Full Version: Can I report Bouced Spam to Spamcop

IHateSpam Aug 4 2004, 12:52 PM

Good day,

Some moronic spammers have gotten a hold of my domain name and are using it as a the sender source (IP's used and mail server aren't mine so I'm pretty sure that I'm not sending it).

In addition to getting nasty emails from people demanding that I stop spamming them, I'm also getting a lot of bounced email being delivered back to me (spam rejected, user known, mailbox full, etc).

So my question is: Can I report this email to the @spam.spamcop.net email address (basicly just by forwarding it).

I'm a bit nervous that my IP address could somehow been interpreted as the sender of the source email) since the message has been bounced back to me; and so have been extracting the source email (when included) and posting it into the web submission form..

The problem is that I've gotten at least 100 bounce backs today alone and the whole process is becoming very tedious

Any one help alleviate my fears?

Thanks

Paul

turetzsr Aug 4 2004, 01:13 PM

Hi, Paul,
...In a word: no, you can't. See SpamCop FAQ: On what type of email should I (not) use SpamCop? (the paragraphs labeled "Bounces).
...IIUC, you are the victim of what is called a "Joe Job" (see entry labeled "joe" at The Net Abuse Jargon File).
...The people who are flaming you are ignorant. Savvy e-mail users are aware that "From" addresses in Internet headers (which is where they are most likely seeing your e-mail address) can be easily forged.
...The good news is that these kinds of "attacks" usually stop after a short while, as the spammers move on to other victims.

dra007 Aug 4 2004, 01:15 PM

I have been getting a lot of bounces recently myself. Seems to be a recent trend and was discussed in more than one thread here. Bottom line is that it is against SpamCop policy to report bounces.

You also have to be careful opening some of these bounces, as most I have recieved recently contained MIME-exploits which can damage your system files!!!

Good luck!

Miss Betsy Aug 4 2004, 04:13 PM

"Joe-Jobs" are generally taken to be malicious. This kind of using a domain name (or an email address) is not intended to hurt the owner, but just so the spammer is harder to trace - spammers don't care who is inconvenienced or hurt by their actions.

However, if you are getting angry emails, it is a good opportunity to enlighten those who don't know about forgeries and to direct them how to do something positive. You can write an 'educational' email back about how 'From' is almost always forged, etc. and also put a disclaimer on your website.

There are others who have had similar problems and lots of people who think that these kinds of bounces are as bad as spam and ought to be reported. However, it has to be done on your own (you can use spamcop to find abuse addresses by entering just the headers and being sure to cancel the report.)

If you are getting loads, then just doing what can be done and filtering the rest to trash is probably all you can do.

Miss Betsy

turetzsr Aug 4 2004, 04:24 PM

> **QUOTE(Miss Betsy @ Aug 4 2004, 05:13 PM)**
>
> "Joe-Jobs" are generally taken to be malicious. This kind of using a domain name (or an email address) is not intended to hurt the owner, but just so the spammer is harder to trace - spammers don't care who is inconvenienced or hurt by their actions.
> <snip>

...Thanks for correcting my misunderstanding!  <g>

Wazoo Aug 4 2004, 04:44 PM

I'm going to suggest that Miss Betsy was typing too fast and forgot to insert one word ....

.... This kind of using a domain name (or an email address) is not intended to hurt the owner ....

I'm thinking that the word "forged" didn't make it to the screen ....

IHateSpam Aug 4 2004, 10:16 PM

Evening all

Thank you for your replies

I have sent some Notifications to some of the ISP in charge of the network segments where the spam comes form (manually reading the smtp headers and then using whois to try and identify who's managing the ip address); with little success (out of the 10 I sent manuall) with only one replying to say it wasn't their network segement; but hasn't replied back to my 2nd reply showing whois data confirming that their email addresse is attached to the IP range in question.

In addition, alot of the IP ranges in use are listed as being managed by ARIN.NET (when Whois'd) and they've responded that they're not responsable for the IP in question (even though they're identified as the contact person under whois - go figure eh)

Just a little more clairification on Bounce backs.

If a spammer sends a spam type email to someone with a forged (but valid) source email address which is then bounced back to the the forged sender address, then is this still not spam?

It usually contains the spammers source message (which usually contains all the smtp headers including the source IP addres)

I'm not saying that the bounce back is spam (Bounces are great [better than sliced bread] as I know that my domain name is being used in forged emails, and most cases the original email is included so I can figure out the Source IP)

I was kinda hoping that Spamcop would be able to process the spammers address from the bounced email from within the original source attachment (I'm able to do it). Then have the Web interface confirm that what it processed is what should be reported (to help stop false submissions)

If I were working for spamcop, I'd be interested in the people who are getting bounce backs.. It be a great source of fresh spammer information. Look at me. I have 200 + bounce backs which I want to investiage and inform the correct persons to whats going on (its quazi personal now  . How many people would spend the time to report spammers (not too many as I'm just as guilty of just deleting them when they come in without even reading them).

Anyhow, what I tried to do (but gave up after about the 10th email) is extract the original spammer email (Using View message source on the bounced email) when its included in the bounce back email (usually as an attachement) and then manually submitting it via the spamcop web interface.

As it stands, I must have about 200 bounced spammer emails (alot of different source addresses).. Now lets say that 1% are being bounced back to me.. that would mean that the spammer could be sending at least 20,000 emails (most likely a lot more) using my domain name. Now how many of thoses people receiving the spam will report it (I'd guess not too many)

Thanks for listening

Paul

IHateSpam Aug 4 2004, 10:28 PM

> **QUOTE(Wazoo @ Aug 4 2004, 05:44 PM)**
>
> I'm going to suggest that Miss Betsy was typing too fast and forgot to insert one word ....
>
> .... This kind of using a domain name (or an email address) is not intended to hurt the owner ....
>
> I'm thinking that the word "forged" didn't make it to the screen ....

Hi Wazoo,

Never thought it was personal.. Usually when spam gets personal, the attacker make the spam look like it came from you.. I had a client who had a x-worker who was spaming on behalf of the company.. It was real nasty (False quotes, email of viruses).. Eventually they paid 'em off to leave 'em alone cause no one else was able to do anything about it.. We had proof (IP's Server logs, etc) ISP wouldn't do anything, cops wouldn't do anything.. So Eventually they had a lawer talk directly to 'em and some form of arrangement was done. Too bad they never got back the hardware that the x-worker stole.

