



Spam and Spyware

Symbiotic Relationships Between Network Parasites

APEC-OECD Joint Workshop Plenary

Suresh Ramasubramanian

Coordinator, APCAUCE



Content Pollution won't go away.

Spam and Malware are a fact of life – here to stay.

- Focus must, therefore, be on mitigation rather than on finding a chimerical “solution”
- A real life analogy – pest control and sanitation, or the control of an epidemic
- Spam and malware have formed a symbiotic relationship, that can be likened to different parasites cooperating to devour a host organism
- Coordinated action required, with a multi-stakeholder, multi-pronged approach that addresses short-term goals, besides implementing long-term measures aimed at the mitigation and prevention of spam.



Far worse in the Asiapac region

- Drain on often limited and expensive bandwidth
- Rampant software piracy propagates malware
 - Pirated software may come with hidden malware
 - Such software does not have access to software updates and security patches
- Users are unaware, so highly vulnerable.
 - They fear going online, even to access legitimate banking and e-governance websites.
- The high value of such sites, often combined with poor security practices, make hackers specifically target them for compromise



Multipronged, Multistakeholder Approaches

- Infrastructure, Logical, Content and Social / Developmental measures required to combat spam and malware.
- Introduction of comprehensive antispam and data privacy laws
- Empowering the executive and judiciary to act against spam and cybercrime, and increase their awareness of these issues
 - This helps avoid fiascos like the arrest of eBay India's CEO.
- Increased cooperation between government, industry, civil society and the general public
- Implementation by ISPs of technical measures, policies and standard operating procedures against spam
- Education and empowerment of users – currently helpless targets of spam, malware and identity theft.
- A detailed treatment of this can be found in the OECD report on Spam Problems in Developing Economies



A startling lack of tangible results so far

- A few minor victories – some prosecution, a slight increase in awareness, some initiatives to secure commonly used software
 - Not nearly enough.
- Massive communication gaps between stakeholders is a major obstacle to coordinated action against spam and malware.
- Several countries in the AsiaPac region now faced with an influx of foreign spammers and malware sites offshoring to their countries.
 - Botnet “command and control centers”
 - Web and DNS hosting of spammer and malware domains
 - Abusers exploit lax ISP policies and the absence of relevant laws,
- This allows spammers and Internet abusers to operate with impunity, and consequently leads to widespread blocking of ISPs that allow themselves to become vectors for spam and malware.
 - This may be compared to quarantining an epidemic hit area



Spam and Malware – Symbiotic Parasites

- Spam is used as a vector to distribute malware and compromise PCs
 - Compromised PCs in turn are used to send even more spam
 - Besides being used for ID theft and DDoS attacks
- This has led to an industrial revolution in spam and malware..
- Abusers have now become a fast moving target, able to switch their operations to any part of the world.
 - Easy for abusers to erase their traces – they control the host machine
 - Abusers hide their origin thoroughly by daisy chaining their way through several compromised machines
- Some criminal spammers are now exclusively using botnets.
 - Botnets give them a high degree of anonymity and economies of scale
- Convergence means that the threats of the Internet have now migrated to conventional telephony – both landline and cellular phones
 - Spam and Viruses now current that specifically target cellphone users



Antispam initiatives in Asia and Worldwide

Law and Regulation

- Some AsiaPac countries have, or are introducing antispam laws - Australia, New Zealand, Korea etc
 - Australia has successfully prosecuted a notorious spammer, Wayne Mansfield, under their antispam law

International cooperation - governments and regulators

- Seoul Melbourne Pact on Antispam – signed by several Asia Pacific regulators. Focuses on information sharing, technical, educational and policy solutions to the spam problem
- London Action Plan – Brings together regulators from the USA, Canada, EU, AsiaPac, as well as international organizations such as the ITU and OECD, civil society antispam organizations, and industry (ISPs and vendors of antispam technology).



APCAUCE – Bringing people together against spam in the Asia Pacific Region

- Asia Pacific Coalition Against Unsolicited Commercial Email
 - Grouping of CAUCE chapters in the Asia Pac region
 - CAUCE is the world's largest volunteer antispam organization, with groups in the USA, Canada, the EU and the Asia Pac region
 - APCAUCE includes members and CAUCE Chapters from Australia, China, Hong Kong, India, Japan, Korea, Malaysia, New Zealand, Taiwan and Thailand
- APCAUCE activities include
 - Technical tutorials and conferences at APNIC, SANOG, APRICOT
 - Speakers include technologists, ISPs, blocklist operators and lawmakers
 - Annual "Regional Update" meetings that bring together regulators, governments, ISP associations and interested citizens from around the region at an informal round table discussion of antispam laws and initiatives in the region. This is an annual event held on the sidelines of APRICOT
 - Contribution of public policy papers on spam related issues to organizations such as the OECD, UNDP/APDIP and the Hong Kong regulator OFTA



