

# SPAM<sup>®</sup>

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

“The Guns...They’ve Stopped.”

Jeff Ballard  
David Parter

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# SPAM<sup>®</sup>

## Concepts and Building Blocks

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

**Hormel**  
Foods

Serving  
Sugges

# Golden Rules

- If you as a server operator say you'll deliver a message **never** silently delete it.
- That means if you accept a message you must either:
  - Deliver the message
  - Send a bounce message (DSN)
    - Do that too much and the Internet will hate you.
- Give legitimate mail a chance to be delivered.
  - Be careful with outright rejections

# Getting the Guns to Stop<sup>®</sup>

- Stop SPAM at the earliest possible spot
- ...preferably before accepting it in the first place.

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

**Hormel**  
Foods

Serving  
Suggest

# What about Mail Server Load?

- Common concern: lots of mail checking on mail servers will cause too much load and result in lost email
- Reality: lots of mail checking on mail servers is easier than handling lots of SPAM.
  - Additional checks is much more than offset by reduced antivirus scanning load and anti-spam scanning
- Be careful about DNS load.

Ingredient  
Pork with  
Ham, Salt  
Water,  
Sugar,  
Sodium  
Nitrite

NET WT.  
12 OZ.  
(340g)



Serving  
Suggest

# Identifying SPAM<sup>®</sup>

- Best filter is the human brain
- What we look for
  - Who its from
  - To
  - Subject
  - Content
  - Expected?

Ingredients:

Pork with  
Ham, Salt,

Water,

Sugar,

Sodium

Nitrite.

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# What can a program do?

- Pattern match
  - Spamassassin and the like
  - Look for known spammy content
    - As content gets more complex cost to scan the content rises
  - Basian (word scoring)
    - Statistical but based on reported spam/ham
- Issues: effectiveness & compute cost

Ingredients:

Pork with  
Ham, Salt,  
Water,

Sugar,  
Sodium

Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

Hormel  
Foods

Serving  
Suggest

# What can we do instead?

- Examining SMTP protocol is a lot cheaper
- Count mistakes/suspicious items:
  - SMTP protocol violations
  - Unverifiable addresses
  - Internet reputation
  - DNS oddities
- Past history
- Use protocol features (like temporary failures)

Ingredients:

Pork with  
Ham, Salt,

Water,

Sugar,

Sodium

Nitrite.

NET WT

12.0Z

(340g)

U.S. DEPARTMENT OF  
AGRICULTURE

GET

SPAM

STUFF

BACK FOR DETAILS

Hormel  
Foods

Serving  
Suggest

# Sender Address Verification<sup>®</sup>

- The SMTP RFC allows for a VRFY command to verify email addresses.
  - Nearly every site on the Internet disables this SMTP command.
- Alternative:
  - Start delivery from <> to <user@example.com> and see if the server accepts that address.
  - Abort before actually sending (before issuing a 'data' command)

# Sender Address Verification (cont)

- What are the costs?
  - Potentially adding load on a third party's mail server.
    - You could be acting in a DDOS attack
  - Adds additional delay
- Some domains (yahoo) do not give meaningful answers
- Recursion hurts

Ingredients:

Pork with  
Ham, Salt,  
Water,

Sugar,  
Sodium

Nitrite.

NET WT.

12 OZ.

(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Sugges

# Recipient Address Verification<sup>®</sup>

- What happens if you run MX servers for domains you do not control?
  - i.e. a border MX server
- To reduce DSN's you really want to check to see if the email is going to a valid address.
- Recursion really hurts.

Ingredients:

Pork with  
Ham, Salt,

Water,  
Sugar,

Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)



SPAM

STUFF

SEE BACK FOR DETAILS

Hormel  
Foods

Serving  
Suggest

# Reputation: Blacklists

- RBL's are another part of the toolkit
- Kinds:
  - List known spammers
  - List known exploitable computers
  - Policy Blacklists (ISP end users who shouldn't be sending mail from that IP)

Ingredients:

Pork with  
Ham, Salt,

Water,  
Sugar,

Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# Reputation: Blacklists (cont)<sup>®</sup>

- Data sources:
  - Spamtrap email addresses
  - End-user reported spam
  - Active scanning

Ingredients:

Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Sugges

# DNS Oddities

- Often spammers use poorly configured servers.

- 127.\*

- Unrouteable addresses (RFC 1918: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

- Non-numeric addresses

- “Missing” MX records

- Unexpected answers

- This might be intentional.

Ingredients:

Pork with  
Ham, Salt,  
Water

Sugar,  
Sodium  
Nitrite.

NET WT  
12 OZ.  
(340g)

U.S.  
DEPARTMENT OF  
AGRICULTURE

Hormel  
Foods

Serving  
Sugges

# SPF

- Sender Policy Framework
- Register legitimate mail servers for a domain in your domains DNS records.
- A mail server can check the SPF record to see if the computer sending this email is permitted to do so for that domain.

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# What's a greylist?