I was just hoping that there was some way (unknown to me) to get this to stop quickly. I think this is the 3rd time that my domain has been used in the last few years.

Getting a little fed up with not being able to easily do something with the spammer information contained in the bounce backs, and am getting tired of writting "Dear <Insert Name Here>. I'm writing to inform you that I am not actually spamming your email address.. Someone is forging the source email address using my domain name.. Please check the following links to help identify the perpertrators" emails..

Paul

Wazoo Aug 4 2004, 11:25 PM

Fearing that this might turn into another one of my novels .... have to start with the initial problem in the these bounces are not handled in a "standard" fashion. Some ISPs kick back the entire original e-mail with an added rejection note, some send the rejection note with a bit of the original e-mail, some simply send a rejection notice.

Now we jump to Julian's tool set. Originally written from the perspective that an e-mail would look like an e-mail, the user submittal of this e-mail would still have it looking like an e-mail, and things would distill the pertinent data, and the reports would end up in the hands of someone that would take real action. As in the early days of the 'net' , instructions were sparse to non-existent, so those that used the tool-set generally "knew" at least some of the background on how e-mail and NNTP worked. Time moved on, SpamCop became more popular for varying levels of experience users, at the same time becoming a target for the spammers to try to outwit.

This leads one to the "gound rule" for s spam submittal, that it look like an actual e-mail (going to frop NNTP for now) ... When a submittal arrives that doesn't look "right" .. the questions include; did the user screw-up, did the spammer mangle something, was data dropped during any of the operations occurring between the user "reading" the spam and

handing the spam to the parser; is there something in the code-base that's screwed up, ... From the programming side, things are much easier when the decision is made that if it doesn't have all the necessary parts, in the right order, parsing is halted rather than risking making / selecting the wrong "notifies" about a wrong item.

The problem with these bounces (reaching back to the first paragraph) is that getting a good and accurate parse out of it with correct targets identified goes directly to the experience and knowledge of the submitting user (and again, assuming that the actual / original / complete spam was included within the bounce) being able to extract the actual spam for submittal. Unfortunately, there are too many users that don't have this knowledge, don't spend the time, screw up and run on autopilot, etc. that were generating too many reports to go to the wrong targets. The only solution is the simple ban on reporting bounces (programming again brings up the decision points needed to sort out why the e-mail doesn't "look right" .. too many headers, too many blank lines in the wrong spot, how mangled did the actual spam get during all the processing - line wraps, word / address divisions, etc. ...)

Now all that said, if you do know what you're doing, can see what you've actually got, then yes, you can still use the parsing tool to help you find the right targets, but the current rules are to then cancel that report and send your own complaint to these targets.

ARIN (American Registry for Internet Numbers) in general assigns the blocks of IP addresses. If the IP address you're looking up references that it's controlled by ARIN, did you then go to the next level and use ARIN's whois to get to the next level of actual assignment? http://www.arin.net/whois/index.html This might be a bad analogy, but complaining to ARIN would be something like complaining to Ford Motor Corporation about the problems you had with a Ford that you'd rented from AVIS ... Granted, the car may have been built and even delivered to AVIS by Ford, but that burnt-out headlight is clearly an AVIS problem ....

Here's hoping that you can find a glimmer of something good in this (but guessing not <g>)

IHateSpam Aug 5 2004, 08:40 PM

Hello

Just a small update.. Up around 4200 bounced spam messages so far

I'm hoping this will end soon and that postmasters aren't looking to add my dns name as a spam filter ;(

I'm actually thinking about writing a parser my self in perl to parse out the source IP on my collection of bounced email to try and see If I can identifty all the IP's being used

Oh well. Back to fighting with my in-box

Paul

BrianL Aug 24 2004, 09:56 AM

Please forgive my playing the Devil's advocate.

Is it not possible that spammers have been clued in to the ban on reporting bounced messages, and are now intentionally forging their messages to look like bounced messages?

As evidence of this I note that almost all the bounced messages I get seem to come from

blocked domains, and I seem to get a lot more bounced messages than I ever used to. Also, I think all of these bounces contain the entire original message, whereas many legitimate bounced messages from months/years ago contained only a snip.

How can I tell whether a "bounced message" is really bounced - versus just made to look that way?

Wazoo Aug 24 2004, 10:03 AM

I'll just point out that it's a known fact that the SpamCop newsgroups and Forums have long been read by some spammers. Analyzing spam for source, construction, and content simply boils down to doing the research and learning what the data bits are in those spams. Start by looking at your "good" e-mail, compare to the "bad" stuff and search out the differences, then figure out "why" the spammer did things different <g>

BrianL Aug 25 2004, 03:09 PM

However sincere and advanced you may be, your answer is less than helpful. I am well aware that spammers read these discussions.

I am already all too familiar with determining the likely IP of the originating source.

I don't know what you mean by "good email" and I don't know what you mean by "bad stuff". I'm not particularly interested in "why" spammers do things. I don't know what you mean by "different" - different from what?

For example, suppose I have a message that appears prima facie to be a bounced message from a Joe job (fraudulently using my e-mail address). I determine the originating IP from the Spamcop automation. The likely originating IP is one that is currently listed on one or more blacklists. Isn't it entirely possible that this message was never bounced at all, and in fact came directly from the spammer in exactly this form?

Put yet another way: Couldn't a spammer intentionally send all his SPAM to the same invalid address of an ISP who dutifully reports bounced e-mails, changing only the reply-to e-mail address for each message (to match the real intended recipient)? Wouldn't this spammer have the effect of all his SPAM being delivered to all of his intended victims, in a form that is identical to a bounced message, and in a format that is not reportable through SpamCop?

Perhaps I really shouldn't have posted this thought here?

Please reconsider more thoughtfully.

Wazoo Aug 25 2004, 03:19 PM

> **QUOTE(BrianL @ Aug 25 2004, 03:09 PM)**
>
> However sincere and advanced you may be, your answer is less than helpful. I am well aware that spammers read these discussions.
>
> I am already all too familiar with determining the likely IP of the originating source.
>
> I don't know what you mean by "good email" and I don't know what you mean by "bad stuff". I'm not particularly interested in "why" spammers do things. I don't know what

> you mean by "different" - different from what?

All that dealt with reading and understanding headers. I'm confused that you state that you understand all that, but are confused over my terms "good" and "bad" e-mail ...???? good = stuff your Mom sent you ..... bad = some lowlife crap .. where do I go from here?

