Nathan Turajski
Jamz Yaneza

Best Practices for Evaluating Anti-spam Solutions

VB 2005, Dublin, Ireland

Benchmarking Validation

- Methodologies
  - Accurate
  - Comprehensive
  - Fair

- Filtering Techniques
  - Pattern matching, Heuristics, IP blocking, Whitelist/Blacklist, Challenge/Response, Community …..

Anti-spam Solutions

- Current Solutions
  - Software
  - Appliance
  - Services
  - Legislation

- Methods
  - Catch rate (effectiveness)
  - Error rate (accuracy)

Content Defined

- Spam
  - UCE, commercial bulk mail
  - Consumers: well defined
  - Enterprise: borderline
- Non-spam
  - Appropriate, predictable, traceable
- Graymail
  - Inappropriate to environment
  - Requires exception capability

Factors for Evaluating Solutions

- Primary
  - Effectiveness
  - Accuracy
  - Resiliency
- Secondary
  - Administration
  - Integration

Testing Failures

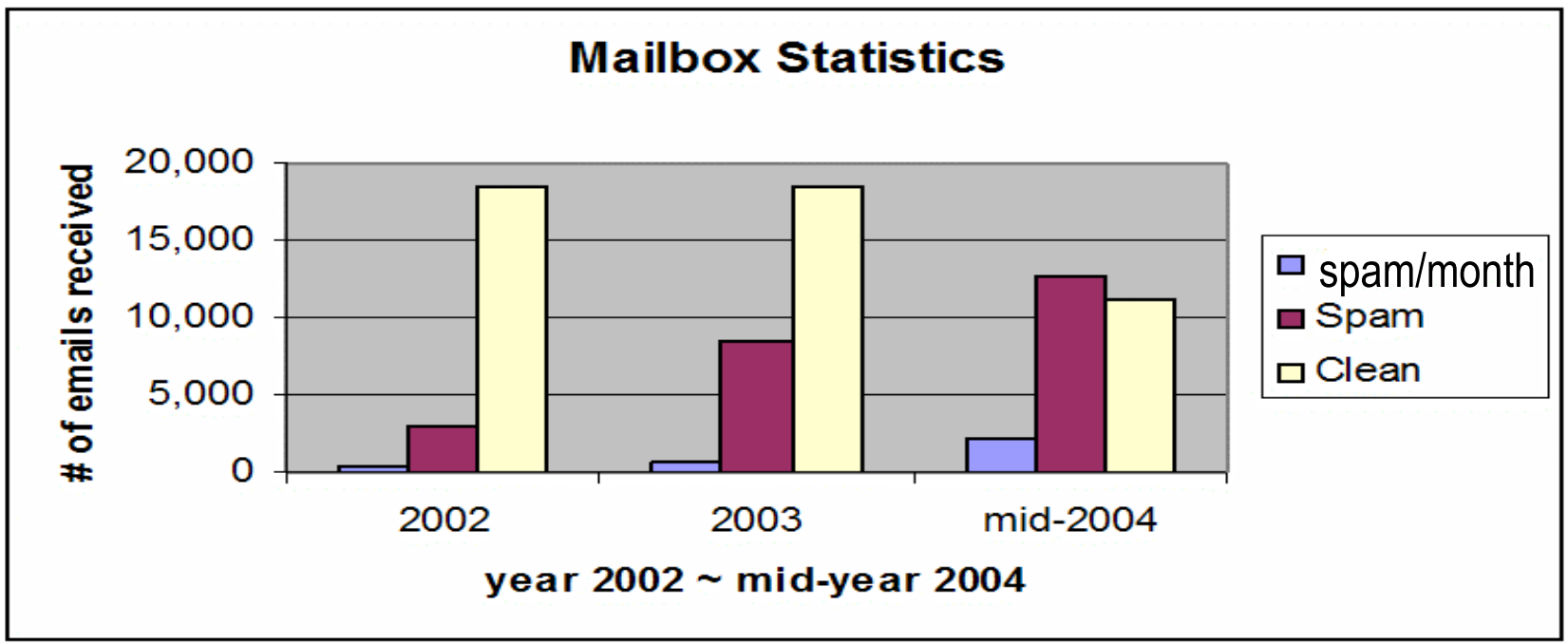
- Confused spam type classification
- Non real-world environment
- Short-term testing cycle
- Fixed regional origins
- Fixed language type
- Non-relative industry
- …. Etc.

