Halte au Spam

Contributions - Réflexions

Paris, le 18 novembre 2004

Blacklists anti-Spam : plus de la moitié des entreprises indexées

Seconde partie : Une étude du filtrage sur liste

Par Frédéric Aoun et Bruno Rasle, co-auteurs du livre « Halte au Spam* » (éditions Eyrolles)

Cette contribution a été présentée lors de la conférence-débat « *Listes noires, listes blanches : efficacité et utilisation* » qui s'est déroulée à Paris le 18 novembre 2004.

Très tôt, la gêne provoquée par le Spam pousse des responsables de messagerie à réagir. Bloquer la réception des messages en provenance de certaines adresses email sources, noms de domaine et adresses IP est leur priorité. Dès lors, le filtrage sur liste noire va rapidement s'imposer.

Ce document a pour objectif d'analyser les apports de cette démarche, mais aussi ses défauts et ses limites, comme les pistes d'amélioration. Il comprend deux parties.

Nous dévoilons dans la première partie les enseignements d'une campagne de mesures que nous avons effectuée sur un panel de grandes entreprises et d'administrations françaises. www.halte-au-spam.com/Blacklists_Resultats.pdf

Cette seconde partie répond aux questions les plus fréquentes, telles que : Qui gère les blacklists ? Comment se retrouve-t-on blacklisté ? Quelle est l'efficacité réelle de ce type de filtrage ? Plusieurs experts et administrateurs de messagerie ont bien voulu enrichir notre étude de leur témoignage. Qu'ils en soient ici remerciés.

Une interview inédite de Steve Linford, le créateur de Spamhaus, éclaire de nombreux points soulevés par notre étude.

Vous y trouverez également en fin de document une synthèse et des conseils si vous souhaitez vous protéger grâce aux listes noires ou si vous vous retrouvez blacklisté.

De quoi parle-t-on ? Dès 1996, la gêne provoquée par le Spam pousse certains responsables de messagerie à réagir. Leur premier instinct est de filtrer la réception des messages en provenance de certaines adresses e-mail sources, noms de domaine et adresses IP. Par « filtrer », on peut entendre « bloquer », « mettre en quarantaine », « laisser passer après avoir étiqueté le message » ou enfin « détruire ».

Il convient à ce propos de ne pas faire la confusion entre la liste et l'usage qui en est fait. Une entreprise pourra décider de marquer les messages suspects, une autre de stopper tout type de trafic, HTTP, FTP, etc., issu d'adresses IP blacklistées, et pas uniquement le flux SMTP. Il n'est donc pas surprenant de relever la mention suivante sur les sites web des listes noires : « Nous ne sommes pas responsables du blocage de vos emails ! ». De même, il convient de ne pas nommer « blacklisting » toutes les actions appliquées par les FAI : ceux-ci utilisent également d'autres techniques, comme le refus des échanges SMTP trop lents ou le décompte du taux d'adresses erronées.

En parallèle, les entreprises gèrent également au niveau local des listes noires et des listes blanches. Ces dernières sont utilisées par exemple pour les relations avec les clients et leurs partenaires. Généralement les messages issus de ces émetteurs ne subissent qu'une vérification allégée, voire aucun contrôle.

Quel en est le principe ? Généralement, un site Internet publie une liste d'adresses IP, d'adresses emails, de domaines, dans un format facilement interrogeable. Il suffit alors aux administrateurs de messagerie de configurer leurs serveurs de façon à interroger cette source d'informations et prendre une décision quant aux messages provenant des sources listées. Comme illustrée par la figure 1, cette consultation s'effectue dans la majorité des cas via une requête DNS†. Si la réponse indique une source répertoriée comme émettrice de spams, le serveur n'a plus qu'à filtrer le courriel. La plupart des MTA‡ supportent ce type de fonctionnement.

Cette étude traite plus particulièrement des listes noires publiques, externes. Rien ne s'oppose à ce qu'une autre technique de filtrage et d'analyse ne soit appliquée par la suite aux messages acceptés, par exemple sur leur contenu ou sur leur enveloppe.

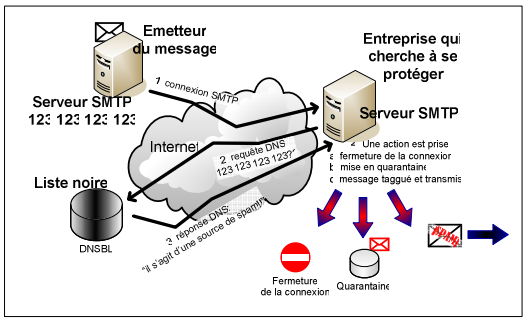

Fig. 1 - Interrogation d'une liste noire publique

Paul Vixie, animateur du service MAPS[1] (*Mail Abuse Prevention System*) a créé en 1997 la liste RBL◊. Son objectif ne se limitait pas au filtrage du spam, mais s'étendait à la sensibilisation des prestataires techniques à cette problématique, et notamment au cas des relais ouverts. ORBS (*Open Relay Behavior modification System*), administrée par le Néo Zélandais Alan Brown, a suivi de peu. Spamhaus a été lancé en 1998 par Steve Linford. En France, l'une des premières listes noires à voir le jour est celle d'Yves Roumazeilles, animateur du site SpamAnti[2].

L'émetteur est-il averti que son message a été rejeté ? Pas toujours. Si une notification de rejet est renvoyée, elle peut être de deux types[3]. La série 4XX signale une erreur temporaire. Dans ce cas, l'émetteur stocke le message et procède à des réémissions. Pour les FAI, et compte tenu des volumes traités, l'impact est loin d'être négligeable. A l'issue de ce processus, l'émetteur est enfin informé de l'échec de son envoi. Les notifications de la série 5XX correspondent à des échecs définitifs. Dans ce cas, l'émetteur est rapidement informé. Chaque FAI définit sa politique en matière de file d'attente, de tentatives de réémission et de durée totale du processus. Lors de nos entretiens avec ces prestataires techniques, il nous a été confirmé que les périodes de blacklisting étaient très pénalisantes pour leurs infrastructures.

On peut également se demander si le fait d'adresser une réponse aux spammeurs ne les aide finalement pas. Certains développeurs de filtres vont jusqu'à préconiser le renvoi d'un « *User unknown* » en espérant que les spammeurs retirent des adresses valides de leurs fichiers. Cette pratique n'a pas forcément bonne presse auprès des internautes, et elle est notamment regrettée par les professionnels du marke-

**www.halte-au-spam.com*

†Domain Name Server (ou System) : Service essentiel d'Internet assurant la conversion des noms de domaines en adresses IP et vice versa.
‡Mail Transport Agent : logiciel de messagerie pour le relayage des emails sur Internet.
◊Marque déposée, propriété de MAPS LLC

ting direct, qui, non seulement voient leurs statistiques de campagne polluées et leurs messages éliminés[4], mais également fondre leurs fichiers.

Concernant la non livraison des messages publicitaires légitimes, peu de chiffres ont circulé. Une étude publiée en mars 2004[5] et menée aux Etats-Unis faisait état d'une moyenne de 18,7% des envois (la note de synthèse indique que « *dans la plupart des cas, ces emails opt-in* ont été assimilés à tort à des spams par les ISP* »). Cette moyenne cachait une grande disparité. Si Earthlink ne bloquait que 7% de ces envois, Netzero en a éliminé sur la même période 37,7%.

Plusieurs types de blacklists ? On peut faire une première distinction entre les blacklists « locales » (par exemple au niveau d'une société ou même d'un internaute), dénommées *Local Deny Lists*, et les blacklists publiques (du type Spamcop ou Spamhaus, par exemple), interrogées à distance. L'utilisation des listes noires locales nécessite maintenance et expertise. Malheureusement, les outils de messagerie standards ne facilitent en rien leur administration : pas de retrait automatique des entrées sur inactivité ni de mise en liste temporaire pour une période plus ou moins longue.

Certaines implémentations des listes publiques autorisent le chargement des listes publiques au niveau local, pour éviter de pénaliser les temps de réponse. Il est possible à un même utilisateur de combiner l'utilisation de ces deux types de listes. Il est possible également d'intégrer ces filtres sur les routeurs d'accès et les *firewall* via des *Access Control List* (ACL). La gestion des blacklists locales est le fait de l'administrateur de messagerie de l'entreprise (donc, une tâche supplémentaire, manuelle le plus souvent), les listes publiques étant gérées par des organismes ad hoc.

Ces listes publiques sont connues sous le nom de DNSBL (*DNS Blackhole List*), ou tout simplement *blacklist*. Certaines sont gratuites, tandis que d'autres sont proposées sous forme de service payant.

Quelques unes de ces listes noires se sont spécialisées selon les critères qui déterminent l'entrée dans la liste, ou selon leur type de fonctionnement. Bien que la majorité d'entre elles restent focalisées sur les sources supposées d'émission de spam, on trouve aussi des listes dédiées aux relais ouverts† ou basées sur le strict respect des standards. Les plus connues Spamcop[6], MAPS[7], DSBL, SPEWS[8] ou ORDB[9] .

Selon une étude publiée en juillet 2004[10], plus du tiers des entreprises américaines ont recours aux listes noires publiques, tandis que 37% d'entre elles gèrent une liste noire interne (ce qui n'est pas incompatible). La liste MAPS, payante, est utilisée par 17% d'entre elles. Viennent ensuite la liste de relais ouverts ORDB (13%), SPEWS (10%), Spamcop (8%) et Spamhaus (6%). Si le pourcentage de sociétés ayant recours aux listes noires était similaire (38%), les chiffres de popularité de ces listes sont fort éloignés de ceux présentés dans l'étude publiée par Clearswift en mars 2004[11], menée auprès de 1260 professionnels de l'informatique (dont 92 français). MAPS n'est créditée que de 5,7% des réponses, contre 9,2% à Spamcop et ORDB, et 5,2% à Spamhaus.

A proprement parler, ces listes comprennent des informations de niveau réseau ou de l'enveloppe, telles des adresses e-mail source, des noms de domaine et des adresses IP. Si cette dernière méthode semble plus efficace (l'adresse IP ne peut être maquillée), elle est plus difficile à gérer qu'une liste de domaines. Ainsi, la liste administrée par Yves Roumazeilles (SpamAnti) est de ce dernier type. Mais les spammeurs n'hésitent pas à utiliser des domaines réputés pour être souvent placés en liste blanche par les internautes (donc ne subissant aucun filtrage). Yves Roumazeilles avoue ainsi avoir vu fondre l'efficacité de sa liste au fil des années, de 90 à 12%.

