Subject: SPAM with Reply-To and DSN notify
Posted by RadimAdmin on Mon, 31 Jul 2017 00:31:36 GMT
View Forum Message <> Reply to Message

hi,

we have encountered an emerging problem with SPAM messages with Reply-To header and delivery notification set.

1. Even in case of marked spam message, KConnect tries to deliver DSN notification to Reply-to address, but with real recipients addresses (not aliases).....this is huge security problem to reveal real addresses to spammers.

2. Server is bloated because of hundreds of delayed DSN messages, because not all Reply-to addresses have existing domains (some have A records, but no MX records).

3. Why is server trying to deliver these DSNs to domains without MX record. It tries to connect to host derived from reply-to address (simply striped part after <at> a tries to connect to SMTP).

4. Message filters do not apply to DSN sent by server itself.

Any advice?

EXAMPLE:
[30/Jul/2017 15:34:29] Sent: Queue-ID: 597dc8e2-00000095, Recipient: <bedag13ek95<_at_>gaxljk.com>, Result: delayed, Status: 4.4.1 Cannot connect to host, Remote-Host: gaxljk.com, Msg-Id: <182948812-47324@xxxxxxxxxx>

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Tue, 08 Aug 2017 12:48:21 GMT
View Forum Message <> Reply to Message

Same here. Getting more and more messages like this; currently a few hundred per day.

Big problem in the making.

Maybe need an option to disable DSN reply messages for any emails that fail any sort of security checks? Including spam lists, black lists, custom rules, called id, spf, AV, etc...

An option to just disable all server delivery reports by category might be tempting too. Or at least turn them off for sender addresses not in a users contacts or white-list.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by Kerio/GFI Brian on Tue, 08 Aug 2017 18:30:29 GMT

View Forum Message <> Reply to Message

In the SMTP server -> Security options, make sure all of the options are enabled.
This issue can happen if you are forwarding messages to another backend mail system and the message was addressed to an unknown recipient. Try to avoid this situation if possible. Kerio Connect only sends delivery status notifications to messages that have passed all security settings and have been received to the queue.
I suggest contacting technical support to investigate how these messages are being received into the queue.
You may find some helpful tips from this KB article
http://manuals.gfi.com/en/kerio/connect/content/server-confi
guration/security/securing-kerio-connect-1239.html

Subject: Re: SPAM with Reply-To and DSN notify
Posted by RadimAdmin on Tue, 08 Aug 2017 19:29:28 GMT
View Forum Message <> Reply to Message

Hi Brian,

we are not forwarding messages to any backend systems.

This issue is with delivery status messages to messages originally MARKED as possible SPAM, not REJECTED as SPAM. There are two threshold settings in SPAM section.

Secondary problem is: spammers are harvesting real addresses using DSN, because DSN to these messages contains real addresses, not aliases.

I think adding a funtionality to disable DSN for messages MARKED as possible spam might solve this issue. And of course adding possiblity to reject messages from domain without valid (or any) MX records. I am unaware of any legit mail from domain with A record only (without MX record).

Support ticket already posted, here is the progress:
1. asking for license number - SENT
2. waiting for 2 days
3. asking for logs and messages samples - SENT
4. waiting for 3 days for answer...

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Mon, 14 Aug 2017 05:54:48 GMT
View Forum Message <> Reply to Message

Here's a log which demonstrates.

[14/Aug/2017 05:19:48] Recv: Queue-ID: 599116d4-00014080, Service: SMTP, From:

<behelqkt3z1s@rmxsmania.com>, To: <sales@mydomain.com>, Size: 3797, Sender-Host: 66.37.0.103, Subject: mivel frissülj 40 fokban? kellemes szell
áráért 2 jár, Msg-Id: <MViobBcyfZPkFFRYOl-4N4SA19<_at_>rmxsmania.com>

[14/Aug/2017 05:19:50] Recv: Queue-ID: 599116d6-00014081, Service: DSN, From: <>, To: <behelqkt3z1s@rmxsmania.com>, Size: 3211, Report: success, Subject: Visszaigazolás: **SPAM** [***] mivel frissülj 40 fokban? kellemes szell
2 jár, Msg-Id: <3737204058-17195<_at_>mail.mydomain.com>

