(Note: The Deliverability Committee is working on a communication to Spamhaus for further information. We'll keep you posted.)

Subscription bombing, ESPs and Spamhaus, August 15, 2016 by laura in Best Practices

A number of ESPs woke up to a more-than-usually-bad Monday morning. Last night Spamhaus listed 10s of networks, including ESPs, on the SBL. The listings all contained the following note:

Problem description
==========
The newsletter service () is using the referenced IP address to send bulk email. Unfortunately, the said newsletter service is not verifying the email address of new subscribers. Due to this, the service can be easily be abused to "listbomb" internet users.

Problem resolution
==========
To have this listing removed, the newsletter service needs to clean up their email address list and ensure that bulk emails are only being sent to recipients who have previously subscribed to their bulk email service.

In addition, the newsletter service needs to take the appropriate actions to prevent further abuse of their service:
a) Implementing CAPTCHA to prevent automated subscriptions
b) Implementing Confirmed Opt In (COI) to prevent that abusers can add random email addresses to the newsletter service that are not owned by the subscriber
c) Read the documentation below

Further reading
==========
Further information can be found on the referenced links below.

Mailing Lists -vs- Spam Lists:

https://www.spamhaus.org/whitepapers/mailinglists/

Confirmed Opt In – A Rose by Any Name:
https://www.spamhaus.org/news/article/635

Spamhaus Marketing FAQ:
https://www.spamhaus.org/faq/section/Marketing%20FAQs

The first thing most folks did, when confronted with the listings, was reach out to other delivery folks. Is this something widespread or was just my ESP listed? The answer is many ESPs were involved.

Mail has been shooting back and forth all day between a number of players. Many folks reached out to contribute what they know. I think it's a credit to the ESP and delivery community how free different folks have been with information.

(Note: the rest of this post is my synthesis of what I've been told from various sources, including Spamhaus. There are a lot of rumors here, but in the interest of getting things out quickly and calming some concerns I'm going to put this out now.)

Full Word in 3d letters in a green metal mailbox to illustrate junk messages overflowing an email inbox

That seems like a Spamhaus policy change.

I've not heard anything definitively one way or another about a policy change at Spamhaus. I think they're all a bit busy. What I do know is that the listings are based on active abuse happening now. Over 100 addresses were added to mailing lists, many from IPs outside the US. These addresses are being mailed from the networks listed on the SBL and led directly to the listings.

It can't be bad enough for a SBL listing.

Yeah, it can. I've had small subscription bombs in the past and they're pretty damn annoying even when it's only a couple dozen emails. The volumes I'm hearing here are significantly high that people cannot use their mailboxes. One sender identified fewer than 10 addresses each signed up to almost 10000 of their customer lists during a 2 week period. Most of those lists were actually COI, but even if they were all COI it still means tens of thousands of emails sent by one ESP to those email addresses. Expand that out to 10 ESPs and you have hundreds of thousands of emails sent to those email addresses.

Other senders have identified addresses that look to be part of the harassment campaign and are working to block mail to those addresses and get them off their lists.

So is this a policy change at Spamhaus?

Maybe, maybe not. It isn't a policy change in that there is active email abuse coming from the listed networks. Spamhaus has long had the policy to list active systems actively involved in email abuse. It's important to note that many (most?) of these listings are dot-zero listings and aren't actually blocking mail. The goal is to get ESPs to clean up customers and stop the abuse.

What does Spamhaus expect us to do?

Speaking for myself, and without attempting to put any words in Spamhaus' mouth, I think they expect you to stop the abuse currently coming from the listed networks. Right now, ESPs are being used as a conduit for abuse and people's mailboxes are being rendered unusable by unsolicited mail from those networks. This is beyond the permission discussion, this is outright harassment and must be addressed.

How do we do that?

A number of ESPs have been searching through their client lists and identified addresses that have all been added to hundreds or thousands of

lists. These are unlikely to be actual subscriptions and should be removed from lists. If the client insists on not removing these addresses, then I strongly suggest requiring they be confirmed with a positive confirmation (click here to continue receiving mail). These aren't real subscriptions, though, I promise you. And, even if they are, even if that person was a great customer of yours and purchased from every mail they received, they will not be purchasing anything until the volume of their mail gets to something manageable.

The recipients should just unsubscribe.

