

EXAMEN PROBATOIRE

Spécialité informatique

janvier 2005



LES FILTRES ANTISPAM

Par : **Jean FRÉOR**

✉ jean_freor@hotmail.com

Soutenance orale : Le 10 janvier 2005
Président de Jury : Professeur Arnaud
Membres du Jury :

SOMMAIRE

Introduction	4
1. Le spam, une nouvelle pollution planétaire.....	5
1.1 Quelques néologismes	5
1.2 À l'origine d'un spam, un spammeur	5
1.2.1 Qui sont les spammeurs ?.....	5
1.2.2 Pourquoi spamment-ils ?	5
1.2.3 Comment récupèrent-ils nos adresses ?	5
1.2.4 Comment spamment-ils ?	6
1.2.5 La répression : une solution ?	6
1.2.6 Les recommandations en vigueur.....	7
1.3 Les conséquences financières du pollupostage	7
1.4 L'évolution quantitative du spam de 2001 à 2005.....	8
2. Les techniques traditionnelles de filtrage du spam.....	9
2.1 Le positionnement du filtre : deux types d'approche	9
2.1.1 Installation d'un logiciel antispam	10
2.1.2 Les services de filtrage en ligne	11
2.2 Les listes blanches/noires, base des procédés de filtrage traditionnels.....	12
2.2.1 Les listes noires	12
2.2.2 Les listes blanches.....	13
2.3 L'analyse par mots-clés	13
2.4 L'analyse lexicologique	14
2.5 Le filtrage bayésien	14
2.5.1 Fonctionnement d'un filtre bayésien	14
2.5.2 L'endroit où s'opère le filtrage bayésien	15
2.5.3 La mise à jour d'une base de données bayésienne	15
2.5.4 Les limites du filtrage bayésien	16
2.6 Le contrôle d'en-tête	17
2.6.1 Détection de la langue	19
3. Des approches complémentaires aux filtres traditionnels	20
3.1 Confirmation de l'expéditeur (Challenge Response).....	20
3.2 Se désabonner ou invalider les messages (Bounce back).....	21
3.3 Réseaux anti-spam collaboratifs	21

3.4 La technologie ne suffit pas : précautions de base	21
3.5 Laisser la main aux utilisateurs	22
3.6 SPF, un référentiel communautaire de serveurs attestés	22
3.6.1 Introduction à SPF	22
3.6.2 Comment SPF fonctionne-t-il ?	22
3.6.3 Un exemple d'utilisation de SPF	23
3.7 RPD, un exemple de technologie innovatrice	24
3.7.1 Fonctionnement général du système RPD	24
3.7.2 Technique de classification des spams	24
3.7.3 Les avantages du système RPD	25
3.7.4 Les limites du système RPD	26
4. Tendances et appréciation des outils antispam	27
4.1 Les contre-attaques réciproques du spam et de l'anti-spam	27
4.1.1 L'anti-antispam	27
4.2 La tendance des procédés antispam	28
4.3 Les principaux critères d'appréciation d'une solution antispam	29
4.3.1 Le piège des faux-positifs.....	29
4.3.2 Souplesse.....	29
4.3.3 Capacité d'auto apprentissage	29
4.3.4 Personnalisation	29
4.3.5 Protection contre les virus.....	29
4.3.6 Contrôle parental	30
4.3.7 Qualité de l'interface	30
4.3.8 Matériel requis	30
4.3.9 Gestion des langues	30
Conclusion	31
Annexe A — Glossaire	33
Annexe B — Table des figures	36
Annexe C — Netographie	37

INTRODUCTION

Le bombardement intempestif de nos boîtes aux lettres électroniques est devenu un phénomène redoutable : entreprises et particuliers reçoivent chaque jour de grosses quantités d'emails indésirables à caractère publicitaire ou frauduleux. C'est ce que l'on appelle les spams. Ces derniers représentent une perte de temps pour chacun ainsi qu'un gaspillage des ressources. Le fléau a explosé au cours de l'année 2004 : après 15 milliards de spams envoyés dans le monde en 2003... il y a en eu 35 l'année suivante. Si bien que la proportion de spams a dépassé les trois quarts du trafic email mondial. C'est pour cette raison que se met en place, plus que jamais, la lutte antispam. Les outils de filtrage du courrier indésirable, conçus pour enrayer ce phénomène, fleurissent ainsi sur le marché, et sont même devenus un enjeu considérable. De même, la protection contre le spam s'impose maintenant comme composante essentielle de la stratégie de sécurité d'un réseau. La problématique guidant la recherche d'efficacité des filtres est la suivante : un filtre antispam idéal devrait assurer un taux de 100% de spams détectés, tout en donnant la garantie qu'aucun mail ne sera considéré à tort comme du spam (ce que l'on appelle les « faux-positifs »).

Les outils antispam utilisent souvent plusieurs techniques combinées. On citera en premier lieu les listes noires ou blanches ("blacklisting" et "whitelisting"). Ces dernières permettent de référencer les expéditeurs de mails dont on sait d'avance qu'ils sont respectivement « spammeurs » ou expéditeurs valides. Mais elles ne suffisent pas : viennent en deuxième lieu les procédés de type heuristique et statistique. Ces filtres se basent sur les caractéristiques communes des emails non sollicités : ils analysent automatiquement le contenu des emails afin de déterminer lesquels d'entre eux sont des spams. Nous trouvons dans cette famille les filtres par mots-clés, les filtres d'en-têtes et surtout les filtres bayésiens, plus « intelligents », issus de la logique probabiliste. En dernier lieu apparaissent peu à peu des techniques nouvelles, conçues pour faire face aux limites posées par les procédés traditionnels, ces derniers s'avérant de plus en plus rigides. Il faut citer à ce titre les systèmes d'authentification de l'expéditeur ou encore les techniques de classification centralisée des spams en temps réel.

Seulement, une limite s'impose très vite à la lutte antispam. Les spammeurs ne sont jamais au bout de leur créativité et n'hésitent pas à faire l'acquisition de ces logiciels afin de mieux connaître leurs modes de fonctionnement, ce qui les aide ainsi à contourner leurs procédés de filtrage. De ce point de vue, on peut parler de techniques « anti-antispam ». On peut alors se demander si le pollupostage va finir par gagner ou perdre progressivement la bataille contre les techniques de lutte contre le spam. Dans l'immédiat subsiste une question subsidiaire mais souvent essentielle, celle de connaître les meilleurs critères d'appréciation d'une solution antispam.

Ce rapport s'emploiera dans une première partie à présenter les différents aspects du spam : origine, auteurs, conséquences, évolution. Les deuxième et troisième parties présenteront, pour l'une, les méthodes traditionnelles de filtrage (à ce sujet, il sera mis en évidence la spécificité de chacune, leurs intérêts ainsi que leurs inconvénients) et, pour l'autre, les méthodes complémentaires de lutte contre le spam : des astuces pour limiter le spam, aux techniques innovatrices. Enfin, seront étudiées dans une quatrième partie les limites générales des solutions antispam, puis leurs tendances. Cette dernière partie sera aussi l'occasion de faire le point sur les critères essentiels à prendre en compte pour qui veut se prémunir contre le spam. Par ailleurs, un glossaire est disponible à la fin de ce rapport ; il définit les termes fréquemment utilisés dans le monde de l'email et de la lutte contre le spam. On trouvera à sa suite une table des figures, puis une bibliographie Internet non exhaustive référençant quelques sites web ayant servi de base de recherche à la rédaction de ce dossier.

1. LE SPAM, UNE NOUVELLE POLLUTION PLANÉTAIRE

1.1 Quelques néologismes

Le mot « spam » est utilisé pour désigner le courrier électronique non sollicité. Il vient d'un sketch des Monty Python dans lequel les comédiens chantent "spam, spam, spam, spam" sans interruption¹. Or, Internet a une prédilection pour les expressions courtes, et le caractère répétitif et incessant de ces paroles reflète parfaitement celui des courriers électroniques non sollicités.

Le mot « spam » a ses équivalents dans notre langue française : « pourriel » ou encore « courrier-rebut ». On parle aussi de « pollupostage » (le fait de diffuser du spam).

1.2 À l'origine d'un spam, un spammeur

1.2.1 Qui sont les spammeurs ?

Les « spammeurs » sont les personnes ou sociétés responsables de l'envoi de spam. Ils restent souvent mystérieux. Il est intéressant de remarquer que seulement 200 organisations professionnelles sont responsables de 80% des attaques mondiales.

1.2.2 Pourquoi spamment-ils ?

On s'aperçoit avec étonnement, mais avec évidence, que la seule raison d'être d'un spam est qu'il est une source de profit pour son expéditeur. Si les spams persistent malgré les moyens mis en œuvre pour les filtrer², la raison est simple : un spam sur quelques milliers trouve preneur, or le pollupostage ne coûte presque rien et les moyens trouvés pour contourner les filtres antispam sont, eux aussi, en progrès continuels.

1.2.3 Comment récupèrent-ils nos adresses ?

Les spammeurs arrivent à connaître nos adresses email de différentes façons :

- Notre fournisseur a revendu tout ou une partie de sa liste d'abonnés à un tiers, qui lui-même l'a revendu à un autre. L'opération peut être faite dans la légalité, mais ce n'est pas toujours le cas ;

¹ Le mot « SPAM » est à l'origine une marque de corned-beef : Spiced Pork And Meat. Il existe un site commercial www.spam.com, mais dédié au pâté du même nom.

² Se référer, pour l'explication des techniques classiques de filtrage, au chapitre 2 de ce rapport (page 9).

- Notre adresse a été générée au hasard en utilisant toutes les combinaisons possibles à partir d'une liste des noms et des prénoms les plus courants (prénom.nom, nom, prénom, nprénom...);
- Qui passe une commande sur un site de commerce électronique ou souscrit aux services d'un site, ou encore d'une liste de diffusion, laisse son adresse électronique. Or, si l'utilisateur oublie de cocher (ou décocher) la case correspondante³, alors il autorise tacitement la diffusion de son adresse électronique. Peut-être n'a-t-il même pas eu ce choix...
- Enfin, et surtout, celui qui contribue à un forum ou laisse son adresse électronique sur une page perso est susceptible d'intégrer un fichier d'adresses. En effet, les spammeurs disposent de robots qui scannent automatiquement le contenu des sites web dans l'objectif d'en extraire les adresses électroniques⁴.

1.2.4 Comment spamment-ils ?

Les robots-spammeurs utilisent :

- Des serveurs SMTP anonymes : serveurs de relais de courrier⁵ en accès libre (dont le notre, avec usurpation d'adresses – en anglais : *Address Spoofing* –);
- Des serveurs proxy publics ;
- Des adresses IP dynamiques.

1.2.5 La répression : une solution ?

Nous pouvons nous demander s'il ne serait pas logique de mettre en œuvre des moyens de traque et de répressions contre les spammeurs, plutôt que des systèmes de filtrage du spam. En effet, de nombreux guides sur le Net apprennent à analyser les en-têtes des emails puis à utiliser des ressources en ligne pour aider à localiser le spammeur et se plaindre auprès de son FAI. Malheureusement, il s'avère que cela ne fait pas gagner du temps, car il est toujours plus facile et rapide d'appuyer sur la touche « Suppr » de son clavier pour supprimer un spam. Il y a eu des débuts de législation, notamment aux États-Unis. Néanmoins, la loi fédérale américaine votée cette année⁶ n'a pas réellement résolu le problème du spam, même si certaines condamnations ont été très sévères⁷.

À savoir : le nombre d'emails commerciaux non sollicités qui ne respectent pas les règles édictées par le législateur américain représente encore 96% des e-mails commerciaux.

³ Contrairement à la loi en vigueur aux U.S.A, la loi française veut que ces cases soient décochées par défaut.

⁴ Les webmaster peuvent utiliser comme astuce l'encodage des adresses emails dans le code source de leurs pages. Ce type d'outil est disponible en ligne, par exemple à cette adresse : http://www.caspam.org/cas_cryptemail.html

⁵ Le propre d'un relais de courrier est qu'il accepte de transmettre les emails a un destinataire quelconque.

⁶ La loi exige en effet d'apposer la mention "SEXUALLY-EXPLICIT" dans l'objet du courriel et au début du message.

⁷ En novembre 2004, un spammeur a été condamné à neuf ans de prison.

1.2.6 Les recommandations en vigueur

Il est également intéressant de se pencher sur les recommandations officielles en vigueur dans le monde de l'Internet à propos du spam. La RFC 2505⁸, par exemple, spécifie des recommandations pour la configuration des serveurs SMTP en vue de la lutte contre le spam. Selon cette RFC, le mécanisme de relais de courrier doit être contrôlé du fait de l'abus de cette fonctionnalité par les spammeurs. Ce mécanisme est donc par défaut interdit sur les serveurs SMTP, mais doit pouvoir être sélectivement autorisée pour les utilisateurs dûment habilités du serveur (par exemple, un fournisseur d'accès doit relayer les mails seulement pour ses clients, mais pas pour les autres). En revanche, pour autoriser le relais de mails, il faut authentifier le client. Ceci peut se faire par le détournement d'un mécanisme existant : *POP-Before-SMTP*⁹. Une autre RFC, la n°2635, concerne le spam, mais celle-ci est à caractère informatif ; il y est moins question de recommandations, et encore moins de standards : on y puise des informations générales sur le spam à destination de chacun (utilisateurs, administrateurs, FAI...). Enfin, il faut noter que ces deux RFC datent de 1999, mais ne semblent pas être obsolètes (par exemple, les protocoles de transport du courrier électronique comme POP ou SMTP ne changent pas d'année en année).