[14/Aug/2017 05:19:50] Sent: Queue-ID: 599116d4-00014080, Recipient: <sales@mydomain.com>, Result: delivered, Status: 2.0.0 , Remote-Host: 127.0.0.1, Msg-Id: <MViobBcyfZPkFFRYOl-4N4SA19<_at_>rmxsmania.com>

Kerio Connect identifies the dodgy e-mail as spam (adding the SPAM prefix to the subject), and then replies to the sender who had requested a delivery receipt. The DSN sits in the msg queue, as Kerio cannot deliver to the spammy sender's MX. I've just deleted 327 such DSN messages from the queue, and 248 were deleted yesterday midday-ish.

As a quick solution, we'd like to be able to disable server-delivery-receipts (preferably all, or at least for those messages deemed probable spam). Maybe that can already be done by manual edit of mailserver.cfg? Users can still choose to reply with read-receipts, although it would also be nice to have an option to remove read-requests from spammy emails too- save users being bombarded with all the work.

No doubt smarter ways to handle the situation could be figured with more than the 5 seconds thought I've given it, but if there's a quick existing way to resolve this without us having to add external processes in-front of Kerio then I'd be very grateful to learn from anyone who's found a solution.

Cheers!

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Mon, 14 Aug 2017 06:06:20 GMT
View Forum Message <> Reply to Message

Brian Carmichael (Kerio) wrote on Tue, 08 August 2017 20:30In the SMTP server -> Security options, make sure all of the options are enabled.
This issue can happen if you are forwarding messages to another backend mail system and the message was addressed to an unknown recipient. Try to avoid this situation if possible. Kerio Connect only sends delivery status notifications to messages that have passed all security settings and have been received to the queue.

Thanks Brian.

To reply your q's... all Security Options ticked and no forwarding. Seems like same situation as @RadimAdmin describes- that DSN's are being sent for probable spams, and the spammers are starting to milk that loophole :)

Subject: Re: SPAM with Reply-To and DSN notify
Posted by Kerio/GFI Brian on Mon, 14 Aug 2017 19:04:55 GMT
View Forum Message <> Reply to Message

Check the Spam Filter -> Spam Rating area. Make sure you are NOT sending bounce messages to the sender. This option is in the "Reached block score limit action".
Otherwise if you view the content of these messages in the queue it could help to identify which component is replying to theses messages.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Tue, 15 Aug 2017 08:06:44 GMT
View Forum Message <> Reply to Message

Brian Carmichael (Kerio) wrote on Mon, 14 August 2017 21:04Check the Spam Filter -> Spam Rating area. Make sure you are NOT sending bounce messages to the sender. This option is in the "Reached block score limit action".
Otherwise if you view the content of these messages in the queue it could help to identify which component is replying to theses messages.

We are NOT sending bounce messages.
However, we DO forward msgs to a local quarantine address (an email address on the Kerio mailserver), should that be something.

Will check the msg queue sources when some more appear....

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Tue, 15 Aug 2017 08:36:33 GMT
View Forum Message <> Reply to Message

Got one...

Seems to show "Mail Delivery Subsystem <postmaster<_at_>mail.mydomain.com>" is sending this delivery receipt, despite having marked the message subject line as spam.

Thanks again for your suggestions, and hope this helps you diagnose.

What I did for testing: Created a custom spam rule to add 6 score to messages with "spam test" in the title, then sent myself a message with the delivery and read receipt options ticked.

Return-Path: <>
Received: from localhost
 by mail.mydomain.com; Tue, 15 Aug 2017 10:22:27 +0200
Date: Tue, 15 Aug 2017 10:22:27 +0200
Message-ID: <3841761417-21799<_at_>mail.mydomain.com>
MIME-Version: 1.0

From: Mail Delivery Subsystem <postmaster<_at_>mail.mydomain.com>
To: <sales<_at_>mydomain.com>
Subject: =?utf-8?Q?Visszaigazol=C3=A1s=3A_**SPAM**_=5B****=5D__spam_test?=
 =?utf-8?Q?_2?=
Content-Type: multipart/report; report-type=delivery-status;
 boundary="MIME-3841761417-2090780927-delim"

...

