Yet another way to fight the spam plague

Julien Reveret

RMLL 07/07/2010

Agenda

1/ How the spam landscape changed during the last few years

2/ Antispam techniques pro and cons

3/ Synspam

4/ Conclusion

How the spam landscape changed during the last years

Back 10 years ago :

- Spammers used open relay servers
- They were « amateurs »
- There were really few tricks (fake unsubscribe forms, dictionnary attacks on big domains, mailing lists archives harvesting)

Back 5 years ago :

- Industrialization was on its way
  - Botnets began to relay spams
  - Malwares were harvesting email addresses
  - Anti-antispam techniques were developed

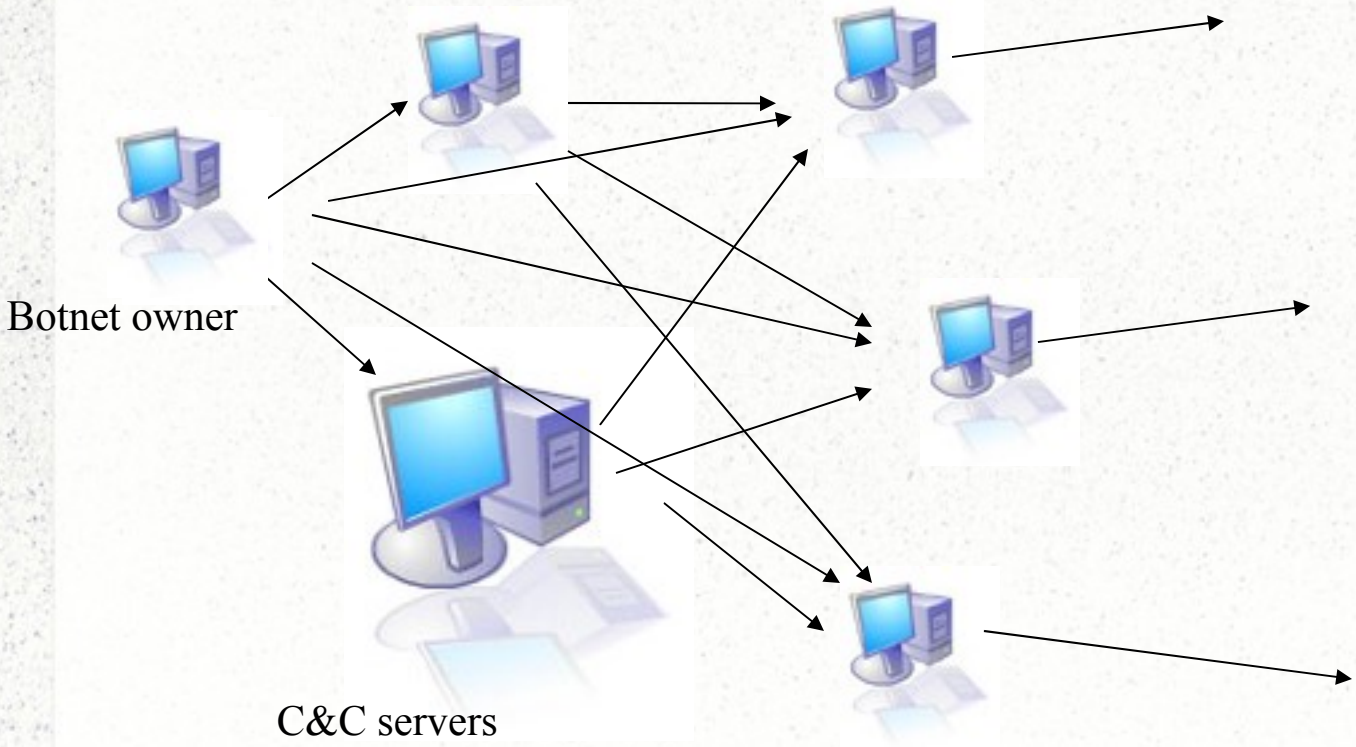
How the spam landscape changed during the last years

Nowadays, more than 90% emails worldwide are spam !