> **QUOTE**
>
> Isn't it entirely possible that this message was never bounced at all, and in fact came directly from the spammer in exactly this form?

Yes it's possible. Happens every day.

> **QUOTE**
>
> Wouldn't this spammer have the effect of all his SPAM being delivered to all of his intended victims, in a form that is identical to a bounced message, and in a format that is not reportable through SpamCop?

Yes, thus the pointing out that spammers read up on how to get around the various blocks, traps, filters, and reporting tools. Again, I don't see what I missed before.

> **QUOTE**
>
> Perhaps I really shouldn't have posted this thought here?
> Please reconsider more thoughtfully.

I'm still a bit lost. Yes, this stuff is done. I'm not sure how much more thought you need on this. If it's just that you're ticked about not being able to report it, that's something you'll have to take up with Julian himself, realizing that a lot of his "rules" stem from folks that don't know what they are doing or take no care in the results.

By the way, the simple forging of address data is not the same as a joe-job.

Miss Betsy Aug 25 2004, 05:56 PM

> **QUOTE**
>
> For example, suppose I have a message that appears prima facie to be a bounced message from a Joe job (fraudulently using my e-mail address). I determine the originating IP from the Spamcop automation. The likely originating IP is one that is currently listed on one or more blacklists. Isn't it entirely possible that this message was never bounced at all, and in fact came directly from the spammer in exactly this form?
>
> Put yet another way: Couldn't a spammer intentionally send all his SPAM to the same invalid address of an ISP who dutifully reports bounced e-mails, changing only the reply-to e-mail address for each message (to match the real intended recipient)? Wouldn't this spammer have the effect of all his SPAM being delivered to all of his intended victims, in a form that is identical to a bounced message, and in a format that is not reportable through

> SpamCop?

IIUC, you have two different examples here of how a spammer could get a spam message delivered past different filters.

However, it all depends on what you mean by 'orginating IP address' - if you mean the 'spam' originating address, then there is no surprise that it is coming from an IP address that is on several blocklists. OTOH, 'bounces' from IP addresses that are listed on blocklists could be that the policy of the IP addresses is to email bounce undeliverable mail, have not listened to complaints, and in consequence, are listed because they have been sending email to spam traps since often spammer mailing lists contain spam trap addresses - if you mean the originating IP address is the address from which the bounce came.

In the second example, it certainly is possible for a spammer to determine that an ISP is still using the 'email bounce' and change the reply to address to match his mailing list so that his spam gets delivered (SPAM gets eaten; spam gets delivered. SPAM is the registered trademark for the luncheon meat. Hormel has been very indulgent about the use of the word 'spam' for unsolicited email and serious spamfighters should respect the difference). However, the person to report to is the ISP who is still using email bounces.

There are two possibilities for reports in every 'bounced' spam: one - a report to the ISP who 'bounces' it to complain about their use of an outdated undeliverable message protocol and two - a report to the ISP of the actual spam (if the headers are included in the bounce). The latter report is for forgery of your email address. Neither report is a report of UCE - which is partly why spamcop does not allow the reporting of bounces. The main reason, however, is that the parser just can't assess all the different possibilities in a reasonable length of time and with reasonable accuracy.

IMHO, spammers don't deliberately try to bounce spam messages because I don't think there would be enough return from buyers. If only 1% buy, then the percentage who would buy from a bounced email would probably be miniscule. I think they don't care whether 50% of the spam run gets bounced around. (though my theory is that a certain percentage of spam doesn't really try to sell anything - like the virus authors, some people probably get perverse pleasure from just evading the filters).

I don't know whether this viewpoint helps you to understand spamcop's ban on bounces or not.

Miss Betsy

clytie Aug 26 2004, 03:44 AM

Thankyou for all the information in this thread.

I do feel for Paul, and for others in this position: I've had the odd bounce before, but not a flood, like today.

Fortunately I could Jabber my husband at work, our local ISP, and ask him to block part of the message text (which was identical in all cases), and the flood dropped to a trickle (auto-aways and those which snip the body text).

All the same, that isn't doing anything about the spamming, and from what you have all said above, there doesn't seem to be much we can do.

I haven't received any personal email (flames, complaints), my flood consisted of auto-bounces and auto-aways ("I'm away right now, not reading my email" etc.). I doubt very much if writing to the ISPs auto-bouncing would achieve anything, but I'll give it a go.

Edit: I was about to do so, discussing it with my husband, when he said that sending a message to the perceived sender when an email is undeliverable is in the RFCs. So it's not only defensible, it's almost mandated. He said, if it's hard for a human to work out if a header is forged, what hope does an ISP have, working automatically with thousands of them? Admittedly, the relevant RFCs were written before the spam/virus plague, but there doesn't seem to have been an update to deal with it.

All of this out of my sphere, but leaves me wondering if there is _anything_ I can do. 
end edit.

What horrifies me (and I'm sure upsets others in this position) is the thought that probably thousands of emails are bothering innocent people, with my name on them. It's really amazing how many people spammers can annoy, when they put their, um, wits into it. Strange use of resources, however sparse.

Thanks for the info above: it really helped to be able to come here and have this thread available.

from Clytie <stirring her inbox around cautiously with a stick>

Miss Betsy Aug 26 2004, 06:32 AM

> **QUOTE**
>
> I was about to do so, discussing it with my husband, when he said that sending a message to the perceived sender when an email is undeliverable is in the RFCs. So it's not only defensible, it's almost mandated. He said, if it's hard for a human to work out if a header is forged, what hope does an ISP have, working automatically with thousands of them? Admittedly, the relevant RFCs were written before the spam/virus plague, but there doesn't seem to have been an update to deal with it.

Your husband is correct that there is an RFC; however, although the RFC has not been revised (AFAIK), the problem has become so widespread that clueful ISPs are no longer using 'email bounces' One reason is that some part of those thousands are hitting spamtraps and they are getting listed (not just by spamcop). Ditto with auto bounces and virus notifications.

You can't report it through spamcop, but it is certainly worthwhile to report it to the offending ISP - particularly if you point out that you are doing them a favor by notifying them. I always point out that the number of real undeliverable mail perhaps lost is miniscule compared to the annoyance caused by the bounces to innocent people. And mention that it (and out of office auto replies) are some other things that have been spoiled by the spammers.