X-Spam-Status: Yes, hits=4.6 required=3.8
 tests=AWL: -0.007, BAYES_00: -1.665, HTML_MESSAGE: 0.001,
 XPRIO: 0.299, CUSTOM_RULE_SUBJECT: 6.00, TOTAL_SCORE: 4.628,autolearn=no
X-Spam-Flag: YES
X-Spam-Level: ****

Subject: Re: SPAM with Reply-To and DSN notify
Posted by Kerio/GFI Brian on Tue, 15 Aug 2017 14:12:43 GMT
View Forum Message <> Reply to Message

It would be better to capture the content of a real (not simulated) DSN message. However, as a solution to your problem you can create an outgoing message filter rule that discards messages with **SPAM** in the subject.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Wed, 16 Aug 2017 04:52:00 GMT
View Forum Message <> Reply to Message

Thank you Brian.

My (mis)understanding was that the server msg filter doesn't work on DSN's or server-originating messages. I've added that filter now and will report back.

For reference, here's a real .eml from the queue this morning. Apart from the return-path tag, the rest appears the same to my untrained eye!

Received: from localhost
 by mail.mydomain.com; Tue, 15 Aug 2017 10:54:12 +0200
Date: Tue, 15 Aug 2017 10:54:12 +0200
Message-ID: <3843666046-22916<_at_>mail.mydomain.com>
MIME-Version: 1.0
From: Mail Delivery Subsystem <postmaster<_at_>mail.mydomain.com>
To: <violah3tbj2a<_at_>spalks.com>
Subject: =?utf-8?Q?Visszaigazol=C3=A1s=3A_**SPAM**_=5B*****=5D__=C5=90R?=
 =?utf-8?Q?=C3=9CLT_ny=C3=A1ri_le=C3=A1raz=C3=A1s=3A_3_l=C3=B3er?=
 =?utf-8?Q?=C5=91s_f=C5=B1r=C3=A9sz=2C_52_k=C3=B6bcentivel=2C_osz?=
 =?utf-8?Q?tr=C3=A1k_min=C5=91s=C3=A9g?=
Content-Type: multipart/report; report-type=delivery-status;
 boundary="MIME-3843666046-28497765-delim"

--MIME-3843666046-28497765-delim
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 8bit

Ezt a tájékoztató üzenetet küldte: mail.mydomain.com.

A szerver sikeresen kézbesítette a levelet

  Subject: **SPAM** [*****]
  Date: Tue, 15 Aug 2017 10:55:53 +0200

a következo címzetteknek:

  <delio<_at_>mydomain.com> (delivered)
--MIME-3843666046-28497765-delim
Content-Type: message/delivery-status

Reporting-MTA: dns; mail.mydomain.com
Arrival-Date: Tue, 15 Aug 2017 10:54:11 +0200

Original-Recipient: delio<_at_>mydomain.com
Final-Recipient: rfc822;delio<_at_>mydomain.com
Action: delivered
Status: 2.0.0

--MIME-3843666046-28497765-delim
Content-Type: text/rfc822-headers

X-Spam-Status: Yes, hits=5.5 required=3.8
 tests=BAYES_50: 1.567, HTML_IMAGE_ONLY_20: 1.546, HTML_MESSAGE: 0.001,
 HTML_SHORT_LINK_IMG_3: 0.148, MIME_HTML_ONLY: 0.723, URIBL_BLOCKED: 0.001,
 URIBL_RHS_DOB: 1.514, TOTAL_SCORE: 5.500,autolearn=no
X-Spam-Flag: YES
X-Spam-Level: *****
Received: from gone.spalks.com ([66.37.0.99])
 by mail.mydomain.com with ESMTP
 for delio<_at_>mydomain.com;
 Tue, 15 Aug 2017 10:54:10 +0200
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=dkim; d=spalks.com;