Botnets can send up to 10 billions spams/day:

- Preventing people from using email as a corporate communication tool
- Wasting ISPs resources
- Stealing money through phishing campaigns
- But making a lot of money…

How the spam landscape changed during the last years



Antispam techniques pro and cons

Among all antispam technologies, you might find these in the top 5:

- **Enforcing RFC standards:**
  sender must respect rfc822
- **DNS-based blacklists:**
  spam sender addresses are updated, sometimes in « real-time »
- **Greylisting:**
  first delivery attempt is refused, sender must retry later
- **Rule-based filtering:**
  headers and body mustn't contain words or expressions defined in the rules
- **Statistical content filtering:**
  use of bayesian filters

Unfortunately all these techniques have been overcome by spammers ☹

Antispam techniques pro and cons

- **Enforcing RFC standards :**
  some zombies can pass through the HELO tests (mostly compromised mail servers or webmails)
  same goes for the MAIL FROM and RCPT TO RFC 822
- **DNS-based blacklists:**
  many DNSBL (sorbs, uce-protect) are known to be quite « facists »
  spammers can also use compromised webmails / servers not listed in DNSBL (at least for some minutes/hours/days)
- **Greylisting :**
  users often complain about this system as it also delays their mails
- **Rule-based filtering:**
  spammers can study rules and find ways to defeat them
- **Statistical content filtering:**
  spammers began sending mails to fool bayesian filters years ago. Also short mails with just an URL are often considered as ham.

Synspam

Why another antispam software ?

- I wasn't completely satisfied by the softwares I tested/used.
- I was using packetbl
  - whose author hadn't time to code his software
  - a scoring mechanism was lacking
  - moreover there were no tests on DNS records

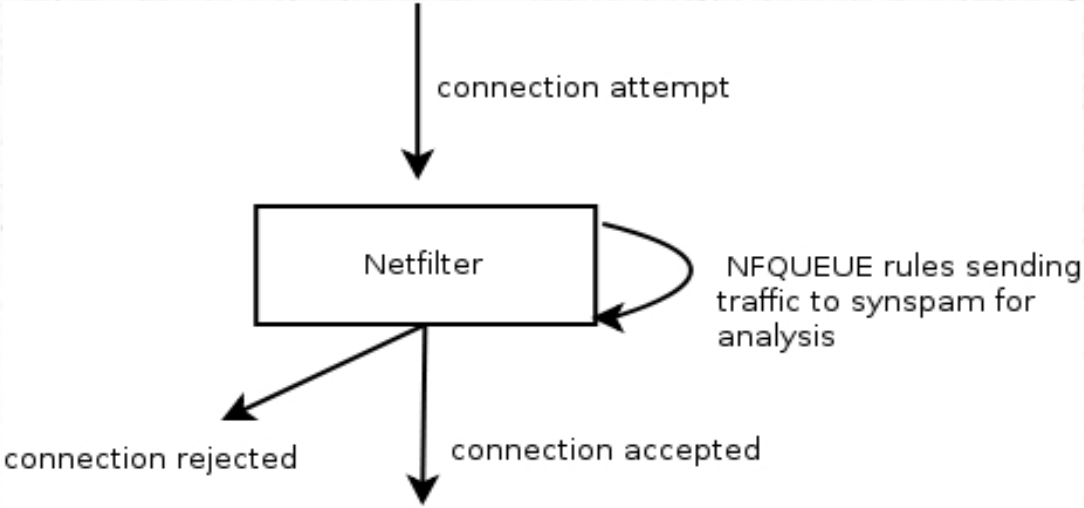
Why should you use synspam :

Softwares like postfw or policyd-weight checks for SMTP dialog problems
Spamassassin/dspam/whatever checks SMTP headers and body
synspam acts as a network-level antispam system

Synspam

What if you could prevent spammers from connecting to your servers ?