Récemment sont apparues des listes comprenant des URL. Elles sont d'un type très différent, en ce sens qu'il ne s'agit pas de blacklists au niveau « réseau », mais d'une chasse au « *call to action* »‡. Jose Marcio Martins Da Cruz, développeur du filtre j-chkmail[12], a récemment enrichi son outil de cette fonctionnalité, en interrogeant la liste SURBL. Cette liste comprend les URL indiqués dans le contenu des spams. Sur leur site Web, une analogie est établie avec un extrait d'un célèbre discours du révérend Martin Luther King : *« I have a dream that my four children will one day live in a nation where they will not be judged by the color of their skin but by the content of their character* ». SURBL[13] indique ainsi juger les spams sur leur contenu plutôt que sur leur origine.

On peut également les distinguer suivant leurs objectifs, les critères d'entrée dans la liste et la procédure de sortie de la liste. Dans notre campagne de mesures dont les résultats sont présentés dans la première partie de cette étude (www.halte-au-spam.com/Blacklists_Resultats.pdf), nous avons veillé à ce que les différents types de listes soient représentés dans notre panel.

Quels sont les avantages de recourir à une liste noire ? Le filtrage sur émetteur évite que le Spam arrive sur les serveurs. Il en découle des économies de bande passante, de stockage et de CPU. De plus, si l'on interroge une base locale, le recours à cette technique est peu consommatrice en ressources, donc rapide. A distance toutefois, les requêtes DNS peuvent prendre plus de temps. Mais ces bénéfices ne sont pas toujours au rendez-vous. Ainsi Postfix émet un code rejet uniquement après le RCPT (donc après avoir engagé le dialogue avec l'émetteur) et ne coupe même pas la connexion dans la foulée.

La facilité d'emploi et le fait que l'usage du filtrage sur liste noire est proposé sur presque toutes les plateformes sont des atouts supplémentaires. Enfin, nul besoin d'analyser le contenu du message (sauf pour les listes d'URL embarquées), ce qui évite tout problème avec la loi qui assimile les emails à des correspondances privées. C'est pour ces différentes raisons que le filtrage sur liste a été – et est encore – très utilisé par les prestataires techniques (FAI◊ ou prestataires de messagerie). Très souvent, ces derniers détruisent simplement les messages provenant de sources mises à l'index[14].

Quelle a été la réaction des spammeurs ? Les spammeurs se sont très vite adaptés à ces filtres, ont appris à contrefaire les données de l'enveloppe des pourriels et à diffuser leurs envois à partir de serveurs innocents, réquisitionnés pour la circonstance à l'insu de leur administrateur. La rapidité avec laquelle les listes noires réagissent est donc primordiale.

Jean-Claude Ayel est responsable Qualité et Méthodes chez Xpedite France. Cette société spécialisée dans le marketing direct fournit aux entreprises des solutions de diffusion de messages électroniques par fax, email, SMS et voix. Membre du Groupe Ptek Holdings (NASDAQ : PTEK), cette société emploie 1 100 salariés au niveau mondial.

Halte au Spam : « Les listes noires vous gênent-elles lors de vos diffusions d'emailings légitimes ? »

Jean-Claude Ayel : « Même si la situation est moins tendue qu'il y a deux ans, nous rencontrons encore ce problème. Nous sommes principalement confrontés aux listes noires basées sur la délation ou sur signalisation de la part des internautes. Pour réduire le taux de plaintes nous avons mis en place une charte anti-spam que nous expliquons à tous nos clients annonceurs. Nous pouvons, à notre seule discrétion, refuser d'exécuter un projet de diffusion si celui-ci risque d'être assimilé à du Spam. »

Halte au Spam : « Avec quels résultats ? »

Jean-Claude Ayel : « Si en février 2004, nous relevions un taux de plaintes de 0,16%, nous sommes tombés à 0,03% en septembre de la même année. Nos efforts en faveur de la qualité des fichiers opt-in et du respect des règles de transparence portent donc leurs fruits. »

**Attention. Nous rappelons qu'il n'existe pas de clair consensus sur la définition de l'opt-in…*
†Un relais ouvert est un serveur SMTP qui permet l'envoi d'un message lorsque ni l'émetteur ni le destinataire ne sont des utilisateurs locaux.
‡Call to action : litt.: « inciter à agir ». Les spams comprennent souvent une URL (ou un numéro de téléphone) et invitent l'internaute à visiter un site Web.
◊FAI : Fournisseur d'accès Internet , ISP(Internet Service Provider)

Halte au Spam : « Pour quelles raisons la situation vous semble-t-elle moins tendue qu'il y a deux ans ? »

Jean-Claude Ayel : « À l'époque les listes noires constituaient quasiment la seule protection contre le spam, alors que plusieurs systèmes de filtrage sont aujourd'hui disponibles. De plus, il est probable que les entités qui gèrent ces listent soient plus attentives qu'elles ne l'étaient auparavant. »

Halte au Spam : « Qui vous blackliste ? »

Jean-Claude Ayel : « A part les listes noires américaines, nous notons encore des « coupures » effectuées par les FAI français, sans doute dues à des filtres qui réagissent uniquement sur les volumes… Nous déplorons le manque de dialogue et de contact entre notre profession et ces prestataires techniques. A quand une procédure unifiée pour prévenir plutôt que guérir ? »

Les spammeurs aguerris sont-ils gênés par ces dispositifs ? On peut imaginer que les spammeurs débutants ou maladroits voient leurs envois bloqués par les listes noires. Mais il est avéré que ces dispositifs gênent certains professionnels du marketing direct.

Pour quelles raisons se retrouve-t-on « blacklisté » ? La bonne et unique raison devrait être « émettre du spam ».

Malheureusement, c'est loin d'être le cas. Un émetteur légitime peut se voir blacklisté même sans jamais avoir émis de spams. Nous avons essayé de recenser les différents cas de figure :

- Le protocole SMTP permettant aux spammeurs toute manipulation des champs « *From* » ou « *Reply to* », les spams semblent provenir d'une source innocente (usurpation du nom de domaine par exemple). Les récepteurs des spams, en toute bonne foi, dénoncent cette source auprès des listes noires de leur choix. Heureusement, les listes sérieuses se basent sur des informations plus fiables.
- Le serveur de la source innocente « cohabite » (chez un même prestataire, sur un même serveur, dans un même bloc d'adresses…) avec une source accusée (à tort ou pas) de spamming, elle-même blacklistée (voir figure 2). A titre d'exemple, la liste blackholes.five-ten-sg annonçait mettre à l'index une classe B dans son intégralité si une seule des adresses IP de cette classe était coupable de spamming ! A la page 102 de notre livre, nous avons relaté notre propre expérience.

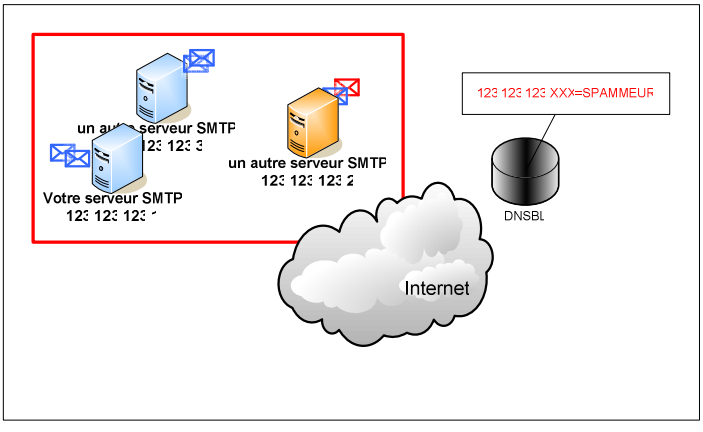

Fig. 2 - Mise à l'index d'un bloc entier d'adresses, une sorte de « punition collective ».

- Votre prestataire technique héberge des pages qui font la promotion de *spamware** (ce qui n'est pas illégal en France). La liste noire DNSPromo[15] blackliste sur ce critère.
- Votre prestataire ne fourni aucun moyen de signaler des abus (service « abuse »). C'était le critère retenu par la liste DeadBeef.
- Un concurrent, ou un ancien collaborateur mécontent, vous dénonce en tant que spammeur. Le système des listes de blocage s'appuie en grande partie sur une certaine forme de délation. Il n'est donc pas impossible qu'une entité soit montrée du doigt à des fins peu honorables. Ainsi, sur le site Spamcop, on peut lire l'avertissement suivant : « Notre système est basé sur les dénonciations des internautes… [ ] Les utilisateurs peuvent accidentellement ou malicieusement dénoncer d'autres messages [que du spam] ». De même, la liste DSBLALL[16] ajoute « *Note that it will likely contain some popular free mail services and the like, if their users maliciously submit entries* ». Le journal israélien Maariv s'est livré en juin 2004 à une expérience intéressante[17]. Un compte Hotmail a été ouvert, sans être utilisé. A partir d'un second compte, une signalisation de spam à été déposée, indiquant le nouveau compte comme étant l'initiateur des pourriels. Un exemplaire « bidonné » de spam était joint à la plainte, construit à partir des éléments d'un spam récupéré quelques jours auparavant, enrichi des références du nouveau compte. Moins de 24 heures plus tard, ce dernier était fermé. Bien qu'il ne s'agisse pas à proprement parler d'une mise en blacklist, la démarche est similaire. L'étude Clearswift indique une très faible participation des entreprises à ces systèmes basés sur la délation (seuls 13,9% des professionnels de l'informatique disent contribuer aux listes noires publiques). La majeure partie des entrées est le fait d'internautes grand public.
- Votre service informatique interne ne gère pas le DNS de façon parfaite… La liste *rfc-ignorant*[18] met à l'index les domaines qui présentent des *MX records* erronés (pointage vers de mauvaises adresses IP, *hostnames* sans *A records*, ou encore MX pointant vers une adresse IP plutôt que vers un *hostname*). Stéphane Bortzmeyer, de l'AFNIC[19], fait remarquer que « nombre de ces exigences sont au delà des standards ». Ainsi un ISP majeur exige la présence du champ PTR[20] pour accepter les messages. Monsieur Bortzmeyer y est franchement opposé, car de nombreux émetteurs n'ont aucune action possible sur ce critère. Il évoque même des pays africains qui n'ont pas ce pouvoir. On peut donc se retrouver blacklisté sur un critère sur lequel on n'a aucune maîtrise ! Dernièrement, un grand FAI français n'a pu tenir cette vérification qu'une journée, après avoir bloqué plusieurs millions de messages, dont une partie émanait de Laposte.net.
- Votre Whois[21] est mal renseigné. Là encore, Stéphane Bortzmeyer trouve la mesure disproportionnée, surtout quand on sait que nombre d'administrateurs hésitent à renseigner les bases ICANN qui ne disposent d'aucune protection, et se voient donc utilisées par les spammeurs. Une grande entreprise française, leader mondial dans son domaine, est mise à l'index pour cette raison (se reporter à la première partie de cette étude www.halte-au-spam.com/Blacklists_Resultats.pdf).
- Votre domaine n'accepte pas de recevoir des courriers électroniques sur une adresse de type postmaster@. (liste *NoPostMaster*[22])
- Votre site Web propose un système de formulaire de type FormMail†, qui génère l'envoi d'emails. La liste SORBS (Spam and Open Relay Blocking System) indique avoir étendu sa liste récemment aux domaines exploitant ce type de formulaire.
- Vous avez eu la « mauvaise idée » de tester votre serveur pour savoir s'il était en relais ouvert… La liste spamsources.yamta.org signale les « spammeurs » qui testent ainsi les serveurs, à la recherche d'*open-relay*[23].
- Vous avez eu la « mauvaise idée » d'ouvrir un bureau en Corée du Sud. La liste korea.services.net bloque tout simplement tous les FAI de ce pays !

