Reportspam un plugin Thunderbird pour escalader les anomalies de filtrage antispam

Serge Aumont
RENATER

Etienne Méléard
RENATER

Hervé Lascaux
IUT de Vannes

Résumé

L'évaluation et la mise au point d'un service de filtrage rendent indispensable la collecte des erreurs de filtrages : les faux positifs et les faux négatifs[1]. Comment organiser cette collecte à l'échelle d'un établissement ou d'un prestataire comme RENATER alors que dans bien des cas seuls les utilisateurs sont à même de constater ces erreurs de diagnostic ? La solution passe par une interface permettant de signaler les spams non détectés au moindre effort. C'est ce que propose l'extension pour Thunderbird **reportspam**.

Mots clefs

SPAM, XUL, Thunderbird, faux positif, faux négatif, Phishing

1 Contexte

l y a fort longtemps que le filtrage antispam n'est plus confié aux seuls fonctions du MUA de chaque utilisateur. Le besoin de protéger les utilisateurs des spams a conduit à l'installation de serveurs de filtrage. Que ces serveurs soient installés par l'organisation titulaire du domaine de messagerie (logiciels libres ou appliances*)* ou opérés par le FAI comme dans le cas de l'offre de service de RENATER, ces fonctions de filtrages sont coûteuses et par nature imparfaites. Il convient donc d'organiser une boucle de retour des erreurs de filtrage (faux positifs et faux négatifs) constatées par les utilisateurs pour les besoins de mise au point des serveurs de filtrage.

Cette boucle est indispensable pour améliorer les dispositifs de filtrage en particulier parce que bon nombre de spammeurs s'acharnent à contourner les protections mises en œuvre, mais aussi pour évaluer le plus objectivement possible la qualité d'un service antispam. En effet, les indicateurs primordiaux pour une telle évaluation devraient être basés sur le décompte des faux négatifs et des faux positifs. La disponibilité de ces chiffres suppose une collaboration active des utilisateurs.

Lorsque le filtrage est assuré localement par le MUA, le traitement des erreurs du filtre antispam peut lui aussi être fait localement. C'est ce que permet le bouton « indésirable » de Thunderbird. Hélas, ce bouton ne permet pas d'alimenter les mécanismes d'amélioration continue du filtrage mutualisé. Celui-ci est généralement organisé via une boucle de collecte des erreurs utilisée en particulier pour compléter ou corriger les blacklist et whitelist intervenant dans le filtrage protocolaire ainsi que pour alimenter les échantillons sur lesquels sont construits les filtres de contenus.

Certes, des pots de miel peuvent collecter automatiquement du spam, mais cette méthode de collecte est elle même imparfaite ; en effet, les messages reçus par des adresses de piège ne sont que partiellement représentatifs des spams qui abondent dans nos boites aux lettres ; en outre cette méthode ne collecte que des faux négatifs. Elle ne saurait remplacer complètement un contrôle humain des scories du filtrage. Parallèlement, les moyens initialement mis en œuvre par RENATER dans ce domaine étaient

[1]Faux positif / faux négatif : un test à deux valeurs possibles produit un « faux positif » lorsqu'il rend « vrai » par erreur. Dans le contexte de la lutte contre le spam, les « faux négatifs » sont des spams non détectés par un filtre, les faux positifs sont eux des messages détectés à tord comme étant du spam.

constitués de deux boites aux lettres par domaine raccordé, l'une dédiée aux faux positifs, l'autre aux faux négatifs. Le postmaster a la possibilité d'alimenter ces boites aux lettres, mais aucun outil n'est fourni aux autres utilisateurs.

Pourtant, l'expérience montre que les utilisateurs se sentent très concernés par les imperfections du système antispam. Ils sont généralement volontaires pour signaler celles-ci lors de la mise en place d'une nouvelle solution antispam dont chacun espère enfin qu'elle nous libère de cette pollution. Toutefois, du fait d'un mode opératoire peu pratique voir même de l'absence de toute instruction dans ce domaine, leur collaboration ne dure pas.

2 L'extension Thunderbird reportspam

Reportspam est une extension pour Thunderbird qui tente de répondre à ce problème.

Après installation, un nouveau bouton de la barre d'outils « entête » permet d'expédier les messages incorrectement traités par le service antispam vers une adresse configurée. Le bouton s'adapte automatiquement au contexte pour signaler un faux négatif ou un faux positif selon qu'une entête de marquage de spam soit ou non présente. Si le message a déjà fait l'objet d'un signalement, le bouton est désactivé. L'opération est aussi accessible sur une sélection de plusieurs messages par le "clic droit". Enfin, une action complémentaire peut être associée au bouton de signalement de faux négatifs : déplacer le message dans un dossier ou le supprimer. Un seul clic permet alors de signaler un spam non détecté et de le mettre dans la corbeille.