- A greylist is an intentional temporary failure that a well-formed SMTP server will attempt to retry after a period of time.
- Spammers often use custom software that isn't well formed (and often don't retry).
  - Although some spammers are **always** retrying email – do you get lots of spam twice?
  - SPAM via an open relay will probably retry
- Cost: Potentially delayed mail

# Demerits

- Assign demerits to messages based upon mistakes/oddities noted.
- The greylist period is a function of the number of demerits.
- Advantage:
  - Likely Spam: many demerits, get long delays
  - Likely Ham: no demerits, no delay
  - Mystery Meat: some demerits, some delay
    - Is your mail server suspicious?

# Restricted addresses

- Internal email addresses often receive spam from external sources.
  - Ex: staff@example.com
- It is a good idea to block this.
- Be careful to give a useful error so that legitimate users using inappropriate SMTP servers have a chance to fix it.

Ingredients:

Pork with  
Ham, Salt,

Water,  
Sugar,

Sodium  
Nitrite

NET WT.  
12 OZ.  
(340g)



Serving  
Suggest

# SPAM®

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

How we do it

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

**Hormel**  
Foods

Serving  
Sugges

# How'd we do it? (CAE)

- Combination of two milters:
  - Mailfromd
    - Enforces Greylisting, internal email addresses, and egregious violations
  - Amavis
    - Enforces file extension restrictions, calls Sophos and ClamAV
      - We use 2 antivirus engines on the server

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# How'd we do it? (CS)

- Call mailfromd as a milter:
  - Mailfromd
    - Enforces Greylisting, and egregious violations
    - ClamAV with SaneSecurity signatures
      - <http://www.sanesecurity.co.uk/clamav/index.htm>

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS  
**Hormel**  
Foods

Serving  
Sugges

# How'd they do it? (DoIT)

- Implemented GROSS
  - Greylisting of Suspicious Sources
  - Uses RBL's only

Ingredients:

Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Sugges

# SPAM<sup>®</sup>

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

A Mailfromd implementation

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# Installation

- Its easy.

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Sugges



# SPAM<sup>®</sup>

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

# Mailfromd

- “Mailfromd is a general-purpose mail filtering daemon for Sendmail and Postfix. It is able to filter both incoming and outgoing messages using criteria of arbitrary complexity, supplied by the administrator in the form of a script file. The daemon interfaces with the MTA using Milter protocol.”

<http://puszcza.gnu.org.ua/software/mailfromd/>

# Mailfromd

- Simple mail filtering language
- Hooks all parts of the SMTP protocol
- Great debugging capabilities (mtasim)

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# Mailfromd's greylisting

- A greylist record is a combination of three fields plus insertion time:
  - 1. Sending IP address
  - 2. SMTP FROM address (sender)
  - 3. RCPT TO address (recipient)
- This triplet is used to uniquely identify a greylist.
- Stored until a defined expire time

Ingredients:

Pork with  
Ham, Salt,

Water,  
Sugar,

Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
SPAM  
STUFF  
SEE BACK FOR DETAILS  
Hormel  
Foods

Serving  
Suggest

# Mailfromd's greylisting (cont)

- `greylist ("sending_ip - from@address - to@address", interval)`
- Returns the amount of time left to greylist (if any)

Ingredients:

Pork with  
Ham, Salt,

Water,  
Sugar,

Sodium  
Nitrite

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Suggest

# How we do it

- Multiple mail servers
- 30 day expire time
- Rolling forced expiration of greylist database
  - First email: entries recorded on all mail servers
  - Greylist is enforced
  - Mail servers flush their database through the month
  - A flushed mail server will reacquire greylist entries, but other servers will have the database.
  - Effect: once greylisted, most regular correspondence will not be delayed.

Ingredients:

Pork, vit.

Ham, Salt,

Water,

Sugar,

Sodium

Nitrite.

NET WT.

12 OZ.

(340g)

U.S. DEPARTMENT OF AGRICULTURE

Hormel Foods

Serving Suggest

# The Greylisting Formula

- The time we wait is the addition of:
  - 15 minutes for 1 RBL or 30 minutes for each RBL if more than 1
  - 15 minutes for 1 demerit or 30 minutes for each demerit if more than 1
  - The Greylist time is unique to each triplet

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS  
**Hormel**  
Foods

Serving  
Suggest

# Noteable exceptions

- What NEVER gets greylisted
  - Email from a UW IP address
    - We know some computers on campus are compromised and sending spam
    - risk is too high if we greylist someone “important”
  - Email to postmaster
    - You’d be surprised how many spammers send junk to postmaster.
  - People on the "spamfriends" list
    - iwannareadeverything@example.com

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
SPAM  
STUFF  
SEE BACK FOR DETAILS  
Hormel  
Foods

Serving  
Sugges

# SPAM<sup>®</sup>

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

So, how does it work?

Lets briefly look at the SMTP  
protocol...

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Sugges

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

# SMTP: HELO/EHLO

- We check how the remote server says hello.
- Ways to get rejected:
  - Claim to be 127.0.0.1 (but isn't)
  - Claim to be a bogon IP address
  - Connect from an IP address where the PTR record starts with "localhost."

Ingredients:

Pork with

Ham, Salt,

Water,

Sugar,

Sodium

Nitrite.

NET WT.

