

Gib SPAM keine Chance

Christoph Wickert

17. März 2011



Postscreen

Christoph Wickert

Postscreen

Postscreen - Gib SPAM keine Chance!

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

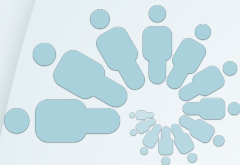
Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup



Inhalt

- ▶ Einführung
- ▶ Postscreen
- ▶ Setup



Einführung

Christoph Wickert

Postscreen

Christoph Wickert

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

Privat

- ▶ Wohnhaft in Münster und Zürich
- ▶ Langjähriger Fedora Mitarbeiter
- ▶ Mitglied im Fedora Advisory Board

Beruflich

- ▶ Senior Engineer bei Kolab Systems
- ▶ Kolab Server Maintainer
- ▶ Kolab Server nutzt postfix



Einführung

Kolab Systems AG

Postscreen

Christoph Wickert

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

Kolab Systems AG

- ▶ gegründet im März 2010
- ▶ Firmensitz in Zürich, Schweiz
- ▶ Entwicklung
- ▶ Paketierung und Anpassungen
- ▶ Hosted Kolab
- ▶ Training und Zertifizierung
- ▶ 2. Level Support für Partner



Einführung Spam

Postscreen

Christoph Wickert

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

White lists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup



Bild: timag (CC-by-SA)



Postscreen

Christoph Wickert

Einführung Spam

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ unerwünscht zugesandte eMail
- ▶ Versand von Spam ist ein lukratives Geschäft
- ▶ > 95% aller Mails sind Spam
- ▶ ... Tendenz steigend
- ▶ > 95% aller Spam-Mails sind von Zombies
- ▶ ... Tendenz steigend
- ▶ zu viel für klassische Spamfilter



Einführung Spam

Postscreen

Christoph Wickert

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup



Bild: Rex Hammock (CC-by-SA)



Postscreen

Christoph Wickert

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

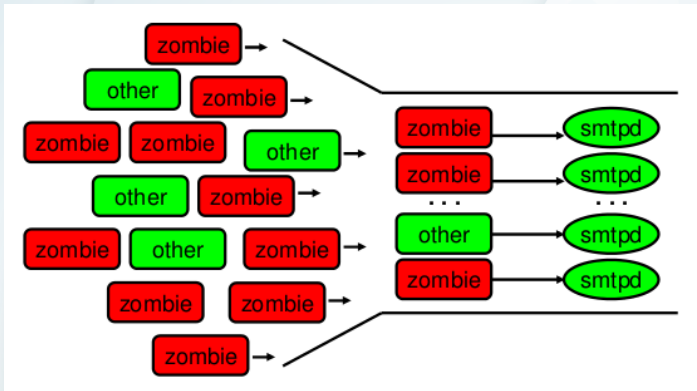
Non-SMTP

Aktionen

Setup

Postscreen Problem

- ▶ smtpd hat `default_process_limit` von 100
- ▶ > 95% davon sind mit Zombies beschäftigt
- ▶ Client muss 5 Minuten warten (RFC 5321)





Postscreen

Christoph Wickert

Postscreen

Idee

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Nicht Spam filtern, sondern Bots
- ▶ Spam sofort abweisen und nichts ins System lassen
- ▶ Spam so 'kostengünstig' wie möglich bekämpfen
- ▶ Tests von einfach und schnell nach aufwändig und langsam



Postscreen

Christoph Wickert

Postscreen

Aufbau

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ `postscreen` lauscht vor dem `smtpd` auf Port 25
- ▶ ein einziger `postscreen` kann viele Hundert Instanzen von `smtpd` schützen
- ▶ filtert Mail und leitet sie an `smtpd` weiter
- ▶ aber: kann keine Authentifizierung, also
- ▶ Alternative: Submission oder SSL



Postscreen

Christoph Wickert

Postscreen

Tests

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

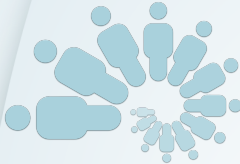
Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup



Tests

- ▶ Whitelists
- ▶ Blacklists
- ▶ Pre-greeting
- ▶ Bare Newline
- ▶ Command Pipelining
- ▶ Non-SMTP