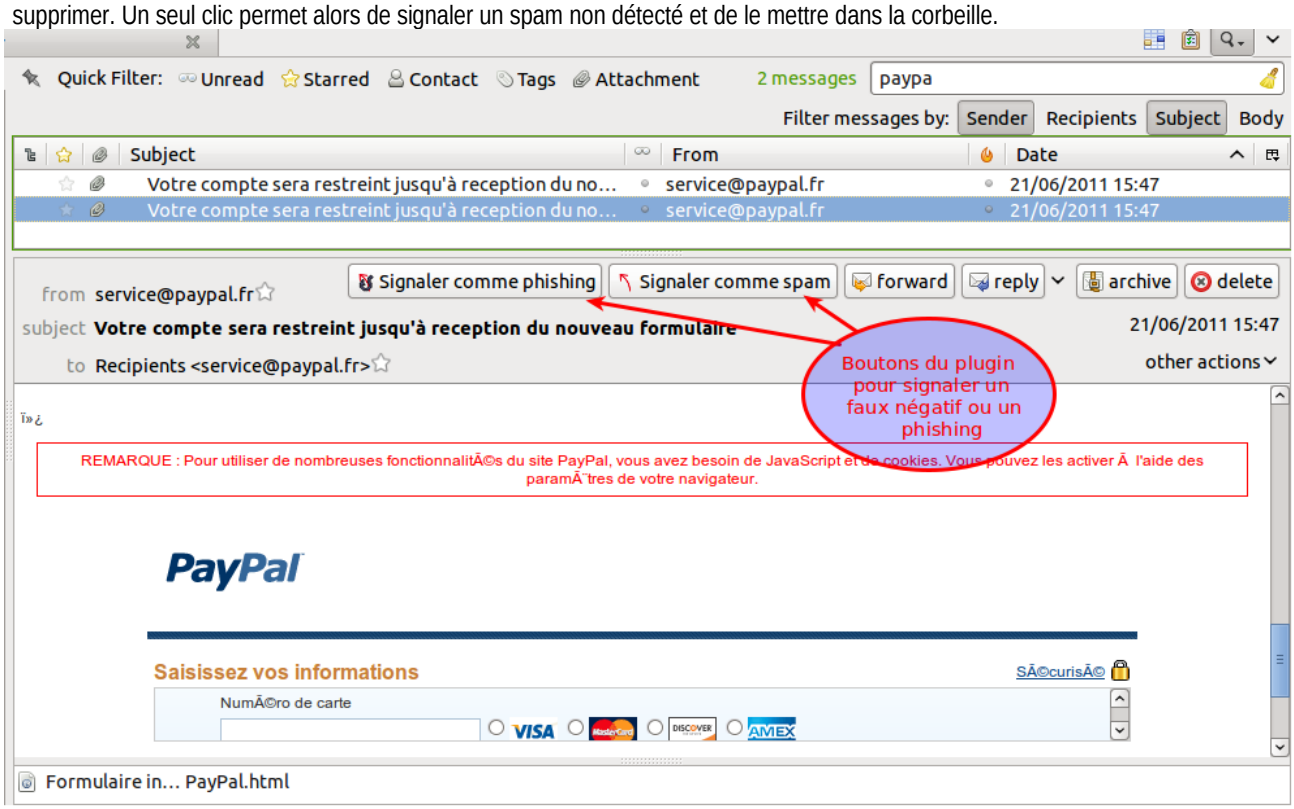

Figure 1 - *reportspam*

Le signalement est assuré soit par l'envoi smtp du message dans un attachement mime, soit par la soumission du message à un serveur web. Les préférences de reportspam permettent :

- de choisir une adresse (mailto ou http) de soumission respectivement pour les faux positifs et pour les faux négatifs
- de spécifier l'entête permettant de reconnaître qu'un message a été marqué ou pas comme un spam grâce à laquelle le plugin adapte le bouton de signalement au contexte faux positif ou faux négatif.

Les utilisateurs avancés peuvent, en outre, activer le signalement de phishing. Le principe est identique au signalement des spams, mais l'adresse de signalement est spécifique. Il est ainsi possible d'organiser au sein d'un établissement la détection précoce d'une campagne de phishing pour mettre en œuvre des contre mesures (bloquer localement ces messages, voir même supprimer des boites lettres les messages de phishing déjà remis avant que ceux-ci ne soit lus ou encore interdire les adresses email et sites web d'hameçonnage.

Il convient de régler ses préférences en fonction des indications de l'opérateur du service de filtrage. Dans le soucis de simplifier au maximum le déploiement de ce plugin, il est distribué avec des valeurs par défauts adaptées aux utilisateurs d'un domaine raccordé à RENATER.

Si un établissement ou un autre prestataire antispam souhaite déployer ce plugin, il peut éditer en ligne[2] la configuration par défaut de l'extension et générer le fichier xul. Il peut alors le mettre à disposition des utilisateurs de son environnement un plugin utilisable sans aucune instruction particulière.

Ce plugin donnera des résultats s'il est utilisé par un nombre assez important de personnes. Nous espérons qu'il sera déployé et décliné pour d'autres MUA tel que Zimbra ou Outlook. Il peut par exemple aider à comparer différents moteurs de filtrage en compétition pour un service. Il faut toutefois rester prudent dans l'interprétation des données collectées qui peuvent dépendre fortement des populations à qui il est donné.

---

[2]Éditeur des préférences par défaut de reportspam http://www.cru.fr/activites/spam/index#comment_changer_la_configuration