

SPAM



Ausschnitt aus Monty Python's Flying Circus
https://www.youtube.com/watch?v=M_eYSuPKP3Y

Rspamd

A horizontal banner featuring a light blue background with a faint world map on the left and several orange envelopes with red dashed lines on the right, arranged as if they are floating or moving across the scene.

Fast, free and open-source spam filtering system
<https://www.rspamd.com>

hexa-, fleaz
2016-12-13

TOC

- Was ist Spam?
- Integration
 - Rmilter
 - Milter und Content Filter
- Architektur
- Rspamd
 - Features
 - Installation
 - Vorteile gegenüber SpamAssassin






Was ist Spam?

Return-Path: <info@dinnerie.biz.ua>
Delivered-To: hexa@ darmstadt.ccc.de
Received: from dinnerie.biz.ua (s1.dinnerie.biz.ua [62.141.44.57])
by venus.chaos.hg.tu-darmstadt.de (Postfix) with ESMTP id 4E3734730
for <hexa@ darmstadt.ccc.de>; Thu, 20 Oct 2016 07:41:17 +0200 (CEST)
Received: from dinnerie.biz.ua (dinnerie.biz.ua [62.141.44.57])
by dinnerie.biz.ua (Postfix) with ESMTPA id C03E6A4BD9CD;
Thu, 20 Oct 2016 02:44:09 +0300 (EEST)
Message-ID: <852201d22a7b\$d7f0eb40\$3c90132c@info>
Reply-To: "Online-Apotheke" <info@dinnerie.biz.ua>
From: "Online-Apotheke" <info@dinnerie.biz.ua>
To: <gcwutzschleife@d-golf.de>
Subject: Bis zu 30% BONUS Pills für alle Bestellungen.
Date: Thu, 20 Oct 2016 02:44:13 +0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_NextPart_000_0006_01D22A7A.D87B9480"
X-MSMail-Priority: Normal
X-Mailer: Microsoft Windows Live Mail 14.0.8117.416
X-MimeOLE: Produced By Microsoft MimeOLE V14.0.8117.416
[...]



Was ist Spam?

Return-Path: <info@dinnerie.biz.ua>
Delivered-To: [hexa@darmstadt.ccc.de](mailto:hexa@ darmstadt.ccc.de)
Received: from dinnerie.biz.ua (s1.dinnerie.biz.ua [62.141.44.57])
by venus.chaos.hg.tu-darmstadt.de (Postfix) with ESMTP id 4E3734730
for <hexa@darmstadt.ccc.de>; Thu, 20 Oct 2016 07:41:17 +0200 (CEST)
Received: from dinnerie.biz.ua (dinnerie.biz.ua [62.141.44.57])
by dinnerie.biz.ua (Postfix) with ESMTPA id C03E6A4BD9CD;
Thu, 20 Oct 2016 02:44:09 +0300 (EEST)
Message-ID: <852201d22a7b5d7f0eb40\$3c90132c@info>
Reply-To: "[Online-Apotheke](mailto:info@dinnerie.biz.ua)" <info@dinnerie.biz.ua>
From: "[Online-Apotheke](mailto:info@dinnerie.biz.ua)" <info@dinnerie.biz.ua>
To: <gcwutzschleife@d-golf.de>
Subject: [Bis zu 30% BONUS Pills fur alle Bestellungen.](#)
Date: Thu, 20 Oct 2016 02:44:13 +0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_NextPart_000_0006_01D22A7A.D87B9480"
X-MSMail-Priority: Normal
X-Mailer: Microsoft Windows Live Mail 14.0.8117.416
X-MimeOLE: Produced By Microsoft MimeOLE V14.0.8117.416
[...]

Indikatoren

-  **Forward-/Reverse-DNS Beziehung**
 - o 62.141.44.57
 - o vps1232331.vs.webtropa-customer.com.
-  **Sender-Policy Framework**
 - o "v=spf1 a mx -all"
-  **DNS Blacklist**
 - o Barracuda
 - o INPS.de
 - o DNS RBL
-  **Bayes**
 - o [Online-Apotheke](mailto:info@dinnerie.biz.ua)
 - o [Pillen](#)
-  **Recipient**
 - o [To](#) ≠ [Delivered-To](#)

Was ist Spam?