Linux 2.6 required
NetFilter queue (nfnetlink) must be enabled
Netfiler “recent” and “mark” modules required



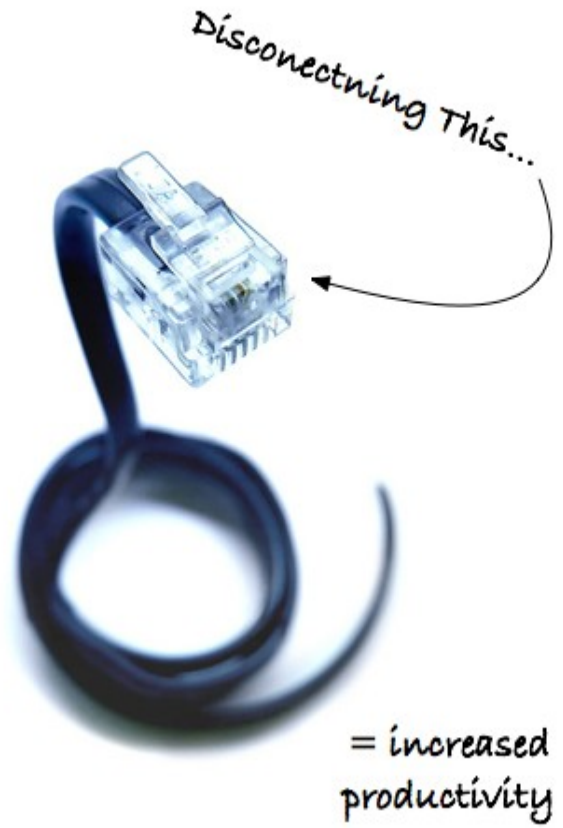
Synspam

Every TCP SYN packet passes these tests:

- Source IP address compared to DNSBL records
- A regex is used to check reverse DNS records
- Blacklisting / whitelisting
- The OS fingerprinting mechanism can distinguish windows systems

And more to come...

DNS sender analysis
Geolocalization
Source AS tracking can help detect spammers haven



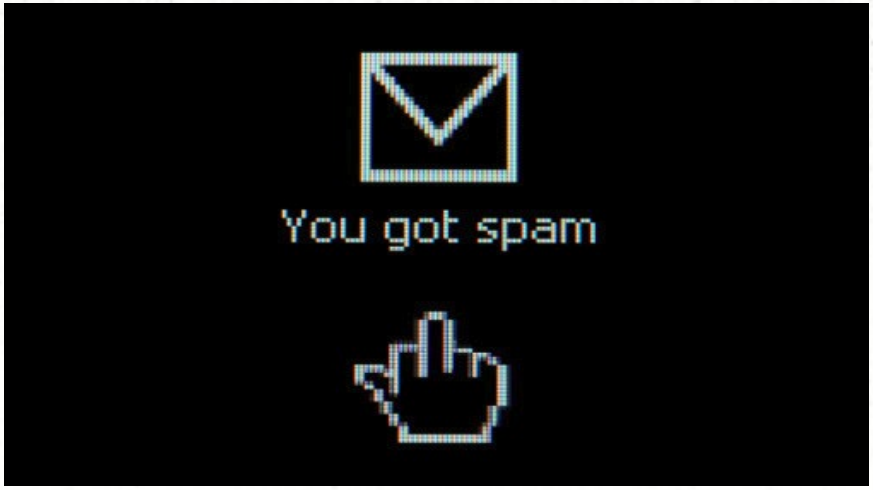
Synspam

Of course there are drawbacks:

Synspam can only check IP and TCP headers

- No L7 protocol check
- No SMTP header or body checks
- Synspam isn't RFC compliant

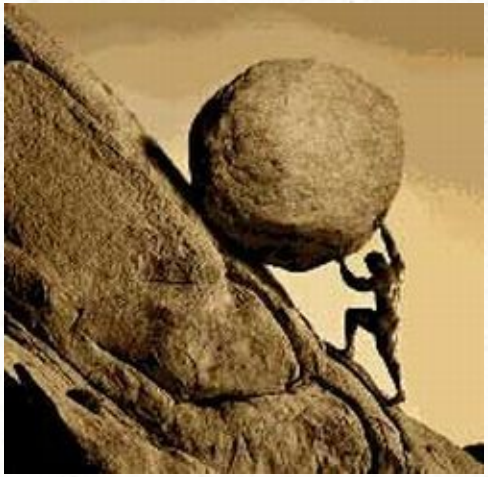
A low threshold means false positives: hard to know who is sending a mail based only on the IP source address



Conclusion

Synspam can help you filter spam without using much resources

Use it as the first level of defense, not alone ;-)



Any questions ?