I don't think anyone answered me when I asked this before, but I don't know why the ISPs can't run the 'bounce' emails through a spam content filter set on high before they send them and dump those that don't pass. Also, an ISP could write a parser for its own use - in fact some of the bounces that I have received actually had the correct IP address added. The reason that there isn't another available for other people on the web is spamcop's ability

to deal with many different header configurations. A private one also doesn't have to send reports or look up abuse desks. That is one reason why it is so stupid that ISPs send email bounces to the 'returnpath' - if they feel that they can't dump undeliverable mail, there are ways to send it to the proper place - it just costs more.

I believe that even aol (one of the worst offenders) has agreed that it is not a good idea to use email bounces.

Glad that your ISP was so helpful. <Knock Knock> I haven't had a flood. Then it would be difficult to notify everyone. At one time, the advice was to complain to the originating ISP about 'forgery of your email address' and that sometimes the originating ISP would listen while it would not stop spammers. I expect that advice is out of date just like the RFC.

Miss Betsy

turetzsr Aug 26 2004, 09:10 AM

...Also see Pinned: FAQ Entry: Why am I getting all these bounces? and SpamCop FAQ: Why are auto-responders (and delayed bounces) bad?.

BrianL Aug 26 2004, 12:00 PM

To all who replied as a result of my inability to understand: Thank you.

I still only understand about 80% of the responses, but I get the gist of it: spammers are winning, and there is very little we can really do.

Miss Betsy: Thank you for pointing out the distinction between the trademark and the annoyance. This was news to me. I shall type "spam" in the future.

I was spoiled by SpamCop's amazing false positive rate of only 5 in 45,000, coupled with a false negative rate of only about 4% for my address. But this morning the bounced e-mails really started flooding my inbox, at a rate as high as 15 per minute at one point.

For future reference, I am not ticked at Julian or anyone at SpamCop. Just frustrated and depressed by my inability to solve or productively address even my personal spam problem.

Miss Betsy Aug 26 2004, 06:58 PM

> **QUOTE**
>
> Just frustrated and depressed by my inability to solve or productively address even my personal spam problem.

Don't let it get you down. It certainly seems that way when the flood comes in, but if you look at the history of spam, the good guys are steadily winning and driving the spammers into desperate measures like using viruses to spread their spew.

Usually the flood doesn't last long so do what you can to control it. And since it is an ever-increasing phenomenon, measures to counteract it will start to be established.

Miss Betsy

clytie Aug 27 2004, 03:34 AM

Thanks for the responses. My husband did say that smarter ISPs don't bounce, but his point was that it's hard to criticize the others doing something that's in the RFCs. I take your point that we can still suggest that they don't do it.

I think one of the worst things about this, as Brian says, is the feeling of powerlessness. Your inbox is swamped, people are attaching your identity to acts of harrassment (which I firmly believe spams are) and you appear to have no decision power at all. Just wait it out, or change your address.

Please point me to any link that shows we are winning against spammers: I need the moral lift.

from Clytie <staring glumly at the huge pile of bounces and aways, clogging her mail pipe>

turetzsr Aug 27 2004, 10:45 AM

> **QUOTE(clytie @ Aug 27 2004, 04:34 AM)**
>
> Thanks for the responses. My husband did say that smarter ISPs don't bounce, but his point was that it's hard to criticize the others doing something that's in the RFCs.

...Fair enough -- until someone points out why it's a bad practice. After they know, I would expect them to stop, forthwith! <g>

> **QUOTE(clytie @ Aug 27 2004, 04:34 AM)**
>
> I take your point that we can still suggest that they don't do it.
> <snip>

Miss Betsy Aug 27 2004, 12:42 PM

When spamcop first began, there were many, many ordinary businesses who thought sending email ads were a great idea. Now, there are few, if any, legitimate businesses who would send unsolicited commercial email (there are still a few, but they get clued in very quickly that unless you have confirmed subscription list, you are going to have problems). Only a couple of years ago there were numerous ISPs who didn't respond to reports of spam or didn't have TOS's and AUP's - now they all do. Spammers now have to use Chinese ISPs or trojaned machines to deliver their spew. Even Comcast finally caved in and, at least, said they would do something about the hundreds of trojaned machines that were sending spam. I haven't seen as many from Comcast as I used to (but that doesn't always mean anything - perhaps the list I am on has changed hands).

Since more and more people are dealing with flooded inboxes with bounces, sooner or later the clueless ISPs will find themselves on blocklists and start listening up. Perhaps even doing something about the source.

Just remember that the squeaky wheel gets the grease. I have been saying forever that if the techie types would only enlist the 'average' spam recipient in demanding blocking that the 'tipping point' would come and spam would no longer be a viable occupation. ISPs have realized that reduction of spam is what most of their customers want. There are certainly

more legitimate email users' dollars than spammer dollars.

Miss Betsy

clytie Aug 27 2004, 09:45 PM

Thanks, Miss Betsy, that is encouraging. What I really had in mind was spammers in stocks, having rotten tomatoes thrown at them (eggs are too expensive nowadays), but what you say is helpful if less satisfying.

from Clytie

Merlyn Aug 27 2004, 11:13 PM

> **QUOTE(clytie @ Aug 27 2004, 10:45 PM)**
>
> What I really had in mind was spammers in stocks, having rotten tomatoes thrown at them

It won't be long.....

dbiel Aug 28 2004, 12:03 AM

> **QUOTE(Merlyn @ Aug 27 2004, 09:13 PM)**
>
> It won't be long.....

Nice dream, I wish it were true!!!!

K.J. Petrie Sep 14 2004, 07:57 AM

> **QUOTE(Miss Betsy @ Aug 27 2004, 12:58 AM)**
>
> Don't let it get you down. It certainly seems that way when the flood comes in, but if you look at the history of spam, the good guys are steadily winning and driving the spammers into desperate measures like using viruses to spread their spew.
>
> Usually the flood doesn't last long so do what you can to control it. And since it is an ever-increasing phenomenon, measures to counteract it will start to be established.
>
> Miss Betsy

I think you're missing the point of what Paul is (and now I am) saying.

We (taking my understanding of his position from his original post) do not find bounced spam a problem. I would be horrified if ISP's stopped bouncing it.