The OECD Antispam Toolkit

- ▶ Produced by the OECD Antispam Task Force
- ▶ Eight pronged approach encompassing
 - Regulation
 - International Enforcement and Cooperation
 - Industry driven solutions
 - Technologies
 - Education and Awareness Programs
 - Cooperation between different groups of stakeholders
 - Spam metrics to measure the effect of antispam initiatives
 - Outreach to non OECD economies.
- ▶ Documents released under the toolkit include an Antispam law enforcement report, and paper on spam problems in developing countries by Suresh Ramasubramanian
- ▶ <http://www.oecd.org/sti/spam/toolkit/>



WSIS Spam and Cybersecurity meetings

- ▶ The ITU Strategy and Policy Unit (SPU) has brought together several stakeholders from government, regulatory authorities, industry and civil society to hold two WSIS thematic meetings.
 - ▶ Thematic meeting on Spam (July 2004)
 - ▶ Thematic meeting on Cybersecurity (July 2005)
- ▶ A consistent theme has been the emphasis on multi-pronged, multi-stakeholder approaches that are inclusive, and keep in mind other legitimate concerns, such as privacy and free speech, when implementing measures against spam and security threats.
- ▶ There is a clear call to ensure that these must coexist so that while human rights are respected, measures for privacy and free speech must not hamper antispam and cybersecurity effort.
- ▶ Representatives of developing countries such Syria and Nigeria, have advocated a global MoU on Spam and spyware



International Cooperation: ISP to ISP

- ISP to ISP cooperation is essential
- Clear and accurate whois records and maintenance of postmaster and abuse mailboxes in order to facilitate reporting of security incidents
 - CERT groups have a vital role to play in coordinating this
 - However the actual action has to be taken by ISPs
- Participation of ISPs in antispam workshops and network operator conferences like SANOG and APRICOT.
- Active participation in Industry groups like MAAWG and Civil Society groups like APCAUCE, that bring ISPs from around the region together
 - APCAUCE will organize a conference track on spam at APRICOT 2006 (Perth)
 - The next MAAWG meeting is from November 8-10 (Montreal, Canada)



Multistakeholder International Cooperation [contd]

- Work together with banks, e-commerce vendors and other legitimate senders of bulk email to ensure that their email is not misdetected as phishing or fraud email
 - Authentication schemes such as DKIM, SPF and Sender ID may have some potential in this regard.
- Work together with CERT groups, law enforcement, civil society antispam organizations such as APCAUCE and spamhaus.org, as well as industry initiatives such as MAAWG and the Anti Phishing Working Group (APWG).
- Work together with the software and give users fast access to secure computing resources (windows update, antivirus software etc) by distributing CDs to their users, or setting up local mirrors and/or Akamai clusters of software
- Work with civil society organizations with a high degree of outreach, like ISOC, for user education initiatives.
- Joint workshops organized by different organizations, are a good place to bring together all relevant stakeholders combine their efforts and broaden the outreach of these efforts.
- ISPs, Industry and Civil Society should work together to give coordinated inputs to the government for comprehensive cybercrime, spam and privacy laws and their effective enforcement



What now? The immediate and foreseeable future

Several different efforts (OECD, WSIS, Civil Society, Industry)

- There is a definite need for some of these initiatives to merge their efforts, or at least to work jointly, so that their joint skills can be harnessed by working together. This also widens the outreach of these efforts, as a larger constituency of governments, organizations and people can be approached.

Startlingly effective short term results perhaps, but long term?

- Even minor increases in targeted spam filtering efforts, or a weakly drafted antispam law, may have an immediately perceptible effect on spam levels. But this may be short lived.
- Capacity building and long-term strategic thinking necessary
- OECD style antispam toolkits, integrated with a broader Internet Governance toolkit approach.
- Develop capacity and cooperation at national and regional levels, and at grassroots levels, for quick and effective results. It may be a long time before any kind of global MoU or joint action on spam makes its efforts felt.
- Identify locally based organizations for cooperation, such as APECTEL and APCAUCE - well placed to use their expertise and outreach in the to play a coordinating and facilitating role in this process.

Q?
A!

Suresh Ramasubramanian
Coordinator, APCAUCE
Manager, Antispam Operations, Outblaze
suresh@outblaze.com