The problems of spam

Ewan Sutherland

Introduction

- Introduction
- The origins
- Variations on the theme
- The rise of phishing and pharming
- Inter-governmental (in)activity
- Conclusions and issues

Spam

- Commercialisation of the Internet
- Electronic mail is “free”
- Spam was originally a tinned meat product from the USA, short for SPicy hAM
- Monty Python’s Flying Circus:
  - The Green Midget Café
  - Every meal included Spam
  - The Spam song

Monty Python's Spam menu

- Egg and spam
- Egg, bacon and spam
- Egg, bacon, sausage and spam
- Spam, bacon, sausage and spam
- Spam, egg, spam, spam, bacon and spam
- Spam, sausage, spam, Spam, spam, bacon, spam, tomato and spam
- Spam, spam, spam, egg, and spam
- Spam, spam, spam, spam, spam, spam, baked beans, spam, spam, spam and spam

Unsolicited advertisements

- Originally the Internet was non-commercial
- As commercial use grew, so did unsolicited electronic mail
- Addresses were freely available
- “spam” grew to unacceptable levels
- Spam became a vector for viruses
- Spam became a profitable business model:
  - even at minimal response rates
  - infinitesimal cost

Filtering at destination

- Companies and individuals are expected to filter out spam on arrival
- Assumes that the cost are insignificant:
  - carriage of spam
  - filtering
- Filtering is never totally effective:
  - false positives
  - false negatives

http://www.email-policy.com/Spam-black-lists.htm

Open relays

- Electronic mail is transmitted by relays
- Some SMTP relays are open for anyone
- In this way spam enters the global system
- SMTP relays should only allow mail from registered clients
- ORDB currently reports 250,000 open relays worldwide

ORDB rankings of open relays

1. USA	82,981	11. Spain	3,079
2. China	25,774	12. India	3,056
3. South Korea	16,421	13. France	2,969
4. Japan	9,921	14. Hong Kong	2,779
5. Taiwan, China	8,468	15. Mexico	2,681
6. Germany	6,233	16. Australia	2,492
7. United Kingdom	5,457	17. Russia	2,420
8. Canada	5,115	18. Poland	2,034
9. Italy	3,661	19. Netherlands	1,559
10. Argentina	3,587	20. Sweden	1,306

http://www.ordb.org/

Spamhaus

- An international non-profit organisation, based in the UK, whose mission is:
  - to track the Internet's Spam gangs
  - to provide dependable real-time anti-spam protection for Internet networks
  - to work with Law Enforcement Agencies to identify and pursue spammers worldwide
  - to lobby governments for effective anti-spam legislation
- It maintains the Register of Known Spam Operations (ROKSO)

80% of spam received by Internet users in North America and Europe can be traced via aliases and addresses, redirects, hosting locations of sites and domains, to a hard-core group of around 200 known spam operations ("spam gangs")

http://www.spamhaus.org/

Spamhaus – countries and ISPs

1.	United States	2,292
2.	China	392
3.	Russia	293
4.	Japan	282
5.	Taiwan	184
6.	Canada	169
7.	South Korea	160
8.	UK	144
9.	Netherlands	139
10.	Hong Kong	124

1.	mci.com	214
2.	sbc.com	90
3.	comcast.net	70
4.	hinet.net	50
5.	ocn.ne.jp	42
6.	nttpc.ne.jp	42
7.	xo.com	39
8.	level3.net	38
9.	interbusiness.it	37
10.	newworldtel.com	32

Sophos rankings

October to December, 2005

1. United States 24.5 %
2. China (inc Hong Kong) 22.3 %
3. South Korea 9.7 %
4. France 5.0 %
5. Canada 3.0 %
6. Brazil 2.6 %
7. Spain 2.5 %
8. Austria 2.4 %
9. Taiwan 2.1 %
10. Poland 2.0 %
10. Japan 2.0 %
12. Germany 1.8 %

http://www.sophos.com

Zombie computers

- A computer compromised by a security cracker, a virus or a trojan horse
- One of many computers in a "botnet", used to perform a malicious task under remote direction
- Owners are unconscious vectors and thus compared to a “zombie”
- Infected computers — predominantly running Windows — are the major delivery method of spam, between 50% and 80%
- Zombie computers allow spammers to avoid detection and bandwidth costs
- They are also used to commit “click fraud” against sites displaying pay-per-click advertising

http://www.microsoft.com/presspass/features/2005/oct05/10-27Zombie.mspx

Ipswitch – current view

- 62% of all e-mail received is spam,
  compared to 57% in the previous quarter
- Pornography was the most common spam (24% of total)
- Second place was offers of mortgages and loans (18%)
- Third place was offers of “medication” (17%)
- Fourth was electronics and pirated software (16%)
- Fifth was attempts to ‘phish’ recipients' banking details with claims of lottery wins and online gambling accounts (10%)

http://www.ipswitch.com/

Variations on a theme

- SPIM – spam on Instant Messaging
- SPIT – spam on Internet Telephony
- SPLOG – spam in weblogs
- mobile Spam:
  - SMS
  - MMS

