Admins - Anomalie #5025

Blacklister l'adresse contact@chic-time.fr

14/12/2020 10:54 - Frédéric Couchet

Statut:	Fermé	**Début:**	14/12/2020
Priorité:	Normale	**Echéance:**	
Assigné à:	Frédéric Couchet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Mars 2021	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Bonjour, l'adresse contact@chic-time.fr a fait du spam massif, et c'est la deuxième fois.

Merci de blacklister cette adresse au niveau de Postfix.

Historique

#1 - 14/12/2020 11:01 - Frédéric Couchet

- Description mis à jour

#2 - 14/12/2020 11:01 - Frédéric Couchet

Voir aussi https://agir.april.org/issues/5025

#3 - 14/12/2020 11:20 - Quentin Gibeaux

- Version cible changé de Backlog à Décembre 2020

#4 - 14/12/2020 11:25 - Quentin Gibeaux

- Statut changé de Nouveau à Résolu

c'est fait :

```
(April) root@mail:/etc/postfix[master$]# git show
(...)
--- a/postfix/hash/sender_access
+++ b/postfix/hash/sender_access
@@ -25,4 +25,5 @@ juliasxnylon@gmx.com        REJECT
 replyonline@ids.apple.org  REJECT
 contact@internet-libre.eu  REJECT
 contact@internet-libre.fr  REJECT
+contact@chic-time.fr       REJECT

(April) root@mail:/etc/postfix[master*$]# postfix reload
```

#5 - 26/12/2020 00:36 - Christian P. Momon

- Assigné à mis à Quentin Gibeaux

#6 - 30/12/2020 22:13 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#7 - 22/01/2021 08:30 - Frédéric Couchet

- Statut changé de Fermé à Confirmé

L'adresse contact@chic-time.fr nous fait du spam massif. Il vaudrait vérifier le blacklistage.

#8 - 22/01/2021 08:37 - Frédéric Couchet

- Version cible changé de Décembre 2020 à Janvier 2021

#9 - 22/01/2021 10:10 - Frédéric Couchet

- Assigné à changé de Quentin Gibeaux à Frédéric Couchet

#10 - 22/01/2021 10:13 - Frédéric Couchet

Le fichier /etc/postfix/hash/sender_access avait bien été modifié mais le fichier sender_access.db n'avait pas été généré, donc

1. cd /etc/postfix/hash/sender_access
2. postmap sender_access

Test d'envoi d'un courriel en utilisant contact@chic-time.fr en From, le courriel est bien rejeté (/var/log/mail.log) :

Jan 22 10:06:19 mail postfix/submission/smtpd[5139]: NOQUEUE: reject: RCPT from lfbn-idf3-1-1027-210.w90-46.abo.wanadoo.fr[90.46.10.210]: 554 5.7.1 <contact@chic-time.fr>: Sender address rejected: Access denied; from=<contact@chic-time.fr> to=<fcouchet@april.org> proto=ESMTP helo=<mail.couchet.org>

