



# SPAM

Aidan McGrath BSc

IT Manager WIT

&

Martin Gibbons

IT Manager GMIT



# E-mail Statistics 2003

- 31 billion e-mails sent daily
- 56 daily e-mails sent per e-mail address
- 174 daily e-mails sent per person
- 34 daily e-mails sent per corporate address
- 10 daily e-mails received per person
- 3.1 e-mail addresses per person
- \$255 million cost to all internet users
- Source: Spam filter review -  
<http://www.spamfilterreview.com/spam-statistics.html>



# Spam Statistics 2003

- 40% of all e-mail considered spam
  - 12.4 billion spam mails sent daily
  - 6 daily spams received per person
  - 2,200 spam mails received annually
  - \$8.9 billion cost of spam to US corporations
  - 28% of users reply to spam
  - 8% of users purchase from spam
- 

# Types Of Spam


● Products	25%
● Financials	20%
● Adult	19%
● Scams	9%
● Health	7%
● Internet	7%
● Leisure	6%
● Spiritual	4%
● Other	3%

# WIT/GMIT Problems

- Users suffering from up to 70% spam
- Spam creates extra load on existing services, equipment and IT Staff
- Cost of processing spam based on 400 staff, avg. salary €36,800 receiving 5 spam per day and taking 3 seconds per mail = €7,500
- Increasing number of requests to change addresses due to spam



# Issues To Consider

- Any solution must not place an extra burden on IT staff, or affect current performance
  - One solution for all servers
  - Management must be at user level
  - Solution must work with web mail
  - Cost per seat licensing can be expensive
  - Support available
  - Implementation must not disrupt service
  - No client software required
  - No client training required
- 

# The Solution



● <http://www.copperfasten.com/>

## ● Hardware

- Intel 4 CPU 1.80GHz
- 1Gb RAM
- 80Gb Hard Drive

## ● OS

- Free BSD 5.2



# The Solution – Applications

- Spam Assassin 2.64
- Amavisd-new 2.1.1
- Postfix 2.1.4
- ClamAV 0.75
- Apache 2.0.50
- MySQL 4.0.21
- PHP 4.3.8
- Also Dee 1.2.48, Razor 2.61, Pyzor 0.4.0 and Perl 5.8.5




# How it works

- Mail is delivered to Copperfasten box
- Heuristic tests carried out on mail
- If mail scores high as either a virus or spam mail, then it is quarantined
- User gets a message that there is quarantined mail
- User checks quarantined mail



# End User Management

- End users manage their own quarantines
  - Can release false positives and can manage their own blacklist / white list
  - Can determine how often to receive quarantine reports
- 

# Spam Quarantine User Report

Mail From: GMT Spam Appliance <ithelpdesk@gmit.ie>


File Edit View Actions Tools Window Help

From: GMT Spam Appliance <ithelpdesk@gmit.ie> CC: [Redacted]

To: martin.gibbons <martin.gibbons@gmit.ie>

Subject: Spam Quarantine Report

Message:



## Spam Quarantine Report

This email contains a list of all messages which have been quarantined as potential spam and/or virus infected messages before they reached your Inbox.

- Click on the **Deliver** link to have a message delivered to your inbox. Messages that contain viruses will be stripped of any attachments before being delivered to avoid any damage to your system.
- Click on the **Whitelist** link to have a message delivered to your inbox and whitelist the sender so that subsequent messages from that sender will no longer be quarantined.
- Click the **Delete** link to have the message delete from your quarantine.
- To delete all of the messages, click the **Delete All Messages** link at the bottom of the Spam Quarantine Report.
- Messages will automatically be deleted from the quarantine after 7 day(s).

If you have questions regarding this report, please contact [ithelpdesk@gmit.ie](mailto:ithelpdesk@gmit.ie)

### Virus Messages (2)

Virus	From	Subject	Date	Actions
Worm.SomeFool.Gen-2	alsdream@estsoft.com	information	Fri 22/10 5:22	[ <a href="#">Delete</a> ]
Worm.SomeFool.Gen-2	chrishumphreyuk@hotmail.com	unknown	Tue 26/10 4:42	[ <a href="#">Delete</a> ]