Nous n'avons par contre pas réussi à vérifier deux autres raisons : On nous a reporté que des entreprises se voyaient listées car leur raison sociale coïncidait avec des termes régulièrement utilisés dans les pourriels, ou sur les sites et forums utilisés par les spammeurs. Nous avons également entendu dire qu'une liste référençait les émetteurs disant du mal d'elle !

**Spamware : outil utilisé par les spammeurs permettant la collecte d'adresses électroniques et l'envoi en nombre d'emails.*

†FormMail est un script très populaire qui permet d'envoyer par mèl des formulaires recueillis sur des pages web. Il est malheureusement vulnérable à de nombreuses attaques qui peuvent permettre à un spammeur de le détourner à son gré.

Mais vous pouvez malheureusement avoir émis réellement des spams, à votre insu :

- car l'un de vos serveurs est un relais ouvert. AOL indique clairement refuser tout message provenant de serveurs ainsi configurés[24] : « […] tout le courrier provenant de votre serveur sera bloqué jusqu'à ce que vous désactiviez le relais ouvert et nous informiez que nous pouvons à nouveau tester votre adresse IP ». Il est vrai que, comme le dit Alan Hodgson, un développeur de Vancouver à l'origine du mouvement ORBS, « *There's no excuse these days apart from technical incompetence for allowing an open mail relay* »[25]. Malheureusement, notre campagne de mesures (www.halte-au-spam.com/Blacklists_Resultats.pdf) montre que de nombreuses grandes entreprises et administrations françaises sont dans ce cas.
- car vous « offrez » aux spammeurs un proxy (par exemple *opm.blitzed.org*, qui liste les *open proxies* HTTP*). Nous avions relaté dans notre livre (page 153) la mésaventure d'un administrateur polonais qui avait émis à son insu plus de 50 Mo de spams† en quelques jours avant de se voir bloqué par Spamcop.
- car les spammeurs profitent de vos *mailbox* avec « réponse automatique » (voir figure 3).

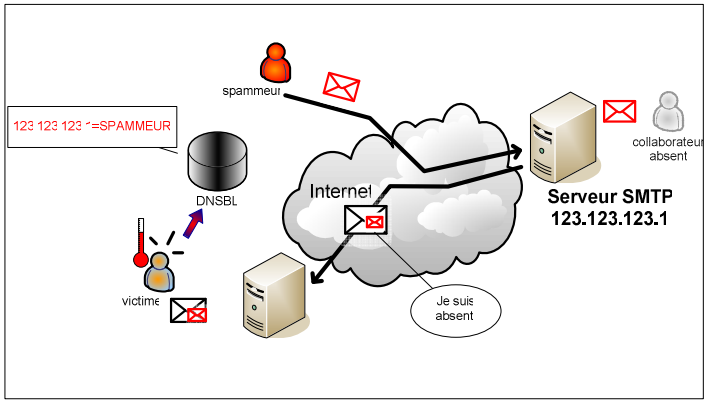

Fig. 3 - Utilisation, par les spammeurs, de la fonction « réponse automatique en cas d'absence ». L'entreprise qui emploie le collaborateur en congés peut se voir accusée de spamming par la victime.

- après avoir « rebondi » sur votre serveur de messagerie (similaire au cas précédent, mais utilise la notification de non livraison, ou NDR).
- car vous avez été victime d'un « *Wifi wardriver* ». En octobre 2004 un californien a été arrêté pour s'être livré à du « wardriving » à la recherche de *hot spot WiFi* non protégés[26]. Il les exploitait pour diffuser des spams invitant à visiter des sites pornographiques.
- car un email émis de votre entité était destiné à un *honeypot*‡. En complément (ou en pondération) des « dénonciations » reçues de la part des internautes, des entités comme Spamcop utilisent cette technique.
- car, par exemple, l'un de vos collaborateurs est membre d'un groupe de musiciens amateurs, et a annoncé son prochain concert en diffusant des courriels depuis son poste de travail. L'un des destinataires, trouvant le message intrusif et non respectueux des pratiques en vigueur, a dénoncé votre domaine auprès d'une liste noire. Dans la même catégorie, on peut inclure les collaborateurs qui effectuent, depuis leur lieu de travail, des opérations d'*email bombing*◊.

Selon la qualité des blacklists, une vérification est menée. Mais dans la plupart des cas, comme il est clairement indiqué sur les pages Web de ces organisations, l'émetteur mis à l'index est considéré comme coupable, jusqu'à ce qu'il ait prouvé son innocence.

Existe-t-il des utilisations « déviantes » des listes noires ? En effet. Au niveau des listes noires locales (sur le poste même de chaque internaute, ou au niveau d'une entreprise) une habitude s'est répandue qui consiste à blacklister un émetteur dont on ne souhaite plus recevoir de message, au lieu de se désabonner d'une Newsletter ou de signaler à un annonceur légitime que l'on ne souhaite plus recevoir ses messages publicitaires… Nous sommes donc dans ce cas en dehors de la stricte protection contre le spam.

Comment savoir si je suis blacklisté ? Vous pouvez vérifier vous-même si les adresses exploitées par votre entreprise sont mises à l'index en consultant les sites Web de chaque blacklist. Des sites[27] consolident en temps réel plusieurs listes, mais ne conservent aucun historique. Vous serez sans doute surpris de l'identité des entreprises montrées du doigt.

La majorité des listes noires informent les entités qu'elles viennent de mettre à l'index par un email adressé à postmaster@ « entité mise à l'index ». Malheureusement, nous rencontrons fréquemment des entreprises qui n'ont pas créé ce type d'adresse et/ou qui ne l'administrent pas correctement. Dans l'une de nos récentes missions de conseil, la liste noire n'acceptait que des messages émanant d'une adresse de ce type pour se faire désindexer. Chez l'un des plus grands FAI français, cette adresse est configurée de façon à détruire tous les messages reçus, car elle est cible d'attaques continuelles. Pour ce prestataire technique, l'adresse opérationnelle et déclarée au RIPE** est en « *abuse* ».

Peut-on ne pas s'apercevoir que l'on est blacklisté ? Oui. Ou plus précisément, il peut se passer un certain temps avant de s'en apercevoir (cf. le cas d'une grande banque, blacklistée pendant plusieurs mois lors de notre campagne de mesure). Vos correspondants ne vont peut-être pas vous signaler immédiatement qu'ils ne reçoivent plus vos courriers électroniques. Il est donc recommandé de surveiller son éventuelle mise à l'index, surtout quand on sait qu'on peut être blacklisté sur une liste B car on est blacklisté sur une liste A… La liste B ne faisant qu'agréger d'autres listes sans aucune vérification. Il est alors urgent de sortir de la première liste, avant de se voir fiché dans d'autres listes.

Qui sont les entreprises blacklistées ? L'étude de Clearswift[28] a révélé que 84% des entreprises ayant répondu au questionnaire (dont 92 en France) avaient été mis à l'index au moins une fois, pour une raison légitime ou abusive. L'étude présentée dans la première partie de ce document (www.halte-au-spam.com/Blacklists_Resultats.pdf), qui porte sur les grandes entreprises et administrations françaises, semble le confirmer. Une étude publiée en octobre 2002 par Assurance Systems[29] indiquait que 100% des entreprises américaines de marketing spécialisées dans la diffusion d'emails publicitaires avaient été un jour ou l'autre blacklistées.

Et rien n'empêche de figurer dans une liste noire que l'on utilise pour se protéger du spam. Si cette mise à l'index n'est pas justifiée, l'équipe d'exploitation peut se poser quelques questions quant à l'efficacité de cette liste… Un grand FAI français nous a confié que c'était l'une des raisons pour lesquelles il n'avait pas recours aux blacklists publiques.

Françoise R. a la charge de l'administration du serveur de messagerie d'une entreprise d'une quinzaine de personnes. Elle a bien voulu nous confier sa réaction après que son entité ait été mise à l'index par Spamcop, dsbl.org et dnsbl.net.au (voir figure 4).

Françoise R. : « J'ai eu l'impression de me déplacer en aveugle, à tâtons et de ne pas comprendre ni ce qu'on me reprochait, ni ce que je devais mettre en oeuvre pour obtenir l'absolution. De plus, j'ai constaté un manque d'information de la part de nos contacts techniques : sans même leur parler de liste noire ou de liste blanche, ils ne connaissaient pas, dans la plupart des cas, le nom du responsable informatique (ou ne savaient pas comment le joindre). Ils ne savent pas dire quelle procédure anti-spam est mise en oeuvre. Ne serait-il pas nécessaire de mettre en place un système - de type « les listes noires pour les nuls » - pour les milliers de PME qui se trouvent confrontées aux problèmes que j'ai rencontrés ?