1.3 Les conséquences financières du pollupostage

La conséquence négative première du spam est qu'il fait perdre du temps à tous. Si on se penche à présent sur les conséquences secondaires (financières) du spam, on s'aperçoit que les statistiques prouvent l'absurdité de sa logique commerciale globale¹⁰ :

- Les profits annuels du spam s'élèvent à 4 millions de dollars
- Les dommages annuels du spam s'élèvent à 15 milliards de dollars¹¹

Il apparaît alors clairement que les profits générés par le pollupostage¹² sont négligeables par rapport aux dommages causés par celui-ci dans les entreprises du monde entier. En l'occurrence, la perte de productivité engendrée s'élève dans chaque entreprise, et chaque année, à 428 dollars en moyenne par employé¹³.

En outre, il est prévu qu'au cours de l'année 2005, les dommages engendrés par les spams seront supérieurs à ceux causés par les virus.

⁸ Cette RFC est disponible sur internet : <http://www.ietf.org/rfc/rfc2505.txt>

⁹ *POP-before-SMTP* est une manière de pallier le manque d'authentification de SMTP en contrôlant les accès par POP ou IMAP, qui, eux, sont authentifiés, et en autorisant les connexions en SMTP pendant un certain temps depuis l'adresse IP ayant servi à se connecter.

¹⁰ Selon les estimations de l'organisme IDC (premier groupe mondial de conseil et d'étude sur les marchés des technologies de l'information)

¹¹ La société Radicati Group a enregistré de son côté une perte de 11 milliards de dollars en 2004 et en prévoit une de 17 milliards pour 2005. Si on fait une moyenne entre 2004 et 2005, les chiffres concordent donc avec ceux de l'institut IDC.

¹² Environ 0,1 % des personnes spammées répondent « favorablement » à ce spam.

¹³ Selon Commtouch, éditeur de solution antispam. Une page sur leur site permet de simuler le coût de la perte de productivité due au spam : http://www.commtouch.com/spam_cost_calculator.shtml

1.4 L'évolution quantitative du spam de 2001 à 2005

En mai 2004, les spams représentaient 76% des courriels reçus en entreprise.

Selon les estimations d'IDC datant d'avril 2004, la variation annuelle connue par les quantités de spam reçus quotidiennement dans le monde sont mise en valeur dans le graphique qui suit :

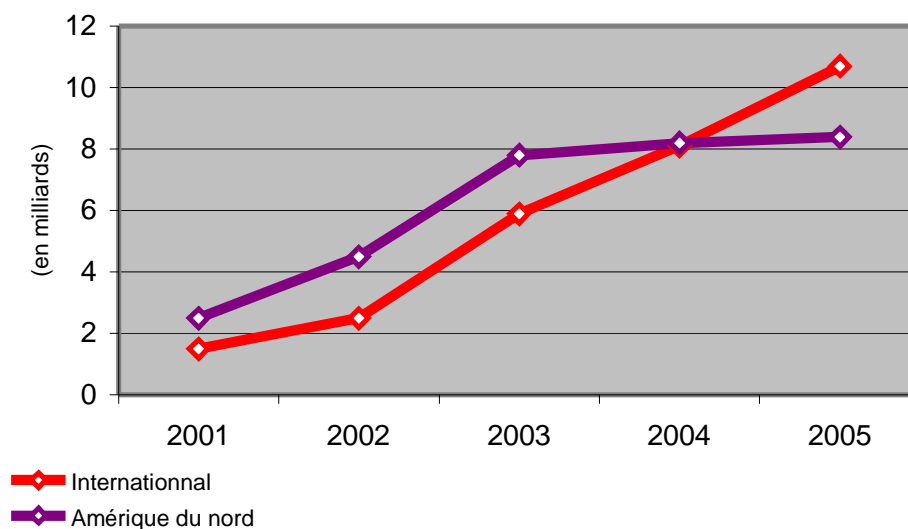


Figure 1 – Évolution de la quantité quotidienne de spam en Amérique du nord et dans le monde entier

Ce graphique révèle deux choses. En premier lieu, la quantité de spam circulant quotidiennement accroît fortement d'année en année, et dans tous les pays du monde. En deuxième lieu, c'est seulement au cours de l'année précédente (2004) que la quantité de spam a été moins importante en Amérique du nord (principalement les USA et le Canada) que dans le reste du monde. Face à ce constat, il apparaît nécessaire d'accorder de plus en plus d'importance au critère de capacité multi-langues d'un système de filtrages du spam. En effet, la proportion de spams en langue anglophone semble perdre du terrain.

Toutefois, les estimations précédentes datant d'avril 2004, il est important de rapporter des chiffres récents sur l'évolution observée ces 6 derniers mois : selon la société FrontBridge, la proportion de spams par rapport au volume total d'emails envoyés est passée de 75% (mai 2004) à 87% (octobre 2004). Ainsi, pour plus de fidélité, il serait nécessaire de revoir nettement à la hausse les chiffres pour 2004 sur la courbe « Figure 1 » ci-dessus.

Bref, ce constat général de la montée continue des quantités de spams incite de plus en plus d'entreprises et de particuliers à se prémunir contre le pollupostage, qui engendre une perte de temps et représente une agressivité continue. Quant à 2005, il est probable que l'on doive également revoir à la hausse la proportion du spam... reste à savoir si les techniques antispam actuelles ne vont pas tarder à faire preuve d'une efficacité propre à décourager les spammeurs, et ainsi faire baisser les quantités de spams envoyés ? Dans l'attente, voyons dans la partie suivante en quoi consistent les procédés antispam.

2. LES TECHNIQUES TRADITIONNELLES DE FILTRAGE DU SPAM

Avant de parler technologie, voyons en premier lieu les différents types d'architecture pour un système utilisant une messagerie protégée par un antisпам.

2.1 Le positionnement du filtre : deux types d'approche

On observe classiquement deux types de scénarios :

- 1) Le filtrage antisпам « à la demande ». Le filtre antisпам est positionné sur un serveur proxy. Le filtrage est alors automatique et transparent. Exemple : le produit *SpamWeed*.
- 2) Le filtrage « vérificateur ». La solution antisпам s'interpose entre l'utilisateur et le serveur POP, qu'elle scrute périodiquement. Exemples : les produits *SpamKiller* ou *Mailwasher*.

Les deux types de scénarii et leurs points forts/faibles sont mis en valeur dans le tableau ci-dessous :

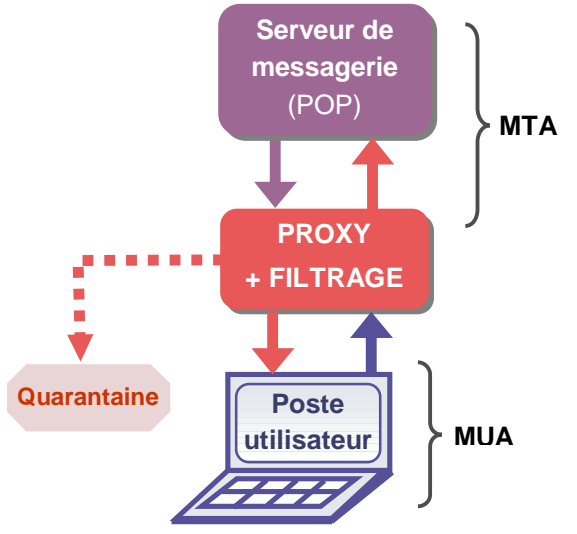
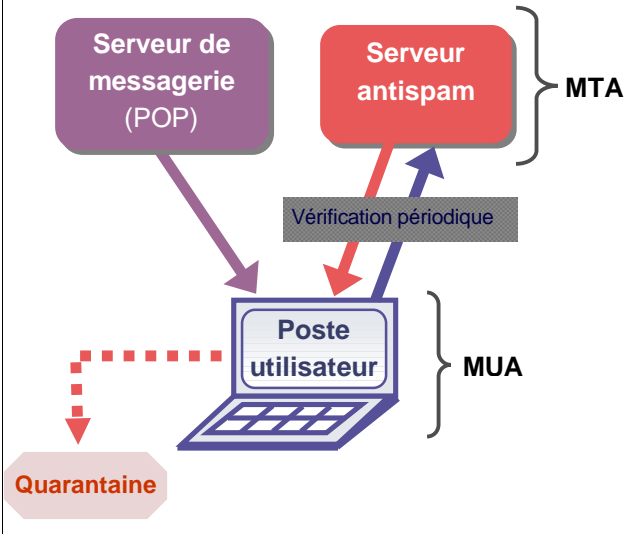
1) Filtrage « à la demande »	2) Filtrage « vérificateur »
<p><u>Schéma architectural :</u></p>  <p>Détails du schéma : Le serveur de messagerie (POP) est relié au proxy + filtrage. Le proxy + filtrage est relié au poste utilisateur. Une quarantaine est reliée au proxy + filtrage. Les composants POP et proxy sont regroupés sous MTA, et le poste utilisateur sous MUA.</p>	<p><u>Schéma architectural :</u></p>  <p>Détails du schéma : Le serveur de messagerie (POP) est relié au poste utilisateur. Le serveur antisпам est relié au poste utilisateur via une vérification périodique. Une quarantaine est reliée au poste utilisateur. Les composants POP et serveur antisпам sont regroupés sous MTA, et le poste utilisateur sous MUA.</p>
<p><u>Avantages</u> : Facilité d'utilisation ; Toutes les opérations sont transparentes pour le client de messagerie.</p>	<p><u>Avantages</u> : Le filtre est personnalisable et paramétrable par l'utilisateur.</p>
<p><u>Inconvénients</u> : Le filtre n'est ni maîtrisable, ni personnalisable selon le contexte utilisateur ; ce dernier ne peut pas classer manuellement ses mails en « spams / pas spams ».</p>	<p><u>Inconvénients</u> : La partie MUA n'est pas toujours bien synchronisée avec le vérificateur anti-spam. De plus, la part de travail laissée à l'utilisateur l'utilisateur n'est plus négligeable.</p>

Figure 2 – Les deux types d'architecture classiques pour l'intégration d'une solution antisпам

2.1.1 Installation d'un logiciel antispam

Qui veut offrir une solution antispam à son serveur de messagerie peut l'installer en tant que logiciel en local se comportant comme une « passerelle de messagerie ». Pour ce faire, il faut s'assurer que ce dernier est le premier à recevoir le courrier destiné au serveur de messagerie (courrier entrant), ainsi que le dernier pour le courrier en partance (courrier sortant). Cette installation est aussi connue sous le nom de « Smart host » (Hôte Actif). Le schéma architectural suivant montre qu'une telle solution antispam s'apparente généralement à un serveur-relais de courrier :

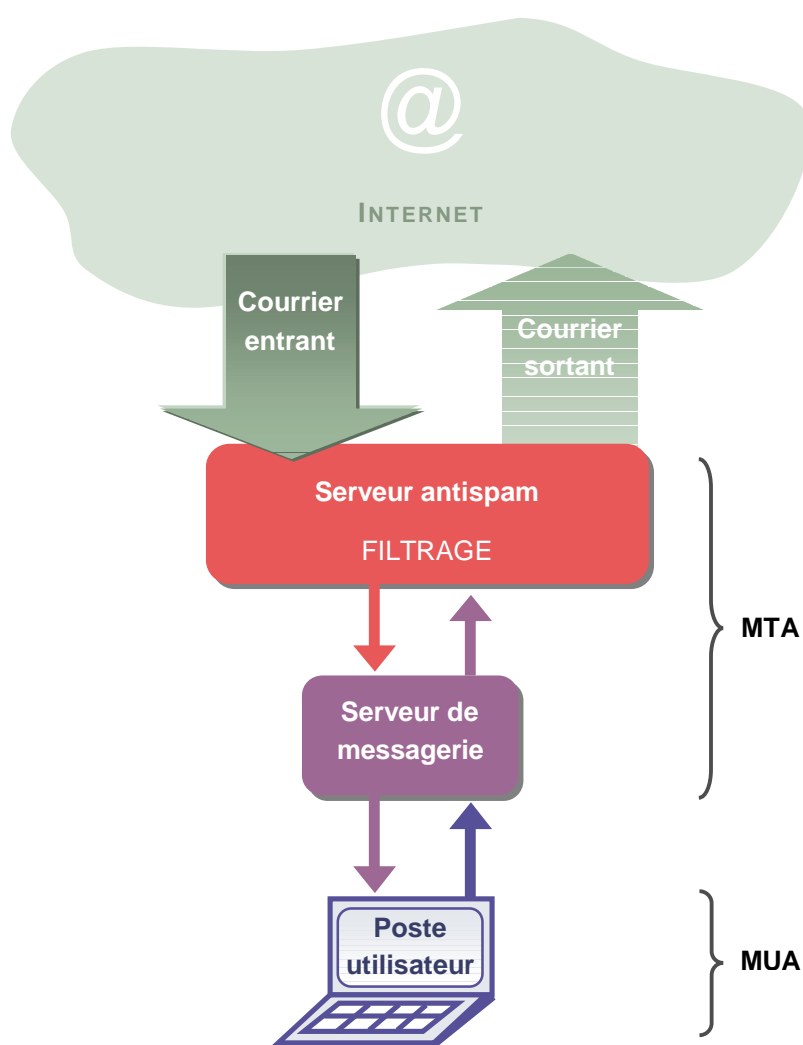


Figure 3 – Architecture d'un système de messagerie exploitant un serveur antispam en interne

Au passage, il faut noter qu'un bon nombre de logiciels antivirus s'interposent d'une façon équivalente entre le courrier entrant/sortant et le serveur de messagerie. On trouve même de nombreuses solutions intégrant à la fois la fonction d'antispam et d'antivirus. On peut citer en exemple l'outil *ProtecMail*¹⁴.

