

# Best Current Practices on spam prevention

*Champika Wijayatunga, APNIC*  
*[champika@apnic.net](mailto:champika@apnic.net)*

**21 April 2006, Beijing, China**

***In conjunction with CNNOG3***

# Overview

- Background: spam
- Problems and prevention
  - Consumers, Businesses and ISPs
- Handling spam
- APNIC involvement

# Background - spam

# Who is responsible for spam?

- Advertisers
  - Technical experts who do their own spamming
  - Businesses who hire a third party to do the spamming
- Spam service providers (most common)
  - Build up hardware, software & expertise need to send spam
  - Advertise their services to distributors
- Spam support services
  - ISPs/web hosting services that take any customer
    - no matter what kind of activity they are involved in

# Statistics – how critical?

- Nearly 75% of email traffic is spam
  - Over 1 billion unsolicited messages sent per month
  - Amount is doubling every 5 months
- AOL & Hotmail block around 2 billion spam each day & still more slipping through
  - Now the figure is 10 times higher than that of 5 years ago

Source: <http://www.postini.com/stats>

## Statistics – how critical?

- Spam volume grows at 37% per month
  - an annual growth of 400%
- Lots of spam appears to use foreign relay
  - Countries may need to work on spam legislations
- Court cases between spammers & innocent victims
  - Only major corporations can afford such court cases

Source: *InformationWeek* Survey

# Problems & Prevention: Consumers

# Problems for consumers

- Privacy
- Concern about children receiving pornographic spam
- Mobile internet devices are getting popular
  - Charges based on contents or time to download
- How the attack works
  - Victims give away their own addresses

# Prevention

- Use caution when choosing sites
- Avoid giveaways & other “too good to be true” sites
- Avoid signing up for sites that use an opt-out policy
- Read sign-up screens carefully
- Read privacy statement carefully

# Prevention

- Know where your email can be found
- Guard your primary email address
- Never click reply to unknown senders
- Be careful with your browser
- Choose an ISP that actively blocks spam
- Find out how to filter your own email

# Problems & Prevention: Businesses

# Problems for businesses

- Technical support costs
- Spoofing (use of legitimate name)
- Harvesting e-mail ids of staff
- Phishing attacks
- Sexual harassment
- Marketing difficulties

# Prevention

- Robot exclusion standards
  - Creating a robot.txt file listing the restrictions or by using meta tags in HTML
- Confuse the robots
  - Obfuscate, html tagging, email ids as images
- Spam poison (sending fake email ids)
- Maintain the privacy
  - Not to forward hoax messages
- Text mails over HTML

# Prevention

- Be careful when using vacation auto responders
- Check for spoofing: IP lookups to verify the hostname
- Web application security
  - Errors, e-mail mining possibilities
- Spam filters
  - Whitelists, blacklists
- Challenge responses

# Problems & Prevention: ISPs

# Problems for ISPs

- Bandwidth
- Storage space
- Dissatisfied customers
- Requirement of additional tech staff
- Higher resource capacities to support excessive e-mail traffic
  - Attacks such as dictionary attacks put a huge drain on ISP servers
- Bounced messages
- SMTP
  - No mechanism to verify the sending server or the accuracy of the from addresses

# Prevention

- Contractual and cooperative solutions
  - AUPs
  - Strong anti-spam policies
  - Pay-to-send and pay-to-transmit models for sending bulk emails
  - E-stamps, Bonded Sender Programs (BSP)

# Prevention

- Technological solutions
  - Efficient tools for end-users
  - Blocking techniques for ISPs
    - Whitelists, blacklists
    - Timing and Grey lists, Bulk counting
  - Re-design the basic email protocol
    - Based on security certificates / like https
  - No open relays
  - E-mail authentication systems
    - SPF, Caller ID, Sender ID