Je recevais en outre des informations contradictoires : d'une part on me demandait de ne pas autoriser le SMTP AUTH, alors que la documen-

**Cette technique présente le grand intérêt pour les spammeurs de ne pas laisser de traces dans les en-têtes SMTP.*
†Soit environ 10 millions de messages.
‡Honeypot (pot de miel ou spamtrap) : piège utilisé par les opposants au spam pour mesurer, analyser ou combattre le phénomène. Mis en œuvre, entre autres, par Spamcop ou Brightmail. Ces sociétés gardent précieusement secrètes les adresses de ces boîtes aux lettres piégées.
◊L'email bombing consiste à adresser (ou faire adresser) un volume très important de courriels pour saturer une boite aux lettres et/ou un serveur de messagerie.
***Le RIPE est l'un des RIR (Regional Internet Registry) qui affectent les ressources d'Internet, telles les adresses IP.*

tation de l'éditeur de mon serveur de messagerie indiquait qu'il fallait absolument cocher la case en question. J'ai fini par me résoudre à aller à l'encontre des instructions de l'éditeur, décision qui s'est avérée bonne.

Notre préjudice ? Une semaine de stress et quelques très mauvaises journées à tourner et retourner le problème dans tous les sens... Après coup, je me suis félicitée d'avoir conservé un abonnement de secours, pour les collaborateurs qui doivent rester en contact permanent avec nos adhérents.

J'ai eu un mal fou à expliquer en interne pourquoi je considérais que le problème était grave et devait être résolu dans les meilleurs délais. Si je n'ai reçu qu'un soutien bien faible, on défilait toutefois dans mon bureau pour me demander si tout était rentré dans l'ordre !

Avoir recours aux listes noires pour se protéger du spam ? Internet n'est pas parfait. Je conçois donc que les responsables des systèmes d'information s'appuient sur des listes noires imparfaites, mais faciles à mettre en œuvre, demandant peu de maintenance et globalement satisfaisantes.

Mais aujourd'hui, je me fais encore l'effet d'une convalescente et me surprends à vérifier régulièrement que nous n'apparaissons pas dans des listes noires… ».

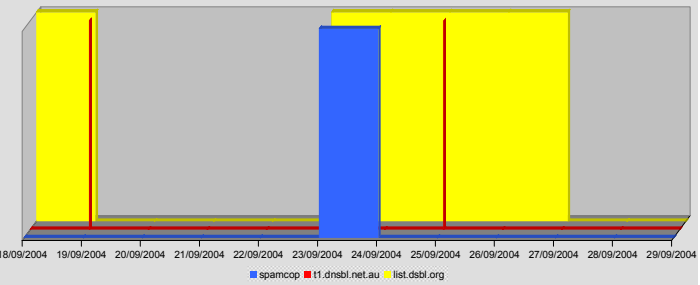

Fig. 4 - Chronogramme des mises en liste d'une entreprise de quinze personnes. On visualise parfaitement sur ce graphe le « recouvrement » entre plusieurs listes noires. Suite à une erreur de configuration, le serveur de messagerie de cette entité s'est retrouvé en open-relay. A partir de ce critère unique, il est intéressant de noter les différences de réaction entre Spamcop (qui ne listera l'entité que pendant la journée du 23 septembre), DSBL (qui listera par deux fois, et sur des périodes plus longues) et DNSBL (qui a indexé – et désindexé – l'entité de façon fugitive à deux reprises). Les autres listes de notre panel sont restées sans réaction (se reporter à la première partie de notre étude quant à la méthodologie utilisée).

Qui gère ces blacklist ? Les bases mutualisées sont maintenues par des groupements d'internautes et par des FAI. Longtemps, les internautes ont été livrés à eux-mêmes face au Spam. Il n'est donc pas surprenant de constater des réactions extrêmes, allant jusqu'à la chasse aux sorcières, avec appel à la délation, sans réel contrôle des institutions. Ce syndrome est particulièrement flagrant aux Etats-Unis, où se sont créées des organisations qui luttent contre le Spam par des moyens radicaux, notamment la gestion des listes noires. Ces shérifs autoproclamés ne redoutent pas les dégâts collatéraux. Dans une interview accordée en octobre 2001, l'un des responsables de MAPS déclarait : « *On liste d'abord et on discute après*… ». Heureusement, comme nous l'avons constaté dans notre étude, il existe des listes gérées de façon professionnelle et responsable.

Mais quel est leur financement ? La plupart sont bénévoles, comme Spamhaus, créée par Steve Linford. Cette équipe bénéficie également de soutien technique de la part de sponsors*. Certains proposent l'accès à leur liste moyennant finance†, à l'instar de MAPS qui a été créé en 1996 en tant qu'entité à but non lucratif et qui s'est transformé en société courant 2000. A titre indicatif, l'abonnement annuel à ses listes RBL (Realtime Blackhole List), RSS (relais ouverts), OPS (proxys ouverts) et DUL (Dynamic User List – qui compte plus de 17 millions d'adresses) coûte plus de 3.000 dollars pour 4.000 utilisateurs. La liste t1.dnsbl.net.au, qui fait partie du panel de notre campagne de mesures, demande 1.800 dollars autraliens par an pour 10.000 requêtes quotidiennes. D'après son gestionnaire, cette somme équilibre les frais de structure.

D'autres se font racheter, comme Spamcop, dont IronPort a fait l'acquisition en novembre 2003, pour un montant non dévoilé. Durant l'été 2004, MAPS a été racheté par Kelkea, dont le CEO, Dave Rand, en était également le fondateur. La majorité enfin tire des ressources de publicités ciblées. L'une d'entre elles propose fort obligeamment, pour un dollar par mois et par domaine, de souscrire à un service qui protège « des blacklists malicieuses » !

Pourquoi se cachent-ils ? Durant l'été 2003, une vague d'attaques en déni de service ont frappé plusieurs sites gérant des listes noires, ce qui a causé l'arrêt de l'une d'entre elles, gérée par Osirusoft[30]. Steve Linford, animateur de Spamhaus, a indiqué avoir reçu des menaces de mort dans une interview qu'il a accordée à la télévision suisse romande en juin 2004[31]. De plus, son site a été la cible d'attaques, notamment en juillet 2003 par SoBig.E et Fizzer. Mais il est vrai qu'il publie la base Rokso[32] (*Register of Known Spams Operations*), qui comprend beaucoup d'informations sur les spammeurs (agissements, adresses postales, patrimoine, plaintes en cours…).

Existe-t-il des listes noires françaises ? Will Spam For Food[33] est un service créé par Pierre Beyssac, Thomas Quinot et Samuel Tardieu. Il se focalise sur les relais et proxys ouverts (SMTP, HTTP et SOCKS). Les adresses IP proviennent de pots de miel et d'un accord avec Spamcop. Le 22 octobre 2004, cette liste recensait par exemple 6.728 machines permettant le relayage, les plus nombreux étant les proxys SOCKS.

Yves Roumazeilles laisse à disposition sur son site[34] une liste de domaines et d'adresses qui comporte environ 4.000 entrées. Sont clairement indiquées les entrées et sorties récentes. Cette liste est constituée à partir des pourriels reçus par son administrateur, des courriers envoyés aux postmasters de ces domaines restés sans réponse ou qui indiquaient un compte e-mail inexistant, ou encore qui indiquaient une politique clairement favorable au spam.

François Bonneville est PDG d'Aricia[35], FAI situé dans l'est de la France. Pour protéger son infrastructure, et ses clients, il a mis en place une première règle : le domaine de l'adresse de l'expéditeur doit exister (rejet d'environ 8 % du courrier). Il y a ajouté les listes noires Spamcop et Ordb (rejet d'environ 14% du courrier), ainsi que ses propres listes noires et blanches, gérées manuellement et enrichies grâce à des pots de miel. Un millier de domaines (majoritairement en .ru) et 400.000 adresses sont ainsi bloquées, ce qui permet d'arrêter environ 10% supplémentaires. Une entrée est automatiquement supprimée après trois mois d'inactivité. Au total, Aricia rejette ainsi environ 32% du courrier entrant avec cette batterie d'outils.
« Lorsque nous blacklistons un serveur, cela est effectué au niveau du *firewall*, donc aucune signalisation n'est faite à l'expéditeur : mon serveur est injoignable pour ce serveur de spam. Dans les autres cas, conformément au RFC 821, le serveur de messagerie renvoie un message d'erreur 550 ou 451 avec quatre types de commentaires : « *We don't accept junk mail from your domain* », « *We don't accept junk mail from your address* », « *unresolvable host name, check your configuration* » ou « *your server is on the xxxx Blocking List* » précise Monsieur Bonneville. Mais certains serveurs -notamment chinois- sont blacklistés alors qu'ils envoient également du courrier intéressant pour certains clients d'Aricia. Aricia a dédié un serveur qui n'a pas recours au filtrage sur liste, pour ceux-ci.

Comment sortir d'une blacklist ? En combien de temps ? Faut-il « payer » ? La première difficulté est de détecter cette situation désagréable, ce qui n'est pas toujours évident. Ensuite il faut identifier la

**On note, par exemple, la présence d'une bannière avec le logo Cisco sur le site de SORBS.*
†Certaines invitent les grandes entreprises qui traitent plusieurs centaines de milliers de messages par jour à télécharger sa base, contre rémunération, en arguant de leur incapacité à supporter une telle charge.

liste noire en question, puis comprendre de quoi on est accusé et s'imprégner de la démarche à suivre pour sortir de la liste. L'étape suivante de ce véritable chemin de croix est d'obtenir un contact avec l'entité qui gère cette liste… En effet, ceux-ci ne communiquent que par l'intermédiaire de leur portail et souvent en anglais. On note des effets de bord assez inattendus. En juin 2003, un internaute britannique avait découvert que BT était mis à l'index par DSBL. En conséquence, il était dans l'incapacité de signaler les pourriels auprès de spamabuse.org, qui utilise justement cette blacklist ![36]

Quand vous aurez réussi à établir le contact, reste à prouver votre bonne foi (si vous avez été blacklisté abusivement) ou à boire la lie jusqu'à la coupe : reconnaître que votre équipe informatique ne respecte pas les RFC, ne gère pas correctement le DNS, ou que vos serveurs de messagerie sont en relais ouvert… Devrez-vous aller jusqu'à proposer de l'argent pour faciliter votre sortie de la liste noire ? Certaines sources nous l'ont affirmé, sans que nous puissions en avoir confirmation. Seule la liste Sorbs indique sur son site exiger une « donation » de 50 dollars, pour sortir de sa liste « Spam ». Cette dernière est gérée manuellement, sur fait avéré et répété de spamming. Au fur et à mesure des envois de pourriels, Sorbs blackliste le bloc entier d'adresses… jusqu'à ce que « quelque chose soit fait ». Les adresses sont ensuite délistées progressivement, à l'exception de l'adresse coupable de la diffusion, qui ne peut être sortie de la liste que moyennant un don de 50 dollars à une « organisation caritative ou à une bonne cause ».