Can Spam Act of USA (2003)

- Delayed by efforts at technical solutions
- Delayed by industry lobbying, especially by direct marketing companies
- Enabled ISPs to sue spammers
- Some legal cases have been concluded
- Has had no discernible effect in reducing the volume of spam originating from the USA

http://www.onguardonline.gov/

China

- Internet Society of China (ISC) and leading service providers are to build a unified electronic mail management platform
- They will cooperate with international anti-spam organizations
- They will create a common blacklist of spam senders
- An anti-spam reporting hotline received 5000 complaints in a few weeks, of which 70% were spam and 28% junk SMS
- Growing problems with SMS
- Government has announced the obligation to register all mail servers

http://www.anti-spam.cn/

Australia

- Passed specific legislation
- Bi-lateral inter-governmental agreements:
  - e.g., Republic of Korea and Australia
- Also a mandated Code of Conduct for operators

Australia – code of conduct

Networks

- not to have open relay or open proxy servers, and to impose the same obligations on their customers
- to scan their own networks for subscribers' misconfigured mail and proxy servers
- to allow for immediate termination of connections where it has become an open relay due to intentional misconfiguration or a zombie
- if notified that a customer's computer is a zombie to warn them and suggest how to correct the problem

Customers

- to provide spam filtering options
- to explain their default filtering of electronic mail
- to advise how to deal with, and report, spam.
- to ensure they prohibit the use of their networks for spamming and to inform their customers

http://www.spam.acma.gov.au/

ENISA report

- European Network and Information Security Agency
- There is no 100% protection against spam
- Protection against incoming spam can only be improved marginally
- Unless economic models for spam change dramatically, there is probably not much more that providers can do next to applying the variety of countermeasures to the largest extent possible
- Most spam originates outside of the EU
- A major problem is that spammers often hide their true identity
- The relationship between those national entities who control electronic communications and those who control transmission of unsolicited emails should also be clarified and simplified
- The terms opt-in and opt-out and the scenarios in which they are applicable could be further clarified
- Providers in Europe are more concerned about spam emails that their customers receive than they are concerned with spam that their customers send
- Enforcement could be further improved to also prevent spam originating from Europe.

http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

Mobile spam

- A major problem in Japan, but spreading
- NTT DoCoMo worked very hard to suppress it
- Text messages from dating services
- SMS to call premium services
- Devices are too small for firewalls and anti-virus software

http://www.gsmworld.com/documents/public_policy/digital_divide/mobile_spam.pdf

419 scams

- Derived from the Nigerian legal code
- Advanced fee scam
- A request for personal information
- Based on promise of a share in an illegal scheme to access money in banks
- Names used include the children and spouses of many former African leaders

http://www.ultrascan.nl/

Phishing

- Pronounced “fishing”
- Phishing for or stealing personal identity and financial account details
- Mail messages and associated websites
- Abuse and hi-jacking of brand names and logos
- 'spoofed' electronic mails to lead consumers to counterfeit websites designed to trick recipients into divulging
  - credit card numbers
  - account usernames and passwords
- Technical subterfuge is used to plant crimeware on PCs to steal credentials directly, e.g., Trojan keylogger spyware
- The Bank of America example uses the genuine web site with redirection to the phishing site
- The PayPal example uses a web site with a name similar to a genuine domain name

Example – Bank of America

Bank of America Higher Standards

Online Banking Alert

Need additional up to the minute account information?
Sign In »

Change of Email Address

Your primary e-mail address for Bank of America Online Banking has been changed.

Did You Know? You can change your address, order checks and more online. Sign in to Online Banking and click on the "Customer Service" tab.

Because your reply will not be transmitted via secure e-mail, the e-mail address that generated this alert will not accept replies. If you would like to contact Bank of America with questions or comments, please sign in to Online Banking and visit the customer service section.

Bank of America, N.A. Member FDIC. Equal Housing Lender

Official Sponsor 2000-2004 U.S. Olympic Teams USA

Example – PayPal

PayPal The way to send and receive money online

Security Measures

Dear Paypal Customer,

In accordance with our major database relocation, we are currently having major adjustments and updates of user accounts to verify that the informations you have provided with us during the sign-up process are true and correct. However, we have noticed some discrepancies regarding your account at Paypal. Possible causes are inaccurate contact information and invalid logout process.

We require you to complete an account verification procedure as part of our security measure.

You must click the link to complete the process.

