Analyser l'entête d'un mail

Création de règle de filtrage avec mfilter (pour Free)

Wullfk

15/03/2012

Apprenez à vérifier la provenance de vos mail et si vous êtes sur Free établissez des règles de filtrage appropriées avec mfilter

ANALYSE DE L'ENTÊTE (HEADER) D'UN MAIL

DÉFINITION DU HEADER :

Le header, (ou en-tête en français) c'est l'entête (CQFD) d'un fichier informatique ou d'un paquet transitant sur un réseau informatique, ce sont aussi les données contenues au début de ce fichier ou du paquet. En transmission de données, les données qui suivent le header sont souvent appelées charge utile ou body.

source Wikipédia.fr : http://fr.wikipedia.org/wiki/Header

LES ÉLÉMENTS DU HEADER :

Dans un **Mail** (*courrier électronique*), le texte (*corps ou body*) est précédé par des lignes de header indiquant :

- l'expéditeur.
- le destinataire.
- le sujet.
- les *timestamps* d'envoi et de réception.
- le serveur de messagerie électronique final.
- etc...

Pour ceux qui veulent en savoir encore plus et que l'anglais ne rebute pas, vous pouvez toujours consulter la RFC 2822 "*Format standard des messages sur Internet*" au tout début Internet s'appelait **ARPANET** NET pour contraction d'Internet, ce n'était pas "*la toile*" immense que l'on connait maintenant.

L'ANALYSE PAR L'EXEMPLE :

Prenons l'exemple type d'un mail nous paraissant suspect, avec en objet du message un titre très racoleur, le but étant de déstabilisé, faire peur, ou faire croire à un gain, au lecteur que vous êtes.

Dans le cas présent, on partira du principe que vous avez rapatrié ce courrier dans votre client mail (Outlook, Thunderbird, etc...) avant d'ouvrir le message allons faire un tour dans le fameux header.

Vous pouvez tout aussi bien voir le header en consultant directement vos message sur le **Webmail** de votre F.A.I (Fournisseur Accès Internet) , l'intérêt c'est que cela pourra vous permettre d'établir certaines règles de filtrage directement à la source de réception de vos courrier, soit dit en passant celons votre F.A.I la création de règle sera plus ou moins facile à paramétré finement, au risque de ne plus rien recevoir si vous commettez des erreurs, les futur éventuelle messages non reçus seront définitivement perdu, mais je vous rassure les règles ça ce corrige, ou se désactive.

Je reviendrai plus longuement sur l'établissement de règles pour le **Webmail Free** particulièrement (c'est mon F.A.I) via l'adresse : http://mfilter.free.fr/

COMMENT RÉCUPÉRER L'ENTÊTE D'UN MAIL DANS SON COURRIELLEUR?

Celons votre client de réception de courrier, la procédure peut légèrement différée. Je ne vais pas tous vous les énumérer, j'ai pris les deux plus connus et utilisé.

- **Outlook 2007**: un clic droit sur le mail, puis cliquez sur *Options des messages*, dans la fenêtre qui s'ouvrira, en bas vous avez le fameux header (l'entête Internet)
- **Thunderbird** : aller dans l'onglet **Affichage**, et sélectionner *Code source du message* y a pas plus simple.

On y trouve les renseignements suivant :

Received: from server.exemple.fr(190.13.06.15)
by smtp.votre-FAI.fr with ESMTP(SMTPD32-4.06)id A09D3203BC;
Mon, 15 Nov 2010 14:19:42 EST
Received: from vilainpirate ([192.288.14.1])
by server1.exemple.fr (8.7.5) ID LAA28548;
Mon, 15 Nov 2010 14:19:42 -0700 (MST)
Message-Id: <599b403f348fd8529caa342af911e6acl@vilainpirate>
Reply-To: hadopi@hadopi.fr
From: bisounours@chezlui.com
To: votre-adresse@votre-FAI.fr
Subject: Message important a votre attention ! - vous avez gagnez
Content-Type: multipart/alternative; boundary="=-nxs_alt_d46cdd99c660e6b04e677477717d6dff"
Date: Mon, 15 Nov 2010 13:19:38 +0100
MIME-Version: 1.0
Content-Type: text/plain;
charset="ISO-8859-2"
X-Priority:3
X-MSMail-Priority:Normal
X-Mailer: Microsoft Outlook Express 4.72.3110.5

Note : *toutes les références de l'exemple sont fictives, toute ressemblance avec des éléments existants ou qui pourraient exister ne serait que pure coïncidence.*

Nous allons détailler point par point la composition de cet en tête.