Spam Trends

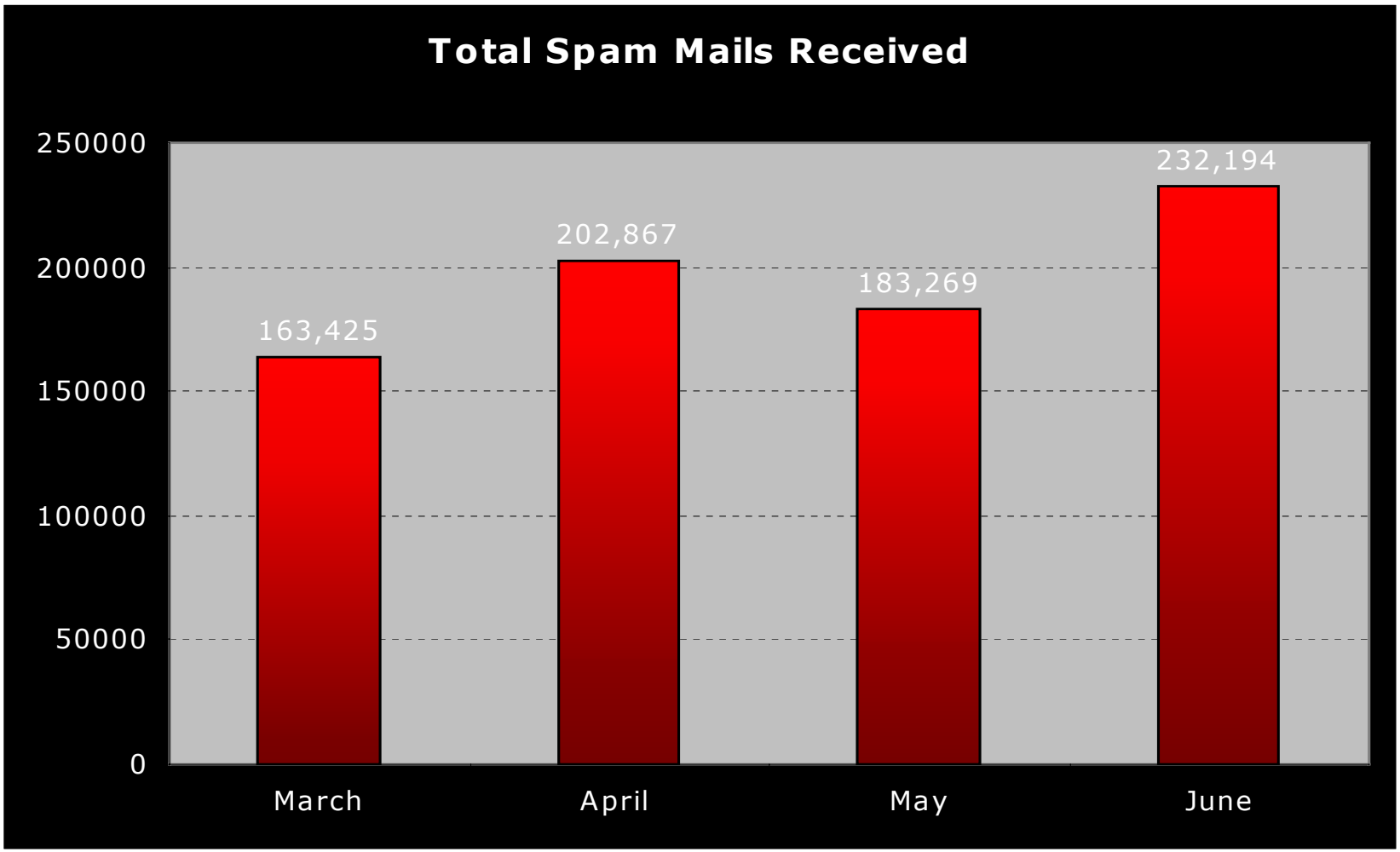
- Estimates vary, but the total amount was usually agreed to have passed 40% by the beginning of 2002
- Email was 50% SPAM by January of 2003
- 65% of all email was SPAM by 2004
- Almost 80% of all email is currently either unwanted advertising or virus-ridden