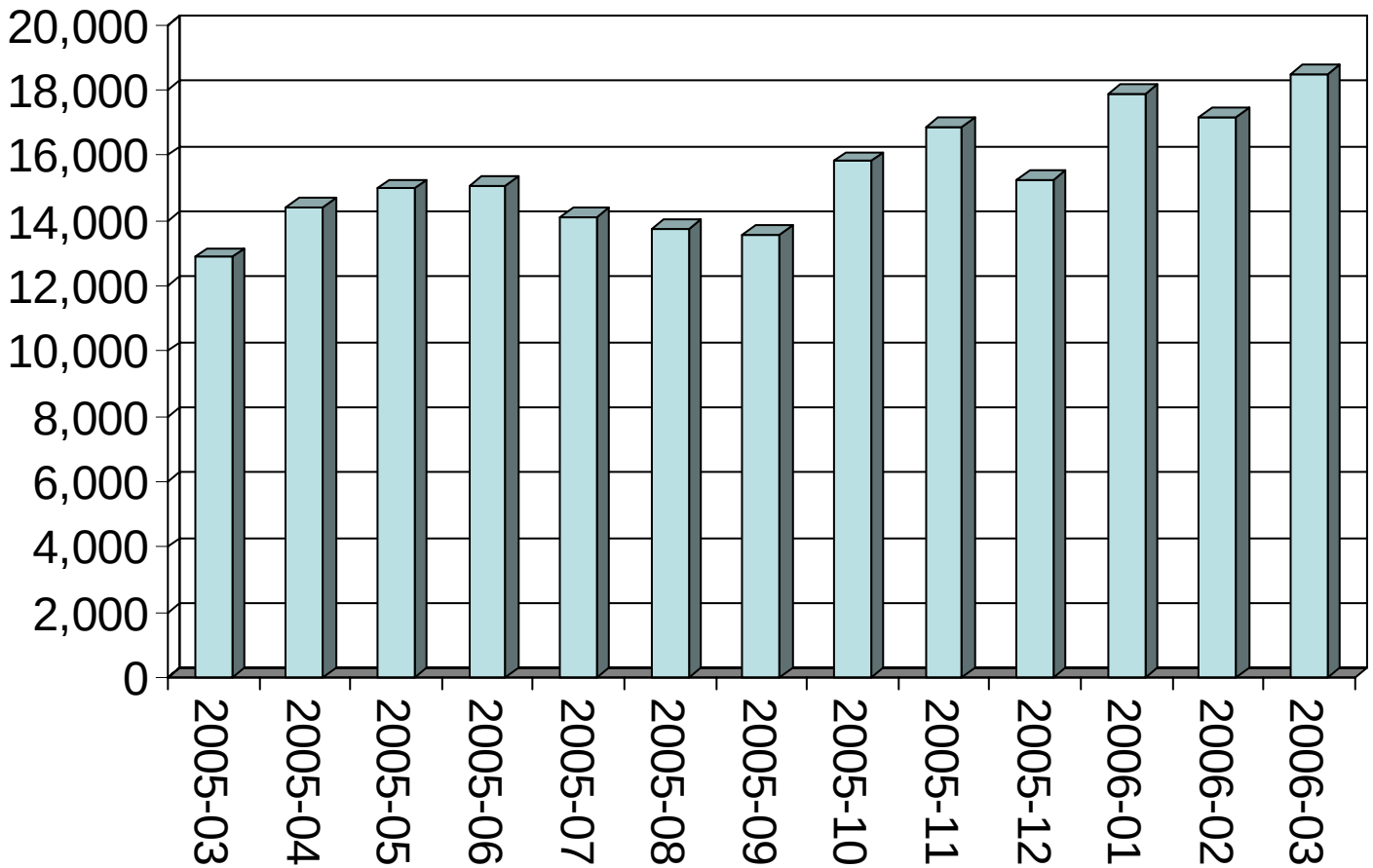
Click here to confirm your account

Please Note

Unable to do so may result to abnormal account behavior during transactions. We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account.
We apologize for any inconvenience.

Sincerely,
PayPal Account Review Department
PayPal Email ID PP560

Reports of individual phishing attacks



http://www.antiphishing.org/

Pharming

- Pharming is derived from phishing, exploiting a vulnerability in the Domain Name Server (DNS)
- A “cracker” takes over the domain name and redirects traffic to another site
- A copy of a bank's website can be used to "phish" for user passwords, PIN numbers and personal information
- It should only be possible when:
  - the original site is not using SSL protection
  - the user ignores warnings about invalid server certificates.
- For example, in January 2005, the domain name for a large New York ISP, Panix, was hijacked to a site in Australia
- Secure e-mail provider Hushmail was also caught by this attack on 24th of April 2005 when the attacker rang up the domain registrar and gained enough information to redirect users to a defaced webpage

