LE SERVEUR EST UTILISE POUR ENVOYER DU SPAM

VÉRIFIER QUE LE SERVEUR BM N'EST PAS RELAI OUVERT

Par défaut postfix est configuré pour être relai ouvert pour le serveur lui-même, ce qui permet aux différent services (webmail, EAS) d'envoyer des mails, il est possible via la console d'administration d'ajouter de nouvelles IP de confiance qui auront le droit d'envoyer des mails via le serveur BM, il s'agit en général de serveur du SI interne (logiciel de gestion des congés, monitoring, etc).

Si un de ces serveur est compromis, un spammer pourra alors utiliser le serveur BM pour envoyer du spam.

Vous pouvez détecter le problème par la présence de beaucoup de ligne du type :

```
Jun 21 08:34:30 centos7 postfix/smtpd[16863]: connect from gateway[192.168.122.111]
Jun 21 08:34:48 centos7 postfix/smtpd[16863]: 1C205316C411: client=gateway[192.168.122.111]
Jun 21 08:34:58 centos7 postfix/cleanup[16869]: 1C205316C411: message-id=<>
Jun 21 08:34:58 centos7 postfix/qmgr[16801]: 1C205316C411: from=<user1@domain.com>, size=233, nrcpt=1
(queue active)
Jun 21 08:34:59 centos7 postfix/smtp[16821]: 1C205316C411: to=<user2@anotherdomain.net>, relay=smtp.
anotherdomain.net[XX.XX.XX.XX]:25, delay=20, delays=20/0/0.35/0.09, dsn=2.0.0, status=sent (250 2.0.0
Ok: queued as 2F10238)
Jun 21 08:34:59 centos7 postfix/qmgr[16801]: 1C205316C411: removed
Jun 21 08:35:04 centos7 postfix/smtpd[16863]: disconnect from gateway[192.168.122.111]
```

La ligne client indique ici l'IP du serveur qui a émis ce mail, ici 192.168.122.111, s'il n'est pas légitime cela signifie que ce serveur est compromis et qu'il est utilisé pour envoyer du spam

les actions à mener :

- supprimer l'ip du serveur incriminé dans la console d'administration BM et sauvegarder la configuration

DÉTECTER L'UTILISATEUR UTILISÉ POUR ENVOYER DU SPAM

La plupart du temps le problème vient d'un spammer qui a trouvé, souvent par bruteforce, le mot de passe d'un compte utilisateur et il va l'utiliser pour envoyer du SPAM.

Vous pouvez identifier les connexions smtp avec la présence de beaucoup de lignes du type :

```
May  5 00:08:55 hermes postfix/smtpd[27666]: 7E079B666CC: client=unknown[46.48.93.60],
sasl_method=LOGIN, sasl_username=admin
```

Les actions à mener :

- changer le mot de passe de l'utilisateur : soit dans BM, soit dans l'annuaire.
- fermer toutes les sessions de cet utilisateur avec la commande :

```
bm-cli user logout login@domain.com
```

- nettoyer la queue postfix pour supprimer les mails en attente d'envoi, pour supprimer tous les mails en queue de l'utilisateur login@domain.net

```
postqueue -p | tail -n +2 | awk 'BEGIN { RS = "" } /login@domain\.net/ { print $1 }' | tr -d '*!'
| postsuper -d -
```

> Cette commande va supprimer tous les mails dans la queue de l'utilisateur, qu'ils soient des SPAM ou des mail légitimes envoyés par l'utilisateur, cette commande peut être longue.

COMMENT SE PROTÉGER DE CES ATTAQUES ?

Limiter les attaques par brute-force

Pour limiter les tentatives de bruteforce, vous pouvez utiliser le plugin password-bruteforce, celui ci va bloquer les tentatives de connexion pendant 20 après 3 échecs d'authentification.

Mettre en place une politique sur les mots de passe

Dans le cas ou vous n'utilisez pas un annuaire pour gérer les utilisateurs, vous pouvez utiliser le plugin `password-sizestrength` qui permet de mettre en place une politique afin de forcer des règles pour les mots de passe.

COMMENT DÉTECTER LE PROBLÈME AU PLUS TÔT ?

Une solution de monitoring permet de détecter rapidement le problème et de réagir avant que votre serveur ne soit blacklisté par les différents services anti-spam.

Bm-tick permet de mettre en place des alertes basées sur une augmentation importante du nombre de mail dans la queue postfix. Vous pouvez configurer cette alerte via le alert builder ou directement utiliser le script suivant :

Ce script va envoyer un mail d'alerte à `admin@domain.net` dès que la queue postfix atteint les 200 messages. En fonction de votre installation il est bien évidemment possible de configurer ces valeurs.