Evaluation Guidelines

- Valid vs. illegitimate mail
  - sampling over time period

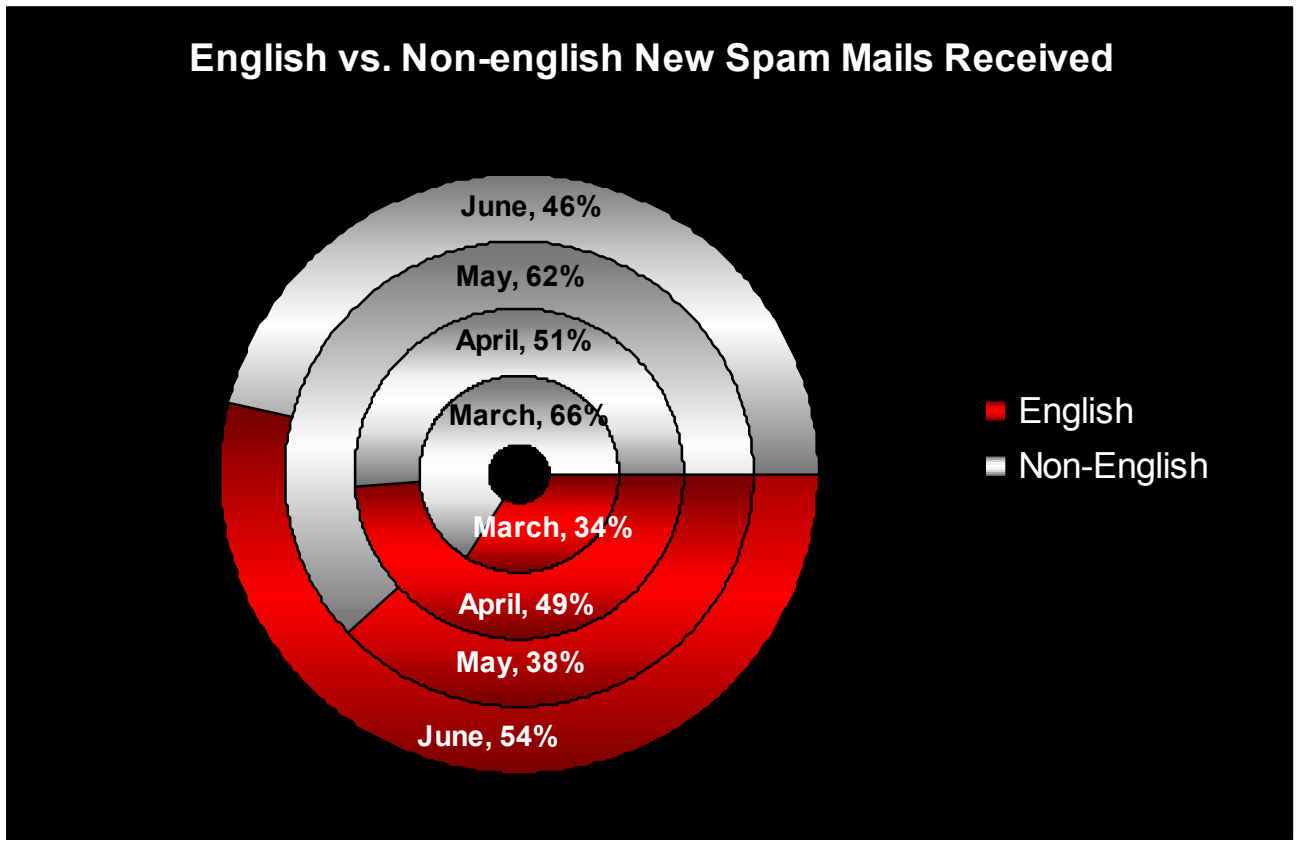


30% Monthly Spam Growth (2005)

