

Re: Return-Path not showing in OE Details

Source: <http://www.tech-archive.net/Archive/Internet/microsoft.public.internet.mail/2004-03/0188.html>

From: *Vanguard* (no-email_at_post-reply-in-newsgroup.invalid)

Date: 03/08/04

Date: Sun, 7 Mar 2004 21:11:53 -0600

"Newsy" said in news:5bee01c4049a\$0f005050\$a601280a@phx.gbl:

- > A friend is using Outlook Express 6. In trouble shooting
- > some viral messages he's received, we see
- > that "Properties"/"Details" and even "Message Source" does
- > not show a "Return-Path" field in any of the messages in
- > his inbox – even legit ones.
- >
- > What's up with this? Could his ISP be stripping this
- > information?

>From what I understand of RFC 2821, "SMTP", the information presented in this header is whatever the sender wants to specify in the MAIL command they send to their SMTP server. Okay, so spammers are going to use a bogus or purloined e-mail address in From and Reply-To but they aren't going to falsify their return-path info? Not likely.

This is one of those defects lingering from the days of naivety when e-mail schemes were still being forged and tested. It's pretty stupid these days to assume the sender will provide a valid reverse-path in their MAIL command. Instead, the sender's SMTP server should overwrite whatever is specified by the sender and instead insert the account name that the sender used to verify to that SMTP server. I believe the sender is not allowed to specify a null string for return-path but maybe blanks are okay. Also, a null reverse-path is allowed under certain circumstances, like when an mail server returns an NDR (non-deliverable report) status message to the sender notifying them that the e-mail was undeliverable for whatever reason. Spammers use this to send their crap to a known and valid major domain but using a recipient username that might not exist. If the username exists, their crap gets delivered. Otherwise, their crap gets returned but since the spammer can also specify whatever they want for the return path then you could be listed (i.e., the spammer pretends to be you sending their crap, so the receiving mail server bounces the NDR back to you which has a null reverse-path since the mail server doesn't want yet another NDR from your mail server should the sender's reverse info be completely bogus).

RFC 2821 says, "All other types of messages (i.e., any message which is

not required by a standards-track RFC to have a null reverse-path) SHOULD be sent with with a valid, non-null reverse-path." Notice the "SHOULD". Again, the old e-mail schemes are naive. This should be a "MUST" plus it should be specified by the sender's SMTP server rather than whatever the sender wants to specify. Some spammers operate their own mail servers but most want to hide by using temp accounts, abusing relays, or otherwise stealing resources from someone else. There are a lot of "SHOULD" which if forcibly changed to "MUST" (by the receiving mail server enforcing the requirement plus also allowing the receiving mail server to authenticate with the sending mail server that the headers are correct) that would make e-mail less abused.

Out of the inbound messages that I have stored in Outlook in various folders (forget about looking at your outbound messages), only a third had the Return-Path header. Since the Return-Path info can be just as bogus as the From and Reply-To headers, I suppose many mail servers see no need to include it in the headers for a delivered message. After all, if a good sender used a valid e-mail address in the From or Reply-To headers than what is specified in the Return-Path is superfluous. So either the info in Return-Path is superfluous or bogus. As proof that client-side software can manipulate the reverse-path in the MAIL command, I've been told that Mailwasher will use a null value just like an mail server when sending its bogus NDR e-mails to make it appear that account is not defined at that domain. The proof (for Mailwasher) will have to be performed by someone that uses that product. I use SpamPal for anti-spam software.