Admins - Anomalie #3254

Les chans IRC de l'april sont victime d'un spam massif

06/08/2018 09:55 - Quentin Gibeaux

Statut:	Fermé	**Début:**	06/08/2018
Priorité:	Normale	**Echéance:**	
Assigné à:	Frédéric Couchet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Octobre 2018	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Des bots viennent massivement spamer le serveur IRC freenode (voir https://freenode.net/news/spambot-attack), les chans april et april-admin sont touchés.

Benj a bricolé un bot (bot-cop) pour kicker sur certains mots clés, mais il y a peut être d'autres mesures à prendre.

Historique

#1 - 07/08/2018 11:53 - Benjamin Drieu

- Statut changé de Nouveau à Confirmé

Le bot bot-cop a été déactivé pour le moment. Il est sur /srv/copbot sur la VM bots. C'est un bot bricolé, donc sans configuration et auto-op.

À la suggestion de porkepix, le bot sigyn a été invité sur les channel #april et #april-admin.

Il est malheureusement un peu facho et a kliné vivivi. J'ai écrit kline@freenode.net pour le déblacklister.

Réponse de Freenode:

```
This message has been automatically generated in response to the
creation of a trouble ticket regarding:

       "Whitelist galanga.april.org (88.191.250.11)",

a summary of which appears at bottom of this message.

PLEASE READ CAREFULLY: We need your internet-routable IP address
to service all network ban (also known as  k-line or d-line)
issues. If you did not include this information in your original
request (quoted below), please take a moment now to point your
browser at http://myip.dk/ ... then reply to this email
with your IP address and hostname.
It's also helpful if you let us know what nick you were using at the
time.

If your request did not concern a network ban, there is no need to reply at
this time.

Your ticket has been assigned an ID of [freenode.net #210990].

Please include the string:

         [freenode.net #210990]

in the subject line of all future correspondence about this issue.
```

En attente.

#2 - 10/08/2018 11:45 - Christian P. Momon

La demande a été prise en compte, vivivi est de retour \o/

#3 - 10/08/2018 11:49 - Christian P. Momon

À propos de Sigyn : https://github.com/freenode/Sigyn

Deux points intéressants :

- si on a des demandes (whitelist, unban…): « feel free to join #freenode-sigyn and ask in there » ;
- si besoin ponctuel de débannir : « If opped in your channel you can ask Sigyn to unkline an user, /**msg Sigyn unkline** , you have a dozen minutes to do so after the kill/kline, it only works if the user was banned due to abuse detected in your channel. »

#4 - 10/08/2018 15:21 - Cédric Heintz

D'ailleurs, le canal #april-admin on pourrait pas le mettre en mode +r ?
Pour que uniquement les utilisateurs authentifiés puissent aller dessus.
Ce serait déjà ça...

#5 - 13/08/2018 10:56 - Frédéric Couchet

- Description mis à jour

#6 - 14/08/2018 16:32 - Frédéric Couchet

Outre le mode +r une personne a suggéré d'utiliser le mode +q $~a sur #april.

Selon https://freenode.net/kb/answer/registration

> If a channel is set to mode +r, you won't be able to join it unless you are registered and identified to NickServ. If you try to join, you might be forwarded to a different channel. If a channel is set toquiet unregistered users (mode +q $~a), you won't be able to speak while on that channel unless you are registered and identified.

Avec le mode +r une personne/un bot ne peut pas rejoindre un salon si elle n'est pas identifiée. Mais si la personne est déjà sur le salon, après le changement de mode, elle peut causer.

Avec le mode +q $~a la personne/le bot non identifiée peut rejoindre le salon mais ne peut pas parler tant qu'elle n'est pas identifiée. Ou tant qu'elle n'est pas voicée (voir ci-dessous)

J'ai fait des tests sur #april-admin.

Pour changer le mode, il faut passer op, et en étant sur #april-admin faire par exemple

> /mode #april-admin +r

ou

> /mode #april-admin +q $~a

Pour enlever ces modes il faut faire :

> /mode #april-admin -r

ou

> /mode #april-admin -q $~a

Cela a bien fonctionné sur #april-admin mais l'une des conséquences a été de bloquer le bot vivivi (qui n'est pas identifié). Même avec les modes +r et +q $~a on peut donner à un nick la possibilité de parler même sans être identifié. Pour cela, par exemple pour permettre à vivivi[4] de causer :

> /msg ChanServ VOICE #april-admin vivivi[4]

Pour enlever le voice :

> /msg ChanServ DEVOICE #april-admin vivivi[4]

Mais la commande voice ne permet de voicer qu'un nick (pas de regexp) et vivivi change régulièrement de numéro. Vu son fonctionnement actuel (changement de numéros en fonction du nombre d'alertes icinga), il va être difficile d'avoir un vivivi identifié.