That's not really possible given the volume of mail. I've heard reports of some victims receiving over 100 emails per minute. More than 1 email per second. I don't know about you, but I can't unsubscribe in one second. This a form of harassment and will render a mailbox totally unusable. Subscription bombs like this are distributed denial of service attacks on individuals. They get so much mail from different places they are unable to use their mailbox for real mail. The hostile traffic can't be blocked because the mail is coming from so many different sources.

What should we look for?

- Addresses that have signed up on many of your lists in August.
- The IP addresses used to sign up those addresses.
- Any other addresses signed up from those IPs.

This will give you a start at looking for the addresses that may be forged into forms. I'm seeing reports that some subscriptions started back on the 2nd and 3rd of August, so going back to Aug 1 makes a nice cutoff point.

OK, we've found them, now what?

Block them. Don't allow your customers to mail them. You, and your customers, are being used as a vehicle to harass people. Then think about things you can do to identify this before it gets to the extreme of a SBL listing. This is the first public incident, I do not believe it will be the last.

Will Spamhaus be addressing this publicly?

I have been told that they should come out with a blog post over the next few days explaining some of the issue. They also know I'm writing about this issue, although they don't know what I'm writing.

What do you think about this?

I think a number of things.
1.I have hand waved over the risk of subscription bombs for years now. I really thought the era of widespread harassment using signups was over. I was wrong. This is an issue and it's something the ESPs, and senders, are going to have to address.
2.I've heard some talk over the last 16 – 22 months that indicated there was some low-level signup forgery going on. There was some discussion about whether or not this was bot activity and how this activity could be discovered and blocked. It never really went anywhere because we didn't have good examples to investigate. We do now.
3.I don't believe this is a drastic shift in Spamhaus policy. They've always been about stopping mail to recipients who didn't ask for it. This is a clear example of abuse and those companies listed are sending large amounts of unsolicited email, if only to a few people. Most of the listings aren't blocking mail and from what I hear Spamhaus is working closely with the ESPs involved.
4.I do believe this incident demonstrates why you need to pay attention to your subscription process and numbers. While in this case neither COI or a welcome series would minimize the effect of the subscription bomb, in less drastic cases you can avoid being a conduit for harassment by limiting the number of emails you send to someone who never, ever responds.
5.Internet harassment seems to be a bigger and bigger issue. I don't know if it's because people are being more open about harassment or if it's actually more common. In either case, it is the responsibility of networks to minimize the harassment. If your network is a conduit for harassment, you need to do something to stop it. I'm working on a couple pieces related to the responsibility of networks to prevent harassment through their services because it is becoming such a major issue.

Overall, I think this should be a major wakeup call for ESPs and senders. You're being used as a conduit for harassment and you have a responsibility to the overall ecosystem and your customers to stop it.

4 comments

steve says

I've seen suggestions that some of the bot driven signups are blog comment spamware that can't tell the difference between a comment form and an email subscription form.

While I'm sure that is going on – and all y'all should do whatever you can to stop that *too* – this is not the same situation, and (at least some of) the recipients are being targeted specifically for harassment (and probably operational sabotage – making a "good guy"'s mailbox unusable can make them unable to do their job).

August 15, 2016, 6:11 pm

Chris says

Having been listbombed back in the 1990s, I shiver to think of how bad it could be these days even with COI.

Note well that at least part of these attacks seemed to be repeated subscription attempts to the same list for the same user (or domain). As such, even with COI, the victim gets hammered with multiple copies of option-confirmation requests.

The first line of defense should be both something like a captcha (which I note many COI systems are already doing), as well as considering rate limiting of how many subscription attempts are permitted to individual recipients (and even domains) to some relatively low number per hour or

per day.

August 15, 2016, 7:35 pm

Stefano Bagnara says

Last month we implemented CAPTCHA on subscription forms for IP being listed on projecthoneypot.org because opt-in request emails generated by bots listed us on senderbase.

This reduced the abusive opt-ins by 90% even if sometimes it will require CAPTCHA to legitimate users.

August 16, 2016, 12:42 am

Paul Kincaid-Smith says

Laura, thank you for synthesizing many observations into a digestible article. You've helped ESPs understand the situation more clearly so they can explore appropriate countermeasures. Kudos to the community for collaborating, and a tip o' the hat to your leadership.