Le greylisting marche toujours très bien, malgré les critiques

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 mai 2009

https://www.bortzmeyer.org/greylisting.html

Sur tous les serveurs de messagerie que je gère, j'active le "*greylisting*", une technique simple mais géniale, qui élimine la moitié des spams avant qu'ils ne soient envoyés. Depuis des années que je m'en sers, les critiques n'ont pas manqué, tournant en général autour de la remarque que « Les spammeurs peuvent s'adapter facilement, en gérant une file d'attente, et donc le "*greylisting*" ne servira plus à rien. ».

Ce raisonnement semble raisonnable mais il a comme gros défaut... de n'être qu'un raisonnement. La réalité le dément régulièrement. Le "*greylisting*" est quasiment aussi efficace qu'au premier jour. (Ce qui n'arrête pas les critiques, qui en général n'ont jamais l'idée de **mesurer** les techniques anti-spam au lieu de supposer.)

Pourquoi les spammeurs, en général très prompts à s'ajuster à toutes les techniques anti-spam, n'ont-ils rien fait contre le "*greylisting*" ? Je ne voudrais pas me mettre à faire de la supposition hasardeuse mais je pense qu'une des raisons est que peu de gens utilisent le "*greylisting*". Tant que la majorité des serveurs ne sont pas protégés, les spammeurs n'ont pas de raison de se fatiguer à contourner cette protection, qui reste donc la plus rentables des techniques anti-spam.

C'est l'illustration parfaite d'un vieux principe de sécurité : « Il n'est pas nécessaire de courir plus vite que l'ours, il suffit de courir plus vite que les autres randonneurs. » Maintenant, peut-être qu'en lisant cet article, des millions de gens vont activer le "*greylisting*", changeant ainsi l'équation [Caractère Unicode non montré [1]].

Petite note technique : j'utilise en général Postfix et le logiciel de "*greylisting*" est, soit postgrey <http://postgrey.schweikert.ch/>, soit l'excellent greyfix <http://www.kim-minh.com/pub/greyfix/>. Le premier se configure ainsi :

1. Car trop difficile à faire afficher par LaTeX

```
# postfix/main.cf
smtpd_recipient_restrictions = permit_mynetworks, [...]
        check_policy_service inet:127.0.0.1:60000
```

postgrey étant lancé par `/usr/sbin/postgrey --pidfile=/var/run/postgrey.pid --daemonize --inet=127.0.0.1:60000`. Le second se configure avec :

```
smtpd_recipient_restrictions = permit_mynetworks, [...]
          check_policy_service unix:private/greyfix
```

greyfix n'est pas lancé séparement mais par Postfix et doit donc être configuré dans le `master.cf` :

```
greyfix    unix  -       n       n       -       -       spawn
  user=nobody argv=/usr/local/sbin/greyfix --greylist-delay 300 --network-prefix 28
```

On voit alors dans le journal de nombreux rejets de spam, qui ne réessaient qu'exceptionnellement :

```
May  5 23:45:23 aetius postfix/smtpd[31070]: NOQUEUE: reject: RCPT from unknown[200.121.246.20]: 450 4.7.1 <
```

Le "*greylisting*" est désormais officiellement documenté dans le RFC 6647[2].

2. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6647.txt`