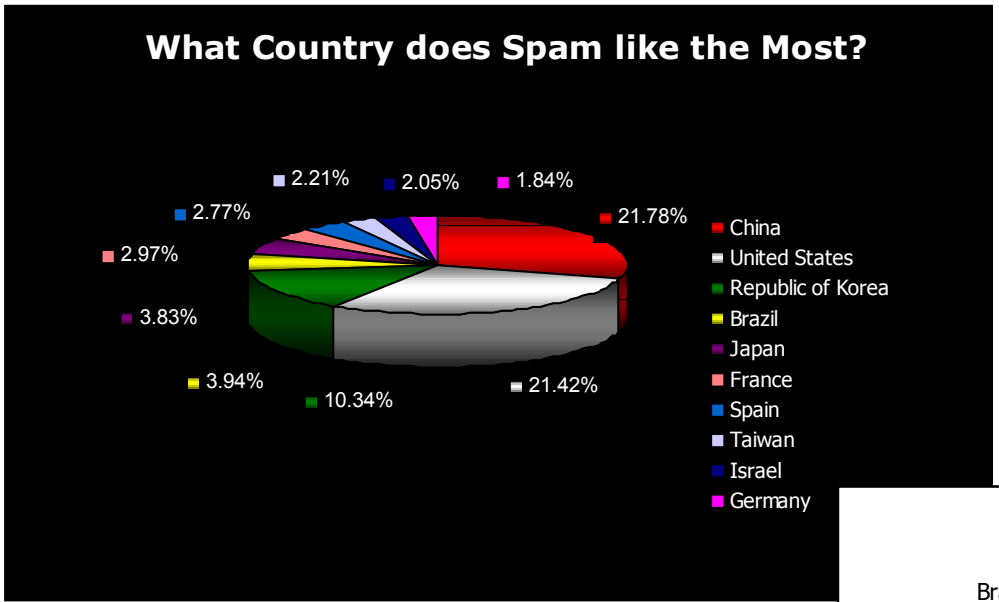


Evaluation Guidelines

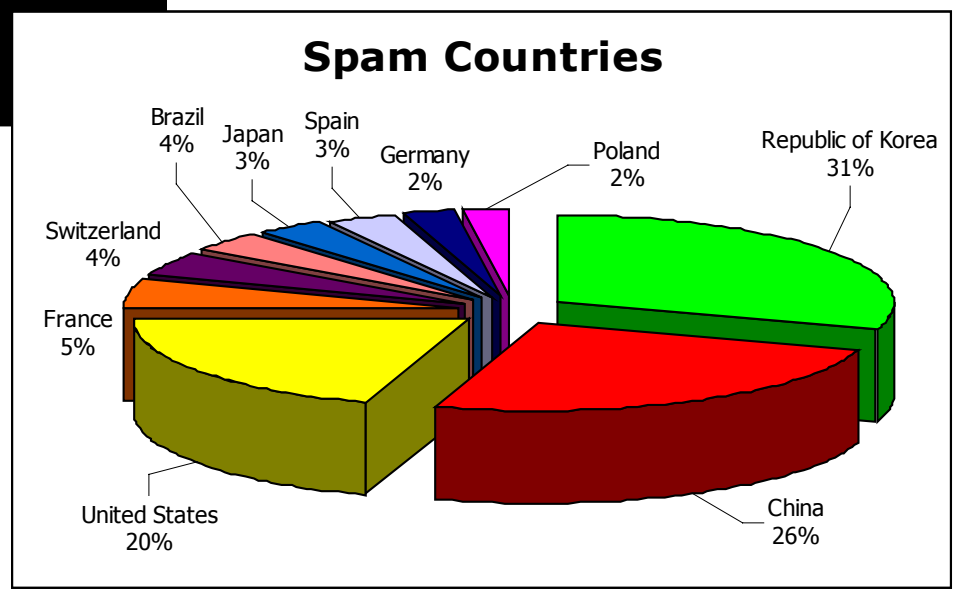
- Predominant language



Evaluation Guidelines