### Spam Messages (11)

Score	From	Subject	Date	Actions
6.1	etv-announcements@cedefop.eu.int	Major European survey on quality...	Wed 20/10 16:22	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
6.7	bounce-tribune-82291259@lists.sit...	SitePoint Tribune #305 - Boost O...	Thu 21/10 21:28	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
9	ptjtt@swankin-turner.com	Bradford New Breed ARMM Equity A...	Sun 24/10 20:27	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
18.8	antoino_pineda_pv@e-logic.nl	Italian Crafted Rolex from \$75 t...	Sat 23/10 18:29	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
20.4	susanaramsey_ic@apcei.com.ph	Order Rolex or other Swiss watch...	Mon 25/10 13:19	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
24.6	jbenson_gv@co.voz.ru	Wouldn't you like to know your c...	Mon 25/10 3:41	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
24.9	eddiancencnk@vjr.lt	Italian Crafted Rolex from \$75 t...	Thu 21/10 21:22	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
25.9	sbountju@msap.com.au	Italian Crafted Rolex from \$75 t...	Fri 22/10 20:16	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
26.5	oflowersun@segerstedtsgymnasium.nu	Order Rolex or other Swiss watch...	Sun 24/10 17:19	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
36.8	gbwalsh_wm@forklift.ru	Get Prescription Drugs to your...	Wed 20/10 23:37	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]
43.5	daebji@mail.com	50,000 VISAS TO THE USA! Get it ...	Sat 23/10 19:51	[ <a href="#">Deliver</a>   <a href="#">Whitelist</a>   <a href="#">Delete</a> ]

[ [Delete All Messages](#) ]

Deliver this report even: [day](#) | [weekday](#) | [Friday](#) | [month](#) | [never](#)

Include the following items in the report: [All quarantined items](#) | [New items since last report only](#)


To view your entire quarantine inbox or manage your preferences, [Click Here](#)

Spam/Virus Protection by Copperfasten Technologies

Date: 27 October 2004 7:05



# Administrative Management

- Set-up appliance, add/delete domains
  - Global blocking of extension types
  - View graphical statistics
- 

# Administrator Web Page

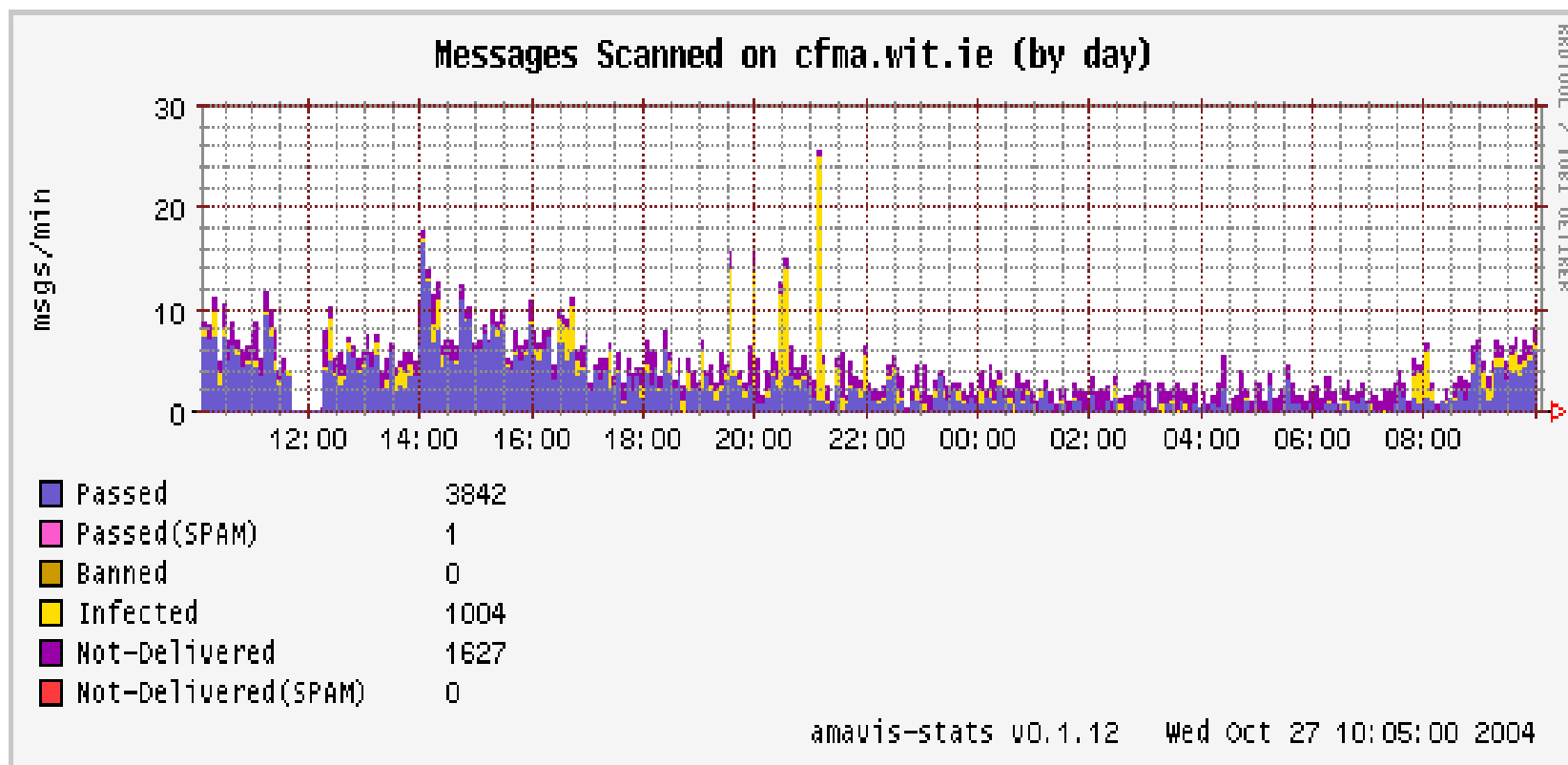
The screenshot shows a Microsoft Internet Explorer browser window displaying the Copperfasten Mail Firewall Appliance administrator interface. The browser's address bar shows the URL `http://gwmailfilter/home.php`. The page title is "Copperfasten - Mail Firewall Appliance".

