Spam Abatement Proposal

"…spammers must be identified and quarantined from the general Internet-using population."
H. Robert Wientzen, president and CEO of the Direct Marketing Association | Optimize Magazine, January 2004, Issue 27

SPAM STATISTICS

• Predicted volume of spam as a percentage of all email by September 2003:
50% (Brightmail Report | July 1, 2003)

• Volume of spam as a percentage of all email in April 2001:
7% (Brightmail Report | July 1, 2003)

• Number of messages being sent daily by notorious spammer Ronnie Scelson:
180,000,000 (CBS News | June 18, 2003)

• Number of spam emails blocked by AOL daily:
2,400,000,000 (Seattle Times | June 16, 2003)

• Percentage of unfiltered incoming email that is spam at MSN and AOL:
80% (Seattle Times | June 16, 2003)

• Percentage of email-using children who receive inappropriate spam on a daily basis:
80% (Symantec Corporation Report | June 9, 2003)

• Percentage of children who report sometimes feeling uncomfortable about spam they receive:
34% (Symantec Corporation Report | June 9, 2003)

• Percentage of children who report sometimes feeling annoyed about spam they receive:
51% (Symantec Corporation Report | June 9, 2003)

• Percentage of children who report sometimes feeling offended about spam they receive:
23% (Symantec Corporation Report | June 9, 2003)

• Percentage of children in the United States who have at least one email account:
76% (Symantec Corporation Report | June 9, 2003)

• Percentage of children who report having received spam advertising x-rated websites:
47% (Symantec Corporation Report | June 9, 2003)

• Percentage of companies that rated "reducing spam" as their top IT priority:
52% (Radicati Group | June 1, 2003)

• Support for anti-spam laws among information technology professionals:
95% (SurfControl Survey | February 12, 2003)

• Percentage of email that will be spam by 2007:
70% (Radicati Group Report | February 11, 2003)

• Projected costs in 2007 for lost productivity at United States businesses due to spam:
$75 billion (Radicati Group Report | February 11, 2003)

• Amount spent by businesses in 2003 on spam filters:
$653 million (Radicati Group Report | February 11, 2003)

• Projected amount to be spent on spam filters by businesses by 2007:
$2.4 billion (Radicati Group Report | February 11, 2003)

• Percentage of voters in the United States who would "strongly support" banning unsolicited email:
73% (Public Opinion Strategies | February 11, 2003)

• Percentage of voters in the United States who are "against" banning unsolicited email:
8% (Public Opinion Strategies | February 11, 2003)

• In 2004, predicted amount companies will spend on servers to deal with spam:
$41,600,000,000 (Radicati Group | February 11, 2003)

• Annual cost of loss in productivity for a 100 person firm from dealing with spam :
$250,000 (Yankee Group Report | February 8, 2003)

• Percentage increase in unsolicited commercial email from 2000 to 2002:
1,800% (ZDNet News, "Spam Outlook Smells Worse" | January 3, 2003)

• In 2003, total cost of spam to United States businesses in lost productivity:
$10 billion (Ferris Research Report | January 2, 2003)

• Percentage of email users who find spam "very annoying":
80% (Harris Interactive Poll | January 1, 2003)

• Percentage of email users who found spam at least "annoying":
96% (Harris Interactive Poll | January 1, 2003)

• Number of spam servers operated by notorious spammer Alan Ralsky:
190 (Detroit Free Press | December 5, 2002)

• Percentage of users who say they spend more than 10 minutes dealing with spam daily:
75% (Symantec Corporation Report | December 2, 2002)

• Percentage of parents who are "very concerned" about their children receiving spam:
77% (Symantec Corporation Report | December 2, 2002)

• In 2002, number of email messages a typical home email user must wade through annually:
2,200 (ABC News, "Consumers Inundated By Spam" | November 30, 2002)

• Estimated global revenue generated by pornographic spam:
$3.2 billion (Sunday Herald | October 4, 2002)

• Percentage of unsolicited email generated by adult websites:
30% (Brightmail Report | August 22, 2002)

• Rank of spam among consumer complaints:
#1 (TechLaw Journal, June 2002 | June 1, 2002)

• Estimated cost to businesses in lost productivity per spam email received:
$1 (BBC News, "Why One Spam Could Cost $50" | April 9, 2002)

• Over the past two years, spam has doubled:
Every 6 months (ZDNet News, "Briefing Book Spam" | March 21, 2002)

• In 2001, amount stolen from consumers through online fraud:
$700 million (Federal Bureau of Investigation, "IFCC 2001 Internet Fraud Report" | January 1, 2002)

Professional spammers (estimates for the number of professional spammers are from 150-300 worldwide) account for approximately 90% of spam sent. These professional spammers have several methods for delivering their payload, but the easiest and most cost effective method is for them to

utilize foreign mail servers. They may pay the owners of these mail servers for email delivery, but most often these professional spammers simply seek out any of the several thousand open relay mail servers or several hundreds of thousands of open proxy computers, allowing them to send their mail without any problems, and with zero cost. It is widely known that the standards for server security are lower in certain countries, making them a spammer's haven.