	Ist Spam	Ist Ham
Als Spam erkannt		False Positive <i>Problematisch</i>
Als Ham erkannt	False Negative <i>Ärgerlich</i>	

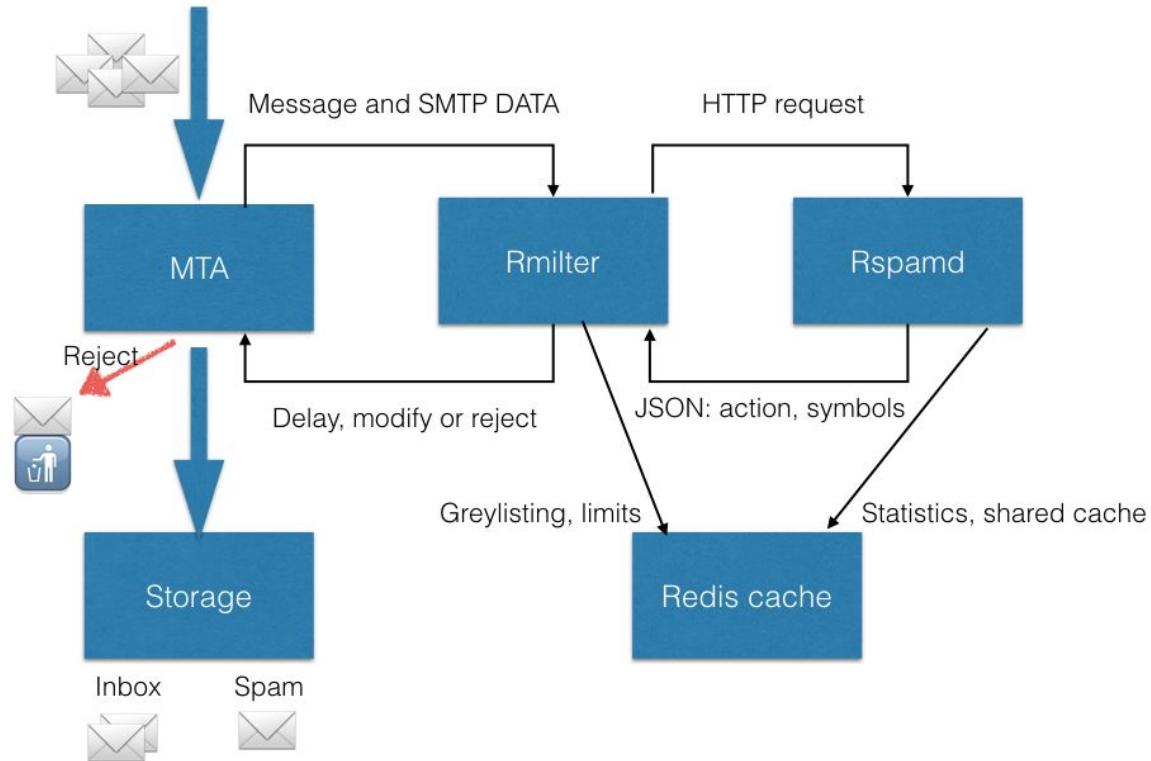
Integration

- Via [rmlter](#) über das milter Protokoll
- milter (Mailfilter)
 - Ermöglicht phasenweise Betrachtung der SMTP Session
 - Jede Phase erlaubt das frühzeitige Ablehnen einer Mail
 - Spart Ressourcen und ermöglicht vielfältige Reaktionen
- rmlter ermöglicht Anbindung von Funktionalitäten wie
 - Spam- und Virens Scanner
 - Greylisting, Ratelimiting (via Redis)
 - Reply Whitelisting (via Redis)
 - DKIM