L'étude Clearswift de mars 2004, a révélé que dans 62% des cas il fallait plus d'une journée pour sortir de ces listes. Pour 21% des répondants aux questionnaires, il leur a fallu plus de cinq jours. A cela, il faut ajouter un certain temps de latence, pendant lequel l'entreprise n'a pas conscience de sa mise à l'index. Notre expérience de terrain nous incite à confirmer ces chiffres.

Dans le cas de listes se contentant de « s'inspirer » d'autres listes, la procédure de désinscription doit être accélérée pour éviter un effet domino (pendant que vous réussissez à vous désinscrire d'une liste, deux autres vous intègrent). Notre campagne de mesures (www.halte-au-spam.com/Blacklists_Resultats.pdf) le confirme.

Provoquent-elles des effets de bord ? Oui. Elles provoquent de multiples « dégâts collatéraux ». La mise à l'index d'émetteurs légitimes (sociétés, internautes, voir pays entiers, comme la Chine ou la Corée) les gêne dans leurs émissions de messages. Cet isolement de domaines entiers est à l'exact opposé à l'esprit même d'Internet (le « réseau des réseaux »). L'*Anti-Spam Coordination Team of Internet Society of China* publie ainsi une liste de 626 adresses IP de serveurs accusés d'émettre du spam[37]. Parmi les 493 adresses situées hors de Chine, une dizaine basées en France, dont des serveurs de l'opérateur « historique ». Les entreprises listées avaient jusqu'au 20 mars 2004 pour mettre « fin à leurs agissements ».

Outside China Feb.18, 2004	Total: 493	
Mail servers located in France		
212.155.248.XXX	213.36.80.XX	213.56.116.XX
213.56.195.XX	213.56.31.XX	213.56.31.XX
213.56.31.XX	213.56.31.XX	212.155.248.XXX

Tableau 1- Extrait du document posté par l'Anti-Spam Coordination Team of Internet Society of China. Il recense des serveurs français accusés d'émettre du spam.

Si vous êtes utilisateur de listes noires, si le Spam présumé n'arrive plus sur votre serveur, il est possible également que des e-mails en provenance d'émetteurs légitimes ne vous parviennent pas non plus. Le rejet pur et simple des messages suspects est la configuration la plus répandue. A titre d'exemple, le fait qu'une administration française figure dans une liste noire américaine vous importe sûrement peu – et même si elle a émis du spam-, surtout si vous attendez d'elle un message important (voir la figure 5). Nous avons mis en évidence une situation de ce type lors de notre campagne de mesures.

Il est cependant possible d'accepter ces messages en les étiquetant « Spam » ou encore en les plaçant en quarantaine. A l'inverse, si votre société se trouve mise à l'index, vous n'avez non seulement aucune assurance que vos messages atteignent leurs destinataires, mais cette mise à l'index est préjudiciable pour votre image de marque. La confirmation penaude du porte-parole de BT courant 2003, après la parution d'articles de presse relatant la mise à l'index de cet opérateur en est un parfait exemple[38] : « *Nous confirmons que nous avons été blacklistés par la liste DSBL, qui percevait la configuration de nos serveurs de messagerie comme incorrecte* ».

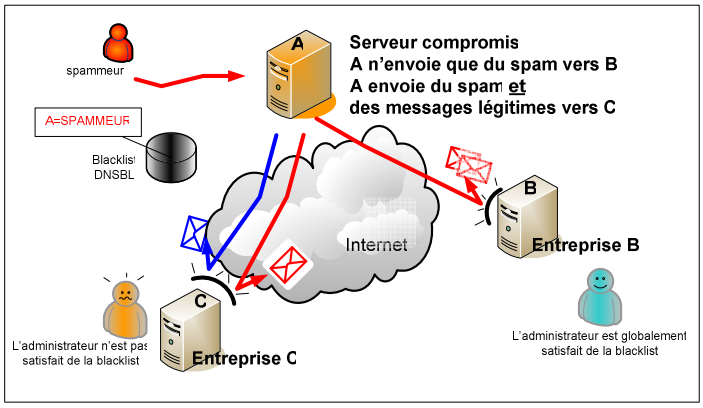

Fig. 5 - Un serveur (A) indexé comme source de spam peut être également une source de messages légitimes pour le récepteur C. Lors de notre campagne de mesures nous avons recensé la mise à l'index d'un grand ministère français. Pour des entités étrangères, il est fort probable que le blocage de ses messages n'engendre pas de faux positifs. Cependant, une entité française faisant appel à la blacklist en question serait sûrement gênée par le rejet de messages légitimes.

Les organismes qui gèrent des blacklist sont-ils visés par des actions en justice ? Oui. Nous donnerons comme exemple typique la condamnation de MAPS en novembre 2000 par un tribunal de Denver pour avoir blacklisté la société 24/7 Exactis. Un représentant de la liste noire MAPS a déclaré que la société 24/7 Exactis avait émis quatre milliards d'email en 2000, et qu'elle était citée dans une douzaine de « plaintes » de la part d'internautes pendant cette même période. Le juge John Kane a qualifié la décision de MAPS « d'irresponsable », en soulignant également qu'elle privait les consommateurs d'informations qu'ils attendaient. Plusieurs plaintes ont également été déposées contre IronPort, suite au rachat de Spamcop. En juillet 2001, l'une des plus anciennes listes noires, ORBS, a été contrainte au sabordage suite à des actions devant la justice Néo Zélandaise de la part d'entreprises s'estimant mises à l'index à tort.

On notera sur ce même sujet, la discrétion des FAI, qui évitent soigneusement d'utiliser le terme même de blacklist.

Sont-elles efficaces ? Du point de vue des FAI, il est certain que cette technique allège considérablement leurs infrastructures. Mais il est difficile d'obtenir des chiffres concordants sur l'efficacité réelle de cette technique du point de vue des destinataires. Les résultats sont étroitement liés aux listes utilisées, à leur mode d'implémentation et à l'utilisation qui est faite de l'information délivrée par la liste. Une étude utilisée en septembre 2002 par *Electronic Frontier Foundation* et *Computer Professionnals for Social Responsability* annonçait pour la liste MAPS RBL un taux de filtrage de 24% pour un taux de faux positif de 34% !

Et nous souscrivons à l'opinion de Paul Graham[39], à l'origine du renouveau des filtres Bayésiens, qui écrit « *A blacklist is only as good as the people running it* ».

Pour éviter cet écueil, il peut être préférable de n'utiliser l'information délivrée par une liste que comme l'un des critères pris en compte par un filtre faisant appel à plusieurs techniques (à pondérer suivant la confiance que l'on place dans la liste ou selon ses critères) et non pas pour prendre une décision binaire (rejet ou acceptation).

Certains administrateurs de messagerie refusent le recours à des listes publiques, préférant conserver le plein contrôle de leur exploitation : « *You're passing control to some other entity, and if you're not in control of your own mail servers then it's a problem for your own business* » déclare ainsi Darren Worley, responsable d'un FAI australien[40].

Sont-elles encore utiles ? Oui, certaines d'entre-elles aident à l'éducation des utilisateurs et « forcent » les administrateurs à suivre des règles de base (gestion saine des DNS, des configurations de serveurs, chasse aux relais ouverts…). Pour les autres… On peut se demander si Internet pourrait « survivre » aujourd'hui sans les blacklists ? Il est aujourd'hui difficile de savoir si les autres modes de protection contre le spam ont pris le relais, notamment au niveau des FAI. A l'énoncé du volume d'emails filtrés par les listes noires majeures, on peut en douter.

Mais ont-elles été efficaces par le passé ? Si pour plusieurs d'entre elles l'apport est aujourd'hui incertain, les listes noires ont constituées ces dernières années l'un des seuls remparts contre le spam et ont permis à l'infrastructure d'Internet de résister, dans l'attente de mesures plus efficaces. Nous leur voyons au moins trois apports indéniables. Premièrement, elle sont assimilables à un véritable dispositif « d'alarme » pour les administrateurs réseaux… De plus, elles créent une sorte de « barrière à l'entrée » pour les spammeurs débutants. Une partie d'entre eux vont être « dégoûtés », les autres seront contraints à l'excellence. La figure 6 illustre cette dichotomie. Enfin, les listes allègent la charge du réseau et des autres dispositifs de filtrage (on peut dire la même chose des solutions d'authentification qui émergent).

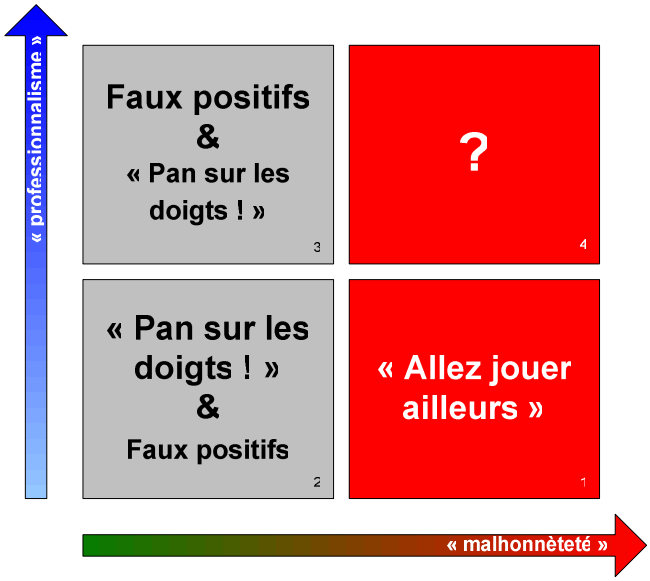

Fig. 6 - Impact supposé des listes noires, en fonction des populations concernées. Pour les spammeurs « débutants » (1) l'impact est sûrement important : ils changent d'activité ou se professionnalisent. Pour les entreprises ayant peu de moyens techniques (2), la mise à l'index constitue un rappel à l'ordre. Elles sont également confrontées aux mises à l'index abusives et aux faux positifs. Les entreprises avec une forte maîtrise technique (3) sont surtout confrontées au blacklistage abusif, et dans une moindre mesure, aux erreurs de configuration occasionnelles. Notre étude ne permet pas d'estimer quel est l'impact exact pour les grands spammeurs (4), c'est une question qui reste en suspens.