Received: from **server.exemple.fr(190.13.06.15)**
by smtp.votre-FAI.fr with ESMTP(SMTPD32-4.06)id A09D3203BC;
Mon, 15 Nov 2010 14:19:42 EST

Adresse IP du serveur par lequel à transité le message (avec la date et l'heure : *timestamp*)**.**

Received: from **vilainpirate ([192.288.14.1])**

Adresse IP du pirate.

by server1.exemple.fr (8.7.5) ID LAA28548;
Mon, 15 Nov 2010 14:19:42 -0700 (MST)

Serveur SMTP utilisé par le pirate (la aussi on retrouve le *timestamp* (voir plus bas pour l'explication))**.**

Message-Id: **<599b403f348fd8529caa342af911e6acl@vilainpirate>**

Nom réseau de l'ordinateur du pirate.

Reply-To: **hadopi@hadopi.fr**

Adresse où sera acheminée votre réponse éventuelle. (Vous aurez remarqué la petite pointe d'humour)

From: **bisounours@chezlui.com**

Adresse présumée du pirate (qui a sans doute été falsifiée).

To: **votre-adresse@votre-FAI.fr**

Votre adresse E-mail. (F.A.I= Fournisseur d'Accès Internet)

Subject: **Message important a votre attention !- vous avez gagnez**

Objet du mail (déjà avec ce genre de titre, moi je reste très suspicieux).

X-Mailer: **Microsoft Outlook Express 4.72.3110.5**

Client mail utilisé par le pirate.

Là on dispose de l'essentiel, mais si on veut pousser un peu plus loin, on peut encore obtenir d'autres renseignements.

Received: from server.exemple.fr(190.13.06.15)
by smtp.votre-FAI.fr with ESMTP(SMTPD32-4.06)id A09D3203BC;
Mon, 15 Nov 2010 14:19:42 EST
Received: from vilainpirate ([192.288.14.1])
by server1.exemple.fr (8.7.5) ID LAA28548;
Mon, 15 Nov 2010 14:19:42 -0700 (MST)

En gras, ce sont les "*timestamp*" (littéralement parlant "*timbre de temps*" c'est vrai que même en Français ce n'est pas plus parlant) on pourrait assimiler ça au tampon de la poste
en fait pour être bref, c'est tout ce qui indique les éléments temporel sur les serveurs.

- le jour.
- la date.
- le mois.
- l'année.
- l'heure.
- le décalage horaire.
- le fuseau horaire.

MIME-Version: 1.0

Sous cette abréviation ce cache le nom suivant : **Multipurpose Internet Mail Extension**, la définition sur Wikipedia nous dit ceci :

"C'est un standard internet qui étend le format de données des courriels pour supporter des textes en différents codage de caractères autres que l'ASCII, des contenus non textuels, des contenus multiples, et des informations d'en-tête en d'autres codages que l'ASCII. Les courriels étant généralement envoyés via le protocole SMTP au format MIME, ces courriels sont souvent appelés courriels SMTP/MIME."

Pour faire simple, dans notre cas **cela indique que le contenu du message est formaté en MIME. Sa valeur est typiquement "1.0"**

charset="ISO-8859-2"

Renvois le type de codage des caractères utilisés. On ne va pas rentrer dans les détails, ça deviendrais trop technique.

Dans le cadre de ce tutoriel, les derniers éléments n'ont pas grande importance, tout au plus cela vous permet de savoir quand le message à transitée sur les différents serveurs, s'il y a un décalage horaire, auquel cas on peut connaitre le fuseau horaire, et enfin le type de codage de caractère qui à été utilisé.

Cet exemple est évidemment très basique en soit, et ce serait vraiment trop réducteur de résumé en disant que tous les headers sont tous aussi simple. Le principale y est, mais il y a bien plus sournois.

- le mail peut avoir transité par un ou des proxy,
- il peut y avoir une multitude de destinataire leur boite mail servant de relais.
- il peut ne pas y avoir d'objet d'indiqué (au quel cas il faut être encore plus méfiant).
- Il peut y avoir des liens cliquables, qui vous renvoie sur une page d'un site détourné (phishing)
- il peut y avoir des pièces jointes avec des fichiers .exe, .pdf, .jpeg, etc... (dans ce cas, avoir la certitude (signature numérique et/ou cryptage) de la provenance, sinon n'ouvrez pas !)