Un autre problème des modes qui restreignent la possibilité de rejoindre un salon/de causer est que cela bloquerait potentiellement une personne qui voudrait signaler un souci avec le SI et qui utiliserait un webchat par exemple. Alors, la personne pourrait signaler le problème sur #april ou un autre salon. Mais #april subit aussi du spam et donc il serait logique de mettre le même mode sur sur #april-admin.

#7 - 15/08/2018 21:58 - Frédéric Couchet

J'ai modifié, au moins temporairement la config du salon #april car la situation devenait vraiment chiante. Il faut désormais être enregistré sur freenode pour parler sur #april ou être voicé (le nick doit avoir le mode +v). J'ai mis le mode +q $~a. Pour cela :

/mode #april +q $~a

L'option +r bloque totalement l'accès aux nicks non enregistrés et laisse peu de chance à une personne de comprendre qu'il faut avoir un nick enregistré, avec le mode +q $q~a la personne peut se connecter sur #april, le topic s'affiche et indique qu'il faut être enregistré pour parler. Et si la personne essaye de parler un message d'erreur s'affiche (qui dépend du client IRC).

Une autre option aurait été de mettre un +r et un +f #april-acceuil. Avec ces deux modes, les personnes ayant un nick non enregistrées sont redirigées vers le salon #april-accueil. Cela fonctionne plutôt bien avec un client irc normal avec un webchat comme par exemple https://www.april.org/salon-irc-de-lapril le renvoi vers le 2e salon n'est pas clair du tout. La fenêtre reste sur le salon #april inutilisable donc la personne a 0,01% de chance de comprendre ce qui se passe.

Il y avait aussi l'option +S pour restreindre l'accès aux personnes qui se connectent en SSL/TLS, mais cela fonctionne pas avec la majorité des interfaces web utilisées.

Au final, le mode +q $~a me paraît le meilleur choix.

J'ai modifié le topic du salon pour que ce soit précisé, j'ai ajouté « Il faut être enregistré sur freenode pour parler, pour s'enregistrer voir https://apr1.org/Vp » https://apr1.org/Vp étant un lien court vers https://debian-facile.org/doc:reseau:freenode#s-enregistrer-sur-freenode Vous pouvez modifier si vous trouvez une page plus simple. J'ai mis un lien court avec les topic sur freenode sont limités en nombre de caractères (390 a priori).

J'ai aussi ajouté une note sur https://www.april.org/salon-irc-de-lapril

Au niveau des bots April présents sur #april pour pouvoir parler soit ils doivent être enregistrés soit ils doivent être voicés par un opérateur (op) du salon.

Donc, pour la revue hebdo par exemple il faudra qu'hebdobot soit enregistré auprès de freenode ou alors être voicé après sa connexion. Pour voicer hebdobot il faut envoyer un message à chanserv :

/msg ChanServ VOICE #april hebdobot

Mise à jour 21 août :

Pour pouvoir faire un VOICE ou DEVOICE être opérateur du salon ne semble pas suffire. C'est peut-être un problème au niveau des droits d'accès du salon.

Il faut soit faire partie des « founders » du salon. Soit il faut ajouter le flag +v dans l'access list du salon pour qu'une personne puisse faire un voice ou devoice.

Pour ajouter le flag +v à cpm_screen :

/msg ChanServ FLAGS #april cpm_screen +v

Pour voir les access list :

/msg ChanServ ACCESS #april list

Finalement j'ai passé cpm_screen en founder. À noter « Only 4 founders allowed per channel. » J'ai donc vu supprimer Sp4rKy des founders. Pour cela :

/msg ChanServ access #april del Sp4kKy founder
/msg ChanServ access #april add cpm_screen founder

Truc bizarre : après avoir passé cpm_screen en founder, ChanServ a devoicé alexandrie sur #april. Je ne sais pas pourquoi et je n'ai pas testé pour voir dans quel cas cela se produit. J'ai remis le voice à alexandrie.