Qu'appelle-t-on blacklisting « dynamique » ? Cette approche intéressante consiste à créer des entrées très dynamiques, de façon automatisée, sur des critères tels que le taux de virus, le taux de spams (détecté par exemple sur un échantillon par un filtre Bayésien), le taux d'erreurs d'adressage ou des changements atypiques des volumes émis. Le prestataire de service Postini[41] fait figure de précurseur en ce domaine.

La sortie de la liste est rapide et également automatique. Certains systèmes avancés intègrent une mémorisation et sont capables d'adopter un comportement de plus en plus sévère. C'est notamment le cas de l'outil j-chkmail[42], développé par José Marcio Martins Da Cruz, chercheur à l'Ecole des Mines. Par définition, cette technique est applicable dans le cas de listes noires locales (ou gérées en interne par les FAI).

José Marcio Martins Da Cruz est Ingénieur chercheur au centre de calcul de l'école des mines de Paris (ENSMP). Il a développé un filtre antispam (j-chkmail) qui s'interface avec Sendmail et qui est utilisé par son école.

Halte au Spam : « Que se passerait-il sur Internet si les blacklists disparaissaient demain ? »

José Marcio Martins Da Cruz : « Chaque jour, notre infrastructure bloque environ 14.000 messages sur le critère des listes. Ces rejets ne sont pas comptabilisés par j-chkmail, puisque Sendmail rejette ces connexions avant même d'appeler le filtre. Sans blacklists, les serveurs de mail seraient plus chargés. Pour un filtre tel que j-chkmail, ça n'aurait probablement pas trop de répercussion, puisque le nombre de rejets par blacklist est comparable au nombre de rejets par le filtre, et la charge de j-chkmail sur le serveur est modeste. Pour des filtres plus gourmands en ressources, tels SpamAssassin, ça serait plus compliqué… si je ne me trompe pas, les critères les plus efficaces de SpamAssassin, sont justement ceux qui font appel à des blacklists. »

Mais peut-on les compléter par un autre type de filtre ? C'est généralement le cas. Rien ne s'oppose à qu'une autre technique de filtrage et d'analyse (comme une authentification SPF ou Sender ID) ne soit appliquée au préalable, comme le représente la figure 7. Les messages non filtrés par les listes noires peuvent être traités par d'autres mécanismes. L'objectif est de décharger ces filtres en aval.

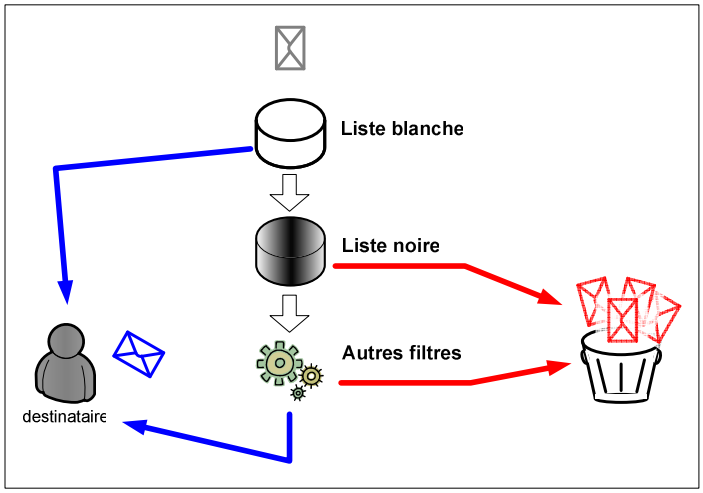

Fig. 7 - Utilisation combinée de plusieurs techniques de filtrage anti-spam (avec utilisation des listes noires en « tout ou rien »). Une autre combinaison voit l'information délivrée par les listes noires utilisée en tant que l'un des critères pondérés (au sein d'un filtre utilisant plusieurs techniques).

Je souhaite utiliser une liste noire publique. Vaut-il mieux en utiliser une seule ou plusieurs ? Chaque liste noire se caractérise par son efficacité (taux de filtrage), son taux de faux-positifs (blocage indu de messages légitimes) et sa « spécialité ». Utiliser plusieurs listes noires, c'est risquer d'additionner les effets pervers (c.a.d. les faux positifs) pour une protection légèrement meilleure. Plutôt que de s'abonner à

l'aveuglette à une multitude de listes sous le prétexte qu'elles sont gratuites, il vaut mieux sélectionner un service performant.

Les dernières trouvailles des spammeurs ne sonnent-elles pas le glas des blacklists ? Depuis le recours par les spammeurs aux parcs de PC « zombies » et à des techniques d'émission extrêmement diffuses (chaque PC, ou relais n'expédie que quelques messages, mais ils sont plusieurs milliers à le faire), le filtrage sur liste noire a perdu en efficacité.

En réponse, certains bloquent systématiquement les adresses IP dynamiques ou résidentielles, considérant anormale l'exploitation d'un serveur de messagerie par un « particulier ».

Gabriel Gross est fondateur et président de la société Dolphian, société française éditrice de logiciels de filtrage dynamique de flux Internet créée en 2001.

Halte au Spam : « Peut-on se protéger du spam sans avoir recours aux listes noires ? »

Gabriel Gross : « Nous avons fait le choix très rapidement de nous passer entièrement des listes noires publiques, et ce pour deux raisons simples : un manque de stabilité et une qualité insuffisante du contenu. Plusieurs serveurs de listes noires ont connu des périodes d'indisponibilité ou de maintenance. Etant hébergées dans des conditions généralement assez sommaires, elles présentent pour notre niveau d'exigence une trop grande vulnérabilité. De plus, nous avons trouvé dans ces listes noires les adresses IP ou les noms de domaines d'entreprises françaises ou européennes bien connues. Les personnes qui contribuent à ces listes sont généralement assez loin des préoccupations d'affaires des entreprises européennes, soit pour des raisons de « philosophie de l'Internet » soit pour des raisons linguistiques, tout simplement. La qualité de filtrage de nos produits prouve qu'il est possible de se passer totalement des listes noires dans le filtrage. Cependant, il n'est pas exclus que pour certains types d'applications, et notamment pour un produit de protection des infrastructures que nous avons en cours de développement, nous fassions appel à une liste qui serait agrégée, hébergée et maintenue en interne. »

Les listes noires peuvent-elles mourir ? Oui. Sous la menace ou sous la charge d'exploitation, certains gérants de listes mettent la clef sous la porte, sans prévenir la plupart du temps. Le problème, c'est que même « mortes », certaines d'entre elles sont encore accessibles et encore interrogées. Si vous avez le malheur de figurer dans celle-ci, vous n'avez aucun moyen de sortir de ces listes… A titre d'exemple, la liste ORBS a cessé d'opérer depuis mars 2002. Lors de notre campagne de mesures, nous avons été témoins de la mort de l'une des listes de notre panel.

Le blacklisting vise à contrôler les emails entrants. Quelles précautions sont prises au niveau des FAI pour contrôler le sens sortant ? Peu d'efforts ont été jusque là consentis sur ce sujet, ce qui abouti à des situations dans lesquelles les FAI se blacklistent mutuellement.

Dans les cas extrêmes, des domaines entiers sont coupés au niveau de certains FAI, ce qui est l'exact opposé du concept même d'Internet.

De façon assez surprenante, l'intervention[43] d'un responsable d'AOL lors de la récente conférence NANOG est passée inaperçue. Il annonçait pourtant clairement que cet ISP n'hésiterait pas à blacklister ses confrères, si ceux-ci ne prenaient pas rapidement de sérieuses mesures – au delà de la simple interdiction en sortie du port 25 depuis des postes abonnés – telles qu'une limitation des rythmes d'émission, et l'implémentation de filtrage anti-spam en sortie et de dispositifs d'authentification SMTP.

Selon une étude publiée en octobre 2004 par la société CyberTrust concernant le *phishing**, les PC français sont régulièrement utilisés comme base d'émission... Et même devant la Chine selon l'un des critères (en nombre de messages) : USA 32%, Corée du Sud 15%, France 6,5%.

D'après nos sources, quelques FAI commencent à s'y attaquer, pour empêcher que les spammeurs ne tirent profit des centaines de milliers de nouveaux PC connectés en ADSL.

Concernant le manque de coopération entre prestataires techniques, nous signalons le témoignage récent de Steve Linford, animateur de Spamhaus, qui a évoqué publiquement les difficultés qu'il éprouve à se faire comprendre des ISP chinois[44], au point qu'il a décidé d'ouvrir un bureau en Chine.

Avec la montée en puissance des dispositifs d'authentification, n'assiste-t-on pas finalement à un recours accru aux *whitelists*, au détriment des *blacklists* ? C'est l'avis d'Yves Roumazeilles, animateur de SpamAnti, selon lequel « un mouvement se confirme en faveur d'une logique selon laquelle nous n'accepterions un courriel que des émetteurs qui nous sont connus, au lieu de refuser ceux de certaines sources ».

Les démarches d'authentification (SPF, Sender ID, Domain Keys) confortent ce mouvement, bien que le fait qu'un message émane d'une émetteur authentifié ne dit rien de son honnêteté. L'émergence des listes « sur réputation », comme *Bonded Sender*[45] et *Sender Base*[46], répondent à ce besoin. Mais de nouvelles questions se font jour, notamment sur la gestion de ces nouvelles listes. On nous a reporté que la société Hotmail exigeait désormais de la part de ses pairs une souscription à ce service, pour voir leurs emails acceptés.