Thus, I propose a very simple, yet effective solution that should cut the spam load by at least 50%, and probably quite a bit more.

Spammers seek out certain servers which exhibit certain characteristics that allow them to send email in anonymity.

The specific server characteristics are as follows:

Open proxy or hijacked proxy
Open relay
No or improper Source IP Reporting
No rDNS and no DNS validation

Open Proxy:
The term *open proxy* refers to the situation when a server allows network connections from anyone, to anywhere, on arbitrary ports and with arbitrary protocols. It means that spammers, for instance, can use that server to send spam without it being traced back to them. Connections made via open proxies are often non-accountable, since the open proxy server may be doing no logging, or if logging is being done, logs may be unavailable to those investigating network incidents.

Open Relay:
A *third-party mail relay* or *open relay* occurs when a mail server processes a mail message where neither the sender nor the recipient is a local user. The mail server is an entirely unrelated third party to this transaction. The message really has no business passing through this server. In the early days of the internet, open relays were considered part of contributing to the internet community. If someone's mail server was down, any other available server could pick up the load. Today, due to widespread abuse, open relays are an all too common internet problem.

Source IP Reporting:
Some older mail servers do not properly format the mail headers such that the message sender's IP address is added. Rather, the mail server inserts *its own* IP address, making it appear as though the spam message originated on the mail server servicing the recipient of the message. Older versions of the IMail server, from Ipswitch, exhibit this behavior. Spammers specifically seek out servers of this type, because it allows them to remain anonymous. Tracking the sender back to the originating IP address is impossible, but even worse, reporting the spam only results in the recipient's mail server being added to Block Lists.

rDNS:
Reverse DNS (rDNS) is a method of resolving an IP address into a domain name, just as the domain name system (DNS) resolves domain names into associated IP addresses. One of the applications of reverse DNS is as a spam filter. Here's how it works: Typically, a spammer uses an invalid IP address, one that doesn't match the domain name. A reverse DNS lookup program inputs IP addresses of incoming messages to a DNS database. If no valid name is found to match the IP address, the server blocks that message.

It is easy to discern that the primary modus operandi of the typical professional spammer is to obfuscate their IP address by whatever means available, to prevent tracking the mail message back to the sender and getting the sender disconnected from their ISP.

Thus, to effectively combat spam, we must expose the spammers IP address(es) by whatever means necessary. The easiest method for doing this is as follows:

Create a law which makes it illegal for companies operating mail servers within the United States and its territories and protectorates to connect to (i.e.: send data to or receive data from) servers (whether within or without the United States) that exhibit the above mentioned characteristics. Part of that law would also make it illegal for ISPs to connect or allow their users to connect to ISPs or web hosts that have an 'abuse score' (discussed later in this text) above a certain limit.

This serves some very useful purposes:

1.) This effectively disconnects the entire United States from the above mentioned 'spammers havens'. This will immediately cut spam by a large amount.
2.) Once the locked-out ISPs or web hosts of these 'spammer havens' realize that they no longer have connectivity with the United States, they will have an incentive to properly configure their servers, and ensure their users' computers are configured, such that spammers cannot use their systems as an open relay or open proxy, and such that tracking spam back to its originating IP address becomes possible.
3.) Systems within the United States will be required by law to be properly configured such that they do not exhibit the above mentioned characteristics. Thus, spammers will find it nearly impossible to send spam from within the United States, requiring that they either cease operations, or move offshore. Even moving offshore would have no effect, because any servers that they could exploit would be blocked from U.S. systems.

One might ask, "What about computers owned by private citizens within the United States, which exhibit open proxy characteristics? The people may not know that their computer is wide open to the internet, and most probably will not know how to fix the problem."

Again, the solution is simple. Put the onus on the ISPs of those private citizens to ensure that their users' computers are not abusing internet resources. If an ISP gets a report of a computer within their domain abusing internet resources, the ISP would be compelled by the rating system (discussed later) to immediately isolate that computer from the internet until it has been properly configured such that internet resource abuse will not happen again.

One might additionally ask, "What enforcement methods would be used to give ISPs and web hosts the proper incentive to follow through and block systems exhibiting the above characteristics, and ensure individual users' computers are protected from hijacking?"

An 'internet abuse tax' and abuse rating system. We already have the capability of reporting spam, of creating Block Lists, of tracking network abuse issue resolution time. Thus, we simply keep track of which ISPs and web hosts are getting abuse reports filed against them (including spamvertised websites), and track the time required to resolve the issue. The product of the number of issues and the average time to resolve issues (the 'abuse score') will serve as an indicator of that particular ISP's or web host's commitment to reducing the costs associated with abuse of the internet.