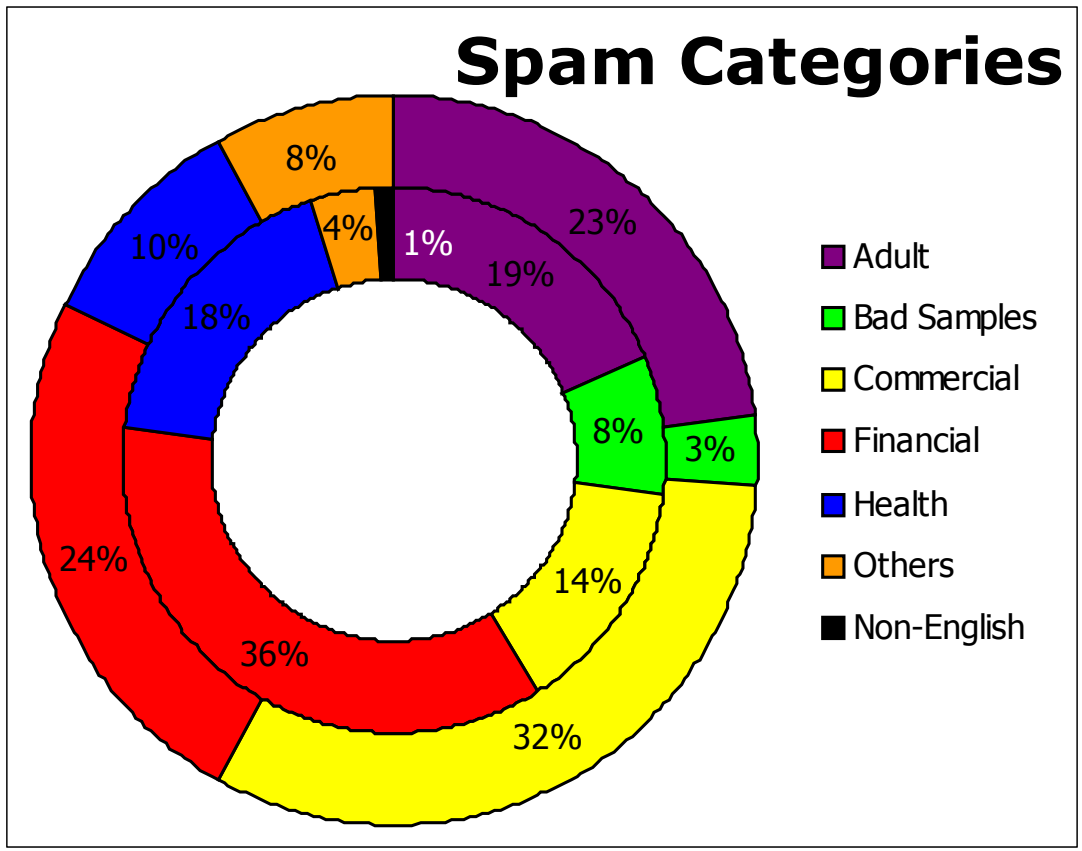
- Point of origin
  - broad mixed sampling



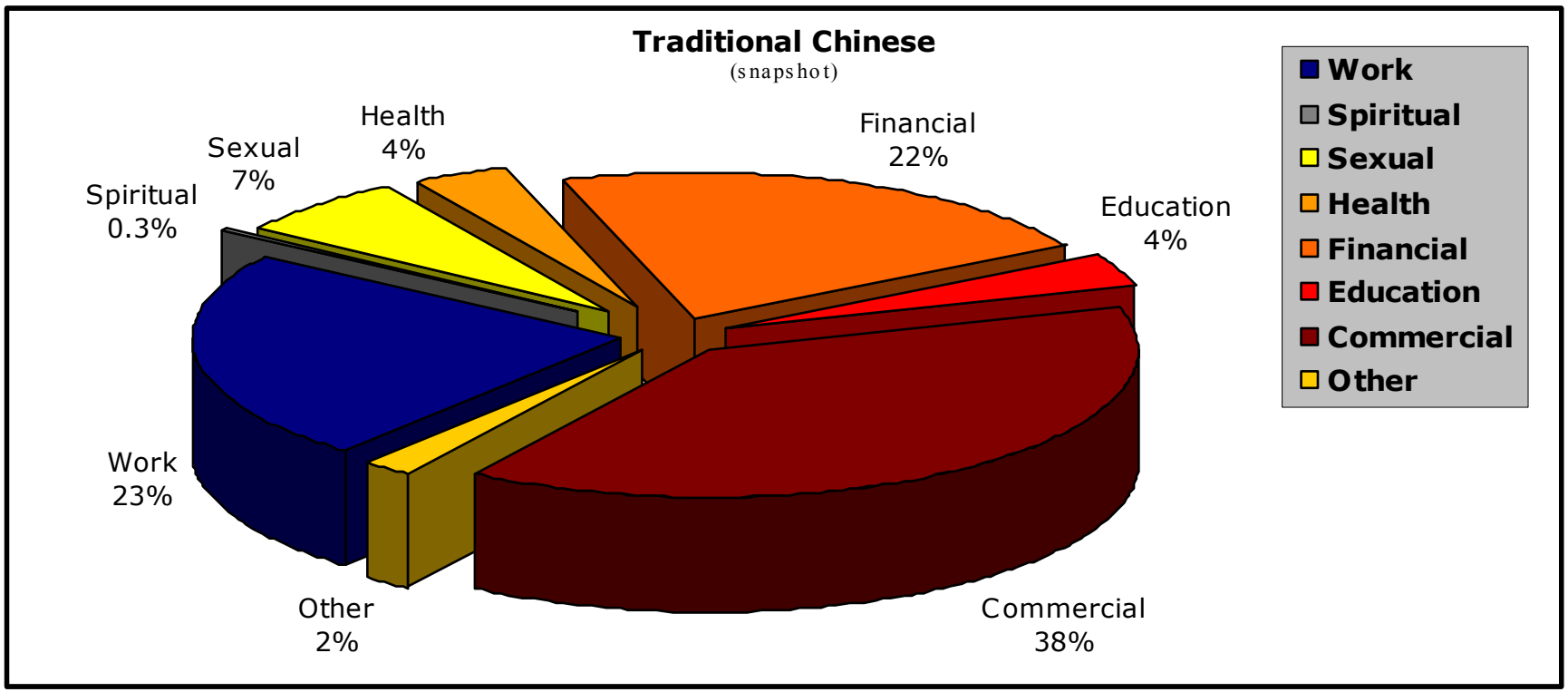
http://www.trendmicro.com/spam-map/default.asp