Milter vs Content Filter

- Content Filter werden nach Annahme der Mail verarbeitet
 - Keine Möglichkeit mehr Mails zu rejecten/dropfen
 - Mails können nur noch verändert werden (bspw. X-Spam-Header)
 - Und müssen dann erneut in Postfix injiziert werden
- Milter können vor der Mailqueue arbeiten
 - Und bei SMTP Events Hooks auslösen, bspw. bei CONNECT, DISCONNECT, HELO, MAIL FROM
- In other news...
 - Benutzt kein QMail...
 - kann nämlich keine Milter...
 - ...und somit kein Rmilter/Rspamd

Architektur



Features

- Eventbasierte Architektur
- Parallele Verarbeitung vieler Regulärer Ausdrücke durch Hyperscan
 - High-performance regular expression matching library
<https://github.com/01org/hyperscan>
- Umfangreich parametrisierbar durch Lua API
- Auswertung und Steuerung über Webfrontend
- Viele Inhaltsfilter-Plugins
 - Reguläre Ausdrücke
 - Fuzzy hashes (erkennen ähnlicher Mails, via Redis)
 - DCC (erkennen von Bulk Mails)
 - Chartable (erkennen von Character Set Auffälligkeiten)

Features

- Viele Policy-Filter
 - SPF, DKIM, DMARC
 - Whitelist, Greylist
 - DNS-Listen (bewerten Reputation des Absenders)
 - URL-Listen (bewerten Links in Mails)
- Statistische Bewertung
 - Bayes Filter (via Redis)
 - Neuronales Netzwerk (via libfann)

Rspamd aggregiert sehr viele Scoring-Methoden und kann dadurch Mails genauer klassifizieren als übliche Spamfilter.

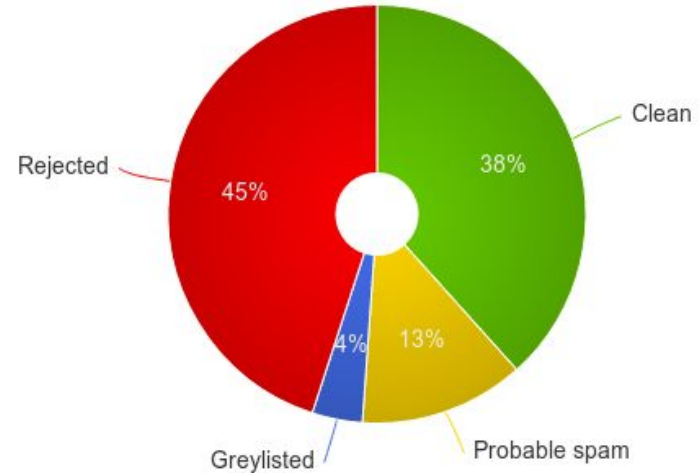
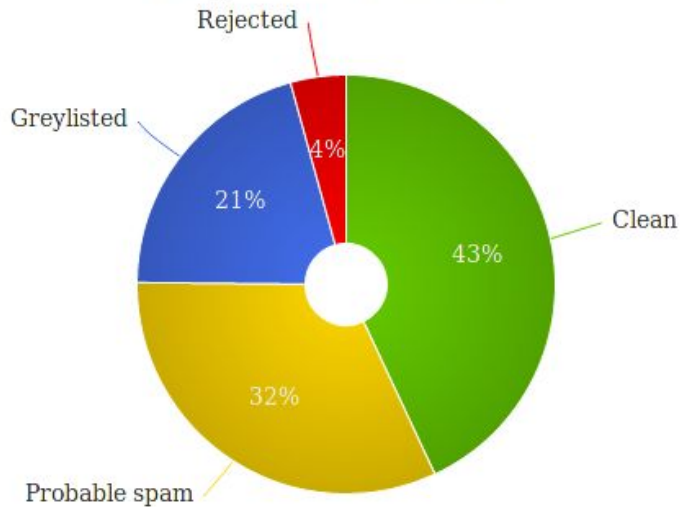
Features: Bayes filter