Ci-dessous un autre exemple d'un header un peu plus compliqué (surtout pour le filtrage direct sur le Webmail de son F.A.I)

+OK 10060 octets

Return-Path: <info@news.gcdo8.com>

Delivered-To: free.fr-monadresse@free.fr

Received: (qmail 9443 invoked from network); 9 Mar 2012 09:32:21 -0000

Received: from mx21-g26.free.fr (HELO tb8.ma86.fr) (212.27.42.83)

by mrelay3-g25.free.fr with SMTP; 9 Mar 2012 09:32:21 -0000

Received: from tb8.ma86.fr ([82.96.167.8])

by mx1-g20.free.fr (MXproxy) for monadresse@free.fr;

Fri, 9 Mar 2012 10:32:21 +0100 (CET)

X-ProXaD-SC: state=HAM score=90

DKIM-Signature: v=1; a=rsa-sha1; s=dkp; d=news.gcdo8.com; l=8536;

t=1331285540; c=relaxed/relaxed;

h=from:to:subject:mime-version:date:message-id:content-type;

bh=ML2Rm5xhJ9EMZ/qvlccawrPocKI=;

b=ERICytPD+6axKTrIsmpBxN2I2h/9XbX/pdGdh07bfYLKybB2xvkkICXcDu9jRyMT

List-Unsubscribe: <http://news.gcdo8.com/desabo.php?mid=7420409524&sid=19088690&hash=9d4d2>

X-IdentID: 7420409524.17101

X-MXBID: 7420409524.0.19088690.0

Precedence: Bulk

X-rpcampaign: PredMJN_17101

From: "Lionel" <info@news.gcdo8.com>

Reply-To: "Lionel" <info@news.gcdo8.com>

Subject: =?ISO-8859-1?B?Vm91cyBhdmV6IHVuIG5vdXZlYXUgbWVzc2FnZQ==?=

To: <monadresse@free.fr>

Return-Path: <info@news.gcdo8.com>

Date: Fri, 09 Mar 2012 10:32:20 +0100

Content-Type: multipart/alternative; boundary="=-nxs_alt_0317d36d8cdd44fc4d7ce8aa9a1bc266"

Message-Id: <e9cef7a8ead7351bba216516db633480.MXSendMail@localhost>

MIME-Version: 1.0

X-Mailer: MXSendMail 1.0

Received: from tb8.ma86.fr (tb8.ma86.fr [127.0.0.1]) by tb8.ma86.fr (Postfix) with ESMTP id 8ecc7599bb85a3a3fbad93801c4fb5d6 for <<monadresse.fr>>; Fri, 09 Mar 2012 10:31:22 +0100

X-EsetId: 02F190220D29F20F59B3CF

--=-nxs_alt_0317d36d8cdd44fc4d7ce8aa9a1bc266

Content-Type: text/plain; charset="UTF-8"

Content-Transfer-Encoding: 7bit

Vous avez un nouveau message (http://news.gcdo8.com/trap/sid19088690/hash9d4d2/mid7420409524)

Chaque jour tentez de gagner des cadeaux.

consultez la version en ligne du message, rendez vous sur cette page (http://news.gcdo8.com/miroir/email.php?eid=17101&ehash=565f3&mid=7420409524&sid=19088690&hash=9d4d2)

Merci d'ajouter info@news.gcdo8.com à votre carnet d'adresses.

Avec notre partenaire ScratchMania, nous vous proposons de découvrir l'histoire de Lionel R. :

Lionel R. a gagné 40 000 euros en un jour sur ScratchMania (http://news.gcdo8.com/static/adredirect.php?cid=20094&sid=19088690&hash=9d4d2&zo=1&mid=7420409524&url=aHR0cDovL2ZyLnNjcmF0Y2htYW5pYS5jb20vP2JyYW5kSWQ9MSZjYW1wYWlnbklkPTc5MiZtZWRpYUlkPTExNjkmYWZmaWxpYXRlUHJvZmlsZU5hbWU9) :

Lionel R. :"Je suis Ebéniste sur Strasbourg. J'ai joué à ScratchMania pour la première fois car ils m'avaient offert 7 euros (http://news.gcdo8.com/static/adredirect.php?cid=20094&sid=19088690&hash=9d4d2&zo=1&mid=7420409524&url=aHR0cDovL2ZyLnNjcmF0Y2htYW5pYS5jb20vP2JyYW5kSWQ9MSZjYW1wYWlnbklkPTc5MiZtZWRpYUlkPTExNjkmYWZmaWxpYXRlUHJvZmlsZU5hbWU9) ... j'ai tout de suite cru à une arnaque comme j'en reçois tous les jours.