A noter que j'ai du passer Sigyn (le bot de freenode qui k-line (kill) les bots qui spamment sur freenode) op sur #april. Selon Porpekix, avec le nouveau mode igyn peut plus voir les messages de spam, seuls les OP vont continuer de les voir. Et si les messages sont plus vus, plus de k-line.

J'ai aussi voicé alexandrie mais il faudra le faire chaque jour vu qu'alexandrie se déconnecte/reconnecte à minuit. Ou alors enregistré alexandrie. Mais bon, c'est un problème mineur.

#8 - 16/08/2018 15:19 - Christian P. Momon

Vivivi est à nouveau banni, (April) root@galanga:/srv/nagios-irc-bot/vivivi.log :

```
<<< :weber.freenode.net 465 vivivivi :You are banned from this server- Please do not spam users or channels on
 freenode. If in error, please contact kline@freenode.net. (2018/8/16 11.00)
Trying to handle event 'yourebannedcreep'.
<<< ERROR :Closing Link: ns3.april.org (*** Banned )
```

A priori, pour les demandes de whitelist, il faut fournir l'adresse PTR (donc ns3.april.org à la place de galanga.april.org).

Sur IRC #april-admin:

```
14:32 < madix> s'il y a une demande de whitelist, demander le whitelist de toutes nos IP/noms de sortie
14:50 < cpm_screen> moui, QGuLL  comment trouver les autres PTR ?
14:52 < QGuLL> "dig ip"
14:53 < QGuLL> plutôt dig PTR 11.250.191.88.in-addr.arpa
14:54 < QGuLL> avec l'ip inversée
14:55 < cpm_screen> moui, mais comment je trouve la bonne ip ?
14:55 < QGuLL> on a pas 56 ip publiques à l'april
14:55 < QGuLL> regarde les ip des différents serveurs
14:55 < QGuLL> et fai
14:55 < QGuLL> + ip failover
```

Envoi d'une demande de whitelist :

```
Le 16/08/2018 à 15:11, Christian Pierre MOMON a écrit :
>
>  Dear Kline,
>
>  In our bot logs :
>
> << :cherryh.freenode.net 465 vivivivi :You are banned from this server-
> Please do not spam users or channels on freenode. If in error, please
> contact kline@freenode.net. (2018/8/16 11.00)
>
>
>  So, this is a request for whitelist our bot servers. The PTR list:
>
> ns3.april.org
> virola.april.org
> calamus.april.org
> vip.april.org
>
>  Our channels: #april, #april-admin, #april-accueil, #april-chapril
>
>  Our organisation: association April (https://www.april.org/).
>
>  Thank's a lot for your help \o/
>
>  Regards,
>
>  Christian (Cpm).
```

La réponse automatique :

```
Le 16/08/2018 à 15:11, Freenode Support via RT a écrit :
> Sujet : [freenode.net #211202] AutoReply: Request for unban and whitelist
> Greetings,
> […]
> Your ticket has been assigned an ID of [freenode.net #211202].
>
> Please include the string:
>
>          [freenode.net #211202]
>
> in the subject line of all future correspondence about this issue.
> To do so, you may reply to this message.
>
>                         Thank you,
>                         kline@freenode.net
```

#9 - 17/08/2018 11:29 - Christian P. Momon

Vivivi est de retour sur #april-admin. Courriel de confirmation reçu :

```
Le 17/08/2018 à 11:20, grumble via RT a écrit
> De : kline@freenode.net
> Sujet : Re: [freenode.net #211202] Request for unban and whitelist
> Hi,
>
> the K-Line has been removed and the exempts/whitelists have been updated.
>
> Kind regards,
```

```
> grumble
```

#10 - 21/08/2018 08:42 - Frédéric Couchet

J'ai également voicé louxor sur #april

#11 - 31/08/2018 13:52 - Quentin Gibeaux

J'ai tenté de passer vivivi en SSL par la modification de son code : option SSL => 1 et port 6697, mais derrière le bot n'apparaissait pas sur le salon, sans que les logs ne viennent parler d'un problème de connexion.
En tcpdump je vouyais bien du traffic (aller/retour) vers le port 6697. J'ignore quel est le problème, mais en l'état ça ne fonctionne pas.

#12 - 31/08/2018 14:02 - Frédéric Couchet

Le spam IRC se poursuit sur le salon #april-admin. Comme on ne peut pas vraiment register vivivi et ses multiples noms, une possibilité serait de passer le salon en mode « secure connexion only ».