12 OZ.

(340g)



Serving  
Sugges

# SMTP: HELO/EHLO (Cont)<sup>®</sup>

- Ways to get demerits:
  - Claim to be the server's IP address (but isn't)
  - Claim to be at a different IP address
  - Put something other than an IP address in brackets
  - Claim to be at something that does not have a DNS entry
  - Claim to be the server (EHLO mx1.cae.wiscc.edu) but not our address
  - Note: Only 1 possible demerit for ehlo checks

# SMTP: MAIL FROM

- We check how the remote server says who the email is from.
- Ways to get rejected:
  - Temporary rejection if the sending rate is too high
    - Different rate for bounces than for senders

Ingredients:

Pork with

Ham, Salt,

Water,

Sugar,

Sodium

Nitrite.

NET WT.

12 OZ.

(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

Hormel  
Foods

Serving  
Sugges

# SMTP: MAIL FROM (Cont)<sup>®</sup>

- Ways to get demerits:

- Don't have the address like address@example.com
- Hostname(client\_addr) looks like a home broadband connection
- Have the domain name or MX server resolves to a bogon (4 demerits)
- 1 demerit if we cannot verify your address
  - Don't check yahoo, they don't play nice
  - CS: 1 demerit for \*yahoo\*

Ingredients:  
Pork with  
Ham, Salt  
Water,  
Sugar,  
Sodium  
Nitrite

NET WT.  
12 OZ.  
(340g)

INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Suggest

# SMTP: RCPT TO

- We check how the remote server says who the email is to.
- Ways to get **rejected**:
  - Address is marked as internal only
  - To: part of the address is a bogon (shouldn't ever happen)
  - The address does not verify
    - We return whatever the next server returns.

Ingredients:

Pork with

Ham, Salt,

Water,

Sugar,

Sodium

Nitrite.

NET WT.

12 OZ.

(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

Hormel  
Foods

Serving  
Sugges

# SMTP: RCPT TO (Cont)

- Ways to get demerits:
  - Address is missing < and >
- Greylisting is added before the RCPT TO is enforced.
  - Can exempt some recipients from greylisting, if desired
- Headers added to aid debugging of user complaints

# SMTP: Body

- We now check messages as they come in -- before we tell the sending party.
- If the message matches an antivirus rule, the sending party gets told right away.
- We are off the hook.

Ingredients:

Pork with  
Ham, Salt,

Water,

Sugar,

Sodium

Nitrite

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# SPAM<sup>®</sup>

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

How well does it work?

Quite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Sugges

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

# WiscMail is GROSS

- On January 21, WiscMail implemented GROSS
- We saw an 86% reduction in spam from all on-campus spam

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

**Hormel**  
Foods

Serving  
Suggest

# Mailfromd rescues CAE <sup>®</sup>

- On March 27, I turned on mailfromd
- We saw a 90% reduction in spam

Ingredients:  
Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET  
**SPAM**  
STUFF  
SEE BACK FOR DETAILS

**Hormel**  
Foods

Serving  
Sugges

# Mailfromd rescues CS

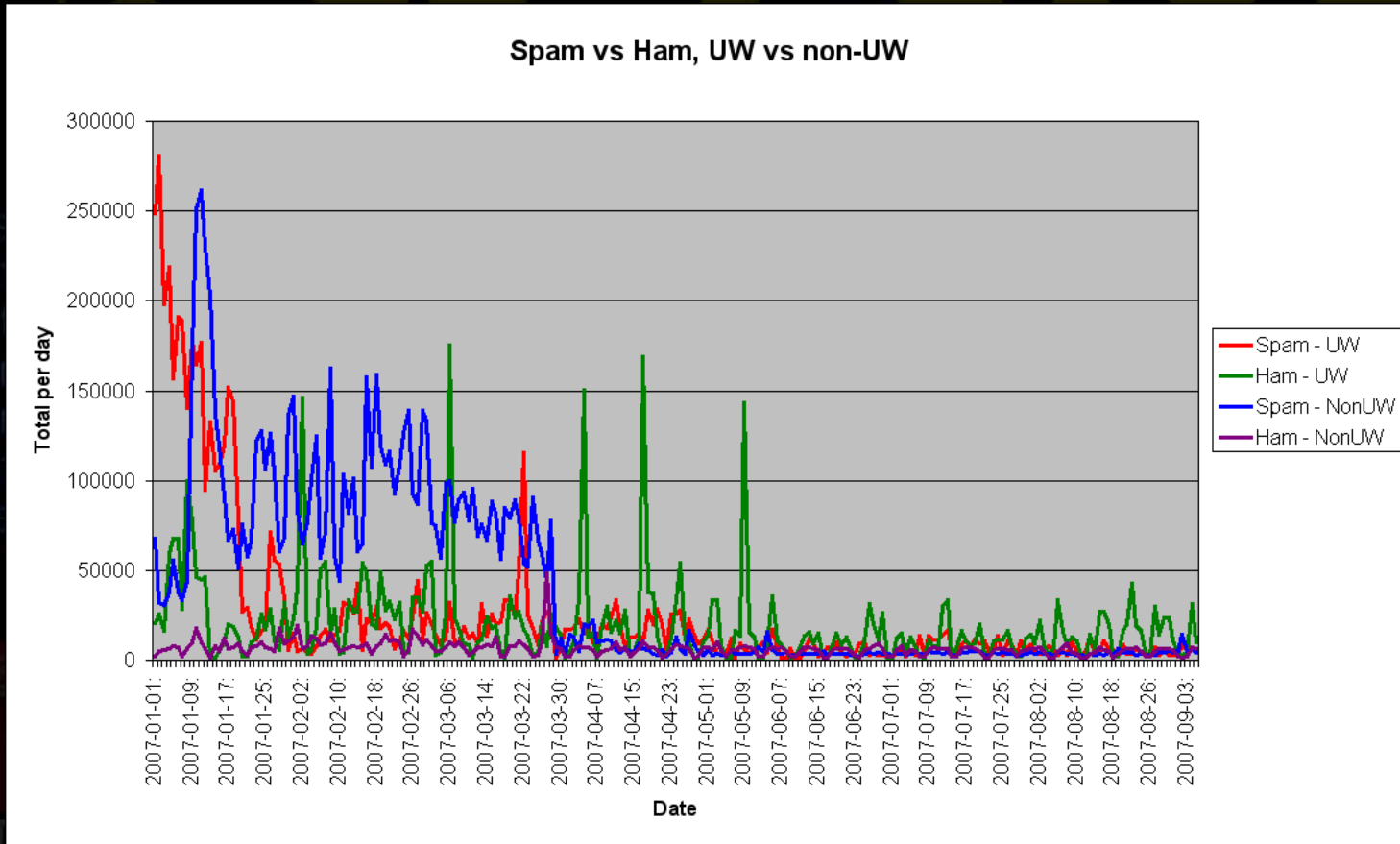
- On July 30, I turned on mailfromd
- We saw a 90+% reduction in spam
- Many compliments
- 2 complaints:
  - 1 about delays
  - 1 about missing mail (remote server timeouts)