- Statistische Analyse
 - Wenn das Wort “Viagra” in der Mail enthalten ist → Höhere Wahrscheinlichkeit für Spam
- Hidden Markov Klassifizierer
- Automatisches Anlernen konfigurierbar
- Manuelles Anlernen über CLI und Webfrontend
- Benötigt 200 Spam/Ham Beispiele
 - Mehr Beispiele für beide Kategorien
 - ⇒ verringert Rate von False Positive/Negative Ergebnissen

Features: Webfrontend

mail.rainownerds.de

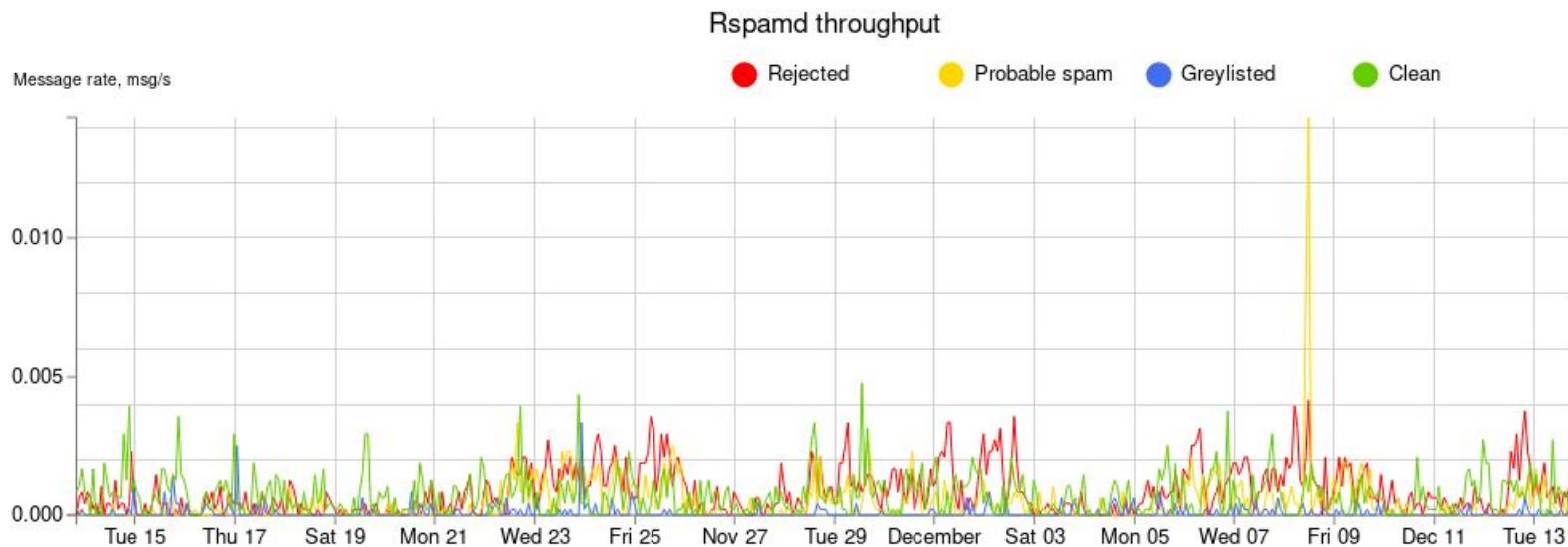
➤ 3.000 E-Mails verarbeitet



mail.darmstadt.ccc.de

➤ 13.000 E-Mails verarbeitet

Features: Webfrontend



Features: Webfrontend

Datum	Absender	IP	Action	Score	Results	Größe	Dauer
2016-12-13 09:37:17	985387a951d12b86635800e4f4d29605@async.facebook.com	2607:f8b0:4003:c06::231	no action	-7.75 / 15.00	TO_DN_ALL, DMARC_POLICY_ALLOW, FORGED_RECIPIENTS_FORWA...	21939	1.048
2016-12-13 09:19:19	E1cGIGP-0005LZ-RO@adexconsultingsolutions.com	195.245.113.205	reject	17.28 / 15.00	MID_RHS_MATCH_FROM, DMARC_NA, HAS_REPLYTO, ADVANCE_FEE_...	4624	0.288
2016-12-13 07:57:10	0206536424.909337.18455.server@rebreatherausbildung.de	118.96.226.11	add header	7.80 / 15.00	RCVD_COUNT_2, R_DKIM_NA, ONCE_RECEIVED, TO_DN_NONE, HAS_...	5787	2.092
2016-12-13 07:17:39	1667616764.327722.04567.server@rebreatherausbildung.de	45.64.237.79	greylist	5.80 / 15.00	RCVD_COUNT_2, R_SPF_NEUTRAL, R_DKIM_NA, ONCE_RECEIVED, T...	5874	1.024