Mais après 25 minutes de jeu, je me suis retouvé avec plus de 750 euros que j'ai tout de suite retiré.

Le soir même, ma femme a essayé, elle aussi, et une des cartes qu'elle a gratté lui a fait gagner 40 000 euros !

Là on dispose d'autres infos non présente dans le premier exemple, comme la taille du message (10060 octets).

On peut facilement deviner à l'avance qu'il s'agit d'un spam pour inciter à aller jouer sur une plateforme de jeux en ligne, après reste à savoir si le lien de redirection se fera bien sur le site de jeux, si tenté que ce dernier existe réellement (on ne va pas tenter le diable)

Un conseil, dans ce cas typique, il ne faut surtout pas répondre à ce genre de courrier, car vous indiquerez au spammeur (voir à un éventuelle pirate) que votre adresse mail est bien valide et aussi votre IP, et vous serez inondé plus encore par la suite par le même genre de sollicitation, voir d'autres à caractère pornographique, ou de rencontre. Et dans l'éventualité d'un hacker de lancer un scan de votre IP pour trouver les ports ouverts et les éventuelles failles de sécurité (antivirus, Windows pas à jour, version de Java, Flash Player obsolètes

Vous constaterez aussi dans la lecture du corps du message, la multitude de fautes d'orthographe ou de grammaire, qui permet déjà d'avoir un doute sur l'authenticité réelle du courrier

À QUOI PEUVENT SERVIR LES PRINCIPAUX ÉLÉMENTS FOURNIS PAR LE HEADER ?

On garde notre premier exemple type.

Le fait de connaitre l'adresse IP du serveur par lequel à transité le message permet de voir le chemin qu'il a emprunté, et mieux encore de connaitre l'adresse IP du fameux pirate.
Avec ces éléments, il n'y a plus qu'à envoyer votre plainte à abuse@exemple.fr et/ou à postmaster@exemple.fr (bien évidement vous remplacerez *exemple.fr* par le nom de domaine du F. A. I ou du serveur SMTP utilisé par le pirate)

abuse et **postmaster** étant valides avec n'importe quel F.A.I
la lecture de l'entête nous permet aussi de voir vers quel adresse sera envoyer notre éventuel réponse.

COMMENT ÉVITER DE RAPATRIÉ CERTAINS MAILS ?

Le principe c'est le filtrage en amont, donc directement sur le serveur mail de votre F.A.I

2 solutions :

1. Vous prenez le temps d'aller sur l'espace mail de votre F.A.I pour faire le tri, de vous à moi c'est assez fastidieux car cela vous contrains de passer par votre navigateur, aller sur le site votre F. A. I, puis dans votre espace client dans lequel vous devrez entrer votre identifiant et le mot de passe du compte, pour enfin accéder à votre boite mail. Franchement y a plus simple.

2. Vous utilisez par un petit logiciel, qui se chargera après configuration de lire vos courriers situés directement sur le serveur de votre F.A.I et dans le cas où vous ne souhaiteriez pas rapatrié certains mails, de les supprimer purement et simplement, sans avoir à ouvrir votre navigateur.

Si dessous 3 logiciels qui accomplissent parfaitement cette tâche :

- **PopTray** : l'ancêtre dans le bon sens du terme
- **POP Peeper** **3.8.1.0 Fr Free**: le petit frère de PopTray (c'est celui que j'utilise actuellement) La dernière version est **POP Peeper Pro 4.0.1** mais uniquement disponible en shareware
- **Magic Mail Monitor** : un nouveau (enfin pour moi, car pas encore testé), ne nécessite pas d'installation.

Le principe reste le même pour les 3, ce qui peut faire la différence ce sont les options fournis, la facilité de prise en main, d'utilisation au quotidien, et enfin la présentation via l'interface graphique, qui reste plus subjective, les gouts et les couleurs étant propre à chacun.

Voilà, je pense qu'avec cette base vous serez plus attentif dans la réception et la lecture de vos mails.

Si cette première étape vous a intéressé et que vous souhaitez poursuivre la lecture, la suite concerne la création de filtre pour le Webmail Free : http://mfilter.free.fr/

RÈGLES MFILTER POUR FREE.FR

C'EST QUOI MFILTER?