The interface features a navigation menu on the left with the following items: Home, System Setup, Content Filtering, Anti-Spam Engine, Reporting, Quarantine, Settings, Filter Rules, Log Files, Online Help, and Logout. The main content area is titled "Home" and contains the following sections:

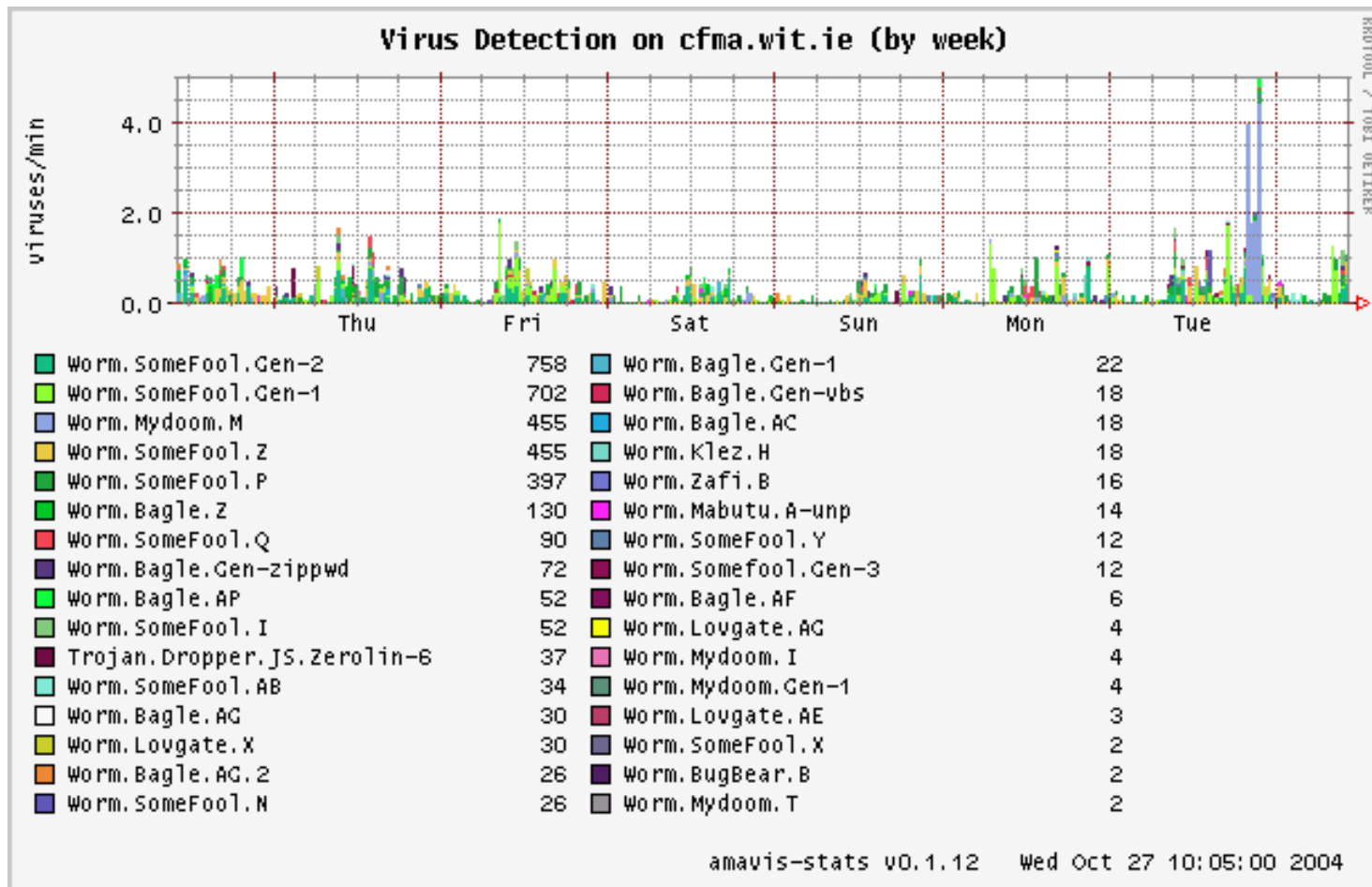
- Home**: Return to Mainmenu
- System Setup**: Configure the Mail Firewall Appliance
- Content Filtering**: Manage content filtering settings
- Anti-Spam Engine**: Manage settings and global/user policies for the Anti-Spam Engine
- Reporting**: Shows the number of emails received and statistics on the number of spam messages and virus messages that were identified.
- Quarantine**: Manage quarantined messages
- Settings**: Manage basic settings
- Filter Rules**: Configure White/Blacklists
- Log Files**: View or download Log Files
- Online Help**: Online help
- Logout**: Logout

