SPAM - and how to deal with it

Turn spam against the spammers and virus writers for fun and profit

Identification of spam

- Spam filtering
- Manually examining it
- Proper identification an absolute must

Reporting Process

- Absolute, positive identification, and confirmation of each and every message
- Extract IP address from header
- WHOIS lookup to obtain ownership of IP
- Confirm validity of Email address from WHOIS record.
- Construct report message - date, time, sample spam (full headers)
- Send report, get back autoreply or bounce.
- Record ticket number from autoreply

Report Failed
(due to bounced message)

- WHOIS Data is bad
- Report bogus WHOIS to ARIN, APNIC, LACNIC, or RIPE, save ticket number for followup.
- Trace route IP address or consult looking glass server to obtain upstream provider
- Repeat reporting process to upstream provider, but add explanation that WHOIS data is invalid, request they pass report to downstream user.

Report Sucessful

- Save and record “Autoreply”
- Record date and ticket number of Autoreply for followup.
- If no autoreply, record date and time of report for followup in 2 weeks.
- IN followup, aggregate ALL spam sent to that specific ISP, send report again, then CC to the ISP’s upstream provider, and to FTC or authorities.

Who to report to

- Usually "abuse@hostname.com" is best Email to use
- If “abuse” email don’t exist, use “hostmaster” or pick technical contact from WHOIS data
- Some, but not all WHOIS records will clearly indicate where to report spam.
- Some WHOIS example outputs

Email Header Analysis

- ONLY the first “received” line cannot be forged. Assume all other information invalid, bogus or forged.
- Dates in headers are almost always wrong. Inaccurate clocks, unclear timezone specifications, is often a problem.
- Spammers always forge “From” email fields, “reply to” fields, and construct confusing headers.

SpamCop reporting service

- Free service available, but not feasable for large volume of spam. Built in delay is very annoying and time consuming.
- Pay service costs approx $1 per megabyte, much faster, but can be expensive if you get a lot of spam, and is still very time consuming.
- Spam older then 48 hours is not reported.
- Older spam is not worth reporting, as it’s more then likely already reported.

What does ISP do with your report

- Reports are processed manually, one report per spam. Few ISP's like to accept multiple spams reports per message. An auto-reply is sent back to the reporter.
- Reports are entered into a database. Actual spam included in the report is ditched, date is recorded, IP address is recorded and looked up for repeats.
- ISP's policies vary, but they usually won't do anything until they get more then 5 reports for any specific customer.
- Most ISP's notify the customer via Email, and sometimes a phone call. Customer is usually given a few days to respond. Some ISP's just cut off the customer's service.

ISP response times

- Usually takes a week before issue is resolved.
- If customer looses their internet service, they usually call ISP’s support line to complain about loss of service.
- ISP then notifies customer the reason for cutoff, some ISP’s won’t restore service until customer can prove they disinfected their machine.
- ISP’s action policies very.

College or Company’s policy

- Some companies won’t allow their employees to connect their personal laptops to corporate networks.
- Military personal are NEVER allowed to connect their laptops to the military networks
- New students are required to run AV software before connecting to dorm network.

Serious issues with reporting

- Reporting of non-spam can get innocent person disconnected from internet. Open to serious abuse or harassment.
- ISP’s are aware of this, and most usually won’t act on reports of non-spam, and is main reason why they manually process them.
- Most ISP’s ignore spam more then 48 hours old. The newer the spam, the better. Spam Cop issues rewards to people who report new spam all the time.

Spam Friendly ISP’s

- Chinanet.cn, Kornet.kr, rt.ru, ls.lv, apollo.lv will all ignore spam reports, but send them anyway, and also CC to their upstream providers.
- Submit them to ROKSO SpamHaus Database, or just simply block ALL mail originating from them.

How to deal with ISP’s that don’t cooperate

- Block ALL mail originating from their IP block. Publish it in all the anti-spam forums.
- Send a “snailmail” letter to the ISP’s upstream provider, phone them, and lodge a formal complaint.

Tracking spam

- Obtain domain name contact via WHOIS.
- WHOIS is often bogus, because when spammer registers domain they contact registrar a few days later and change their contact info to some false contact.
- Follow the money trail - as despicable as it sounds, order that penis enlargement kit or Viagra. When you get your statement, contact the bank or E-Commerce provider and lodge a complaint.
- Follow the shipping trail.

Dealing with BOGUS domain records

- Report BOGUS records to registrar - joker.com is the worst, CC your report to "ICANN.org"
- Domain owners have 2 weeks to respond or loose their domains. Many spammer's domains have been shut down this way. But at least 2 - 3 followups are necessary to get them to react.

Auto-Reporting

- When done right, can make a significant dent in the spammers “bottom line”
- Requires accurate database, which often needs constant updating.
- Requires attention, care, and feeding.
- Requires responsibility and care
- Can NEVER be fully automated

APNIC, LACNIC, ARIN, RIPE

- These organizations assign IP address space
- Never report spam to them
- They have NO authority to stop or put pressure in ISP’s
- They maintain WHOIS database records, but are often lax in keeping them updated, mostly due to the fact they are under funded, and over worked.
- They always appreciate getting reports on outdated or incorrect records.

Asian ISP’s

- A lot of them just ignore spam reports, especially China, and Korea.
- Recently, they are actually starting to respond to reports. China better then Korea
- Thailand, India, and Malaysia are average, but are slow to respond.
- Asian ISP’s who offer WIFI to travelers usually won’t relay mail anymore.

American ISP’s

- Web based mail services like Yahoo, Hotmail, etc will disconnect offenders first and ask questions later.
- Cable modem and DSL providers often restrict or rate limit port 25 traffic now, and if exceeded, will disconnect service for 24 hours. Some USA providers will disallow port 25 traffic alltogether.
- They respond in an average of about 3 - 4 days.
- Commercial T1 providers are now starting to take reports very seriously.

West European ISP’s

- Most follow American standards, but France is getting lax.   Spain is the worst, (telefonica.es, proxad.net)
- Turkey IP blocks assigned through RIPE often have the most inaccurate WHOIS records.
- European response time is slightly slower on an average, based on my Analysis.

Eastern European ISP

- Russia is the worst. Most Russian ISP’s are controlled and owned by the Russian Mafia, and almost ALL of them ignore spam complaints. Rt.ru, usinfo.ru
- Most welcome American spammers with open arms, and American hard currency.

Middle Eastern ISP’s

- Very little spam originates from Mid East ISP’s, but spam from Iran is picking up.
- Hardly any from Iraq, but Arabian penninsula has SOME, but most ISP’s respond quickly.
- Isreal ISP’s are about like European, and most have Zero tolerance to spammage.
- Very little spam from Afganistan, or Packistan, or any of the “stan” countries.

SpamCrunchers Reporting system

- Database is text file - 430k in size. Can be exported into ANY database.
- Written in Python
- All the database is ram resident during reporting, including the spam. Lookup times are a few milliseconds.
- Can report up to 10 megs of spam in a single chunk

SpamCrunchers (cont)

- Currently under field testing… Shell based GUI.
- Intention of implementing WEB based GUI.
- Operates on ANY platform
- Current version requires a lot of “care and feeding”
- FLOW DIAGRAM
- DEMO