¹⁴ Site commercial : <http://www.protecmail.com/fr/>

2.1.2 Les services de filtrage en ligne

Il faut préciser que certaines solutions antispam telle que *ProtecMail* (logiciel déjà cité précédemment) sont également disponibles dans des versions dites « en ligne ». L'emplacement du système de filtrage n'est alors plus situé au niveau du serveur de messagerie du client, mais au niveau du serveur distant (sur Internet) offrant ce service. Ce sont, le plus souvent, des particuliers qui optent pour cette solution. En effet, leur serveur de messagerie (niveau MTA) est généralement déjà un service en ligne¹⁵, c'est-à-dire situé sur internet.

Le schéma ci-dessous met en évidence la différence architecturale qui oppose cette méthode avec l'utilisation d'un logiciel antispam local.

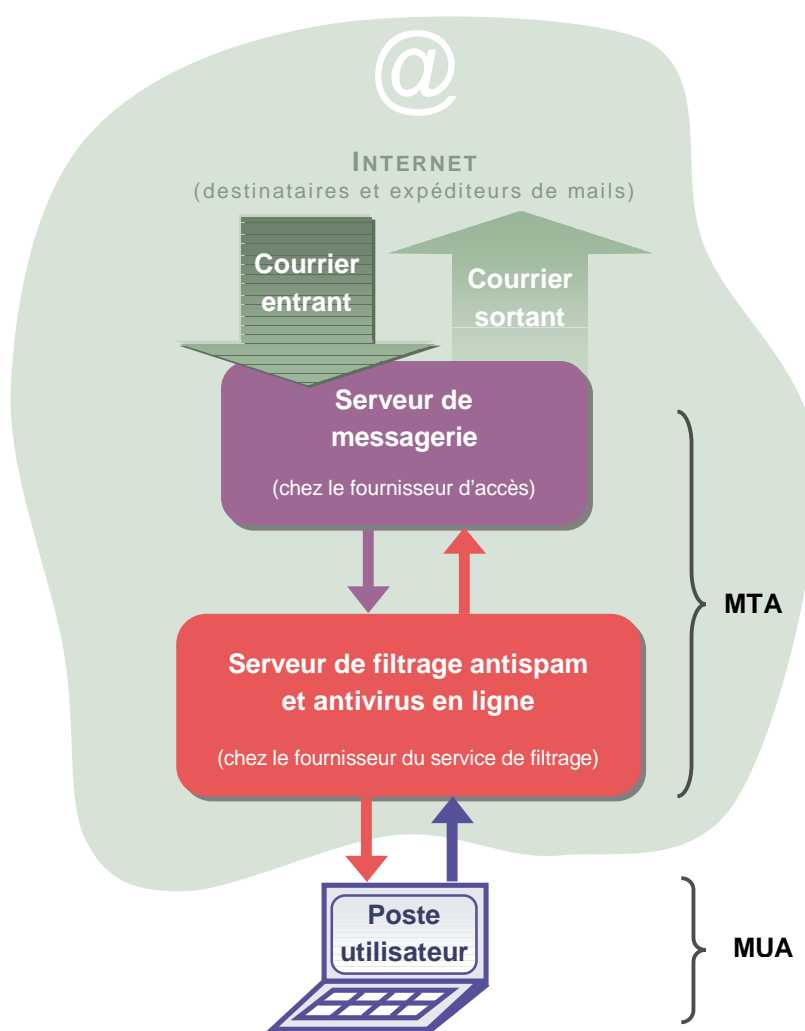


Figure 4 – Architecture d'un système de messagerie exploitant un service de filtrage en ligne

En l'occurrence, le service de filtrage en ligne proposé par *ProtecMail* est très bon marché¹⁶. Cette solution consiste à faire transiter les mails de leurs utilisateurs par leur serveur centralisé. Il suffit de configurer son logiciel de messagerie (de niveau MUA) pour que celui-ci pointe vers le serveur de

¹⁵ Exemple : le serveur de messagerie du fournisseur d'accès Free (smtp.free.fr).

¹⁶ Ce service ne coûte que 1,5 € par mois (prix relevé en janvier 2005) ce qui convient d'autant mieux à des particuliers.

ProtecMail. Ce dernier, situé sur Internet, sait auprès de quel serveur de messagerie (niveau MTA) récolter les mails susceptibles de contenir des spams ou des virus.

L'avantage de ce type de service est double. D'une part, il permet à ses bénéficiaires d'éliminer une majorité de spam avant leur téléchargement, ce qui diminue leur temps de connexion (ce qui n'est pas négligeable pour les utilisateurs d'un modem téléphonique 56Kb/s). D'autre part, il n'y a ni logiciel à installer, ni de mises à jour régulières à planifier : il suffit juste de paramétrer ce service une fois pour toutes. En revanche, un inconvénient des services de filtrage en ligne est de rendre difficile, voire impossible, la maîtrise du filtrage des courriels.

D'autres exemples de services de filtrages peuvent être *Clinbox* de Dolphian, ou *Pop3Scan*, ou encore *Vade Retro ASP* de Goto.

2.2 Les listes blanches/noires, base des procédés de filtrage traditionnels

La politique de liste blanche et de liste noire¹⁷ n'est pas propre au domaine de la lutte antispam : les serveurs proxy des entreprises en sont souvent pourvus afin de restreindre l'accès vers les sites web n'étant pas jugés en relation avec l'activité professionnelle exercée. Dans ce cas, l'expression « liste noire » désigne une liste contenant les URLs interdites. Au contraire, l'expression « liste blanche » contient les URLs autorisées. Ce concept impose souvent un compromis entre le coût d'entretien de la liste blanche par les administrateurs de l'entreprise et la perte engendrée¹⁸ par le fait que certains sites ne sont pas couverts par la liste noire. Il faut évaluer la taille d'une liste blanche, ainsi que son évolution dans le temps. Quant aux listes noires, elles sont mises à jour régulièrement, et, le plus souvent, par des sociétés spécialisées fournissant ce service.

Dans le cas de l'antispam, les listes blanches ou noires ne référencent plus les URLs autorisées ou interdites, mais plutôt les expéditeurs de mails (tantôt correspondants légitimes, tantôt spammeurs présumés).

2.2.1 Les listes noires

Jusqu'à aujourd'hui, la « liste noire » est sous-doute la technique de filtrage la plus commune (que la solution soit positionnée ou non sur le poste client). La logique de cette technique consiste à « marquer » certaines adresses email (ou certains domaines) dont on ne souhaite plus recevoir de message.

Le problème posé par cette approche est que les utilisateurs doivent maintenir manuellement et/ou mettre régulièrement à jour leur liste noire auprès d'une base de données centralisée afin de toujours posséder la dernière version de la liste des « expéditeurs illégitimes ». De plus, cette technique peine en réalité à bloquer le spam, parce que les spammeurs peuvent trop facilement modifier leurs adresses emails entre chaque envoi de spams, et rendent ainsi la liste noire inutile.

Il existe aussi des listes noires, mais basée sur le contenu des messages : l'exercice consiste à classifier certains mots-clés comme étant illicites et bloquer les emails qui contiennent ces mots. C'est ce que l'on appelle les filtres par mots-clés (se reporter plus loin : paragraphe 2.3, page 13).

¹⁷ En anglais : « blacklisting / whitelisting »

¹⁸ Cette perte est double : l'occupation de la bande passante ainsi que la perte de productivité.

2.2.2 Les listes blanches

Le filtrage de spams par liste blanche, comme par listes noires, nécessite l'usage d'un outil spécifique qui permet à la fois des mises à jour fréquentes et une personnalisation possible du contenu de ces listes.

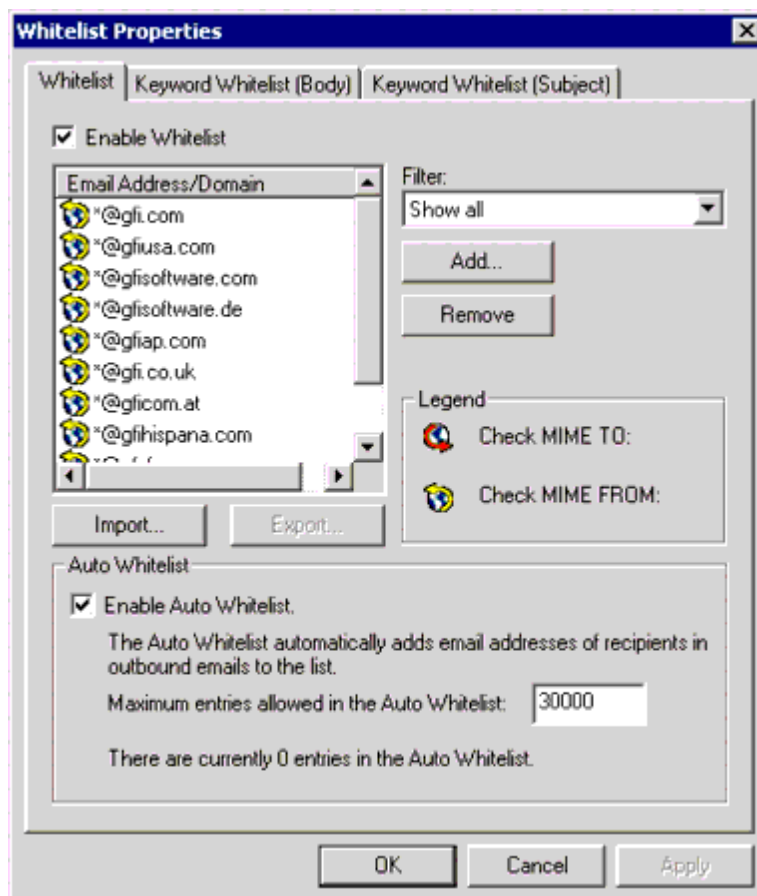


Figure 5 – Configuration d'une liste blanche dans le logiciel GFI MailEssentials

L'inconvénient des listes blanches est que le destinataire doit traiter manuellement les messages provenant d'expéditeurs inconnus.

Il n'est jamais conseillé de compter uniquement sur les listes noires ou listes blanches. En effet, ces méthodes se sont pas gérables pour ceux qui reçoivent une grande quantité de messages provenant de personnes inconnues. Cependant, la technologie en elle-même n'est pas complètement inutile. Elle peut être utilisée en complément à d'autres technologies pour améliorer les taux de détection et rendre les produits anti-spam plus simples d'utilisation et plus personnalisables.

2.3 L'analyse par mots-clés

La correspondance par mots-clés est une très ancienne méthode. Elle marque les messages en tant que spam si certains « mots suspects » sont détectés, et les marque plus favorablement en courrier valide si certains « bon mots » sont trouvés.

Cette approche implique d'analyser le corps d'un email pour des mots-clés spécifiques et des expressions (exemples : « sexe », « Viagra »). Ces mots sont en effet peu susceptibles d'apparaître dans une correspondance professionnelle classique. Mais l'analyse de mot-clé en tant que solution antispam autonome est une technique très primitive, car :

- Elle produit un taux élevé de faux-positifs (messages légitimes marqués en tant que spam) ;
- Il est possible pour les spammeurs d'abandonner certains mots-clés et d'en utiliser d'autres pour exprimer la même chose ;
- Elle ne peut rien contre les mots suspects incorporés dans des images... À moins, bien sûr, de disposer d'un produit antispam avec reconnaissance de caractères intégrée, mais ce n'est apparemment pas proposé sur le marché à ce jour ;

2.4 L'analyse lexicologique

Une problématique se pose fréquemment dans la lutte antispam : la présence d'un mot ou d'une expression suspecte par elle-même ne signifie pas nécessairement que le message en question est un spam : il faut donc à tout prix éviter qu'il soit reconnu à tort comme un spam. À la différence de l'analyse par mots-clés, l'analyse lexicologique analyse le contexte de tous les mots et les expressions dans un message particulier. À chaque mot ou expression est assigné un poids qui dépend principalement du contexte dans lequel on le trouve.