NET WT.  
12 OZ.  
(340g)



Serving  
Sugges

# CAE Ham vs. Spam!



Ingredients  
Pork with  
Ham, Salt  
Water  
Sugar  
Sodium  
Nitrite

NET WT.  
12 OZ.  
(340g)

INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE



Serving  
Suggest

# CAE: Spamd results

- % Drop of Spamassassin bands:
  - Below 0: down 26% (summer)
  - 0-5: down 49%
  - 5-10: down 76%
  - 10-15 down 87%
  - 15+: down 97%

Ingredients:

Pork with  
Ham, Salt,

Water,  
Sugar,

Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

**Hormel**  
Foods

Serving  
Sugges

# CS mailfromd stats: All Messages

SENT: 2997

REJECT: 10271

TMP REJECT: 229797

LOST INPUT: 112269



1 day, 1 server of 6

# CS mailfromd stats: temporary rejections

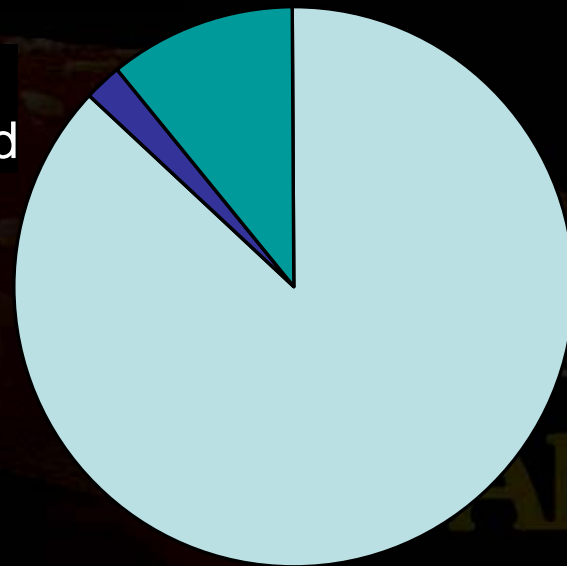
GREYLISTED: 195054

STILL GREYLISTED: 4687

RATE LIMITED: 24582

■ rate-limit

■ still greylisted



■ greylisted

1 day, 1 server of 6

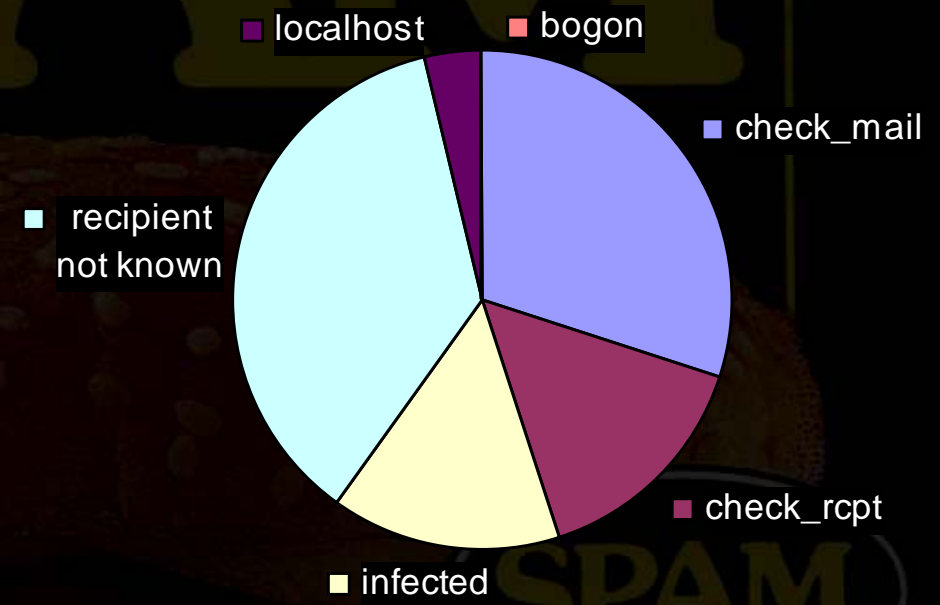
NET WT.  
12 OZ.  
(340g)



Serving Suggest

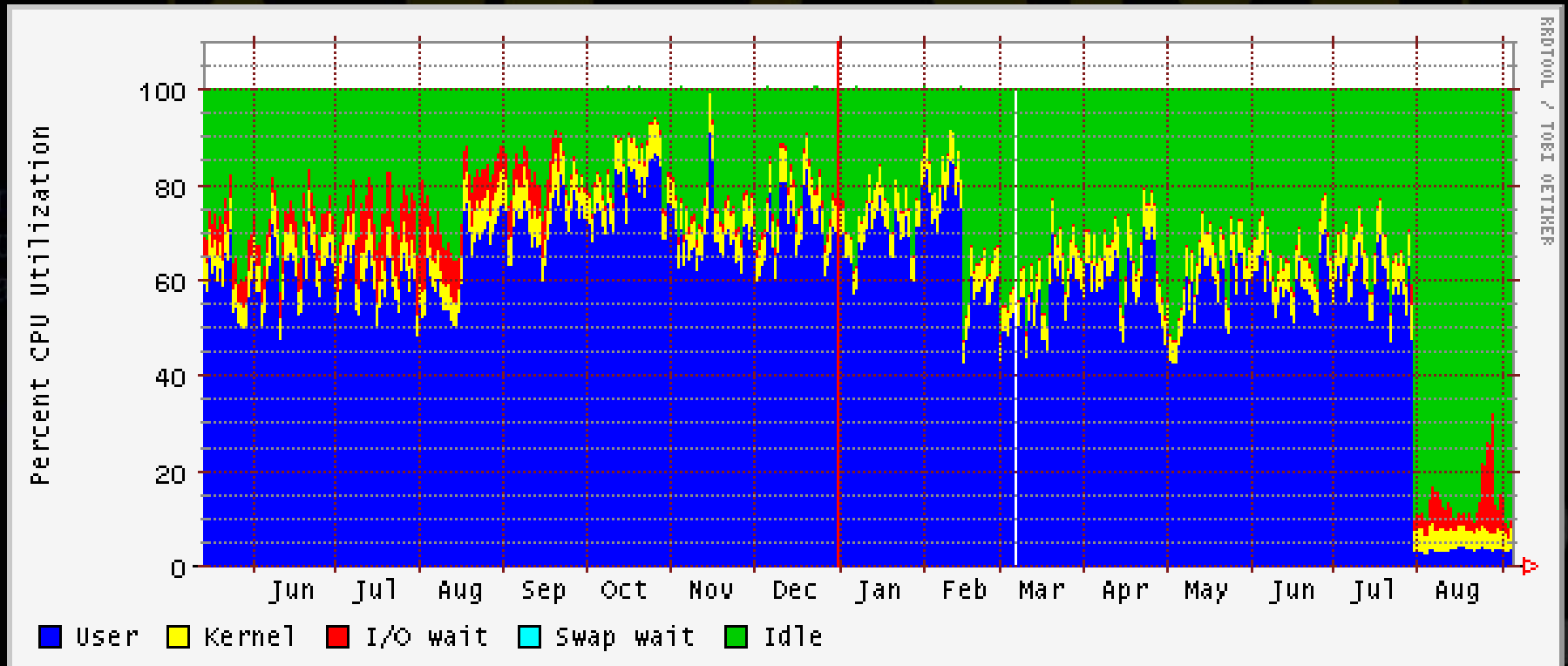
# CS mailfromd stats: rejections

Check\_mail: 3084  
Check\_rcpt (relaying): 1537  
Infected: 1510  
Recipient unknown: 3745  
Localhost: 380  
Bogon: 1