#11 - 22/01/2021 10:13 - Frédéric Couchet

- Statut changé de Confirmé à Fermé

#12 - 11/03/2021 16:36 - Frédéric Couchet

- Statut changé de Fermé à En cours de traitement

- Version cible changé de Janvier 2021 à Mars 2021

De nouveau des spams en provenance de chic-time.fr. Les spammeurs ont visiblement changé leur méthode d'envoi :

```
Mar 11 15:48:10 mail postfix/smtpd[16054]: 5AF1A149B: client=localhost[127.0.0.1]
Mar 11 15:48:10 mail postfix/cleanup[16048]: 5AF1A149B: message-id=<0102017821c24e31-0df71ce1-a290-4a2f-8803-518a83de5867-000000@eu-west-1.amazonses.com>
Mar 11 15:48:10 mail opendkim[12116]: 5AF1A149B: no signing table match for 'contact@chic-time.fr'
Mar 11 15:48:10 mail opendkim[12116]: 5AF1A149B: message has signatures from chic-time.fr, amazonses.com
Mar 11 15:48:10 mail opendkim[12116]: 5AF1A149B: DKIM verification successful
Mar 11 15:48:10 mail opendkim[12116]: 5AF1A149B: s=korlgceugryh2wyxqyrv3wivzxgjh6oa d=chic-time.fr SSL
Mar 11 15:48:10 mail postfix/qmgr[16022]: 5AF1A149B: from=<SRS0=nRcZ=IJ=eu-west-1.amazonses.com=0102017821c24e31-0df71ce1-a290-4a2f-8803-518a83de5867-000000@april.org>, size=57341, nrcpt=1 (queue active)
Mar 11 15:48:10 mail postfix/smtp[16051]: 79A4A145A: to=<mad@april.org>, relay=127.0.0.1[127.0.0.1]:10024, delay=4.4, delays=0.34/0/0/4, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 5AF1A149B)
Mar 11 15:48:11 mail postfix/local[16170]: 5AF1A149B: to=<mad@april.org>, relay=local, delay=0.67, delays=0.46/0/0/0.21, dsn=2.0.0, status=sent (forwarded as D72E2145A)
Mar 11 15:48:11 mail postfix/qmgr[16022]: 5AF1A149B: removed
```

j'ai ajouté chic-time.fr dans /etc/postfix/hash/domain_access.map (puis cd .. ; make) avec un reject peut-être faudrait-il mettre aussi amazonses.com

#13 - 11/03/2021 19:16 - Frédéric Couchet

Solution mise en œuvre : le filtre des headers.

```
vi /etc/postfix/conf.d/50-restrictions.conf
```

ajout de

```
header_checks = regexp:/etc/postfix/header_checks
```

création de /etc/postfix/header_checks contenant

```
/^From:.*contact@chic-time.fr.*/ REJECT
```

Génération de la config et reload de postfix :

```
cd /etc/postfix
make
postfix reload
```

Vérification avec

```
grep chic-time /var/log/mail.log
```

```
Mar 11 19:04:58 mail postfix/cleanup[15868]: 50949139C: reject: header From: Chic Time <contact@chic-time.fr> from a52-154.smtp-out.eu-west-1.amazonses.com[54.240.52.154]; from=<SRS0=ezvM=IJ=eu-west-1.amazonses.com=0102017822768b01-73d56c87-152e-4385-b2cc-c9a3
```

```
85505ec0-000000@april.org> to=<chapril-request@april.org> proto=ESMTP helo=<a52-154.smtp-out.eu-west-1.amazons
es.com>: 5.7.1 messa
ge content rejected
```

#14 - 31/03/2021 21:58 - Quentin Gibeaux

- Statut changé de En cours de traitement à Fermé

- Version cible changé de Mars 2021 à Avril 2021

#15 - 31/03/2021 21:59 - Quentin Gibeaux

- Version cible changé de Avril 2021 à Mars 2021

#16 - 10/04/2021 08:55 - Frédéric Couchet

Nouveaux spams, ce coup-ci c'est @chic-time.com (et non plus .fr). Modification de /etc/postfix/header_checks pour ajouter

```
/^From:.*contact@chic-time.com.*/ REJECT
```

Puis

```
cd /etc/postfix
make
postfix reload
```

Puis

```
git commit -a
```

#17 - 12/04/2021 14:27 - Frédéric Couchet

je n'avais pas vu que ce n'était pas l'adresse contact@ de chic-time qui spamait ce coup-ci mais l'adresse audrey@. En conséquence :

Modification de /etc/postfix/header_checks

```
/^From:.*@chic-time.fr.*/ REJECT
/^From:.*@chic-time.com.*/ REJECT
```

Puis

```
cd /etc/postfix
make
postfix reload
```

Vérification dans les logs :

Apr 12 12:20:09 mail postfix/cleanup[32485]: 461225AB: reject: header From: Audrey de Chic Time <audrey@chic-time.com> from a52-155.smtp-out.eu-west-1.amazonses.com[54.240.52.155]; from=<SRS0=jqb3=JJ=eu-west-1.amazonses.com=01020178c5987ce6-9abb2ed0-c8da-4894-8222-a583053728b8-000000@april.org> to=<XXXXX> proto=ESMTP helo=<a52-155.smtp-out.eu-west-1.amazonses.com>: 5.7.1 message content rejected