2.5 Le filtrage bayésien

Le filtrage bayésien est une technique dite adaptative, qui reflète notre propre définition de ce qu'est et n'est pas un spam. Il se situe parmi les techniques de détection du spam les plus efficaces, ce qui le rend très populaire dans le champ de bataille de l'anti-spam. Ce que l'on appelle la « classification naïve bayésienne » ne date pas d'aujourd'hui, mais de 1763, basée sur la théorie statistique du scientifique anglais T. Bayes.

Le principe de tout filtre bayésien est d'apprendre par les exemples. En effet, lors d'une première utilisation, il peut paraître insatisfaisant. Cependant, après quelques jours d'entraînement, il devient extrêmement précis. Bien que l'entraînement puisse être légèrement gênant, comparé aux efforts requis par les autres méthodes, cela reste trivial, et les avantages pèsent bien plus lourd que le coût exigé.

L'intérêt incontestable de cette méthode est qu'elle bénéficie d'un taux élevé de détection de spam, tout en garantissant un nombre très bas de faux-positifs. Dans l'article écrit par Paul Graham¹⁹, "Un plan pour le spam", l'auteur affirme qu'après une petite période d'apprentissage, les filtres bayésiens bloquent plus de 99,5% des spams, avec 0,03% de faux-positif. Une solution comme 'GFI MailEssentials' à base de filtre bayésien, estime son taux de reconnaissance du spam à 98% après une période de seulement deux semaines²⁰.

2.5.1 Fonctionnement d'un filtre bayésien

Imaginons un courrier candidat au filtrage bayésien. Supposons que ce courrier contienne certains mots qui avaient déjà été repérés auparavant dans des courriers considérés comme spam. Supposons également que ces mots ne sont encore jamais apparus dans un courrier valide (encore appelé « ham » – en raison de « Paul Graham » ?). Alors, il est légitime de considérer que ce courrier électronique est un spam.

¹⁹ Paul Graham est le "gourou" de la technique Bayésienne. : <http://www.paulgraham.com/spam.html>

²⁰ Voir la page d'argumentation sur leur site : <http://www.gfsfrance.com/fr/mes/meswhy.htm>

C'est ainsi qu'un filtre bayésien accumule sans cesse les résultats de ses analyses, qui sont eux-mêmes utilisés par la suite pour aider à démasquer des courriers futurs, comme le montre le schéma suivant :

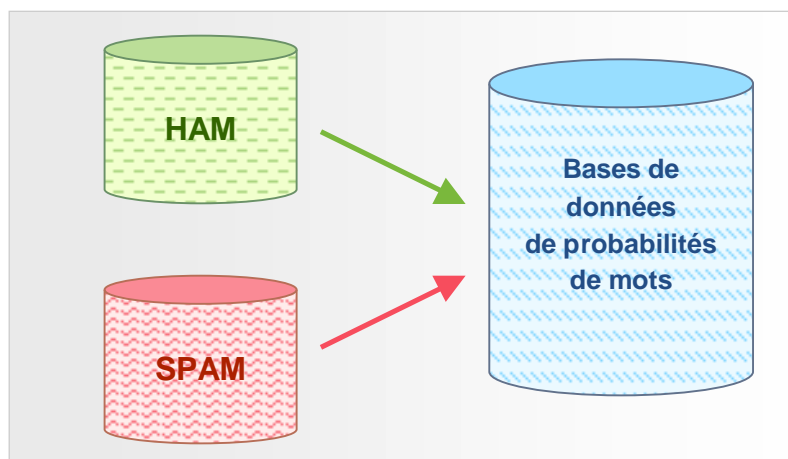


Figure 6 – Création d'une base de données de mots pour le filtre bayésien

C'est une valeur de probabilité qui est affectée à chaque mot ou unité lexicale. Celle-ci est basée sur des calculs qui tiennent compte du nombre de fois que ce mot se présente en tant que spam, par opposition au « ham » qui est le courrier valide. Cela se fait en analysant d'une part le courrier sortant des utilisateurs, et d'autre part les spams connus : tous les mots et unités lexicales des deux regroupements de courrier sont analysés pour définir la probabilité pour qu'un courrier soit un spam.

Cette probabilité par mot est calculée de la façon suivante : si par exemple le mot « mortgage »²¹ apparaît dans 400 des 3.000 messages spam, et dans 5 des 300 messages légitimes, alors sa probabilité d'être un spam serait de 0,8889. (²²)

Il est alors logique de concevoir qu'un filtre bayésien a besoin d'un minimum de temps pour devenir pleinement efficace. C'est ce que l'on appelle le « temps d'apprentissage » du filtre bayésien. Le produit *GFI MailEssentials* est un exemple de solution antispam utilisant le filtre bayésien comme technique de défense principale. En effet, la société GFI recommande de laisser au filtre le temps de s'adapter à sa messagerie pendant au moins une semaine, durant laquelle l'utilisateur est sollicité pour aider le système à classifier le courrier en « spam / pas spam ». Selon GFI, c'est seulement après cette période qu'il devient utile d'activer le filtrage.

2.5.2 L'endroit où s'opère le filtrage bayésien

Le serveur sur lequel est installé le filtre bayésien est généralement placé en amont du serveur de messagerie (MTA).

2.5.3 La mise à jour d'une base de données bayésienne

Beaucoup de logiciels à base de filtre bayésien rendent possible d'utiliser une mise à jour des dictionnaires de probabilités de mots à partir d'un serveur centralisé sur Internet, donc commun aux entreprises du monde entier qui utilise ce logiciel. Cela revient du partage d'informations.

²¹ En français : « Hypothèque »

²² Le calcul est le suivant : $[400/3000] / [5/300 + 400/3000]$

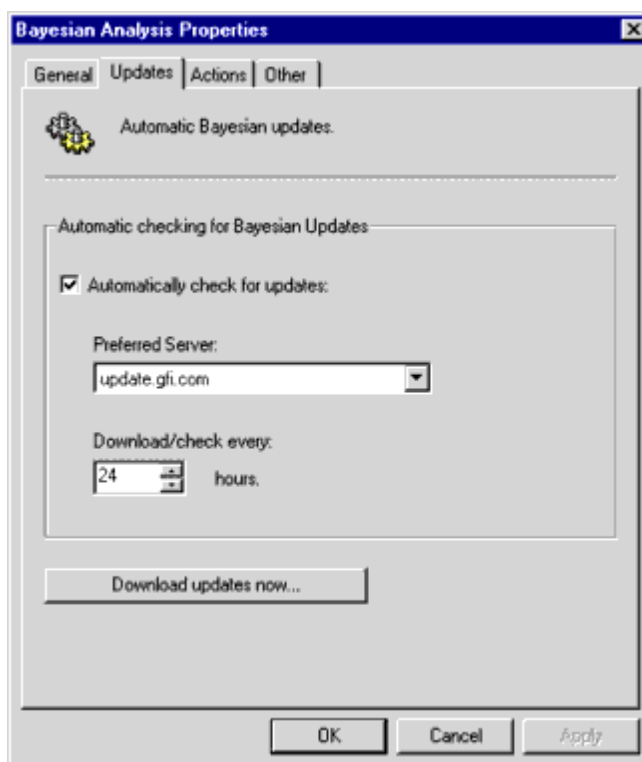


Figure 7 – Paramétrage des mises à jour d'un filtre bayésien dans GFI MailEssentials

2.5.4 Les limites du filtrage bayésien

Si les filtres bayésiens sont actuellement réputés pour leur efficacité, cela ne durera peut-être pas :

- La phase d'apprentissage d'un filtre bayésien dure souvent plus longtemps que ce que l'on lit dans les argumentaires commerciaux des différents produits : il faudrait en réalité compter plusieurs mois, et non 2 semaines comme le prétend GFI.
- Ils sont facilement contournables par les spammeurs et ne peuvent pas analyser les spams dans toutes les langues, et particulièrement ceux à base d'images — Cf. page 27 : « **Leurres pour dictionnaires anti-bayésiens** » ;
- Ces filtres sont inefficaces contre la fraude. Par exemple, un spam connu est celui d'une fausse banque (*CitiBank*) nous conviant à saisir sur leur site notre numéro de carte bleue ainsi que notre code confidentiel²³... De plus, ce spam est à base d'image, ce qui nous renvoie de toute façon à l'inconvénient détaillé dans le point précédent. Ceux qui sont en mode texte contiennent un vocabulaire commercial non suspect, et n'ont donc pas de raison d'être interceptés par un filtre bayésien.
- Les filtres bayésiens sont souvent utilisés avec une mise à jour régulière auprès d'une base de données centralisée commune à tous les utilisateurs d'un même produit (voir paragraphe précédent). C'est un tort, car là se situe justement l'intérêt d'un filtre bayésien : pouvoir s'adapter à un contexte unique.

²³ Ce que l'on appelle le « Phishing ». En 2004, la somme considérable de 137 millions de dollars a été prélevée par Phishing.

Au regard de ces inconvénients, la remarque suivante de la part d'Arabella Hallawell²⁴, aussi étonnante qu'elle puisse paraître pour les inconditionnels du filtrage bayésien, serait donc pleinement justifiée : « Les filtres bayésiens ont montré qu'ils n'étaient pas fiables pour filtrer les spams en entreprise ».

2.6 Le contrôle d'en-tête

Dans certains logiciels antispam, un module permet de contrôler l'en-tête de chaque email pour renforcer les chances de détecter les spams. Un tel module analyse chaque champ individuel d'une en-tête, soient les champs « SMTP » et « MIME ». Les champs SMTP sont spécifiés par le serveur de messagerie, alors que les champs MIME sont spécifiés par le client de messagerie (qui crypte le mail en MIME).

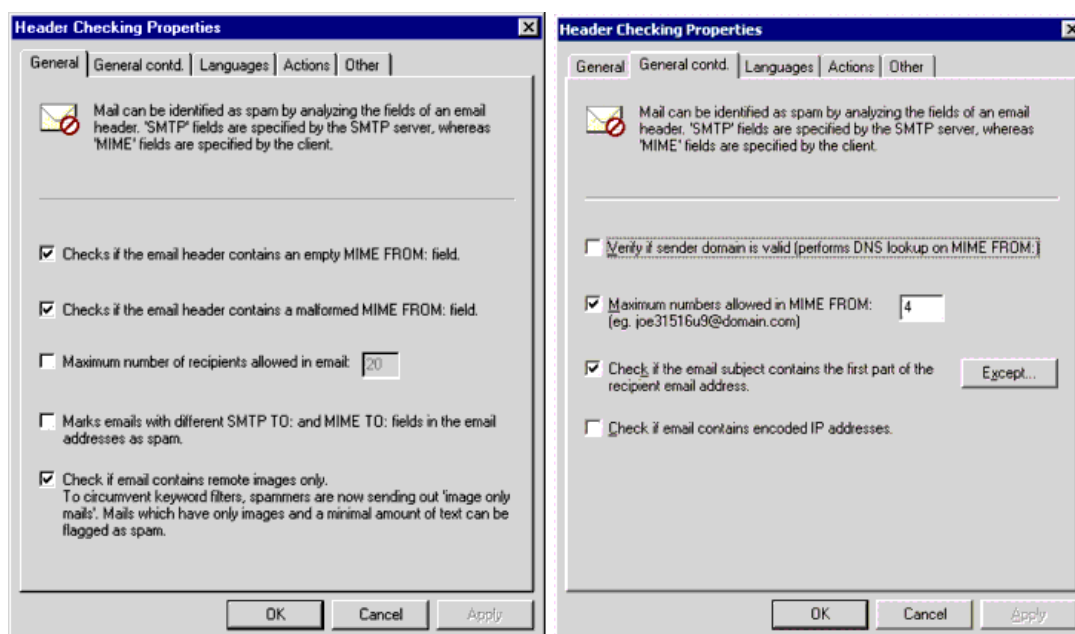


Figure 8 – Configuration du contrôle d'en-tête dans GFI MailEssentials

La copie d'écran ci-dessus montre l'onglet général de la fenêtre des propriétés du contrôle d'en-tête de la solution GFI MailEssentials. Cette fenêtre propose les options suivantes, qui sont communes à la plupart des filtres d'entêtes :

1. 'Checks if the email header contains empty MIME "From:" field'. Cette fonctionnalité vérifie si l'expéditeur s'est identifié dans le champ `FROM`. Si ce champ est vide, alors ce mail provient très certainement d'un spammeur ;
2. 'Checks if the email header contains a malformed MIME "From:"'. Cette fonction vérifie si l'en-tête MIME du champ expéditeur est correcte, c'est-à-dire s'il correspond aux RFC (les spammeurs y insèrent souvent une adresse erronée).
3. 'Marks emails with recipient lists of more then X recipients as spam'. Cette fonctionnalité marque les courriers comme spam s'ils sont adressés à un grand nombre de destinataires. Cela arrive lorsque le spammeur est « juniors » ou négligent. Mais attention, il peut aussi s'agir de mails d'amis au contenu humoristique, ou encore, par exemple, de vœux de fin d'année. Il est donc

²⁴ Directeur de recherche de la Gartner, citation datant du 8 mars 2004.

essentiel de notifier dans une liste d'exceptions, si on utilise ce type d'option, les expéditeurs légitimes susceptibles d'envoyer des mails à grand nombre de destinataires.

