Admins - Anomalie #1790

Des personnes envoient des courriels à des listes April et il y a le champ From de la liste comme adresse d'expédition

14/09/2016 22:42 - Frédéric Couchet

Statut:	Fermé	**Début:**	14/09/2016
Priorité:	Normale	**Echéance:**	
Assigné à:	Benjamin Drieu	**% réalisé:**	50%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Isabella a signalé que cela fait la 3e fois en 2 jours qu'un adhérent écrit à l'April (à la liste secretaire AT april DOT org) et a dans le champ From l'adresse secretaire AT april DOT org au lieu de l'adresse courriel réelle de l'adhérent. Dans ces cas, c'est bien l'adhérent qui a envoyé directement un courriel avec son courrieleur.

On a eu aussi le même comportement avec un courriel arrivé sur la liste contact AT april DOT org envoyé via le formulaire de contact (la personne a sélectionné la catégorie « Demande de droits d'accès et de modification de données personnelles »). Le formulaire envoie le courriel à contact@, Sympa renvoie à l'expéditeur une demande de confirmation et la personne a répondu à ce courriel pour confirmer l'envoi sur la liste contact@.

Comme il y a des infos personnelles dans les courriels je ne les mets pas en ligne, je les envoie sur la liste admins@.

Historique

#1 - 14/09/2016 22:48 - Frédéric Couchet

- Description mis à jour

#2 - 14/09/2016 23:56 - Benjamin Drieu

- Statut changé de Nouveau à En cours de traitement

- Assigné à mis à Benjamin Drieu

Résolu **en partie** : un problème de ces gros pénibles de DKIM/DMARC. C'est résumé ici : https://www.sympa.org/manual/dmarc

Mais pour faire tl;dr : en gros, pour éviter de se faire rejeter certains mails envoyés par des domaines pénibles (laposte.net, yahoo.*, etc.), sympa doit réécrire le from: pour le remplacer par autre chose (par ex. le nom de la liste). C'est über pénible.

Du coup, j'ai ajouté le paramètre suivant à sympa.conf :
dmarc_protection_phrase name_email_via_list

Il ne résoud pas le problème mais se contente d'afficher le nom de la personne dans le from: réécrit.

Si certains comprennent mieux que moi les différentes implications de ces bouses, je suis preneur. Je crois avoir saisi mais que l'internet moderne est devenu compliqué pour envoyer des courriels ...

#3 - 15/09/2016 08:40 - Edouard Dausque

A noter que le vrai "From" reste bien dans le Reply-To, donc il devrait y avoir peu de gêne côté utilisateur.
Le comportement me semble logique car les serveurs de l'april ne sont pas sensés envoyer des mails avec un "From" différent de "@april.org".

Oui, l'internet moderne est devenu compliqué pour envoyer des courriels..
Petite note : http://www.openspf.org/SRS

#4 - 15/09/2016 12:12 - Frédéric Couchet

Edouard Dausque a écrit :

> A noter que le vrai "From" reste bien dans le Reply-To, donc il devrait y avoir peu de gêne côté utilisateur.

Ce n'est pas le cas dans les deux exemples que j'ai envoyé sur admins@ (Wed, 14 Sep 2016 22:44:05, Message-ID: <87eg4m6wkq.fsf@absinthe.couchet.org>). Le champ Reply-To ne contient pas le « vrai From ».

#5 - 15/09/2016 12:16 - Frédéric Couchet

Quelqu'un a fait un test avec une adresse en laposte.net ou @yahoo.fr en envoyant un courriel à secretaire par exemple ? ou demander à quelqu'un ayant une adresse de faire le test ?

#6 - 15/09/2016 12:16 - Frédéric Couchet

- % réalisé changé de 0 à 50

#7 - 22/09/2016 09:34 - Frédéric Couchet

Malgré la modification faite dans la config de Sympa J'ai demandé mardi soir sur #april si des personnes ont des adresses en laposte.net ou @yahoo.fr pour faire des tests. François Revol (mmu_man) et Grégory Chapuis (gregorio) ont répondu présents.

J'ai envoyé sur admins@ une mailbox avec les deux courriels de test.

L'adresse courriel de François Revol apparaît bien dans le From mais pas celle de Grégory Chapuis. Étrange.

De plus, le reply-to est positionné sur secretaire@ vu que c'est le champ From. Est-il possible avec Sympa/DMARC d'avoir aussi dans le reply-to l'adresse réelle de la personne qui a envoyé le message ?

Les risques de ne répondre qu'à la liste sont importants.

#8 - 22/09/2016 09:36 - Frédéric Couchet

La demande #1790 a été mise à jour par François Poulain.

Concernant le reply-to munging sur un email dmarc, ça à l'air codé comme ça.

Vu que le bugtracker de Renater est inaccessible aux non universitaires (et que en tant qu'ancien universitaire je n'ai aucune idée de comment me connecter à leur fédération), je vais poster un message sur la ML.

#9 - 22/09/2016 09:36 - Frédéric Couchet

La demande #1790 a été mise à jour par François Poulain.

