xmpp.chapril.org - Demande #4461

Contre-mesures envers les spambots actuels

07/05/2020 08:13 - pitchum .

Statut:	Fermé	**Début:**	07/05/2020
Priorité:	Normale	**Echéance:**	
Assigné à:	pitchum .	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Sprint 2020 mai		
Difficulté:	4 Fastidieux		

Description

Après investigration dans la BDD je pense qu'on peut facilement identifier un certain nombre de comptes XMPP douteux.
72 comptes actuels n'ont pour seuls contacts : garryh@exploit.im, jabservice@jabbim.com, jabservise@xmpp.jp.
Et encore, ils n'ont pas même pas demandé d'autorisation d'abonnement.
Les symptômes :

```
sudo -u ejabberd ejabberdctl get_roster xxxxx chapril.org
garryh@exploit.im               none    out
jabservice@jabbim.com           none    out
jabservise@xmpp.jp              none    out
```

Ces comptes ont commencé à fleurir à partir du 9 avril.
Je ne sais pas encore quel impact négatif ses comptes peuvent avoir et s'il serait utile ou non de réagir.

En attendant j'ai créé une vue dans la BDD pour lister les comptes concernés.

```
psql -U ejabberd -h localhost ejabberd -c "select * from v_user_probable_spammer" -t
```

Demandes liées:

Lié à xmpp.chapril.org - Demande #5065: Lutte contre les spambots, améliorati...	**Fermé**	**27/12/2020**

Historique

#1 - 10/05/2020 17:32 - pitchum .

- Sujet changé de spambots, que faire ? à Contre-mesures envers les spambots actuels

- Statut changé de Nouveau à En cours de traitement

- Priorité changé de Normale à Élevée

- % réalisé changé de 0 à 20

- Difficulté changé de 2 Facile à 4 Fastidieux

J'ai mis en place des règles *fail2ban* qui devraient fortement diminuer la nuisance des comptes de spam créés.
Cf. la forge April.

Malheureusement ces règles n'empêchent pas la création des comptes car les créations de comptes se font toujours avec des adresses IP différentes. En revanche une fois créés, les comptes sont utilisés avec des IPs qui changent peu (une même IP a été utilisé jusqu'à 21 fois en moins de 48h. C'est donc cette IP que je bloque, pendant 48h. Ça réduira la nuisance causée aux 3 serveurs XMPP ciblés.

Pour l'instant je m'occupe de supprimer ces comptes bidons à la main à posteriori.

#2 - 16/05/2020 22:53 - Christian P. Momon

- Version cible mis à Backlog

#3 - 02/06/2020 20:06 - pitchum .

- Statut changé de En cours de traitement à Résolu

- % réalisé changé de 20 à 100

Pas de récidive depuis un bon moment.
Le fail2ban ne sert plus du tout. Je le laisse quand même à tout hasard. Et puis il pourra éventuellement être complété plus tard.
Je clôture.

#4 - 03/06/2020 21:50 - pitchum .

- Statut changé de Résolu à Fermé

#5 - 04/06/2020 00:55 - Christian P. Momon

- Version cible changé de Backlog à Sprint 2020 mai

#6 - 26/12/2020 20:01 - Adrien Bourmault

- Statut changé de Fermé à En cours de traitement

- Assigné à changé de pitchum . à Adrien Bourmault

- Priorité changé de Élevée à Normale

- Version cible changé de Sprint 2020 mai à Backlog

#7 - 27/12/2020 17:47 - Adrien Bourmault

- Lié à Demande #5065: Lutte contre les spambots, amélioration des captchas et contre-mesures ajouté

#8 - 27/12/2020 17:54 - Adrien Bourmault

- Statut changé de En cours de traitement à Fermé

- Assigné à changé de Adrien Bourmault à pitchum .

#9 - 27/12/2020 18:01 - Adrien Bourmault

- Version cible changé de Backlog à Sprint 2020 mai