Postscreen

Christoph Wickert

Tests

Statische Whitelists

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Weiße Liste erlaubter Clients
- ▶ Erster Test, bei Erfolg werden alle weiteren übersprungen und die Mail wird direkt an den `smtpd` weitergeleitet
- ▶ Spart Zeit (und Nerven)
- ▶ Workaround für kaputte Clients
- ▶ Parameter: `postscreen_access_list`
- ▶ Vorgabe: `mynetworks`
- ▶ Erweitern um: `permit_mynetworks`



Postscreen

Christoph Wickert

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

Tests

Whitelists

```
/etc/postfix/main.cf
```

```
postscreen_access_list = permit_mynetworks,  
cidr:/etc/postfix/postscreen_whitelist.cidr
```

```
/etc/postfix/postscreen_whitelist.cidr
```

```
192.168.254.0/24 permit  
84.165.98.32      permit
```

- ▶ Syntax wie bei postfix
- ▶ Regeln werden der Reihenfolge nach abgearbeitet



Postscreen

Christoph Wickert

Tests

Temporäre Whitelists

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Temporäre / dynamische weiße Liste erlaubter Clients
- ▶ Automatisch angelegter Cache aus erfolgreichen Tests
- ▶ Gültigkeitsdauer: `postscreen*_ttl`
- ▶ Aufräumen alle 12 Stunden:
`postscreen_cache_cleanup_interval = 12h`
- ▶ Ab postfix 2.9: Sharing von temporären Whitelists im Netzwerk mit `proxymap`
- ▶ Alternativer Ansatz mit `memcache_map`



Postscreen

Christoph Wickert

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

Tests

Statische Blacklists

- ▶ Schwarze Liste verbotener Clients
- ▶ Gleiche Regeln wie bei Whitelists

```
/etc/postfix/main.cf
```

```
postscreen_access_list = permit_mynetworks,  
cidr:/etc/postfix/postscreen_access.cidr
```

```
/etc/postfix/postscreen_access.cidr
```

```
192.168.254.0/24  permit  
84.165.98.32     permit  
# 192.168.* ausschließen, aber nicht 192.168.0.1  
192.168.0.1      permit  
192.168.0.0/16   reject
```



Postscreen

Christoph Wickert

Tests

Dynamische Blacklists

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ DNS-based Blackhole Lists (DNSBL)
- ▶ Datenbanken erkannter Spammer im Internet
- ▶ verschiedene Anbieter, frei und kommerziell
- ▶ mehrere Anbieter nutzen!
- ▶ Gewichtung und Schwellenwert konfigurierbar

```
/etc/postfix/main.cf
```

```
postscreen_dnsbl_sites = zen.spamhaus.org*2  
                        bl.spamcop.net*1 b.barracudacentral.org*1  
postscreen_dnsbl_threshold = 2
```




Postscreen

Christoph Wickert

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

Tests

Pre-Geeting

Ein typischer SMTP Dialog

```
220 mail.example.net ESMTP Postfix
HELO client.example.net
250 mail.example.net
MAIL FROM: joerg@example.net
250 OK
RCPT TO: sabine@example.net
250 OK
DATA
354 End data with <CR><LF>
From: Jörg Mustermann <joerg@example.net>
To: Sabine Musterfrau <sabine@example.net>
Subject: HDL

Hallo Lausemädchen, wir sehen uns nachher.
.
250 OK: queued as E82C21839B9
QUIT
221 Bye
```



Postscreen

Christoph Wickert

Tests

Pre-Greeting

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Spam-Bots haben es eilig
- ▶ Nach $< 1,5$ Stunden landen die meisten auf einer DNSBL
- ▶ Bots warten nicht auf HELO, sondern senden sofort
- ▶ Verzögern (aber nicht zu lange)
- ▶ Verwirren!

```
/etc/postfix/main.cf
```

```
postscreen_greet_wait = 6s
```

```
postscreen_greet_banner = 220-mail.example.net
```



Postscreen

Christoph Wickert

Tests

Deep Protocol Tests

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ aufwändig
- ▶ problematisch

Probleme

- ▶ Nach dem 220 HELO kann eine Verbindung nicht mehr an smtpd weitergegeben werden.
- ▶ postfix setzt die Clients auf die temporäre Whitelist und sendet einen Statuscode 4xx zurück.
- ▶ Client muss erneut Verbindung aufbauen und wird durchgelassen.



