

---

## Google Named No. 3 Spam Provider

(2009-01-06) - Contributed by Larry Seltzer

New forms of spam and similar abuse find a welcome home at Google, and the company doesn't yet seem up to the security task of fighting them. Perhaps it's a responsiveness issue.

Much has been made of the recent revelation that Google had reached No. 4 on Spamhaus' list of "The 10 Worst Spam Service ISPs." In fact, as I check now, Google is No. 3.

It's no secret why Gmail is such a big spamming source now: Spammers have had success cracking the CAPTCHA tests and creating Gmail accounts from which to spam. Because the spam comes from a domain reputation systems can't block because it's so popular, spam from these accounts has an advantage in getting past many anti-spam systems.

But some other ISPs and mail service providers with lousy reputations, in the older sense of the word, are not in the top 10. Microsoft had been a fixture in the Spamhaus list and Comcast was once known as a happy hunting ground for botnet herders. Both of these companies seem to have turned the corner.

I could tell Comcast had changed its ways when I saw a discussion on a mailing list I'm on (I'll protect their reputations by not mentioning the name) where users were all steamed that Comcast had blocked access to external SMTP connections through TCP port 25.

This is the single most effective way that ISPs can block spam from coming out of their networks from botnets, and in fact there are other ports that need to be blocked nowadays, like SMB networking. Bots usually send e-mail directly out port 25 to the recipient domain, which usually works because, by default, port 25 is unauthenticated. If you want to use a non-Comcast mail server, you have to use TCP port 587, which is authenticated by default. I don't know for sure, but I'll wager the conventional ISPs on Spamhaus' list, headed up by sistemnet.com.tr (that's Systemnet Telekom in Turkey), give unfettered access to port 25.

Richard D G Cox, CIO of The Spamhaus Project, says the real difference these days isn't just stuff like port 25 blocking ("That's such a 'nineties' (or should that be 'eighties'?) issue"), but responsiveness to complaints, and not just from well-known complainers like Spamhaus.

Cox said, "You see, one of the most difficult things for any organization to accomplish is to see their own operation as it is seen from outside the organization. And that is especially true of IT-related organizations." It's easy to relate to this. And it's not just having the right perspective; lots of organizations probably figure they have their hands full going after the problems they know about. But if they're falling behind, it means they're not dedicating sufficient resources to the problem.

{mospagebreak title=Blocking Spam}

Spammers and other abusers are constantly attacking and testing networks. If an ISP's abuse team is unwilling to listen to outside complaints and take them

---

seriously, then testing will be missed and perhaps develop into full-scale abuse, perhaps a botnet. Now that's expensive for an ISP.

The flip side of port 25 blocking is the Spamhaus PBL or Policy Block List. Absent special arrangements between a user and a service, the user ranges at consumer ISPs can be said not to be legitimate sources for SMTP traffic. The PBL is a list of such ranges that recipients can block wholesale, and then put in exceptions as warranted.

And it's not just spam that gets ISPs on lists like this. The Spamhaus Top 10 also reflects hosting of spam URLs, fast-flux DNS servers and other abusive practices. Look at the Spamhaus complaint list for Google, for example, and you'll see more than one incident related to hosting of spam URLs on blogspot.com. There are also many complaints about docs.google.com being used as a spam redirector.

And since this is a chance to take a dig at it, I'll note that my own ISP, verizon.com, is listed at No. 9 and is the source for the infamous Gevalia coffee spam.

I actually think the spam abuse flood currently sweeping over Google caught the company by surprise, as it did Yahoo and Microsoft in their day. Think of the work it must have taken for Microsoft and Comcast to dig themselves out of this hole. Of course, Microsoft may be No. 11 and I wouldn't know, but Cox said Comcast, in recent years, has become "an impressively proactive ISP and they stomp out a lot of abuse as soon as their people are aware of it."

So ISPs really can turn it around if they're willing to do the right thing. There's no doubt in my mind that the work an ISP does to eliminate this sort of abuse from its network will also improve the quality of experience and support for users, especially its own, but also outsiders.

Security Center  
Editor Larry Seltzer  
has worked in and written about the computer industry since 1983.

For insights on security coverage around the Web, take a look at eWEEK.com Security Center Editor Larry Seltzer's blog Cheap Hack.