Evaluation Guidelines

- Industry definitions
  - overlap of needs vs. excess

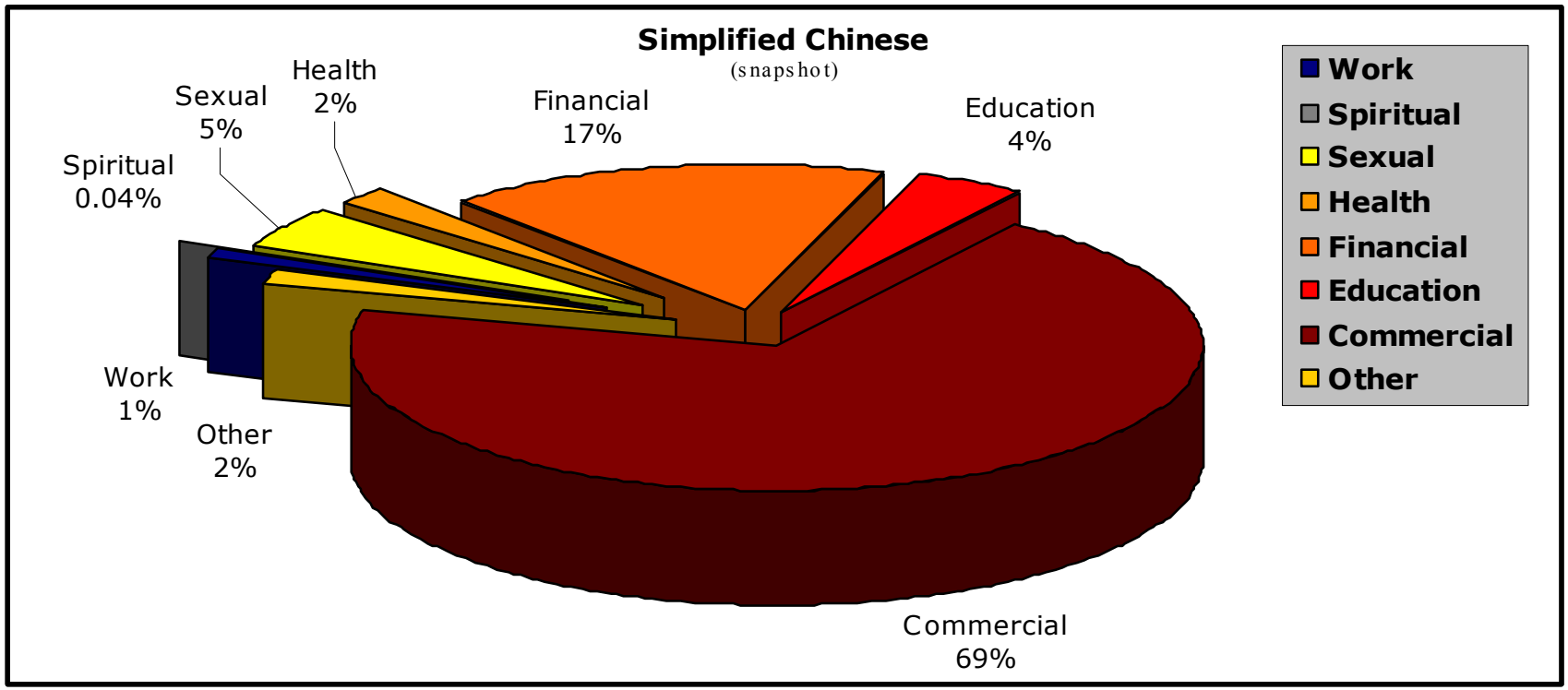


Chinese Language (traditional)