What I do find a problem is that my domain is being defamed, and my potential connectivity also, if the domain gets blocked on a widespread basis. The domain is my online identity - it's even a Registered Trade Mark in my own country - and that identity has been stolen. I currently spend 2-3 hours every day trying to defend it, and to no avail because the spamvertised sites are in China. I need my life back from these crooks, or I will go under.

The problem began at the turn of the year, and I reported it, and the Chinese hosts shut down the websites, and the problem went away for six months. Then, in July, it started again. I complained and within a couple of days the sites were unreachable and the bounces stopped. For the next month I was spammed with empty E-mails, about 30 a day, which I filtered on subject. The day these stopped (31st August) the bounces began again. I complained to the ISPs, but this time they've found hosting companies who don't care, and I don't know what to do.

I can't fight this on my own. I need the help of fellow-sufferers, and I thought Spamcop was the obvious place to look, so you can imagine my dismay at being told in the FAQ the spam was not my problem. It certainly *feels* like my problem. I would suggest it's far more damaging and distressing than ordinary Spam. For the second day running it's lunchtime and I haven't even stopped for breakfast yet, because I have to defend my name.

I understand there may well be technical problems which make it difficult to handle bounced Spam, but it's an even bigger menace for the victims than ordinary Spam. Please, someone, come up with an answer. Point us in the right direction, at least.

KJP

StevenUnderwood Sep 14 2004, 08:16 AM

> **QUOTE**
>
> What I do find a problem is that my domain is being defamed, and my potential connectivity also, if the domain gets blocked on a widespread basis.

How is your domain being defamed by having it forged as the sender of spam. From my conversations with people, most now know that the from address is usually forged in junk mail (except for MicroSoft apparently, see thread in Lounge). I have not seen an email at my place of business complaining about a spam they received because our address was the sender in over a year now.

"Domains" do NOT generally get blocked, IP addresses (and maybe ranges in some bls) do. If your IP is not sending spam, the likelyhood of it being blocked are extremely low. With the spamcop email system and other systems (I use Postini at work which also has this feature), someone may place a domain on their personal blacklist but I personnaly only have 1 entry in my blacklist and none on my company blacklist.

> **QUOTE**
>
> I currently spend 2-3 hours every day trying to defend it, and to no avail because the

> spamvertised sites are in China. I need my life back from these crooks, or I will go under.

This situation sounds more like a Joe-job (using your domain name to sell their junk) than the simple bounces most people get. More description of what is being received is needed here, I think.

Wazoo Sep 14 2004, 09:03 AM

> **QUOTE**
>
> I understand there may well be technical problems which make it difficult to handle bounced Spam, but it's an even bigger menace for the victims than ordinary Spam. Please, someone, come up with an answer. Point us in the right direction, at least

Pointing to the "right dierection" is also part of that package of "technical issues" ... Strangely eough, I just spent over an hour on the phone last night with one of my brothers, it seems his name had been drawn out of the hat and he wanted me to tell him how to handle the MAILER-DEAMON e-mails he was now getting ... 3,500 the first connection .. after deleting the crap out of those, he then reconnected and found he had to wait for the next 450+ to download ... this on a 56k dial-up ...

Here's the basic problem ... pick one spammer, who is going to deliver the 250,000 e-mails some other idiot has paid this spammer to deliver .. spammer fires up his neat-o software to handle that high-speed e-mail advertising/marketing delivery process ....

This software includes the functions of using e-mail addresses already culled from somewhere else, generating more "new" e-mail addresses by using the "names" from that culled list and attaching those names to other domain names .. thus "doubling" the original list on the first pass ... toggle the domain name again, now the send-list has tripled ... That the addresses aren't any good is of no consequence, as the contract only specified "send out 250,000 e-mails" ....

The spammer would like to not have to change his/her own account set-up all the time, so this outgoing e-mail traffic isn't going to use his/her e-mail server to get out .. so spammer pulls up that list of compromised e-mail servers that someone else has found/hacked, pumps some spam through that compromised e-amil server. To speed things up, the list of compromised machines that have been found/hacked by someone else that now have the capability to spew forth quantities of e-mail is pulled up and these systems are tapped into .... This type of activity continues until that spam run is done, then the next get-rich-quick-idiot's spam run gets put into the queue.

Somewhere in the process, a random generator, another list, or just because you complained to a spam-friendly ISP that passed on your complaint to this spammer ... your name comes up as part of the "hide the source" bit and now these spams are going into the world with your address in the From: line.

You start getting the bounces from the systems that follow the rules of being nice that date back to the origins of the "net" .. letting "you" know that you'd obviously mis-typed the address or got mixed up when you typed in the To: address. Ok, you could send an e-mail to an admin at that suystem and tell them that time has moved on, things have changed, and the days of bouncing e-mail back to what's seen in the From: line is something that's been destroyed by spammers and should cease. Maybe you'll convince that ISP.

The problem is that your bounces are coming from all over ... and now you're stuck with trying to work with the different types of bounces (some have the complete original e-mail attached or in-line, others only provide a few header lines to show the "wrong" address, others give broken crap as maybe there was also a virus/trojan in the spam that got manipulated/mangled in the process of handling ..)

Places to send your complaints now include stupid/lazy ISPs, compromised computers owned by Mr. & Mrs. Clueless in Seattle, Joe 6-pack in Witchita, on and on .... but the point is, one spammer is responsible for the spew, but your receipt of bounced e-mails might include 3,000 different sources from that 250,000 spam delivery run. How much time do you want to spend on trying to track down and notify that list, noting that most, like the compromised "home" computers will never see the "postmaster" e-mail and whether their ISP gets involved is a coin-toss ...

Yes, the SpamCop parser can be used to track down the source (for use in making your own manual complaint), but then one is back to the knowledge of the reporter as to selecting what part of the headers to feed the parser, and that's even making the assumption that what's needed was included in the bounce (if we're talking about reporting the spam source) .... and unfortunately, this scenario hasn't worked all that well, too many folks simply submitting the whole lot and hitting "Send" ... Thus the official words of "Bounces will not be reported via SpamCop" these days.

Solutions? None good, short of finding the spammer and changing his/her outlook on life and such ...