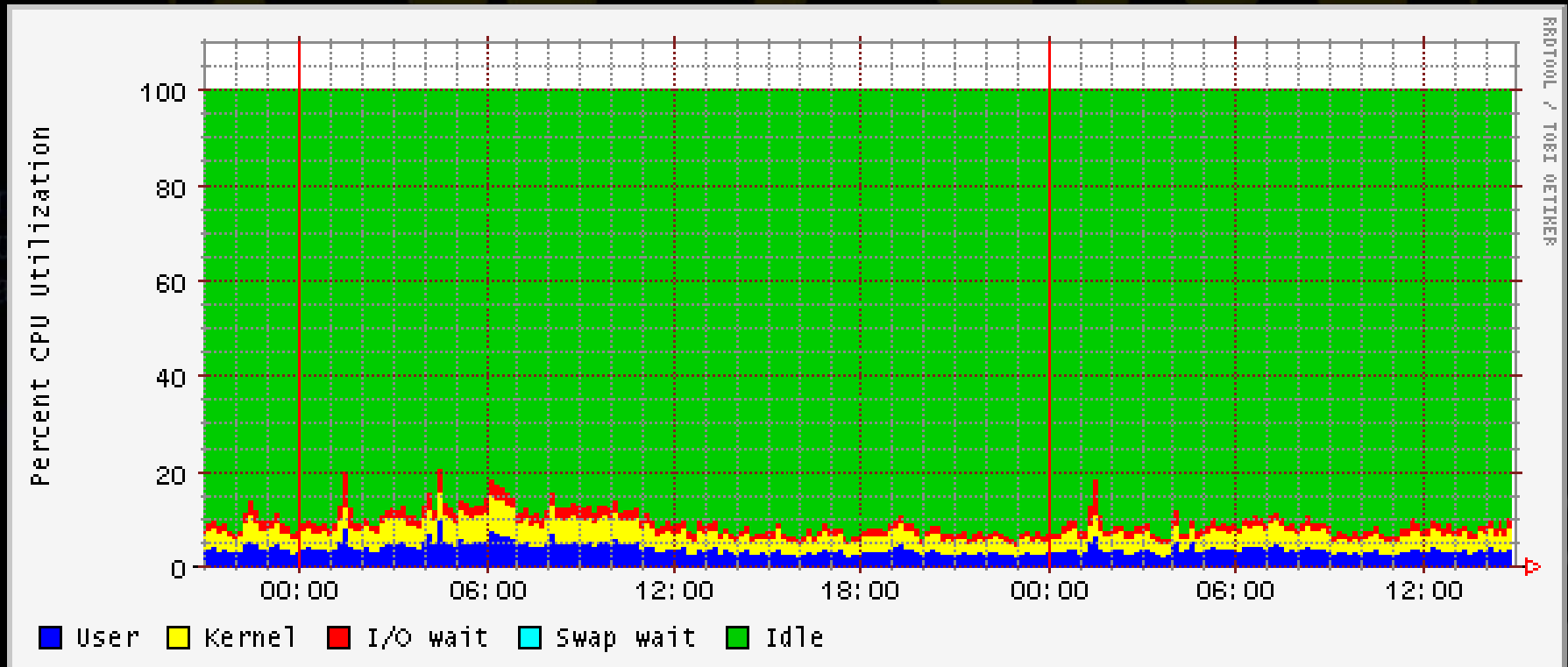
1 day, 1 server of 6

# Yearly CPU



- Pop quiz: identify when CS implemented mailfromd...