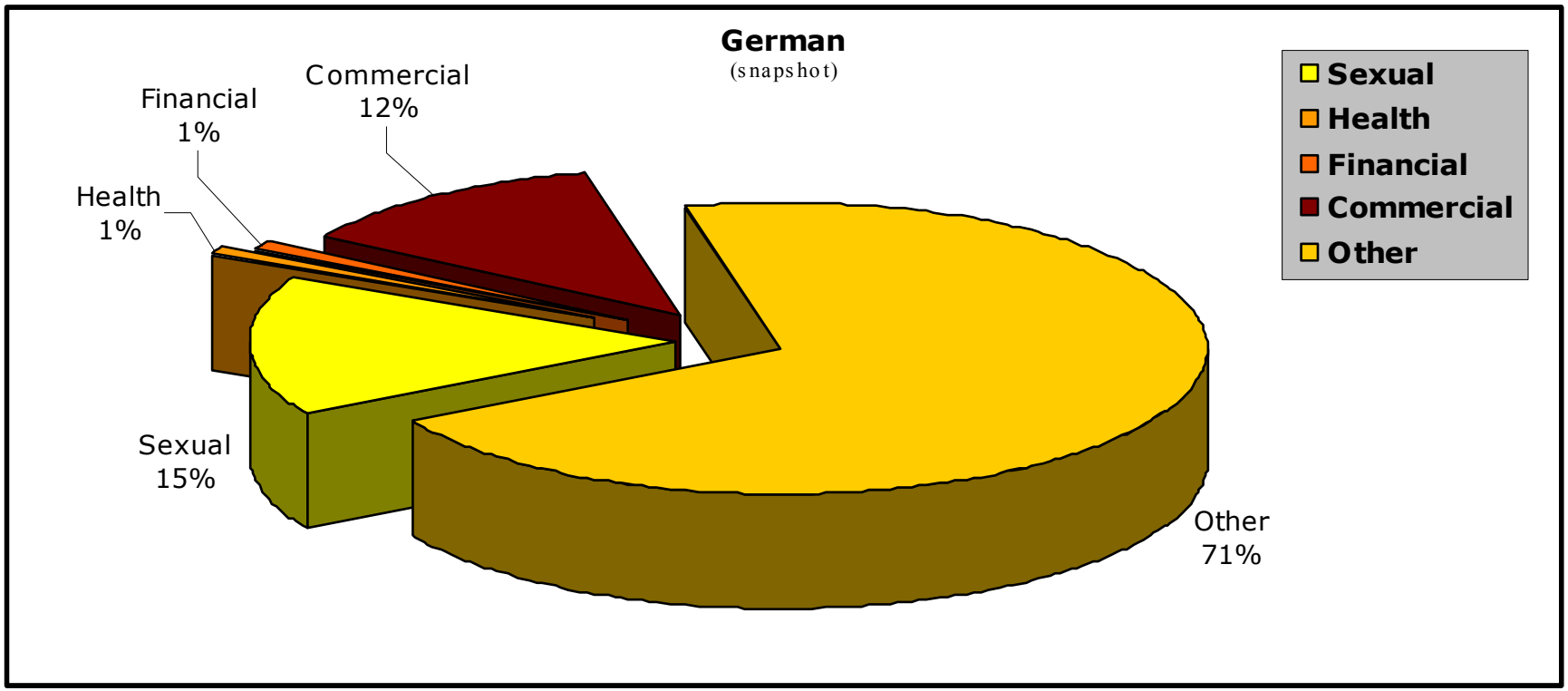
- Summary:
  - 38% commercial offers, 23% work related, 22% financial, 7% sex related

Chinese Language (simplified)



- Summary:
  - 69% commercial offers, 17% financial, 7% sex related, 4% education

German Language



- Summary:
  - 15% sex related, 12% commercial, 71% mixed offers

Evaluation Guidelines

- Timeliness
  - update frequency
  - distribution strain on network/system
  - correction efficiency

Evaluation Guidelines

- Summary
  - Efficiency and accuracy dependent on spam classification and audience
  - Used testing samples to be valid and fixed
  - Overall results used for evaluation
  - False positive graymail vs. legitimate mail
  - Unmodified message delivery

Other Considerations

- Product configuration and tuning
  - Out of the box state
  - Vendor recommended tuning
  - Tolerance rating based on audience target
  - Long-term testing timeframe