Mfilter est le filtre de courrier proposé par Free, à ne pas confondre avec les filtres créé dans le Webmail car à la différence de ce dernier mfilter est indépendant et propre à chaque boite mail (il faut s'y connecter) il agit dès que les messages arrivent, même si vous n'êtes pas en ligne, contrairement aux filtres du Webmail qui eux n'agissent que lorsque vous consulter vos message sur le Webmail (en direct, sans rapatriement sur un Courrielleur)

CONNEXION À MFILTER.

Rendez-vous sur l'adresse http://mfilter.free.fr/

Saisir l'adresse et le mot de passe du compte mail (*figure 1*) dont vous souhaitez ajouter ou modifier les filtres de courrier

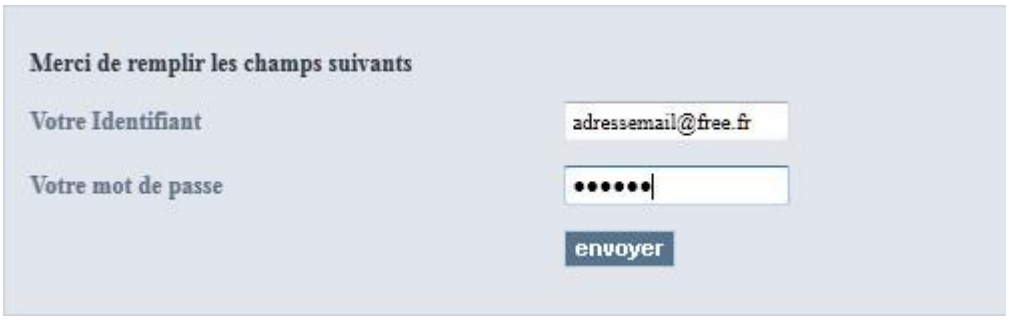

Figure 1 - connexion mfilter

Figure 2 - la page des filtres

Une fois l'identifiant et le mot de passe validé, vous obtiendrez la fenêtre ci dessus (*figure 2*) elle est vide si vous avez définis aucun filtre.

Bien qu'il ne soit pas parfait, mfilter reste assez efficace, si vos règles sont correctement définies.

Vous ne pourrez tout de même pas réaliser certains filtrages :

- Sur la taille de pièce jointe.
- Sur le contenu du message ou de pièce jointe.

Sachez qu'il faut toujours mettre en premier les règles dites "passantes" (acceptation) par rapport aux règles dites "bloquantes" (destruction, spam)

La zone de flèches à droite vous permet de positionner vos filtres (ex : +1 remonte le filtre selectionné d'une place, -1 le descend)

Quatre boutons sont disponibles.

1. **Supprimer** ➔ supprime le filtre sélectionné.
2. **Dupliquer** ➔ créer une copie du filtre sélectionné. (évite de ressaisir tous les paramètres)
3. **Ajouter** ➔ ajoute un filtre.
4. **Afficher** ➔ édite le filtre sélectionné pour le modifier.

FILTRE STANDARD.

Free propose par défaut 4 filtres de bases que l'on active en cochant des cases via cette adresse : http://mfilter.free.fr/antispam/ après s'être authentifier avec l'adresse mail concerné et son mot de passe.

1. Les mails indésirables (SPAM).

2. Les mails contenant des fichiers attachés exécutables.
3. Les mails ou je suis en copie cachée.
4. Les bounces qui ne sortent pas des serveurs de Free.

Une fois les cases cochés en regard des filtres standard que l'on souhaite, ceux si sont automatiquement crée dans mfilter

Ils apparaitront avec leur nom précédé de **[preset]** (présélection) qui disparaitra dès que le filtre sera édité

L'accès à http://mfilter.free.fr/antispam/ est quelque peu laborieux, après une attente relativement longue, une fois que l'on a coché les filtres qui nous intéressent, il n'est pas rare (voir même systématiquement) d'obtenir en retour ce message d'erreur.

Le serveur rencontre une difficulté à écrire votre règle (surcharge ?).
Veuillez recommencer dans quelques instants. Merci !

Note : le filtre pour le SPAM ce nomme **Scoring** (*figure 3*) car c'est sur paramètres (Score) qu'il agit, par défaut celui-ci est à 100 (valeur standard établi en mai 2005), mais vous pouvez le modifier

LE SCORE

Le Score c'est l'examen automatique de chaque message reçu par le serveur Free. Après analyse, un score est attribué à chaque message présent. Lorsque le score est supérieur à 100 (standard), le message est suspecté d'être un spam.

