Kevin A. McGrail
kmcgrail@InfraShield.com

Fighting Spam with Perl using Apache SpamAssassin & MIMEDefang

Introduction

Who am I? PAUSE: kmcgrail

Apache SpamAssassin

Milters

MIMEDefang

Solving Email & Spam Issues with Perl

https://www.linkedin.com/in/kmcgrail

INFRASHIELD

What is Apache SpamAssassin?

A Scoring Framework

An API & a Program

Stops Spam

Spam Markers:

- Consent vs. Content i.e. what is Spam?
- Transactional/Relational
- RFC-Compliance

Writing your own rules

KAM.cf

Meta Rules cause the least FPs

Test your Syntax: spamassassin --lint

Rules only affect YOUR installation!

Think about Custom Rules for your Firm

Pfizer Story

Example Meta Rule

```
#HEART ATTACK SPAM

body __KAM_HEARTPROD1 /heart ?attack/i
body __KAM_HEARTPROD2 /enzyme/i
header __KAM_HEARTPROD3 Subject =~ /heart attack|healthy.{4,10}cells/i
header __KAM_HEARTPROD4 From =~ /clear 7/i

meta KAM_HEARTPROD (__KAM_HEARTPROD1 + __KAM_HEARTPROD2 + __KAM_HEARTPROD3 +
__KAM_HEARTPROD4 >= 4)
describe KAM_HEARTPROD Snake Oil Heart Health du Jour
score KAM_HEARTPROD 7.0
```

SA 3.4 vs 4.0 Gotcha with the Subject!

Writing Rules

https://wiki.apache.org/spamassassin/WritingRules

Tips on Regular Expression

“Some people, when confronted with a problem, think "I know, I'll use regular expressions." Now they have two problems.” - Jamie Zawinski

https://perldoc.perl.org/perlre.html
https://www.learn-perl.org/en/Regular_Expressions

Use mutt macros: macro index \cy "<pipe-message>spamassassin -t -D 2>&1 | grep -e KAM -e Content\\ analysis<enter>\n" "Test Message with Spamassassin for PCCC Rules"

Daemonizing SpamAssassin

1. spamc/spamd
2. MIMEDefang
3. Amavisd-new
4. exim

daemon noun

dae·mon

5. daemon : a software program or process that runs in the background
https://www.merriam-webster.com/dictionary/daemon

Why Daemonize?

1. Compilation / Startup

   &

2. Why I use spamc/spamd w/MIMEDefang.

Quiz Break

Quiz - Part A

*$s

Quiz - Part B

8-)}---o

Quiz - Part C

>^..^<

Quiz - Part D

Quiz - Part E

8-)[>-=/ / / >

@}-;-'---

<3

What is a Milter?

A Milter (Mail fILTER) is both the protocol & the Library

Invented by Sendmail

Postfix can use it too

Similar features in exim

What is MIMEDefang?

E-Mail filtering framework using Sendmail's Milter interface

MIMEDefang provides mechanism; you provide policy - Dianne F. Skoll

Perform midstream commands on SMTP conversations

What is a MIMEDefang filter?

The filter is the policy

Written in Perl

Allows you to be a party to the SMTP conversation at various points using the flexibility of Perl

Also let’s you use the Milter API to change the email

Getting Started with MIMEDefang

MIMEDefang is part of EPEL on CentOS/Red Hat

Install epel using the following command: yum install epel-release

Refresh repo by typing the following command: yum repolist

yum remove postfix

yum install sendmail sendmail-cf sendmail-devel spamassassin mimedefang

```
echo "INPUT_MAIL_FILTER(\`mimedefang', \`S=unix:/var/spool/MIMEDefang/mimedefang.sock,
F=T, T=C:15m;S:4m;R:4m;E:10m')" >> /etc/mail/sendmail.mc
make -C /etc/mail
```

Getting Started with MIMEDefang (more)

Change a few default settings in /etc/sysconfig/mimedefang

LOG_FILTER_TIME=yes
MX_RELAY_CHECK=yes
MX_HELO_CHECK=yes
MX_SENDER_CHECK=yes
MX_RECIPIENT_CHECK=yes
MX_TICK_REQUEST=60
MX_TICK_PARALLEL=3

systemctl start mimedefang
systemctl start sendmail

Also enable them and run sa-update

A Simple Filter to Demonstrate the Framework

- Go through /etc/mail/mimedefang-filter
  - Missing use Mail::SpamAssassin

- Has debug statements and just “listens”

- tail -f /var/log/maillog

Inject an Email Manually

Monitor the maillogs & Inject an email directly into the SMTP MTA:

telnet localhost 25
helo test.com
mail from: kevin@test.com
rcpt to: root
data
Subject: This is a test
Date: jasjdkasjdksajd

This is a message

.

^^^^ That's a period there....

Pick a Victim

Continue Monitoring the logs

2xx/4xx/5xx

Pick a victim

Integrating MIMEDefang with SpamAssassin

filter_end

spamc

action_change_header_immediately

Storytime

Doing the Impossible AKA Cannonball Run

Integrating MySQL queries

Or JSON, Redis, SQL, LDAP, DNS Queries

Let’s Look through mimedefang-filter-mysql-spamc.examples

Looking at Reverse Pointers and SMTP HELO

1. Net-ValidMX - Will put a new release on CPAN soon!
2. X-KAM-Reverse: Failed / Suspect
3. HELO Checks (yourself, “friend”)

Fixing RFC non compliant software

- Headers wrong?
- Date issues?
- Need DKIM support?

More Demonstrations!

Mitigate CVE Exploits

Example:

filter_recipient

https://news.cpanel.com/urgent-updates-for-70-76-and-78-and-exim-cve-2019-10149/

```
#EXIM EXPLOIT 2019 June
 if ($recip =~ /root\+\$\{run/i) {
   $explanation = "Invalid user";
   $answer = 'REJECT';
   return ($answer, $explanation);
 }
```

What about Web Forms & Forums?

Synthesizing Email Headers

First, use Captcha

Second, Use the data on your form to check the MX

Third, create an “email” from the data with the name, from email, Subject and content.

Finally, Use your spamd cluster to send a spamc query over to check it!

Other tools to look at:

- Orange (https://orangeassassin.org/)
- rspamd
- exim

Some Resources:

PCCC SPAM Compendium

https://raptor.pccc.com/raptor.cgim?template=email_spam_compendium

Combating Spam Using Sendmail, MIMEDefang and Perl

https://mimedefang.org/static/mimedefang-lisa04.pdf

Exim Embedded Perl

https://www.exim.org/exim-html-current/doc/html/spec_html/ch-embedded_perl.html &

https://github.com/Exim4U/src/tree/master/etc/exim/exim.pl

Thanks!

Demo Filters are at https://s.apache.org/tpc19files

Slides are at: https://s.apache.org/tpc19

Image Credits:

KAM photo taken by Ted King, used with permission.
Drawing by Kade McGrail, used with permission
Thanks to James Thompson at cPanel for the Apache SpamAssassin Logo
https://www.pexels.com/photo/person-writing-on-notebook-669615/
https://www.pexels.com/photo/brown-envelopes-in-mail-box-1919343/

Kevin A. McGrail
www.linkedin.com/in/kmcgrail