The worst 25% of ISPs and web hosts within the U.S. will be required to pay a tax to the government, the amount based upon the difference between their individual 'abuse score' and the aggregate 'abuse score' of the best 25%. Since all ISPs and web hosts will receive spurious reports of spam and

network abuse (due to false reports, virii, etc), the ‘worst 25%’ part of the equation filters out all but the worst offenders, ensuring that only the truly spam-friendly ISPs and web hosts are taxed. The ‘best 25%’ part of the equation takes into account that there may be spikes in reports for ALL ISPs and web hosts due to new, fast spreading virii. This filters that out.

Whereas before, certain ISPs and web hosts thought it more profitable to host the spammers, or to simply do nothing when they received an abuse report, they must now balance the profit from hosting and enabling spammers with the cost of the Internet Abuse Tax.

The money from the Internet Abuse Tax would be applied toward:

1) internet connectivity initiatives aimed at:

   a) lower income persons
   b) disabled persons
   c) persons in rural areas

2) national educational campaigns designed to:

   a) teach people about the dangers of directly responding in any way to offers propagated via spam
   b) teach people methods of securing their computers.

Example and Assumptions:

Let us assume that for the worst 25% of internet abuse offending ISPs and web hosts, there are 2.4 billion email messages sent out each day. This is a conservative estimate.

Let’s further assume that .05% of total spam is actually reported. This is the approximate amount of spam that is actually reported.

And we’ll assume that the average time to resolve an internet abuse issue is 30 minutes.

Thus, for all of the worst 25%, there are 1,200,000 internet abuse reports per day.

Thus, the aggregate ‘abuse score’ for the worst 25% offenders would be:

1,200,000 * 30 = 36,000,000 abuse points

Let us assume that for the best 25% of ISPs and web hosts, there are 200,000 internet abuse reports, and the average time to resolve an internet abuse issue is 30 minutes.

Thus, for all of the best 25% of ISPs and web hosts, the aggregate ‘abuse score’ is:

200,000 * 30 = 6,000,000 abuse points

The difference between the best 25% and the worst 25% would then be 30,000,000 abuse points.

Assuming that the federal government imposes a tax of 10¢ per ‘abuse point’, this would mean that the total number of worst 25% offenders would end up paying an aggregated $3,000,000.00 per day.

Each individual ISP contributing to the worst 25% score would pay an amount consummate with their contribution to the ‘abuse score’.

This would serve as a very effective incentive for these spam friendly ISPs and web hosts to disassociate themselves from spammers and ensure that their servers and their users’ computers are secured such that they could not be abused by spammers. Legitimate ISPs and web hosts would quickly learn to include in their contractual agreements, clauses that allow them to charge the actual spammers on their systems for the damages.

Another point that should be made is the issue of unresolved and irresolvable abuse reports. In these cases, the time applied should max out at a fairly high value, such as 300 minutes. Thus, for ISPs and web hosts who ignore abuse reports, and do so on a wide scale, they’ll find that their ‘abuse score’ (and their resultant internet abuse tax amount) quickly rises (but is not infinite), but for the legitimate ISPs and web hosts who will invariably receive a certain number (albeit a low number) of these types of reports, it will not be such that it would put them into the ‘worst 25%’ group, and even if it did, there is a set maximum amount of tax that could be imposed per irresolvable abuse report.

Total cost savings:

Assuming that this proposal reduces spam by 50%, we can immediately see a cost savings for the U.S. of approximately $5B in regained business productivity, $20B on new equipment savings, $350M in reduced fraud via email, $325M on spam filters. Total of approximately $25.6B / year.

Total internet abuse tax income:

It is impossible to estimate the total amount of tax that could be collected. Obviously, ISPs and web hosts will reconfigure their systems to tighten security, and will disassociate themselves from spammers, so the amount will decrease over time. Because the worst 25% will always pay some amount of tax, irregardless of the total number of abuse reports received, there will always be the pressure to continue improving security to lower their Internet Abuse Tax bill and to get out of the worst 25% group.

We will most definitely hear loud protests from the largest ISPs, since by sheer dint of the fact that they host larger numbers of users, they will obviously be subject to a greater amount of abuse. The thing is, they are also the worst offenders, in terms of the amount of spam sent vs. numbers of users. Obviously, they will have to lead the internet in securing their own machines and the machines of their users. The innovations and techniques which they develop (and which they can afford to develop) to reduce internet abuse will then be easily and cheaply available to other, smaller system operators, benefiting all.

The days of allowing certain individuals to abuse a world-wide system to the tune of tens of billions of dollars for their own gain, are over. If something is not done, email will be literally swamped and will become unusable. It is very near that stage now.