Whitelist known good addresses, rest goes into a bitbucket - not a business deal
Filter incoming based on something (like MAILER ...) but not all matches, so rules start getting big
Take the time to try to educate those systems doing the bouncing based on bad From: line contents
Change your address

Just a few of the many possible "solutions" .. but I suspect you'll agree, none of them are good ...on the other hand, it's pretty rare that one can get over the $250,000 threshold to get the FBI involved in pursuing the cause of all these problems ... the lowlife spammer ...

dra007 Sep 14 2004, 01:33 PM

My problem is that a lot of if not most bounces I get daily contain virus attachments or mime exploits. That is what makes it a nuisance, not knowing when one of them will make it past the various protection and defanging stages.

K.J. Petrie Sep 15 2004, 06:31 AM

> **QUOTE(StevenUnderwood @ Sep 14 2004, 02:16 PM)**
>
> How is your domain being defamed by having it forged as the sender of spam....
>
> "Domains" do NOT generally get blocked, IP addresses (and maybe ranges in some bls) do.

Thanks, that may be true in the Unix world, but most people I know use Outlook Express or something similar to receive their E-mail. Filtering by domain name is all they have.

In the majority of cases that won't matter, because I'll never have cause to E-mail them, but among those millions setting filters against my domain, may be friends who don't recognise it or people I am yet to meet.

My social life is already being disrupted by friends not receiving my E-mails, and while I've been writing this my stockbroker has just phoned because a transaction nearly went astray when they failed to receive my instructions (that represents a fifth of my life savings). AoL blocked my domain at the beginning of the year. So I think it does happen.

I think the term Joe-job may well apply to what is happening here, though I'm not an expert on Internet slang (sorry - technical language). Someone is sending Spam advertising prescription drugs for sale at websites hosted at various Ips in China (Chinanet, Unicom), pointed to by a variety of domains which change every few days. (The registrants are giving postal addresses in Poland, Benin, or wherever, though their E-mail addresses look similar.) And yes, the From: header has a fictitious name followed by a random string @instabook.com (which is my domain name). The Spam originates from various networks all over the world, and one ISP has told me the sender is a virus, so it's probably trojanised machines being used to send it.

I only get to know about the Spam that bounces, but that's the tip of an iceberg, because I don't believe the Spammer is only sending a dozen or so a day. The vast majority are not being bounced. Whether they are getting through or just being deleted I can't say. If this activity has resulted in ISPs not bouncing undelivered mail the spammers have already won, because E-mail has ceased to be a reliable system where we can be reasonably confident our messages have been delivered.

I think it's defamatory to have one's name associated with antisocial and possibly illegal activity. It certainly feels that way.

And you're right. I haven't got the time. Which is why I was hoping there were others who might have the expertise to help me beat this menace. Spamcop seemed the obvious service to do that.

KJP

dougsonos Sep 15 2004, 07:47 AM

> **QUOTE**
>
> I don't think anyone answered me when I asked this before, but I don't know why the ISPs can't run the 'bounce' emails through a spam content filter set on high before they send them and dump those that don't pass. Also, an ISP could write a parser for its own use - in fact some of the bounces that I have received actually had the correct IP address added. The reason that there isn't another available for other people on the web is spamcop's ability to deal with many different header configurations. A private one also doesn't have to send reports or look up abuse desks. That is one reason why it is so stupid that ISPs send email bounces to the 'returnpath' - if they feel that they can't dump undeliverable mail, there are ways to send it to the proper place - it just costs more.

I've been getting about 300-400 bounces a day for the last month. I finally figured out how

to filter most of the bounces on the receiving end and it is not pretty (procmail => a little filter I wrote to look for a From header in a form other than the one I use to sign my mail).

My bounces go through SpamAssassin -- which sees something that convinces it that they aren't spam, even with the original spam in the message -- the Bayesian filter reports 0% probability of spam.

I lost a couple days banging my head on the way that Exim + the virtual hosting software (cPanel) run by my ISP does not allow the normal Exim filtering mechanism to operate on bounces.

I guess all this is to say that separating the bounced spams from bounces you might actually want to see is not a simple task... it's taken most of my spare time over a week and a half to get the bounces under control.

Doug

dbiel Sep 15 2004, 08:49 AM

K.J. Petrie, it sounds like your problem is much bigger than just bounces.
Most ISP blocking is IP based, not domain name based. End users tend to block based on domain name. I would doublt that your stock broker would have blocked your domain, so the assumption would be that the ISP was blocking your IP address. Note: sender based blocking does not exist, all blocking is done at the receiving end with the exception of blocking by your own ISP and if that is the case then you have even bigger problems.
Have you read the FAQ Why Am I Blocked? FAQ, Please read before posting If not please read and come back and post more information so we can try to help.
Also have you read FAQ Entry: Why am I getting all these bounces?
I agree with you about it being a major problem and the fact that you are being hurt by it, but I do not believe that it is the entire or even major part of your specific problem with people not receiveing your mail.
We look forward to hearing from you with information about the mailserver you are using to send your mail. It may be that "you" are actually the one that is sending the spam without knowing it. In this case "you" means the IP number of the mailserver you are using to send your mail.

Miss Betsy Sep 15 2004, 08:58 AM

I can see how that is true for /after/ the bounce message has been created and when the recipient is trying to sort real email from bounce emails - and goes a long way towards explaining why spamcop doesn't accept bounces for processing!

However, the receiving ISP still has the original email that he could filter with a much higher setting for spam (since it is suspect). Only after the email passes the spam and virus filter would the process send an undeliverable email message. Even though, some real undeliverable emails may be lost with high settings, the percentage is bound to be miniscule compared to the nuisance for those who are receiving bounce emails to forged addresses. The possibility is that real undeliverable email will pass the test and the person notified is still there. It would be preferable to simply dumping all undeliverable email and definitely better than 'bouncing' it.

The cost of even doing that extra step of putting the email through a virus filter or spam filter might be enough to keep those who are cheap from doing it though. It would probably mean more hardware. I think that's why many ISPs don't use blocklists and use content filters instead to filter spam.

Miss Betsy

turetzsr Sep 15 2004, 01:46 PM

> **QUOTE(K.J. Petrie @ Sep 15 2004, 07:31 AM)**
>
> <snip>
> In the majority of cases that won't matter, because I'll never have cause to E-mail them, but among those millions setting filters against my domain, may be friends who don't recognise it or people I am yet to meet.

...To avoid that, e-mail should not be the first contact vehicle! <g>

> **QUOTE(K.J. Petrie @ Sep 15 2004, 07:31 AM)**
>
> My social life is already being disrupted by friends not receiving my E-mails, and while I've been writing this my stockbroker has just phoned because a transaction nearly went astray when they failed to receive my instructions (that represents a fifth of my life savings). AoL blocked my domain at the beginning of the year. So I think it does happen.