Steve Linford est le créateur et l'animateur de l'une des organisations qui luttent contre le Spam, Spamhaus. Dans une vie antérieure, il a participé à l'organisation de tournées des Pink Floyd et de Michael Jackson. Basé en Angleterre et créée en 1998, Spamhaus anime plusieurs listes noires (dont l'une fait partie de notre campagne de mesures) ainsi que la base de connaissance ROKSO. En octobre 2004, la Commission Européenne a annoncé s'être attaché les services de Steve Linford, en tant que conseiller sur le sujet Spam.

Halte au Spam : Pouvez vous nous indiquer combien d'entités utilisent vos listes ?

Steve Linford : Actuellement 260 millions de boîtes aux lettres sont protégées par nos blocklists SBL et XBL. Nos principaux utilisateurs sont les FAI (environ 420, parmi les plus grands, tels que Google Gmail, Mail.com ou Juno.com), les grandes entreprises (compagnies aériennes, banques…), les universités, les milieux gouvernementaux (dont le gouvernement britannique) et le secteur de la défense (avec, entre autres, l'US Navy et l'US Army).

Halte au Spam : On attribue souvent un taux de faux positif élevé au filtrage sur liste noire. Le confirmez vous ?

Steve Linford : Qui le dit ? Les éditeurs d'outils anti-spam qui sont en concurrence directe avec les blocklists ? Le fait est que si vous utilisez l'une de ces listes noires agressives administrées par quelques adolescents comme un passe-temps, vous risquez fort de bloquer des messages utiles. Et il y en a tant, de ces petites listes, gérées comme un loisir ! Mais qui les utilise ? Aucun FAI en tout cas. Si l'un d'entre eux s'y amusait, il se ferait « éjecter » de son marché en quelques semaines.

Nos listes SBL et XBL filtrent 8 milliards de spam chaque jour. Notre taux extrêmement faible de faux-positifs fait qu'il est rare qu'un émetteur innocent se retrouve listé chez nous, alors que nous bloquons chaque jour autant de spams que tous les filtres réunis. La plupart des éditeurs de filtres commerciaux se rengorgent du taux de faux positifs de « seulement » 0,5%, voire moins. Si nous avions un tel taux, nous bloquerions quotidiennement des centaines de milliers de messages utiles, ce qui ne manquerait pas de provoquer une levée de boucliers !

**Le* phishing *est une technique frauduleuse, qui vise à obtenir de la part de l'internaute des informations confidentielles (codes, numéro de cartes bancaires, etc.) en se faisant passer par une entité de confiance (généralement sa banque). L'e-mail est très souvent utilisé à ces fins.*

Halte au Spam : Il nous paraît important de différencier les listes qui indexent les serveurs en relais ouverts. Pouvez-vous nous indiquer le nombre d'entrées qui correspondent à ce critère ?

Steve Linford : Cela m'est impossible, mais le chiffre est très élevé. Notre liste XBL (Exploits Blocklist) référencie seulement les machines compromises et exploitées par les spammeurs, comme les machines infectées par des chevaux de Troie et qui diffusent des pourriels à l'insu de leurs propriétaires. Cette catégorie représente plus de 4 millions d'entrées actuellement, dont une forte majorité de PC sur des accès ADSL.

Halte au Spam : Combien d'entre elles sont finalement retirées, une fois le problème résolu ?

Steve Linford : La sortie de la liste XBL est opérée automatiquement, dès que le propriétaire du PC en question a sécurisé son poste et nous a adressé une simple demande de sortie de liste (via notre site Web).

Halte au Spam : Combien d'entre eux correspondent à des faux-positifs ?

Steve Linford : Ce concept est difficile à définir et un faux-positif avéré nous est quasiment inconnu. Chaque adresse IP est listée pour une raison claire, indiquée dans la blocklist. Nous pouvons imaginer une situation dans laquelle le spammeur émet un million de spams proposant du Viagra, ce qui provoque la mise à l'index de l'adresse correspondante. Quand la mère du spammeur veut utiliser le même poste pour émettre des messages utiles, ceux-ci seront bloqués. Pour les destinataires de ces messages innocents, il s'agit de faux-positifs. Pour nous, ça n'en est pas vraiment, car nous avons la preuve que la machine est utilisée pour diffuser des pourriels en masse.

Halte au Spam : Les personnes qui ne se plaignent auprès de vous qu'une seule fois ne sont-elles pas en fait des spammeurs qui tentent de bluffer pour sortir des listes ?

Steve Linford : Nous notons rarement ce type de comportement. Pour notre liste SBL (Spamhaus Block List), nous recevons quotidiennement environ 100 à 150 demandes de sortie, qui proviennent en majorité de FAI qui nous annoncent qu'ils sont intervenus plus haut dans leur infrastructure et ont mis fin aux émissions. Nous avons également des réactions de la part d'émetteurs, qui mettent en avant leur respect de la loi CAN-SPAM… mais tous les spammeurs assurent ne pas faire de spamming. A l'exposé des preuves en notre possession, ils nous jurent que la totalité des 10 millions d'adresses qu'ils visent sont en opt-in.

Halte au Spam : Avez vous mis en place un dispositif spécifique pour gérer ce type de demande ?

Steve Linford : Oui, notre interface est disponible 24 heures sur 24, 7 jours sur 7. Tout émetteur bloqué indûment est retiré dans l'heure qui suit.

Halte au Spam : Traitez vous d'une façon prioritaire les entreprises connues ?

Steve Linford : Ce type d'entreprises n'apparaît jamais sur nos listes. C'est un mythe que d'affirmer que nous bloquons des entités par erreur. En fait, c'est extrêmement rare. Nous n'avons pas d'exemple de sociétés réelles bloquées à tort.

Halte au Spam : Dans certains cas – nous pensons notamment aux « relais ouverts » – les listes noires ne sont elles pas une façon d'éduquer les exploitants de messagerie, et de les forcer à plus de professionnalisme ?

Steve Linford : Pas pour nous (de toute façon, nous n'exploitons pas de liste d'open relais). Nous ne listons que des émetteurs de spams. Ces deux dernières années, les spammeurs ont réussi à infecter chaque semaine plus de 100.000 nouveaux postes. Personne n'a suffisamment de ressources pour contacter les propriétaires de ces PC. Nous vivons une situation dans laquelle nous pouvons seulement protéger nos utilisateurs de ces parcs de PC zombies.

Halte au Spam : La plupart des FAI français sont régulièrement listés. Comment l'expliquez vous ? Quelles relations entretenez vous avec cette catégorie d'acteurs ?

Steve Linford : Nous ne bloquons pas – et n'avons jamais bloqué – de FAI français. Les listes concernées appartiennent sans doute à la catégorie « adolescents en mal de passe-temps », qu'aucun prestataire technique sérieux ne voudrait utiliser. Il existe par exemple une « wanadoo-fr.blackholes.us »*, mais personne ne l'utilise.

Halte au Spam : Etes vous gênés par l'image que donnent les listes trop agressives ?

Steve Linford : Oui. Souvent, les journalistes ne font pas de différence entre nous et ces listes irresponsables et agressives. Or il existe des centaines de blacklists, la plupart administrées de façon anonyme, une majorité ne comptant qu'une poignée d'utilisateurs.

Halte au Spam : Dans notre campagne de mesures, nous avons relevé qu'une grande entreprise française, leader mondial de sa spécialité, est mise à l'index depuis plusieurs mois par rfc-ignorant.org pour un WHOIS « visiblement faux, inexact ou incomplet »…

Steve Linford : Notre domaine Spamhaus.org est lui-même indexé dans cette liste, comme pratiquement tous les domaines en .uk. Mais aucun FAI n'utilise cette liste et je ne connais aucune personne sensée qui y a recours.

Halte au Spam : Le mode de fonctionnement de la plupart des listes est pour le moins obscur. Même si l'on peut comprendre qu'une certaine discrétion vis-à-vis des spammeurs est nécessaire, ne la trouvez vous pas excessive ?

Steve Linford : C'est un fait que la grande majorité des blacklists est gérée par des personnes isolées, comme un hobby, et qu'ils sont totalement hors contrôle. Chacun peut, en quelques minutes, créer sa propre liste selon les critères de son choix, et bloquer le monde entier s'il le désire. Bien fou serait le FAI qui retiendrait cette liste.

Halte au Spam : N'est-il pas temps que les pouvoirs publics ou des institutions telles que les NIC ou les Organisations de protection des données personnelles se chargent de ces missions ?

Steve Linford : Ils n'en ont pas la capacité. D'ailleurs rien ne les empêche de le faire dès aujourd'hui…mais ils ne le font pas car ils ne disposent ni des compétences, ni de l'expérience concernant le monde des spammeurs et leur façon d'opérer. A titre d'exemple, l'Internet Socitey of China a créé une liste noire, présentée comme un moyen efficace d'éradiquer le spam, avec le soutien du gouvernement. Elle est mise à jour quatre fois dans l'année, comporte quelques centaines d'adresses, ne filtre aucun pourriel et indexe des serveurs taïwanais pour des raisons de politique internationale… Personne ne l'utilise.

Halte au Spam : Que pensez vous par contre d'un « label » qui pourrait concerner le mode de fonctionnement et les procédures mises en œuvre par les listes ?

Steve Linford : Il serait la marque forte d'une reconnaissance de la part des autorités, mais certains y verraient une tentative de contrôle des ressources d'Internet par les gouvernements.

Halte au Spam : Les blacklists sont elles efficaces ? Plus précisément, ont-elles une efficacité supérieure sur certaines catégories de spammeurs ? Les plus « professionnels » d'entre eux sont-ils réellement gênés par elles ?

Steve Linford : Je ne peux répondre que pour nos listes SBL et XBL. Les serveurs de messagerie qui les utilisent bloquent 75 à 85% des spams durant la phase SMTP (sans acceptation du message). Une analy-

**Voir www.blackholes.us.*

se à la recherche d'URL embarquées rejette environ 80 à 90% des pourriels qui ont réussi à passer la première étape. Donc, en utilisant uniquement le couple SBL – XBL, c'est 95% du spam qui est rejeté.

Halte au Spam : Que peut-il être répondu aux tenants des nouvelles techniques antispam, selon lesquels les listes noires ont un futur incertain ?