Adware

- Automatically plays, displays, or downloads advertising material to a computer after the software is installed or while the application is being used
- Some legitimate adware based applications
- A major problem with P2P applications
- Software available to remove adware and spyware

http://www.lavasoft.de/

Spyware

- a broad category of malicious software (“malware”) designed to intercept or take partial control of a computer's operation without the informed consent of the owner or user
- refers broadly to software that subverts the computer's operation for the benefit of a third party
- Unlike viruses and worms it does not usually self-replicate
- spyware exploits infected computers for commercial gain
  - Delivery of unsolicited pop-up advertisements
  - Theft of personal information (including credit card numbers)
  - monitoring of web-browsing for marketing
  - routing of HTTP requests to advertising sites
- A very serious security threats to systems running Microsoft Windows
- Microsoft has produced Defender to identify and remove spyware

Spam in developing countries

- ISPs and network providers lack the capacity and resources to deal with sudden surges in spam, causing mail servers to break down or to function at a sub-optimal level
- Their capacity to cope with even normal (though fairly high) levels of spam is much weakened because resources such as hardware, bandwidth and software licenses tend to cost much more as a percentage of an ISP's budget
- End users, both consumers and business, may lack knowledge of potential resources available to them to take effective action, and even those resources that they do have available cost relatively more.
- Many people rely on hosted electronic mail services with limits on mailbox sizes
- Accessing mail becomes too expensive if per-minute charges paid to cybercafé owners are consumed by deleting spam from mailboxes
- Legitimate mail bounces, because the mailbox quotas are filled by spam

http://www.oecd.org/dataoecd/5/47/34935342.pdf

Developing countries

- A much more serious problem than in developing countries
- Few developing countries have effective anti-spam laws or the resources to enforce such laws
- ISPs are ill-equipped to deal with these issues, in terms of:
  - technical knowledge
  - money
  - equipment
- The effects of spam and net abuse make people wary of using the Internet

ITU Workshop on Countering Spam

No “silver bullet” solution, instead a combination of:

- Strong, enforceable legislation
- Continued development of technical measures
- Establishment of meaningful industry partnerships, especially among ISPs, mobile carriers and direct marketing associations
- Education of consumers and industry players about anti-spam measures and Internet security practices
- International cooperation among government, industry, consumer, business and anti-spam groups, for a global and coordinated approach to the problem

http://www.itu.int/osg/spu/spam/
http://www.itu.int/osg/spu/spam/chairman-report.pdf

OECD spam task force

- Created to address this urgent problem
- Spam is dangerous and costly for business and consumers. It disrupts networks, cuts productivity, spreads viruses and is increasingly used by criminals who steal passwords to access confidential information and often bank accounts
- The OECD calls on governments to establish clear national anti-spam policies and give enforcement authorities more power and resources
- International cooperation is also key
- Educating people on the risks of spam and how to deal with it is also important

http://www.oecd-antispam.org/

OECD – towards a culture of security

- Guidelines for the Security of Information Systems and Networks
- Originally adopted in 1992
- Revised and adopted by OECD Council in July 2002:
  - Promote a culture of security among all participants as a means of protecting information systems and networks
  - Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation
  - Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used
  - Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks
  - Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures
  - Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards

http://www.oecd.org/document/48/0,2340,en_2649_33703_15582250_1_1_1_1,00.html

UN General Assembly

Creation of a global culture of cybersecurity (A/58/199)

1. Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.
2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.
3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.
4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.
5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
6. Ensure that data availability policies take into account the need to protect critical information infrastructures.
7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States.
8. Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities.
9. Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate.
10. Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.
11. Promote national and international research and development and encourage the application of security technologies that meet international standards.

http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/58/199&Lang=E

G8 High-tech Crime 24/7 Network

- Network of 24-hour points of contact for high-tech crime:
  - 40 members
  - Critical Information Infrastructure Protection Directory
- Negotiation of widely-accepted principles and action plan to combat high-tech crime, adopted by G8 Justice Ministers and endorsed by G8 Heads of State
- Best practices documents
- Assessments of threats to and effect on law enforcement from new wireless technologies, encryption, viruses, worms and other malicious code
- Training conferences for cybercrime agencies
- Conferences for law enforcement and industry on improved cooperation and tracing criminal and terrorist communications

Conclusions

- The Internet is now heavily criminalised
- Failure to control for electronic mail led to other forms of criminal activity
- Fraud is endemic and cannot be brought under control
- Criminals are using a venture capital model to develop new schemes
- Governments have been shown to be ineffective in containing problems
- Users have to face high costs in software and hardware to resist the rising tide of malware

Ewan Sutherland

- http://.www.3wan.net/teaching/strategy2006/
- 3wan [at] 3wan.net
- ewan [at] gstit.edu.et
- skype://sutherla
- +44 141 416 06 66