Pour visualiser la valeur des scores, il suffit d'accéder au Webmail du compte spécifier (http:/imp.free.fr/)

Lorsque vous êtes sur votre compte mail, cliquer sur Espace disque, et sur la nouvelle page qui s'affiche, cliquer sur la loupe à gauche du nom du répertoire.

Une fois le répertoire ouvert, celui liste les 100 premiers mails, avec leur score.

En rouge vous distinguerez les critères de scoring (décalage horaire, URL d'origine,….et le score).

Cette observation vous permettra de corriger le seuil de filtrage (laisser à 100 en cas de doute)

LES BOUNCES

Pour ce qui est du filtre sur les *bounces* voilà ce que dit l'aide de Free :

> **Pas de bounces "externes"**
>
> *Les spams sont dans leur quasi-totalité envoyés en usurpant l'identité de l'émetteur. Certains serveurs envoient malheureusement des notifications de non délivrance (les bounces) aux émetteurs usurpés. Ceci peut occasionner une pollution non négligeable de votre boite mail. cachée ou Blind Carbon Copy).*
>
> *Si ce problème vous arrive, cette option permet de supprimer bon nombre de ces bounces*

s'ils ne sont pas issus des serveurs de mails de Free.

Néanmoins, si vous utilisez un serveur SMTP autre que celui fourni par Free, il est déconseillé d'activer cette option (puisque les bounces ne seront pas issus de nos serveurs) ou si vous attendez des réponses à des bounces (le filtre se basant sur le contenu du champ subject, il ne fera pas de différence entre un bounce ou une réponse à un bounce).

Si néanmoins vous souhaitez activer cette option, vous pourrez préciser des exceptions à cette règle en utilisant l'interface http://mfilter.free.fr .

Avant de poursuivre je vous recommande de créer des dossiers spécifiques (spam, rejet, PJ, etc…) sur votre Webmail dans lesquels les mails dont les règles filtrage s'appliqueraient soient classé dans les répertoires spécifiques, plutôt que de les supprimer directement auquel cas vous ne pourriez rien récupérer (même dans votre corbeille "*Trash*"), vos mail serait définitivement perdu.

CONSTITUTION DES FILTRES STANDARDS.