Postscreen

Christoph Wickert

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

Tests

Bare Newline

- ▶ SMTP-Protokoll ist Zeilenorientiert
- ▶ Zeilen enden auf <CR><LF>
- ▶ Bare Newlines sind unvollständigen Zeilenenden nur mit <LF>
- ▶ Wirksamkeit begrenzt, nur noch wenige Bots machen es
- ▶ Vorgabe: deaktiviert

```
/etc/postfix/main.cf
```

```
postscreen_bare_newline_enable = yes  
postscreen_bare_newline_action = ignore
```



Postscreen

Christoph Wickert

Tests

Command Pipelining

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Erkennt Bots, die mehrere Kommandos senden und nicht auf Antworten warten
- ▶ Vorgabe: deaktiviert

```
/etc/postfix/main.cf
```

```
postscreen_pipelining_enable = yes  
postscreen_pipelining_action = enforce
```



Postscreen

Christoph Wickert

Tests

Non-SMTP

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Erkennt Bots, die offene Proxys nutzen
- ▶ Nutzen Komandos, die nicht im SMTP-Protokoll vorkommen
- ▶ Vorgabe: deaktiviert

```
/etc/postfix/main.cf
```

```
postscreen_non_smtp_command_enable = yes  
postscreen_non_smtp_command_action = drop  
postscreen_forbidden_commands =  
smtpd_forbidden_commands
```



Postscreen

Christoph Wickert

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

Tests

Aktionen

Aktionen

- ▶ **ignore** ignoriert das Testergebnis und führt weitere Tests aus
 - ▶ **drop** beendet die Verbindung sofort mit Status 521 (Does not accept mail)
 - ▶ **enforce** wartet weitere Tests ab und antwortet solange mit Status 550 (Mailbox unavailable)
-
- ▶ So viel loggen wie möglich, deshalb lieber **enforce** als **drop**
 - ▶ **drop** kann vom Client als Verbindungsabbruch interpretiert werden. Bots, die man eigentlich loswerden will, kommen wieder.



Umstieg auf postscreen

Postscreen

Christoph Wickert

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

```
/etc/postfix/master.fc
```

Aus

```
smtp      inet  n -  n -  - smtpd -o Parameter  
wird
```

```
smtp      inet  n -  n -  1  postscreen
```

```
smtpd     pass  - -  n -  - smtpd -o Parameter
```

- ▶ Man beachte das Prozesslimit von 1: Nur eine **postscreen** Instanz!
- ▶ Alle Parameter übernehmen!
- ▶ **postfix reload**



Authentifizierung

trotz postfixscreen

Postscreen

Christoph Wickert

Inhalt:

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

```
/etc/postfix/master.cf
```

```
192.168.13.20:smtp    inet  n - n - - smtpd
-o myhostname=mail.example.net
178.146.13.20:smtp    inet  n - n - 1
postscreen
178.146.13.20:smtpd   pass  - - n - - smtpd
-o myhostname=mail-external.example.net
```

- ▶ 2 IPs/Hostnamen für 2 Postfix Instanzen
- ▶ Interner postfix weiterhin auf Post 25
- ▶ MX Record auf externen postfix ändern



Postscreen

Christoph Wickert

Referenzen

Weitere Informationen

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Postscreen README
http://www.postfix.org/POSTSCREEN_README.html
- ▶ Wietse Venema "Zombies suck the life out of the mail server":
<http://www.postfix.org/postscreen-2010.pdf>
- ▶ Ralf Hildebrandt Neuerungen in postscreen 2.8
<http://os-t.de/vortraege/ralfhildebrandt.pdf>



Postscreen

Christoph Wickert

Referenzen

Abbildungsverzeichnis

Inhalt :

Einführung

Spam

Postscreen

Problem

Idee

Aufbau

Tests

Whitelists

Blacklists

Pre-Greeting

Deep Protocol Tests

Bare Newline

Command Pipelining

Non-SMTP

Aktionen

Setup

- ▶ Bild Spam 1:
<http://www.flickr.com/photos/27308606@N04/3920588954>
- ▶ Bild Spam 2:
<http://www.flickr.com/photos/rexblog/6607524945>