

grey listing au Laboratoire ARAGO

ou l'éradication des SPAM

09-Jan-2006

Cela fait maintenant 6 jours que le service informatique à installé un système antispam appelé *GreyListing (Liste Grise)*

Les résultats sont **éloquents**, le taux de Spam et de virus reçus en 3 jours a chuté d'environ 98% à partir du jour où le système de GreyListing a été mis en place.

En contrepartie, avant d'enteriner cette expérience qui semble faire ses preuves, il faut connaître les **inconvenients** d'un tel système.

Le procédé induit en effet un délai d'environ 10-15mn en moyenne dans la réception d'un mail provenant de sites distants (sauf si ces sites sont jugés de confiance et mis en liste blanche localement)...

Le [procédé de Liste Grise](#) se base sur le fait que les spammeurs font du "*Fire and Forget*"

C'est à dire qu'ils envoient des milliers de mails de Spam, et qu'ils arrêtent après coup leur serveur de mail ou leur PC d'émission... Leur visibilité n'est donc que temporaire sur Internet.

Partant de cette constatation, le procédé de liste grise est le suivant :

- Grace au greylisting, notre serveur de mail refuse tous les mails reçus, en provoquant une erreur temporaire qui demande au serveur distant de réémettre (ceci est la norme des serveurs SMTP qui est implémentée dans tous les serveurs de mail respectants la norme)
- 2 cas se présentent alors :
 - a/ soit le serveur distant réémet son message (représenté par le triplet (*machine cliente*, *@ emetteur*, *@destination*)), et notre serveur le laisse alors rentrer lors de la 2ème présentation
 - b/ soit le serveur distant émetteur ne réémet pas...le mail (le premier qui a été refusé) est donc perdu...puisqu'il n'a pas été réémit.

Comme indiqué plus haut, le seul désagrément pour vous utilisateurs est un certain délai dans la réception des mails. Lors de la réception ce délai vous est notifié dans les entêtes du message sous la forme :

- X-Greylst: delayed 1396 seconds by postgrey-1.21 at arago-bis; Thu, 05 Jan 2006 10:47:33 CET

En effet lors du refus temporaire, le serveur distant stocke le message refusé, et essaie de le réémettre à intervalles réguliers. Le plus souvent il y parvient dans les 15 minutes qui suivent en moyenne... (avec toutefois un écart type qui peut être important dans certains cas si le serveur distant ne réémet pas suffisamment rapidement)

Il faut noter que ce délai (quand toutefois il est perceptible) n'a lieu QUE la première fois où le message représenté par un *triplet (machine cliente, email expéditeur, email destinataire)* se présente à notre serveur de messagerie !

Dès la 2ème fois, ce même *triplet* rentre sans aucun refus ni délai dans notre serveur.

Systeme de Liste Blanche associé

Bien entendu pour des sites de confiance réputés a priori sans spam (cnrs.fr, upmc.fr ...etc) il est légitime de vouloir échapper au délai induit par la liste grise. Nous mettons ces sites de confiance en liste blanche. Dans ce cas là, il n'y a aucun refus, tous les mails rentrent immédiatement.

N'hésitez pas à nous [proposer des sites "de confiance"](#) pour compléter cette liste !

En conclusion

Vous voudrez bien nous faire savoir si vous trouvez une objection personnelle à laisser le système de Liste Grise en place sur le serveur de mail du Laboratoire ARAGO pour la réception de vos mails.

En cas d'objection (pas de liste grise pour vous), nous vous proposerons d'échapper à ce procédé immédiatement et sans problème. (vous n'aurez donc plus de délai de réception de mail, mais vous recevrez autant de spam qu'avant)