The page also displays the date and time: "Wed, Oct 27 2004 14:13:30". At the bottom left, it shows "Release 2.05 © Copperfasten 2004". The bottom right of the browser window shows the status bar with "Local intranet".

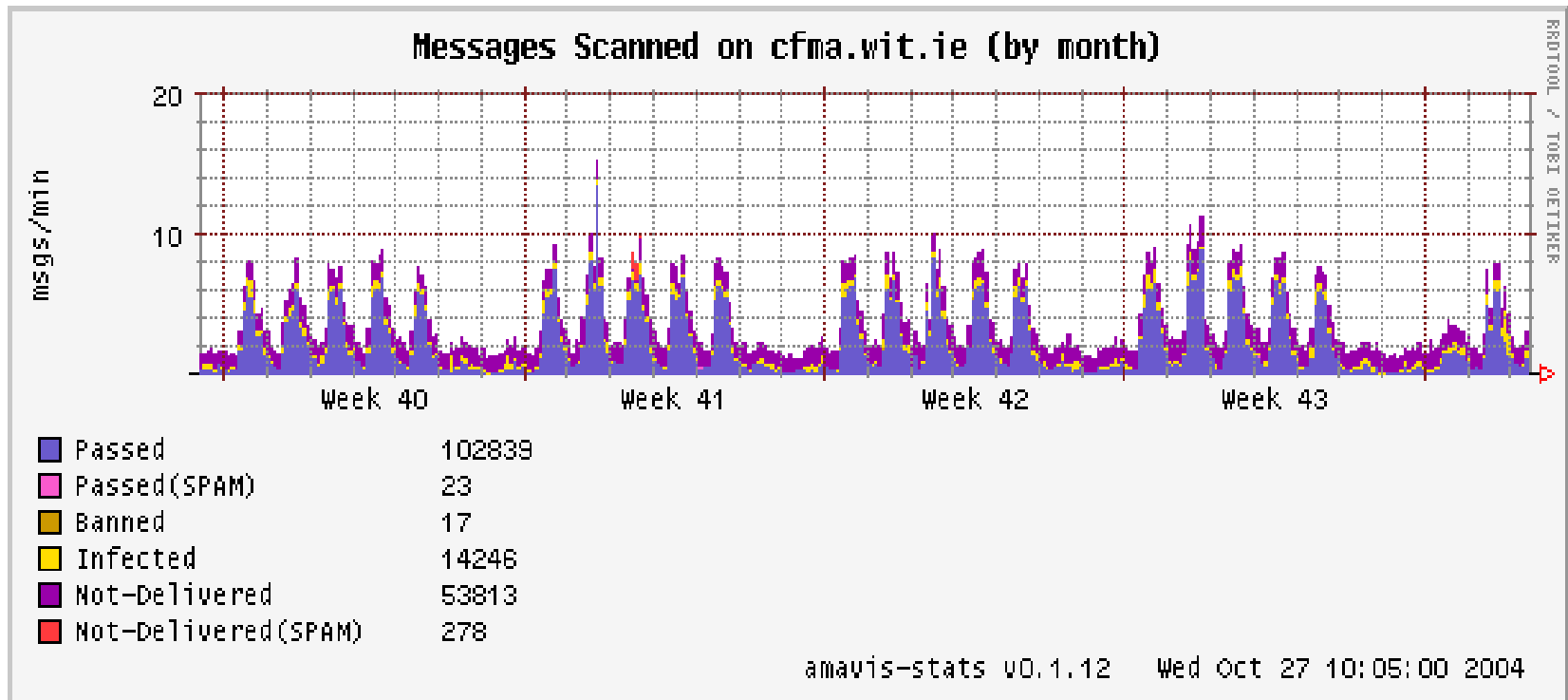
# Daily Mail Stats



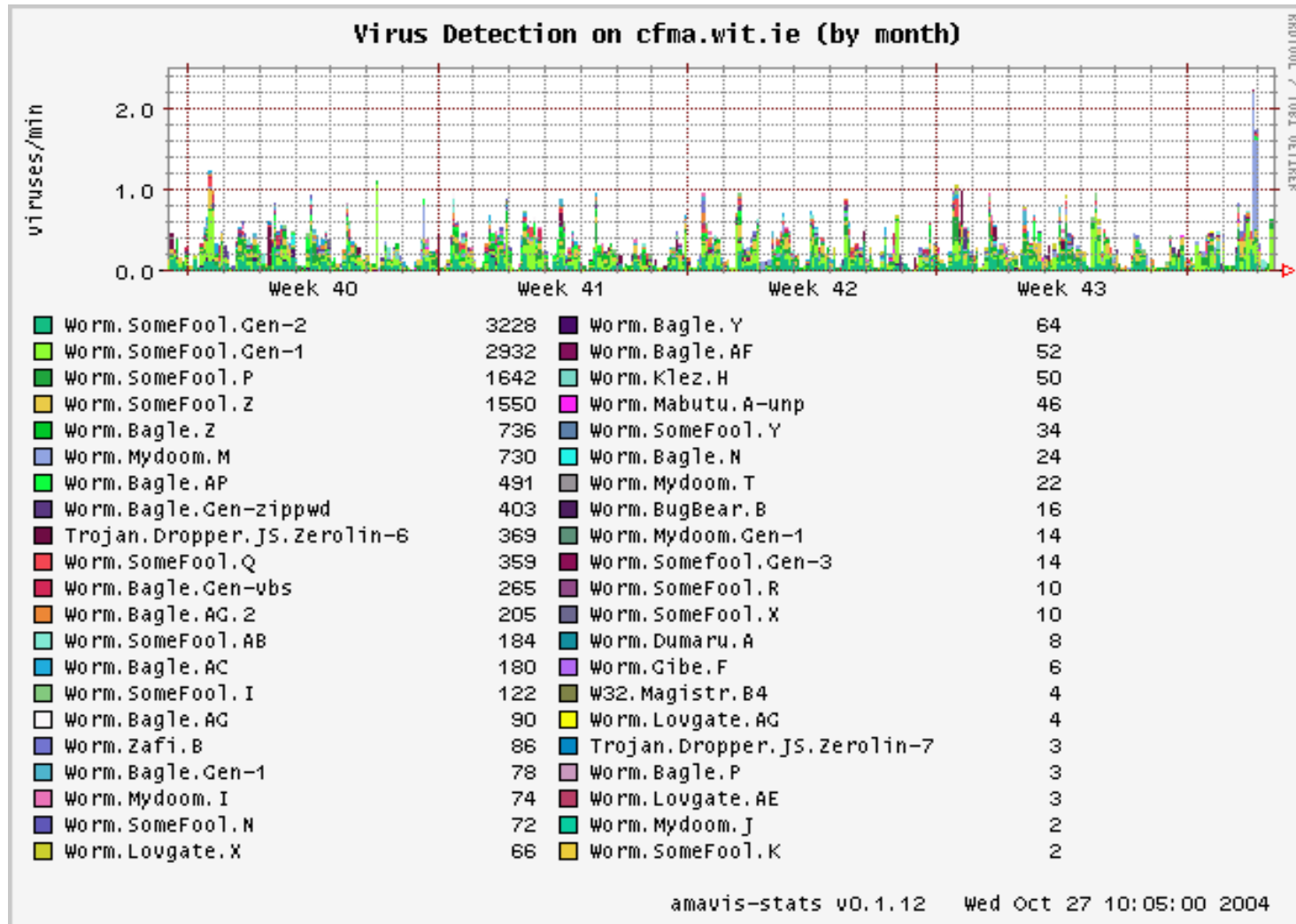
# Daily Virus Stats



# Monthly Spam Stats



# Monthly Virus Stats





Questions?

