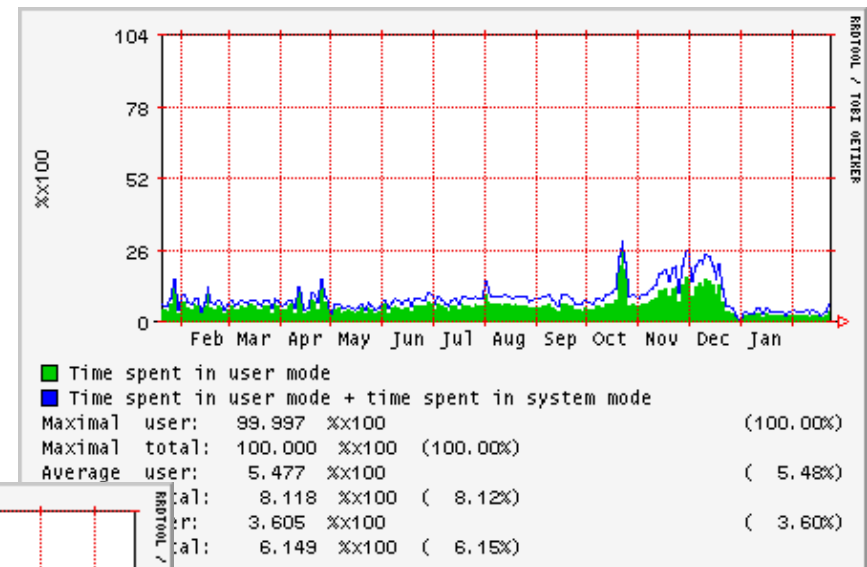
- *Exim:*
  - Default reverse 'Mail From:' lookup will fail, if GREETDELAY > 30 secs
- *Authenticated Users:*
  - Legitimate Users, using SMTP Authentication will need GREETDELAY secs before they can authenticate manually
  - This is a convenience problem only
- *Spammers:*
  - Forced to start a new cycle in developing more advanced SMTP engines
  - Maybe even more difficult to overcome

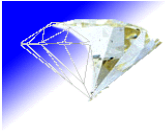




## Other Impacts due to GREETDELAY ...

- Using content-filtering techniques, GREETDELAY will greatly reduce the system load (with the same SMTP concurrency).
- BotNets are known to be also a major source of viruses -- eliminated by GREETDELAY.





Thanks to...

---

- Probiernix:  
[http://www.heise.de/ix/news/foren/go.shtml?read=1&msg\\_id=11829816&forum\\_id=109974](http://www.heise.de/ix/news/foren/go.shtml?read=1&msg_id=11829816&forum_id=109974)
- Dominik:  
<http://www.rlp.lidi.de>
- Peter:  
<http://www.wdr.de>