Pour les membres de l'équipe salariée qui utilisent Pigdin. Voici les modifications à faire :

Pour Freenode :

Dans Pidgin, aller dans Comptes -> Gérer les comptes -> sélectionner le compte freenode -> Cliquer sur modifier -> Cliquer sur l'onglet Avancé puis remplacer 6667 par 6697 dans Port, cocher la case "Utiliser SSL", cocher la case "Authenticate with SASL".

Pour Geeknode c'est la même chose sauf qu'il **ne faut pas cocher** la case "Authenticate with SASL". Je ne sais pas du tout pourquoi il ne faut pas cocher la case.

#13 - 10/09/2018 10:38 - Frédéric Couchet

Bot-cop a été remis sur le salon (je ne sais pas quand) mais il kicke incorrectement :

[09/10/18 10:32] <PoluX[1]_> si ça marchait fallait pas toucher. :) *** bot-cop (~bot-cop@virola.april.org) has kicked PoluX[1]_ off channel #april-admin: PoluX[1]_

```
&lt;madix&gt; PoluX[1]_: j'allais te dire (avant que tu te fasses kické) que c'était l'upgrade automatique
                debian stretch
                 *** You have been kicked off channel #april-admin by bot-cop (~bot-cop@virola.april.org
): madix

&lt;QGuLL&gt; il ne kick pas pour rien, il faut pas dire a + l + l + a /o\
```

Merci svp de virer bop-cop ou de le corriger.

#14 - 12/09/2018 16:01 - Frédéric Couchet

En fait, il suffit d'enregistrer vivivi :

<olasd> madix: je comprends pas tes remarques à propos de vivivi sur #3254; le fait d'avoir un compte freenode identifié ne t'empêche pas de changer de nick

<olasd> /msg nickserv identify nick password fonctionne quel que soit ton nick courant

<olasd> (avec nick l'identifiant du compte dans la commande identify)

<olasd> pareil pour l'authentification par certificat client tls, ça va fonctionner et t'associer à ton compte enregistré quel que soit le nick avec lequel tu te connectes

<madix> olasd: tu veux dire que si on register vivivi, et qu'à un moment vivivi devient vivivi[1] il est toujours considéré comme identifié et il peut donc causer sur le salon ?

<olasd> ben oui

<madix> je ne savais pas, je pensais que si on change de nick il faut s'identifier de nouveau avec le nouveau nick

<madix> mais si ce n'est pas le cas, c'est très bien

#15 - 30/09/2018 15:52 - Benjamin Drieu

J'ai fait un mode +q $~a sur #april-admin
Et patché vivivi et agirbot (seuls bots à ma connaissance à utiliser ce channel).

J'ai enregistré les nicks agirbot et vivivi sur nickserv et poussé les mdp sur le keepass admin.

Botcop n'a donc plus lieu d'être, je le débranche pour le moment.

#16 - 30/09/2018 15:53 - Benjamin Drieu

Il faudrait maintenant patcher les bots de #april (alexandrie et hebdobot).

#17 - 01/10/2018 12:28 - Quentin Gibeaux

J'ai passé #april-admin en +r ("Prevents users who are not identified to services from joining the channel.") pour filtrer les aller/venu des bots

#18 - 01/10/2018 17:10 - Christian P. Momon

Avancement pour Hebdobot : https://agir.april.org/issues/3329#note-2
Reste une étape de test à faire avant déploiement.

#19 - 26/10/2018 16:39 - Frédéric Couchet

On ne sait pas trop si le spam continue sur freenode (pas de news sur freenode.net) mais on peut supposer que c'est peut-être terminer.

J'enlève donc sur #april et #april-admin le mode +q $~a

Pour cela passer op, puis sur #april (et même principe pour #april-admin)

/mode #april -q $~a

Si le spam revient remettre le mode :

/mode #april +q $~a

#20 - 26/10/2018 16:54 - Quentin Gibeaux

J'ai enlevé le +r sur #april-admin

#21 - 29/10/2018 09:49 - Frédéric Couchet

- Version cible changé de Backlog à Octobre 2018

#22 - 29/10/2018 09:51 - Frédéric Couchet

- Statut changé de Confirmé à Résolu

#23 - 07/11/2018 21:14 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#24 - 26/12/2020 02:20 - Christian P. Momon

- Assigné à mis à Frédéric Couchet