

Sommaire

SpamAssassin, Mon ami, ce Tueur.....	1
Au début il y a eu le délit.....	2
La préparation du tueur (et de ses acolytes).....	3
Installation de SpamAssassin.....	3
Configuration.....	3
Ces tueurs occasionnels: les utilisateurs.....	4
Installation de Vipul Razor.....	5
Le Nettoyeur ProcMail (l'accompagnateur du criminel).....	6
Le tueur en action.....	7
Intégrer SpamAssassin dans «Kmail».....	7
Intégrer SpamAssassin dans «Evolution».....	7
L'expérience rend maître.....	9
les faux négatifs.....	9
les faux positifs.....	9
Le crime était presque parfait.....	10
Quelques Liens.....	11
Conclusion.....	12
Bayes.....	12
Le GreyListing ou une mauvaise farce aux Spammeurs :.....	12
Copyright.....	13

SpamAssassin, Mon ami, ce Tueur

SpamAssassin, Mon ami, ce Tueur

Par Albert

SpamAssassin est un logiciel merveilleux disponible sur de nombreuses stations. C'est un tueur de Spam comme il se définit lui-même. Mais qu'est-ce que le Spam?

Le mot est d'origine américaine, il désigne le nom d'un aliment recomposé que mangeaient les soldats et le peuple américain pendant la seconde guerre mondiale. Il était réputé pour être in mangeable, mais pour avoir une longue durée de conservation (du moins pour l'époque) un pâté épicé à base de porc et de viandes, le SPAM (Spiced Pork And Meat). Mais cela n'explique pas tout, les Monty Python, célèbres humoristes anglais, y sont aussi pour quelque chose... C'est grâce ou à cause de l'un de leurs sketches de leur non moins incroyable rendez-vous hebdomadaire diffusé sur la BBC entre 1969 et 1973, le Monty Python Flying Circus (voir lien en fin d'article) que ce nom est utilisé pour désigner le courrier non sollicité...

Au début il y a eu le délit

Le Spam est un fléau, malheureusement trop simple à mettre en œuvre pour que celui-ci s'arrête un jour, même si l'Europe et notre gouvernement (à travers la Loi sur l'Économie numérique) veulent essayer d'en enrayer le développement actuel...

La préparation du tueur (et de ses acolytes)

Installation de SpamAssassin

Vous le trouverez à cette adresse : <http://SpamAssassin.org/>

L'installation de SpamAssassin ne devrait pas vous causer de grands problèmes sous Mandrake, Debian ou Fedora. Exécutez simplement en tant que «root» ou à partir du interface graphique un «urpmi SpamAssassin» dans le cas du premier et un «apt-get install spamassassin» dans le cas du deuxième et troisième. SpamAssassin est une application GPL écrite en Perl.

Configuration

(fichier de configuration valable à partir de la version 2.5, version actuelle : 2.63)

Éditez le fichier «local.cf» (généralement placé dans le répertoire /etc/mail/SpamAssassin/ ou /etc/SpamAssassin)

```
# Combien de fois le message devra-t'il être marqué pour être reconnu comme du spam
required_hits 5.0
```

```
# Doit-on changer le sujet du message considéré comme spam (0=non / 1=oui)
rewrite_subject 1
```

```
# Texte à rajouter devant l'intitulé du message si le «rewrite_sujet» est activé
subject_tag *****SPAM*****
```

```
# Encapsuler le spam dans le message comme une pièce attachée (0=non / 1=oui)
report_safe 1
```

```
# Use terse version of the spam report
use_terse_report 0
```

```
# Utilisation du protocole de Bayes
use_bayes 1
```

```
# Activation de l'auto-apprentissage Bayésien
auto_learn 1
```

```
# Autoriser les préférences des utilisateurs (0=non / 1=oui) : peut être considéré comme un
# trou de sécurité par certains administrateurs...
allow_user_rules 0
```

```
# Activer ou pas les agents de contrôles extérieurs (0=non / 1=oui)
skip_rbl_checks 0
use_razor2 1
use_dcc 0
use_pyzor 0
```

```
# Les mails dont le code pays se termine par le suffixe suivant ne sont pas considérés par défaut comme du
```

```
spam
ok_languages fr
```

```
# Chaque système d'exploitation utilise un type de «locales» (encodage de caractères qui lui est propre)
# selon la région dans laquelle il se situe (c'est en fait l'utilisateur qui définit ses locales lors de l'installation)
ok_locales fr en es it be
```

```
auto_whitelist_path /var/spool/SpamAssassin/auto-whitelist
auto_whitelist_file_mode 0666
```