# Daily CPU

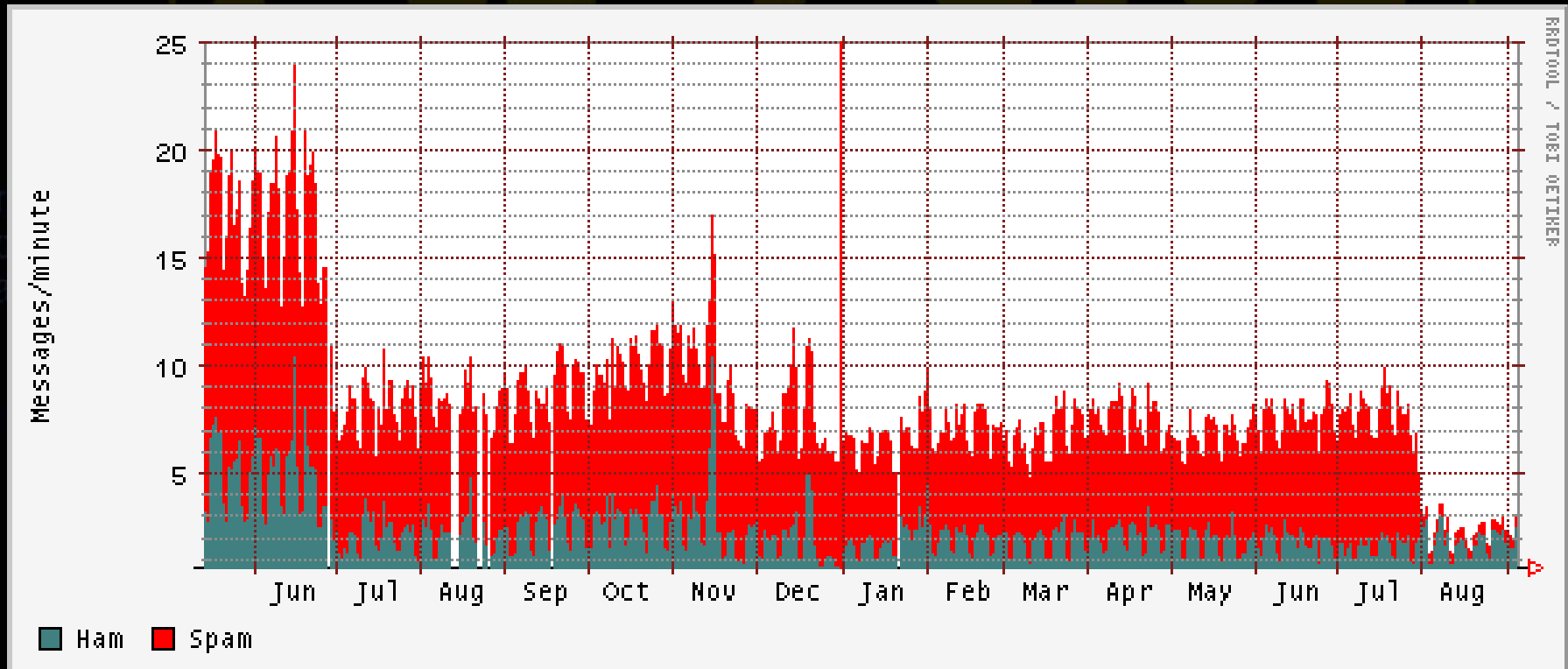


- As you can see, the CPU load graph looks much better these days...



Serving Suggest

# SPAM Year

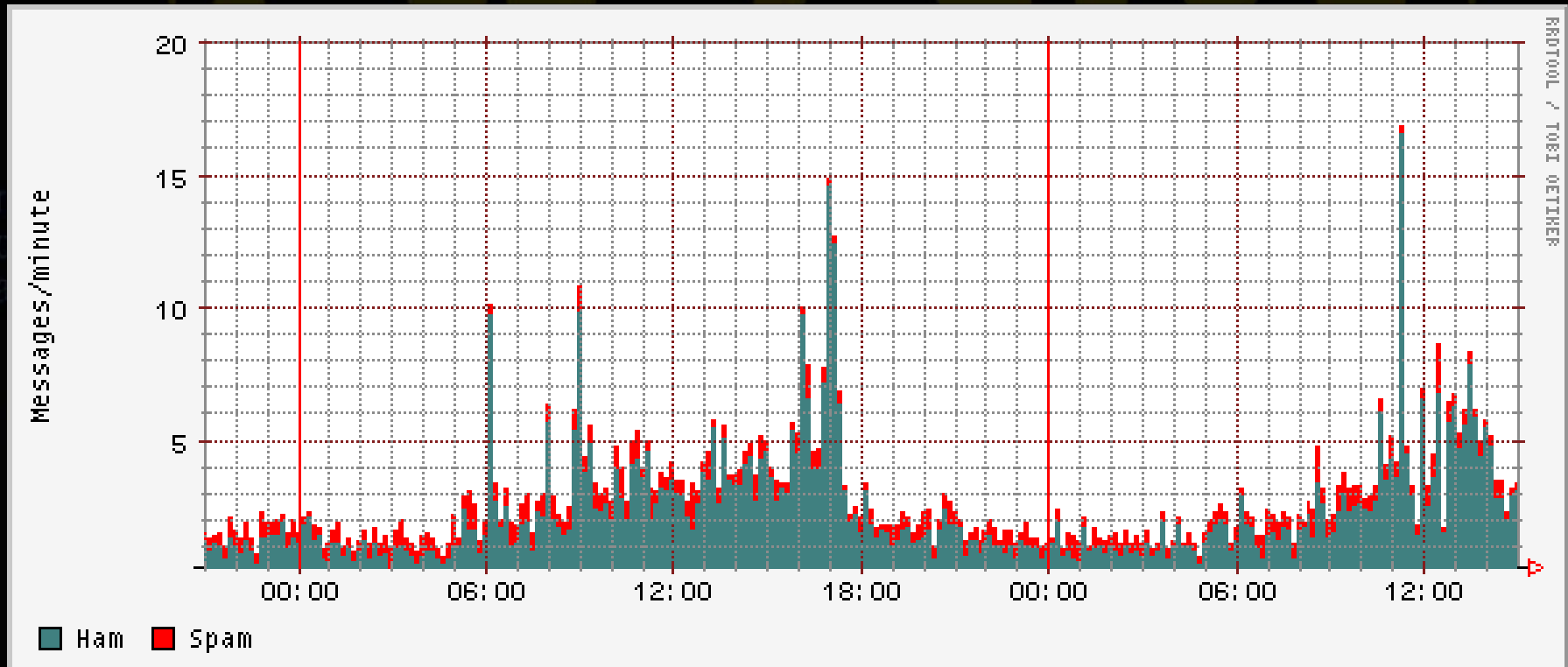


- HAM — unchanged, SPAM — not unchanged



Serving Suggest

# SPAM Day



- As you can see, at CS, SPAM is now constant through the day.



Serving Suggest

# What do the users say?

“I have not noticed any ill effects from your new policies except occasional delays of several minutes from on-line stores and such. Keep up the good work!