# Prevention

- Legal solutions
  - Legislation that targets fraudulent or destructive conduct
  - Forged headers can be made illegal
  - Illegal to send emails with falsified routing information
  - Labeling ( ex: [ADV:] or [ADV:ADLT] )
  - Mandatory unsubscribe or opt-out (options to reject emails) requirements
  - Restrictions on email harvesting
  - Opt-in (options to receive email)

# Handling spam

# Email headers

**Return-Path:** hptimeline@yahoo.com  
**Received:** from ns.isoutsider.com (unknown [210.109.171.2]) by receiving.my-isp.com (8.9.3/8.9.3) with ESMTP id FSW930923; Sun, 31 Aug 2003 22:59:28 -700 (PDT)  
**Received:** from adventures (CPE – 65-31-127-1.wi.rr.com [65.31.127.1]) by ns.ioutsider.com (8.11.6/8.11.6) with ESMTP id h7JFLKK09863; Sun, 31 Aug 2003 22:56:22 +0900  
**Message – Id:** 200308191.h7JK09867@ns.isoutsider.com  
**Received:** from billclinton.whitehouse.gov ([184.325.23.124]) by mailout.yahoo.com (Postfix) With SMTP id 7600A32641; Sun, 31 Aug 2003 11:40:44 -0700 (PDT)  
**From:** hptimeline@yahoo.com  
**To:** <undisclosed.Recipients>  
**Subject:** Look Great for the Spring with Discounts on HGH (human Growth hormone)!!!!  
**Date:** Sat, 30 Aug 2003 02:10:21 -0800  
**MIME-Version:** 1.0  
**Reply-To:** hptimeline@yahoo.com  
**Errors-To:** pow@163.com

# Following the flow of email headers

- Every time an email message passes through a mail server, that system adds a received line
- Most recent one should be the one that says who delivered to your ISP

Received: from **ns.isoutsider.com** (unknown [210.109.171.2]) by **receiving.my-isp.com** (8.9.3/8.9.3) with ESMTP id FSW930923; Sun, 31 Aug 2003 22:59:28 -700 (PDT)

# Following the flow of email headers

- As you are sure that your ISP may not be sending you spam, you can look for ns.isoutsider.com

- **Received: from adventures (CPE – 65-31-127-1.wi.rr.com [65.31.127.1]) by ns.ioutsider.com (8.11.6/8.11.6) with ESMTP id h7JFLKK09863; Sun, 31 Aug 2003 22:56:22 +0900**

# Following the flow of email headers

**Received: from billclinton.whitehouse.gov  
([184.325.23.124]) by mailout.yahoo.com (Postfix)  
With SMTP id 7600A32641; Sun, 31 Aug 2003 11:40:44  
-0700 (PDT)**

- Suspensions about the legitimacy of this Received line
- Seems you have reached a deadend
  - Leaves with adventures or CPE-65-31-127-1.wi.rr.com as the end of the trail

## Looking at the last verifiable mail handling server

- Use a tool (nslookup) which enables you to find out whether these computer names and IP addresses match each other
  - Forward and reverse lookups

**Ns.isoutsider.com resolves to 210.109.171.2**

**CPE-65-31-127-1.wi.rr.com resolves to 65.31.127.1**

**Error – billclinton.whitehouse.gov doesn't exist**

# Investigating contents of spam

- Example

**Wholesale Prescription Medications  
DISCREET OVERNIGHT PHARMACY !**

**Now get HGH, Vicodin, Sex Organ Enhancements,  
Prozac, Viagr@, BustPro, Zoloft, Propecia. And  
many, many more!**

**Just e-mail doctorfeelgood328@yahoo.com, or visit  
our website at [http://1024349897/HGH\\_13/specialoffer.html](http://1024349897/HGH_13/specialoffer.html)**

- Web page address looks a bit strange
  - 1024349897 translates into 61.14.86.201
    - URL tool [www.sampade.org/t](http://www.sampade.org/t)
  - Translates to c201.h061014086.is.net.tw