FILTRE ANTI SPAM

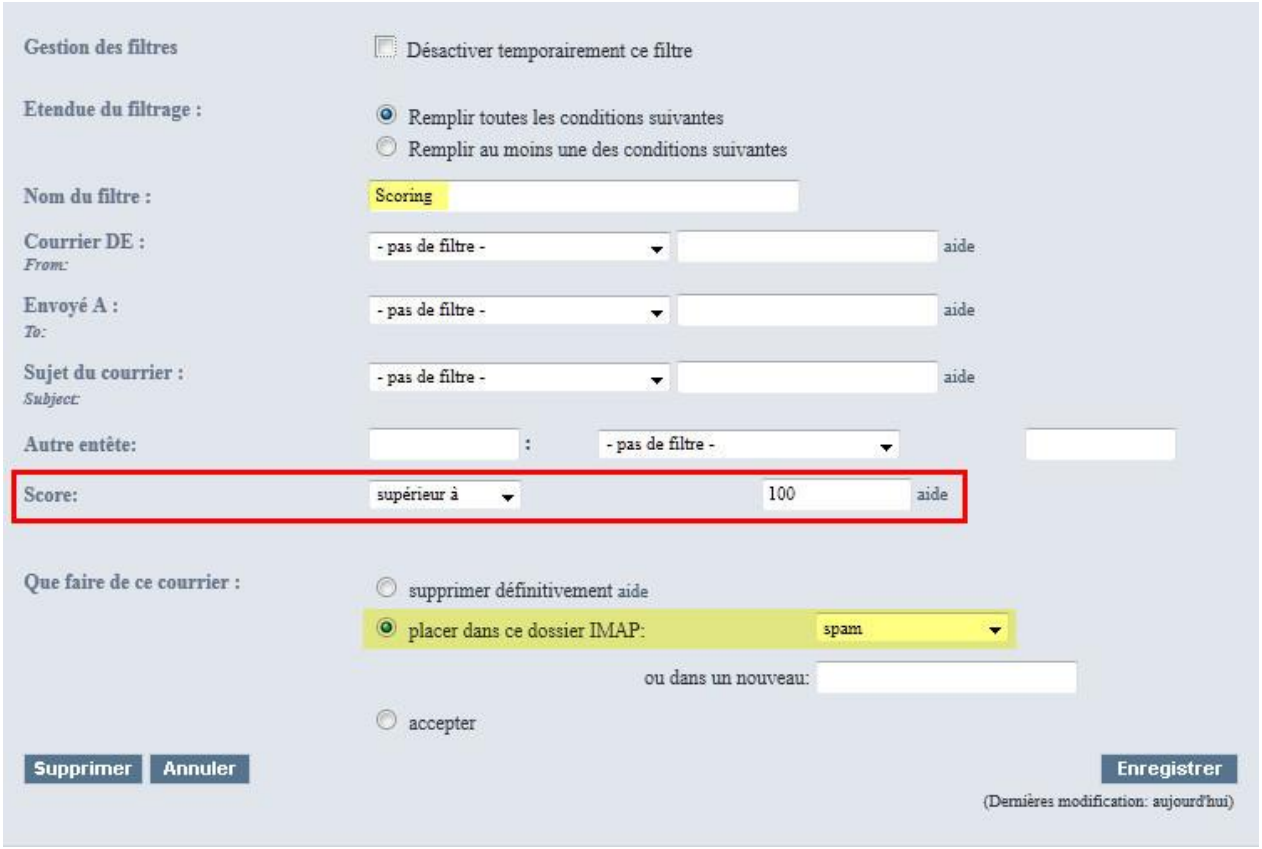

Figure 3 - filtre ANTI SPAM

Comme je l'ai expliqué un peu plus haut le filtre anti SPAM ce nomme **Scoring** (*figure 3*) et seul le champ *Score* est utilisé (100 par défaut), libre à vous de le modifier, mais faites tout de même des tests pour éviter que le moindre mail ne soit qualifier de SPAM sans que cela en soit

Cocher "**placer dans ce dossier IMAP**" et sélectionner un dossier que vous aurez préalablement créé (ex: "*spam*") pour ranger les courriers correspondant au filtre

FILTRE SUR LES FICHIERS ATTACHÉS EXÉCUTABLE.

