“System Maintenance: Please verify your details”

Or “bloody scammers, they’re at it again”

“System Maintenance: Please verify your details”

From: J.Bloggs@some-uni.ac.uk
Reply-to: dodgy@bigfreemailer.com
Date: Thu, 28 May 2009 09:00:00 +0100
Subject: SOME-UNI.AC.UK WEBMAIL MAINTENANCE

Dear E-mail User,

To complete your Account Verification process, you are to reply this message and enter your Username and Password respectively in the space provided below this email.You are required to do this before the next 48hrs of receipt of this e-mail, or your mail Account will be de-activated and erased from our Database. Your account can also be verified at:

https://student.some-uni.ac.uk/webmail/

Enter Username ( )
Enter Password ( )

Thank you for using SOME-UNI.AC.UK WEBMAIL

Today’s session

- Evolution of spam
- Defences
- Our new approach to spear phishing

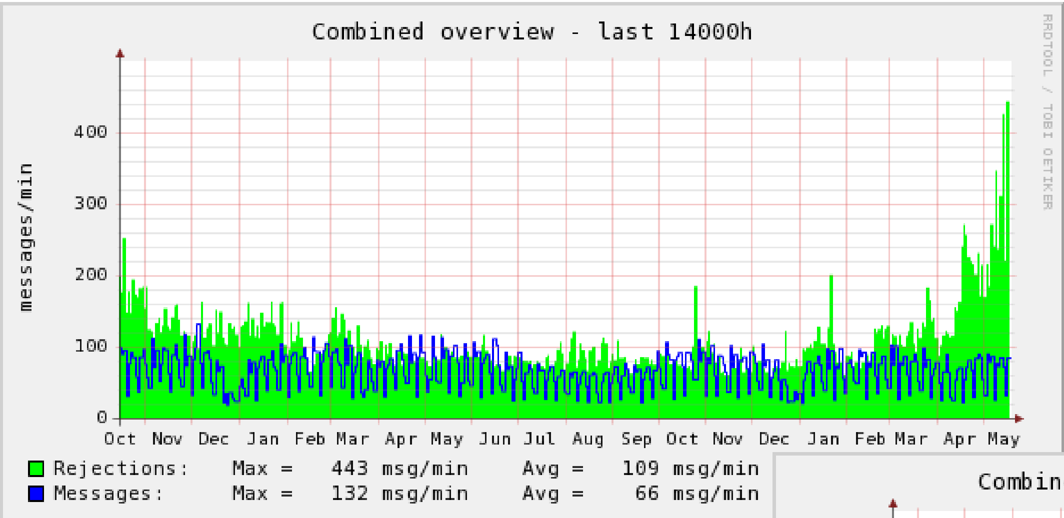
Evolution of spam

- Originally no more than an irritation

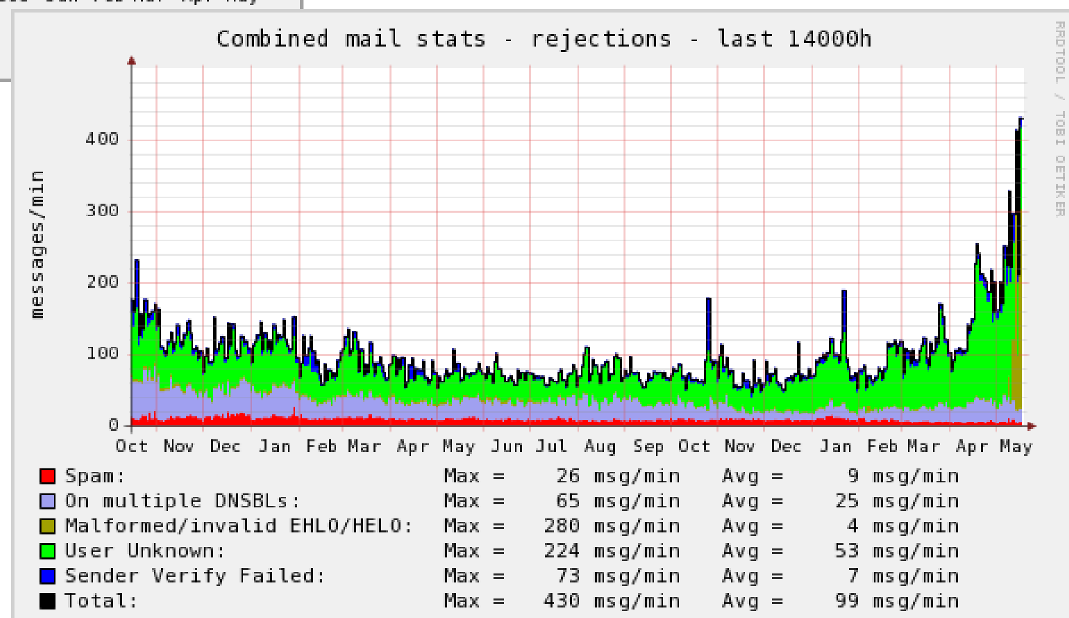
- Marketing, sales – relatively innocuous