...Yes, spammers have ruined the internet for everyone! This is a valuable lesson, though -- internet e-mail is not a guaranteed delivery mechanism, so you should not rely on it for important matters. Besides spammers, backhoes can break datacomm lines, servers can crash, packets of data can be lost.

> **QUOTE(K.J. Petrie @ Sep 15 2004, 07:31 AM)**
>
> I think the term Joe-job may well apply to what is happening here, though I'm not an expert on Internet slang (sorry - technical language).
> <snip>

...One of the aforementioned pinned items, Pinned: Original SpamCop FAQ Plus - Read before Posting, has link to another page that includes a link to The Net Abuse Jargon File which contains a reference to a "joe."

> **QUOTE(K.J. Petrie @ Sep 15 2004, 07:31 AM)**
>
> I think it's defamatory to have one's name associated with antisocial and possibly illegal activity. It certainly feels that way.
> <snip>

...But no one with any sense will assume that you have anything to do with it. IIUC (If I understand correctly), in order to have defamation, there must be damages arising from "reasonable ordinary prudent" people relying on the false information. <g>

K.J. Petrie Sep 20 2004, 10:13 AM

Thanks, dbiel,

I send through relay.pol.net.uk as its alias smtp.wanadoo.co.uk which has IP addresses of 195.92.195.153 and 195.92.193.153.

Wanadoo is a pretty major European ISP, and has recently taken over the entire Freeserve network in the UK, so whilst spammers will almost certainly use it occasionally, I wouldn't expect any responsible list operator to include it. I'm certainly not suggesting that SpamCop has.

None of the bounced messages originated from this network. Most of them originated in the Far East, a few from the US, a few from Germany, and a few from Spain.

Earlier today the abuse addresses at cj.net and apol.com.tw 553ed my complaints about spam sent from their network! I resent my complaints (through the same server) using an old domain (at which I can also receive mail) for the From: address, except that I forgot to change the From address on one of them, and it came straight back. The others did not. So at least one of these ISPs appears to be blocking by domain. As I said in an earlier post, I think it does happen. Whether these ISPs are reasonable ordinary prudent people I can't say.

KJP

dra007 Sep 20 2004, 10:38 AM

I sure wish there was a place to report these <<bouncers>> somewhere. All of the bounce I get now have MIME-exploits or viruses attached and for the most part spoof my own domain name.

Are these idiots so clueless that they don't realize the real IP can be parsed out? As far as dealing with that abuse I have reached an impass as my ISP is just as cluless in stopping or dealing with the bounces. I am sorry if I sound frustrated, I am!

I am done with posting examples here ...I just wish someone would come up with a feasable idea on how to deal with such abuse.

StevenUnderwood Sep 20 2004, 10:54 AM

> **QUOTE**
>
> I just wish someone would come up with a feasable idea on how to deal with such abuse

Your idea of feasible seems to be hand it off to someone else to deal with.

I have told you how I deal with every piece of virus infected message that postini stops and every misdirected bounce I receive and it has worked grreat for me. Only a few different IP's have I ever had to blocklist for ignoring the message they were infected and the problem was gone within the 30 day expiration of the block I instituted. Usually, I have received messages that the problem was found and fixed and thank yous. The misdirected bounces have gotten a few replies asking for more information. There is only one domain that took longer than a week to stop sending them to me. THose now seem to have stopped as well.

At this point in time, totally eliminating unwanted email is not a likely scenario without starting with a completely fresh email address that is a random set of letters and numbers.

dra007 Sep 20 2004, 11:59 AM

> **QUOTE(StevenUnderwood @ Sep 20 2004, 10:54 AM)**
>
> Your idea of feasible seems to be hand it off to someone else to deal with.
>
> I have told you how I deal with every piece of virus infected message that postini stops and every misdirected bounce I receive and it has worked grreat for me. .../snip

Only my ISP has that feature available to them and they refuse to do it. So, all is left for me is live with the abuse. As for contacting the senders I have, many times, all I got was more abuse. I have even contacted the upstream providers, all in vain. We are beating on a dead horse here. And I keep repeating myself, it's not the occasional abuse that bothers me, but the abuse that has persisted and continuses daily for months, and nothing ever seems to work against it. The abuse desks that are resposive, are soon forgotten (and forgiven).

K.J. Petrie Sep 20 2004, 06:44 PM

> **QUOTE(K.J. Petrie @ Sep 20 2004, 04:13 PM)**
>
> Earlier today the abuse addresses at cj.net and apol.com.tw 553ed my complaints about spam sent from their network! I resent my complaints (through the same server) using an old domain (at which I can also receive mail) for the From: address, except that I forgot to change the From address on one of them, and it came straight back. The others did not. So at least one of these ISPs appears to be blocking by domain. As I said in an earlier post, I think it does happen. Whether these ISPs are reasonable ordinary prudent people I can't say.

I take it all back. They just took their time returning, that's all. So some ISPs are blocking Wanadoo! That's mystifying. They're one of the biggest providers in the EU and as respectable as they come! Doubtless they will get the odd nasty customer who'll abuse their network, and they'll throw them off just as quick, but perhaps if they get another rogue customer the next day... and the day after, which I suppose is inevitable when they're that big...

K.J. Petrie Sep 20 2004, 06:55 PM

> **QUOTE(turetzsr @ Sep 15 2004, 07:46 PM)**
>
> ...But no one with any sense will assume that you have anything to do with it. IIUC (If I understand correctly), in order to have defamation, there must be damages arising from "reasonable ordinary prudent" people relying on the false information. <g>

If the spammers/joers are relying on that defence they're going to get burnt. In England, the measure is the "right-thinking" person, and it takes no account of whether the falsehood is credible, only whether, in the eyes of a "right-thinking" person, it tends to lower the plaintiff's reputation. The more obviously untrue the allegation, the more culpable an English jury will consider the defamer, as he/she should have realised they were propogating an untrue slur, and the bigger the damages they will award.

Pity I haven't got the millions it takes to bring a successful action...

KJP

StevenUnderwood Sep 20 2004, 07:33 PM

> **QUOTE**
>
> So some ISPs are blocking Wanadoo!