# Address the complaints

- Most of the ISPs have their terms of service on their websites
  - Prohibits any form of spam-related activity
  - Provide an address for filing the complaints
  - Most commonly abuse@followed by the domain name

# Sending complaints

- Nicely :-)
  - Don't transfer your anger at spammer to the ISP
  - Spamming isn't really ISP's fault

**Dear Administrator,**

**I received a piece of spam that I have attached below.  
The headers appear to have originated at RoadRunner  
and been relayed via ns.isoutsider.com, and it advertises  
both a mailbox at Yahoo.com and a webpage at is.net.tw.  
Please take appropriate action to stop this spammer.**

**Thanks!**

# Sending complaints

- Make sure you attach a complete copy of the spam
  - Including all headers
  - Turn off any HTML or RTF formatting
    - Bold, colored stuff, embedded pictures etc
  - Send the message in plain text
- Some ISPs send acknowledgements but some do not
  - Most departments handling abuse are overworked and understaffed
  - Let them kill a few more spammers instead of responding to you :-)

# Sending complaints

- Sometimes the complaints can bounce back as undeliverable
- Try some whois inquiries
  - You can find more addresses to send the complaints
- Use traceroute
  - Find out where the spammer is getting the internet connection
- Sometimes the ISP doesn't care much about the problems caused by spammers
  - However the upstream ISPs may be able to help you

# Sending complaints

- Sometimes the results of traceroute can go cold after a private IP address
- So find the upstreams using whois
- Don't complain to IANA :-)
- If everything fails:
  - send documentation of your efforts to your ISP and ask it to block the spamming sites at their routers
    - If ISP is not responsive, it's time to look for an ISP who offers better services

# Fighting spam with spam

- Not a good idea
- One of the common tricks of the spammer is to relay their messages via an innocent third party mail server
  - So don't flood the innocent site with your complaints
- A common trick is to forge mail headers
  - Looks like the mail originated elsewhere
- So if ISP claims innocence don't fight back!
  - They may really be innocent

## If blacklisted – What ISPs should do?

- Contact the blacklist directly
- Need to request the blacklists to quickly de-list you
  - Submit a request to retest your "repaired" mail server
  - Propagation time after you are de-listed (may be ~ a week or so)
  - Destination mail server administrators pull the updated lists at times they prefer
- After that
  - Update your anti-virus software
  - Make sure your network is secured
- Don't send any more spam from your network

# APNIC's involvement

# Detecting the spam/abuse

- Software to detect network abuse
  - Mostly designed to search the ARIN Whois database
  - May refer to APNIC
- Many websites with whois lookup functions has the same limitations
- However the IP addresses are registered by five RIRs on a regional basis

# Detecting the spam/abuse

- If a standard search refers you to APNIC
  - Means only that the network in question is registered in the AP region
  - Does not mean that APNIC is responsible or that the hacker/spammer is using APNIC network

## Investigation of complaints

- APNIC is not able to investigate these complaints
- Can use the APNIC Whois database to find out where to take your complaint
- APNIC does not regulate the conduct of Internet activity (legally or in practice)

# Investigation of complaints

- Laws relating to network abuse vary from country to country
- Investigation possibilities
  - Cooperation of the network administrators
  - law enforcement agencies
    - Local jurisdiction
    - Jurisdiction where the problem originates

# How can APNIC help you?

- The APNIC Whois Database
  - Holds IP address records within the AP region
  - Can use this database to track down the source of the network abuse
  - Can find contact details of the relevant network administrators
    - Not the individual users
    - Use administrators log files to contact the individual involved

## How can APNIC help you?

- Education of network operators in the Asia Pacific community
  - Address policies and the importance of registration of resources
- Community discussions can be raised in the APNIC open policy meetings, mailing lists, etc.

# Summary

- Background: spam
- Problems & prevention
  - Consumers, Businesses, ISPs
- Handling spam
- APNIC involvement

# Questions?