4. 'Marks email with different SMTP "to:" et MIME "to:" fields in the email addresses as spam'. Vérifie si les SMTP « to: » et MIME « to: » sont les mêmes. Le serveur de messagerie d'un spammeurs doit forcément inclure une adresse SMTP « to: ». Cependant, l'adresse email MIME to: est souvent omise ou est différente. Cette fonction bloque beaucoup de spams, mais certains serveurs de listes n'incluent pas de MIME « to: » non plus. Donc, pour utiliser cette fonction, il faut mettre sur liste blanche les adresses des expéditeurs de newsletters si elles sont marquées comme spam par cette fonction.
5. L'email contient-il principalement des images localisées à distance ? En effet, pour éviter les filtres de mots-clés tout en faisant en sorte d'alléger leurs mails, les spammeurs envoient souvent des emails contenant des images localisées sur Internet, et pas dans la source du mail. GFI MailEssentials peut marquer comme spam les courriers présentant à la fois cette caractéristique et une quantité minimale de texte.
6. 'Verify if sender domain is valid'. Cette fonction met le point sur une autre forme de filtrage du spam souvent utilisée : la « résolution DNS ». Une vérification DNS du domaine spécifié dans le champ MIME du destinataire est réalisée, afin de savoir si ce domaine existe bien. Si le domaine n'est pas valide, c'est un indice supplémentaire pour identifier du spam.

Remarque : Cette fonction requiert que le serveur DNS soit correctement configuré. Si le serveur DNS n'est pas correctement configuré (ce serait souvent le cas), il y a un délai et le courrier sera traité lentement, en plus beaucoup d'emails valides seront marqués comme spams.

7. S'il y a plus de 3 chiffres dans le champ MIME « from », l'expéditeur est la plupart du temps un spammeur. La raison est que les spammeurs utilisent souvent des outils de création automatique de l'adresse de réponse (« reply to ») : adresses sur Hotmail et autres services de messagerie gratuite. Ils emploient fréquemment au moins trois caractères dans ce champ pour s'assurer que cette zone soit unique.
8. Une dernière vérification est possible : est-ce que l'objet de l'email correspond au début de l'adresse électronique du destinataire ? En effet, afin de personnaliser le spam, les spammeurs incluent fréquemment la première partie de l'adresse électronique du destinataire dans l'objet du spam. Ils utilisent cette particularité avec des adresses génériques telles *sales@company.com*. La vigilance est alors nécessaire : un client qui répond à une réponse automatique avec un objet tel que « votre mail à notre service commercial » serait alors qualifié de spam. Pour éviter ceci, il est possible d'indiquer une liste d'exceptions comprenant les adresses email pour lesquelles ce contrôle ne devrait pas être réalisé.
9. Voir si le message contient des adresses IP encodées - cette vérification recherche un URL avec des encodages octaux/hexadécimaux (<http://0072389472/hello.com>) ou avec une combinaison de nom d'utilisateur/mot de passe (exemple : www.citibank.com@scammer.com).

Ces tours sont souvent utilisés par les spammeurs ainsi que par les pirates informatique. Serait alors marqué comme spam : <http://12312www.microsoft.com:hello%01@123123>.

2.6.1 Détection de la langue

Il faut citer en dernier lieu, l'adaptation multi-langues d'un filtre antispam, ce qui est de plus en plus requis étant donné que le spam est de moins en moins anglophone en proportion par rapport aux quantités de spams envoyés dans le monde.

Reprenons à titre d'exemple le même logiciel (GFI MailEssentials) et, plus précisément, l'onglet 'langages' dans la boîte de dialogue de ses propriétés du contrôle d'en-tête. Celle-ci contient les options de détection de langue :

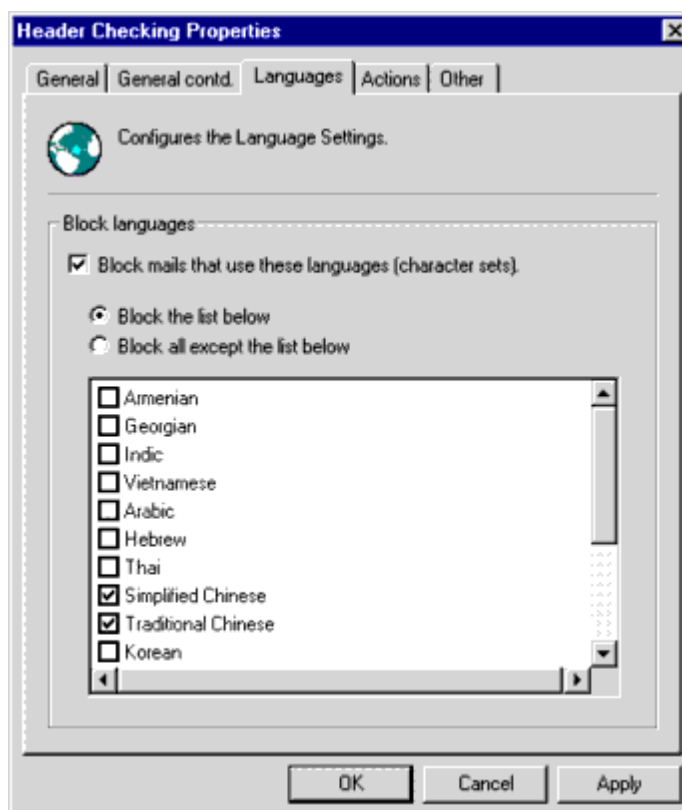


Figure 9 – Paramétrage de la langue dans GFI MailEssentials

Beaucoup de ces courriers indésirables ne sont même pas dans la langue de l'utilisateur, ce qui signifie qu'ils peuvent très simplement réduire le spam en bloquant le courrier écrit en chinois ou en vietnamien, par exemple. En fait, avec ce critère on peut bloquer le courrier selon qu'il utilise tel ou tel jeu de caractères : GFI MailEssentials, par exemple, ne peut pas distinguer l'italien du français parce que ces deux langues utilisent le même jeu de caractères... ce qui, d'un certain point de vue, constitue une limite.

3. DES APPROCHES COMPLÉMENTAIRES AUX FILTRES TRADITIONNELS

À l'image des tentatives de traque des spammeurs (qui, au demeurant, se révèlent inefficaces) il existe des moyens de lutte contre le spam complémentaires aux techniques traditionnelles de filtrage exposées précédemment dans ce rapport. Cela peut aller de simples recommandations sur les habitudes à prendre en tant qu'utilisateur, jusqu'aux méthodes récentes (brevetées ou non) de filtrage du spam.

3.1 *Confirmation de l'expéditeur (Challenge Response)*

C'est une astuce devenue relativement populaire : l'idée est d'envoyer un "challenge" à l'expéditeur du message, lequel devra y répondre. Si une réponse est reçue, l'expéditeur est ajouté à la liste blanche et ne sera plus questionné. Dans le cas contraire, les messages de cet expéditeur ne seront plus affichés dans la boîte de réception, car mis en liste noire.

Cependant, la recommandation est de ne jamais utiliser cette méthode, car, quoi qu'en disent les partisans de cette technologie ou l'impression positive qu'elle peut laisser, ce n'est pas un moyen sûr. Cette technique a des conséquences fortement indésirables ; voici une liste non exhaustive des inconvénients de la technique challenge-response :

- Elle est inamicale et impolie pour les expéditeurs légitimes ;
- Les expéditeurs légitimes peuvent, à l'occasion, utiliser une autre adresse email, qui elle n'a pas été ajoutée à la liste blanche. Elle aussi devra être confirmée, ce qui est encore plus frustrant ;
- Les expéditeurs légitimes peuvent oublier de répondre ou recevoir le message seulement quelques jours plus tard, lorsqu'ils sont en déplacement ou n'ont pas accès à leurs ordinateurs. Dans ce cas, le message original (éventuellement très important) peut être significativement retardé ;
- Si l'expéditeur et le destinataire installent tous deux un logiciel basé sur le principe de confirmation, ils pourraient obtenir une boucle sans fin de confirmations, laquelle paralyserait le système ;
- Les messages provenant de services automatiques, telles les confirmations d'enregistrement ou de transaction (utilisées par des sites comme Amazon ou e-Bay), ne parviendront jamais à atteindre la boîte de réception de l'utilisateur : les messages de ce type sont envoyés par des robots... qui ne répondent jamais aux confirmations ;
- Les souscripteurs de bulletins d'informations seront bombardés de messages de confirmation ;

- Pour les gros FAI, les nombreux messages de confirmation doubleront leur trafic et pénaliseront significativement leurs systèmes. C'est certain que ces FAI ne seraient pas très heureux de voir leurs systèmes, déjà bien lésés, doublement alourdis à cause des spammeurs.

Steve Atkins, un consultant antispam à Redwood City, Californie, affirme ce qui suit (traduit de l'anglais) : « Cette technologie est suffisamment tentante pour que les gens l'utilisent et ne réalisent pas toutes les mauvaises choses qui commenceront à se produire ». Ainsi, si l'on est très heureux de voir sa boîte de réception propre après avoir utilisé cette technique, il est très souhaitable d'examiner la liste ci-dessus afin de voir si on n'est pas affecté d'une quelconque façon par un de ces inconvénients.

Réfléchir à deux fois, donc, avant d'utiliser cette trouvaille aux effets souvent indésirables.

3.2 Se désabonner ou invalider les messages (Bounce back)

Certains produits antispam offrent la possibilité de renvoyer au spammeur les messages non désirés, spécifiant que l'adresse email est fausse ou n'existe pas, et dans l'espoir d'être retiré de sa liste de diffusion. Mais cette méthode peine à stopper le spam, car d'une part les spammeurs ne vérifient pas les emails retournés, et d'autre part cela confirme que l'adresse destinataire existe, cela peut donc empirer le phénomène. De plus, dans les cas « d'usurpation d'adresse », cela risque de polluer des innocents, puisque l'adresse de l'expéditeur peut être celle d'un ami qui, lui, n'a pas envoyé ce message. Il n'est donc pas particulièrement conseillé d'utiliser cette méthode.

3.3 Réseaux anti-spam collaboratifs

Les partisans de la technologie anti-spam collaborative affirment que les spammeurs envoient généralement le même message à des millions de personnes. Ainsi, si un utilisateur trouve un message de spam, il ou elle peut utiliser un « réseau communautaire » afin d'envoyer une "signature" du message à tous les utilisateurs ayant souscrit au même service. L'intérêt c'est que l'action d'un utilisateur empêchera les autres utilisateurs d'être dérangés par le même message.

Cette technologie fonctionne. Elle comporte cependant quelques inconvénients :

- 1) Le taux de détection des réseaux communautaires n'est pas toujours aussi élevé qu'il est sensé l'être ;
- 2) Des tests effectués par la société SpamWeed ont démontré que, d'un point de vue général, tous les produits fondés sur des "bases de données de définitions de spam mis à jour en ligne" causeront certaines gênes à l'usage. Selon eux, la vitesse de détection est lente et sujette aux erreurs réseau. Mais il faut préciser que SpamWeed est lui aussi une solution antispam. De plus, l'expérience concrète des utilisateurs dépend de la conception et de la qualité de chaque produit.

3.4 La technologie ne suffit pas : précautions de base

On ne sera pas sans rappeler l'importance de « prévenir plutôt que guérir », et ce autant que possible. Dans le domaine de la lutte antispam, certaines précautions de bases devraient être en effet le réflexe de tout utilisateur de courrier électronique. Elles sont les suivantes :

- La première des recommandations aux utilisateurs est de ne pas choisir de se désinscrire d'un spam. En effet, tout lien de désinscription dans un spam est trompeur : il sert en fait à vérifier

que l'adresse email est valide. Ainsi, celui qui se désinscrit recevra à coup sûr encore plus de spam.

- Éviter de communiquer son adresse e-mail sur un site dont on n'est pas sûr. Sinon, c'est prendre inévitablement le risque qu'elle finisse un jour dans les mains des spammeurs. Ainsi, si on est amené à communiquer son adresse électronique pour bénéficier d'un service, recevoir des bulletins d'information, effectuer un achat en ligne ou accéder à une partie à accès restreint d'un site Web, il faut à tout prix être prudent, et donner le moins possible son adresse.
- Utiliser une adresse jetable. Pour éviter toute pollution de son adresse principale, il est bon d'en avoir une qui soit annexe, ou temporaire (qui s'autodétruit ou que l'on supprime manuellement).
- Cf. paragraphe 1.2.3 « Comment récupèrent-ils nos adresses ? » page 5.

3.5 Laisser la main aux utilisateurs

Malgré une automatisation certaine du filtrage du spam rendu possible par des outils comme les filtres bayésiens, il est toutefois utile pour les administrateurs de laisser le contrôle aux utilisateurs, en leur permettant de faire savoir au système ce qu'ils considèrent, eux, comme spam. C'est en particulier lors de la phase d'apprentissage d'un filtre bayésien que cette étape est hautement recommandée. De la même façon, si un système laisse les utilisateurs ajouter eux-même leurs destinataires valides à des listes blanches, alors le risque de faux-positifs sera diminué.