-Philip”

Ingredients:

Pork with  
Ham, Salt,  
Water,  
Sugar,  
Sodium  
Nitrite.

NET WT.  
12 OZ.  
(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET

SPAM

STUFF

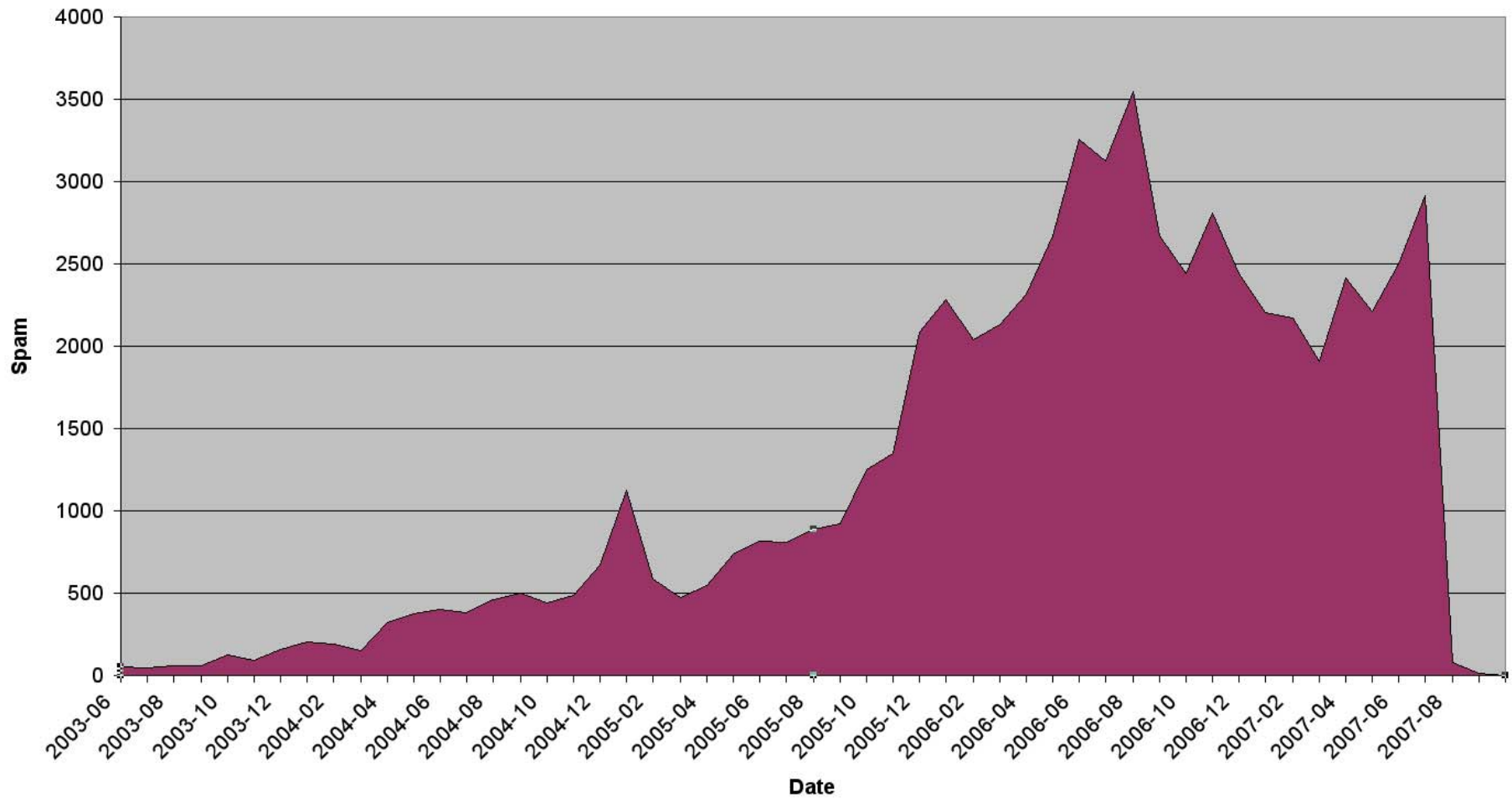
SEE BACK FOR DETAILS

Hormel  
Foods

Serving  
Suggest

# Philip's stats

Philip Wells



# A CAE Response

A faculty member inquired this morning about the significantly reduced level of spam he was receiving. He was at least somewhat concerned about false positives with the servers actually blocking some spam as opposed to just marking and delivering it. Do you have any more details yet on the changes that have been implemented? Thanks.

# Things to think about

- CS gives a demerit for all yahoo mail. Too aggressive? Maybe only non-us yahoo?
- Databases grow large – need to compact regularly

Ingredients:

Pork with

Ham, Salt,

Water,

Sugar,

Sodium

Nitrite.

NET WT.

12 OZ.

(340g)

U.S.  
INSPECTED  
AND PASSED BY  
DEPARTMENT OF  
AGRICULTURE

GET

SPAM

STUFF

SEE BACK FOR DETAILS

Hormel  
Foods

Serving  
Suggest