Michael Moncur développeur de SpamAssassin a créé un générateur de fichier «local.cf», vous le trouverez à cette adresse : <http://www.yrex.com/spam/spamconfig.php>

Ces tueurs occasionnels: les utilisateurs

Les préférences que nous avons définies s'appliquent au niveau du système tout entier, et si personne demande à l'administrateur de le modifier, elles s'appliqueront aussi à tous les utilisateurs.

Il existe donc pour ceux-ci, un petit fichier qui une fois modifié, leur permettra de passer outre la configuration de l'administrateur, ou du moins sur quelques points fondamentaux...

À la racine de votre répertoire, veuillez pointer vers le sous-répertoire «.spamassassin» et éditer le fichier «users_prefs»

Par défaut quel score doit atteindre un courrier dans les tests effectués par SpamAssassin pour être considéré comme non désiré ?

```
required_hits 5
```

Les listes blanches et noires, comme leur nom l'indique, permettent à l'utilisateur de définir par défaut quelles peuvent être les adresses qui doivent et ne doivent pas passer.

```
whitelist_from contact@lea-linux.org, @linuxfrench.net, *.asill.org
blacklist_from *.microsoft.com
```

Il existe bien entendu une commande inverse pour ces deux-là: unwhitelist_from et unblacklist_from

Par défaut SpamAssassin définit certaines règles au niveau des messages qui peuvent être considérés comme Spam, il donne un score à chacun, si le message atteint celui-ci lors de l'analyse, il est alors considéré comme indésirable... Mais l'utilisateur a la possibilité d'en changer la valeur. Vous trouverez plus d'informations sur les tests effectués par SpamAssassin à cette adresse : <http://SpamAssassin.org/tests.html>

Les tests se présentent de cette manière, à vous d'en adapter les valeurs selon vos nécessités :

```
# score SYMBOLIC_TEST_NAME n.nn
```

Par exemple :

```
score HTML_COMMENT_8BITS      0
score UPPERCASE_25_50         0
score UPPERCASE_50_75         0
score UPPERCASE_75_100        0
```

Vous pouvez aussi en profiter pour jeter un coup d'œil sur le fichier «bayes_journal». Il contient la totalité des mots utilisés par le système Bayésien pour l'identification du pourriel...

Installation de Vipul Razor

Vous le trouverez à cette adresse : <http://razor.sourceforge.net/>

«Vipul's Razor» est un système de détection et de filtrage de spam basé sur un réseau peer 2 peer (P2P) écrit en Perl. La licence utilisé par Vipul Razor est l' «Artistic Licence», tout comme le langage dans lequel il est programmé.

Une fois Razor installé lancez dans une fenêtre shell la commande suivante :

```
$ razor-admin -create
```

Cette commande va créer un sous-répertoire . Razor dans votre répertoire personnel, dans lequel il va aller copier tous les fichiers de configuration de Razor. Sauf si vous voulez participer à l'action qu'effectue Razor pour lutter contre le Spam, il ne vous est pas nécessaire d'aller modifier ces fichiers. (pour cela vous pouvez toutefois aller consulter la documentation en ligne de Vipul : <http://razor.sourceforge.net/docs/>)

Il existe un autre agent équivalent à Razor, «Pyzor», il est tout à fait possible de l'interfacer à SpamAssassin, Mais n'offrant pas aujourd'hui tous les avantages de Razor, nous n'en parlerons pas. JE vous conseille quand même de surveiller de temps en temps ce projet qui semble prometteur...

Le Nettoyeur ProcMail (l'accompagnateur du criminel)

Cet outil est appelé par le serveur de messagerie lors de la réception de vos messages avant même que ceux-ci ne soient déposés dans votre boîte aux lettres.

Pour configurer Procmail, créez un fichier procmailrc dans le répertoire /etc en tant que «root» avec votre éditeur de fichier préféré.

