ITU WSIS Thematic Meeting on Countering Spam: The Scope of the problem

Mark Sunner, Chief Technical Officer
MessageLabs

6th July 2004
MessageLabs protects businesses worldwide against email threats reaching their networks.

- Over 8,700 Business Customers Globally
- More than 2.5 million End Users
- 400 Global Enterprises With Over 2,500 Employees
- Over 55 Million Business Emails Scanned Per Day
- 99% Customer Retention Rate
- Sole Focus On Business Enterprise Market
Dynamic Global Platform

- Secure email management service
- Globally distributed architecture
- 24/7 threat monitoring and response
- Provisioning and supporting clients 24/7 - globally
- Instant scanning over 55 million business emails a day
Operating at the Internet Level

The MessageLabs Service

- Client Simply Points MX (Mail Exchange) Record to MessageLabs
- Email is Scanned and Handed to Client Mail Server – Protected & Controlled
- All Threats are Kept AWAY from the Client Network
Skeptic™ Predictive Technology

- Predictive technology identifies **unknown** and **dynamic** threats
- 6+ years R&D

- 2Gb+ self learning rules knowledge base:
  - Virus & Spam “DNA”
  - Thousands of Heuristic Rules
  - Known Security Vulnerabilities

- Analysis of traffic patterns
- Thresholds are dynamic & action taken accordingly
Global Spam Patterns and Trends

Spam to Mail Ratio

Mail Received
Spam Received
Percentage of Email
Ratio Trend

Mail/Spam Volume
Ratio in Mail

January
February
March
April
May
June
July
August
September
October
November
December

2002
2003
2004
Email is now considered a business-critical application (Gartner Sept 2003)

Email is also considered a legal document and industry is required to treat it as such

June 2004: 1 in 10.8 (9.3%) emails contained viruses; equivalent to 37.6 virus borne emails every second

June 2004: Spam accounted for 85.3% of email traffic; equivalent to 305.5 spam messages per second
- US >80%, UK 50-60%, Germany 40%, Australia 30%, Netherlands 30%, Hong Kong 25%
Recent viruses contain Remote Access Trojan (RAT) component
- Fizzer, Sobig, MyDoom, Sober
- Spyware: leaking information to spammers

Case study: Sobig.F
- Sobig.F was the fastest spreading email worm in the past 4 years
- It generated over 200 million infected email messages during its first week of activity
- Staged deployment of WinGate Proxy software

Currently 70% of spam intercepted by MessageLabs is sent via open proxies
- Spammers will portscan for open proxies
- Some Ratware comes with pre-set lists or daily updated lists
- This leads to 50,000 new zombies appearing each week
- Traded online as potential open proxies for the spammers or as hosts for everything from paedophile images, DDoS attacks (distributed denial of service) to Phishing scams
- Some estimates suggest that 15% to 25% of the Internet may be controlled by spammers or criminal gangs
The “Bot-net” Phenomenon

- Around 70% of all spam is sent via an open proxy
- 75% of which originated from virus infected domains

Early example of trojan with spam connections
Case Study: MyDoom.A

Window of Vulnerability: 9 hours, 58 minutes
Growth of Open Proxies
The Impact of Spam Legislation

- New EU spam legislation enacted in December 2003
  - In December 2003, 62.7% of email scanned was spam, rising to 63.0% in January 2004
  - >70% of spam sent to UK in January originated in the US
    - Figure set to rise to >80% by July 2004
  - Open to interpretation
  - Jurisdiction not clearly defined

- EU/US legislation unlikely to ease spam epidemic
  - CAN-SPAM opt-out vs. opt-in
  - Majority of CAN-SPAM compliant spam is “dressed-up” to appear legitimate
  - Regulation for a previously ungoverned industry

- Corporate governance (e.g. Sarbanes-Oxley, Basel-2)
  - Email archiving policies
  - Risk Management
Tackling Spam

- Legal framework is only part of an overall solution
  - Less appealing
  - Difficult to operate and be profitable
  - “Locks” vs. “Laws”
- Need a technology based solution as well
  - IP Block-listing / Permitted sender lists
  - Fingerprints / Signatures
  - Collaborative filtering
  - Heuristics
  - Statistical methods, e.g. Bayes
  - Sender Warranted Email, e.g. Habeas haiku
  - Open Proxy detection
  - URL signatures
- Phishing emails intercepted by MessageLabs
Phishing: A Global Problem

- Worldwide Phishing
Any Questions?

www.messagelabs.com/intelligence