3.6 SPF, un référentiel communautaire de serveurs attestés

Sous ce principe, tout serveur de messagerie est invité à se faire « certifier conforme » pour se distinguer officiellement des « robots-spammeurs ».

3.6.1 Introduction à SPF

SFP (pour *Sender Policy Framework*) est un effort communautaire qui gagne rapidement du terrain. Ce référentiel requiert que l'entreprise d'un expéditeur ait publié son serveur de messagerie dans un « enregistrement SPF ». Par exemple, si un email est envoyé à partir de `xyz@societeABC.com`, alors `societeABC.com` doit publier un enregistrement SPF pour que le référentiel SPF puisse déterminer si le message était réellement envoyé à partir du réseau `societeABC.com`, ou s'il a été forgé. Si un enregistrement SPF n'est pas publié par `societeABC.com`, le résultat SPF sera "inconnu".

Les domaines enregistrés à SPF ont la garantie que chacun de leurs courriers sortants seront obligatoirement admis par les filtres antispam des autres sociétés, à condition qu'ils utilisent un filtre tirant partie de SPF.

3.6.2 Comment SPF fonctionne-t-il ?

Les domaines utilisent des enregistrements publics (DNS) pour diriger les requêtes pour différents services (web, email, etc.) vers les machines qui offrent ces services. Tout domaine publie déjà un enregistrement email (MX) pour indiquer au monde quelles machines reçoivent les emails pour ce domaine.

La copie d'écran suivante montre un exemple d'exploitation de SPF dans un logiciel (ici, *GFI MailEssentials*). Cet exemple montre que l'on peut définir un niveau de blocage, ainsi qu'une configuration des exceptions :

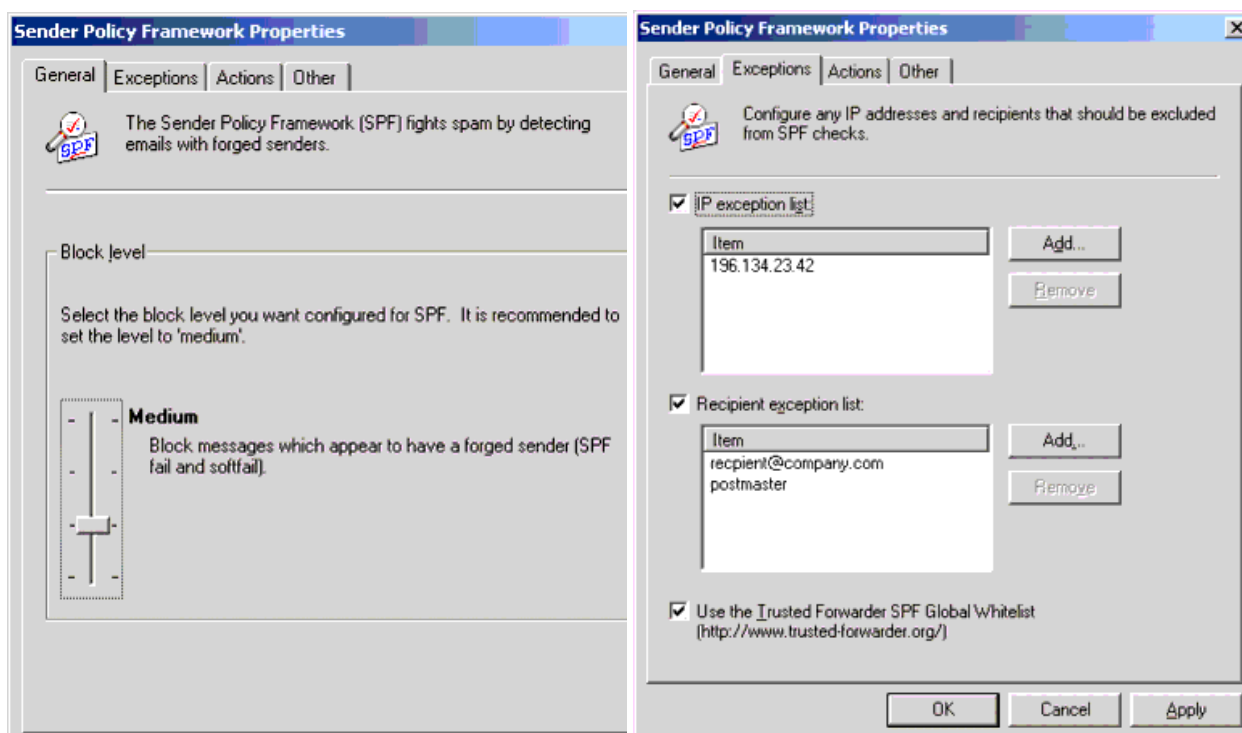


Figure 10 – Exemple de paramétrage du SPF dans GFI MailEssentials

SPF fonctionne par domaine, publiant un enregistrement texte dans le DNS de ces domaines afin d'indiquer au monde quelles machines envoient le message à partir du domaine. Quand on reçoit un message à partir d'un domaine, un logiciel exploitant SPF (comme par exemple *GFI MailEssentials*) peut vérifier ces enregistrements afin de s'assurer que les messages proviennent d'expéditeurs sûrs. Mais il n'est pas obligatoire, bien sûr, de publier un enregistrement SPF²⁵.

3.6.3 Un exemple d'utilisation de SPF

- 1) Supposons qu'un spammeur forge `societeABC.com` et essaye de nous envoyer un spam.
- 2) Il se connecte à partir d'un endroit autre que SociétéABC.
- 3) Une fois le message envoyé, on voit « FROM: <adresse_forgee@SocieteABC.com> » , mais on n'est pas obligé de le croire. On peut demander à SociétéABC si l'adresse IP provient de leur réseau.
- 4) Dans cet exemple, SociétéABC publie un enregistrement SPF. Cet enregistrement indique à GFI MailEssentials comment déterminer si la machine expéditrice est autorisée à envoyer des emails au nom de SociétéABC.
- 5) Si SociétéABC indique qu'il reconnaît la machine expéditrice, celui-ci passe, et on peut penser que l'expéditeur est effectivement celui qu'il prétend être. Si le message ne passe pas les tests SPF, alors c'est un message forgé. C'est de cette manière que vous pouvez penser qu'il s'agit vraisemblablement d'un spammeur.

Pour plus d'informations sur SPF et comment il fonctionne, le site Internet du *Sender Policy Framework* est <http://spf.pobox.com>.

²⁵ Pour publier un enregistrement SPF, utiliser l'assistant SPF sur : <http://spf.pobox.com/wizard.html>

3.7 RPD, un exemple de technologie innovatrice

Un exemple de technologie antispam innovatrice est RPD²⁶, brevet de la société Commtouch. Celle-ci se repose sur le fait que les spammeurs envoient un seul spam en masse, et sur une période relativement courte : RPD utilise un ensemble d'algorithmes sophistiqués dédiés à l'analyse du trafic Internet dans les points clés autour du monde, pour détecter les contenus répétitifs d'un mail à l'autre. Plusieurs serveurs sont ainsi positionnés en permanence dans le monde entier. Le centre de détection mondiale RPD est ainsi capable de suivre à la trace une manifestation de spam dès son commencement, et donc de stopper ce spam chez tous les clients exploitant la solution RPD.

3.7.1 Fonctionnement général du système RPD

Cette solution consiste ainsi à classer les spams du monde entier en temps réel en offrant aux clients une vitesse de détection maximale. Le schéma architectural suivant met en évidence du fonctionnement de la solution RPD.

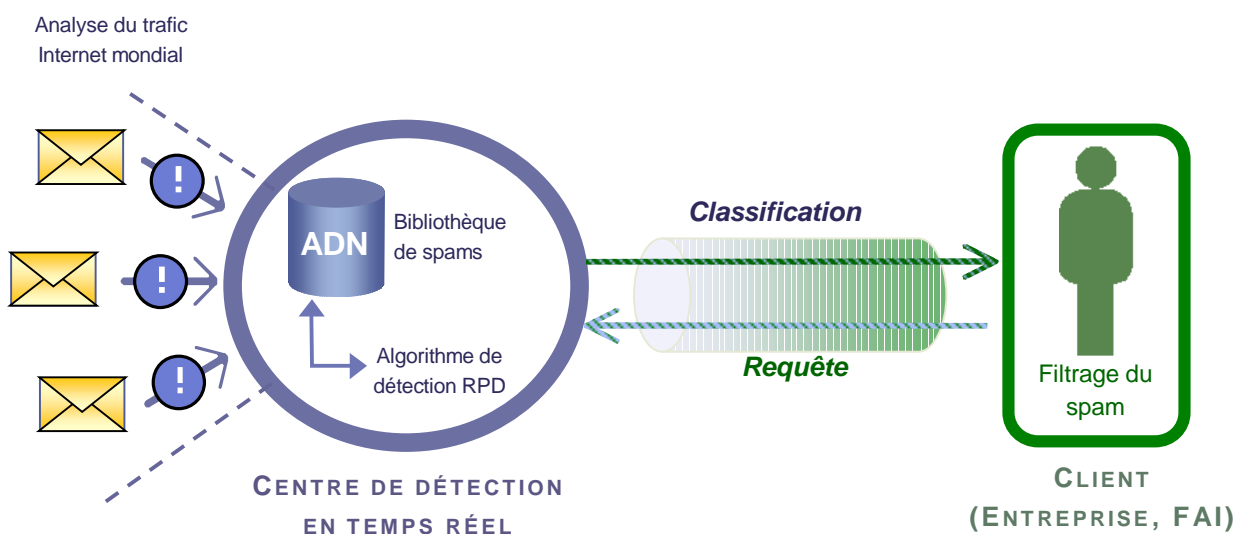


Figure 11 – Schéma de fonctionnement du système RPD

Mais comment RPD fait-t-il pour identifier les mails, afin de savoir s'il est ham ou spam ?

3.7.2 Technique de classification des spams

La classification d'un spam ne se fait pas par des méthodes traditionnelles comme les filtres bayésiens ou les mots-clés, mais par échantillonnage. De plus, une résolution DNS du nom de domaine inscrit dans l'en-tête du mail est adjointe à l'échantillonnage des emails.

²⁶ RPD pour "Recurrent Pattern Detection". En français : « Détection de modèles récurrents ».

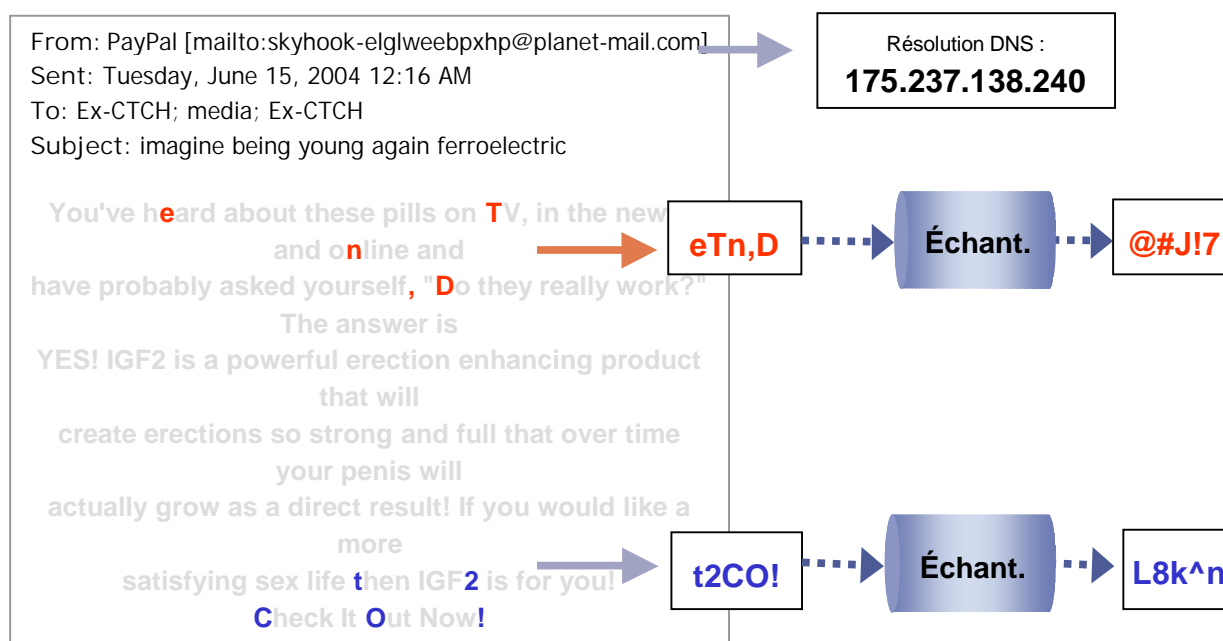


Figure 12 – Exemple d'échantillonnage d'un email par RPD

3.7.3 Les avantages du système RPD

RPD scrute les « épidémies » de spams en temps réel. Grâce à cela :

- Le système n'est plus « réactif », mais « proactif ». La caractéristique d'un système proactif est qu'il est capable d'anticiper sur les événements à venir ; dans le cas de l'antispam RPD, cela revient à bloquer la propagation d'un spam avant que celle-ci ne se développe (la majorité des produits antispam sont, au contraire, dits « réactifs ») ;
- Les spams sont bloqués très vite : en quelques minutes, la propagation d'un spam est identifiée et les clients RPD sont avertis : il leur est donné le résultat de l'échantillonnage du contenu du spam, afin qu'ils sachent quels mails ils devront bloquer par la suite.