L'appel à SpamAssassin se fait de la manière suivante :
(recopiez le contenu du fichier ci-dessous, et faites attention à respecter l'indentation)

```
#Run Procmail as user
DROPPRIVS=yes
```

```
LOGFILE=/var/log/procmail.log
VERBOSE=ON
```

```
# SpamAssassin
# Règle évitant de contrôler les mails supérieurs à 100ko, cela évite que SpamAssassin ne # consomme trop
de ressources systèmes, et les courriers supérieurs à cette taille sont rares... :0fw * <102400
```

```
# appel du deamon SpamAssassin
| /usr/bin/spamc -f
```

```
:0e
{
  EXITCODE=$?
}
```

Le tueur en action

----- Début de Rapport SpamAssassin -----

Ce message est probablement du SPAM (message non sollicité envoyé en masse, publicité, escroquerie...).

Intégrer SpamAssassin dans «Kmail»

Rien de vraiment très compliqué, dans le menu «configuration», cliquez sur «configurer les filtres. Une nouvelle fenêtre apparaît. Nous devons créer deux filtres pour gérer complètement le spam à partir de cette applicatif.

Créez un nouveau filtre, nommez le «vérification spam» par exemple, dans la partie «critères de filtrage» cliquez sur «doit correspondre à tous les critères suivant», en dessous dans le premier ascenseur sélectionnez «size» et comme règle «est supérieur ou égal à» et là saisissez dans la case prévue à cet effet le chiffre 0.

Dans le cadre «actions du filtre» sélectionnez dans l'ascenseur «utiliser le programme de filtre», et la selon la rapidité de votre machine tapez soit :

«spamc -c» (si SpamAssassin a été activé comme deamon au démarrage du système)

«spamd -d» (ceci est généralement le cas lors d'une installation sur MandrakeLinux ou Debian) ;

«SpamAssassin -L» qui appellera le programme à chaque vérification.

Et enfin dans le cadre «options avancées» activez le filtrage «aux nouveaux messages» et sur «filtrage manuel».

Créez ensuite un autre filtre de traitement du spam, nommez-le. Dans la partie «critères de filtrage» cliquez sur «doit correspondre à au moins un des critères». Dans l'ascenseur, s'il n'existe pas, rajoutez «X-Spam-Flag», «contient» et en réponse «yes» (à l'endroit où vous avez mis le 0 tout à l'heure).

Dans le cadre «actions du filtre» placez-les dans un répertoire dédié en sélectionnant dans le premier ascenseur «mettre dans le dossier» et dans l'ascenseur de droite sélectionnez le répertoire choisi par vos soins.

Enfin dans le cadre «options avancées», activez le filtrage «aux nouveaux messages» ainsi que sur le «filtrage manuel», sans oublier d'arrêter le traitement pour que vos spams ne soient pas analysés par vos autres filtres de messagerie... (cochez donc «Si ce filtre est applicable, ne pas poursuivre»).

Pensez enfin, si vous aviez déjà défini d'autres filtres, à mettre ces deux-là en haut de liste ! C'est en effet eux qui doivent être appelés en premier...

Intégrer SpamAssassin dans «Evolution»

La création des filtres de messagerie dans Evolution est très similaire à celle de Kmail. Pour cela, à partir de «la boîte de réception» sélectionnez dans le menu «outils» la ligne «filtres...» Ajoutez-en un nouveau et nommez-le.

Dans le cadre «si...» sélectionnez dans l'ascenseur «Envoyer le message dans une commande shell»(*) et tapez «spamc -c». Dans le cadre «alors...» cliquez sur l'ascenseur de gauche sélectionnez «Déplacer vers le dossier» et sélectionnez celui-ci dans l'ascenseur de droite. Rappelez-vous que celui-ci doit être au format «mbox», cliquez ensuite sur «ajouter» et dans le menu déroulant, cherchez «arrêter le traitement». Voilà c'est fini.

Reseau-message-spamassassin

()Anotation kmchen: cette option n'existe plus en version 2.4.2.1. Personnellement j'ai cliqué "canal d'accès au programme" tapé "spam-c" et cliqué "retourne 0". Résultats à confirmer...*

L'expérience rend maître

En plus de toutes ces possibilités, il est aussi possible de faire apprendre à SpamAssassin certaines choses. Notamment ne pas se tromper de cible, et ne pas, par exemple, envoyer certains messages importants trop facilement à la poubelle car considérés comme «Spam» ou au contraire être trop «coulant» et laisser passer des messages qui sont en fait non sollicités!