Le courriel:

```
From: François Poulain <fpoulain@metrodore.fr>
To: Sympa-users@listes.renater.fr
Subject: DMARC protection breaks reply-to munging?
Date: Wed, 21 Sep 2016 11:06:26 +0200
X-Mailer: Claws Mail 3.11.1 (GTK+ 2.24.25; x86_64-pc-linux-gnu)

Hi,

It seems that the DMARC protection mode break the reply-to munging when
it is set to "all" or "sender", because the reply-to munging is done in
distribute_msg after the sender munging.

Maybe, the reply-to munging in distribute_msg should take care of the
existence of the X-Original-From header.

Maybe, other features should take care of the existence of the
X-Original-From header. Sender anonymisation, for example.

I was not able to connect to the bugtracker. Is it possible to do this
without being member of a french university?

Best regards.
François

--
```

Amha ya un petit patch à faire pour simplement tenir compte de X-Original-From dans le code de /usr/share/sympa/lib/List.pm vers la ligne 3078.

#10 - 22/09/2016 09:37 - Frédéric Couchet

La demande #1790 a été mise à jour par François Poulain.

Le patch suivant fonctionne. Testé depuis une adresse @laposte.net puis depuis une adresse honnête, sur mon serveur.

```
--- /tmp/List.pm    2016-09-21 11:15:27.200762248 +0200
+++ /usr/share/sympa/lib/List.pm    2016-09-21 11:35:37.950679623 +0200
@@ -3068,6 +3068,7 @@
     if ($self->{'admin'}{'reply_to_header'}) {
     unless ($hdr->get('Reply-To') && ($self->{'admin'}{'reply_to_header'}{'apply'} ne 'forced')) {
         my $reply;
+        my $from = $hdr->get('X-Original-From') ? $hdr->get('X-Original-From') : $hdr->get('From');

         $hdr->delete('Reply-To');
         $hdr->delete('Resent-Reply-To');
@@ -3075,9 +3076,9 @@
         if ($self->{'admin'}{'reply_to_header'}{'value'} eq 'list') {
         $reply = "$name\@$host";
         }elsif ($self->{'admin'}{'reply_to_header'}{'value'} eq 'sender') {
-        $reply = $hdr->get('From');
+        $reply = $from;
         }elsif ($self->{'admin'}{'reply_to_header'}{'value'} eq 'all') {
-        $reply = "$name\@$host,".$hdr->get('From');
+        $reply = "$name\@$host,".$from;
         }elsif ($self->{'admin'}{'reply_to_header'}{'value'} eq 'other_email') {
         $reply = $self->{'admin'}{'reply_to_header'}{'other_email'};
         }
```

#11 - 22/09/2016 09:38 - Frédéric Couchet

La demande #1790 a été mise à jour par Quentin Gibeaux.

J'ai patché la dernière version stable debian de sympa (celle qui est installée apparemment) avec le patch de PoluX, et ai commité sur le git la source.
Puis j'ai buildé et poussé sur le dépot april le paquet patché

#12 - 22/09/2016 09:39 - Frédéric Couchet

La réécriture du champ From par Sympa pose un souci avec certains
courrieleur (Mutt, Evolution, Roundcube).

Le champ From est par exemple réécrit ainsi :

From: Toto Tata via listedediffusion@april.org

Mais Mutt, Evolution et autre affiche

From: Toto Tata (toto@foo.bar) via listedediffusion@april.org

Comme l'indique la RFC https://tools.ietf.org/html/rfc5322

```
Strings of characters enclosed in parentheses are considered comments
    so long as they do not appear within a "quoted-string", as defined in
    section 3.2.4.  Comments may nest.
```

Les parentheses ajoutées par Sympa doivent donc être échappées :

From: Toto Tata "(toto@foo.bar)" via listedediffusion@april.org

#13 - 25/10/2016 15:37 - François Poulain

Aussi, mon patch est troué en ce sens que le champ X-Original-From a pu être forgé.

La bonne façon de faire est de changer le code de sympa pour faire la bidouille DMARC **après** quelques autres bidouilles comme le reply-to munging. Mais c'est un gros travail.

Par ailleurs, ce code n'est pas près d'évoluer car il n'y a malheureusement pas de paquet sympa backporté dans Jessie.

Perso je propose, quitte à avoir des sources à maintenir, de migrer sympa vers la version stable upstream (la 6.2). Le mode de protection DMARC y sera mieux géré et en cadeau bonus on aura le droit à une css façon web 2.0.

#14 - 01/02/2017 22:20 - François Poulain

Toujours d'actu. Perso je défend l'installation de sympa 6.2. Faut vérifier que les scénario dtc ne cassent pas. Pour info, niveau maintenance de sécurité l'enjeu n'a pas l'air lourd :
https://lists.debian.org/cgi-bin/search?P=sympa&DEFAULTOP=or&B=Gdebian-security-announce&SORT=&HITSPERPAGE=10 (c'est pas du wordpress, quoi)

#15 - 09/06/2017 16:54 - François Poulain

- Statut changé de En cours de traitement à Fermé

Ça viendra avec Debian Stretch.