Other Considerations

- Filter technique testing
  - Signature matching
    - Focus: catch efficiency and update timeliness
  - Heuristic rules
    - Focus: false positive rate and mitigation tools
  - Hybrid techniques
    - Focus: accuracy and update timeliness
  - IP filtering
    - Focus: delivery efficiency and mitigation tools

Other Considerations

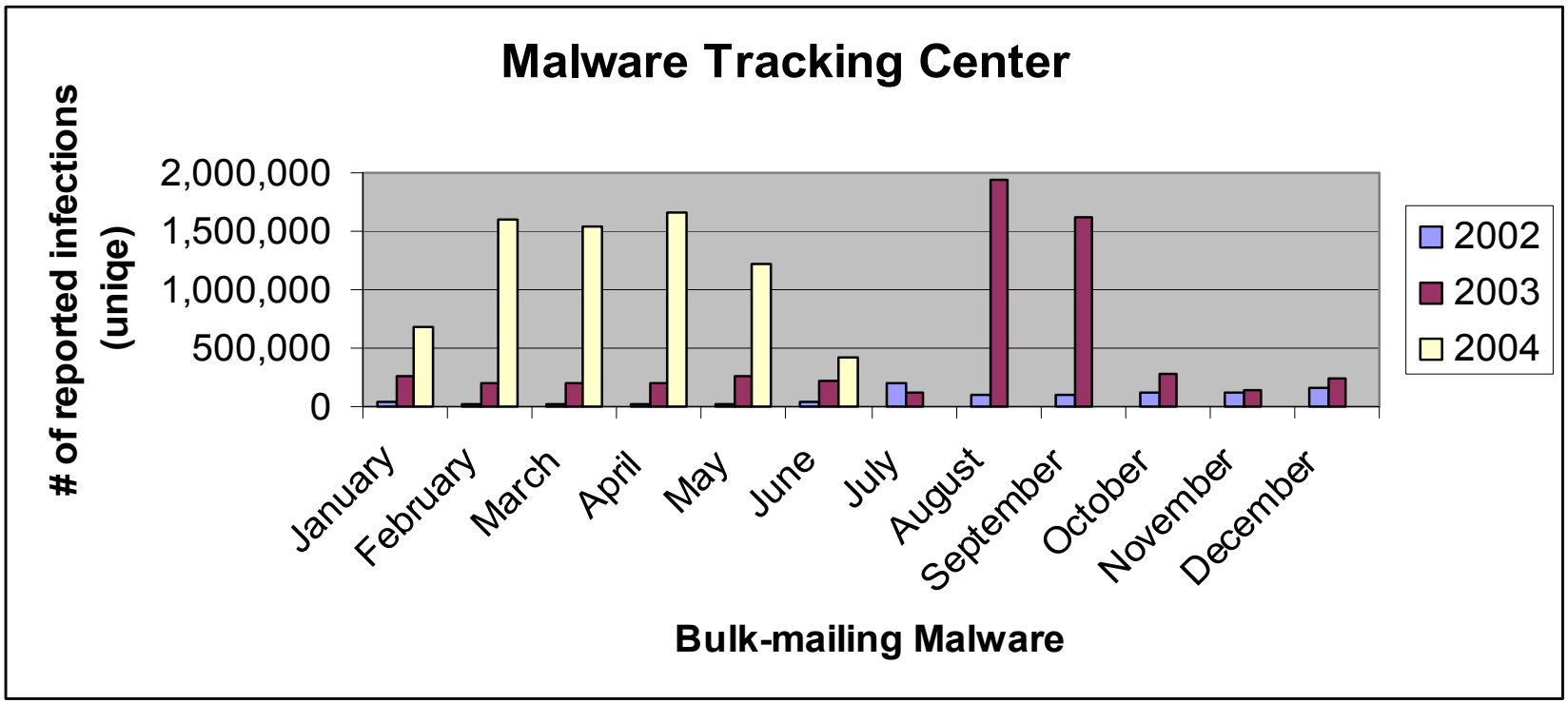
- Performance
  - Deployment time
  - Management reporting tools
  - Update overheard
  - Message latency

SUMMARY

- Comprehensive evaluation includes
  - scalability and resiliency
  - long term performance
  - customer specific goals
  - exception handling
  - minimal administration

Questions?

Mass-mailing malware spam



- Summary:
  - 2003, due to Mimail, Blaster, and Sobig
  - 2004, due to Bagle, Mydoom, Netsky, and Sasser