

Re: Is predictable spam filtering a vulnerability?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-06/0418.html>

From: Sean Straw / PSE (PSE-L_at_mail.professional.org)

Date: 06/25/04

Date: Thu, 24 Jun 2004 22:08:14 -0700

To: bugtraq@securityfocus.com

At 10:44 2004-06-24 -0700, John Fitzgibbon wrote:

>*This, IMHO, is a cop-out on the part of the receiving mail administrator.*

You're welcome to your opinion. I don't happen to agree with it.

Many sites employ SpamAssassin and the like to simply FLAG messages and pass them along to the intended recipient, who can then employ their own filter process within their email client (or with procmail, etc) to do as they wish with the messages (which I assure you, doesn't generally involve bouncing any NDNs to the apparent sender, and is so far past the SMTP transaction that result codes aren't part of the picture). Unfortunatley, those users who don't have shell access generally end up having to DOWNLOAD the crap and THEN deal with it. Speak with users who value their time, and you'll find in most cases, they're rather keen on not downloading junk to their workstation.

Then there's the least common denominator: the mass-market internet consumer user. The yo-yo using whatever ISP was cheap the day they went looking to get online, and end up with usernames ending in numeric sequences. They either hawk over their email, or more commonly, check mail about twice a week (if that), and when they're deluged with junk, they select a pile of email in their inbox and hit DELETE to get rid of it all, figuring that if someone sent them something important, they'll send it again, or give them a call. I'm ashamed to say, I've got relatives who fit into this category, and despite frequent reminders, they still do this and send out a followup message to everyone in their addressbook saying "I'm back online, and just deleted all my mail, so if you sent me something important, just send it again."

Reasonably intelligent folk can manage with an archive-and-report mechanism just fine. The rest of the net however, wouldn't know the difference anyway. Most endusers can't comprehend a standard bounce message, and a bounce message referring to a DNSBL or any number of other rejection reasons really sends some people for a spin as they fail to sort WHO refused the mail.

SecurityFocus Bugtraq: Re: Is predictable spam filtering a vulnerability?

On a good ISP, users on the receiving host NOT wanting to subject their email to post-SMTP time mail filtering certainly have the ability to opt in or out of such filtering. So, if the RECIPIENT has opted to silently discard (well, archive and report) mail which has been classified as junk, why should the sender have to be notified?

Of course, what do I know? Up till now, I assumed intelligent folk could manage to send a reply to a listserv without also sending an unnecessary carbon to the original message poster, and if not, at least courteous people would pay attention to the sigline making such a request...

*>You're telling your clients, "Here's the list of 100's of emails per day that
>we silently ignored on your behalf, now you go figure out if you needed any
>of them".*

Er, as versus bouncing messages to the sender, in which case the recipient doesn't even KNOW that someone tried to send them anything? That logic is no better. If the sender knows of no other way to reach the intended recipient, how is it that they're supposed to get through?

Does the same logic apply to twit filters? If someone were on a mailing list and BOUNCED messages because of the author of those messages (and yes, this does happen), I'd consider that abuse and kick the filtering user -- either those messages are bouncing to the admin (who sure as hell doesn't need the extra crap), or to the author, who was posting to the LIST, not to the individual recipient.

The archive and report approach means that the intended recipient HAS CONTROL over their email -- if something was misclassified, they can recover it from the archive, greenlist the sender, and get on with life. Compare that to someone trying to email them something and getting a bounce and not necessarily having any alternate method of establishing contact.

For me, glancing through the report takes barely over a minute each morning, and is a *LOT* less aggravating than pouring through some mailfolder and finding it peppered with spam. I personally find that when there are false positives, they're worthless junk anyway -- mumbling idiots on a listserv using an abundance of punctuation in the subject line, HTML only email, and a flakey email address, etc, and thus aren't even something I'd have elected to read had it shown up in my mailbox to begin with, so I spend virtually no time recovering messages from the archive.

*>For all the good that does, you may as well just deliver everything
>and let the user sort through their inbox.*

The user isn't forced to deal with DOWNLOADING the crap in their regular mail stream, and yet they retain control over recovering from false positives. This is a cop out?

This beats the turd out of the moronic "prove you love me" schemes where in order to send a message to someone (who may have emailed you directly to

Re: Is predictable spam filtering a vulnerability?

SecurityFocus Bugtraq: Re: Is predictable spam filtering a vulnerability?

begin with, so you're actually REPLYING to them), you've got to respond to some automated system at their mail server that insists that if you're not a spammer, you've got the time to manage THEIR spam problem for them. Even EARTHLINK does this. I don't bother to waste my time with them – when met with a PYLM autoresponder, I just quit corresponding — invariably, it seems to be when I'm wasting my time answering a question someone sent me out of the blue anyway.

>A 5xx provides timely feedback to legitimate senders, (without bouncing to >faked addresses), so that they can find another means to contact the >receiver.

What on earth do you mean "without bouncing to faked addresses"? Sure, totally bogus addresses won't get bounces (not that the mail system won't attempt to deliver them – and I can attest that doing so CAN in fact get you blacklisted – yahoo for instance dynamically blocks all mail from your server after you've attempted to deliver mail to a sufficient number of invalid recipients – not just in ONE message, but a plurality of messages) – but Joe-Jobs and other forgeries get FLOODED with bounces for messages THEY DID NOT SEND. As an administrator of several mailing lists, I can tell you that getting bounces from A/V systems that send advisories to the From: address on messages containing viruses KNOWN to employ forgery is rather aggravating.

*>Archiving the dropped mail *and* terminating with a 5xx would be a much >better approach.*

I believe your opinion of how much better this approach is would be dramatically different once you've had actual experience cleaning up after a joe-job.

Perhaps it'd help if you looked at the archive and report approach from another perspective: what if the user received the email but didn't bother to open it because the subject/etc looked like spam anyway? There's nothing that says that just because delivery was successful that someone will actually READ the email, so why should the user have to download it to their system? If they have ready ACCESS to the messages, it is virtually the same as if it was delivered to their mailbox, and as a new user becomes more familiar with the archive-and-report mechanism and finds that it virtually never has a significant false positive, checking it becomes more an issue if you were expecting a message (or received a phone call about one) that you didn't see in your inbox.

This is my last post on this topic – while spam is a problem many have an interest in dealing with, we've gone *FAR* afield of any security issue related to sending or not sending bounces, and there are much better lists for discussion of spam fighting techniques.

[big snip]

SecurityFocus Bugtraq: Re: Is predictable spam filtering a vulnerability?

Bugtraq has a webarchive, so wholesale copies of previous messages seem a major waste of bandwidth, esp when you factor the number of recipients on this list, each receiving a custom delivered copy of the message.

Please DO NOT carbon me on list replies. I'll get my copy from the list.
Founding member of the campaign against email bloat.