h=Date:To:Subject:Message-ID:From:Reply-To:MIME-Version:Content-Type:Content-Transfer-Encoding; i=violah3tbj2a<_at_>spalks.com;
 bh=Hamk0Y0BvBrkfSpaOf7FDTklK84=;

b=SUQi/cDju7Hz/BB6k9vP9dbtTZJLbdM5pjTka93joNgU0jS7neJ1TFirAnbvCro3lgQ8oNIoX4Ac

9n4zfP91nXcp0LkhXBE+t3xqPcOqsPizIeGt6PIHjQoqycdkp0U/vvaW/k1Gm9/OokOqICN5KE8W

bUiEMcpFsGpt4TUgTk8=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=dkim; d=spalks.com;

b=LXlLUSSUpy/jxVkSYAj9leQWIowCTQRgvUWZ6fPWjP7iB+hKYQmnXocg5WbY96dxopENd
IxcgbBO

fBRe6SsK4IPJ2LwCkBgKcRGiZvjuF5IHXpju1YHu2OZ7o2D2ugnInrT7K2C3r7H0tlU3wBA9oG
0w
vL0HzNUbYC6Yv0theIA=;
Date: Tue, 15 Aug 2017 10:55:53 +0200
To: <delio<_at_>mydomain.com>
X-Original-Subject:
=?UTF-8?Q?=C5=90R=C3=9CLT_ny=C3=A1ri_le=C3=A1raz=C3=A1s:_3_l=C3=B3er=C5=91
s_f=C5=B1r=C3=A9sz,_52_k=C3=B6bcentivel,_osztr=C3=A1k_min=C5=91s=C3=A9g?=
Subject: **SPAM** [*****]
=?UTF-8?Q?=C5=90R=C3=9CLT_ny=C3=A1ri_le=C3=A1raz=C3=A1s:_3_l=C3=B3er=C5=91
s_f=C5=B1r=C3=A9sz,_52_k=C3=B6bcentivel,_osztr=C3=A1k_min=C5=91s=C3=A9g?=
Message-ID: <axzxsnhqiqolsqsfvotrfmeucvkckpfc<_at_>spalks.com>
Return-Path: ua16vc1esky8ftic8.joNmls<_at_>spalks.com
From: =?UTF-8?Q?Viola?= <violah3tbj2a<_at_>spalks.com>
Reply-To: violah3tbj2a<_at_>spalks.com
MIME-Version: 1.0
X-Priority: 3
Precedence: bulk
X-Mailer: class SMTPMail
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

--MIME-3843666046-28497765-delim--

This is what shows (over and over) in the Warning log:

Cannot connect to SMTP server spalks.com. Messages will stay in the message queue.

To give some perspective, their are currently 247 such messages in the queue. Not counted how many different sending-domains, but looks like 20 or so different ones.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Wed, 16 Aug 2017 06:39:34 GMT
View Forum Message <> Reply to Message

Update-

Unfortunately the DSN/server messages were NOT processed by the global message filter. I've enabled sieve-msgs in debug log, and can see the rule processing everything except the DSN's.

sample for non-dsn (normal email) message indicates the filter is operational:

[16/Aug/2017 08:13:34][8046] {sieve} Global sieve rule keriodb://sieverule/ca700663-8f8e-41a2-b0f9-7ab125e9ffd3 (**SPAM**) successfully parsed.

I've also tried adding a filter for all messages from the postmaster email address (postmaster<_at_>mail.mydomain.com), but that doesn't pick up any messages either.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by Kerio/GFI Brian on Wed, 16 Aug 2017 17:05:58 GMT
View Forum Message <> Reply to Message

The rule should be in the Outgoing rules and should specify if any of the following conditions are met:
Subject contains **SPAM**
Discard message

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Thu, 17 Aug 2017 04:12:09 GMT
View Forum Message <> Reply to Message

Correct. And that doesn't discard them when they are sent by the server (ie. DSN messages).

The rule does discard a test message, which I sent myself.

Furthermore, nothing appears in the "sieve filter" debug log for DSN types of messages. whereas logs appear for all other user messages.

All this leads me to deduce that DSN messages skip the filter...