Deux cas se présentent alors à nous.

les faux négatifs

Malgré toute la bonne volonté de SpamAssassin ainsi que celle de ses acolytes, il est encore possible que certains courriers ne reçoivent pas la punition qu'ils méritent, pour cela une solution existe :

Dans une fenêtre shell, tapez :

```
sa-learn --spam --mbox .Mail/Spam
```

les faux positifs

Il arrive malheureusement que SpamAssassin fasse des victimes qui n'en sont pas, c'est à dire prendre des courriels valides pour du courrier non sollicité, dans ce cas vous pouvez le lui faire savoir, pour que cela ne se reproduise plus dans l'avenir...

Dans une fenêtre shell, tapez :

```
sa-learn --ham --mbox .Mail/Spam
```

Dans ces deux cas vous devrez avant d'exécuter ces deux commandes créer préalablement un répertoire pour chacun d'eux. Celui-ci doit être obligatoirement au format «mbox» et non «maildir» si vous souhaitez qu'il soit reconnu par SpamAssassin, et que vos données puissent y être traitées...

Le crime était presque parfait...

Presque parfait en effet mais pas complètement, pour cela il faudrait que les spammeurs n'évoluent plus, que les logiciels estampillés «Made in Redmond USA» nous arrivent moins buggés et soient surtout la cible privilégiée vue la facilité avec laquelle cela peut être fait, de les détourner de leur usage initial afin d'inonder tout le monde de pourriels en pagaille et par de la même saturer le réseau.

Quelques Liens

<http://caspam.org/>

<http://www.arobase.org/spam/comprendre-montypython.htm>

<http://fr.wikipedia.org/wiki/Spam>

<http://www.spamanti.net/>

<http://fr.wikipedia.org/wiki/Bayes>

<http://www.euro.cauce.org/fr/index.html>

Conclusion

Sachez enfin qu'il est possible de lier SpamAssassin à un Anti-Virus comme Clamav par exemple et de gérer le Spam du côté serveur (grâce à Postfix, Qmail, sendmail, exim, etc.), c'est-à-dire avant que chaque utilisateur ait eu l'occasion d'ouvrir son client de courriel. Mais cela est une autre histoire...

Un mot sur Mozilla et Thunderbird : Mozilla dans sa version complète et Thunderbird intègrent un système qui leur est propre pour lutter contre le Spam, après plusieurs tests, et malgré des améliorations depuis de nombreuses versions, je trouve personnellement que ces deux applicatifs n'ont pas encore le niveau requis pour lutter efficacement contre le Spam...

Bayes

«Thomas Bayes (env. 1702, Londres – 7 avril 1761) mathématicien britannique et pasteur de l'Église presbytérienne, connu pour avoir formulé le théorème de Bayes.» (source Wikipedia) Son théorème, utilisé aujourd'hui par de nombreuses applications de lutte contre le Spam est en fait une théorie sur les probabilités. Donc pour nous de savoir si un courrier a plus de chance d'être valide ou non...

Le GreyListing ou une mauvaise farce aux Spammeurs :

Evan Harris (l'un des principaux concepteurs de SpamAssassin) a eu l'idée géniale de rendre la vie des spammeurs un peu plus difficile...

En effet, l'applicatif d'Evan retarde au maximum ses réponses d'accessibilité demandés par les Spammeurs sur ses serveurs, en faisant ceci : il ralentit l'envoi des données et par la même l'envoi de courriers non sollicités.

Plus d'informations sur ce projet.

Pour compléter vos listes Noires ou les serveurs de courriels qui permettent à ceux-ci de se propager, veuillez pointer vos navigateurs vers ces deux adresses :

<http://www.spamcop.net>

<http://www.dsbl.org>

Cette page est issue de la documentation 'pré-wiki' de Léa a été convertie avec HTML::WikiConverter. Elle fut créée par Albert le 05/11/2004.

Copyright

Copyright © 05/11/2004, Albert



*Ce document est publié sous licence Creative Commons
Attribution, Partage à l'identique, Contexte non commercial 2.0 :
<http://creativecommons.org/licenses/by-nc-sa/2.0/fr/>*