- Developed over the years
  - advance fee fraud, lottery scams etc
  - still money-related in the main
- Now much more sinister

Volume



- Huge volume



- Huge numbers of machines

Defence in depth

- Filtering as messages arrive
  - Network level
  - Protocol level
  - DNSBLs
  - IP, Netblock, AS Reputation checks
  - Signatures (DCC Servers for example)
  - Anti Virus
  - Content scanning
  - Heuristics
  - ...
  - What's next? (Not the FUSSP, that's for sure)
- How do we keep up?

A New Approach

- We can’t control the input properly...
- ...but (fanfare): we can control the output.
- ...we can then protect our systems and users
- Our solution is called Kochi:
  - http://oss.lboro.ac.uk/

Kochi – How it works

- Content scanning of “outbound” messages
  - “Outbound” == traversing our mail routing infrastructure
  - Message passed during SMTP transaction by MTA to a filter daemon (written in Perl)
    - Uses ClamAV’s daemon API
    - Already accessible to a large number of MTA applications
  - Simple pass/fail result, with details

How it works in more detail

- First search for key words (big, complex regex) such as
    - user, username, pass, password
- If keywords found (or skipped), tokenise email into candidate user/pass strings
    - Our defined password policy gives us a regex:

```
## Regular expression matching valid passwords
      my $regex = qr{
         (?: (?=\S*?[a-z])(?=\S*?[A-Z])(?=\S*?[0-9])
           | (?=\S*?[a-z])(?=\S*?[A-Z])(?=\S*?[^a-zA-Z0-9\s])
           | (?=\S*?[A-Z])(?=\S*?[0-9])(?=\S*?[^a-zA-Z0-9\s])
         )[-0-9a-zA-Z_=\+\!"\$\%^\&\*\(\)\[\]\{\}\\;:\'\@#~\/\?\.,<>\|\`]{6,}
      }x;
```

    - Likewise for usernames (big regex!)

Token Pair Authentication

- Can hook into all manner of authentication schemes (did I say it’s written in Perl?)
- If PAM available
  - combine auth schemes
  - check multiple auth backends
  - “abstract” methodology tailored to platform
- Pass/Fail is cached to limit impact on auth backend
- If authentication succeeds...

Acting on detection results

- ...your choice of action
- Don’t bounce or reject the message!
- We discard the message and generate an autoreply in a standard format:

```
Your message with subject "$h_Subject:", contained a valid Loughborough
University username and password.

The message has not been sent.

Usernames and passwords must never be disclosed by e-mail.

If you feel you have received this message in error, please forward this
message to it.services@lboro.ac.uk

--
IT Services <it.services@lboro.ac.uk>
```