De plus, grâce à la technique de classification RPD :

- Le système n'est pas dépendant du niveau de sophistication du spam (les diverses astuces des spammeurs pour passer outre les mailles des filtres n'ont plus d'effet) car le spam n'est plus défini selon des mots-clés ou encore une adresse email, mais selon une signature par échantillonnage de son contenu ;
- De la même manière, il n'y a plus de dépendance de la langue utilisée dans le spam ;
- Il n'y a (presque) aucun faux-positif ;
- Le système offre un taux élevé de détection du spam.

De plus :

- Comme c'est le cas avec les filtres bayésiens, il n'y a pas (ou peu) de période d'apprentissage durant laquelle les spams continuent d'arriver dans les boîtes aux lettres.

- Si un utilisateur ou un système de filtrage local considère malgré tout comme spam un message qu'il vient de recevoir, il peut le soumettre au centre de détection RPD pour aider ce dernier à enrichir sa base ;
- Selon le paramétrage client, il est possible de recevoir les spams détectés par le système centralisé (ceux-ci sont disponibles dans un dossier de quarantaine).

3.7.4 Les limites du système RPD

Le challenge est de classer un spam dans les premières minutes de sa propagation, et ainsi l'empêcher d'atteindre la plupart des messageries utilisateurs. En revanche, avant que ce spam soit identifié (soit durant ces premières minutes) un certain nombre d'exemplaires du spam en question ont déjà atteint les boîtes aux lettres. Il restera alors, pour celles-ci, l'utilisation d'un filtre traditionnel en local, comme une liste noire ou un filtre bayésien.

De plus, RPD sera inefficace contre les spams à petite échelle puisqu'il se base sur les envois massifs de courriels.

4. TENDANCES ET APPRÉCIATION DES OUTILS ANTISPAM

4.1 Les contre-attaques réciproques du spam et de l'anti-spam

On assiste à un cercle vicieux qui évolue : le camp des spammeurs et celui des produits antispam inventent chacun des procédés nouveaux pour esquiver ceux du camp adverse.

4.1.1 L'anti-antispam

Les spammeurs arrivent à déjouer les techniques antispam traditionnelles. Voici quelques uns de leurs procédés :

- **Inversement de l'ordre des lettres**

La phrase suivante serait immédiatement interceptée par un filtre heuristique ou bayésien :

– “FOR SUPER VIAGRA TOUCH HERE”

Mais celle-ci, astucieuse et loin d'être incompréhensible, aura beaucoup moins de chances de l'être :

– “FOR SUEPR VAIRGA TOCUH HERE”

- **Mutations des mots**

Si le mot « VIAGRA » a une forte probabilité d'être détecté, sans-doute le mot « V1AGRA » ne le sera pas. De la même façon, « MORTAGE » peut être muté en « M0RTAGE » (zéro à la place du 0).

Enfin, une autre astuce consiste à écrire de cette façon : « v*i*a*g*r*a ».

- « **Encre invisible** »

Lorsque l'on lit dans un mail : “M o r t g a g e” cela peut correspondre, dans le code source du mail, à : “Mxo1ryttgvaqg8e” (certaines parties du mot peuvent être en police blanche sur fond blanc).

- **Leurres pour dictionnaires anti-bayésiens**

On le sait, un dictionnaire bayésien dispose d'une base de données de « mots valides ». Ainsi, certains spammeurs garnissent leurs messages de mots susceptibles d'être reconnus valides par les filtres bayésiens, par exemple un article de la CNN, éventuellement dans une police invisible ou minuscule. Ceci, afin d'augmenter le taux de crédibilité calculé par les filtres bayésiens.

La figure suivante est un exemple de contenu de message électronique utilisant conjointement ces deux astuces.



Figure 13 – Email marketing contournant avec astuce les filtres Heuristiques et bayésiens

4.2 La tendance des procédés antispam

De même que tout mal se guérit à sa source, le niveau de positionnement des filtres antispam a tendance à se rapprocher de plus en plus de l'expéditeur, et ce, pour un fonctionnement optimal. En effet, le spam peut être bloqué avant qu'il ne parvienne à notre boîte aux lettres, c'est-à-dire au niveau du serveur proxy. Et, plus encore, il est à présent possible de le bloquer à un niveau encore plus proche de sa source grâce à certains produits comme *Caller ID*. À propos de ce dernier, le fournisseur d'accès Internet AOL affirmait récemment : "Nous saluons les efforts de Microsoft". Ce qui ne l'a cependant pas empêché de conclure : "Il y a encore des progrès à faire et beaucoup de travail à accomplir". Les produits antispam sont en continuel progrès mais ont en effet encore du chemin à parcourir. Arriveront-ils à décourager les spammeurs ? Dans l'attente, tout est permis de croire que le point de vue économique des sociétés concevant les produits antispam est tel qu'ils n'auront jamais intérêt à se débarrasser définitivement d'eux !

Les techniques traditionnelles de filtrage du spam, comme par exemple les listes noires ou les recherches par mots-clés, sont souvent connues pour être rigides. En outre, ce sont des méthodes considérées comme étant consommatrices de temps processeur. La tendance des outils antispam est de combiner les filtres statistiques (traditionnels) et des techniques avancées propres à tel ou tel éditeur. Ces nouvelles techniques peuvent être par exemple la classification centralisée des spams à base de signature (exemple : *RPD* de Commtouch). Ce peut être aussi les systèmes de certification de l'expéditeur (comme *DomainKeys*, de Yahoo) ou de l'adresse IP de son serveur SMTP (comme *BrightMail*, de Symantec). Enfin, certains fournisseurs de messagerie mettent en place des solutions annexes comme les filtres d'images d'*Hotmail* (Microsoft). Ces derniers consistent à n'afficher les images contenues dans un email que si ce dernier a été envoyé par un expéditeur connu dans le

carnet d'adresses. Cela permet notamment de protéger ses enfants des images au contenu choquant.

4.3 Les principaux critères d'appréciation d'une solution antispam

Faisons à présent un point sur les critères principaux à prendre en compte pour juger de la qualité d'une solution de filtrage du spam. Les points suivants sont considérés comme étant des qualités requises pour un produit antispam de bonne qualité.

4.3.1 Le piège des faux-positifs

On rappellera qu'une solution antispam qui en apparence est efficace et satisfaisante, peut en réalité cacher un dysfonctionnement grave : bloquer régulièrement de vrai message (les faux-positifs). Il va alors de soi que plus l'outil antispam est susceptible de bloquer par erreur des messages légitimes, plus s'impose la nécessité d'un accès régulier aux mails mis en quarantaine. Il est en l'occurrence indispensable que cet accès soit tout simplement possible, ce qui n'est pas toujours le cas, en particulier avec des solutions filtrant les emails au niveau d'un proxy²⁷.

4.3.2 Souplesse

Éviter les techniques rigides comme les listes noires ou filtres par mots-clés. Au contraire, une liste blanche par exemple peut être gérée d'une manière automatique et intelligente, par analyse du contenu des messages que l'utilisateur reçoit.

4.3.3 Capacité d'auto apprentissage

Un outil idéal est intelligent, donc ne s'arrête jamais d'apprendre. Si cet outil n'a pas réussi à bloquer un pourriel, ou s'il a malencontreusement bloqué un message légitime, il est de coutume de pouvoir déplacer le message vers la bonne boîte. *SpamWeed* se souviendra de son erreur et son jugement s'en trouvera amélioré. Par conséquent, plus vous utilisez *SpamWeed*, plus il devient performant.

4.3.4 Personnalisation

Chaque personne possède une vision différente de sa messagerie. Il suffit d'imaginer par exemple qu'une entreprise peut avoir comme activité principale de revendre des produits comme le Viagra. Il va alors de soi que dans la messagerie de cette entreprise, les mails contenant le mot 'Viagra' ne devront pas être interprétés comme ailleurs. Pour reprendre l'exemple du logiciel *SpamWeed*, ce dernier respecte complètement ces différences propres aux personnes et aux entreprises et, après avoir "appris" les habitudes personnelles de chaque utilisateur, il suit leurs logiques, et classifiera ainsi les spams en fonction de chacun, selon le contenu des mails qu'ils reçoivent et qu'ils considèrent comme valides.

4.3.5 Protection contre les virus

Il est désormais courant qu'un logiciel de protection soit à la fois une barrière contre le spam et contre les virus. En effet, une solution « deux-en-un », comme par exemple le produit *ProtecMail*,

²⁷ Se référer au paragraphe « Le positionnement du filtre : deux types d'approche », page 9.

peut faire gagner du temps, être moins chère que deux logiciels distincts, ou tout simplement faciliter la vie.

4.3.6 Contrôle parental

De nombreux messages de spam contiennent des images répugnantes qui peuvent être dangereuses ou indécentes pour vos enfants. *SpamWeed* fournit un contrôle parental unique en son genre, qui vous permet d'écartier de vos enfants les messages dangereux.

4.3.7 Qualité de l'interface

Pour utiliser certains produits anti-spam, il faut être un expert (maintenance, utilisation de chaînes d'expressions régulières...). Or, le spam concernant le grand public, il est évident que tous les produits antispam ne doivent pas être accessibles seulement aux experts.

On recherchera en général le confort et la facilité d'utilisation. Le plus important restera sans doute la rapidité de manipulation, étant donné que qu'un produit antispam doit faire gagner plus de temps qu'il en fait perdre. Ainsi, les utilisateurs ne doivent pas passer trop de temps à manipuler le filtre pour obtenir des résultats de filtrage satisfaisants.

4.3.8 Matériel requis

Certains produits antispam ont l'inconvénient de devoir être installé sur une machine dédiée. Par exemple, on ne peut pas installer le produit *Trend Micro* sur le serveur de messagerie. Ces limitations ne conviennent pas toujours à tout le monde.

4.3.9 Gestion des langues

C'est plutôt un critère d'avenir : un logiciel comme par exemple *BrightMail 6.0* (Symantec) gère 11 langues différentes. En effet, tout produit qui utilise des filtres statistiques doit s'adapter à une progression de plus en plus rapide des spams écrits dans un langage autre que l'anglais. Environ 10% à 15% du spam mondial n'est pas en anglais.

CONCLUSION

Comme c'est déjà le cas avec les virus informatiques, les lois contre le spam ne règlent rien : la proportion de courrier indésirable dans nos boîtes aux lettres est en progression continue. C'est pourquoi des solutions antispam sont plus que jamais nécessaires pour protéger à la fois les ressources réseaux et la tranquillité de chacun. La conception et le choix d'une solution antispam sont cependant plus litigieux que pour un antivirus car, à la différence des virus, tout le monde n'a pas systématiquement la même définition de ce qu'est un message indésirable.

Un même piège est récurrent, quelque soit les filtres utilisés : un produit antispam qui fonctionne bien peut aussi fonctionner « trop bien ». En d'autres termes, le risque de faux positifs n'étant pas négligeable pour certains produits, il est important que les utilisateurs de messageries aient accès aux messages mis en quarantaine par leur solution antispam. Et pourtant, l'idéal serait que l'utilisateur ne se rende même pas compte qu'un filtre anti-spam existe : cela lui faciliterait la vie, et éviterait aussi qu'il configure mal son filtre (car un paramétrage trop agressif augmente classiquement le nombre de faux-positifs).

Les techniques évoluent, car les procédés traditionnels de filtrage du spam (comme les listes noires ou les recherches par mots-clés) s'avèrent très rigides à l'utilisation. Même les filtres bayésiens (de type statistique), les plus efficaces des procédés classiques, deviendront de plus en plus inefficaces contre les nouvelles techniques « anti-antispam ». En effet, les courriers indésirables comportent de plus en plus d'images ou de vocabulaire dit « anti-heuristique » (à base de mots valides ou transformés). De plus, les spams sont de moins en moins anglophones, ce qui révèle la faiblesse de nombreux filtres, pauvres en gestion multi-langues. De plus, les filtres bayésiens ne sont pas toujours bien utilisés, par exemple lorsque leurs bases de données de mots sont uniquement mises à jours à partir de serveurs centralisés (ce qui n'est pas approprié à leur nature, qui consiste à s'adapter).