I get AT LEAST 1 spam message from a Wanadoo IP every day. The last 2 days have been:

Subject: we carry vicodin (fegfipc@ALagny-152-1-31-206.w83-112.abo.wanadoo.fr [83.112.100.206])
Subject: An amazing technology to meet your changing needs... (hvs-w-19fc.adsl.wanadoo.nl [212.129.153.252])

Both of these are from what seem to be DHCP served accounts, probably virus infected, so the Wanadoo servers would not be listed. But these should be blocked for sending spam.

dra007 Sep 20 2004, 09:55 PM

I do to, but haven't seen Wanadoo since sometimes last week. Now it's mostly kornet and chinanet. Some in Brazil, Taiwan and few other places. And some are quite interisting; places you wouldn't think are connected to internet, let alone spew spam.

K.J. Petrie Sep 25 2004, 04:47 PM

My problem remains. I am being joed, the E-mail advertises a website at 61.240.131.219 which isn't on your blocklist because I am not allowed to report the spamvertising. If I could report it it might get the hosting company (UNICOM) to take notice...

I have dozens of E-mails containing the evidence for nearly a month now, and I am powerless because there isn't a means for me to report the problem, and the spammers are getting away with it! They mustn't be allowed to get away with it. It's like letting terrorists get away with it. In fact, it is a form of terrorism.

Wazoo Sep 25 2004, 06:04 PM

The BL doesn't do websites ... only the IP of the spam spew source, usually an e-mail server, sometimes the IP of a compromised machine ....

I have to tell you, "dozens of e-mails for nearly a month" isn't much of a deal ... this is as compared to the last time one of my addresses was used as a forged From: line ... I'm

talking 3 to 8,000 bounces in a single day .. and as I recollect, this went on for about three weeks. You still haven't offered enough detail to convince me that you are being joe-jobbed ... thus far all you've yet described is a forgery of the alleged From: address.

There is nothing preventing you from manually reporting this stuff yourself, if the bouce contains enough data to track anything down.

dbiel Sep 26 2004, 03:40 AM

> **QUOTE(K.J. Petrie @ Sep 25 2004, 02:47 PM)**
>
> My problem remains. I am being joed, the E-mail advertises a website at 61.240.131.219 which isn't on your blocklist because I am not allowed to report the spamvertising. If I could report it it might get the hosting company (UNICOM) to take notice...
>
> I have dozens of E-mails containing the evidence for nearly a month now, and I am powerless because there isn't a means for me to report the problem, and the spammers are getting away with it! They mustn't be allowed to get away with it. It's like letting terrorists get away with it. In fact, it is a form of terrorism.

Remember that SpamCop is only a tool to help you report Spam. It has put in place limitations to help prevent abuse. Reporting remains an individual issue. You are free to report anything that you choose to report, but faulty reporting does not help anyone. Note: there is actually NO restrictions on using the SpamCop parsing tool to help identify sources of any message (spam or otherwise). The restrictions apply on the use of the reporting portion of the tool only. If your statements are a true reflection of your beliefs, then do something about it. Don't complain about a tool that is provided to help you. When you are trying to build something you will most often use several tools. Even hammering in a nail sometimes requires a drill to drill a pilot hole first to prevent splitting the wood. Remember that the tools can do nothing by themselves, they need someone to use them. SpamCop is but one tool in the fight against spam. If it is the only tool that you choose to use then your statement is actually nothing but a pile of hot air.

Miss Betsy Sep 26 2004, 08:06 AM

If I read everything correctly, you don't have enough time to really go after the spammers who are using your domain name in the From:

Most people *feel* the way you do that it is a defamation of character to have /their/ domain associated with spam - even if they realize that prudent, knowledgable people don't pay any attention to the From in spam.

Unfortunately, no one has either the time or money to get any action taken in all the countries of the world who might actually be able to do something about stopping this practice.

Many people apparently have had to abandon some domains and start over.

So the short answer is that spamcop is a tool (as was explained in another post) and in this case, the wrong tool to protect /your/ domain. The spamcop blocklist is a long term tool to identify spam before it enters the inbox by either rejecting at the server or putting it in a special place. The result is that ISPs who are interested in providing reliable email service take care not to have spammers on their networks and, if a spammer is reported, take

action immediately so that any interruption of service is no more serious or inconveniencing than a traffic jam.

The idiots like MS and McAfee still perpetuate the myth that the From can identify the sender. The best defense against the good name of your domain would be to conduct an educational PR campaign so that ordinary end users are aware that the 'block this sender' is a hoax

Miss Betsy

dra007 Sep 26 2004, 08:11 AM

> **QUOTE**
>
> SpamCop is but one tool in the fight against spam. If it is the only tool that you choose to use then your statement is actually nothing but a pile of hot air.

The bottom line is that bounces due to spoofed domains have become as problematic and numerous as spam itself. See, for example, the discussion started in the lounge about Microsoft suggesting bounces would work to prevent spam.

The issue a lot of us have raised is not how to manually parse and report 200 or more bounces a day. Nobody in their right mind would take the time to do such thing. Instead, it was raised as a legitimate issue to stimulate discussion on finding an efficient method to deal with it. It is evident that these bounces are raising new challanges and technical questions. It is also evident to me and others that spoofing reporters' domain names and e-mail addresses s is another way to abuse and intimidate the reporting side of the spam fight. In fact, when I first started reporting, I was getting 10-100x more bounces than I was getting spam.

K.J. Petrie Sep 27 2004, 04:41 AM

> **QUOTE(dbiel @ Sep 26 2004, 09:40 AM)**
>
> If your statements are a true reflection of your beliefs, then do something about it.

Great idea. What is "something"? Any (sensible) suggestions would be welcome.
KJP

Miss Betsy Sep 27 2004, 08:31 AM

Several people have suggested several different things - most of them are time consuming for very little immediate return.

One thing that no one has suggested is that you complain to Wanadoo about unreliable service (or whoever is the owner of the IP address that is being blocked). IMHO, it is the *sender* of email that needs to *do* something about spam. Receivers should have little or no inconvenience.

Many large ISPs have been very slow to respond to complaints about spam coming from their networks, but eventually they all seem to start paying attention because they get enough complaints from their *paying* customers.

You have a range of options: from the most time consuming: learn how to read headers and find upstreams and go after the spammer by reporting and complaining to as many different people as you can that might have influence - not only by email but by phone and snail mail to the least timeconsuming: use a good filter to bit bucket the bounces and forget about it.

Miss Betsy