Side effects - good

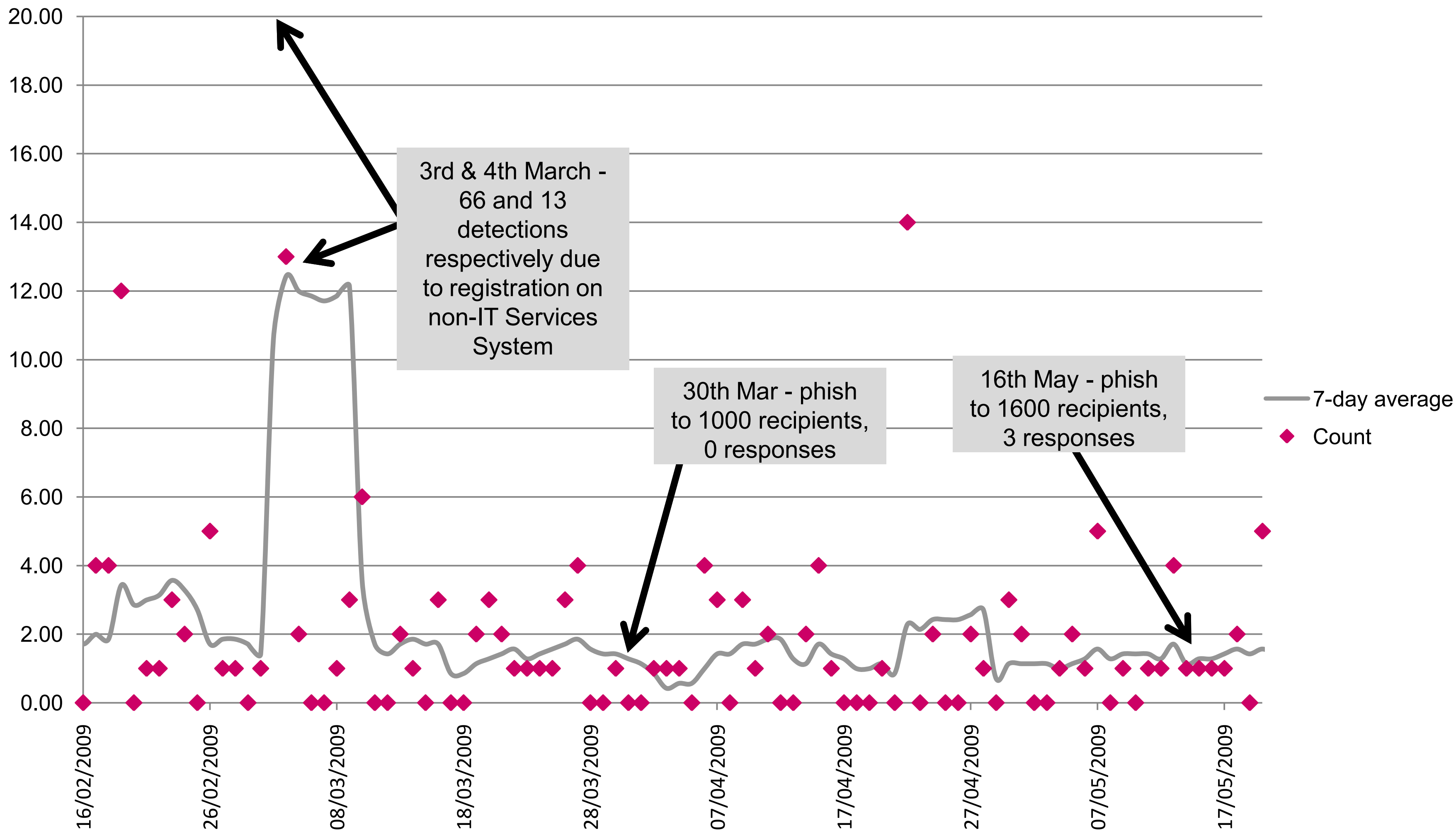
- Not only stops phishing
- Enforces local policy
  - Acceptable Use
  - Security
  - Good IT practice

- ...some users try to brute-force around it!

Side effects - bad

- Difficult to utilise in systems with lockout after repeated failures
  - Accounts **will** be locked!
  - ...can use abstraction in certain systems
  - Windows Server 2008 AD has “fine grained” password security policies but can still be a problem
- Makes it near impossible to send passwords for “user registered” services

Some statistics



Summary

- Spam, phishing very difficult to stop
- Concentrate where possible on detection of responses
- Kochi can help!

  - http://oss.lboro.ac.uk/kochi1.html

- Graeme Fowler, G.E.Fowler@lboro.ac.uk