En définitive, les tendances des procédés antispam sont diverses. Il faut dire que chacun y va de ses trouvailles à caractère propriétaire, sans compter que ces nouveaux procédés sont rarement autonomes, puisque souvent polyvalents : la majorité des produits antispam utilisent conjointement plusieurs techniques de filtrage traditionnel, le tout étant parfois associé à des méthodes brevetées inventées par l'éditeur. La pensée commune est que, dans un système utilisant plusieurs filtres, les avantages des uns compensent les inconvénients des autres. D'une part, de grands comptes lancent depuis peu de nouvelles techniques de filtrage par authentification de l'expéditeur (selon son domaine ou encore son IP). Par exemple, le produit *Symantec BrightMail 6.0* implémente l'idée de référencer les adresses IP autorisées ou interdites. D'autre part, il faut noter qu'une autre tendance, plus générale, est d'utilisation des filtres polyvalents, de plus en plus multi-langues, mariés à des techniques nouvelles. En outre, on parle de plus en plus de techniques dites « proactives », dans le sens où elles s'évertuent à stopper les messages indésirables avant qu'ils ne parviennent aux boîtes aux lettres. On peut enfin se demander si des logiciels d'OCR (reconnaissance de caractères) seront dans l'avenir intégrés à des solutions antispam, car les spams sont de plus en plus constitués d'images.

Autre réflexion : utiliser une base de données centralisée, partagée entre des utilisateurs du monde entier, peut représenter un avantage comme un inconvénient : tout dépend du type d'information que l'on veut centraliser. En effet, si l'on met à jour un dictionnaire pour filtre bayésien à partir d'une base unique en ligne, alors ce filtre perdra de son intérêt pour deux raisons. D'une part, les filtres

bayésiens, qui sont en l'occurrence parmi les plus performants, sont faits pour s'adapter à un contexte professionnel ou amical particulier : ils doivent correspondre à un usage attentif et personnel, et pas une base de mots interdits ou autorisés qui soit universelle. D'autre part, les spammeurs connaissent les dictionnaires bayésiens mis à disposition de tous, et trouvent donc les manières détournées pour duper ces filtres. Par contre, l'utilisation d'informations centralisées peut représenter un réel avantage lorsque ce sont les spams eux-même, et pas leurs caractéristiques, qui sont spécifiquement référencés en temps réel dans une base de données partagée : de cette manière, il est possible de stopper très vite la propagation d'un pollupostage. On trouve aussi, dans cette même catégorie de solutions, ce que l'on appelle l'effort communautaire, dont l'archétype est SPF : un système libre et centralisé permettant la certification des domaines de messagerie.

Au sujet des systèmes de centralisation ou de certification, nombreux sont les éditeurs à prétendre que leur produit fonctionnera de manière optimale lorsque tout le monde l'aura adopté. Il faut donc dire ce qui est : de ce point de vue, la concurrence qui oppose les éditeurs de solution antispam ne constitue pas que des avantages. N'est-ce donc pas l'idée de « solution universelle » qui puisse apporter le plus d'espérance en terme d'efficacité ? On y est plus ou moins rendu avec des exemples de solutions communautaires comme SPF : reste à généraliser ce type de solution aux domaines et entreprises du monde entier. En attendant, les éditeurs privés de solutions antispam ont encore de beaux jours devant eux : ces derniers, en 2004, ont généré des revenus de 979 millions de dollars²⁸.

Par ailleurs, il est bon de préciser que la mise en application de certaines techniques antispam risquent de poser un problème de respect de la vie privée. Ce peut être lorsqu'une équipe de spécialistes s'interpose entre Internet et les utilisateurs pour validation manuelle des classifications de spams.

En dernier lieu, il est intéressant de noter qu'un nouveau type de pollupostage est en train de faire son apparition : les spams commencent à arriver peu à peu sous forme de SMS sur nos téléphones portables. Sous cette forme, le coût d'envoi est inévitablement plus élevé pour les spammeurs. Ce qui est d'autant plus inquiétant, car pour eux, le jeu en vaut quand même la chandelle... Les systèmes d'exploitation de nos téléphones portables seront-ils donc, dans l'avenir, pourvus d'options de filtrage antispam ?

²⁸ Selon le *Radicali Group*. (Selon une estimation réalisée par cette même société, les éditeurs de solutions antispam généreront en 2008 un profit de 1 740 millions de dollars.)

ANNEXE A — GLOSSAIRE

Address Spoofing (ou IP spoofing) : Usurpation d'adresse. Consiste à se faire passer pour quelqu'un d'autre, en utilisant son adresse sur le réseau. On peut ainsi faire croire que la connexion ou le message reçu provient d'un compte d'utilisateur autorisé.

Antispam : De nature à combattre le spam. Peuvent être dits « antispam » des solutions, logiciels, filtres...

bayésien : Nature d'un filtre antispam dont le fonctionnement est issu de la théorie de la décision (1763).

Blacklist : Cf. « Liste noire ».

Courriel : Courrier électronique (en anglais : « email »).

Domaine (Nom de domaine) : Qui se connecte à Internet fait partie d'un domaine, dont le nom est unique au monde (ex : yahoo.fr).

FAI : fournisseur d'accès à Internet.

Faux-positif : Il s'agit, dans notre domaine²⁹, du courrier considéré à tort comme du spam.

Firewall : Aussi appelé pare-feu, un firewall est un dispositif (matériel et/ou logiciel) situé entre le réseau d'une organisation et l'Internet. Son but est d'empêcher les intrusions.

GFI MailEssentials : Solution antispam incluant les modules complémentaires suivants : des listes noires et/ou blanches, un filtre bayésien, un système de vérification par mot clé et une analyse d'en-tête.

Ham : Courriel non indésirable (par opposition au spam).

Internet : Réseau de portée mondiale interconnectant des centaines de réseaux spécifiques et auquel sont reliés quelques dizaines de millions d'utilisateurs individuels et professionnels.

IP (Internet protocol) : Définition du format des messages véhiculant sur le réseau Internet.

Liste blanche : Liste d'adresses email, domaines ou URL étant les seuls à être autorisés.

Liste de diffusion : Permet de faire parvenir aux personnes intéressées des courriels fréquents sur les sujets de leur choix (encore appelée « Mailing list » ou « liste de publipostage »).

²⁹ Ce terme est également employé dans d'autres domaines, comme celui de la médecine.

Liste noire : Liste d'adresses email, domaines ou URL interdits.

MIME : Système de codage qui permet d'envoyer plus que des caractères simples et sans accents (i.e. ASCII). MIME permet par exemple l'envoi de fichiers joints.

MTA (Mail Transfert Agent) : Logiciel serveur de mail, responsable du transport du courrier, comme Postfix, Sendmail³⁰ ou Microsoft Exchange. Un utilisateur n'est jamais en contact avec un tel serveur, mais utilise un autre programme appelé MUA (« mail user agent ») – ou encore « client email » – qui se charge de contacter le MTA pour envoyer le message.

MUA (Mail User Agent) : Logiciel utilisé pour composer, lire, envoyer et recevoir du courrier. Exemples : Outlook Express, Kmail, Eudora.

ORDB : La liste ORDB est une base de données accessible mise à jour par ORDB.org. ORDB.org est une organisation à but non lucratif, qui stocke les adresses IP des relais SMTP ouverts vérifiés. Ces relais sont probablement employés pour l'envoi en masse de courriels non sollicités, aussi connu sous le nom de spam. L'accès à cette liste permet aux administrateurs système d'accepter ou de refuser le courrier des serveurs en provenance de ces adresses.

Phishing : Récupération de données confidentielles par usurpation d'identité. Contraction de phreaking (lui-même contraction de "phone" et "freak") et fishing. Le phishing tente d'amener un Internaute à dévoiler des données sensibles (comme son code de carte de crédit par exemple) en lui envoyant un email déguisé pour ressembler à celui d'une banque et en le redirigeant ensuite vers un site également déguisé.

Pollupostage : Envoi de spam.

POP (Post Office Protocol) : Protocole permettant de récupérer des messages électroniques stockés sur un serveur de messagerie. De nombreux fournisseurs d'accès mettent à disposition auprès de leurs abonnés un serveur de messagerie de type POP.

Protocole : Un protocole correspond aux normes établies entre deux entités (logicielles ou matérielles) pour la communication d'informations ou de commandes.

Proxy : Unique machine d'un réseau local connectée à l'internet et effectuant les requêtes internet pour les autres ordinateurs du réseau, comme demander une page web. Un proxy peut aussi jouer le rôle de pare-feu pour bloquer les accès ou sorties non autorisés.

RFC (Request for Comments) : Ensemble de documents faisant référence auprès de la Communauté Internet : ils décrivent, spécifient, aident à l'implémentation, standardisent et débattent de la majorité des normes, standards, technologies et protocoles liés à Internet et aux réseaux en général.

³⁰ Sendmail est un logiciel libre (comme Postfix), et représente **50% du trafic mondial** : <http://www.sendmail.org/>

Serveur : Ressource informatique capable de délivrer une information ou d'effectuer un traitement à la requête d'autres équipements installés en réseau.

SMTP (Simple Mail Transfer Protocol) : Protocole permettant l'envoi de courrier électronique entre différents serveurs sur le réseau Internet. Lorsqu'un internaute envoie un courrier électronique à un destinataire, le serveur de messagerie de son fournisseur d'accès joue avec d'autres serveurs SMTP le rôle de relais jusqu'au destinataire.

Spam : Courriel abusif et indésirable, généralement à caractère commercial, envoyé à une masse de destinataires non avertis.

TCP/IP (Transmission Control Protocol/Internet Protocol) : C'est l'ensemble des protocoles qui définissent les échanges sur l'Internet.

URL : Une URL (Uniform Resource Locator) correspond à l'adresse d'une page web sur le réseau.

Web (World Wide Web – WWW) : Le web est une interface multimédia fondée sur le principe de l'hypertexte. Développé en 1992 par le CERN, le web est devenu l'interface standard de consultation sur internet. Pour se connecter à un serveur web, il faut posséder un navigateur, c'est-à-dire un logiciel permettant d'interpréter les pages HTML (les plus répandus sont Internet Explorer et Mozilla Firefox).

Web (site) : Ensemble de pages liées entre elles par des liens hypertextes, consultables à distance. Ces pages sont hébergées sur un ordinateur, appelé serveur (relié à internet).

Whitelist : Cf. « Liste blanche ».

ANNEXE B — TABLE DES FIGURES

Figure 1 – Évolution de la quantité quotidienne de spam en Amérique du nord et dans le monde entier	8
Figure 2 – Les deux types d'architecture classiques pour l'intégration d'une solution antispam	9
Figure 3 – Architecture d'un système de messagerie exploitant un serveur antispam en interne	10
Figure 4 – Architecture d'un système de messagerie exploitant un service de filtrage en ligne	11
Figure 5 – Configuration d'une liste blanche dans le logiciel GFI MailEssentials	13
Figure 6 – Création d'une base de données de mots pour le filtre bayésien	15
Figure 7 – Paramétrage des mises à jour d'un filtre bayésien dans GFI MailEssentials	16
Figure 8 – Configuration du contrôle d'en-tête dans GFI MailEssentials	17
Figure 9 – Paramétrage de la langue dans GFI MailEssentials	19
Figure 10 – Exemple de paramétrage du SPF dans GFI MailEssentials	23
Figure 11 – Schéma de fonctionnement du système RPD	24
Figure 12 – Exemple d'échantillonnage d'un email par RPD	25
Figure 13 – Email marketing contournant avec astuce les filtres Heuristiques et bayésiens	28

ANNEXE C — NETOGRAPHIE

Les références internet suivantes ont servi de base de connaissance et de réflexion pour ce rapport.

Quelques articles et sites informatifs :

<http://www.arobase.org/spam/>

Rubrique sur *Arobase.org* (site de généralités et d'actualités sur l'email) concernant le spam.

<http://www.idc.com>

Groupe de conseil et d'étude sur les marchés des technologies de l'information.

<http://www.paulgraham.com/spam.html>

"Un plan pour le spam" : article en anglais de Paul Graham (gourou du filtrage bayésien).

<http://caspam.org/>

CASPAM : collectif antispam. Conseils, actualité, outils antispam, forum...

Quelques produits antispam :

<http://www.symantec.com/region/can/fr/product/brightmail/>

Brightmail Antispam (Symantec) : protection antispam multi-couches. Ce produit exploite plus de 17 technologies de filtrage différentes.

<http://www.commtouch.com/>

Technologie *RPD* : solution innovatrice de filtrage du spam par classification en temps réel.

<http://www.gfi.com/mes/>

GFI MailEssentials, solution antispam à base de filtre bayésien.

<http://fr.spamweed.com>

SpamWeed : Solution antispam utilisant à la fois des techniques avancées et traditionnelles.

<http://www.protecmail.com/fr/>

ProtecMail : Une des nombreuses solutions combinant antispam et antivirus. Celle-ci a la particularité d'offrir deux modes d'antispam : en ligne, ou en local.

<http://perso.wanadoo.fr/dbecaert/sk.htm>

Sk.pl : un outil antispam libre de droit (pour les programmeurs) sous forme de script Perl.³¹

<http://www.qurb.com/fr/help/tour/>

Qurb, logiciel antispam que l'on peut installer comme module additionnel dans le MUA Outlook ou Outlook Express. Qurb gère des listes blanches d'une manière automatique.

³¹ Ce script est l'amélioration d'un premier script écrit par un certain Chris Bagwell, mais auquel a été ajoutée l'automatisation de la destruction du spam. Le script initial *poppy.pl* permettait de consulter sa boîte aux lettres et de détruire les mails indésirables directement sur le serveur du FAI. L'inconvénient de *Sk.pl* est qu'il ne gère pas de mise en quarantaine.