Beste Scores erreichen u. a.

- 10.5 twitter.com
- 7.5 facebook.com
- 5.7 paypal.com
- 3.8 tickets.darmstadt.freifunk.net
- 3.3 darmstadt.ccc.de

Installation

`/etc/postfix/main.cf`

```
smtpd_milters = unix:/var/run/rmilter/rmilter.sock

milter_protocol = 6
milter_mail_macros = i {mail_addr} {client_addr} {client_name} {auth_authen}

# skip mail without checks if milter will die
milter_default_action = accept
```


Installation

/etc/rmilter.conf.common

```
spamd {  
    servers = spam1.example.com:11333, spam2.example.com;  
  
    # reject_message - reject message for spam  
    reject_message = "Spam message rejected; If this is not spam contact abuse at example.com";  
  
    # whitelist - list of ips or nets that should be not checked with spamd  
    whitelist = 10.0.0.0/8;  
  
    # use rspamd action for greylisting  
    spamd_greylist = yes;  
  
    ...  
}
```

Beispielhafte, vollständige Konfiguration unter <http://rspamd.com/rmilter/>

Vorteile gegenüber SpamAssassin

- Integration über milter (statt content_filter)
- Höhere Effizienz
 - Höherer Durchsatz/Zeit bei gleichem Filtersatz
 - State machine für Zerlegung von Mail Struktur, statt Reguläre Ausdrücke
- Mehr Scoring-Metriken
- Modernes Webfrontend
 - Auswertung des verarbeiteten Mailaufkommens
 - Konfiguration der Filtersymbole
 - Anlernen von Spam/Ham/Fuzzy
- Größerer Kontextraum für Bayes Klassifizierer

Probleme

- Manche Indikatoren benötigen Zeit
 - Um verlässliche Ergebnisse (z.B. via Reputation) bieten zu können
 - Spam der gerade durchkam, kann eine Stunde später perfekt als Spam erkannt werden
- Bayes Filter Training
 - benötigt vorsortierten Spam/Ham
- False Positive/Negative können problematisch werden
 - mit Bayes und/oder Whitelisting gegensteuern

Goodie: Thunderbird Plugin

From Stephan Voeth <voeth@asta.tu-darmstadt.de>★

Subject **[cda] Gemeinsam gegen (Video)überwachung**

To lounge@computerwerk.org★, kontakt@demokratie-statt-ueberwachung.de★, public@lists.darmstadt.ccc.de★

Score ● 5.9 (Bayes: undefined, Fuzzy: undefined) Scan time: 0.41

Greylist Greylisted for 317 seconds, whitelisted till 2016-11-20 01:06:36, type: data hash

Rules MIME_BAD_ATTACHMENT(4.00), FORGED_MUA_MOZILLA_MAIL_MSGID_UNKNOWN(2.50), MIME_UNKNOWN(0.10), DMARC_NA(0.00), RCVD_IN_DNSWL_MED(-0.50), R_DKIM_NA(0.00), MIME_GOOD(-0.20)

← Reply | Reply List | → Forward

Um zu Verstehen wie die Mails bewertet und behandelt wurden gibt es den umfangreichen X-Spamd-Result Header.

Das Thunderbird-Plugin **Rspamd-spamness** macht diese Bewertung sichtbar.

<https://github.com/moisseev/rspamd-spamnes>

Danke für eure Aufmerksamkeit!

Habt ihr noch Fragen?

Slides

<https://s.fleaz.me/WyD>