Brian, could I ask specifically... Are you 100% that all outgoing messages originating from the server itself (such as DSN messages) do get parsed by the filters?

If you are certain, then I sure will look for other reasons why the filter on those messages doesn't get actioned.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by Kerio/GFI Brian on Thu, 17 Aug 2017 14:05:00 GMT
View Forum Message <> Reply to Message

I've done some testing and it seems that the outgoing rules apply to bounces from the spam filter, however if I request a delivery receipt then I am able to reproduce the behavior you describe. It does seem to skip the outgoing rules for some reason. So it seems there are two issues here:
1. There is no possibility to disable delivery receipt confirmation messages.
2. Outgoing rules do not apply to DSN messages.
I will file a bug for these two items.

Unfortunately I can't find any other solution to this problem.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by atomitech on Thu, 17 Aug 2017 15:30:38 GMT
View Forum Message <> Reply to Message

Sounds right. Thanks for taking the time out to test.

With regard including system msgs (like DSN, AV warnings, etc..) into the global msg filter, if occurred to me that could come with risks of creating a message loop with certain actions (such as forwarding the email to a local user and then matching on the same conditions, perhaps if only a subject match is used). That sort of potential complication could be why they were left off originally :)

A safer/simpler approach might be to provide 2 tick boxes in the appropriate places. One to disable DSN (server delivery notification) for all messages associated to a domain, and the other to disable DSN's only for those messages detected as spam or failing any other security checks. (Although the later arguably might be best as the default behaviour anyhow, without need for a tickbox; and seemingly it almost is, just that those msgs classified as spam -but not blocked as spam- are not having the DSN's discarded).

OK, time to clear the mind of all this, and look forward to a possible future improvement.

Many thanks again Brian.
Great support as always.

Subject: Re: SPAM with Reply-To and DSN notify
Posted by paul_jcs on Thu, 09 Nov 2017 11:34:22 GMT
View Forum Message <> Reply to Message

Hi

Did this ever get resolved?

I have a client running Kerio Connect 9.2.2 Patch 1. They are currently blacklisted on Barracuda but the only strange behaviour or the DSN report emails in the Message Queue.

The server has the same "Report: autoreply, User: Global deliver rule" in the Mail log for every email in the Message Queue.

Is there a way to disable DSN either in the web admin or mailserver.cfg file?

Subject: Re: SPAM with Reply-To and DSN notify
Posted by damjanh on Thu, 24 May 2018 11:16:30 GMT

View Forum Message <> Reply to Message

I have the same trouble.
mail_report.cpp: Cannot open report file 'dsn-success' in language

Subject: Re: SPAM with Reply-To and DSN notify
Posted by guyhemmings on Wed, 13 Jun 2018 11:39:55 GMT
View Forum Message <> Reply to Message

Have we a solution for the inability to DSNs going out from the KC server yet? As we know now, no method of rules is able to control the process.

The forum entry is 9 months old and there appears to be no update...

Guy

Subject: Re: SPAM with Reply-To and DSN notify
Posted by guyhemmings on Wed, 13 Jun 2018 11:43:42 GMT
View Forum Message <> Reply to Message

Has anyone any news on this one. I can find no solution to stop KC from sending DSNs, and the question here seems unanswered after 9 months! Not looking good. The twitter feed does get any responses to queries, only seems to contain adverts from GFI for KC.

:-/

Guy

RadimAdmin wrote on Tue, 08 August 2017 21:29Hi Brian,

we are not forwarding messages to any backend systems.

This issue is with delivery status messages to messages originally MARKED as possible SPAM, not REJECTED as SPAM. There are two threshold settings in SPAM section.

Secondary problem is: spammers are harvesting real addresses using DSN, because DSN to these messages contains real addresses, not aliases.

I think adding a funtionality to disable DSN for messages MARKED as possible spam might solve this issue. And of course adding possiblity to reject messages from domain without valid (or any) MX records. I am unaware of any legit mail from domain with A record only (without MX record).

Support ticket already posted, here is the progress:
1. asking for license number - SENT
2. waiting for 2 days
3. asking for logs and messages samples - SENT
4. waiting for 3 days for answer...