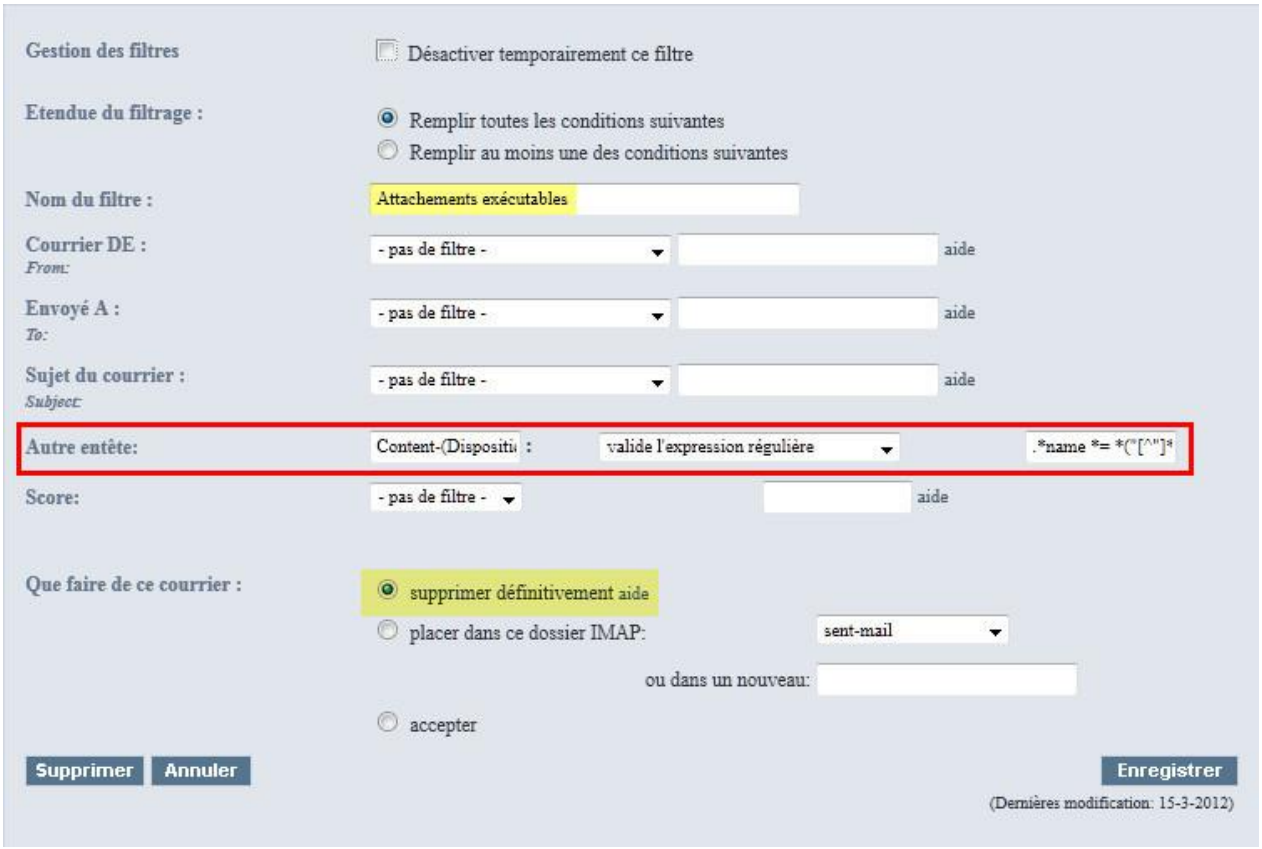

Figure 4 - filtre attachement exécutables

Dans **AUTRE ENTÊTE ➔ Content-(Disposition|Type) ➔ valide l'expression régulière ➔** .*name *= *("[^"]*\.(exe|vbs|pif|scr|bat|cmd|com|cpl)"|[^";]*\.(exe|vbs|pif|scr|bat|cmd|com|cpl)) *($|;)

En fonction de votre choix, laisser sur "**supprimer définitivement**" (*figure 4*) ou Cocher "**placer dans ce dossier IMAP**" et sélectionner un dossier que vous aurez préalablement créé: exemple ici vous pourriez avoir un dossier nommé "*PJ*" (pour Pièce jointe)

On recherche dans les entêtes **Content-Dispsotion** ou **Content-Type** le mot **name** (ou filename) puis un nom entre guillemets portant une extension défini dans la règle

FILTRE SUR PAS DE COPIE CACHÉE

Figure 5 - filtre pas de copie cachée

Dans **AUTRE ENTÊTE ➔ (To|Cc) ➔ valide l'expression régulière ➔** .*identifiant(\+[^@]*)?@(free|online)\.fr

En fonction de votre choix, laisser sur "**supprimer définitivement**" (*figure 5*) ou Cocher "**placer dans ce dossier IMAP**" et sélectionner votre dossier créé pour ce type de mail: ex "*Copie Cachee"* (éviter les accents)

On recherche si l'**identifiant** est absent des entêtes **To** et **Cc**

FILTRE SUR PAS DE BOUNCES

Figure 6 - Filtre pas de bounces

Dans **SUJET ➔ valide l'expression régulière ➔** .*(Undeliver(ed|able) Mail|Mail delivery failed|failure notice|Delivery Status Notification|Returned mail

Dans **AUTRE ENTÊTE ➔ RECEIVED ➔ ne valide l'expression régulière ➔** from 212[.]27[.](42|60)[.][0-9]+.*by [a-zA-Z0-9-]+[.]free[.]fr

En fonction de votre choix, laisser sur "**supprimer définitivement**" (*figure 6*) ou Cocher "**placer dans ce dossier IMAP**" et sélectionner votre dossier créé pour ce type de mail : ex: "*Rejet*"

On recherche une redirection du courrier non délivré qui n'est pas passé par le serveur Free (je ne suis pas sûre de mon explication sur ce point, ce reporter plus haut sur la définition de Free sur les bounces)

Celons les résultats que vous obtiendrez lors de vos test vous pourrez si vous le souhaitez le désactiver (*figure 6*)

Voilà on a fait le tour des paramètres des filtres standard, que vous pouvez si vous le souhaitez modifier à votre convenance, mais là encore des tests s'imposent, pour vérifier le bon fonctionnement du/des filtres

Prenez bien conscience que les dossiers IMAP créer sont là pour vous permettre de tester vos filtre, une fois ceux-ci correctement paramétré et opérationnel, libre à vous de supprimer certains dossiers devenus inutile, en prenant soin de modifier vos règles en conséquences.

Vous avez toujours la possibilité de suspendre ou de supprimer une règle de filtrage qui ne vous convient pas

L'inconvénient pendant la période de test que vous définirez (une ou deux semaines), c'est qu'il vous faudra vérifier assez régulièrement vos courriers directement sur votre Webmail afin de vérifier vos dossiers et si nécessaire faire un nettoyage, afin de ne pas saturer l'espace disque alloué à votre adresse mail (25Mo)