Steve Linford : Que dire ? A part que cette position est celle d'éditeurs qui y ont un intérêt commercial ? Nous ne voyons aucune de ces techniques atteindre notre niveau d'efficacité, avec un taux de faux-positifs inférieur. La plupart d'entre elles détruisent les messages –une pratique à laquelle nous sommes opposés-, au lieu de les rejeter. Au contraire, un émetteur dont le message est refusé par nos listes en est immédiatement informé. Nous indiquons la raison et la démarche à suivre pour nous contacter. Les filtres antispam – y compris ceux utilisant les « nouvelles techniques » de filtrage- détruisent le plus souvent ces messages sans que ni l'émetteur ni le destinataire en soient informés.

Pour clore cette étude, nous vous proposons tout d'abord quelques points de réflexion, puis une série de conseils selon que vous souhaitiez vous protéger avec une liste noire ou que vous soyez vous même blacklisté.

Axes de réflexion :

- Ne serait-il pas temps de faire un tri dans les blacklists, de ne conserver que celles dont la pertinence est reconnue, et dont les critères sont indiscutables ?
- Est-il envisageable de confier leur gestion à des organismes contrôlés par les pouvoirs publics ou bien de faire auditer leurs méthodes par des organismes publics ad hoc (cf. notre proposition[47], même si nous la considérons nous-même comme utopique) ? Cette dernière approche permettrait de garder une certaine discrétion vis-à-vis des spammeurs, d'encourager les gestionnaires de listes à l'excellence, d'encourager la coopération entre les gestionnaires de liste et de fournir aux internautes et utilisateurs de listes un élément de choix.
- Pour celles qui sont basées sous une forme ou une autre de « délation », il serait sain de n'accepter que les « contributions » d'internautes acceptant d'agir à visage découvert, et non sous couvert d'anonymat.
- Pourrait-on inciter les gérants de listes à améliorer leurs procédures, et notamment celles qui informent les entités qui viennent d'être mises à l'index ?
- Ne faudrait-il pas aider les exploitants de messagerie à monter en compétences ? En parallèle de la sophistication accrue des techniques utilisées par les spammeurs, la tâche des exploitants de messagerie est de plus en plus complexe. Comme nous l'a indiqué monsieur Bortzmeyer, « Force est de constater que le niveau de compétences demandé aux administrateurs de messagerie est en train de s'élever. Il ne suffira bientôt plus de veiller aux respects des standards, mais également de respecter les habitudes de chacun si l'on veut que ses messages soient correctement véhiculés et délivrés ! ».

Vous souhaitez vous protéger avec des listes noires. Quels conseils suivre ?

- Compte tenu des effets de bord de cette technique, astreignez vous à en comprendre au préalable le mécanisme – et les éventuels impacts – avant de la mettre en œuvre,
- evaluez l'apport (relatif) de ce type de filtrage par rapport aux autres méthodes qui seront sans doute utilisées dans votre dispositif global anti-spam,
- mettez en place des indicateurs, notamment pour pallier (rapidement et facilement) à d'éventuels faux positifs,
- choisissez avec soin votre catégorie de blacklist (c'est à dire ses objectifs et les critères qui président à l'entrée et à la sortie), et votre blacklist, au sein de cette catégorie,
- donnez la priorité aux listes dédiées aux proxys ouverts (à ne pas confondre avec les relais SMTP ouverts), pour limiter les faux positifs* ; Par conception, aucun proxy ne devrait émettre des courriers électroniques,
- réfléchissez à l'usage que vous allez faire de l'information délivrée par la liste. Au début, n'utilisez cette indication que comme un critère pondéré, et non pas pour prendre une décision sans appel,
- posez vous la question du nombre de blacklists à utiliser,
- pour ne pas ralentir le traitement de vos emails, veillez à optimiser vos flux DNS (par exemple en ayant recours à des solutions de caching),
- soyez capable de surveiller des critères pertinents (pour pouvoir prendre les bonnes décisions ; dévalider la blacklist, en changer…), comme le taux de faux positif comparé au taux de capture,
- suivez la vie (et la mort) des entités qui gèrent les blacklists[48],
- posez vous la question si vous allez informer les émetteurs de votre filtrage (et soyez explicite),
- réfléchissez à la mise sur pied d'une whitelist comprenant vos partenaires, clients, fournisseurs, relations, administrations…

Vous êtes blacklisté. Que faire, et dans quel ordre ?

- prévoyez une adresse IP au cas où…, un nom de domaine au cas où, un repli sur un FAI…,
- créez une adresse postmaster et gérez correctement la boîte aux lettres associée (prévoir plutôt que guérir), pour détecter rapidement les notifications de mise à l'index,
- récoltez les informations précises qui témoignent de votre mise à l'index,
- identifiez la ou les listes sur laquelle vous figurez,
- prenez connaissance de ses caractéristiques (critères d'entrée, politique, processus de sortie),
- vérifiez votre situation vis-à-vis de ces éléments,
- vérifiez la configuration de vos DNS et de vos déclarations WHOIS,
- apportez les éventuels correctifs,
- prenez contact avec la liste, faites vous connaître et fournissez les preuves des correctifs,
- mettre en place un processus de test pour s'assurer de la sortie effective de la liste,
- si la sortie de la liste s'annonce longue, évaluez l'impact et d'éventuels solutions de repli (information des collaborateurs par exemple).

Sources et références :

[1] www.mail-abuse.com
[2] www.SpamAnti.net
[3] Pour les « SMTP Return Codes » se reporter à la page www.ietf.org/rfc/rfc2505.txt
[4] Dans cette étude, nous ne faisons référence qu'aux professionnels respectueux des droits des internautes et des différentes lois et codes de déontologie en vigueur.
[5] « Email blocking and filtering report », mars 2004 Return Path, www.returnpath.biz
[6] www.Spamcop.net
[7] www.mail-abuse.com (Mail Abuse Prevention System)
[8] http://spews.org (pour Spam Prevention Early Warning System)
[9] www.ordb.org
[10] Source Return Path, juillet 2004, étude menée sur 168 entreprises américaines.

**Avec cette catégorie de listes, un blocage de la connexion peut être mis en place, avec peu de risques de perdre des messages utiles.*

[11] « Spam Monitor Survey Volume II », Clearswift, p.17 www.clearswift.com
[12] http://j-chkmail.ensmp.fr
[13] www.surbl.org
[14] AOL et Hotmail déclarent détruire ainsi quotidiennement plusieurs milliards de pourriels, dont une partie est détectée par blacklist. A ce propos, on peut se demander sur quelle base est fait ce comptage… En effet, après avoir coupé la connexion avec un émetteur, il est difficile de comptabiliser les messages que celui-ci s'apprêtait à diffuser.
[15] www.dnsbl.org
[16] http://dsbl.org/main
[17] www.maarivintl.com/index.cfm?fuseaction=article&articleID=8904
[18] www.rfc-ignorant.org
[19] L'AFNIC est le centre d'information et de gestion des noms de domaine Internet pour la France www.afnic.fr
[20] Cette modalité de filtrage consiste à lancer une résolution DNS inverse de l'adresse IP émettrice, à vérifier qu'elle correspond au domaine annoncé par l'émetteur, à vérifier la présence d'une entrée dans le DNS et celle de l'existence du domaine annoncé dans l'enveloppe. Le relais récepteur vérifie auprès de son serveur DNS à qui correspond l'adresse. En l'absence de réponse, on conclut qu'il s'agit probablement d'un spammeur.
[21] Whois www.whois.net
[22] www.rfc-ignorant.org/policy-postmaster.php
[23] Pour déterminer si un relais est ouvert, se référer aux pages 136 à 140 du livre « Halte au Spam ». Pour fermer un relais ouvert, se reporter aux pages 140 à 152.
[24] http://postmaster.info.aol.fr/professionnels/infos/relais.html
[25] www.wired.com/news/culture/0,1284,44876,00.html
[26] www.tmcnet.com/tmcnet/articles/2004/100104jt2.htm
[27] www.declude.com/Articles.asp?ID=97&Redirected=Y ou encore www.moensted.dk/spam/
[28] « Spam Monitor Survey Volume II », Clearswift, p.17 www.clearswift.com
[29] « Avoid the Spam Filter Trap », Assurance Systems, octobre 2002
[30] « *An anti-spam service has been shut down after a series of attacks* », par Patrick Gray, ZDNet Australia, août 2003 http://news.zdnet.co.uk/internet/security/0,39020375,39115930,00.htm
[31] www.tsr.ch/tsr/index.html?siteSect=311201&sid=5021872
[32] www.Spamhaus.org/rokso/index.lasso
[33] http://dynamic.rfc1149.net/wsff.phtml.fr
[34] www.spamanti.net/fr/domains.php
[35] www.aricia.fr
[36] www.silicon.com/research/specialreports/thespamreport/0,39025001,10004537,00.htm
[37] «Anti-Spam Coordination Team (ASCT) of Internet Society of China (ISC) declare the 3rd Edition of Mail Servers Sending Spam List» http://www.isc.org.cn/20020417/ca226065.htm
[38] « BT blocked by spam blacklist", par Will Sturgeon, Silicon.com, 6 juin 2003 www.silicon.com/research/specialreports/thespamreport/0,39025001,10004537,00.htm
[39] Filters vs. Blacklists www.paulgraham.com/falsepositives.html
[40] « An anti-spam service has been shut down after a series of attacks », par Patrick Gray, ZDNet Australia, août 2003 http://news.zdnet.co.uk/internet/security/0,39020375,39115930,00.htm
[41] www.postini.com
[42] http://j-chkmail.ensmp.fr
[43] www.circleid.com/article/794_0_1_0_C/
[44] www.guardian.co.uk/online/news/0,12597,1237103,00.html
[45] www.bondedsender.com
[46] www.senderbase.org
[47] « Halte au Spam » éditions Eyrolles, page 261
[48] Une liste des DNSBL mortes peut être consultée à http://spamlinks.openrbl.org/filter-dnsbl-dead.htm

Nous vous invitons à prendre connaissance de la première partie de cette étude. Elle présente les enseignements d'une campagne de mesures que nous avons effectuée sur un panel de grandes entreprises et administrations françaises. www.halte-au-spam.com/Blacklists_Resultats.pdf

Autres études disponibles sur www.halte-au-spam.com :

- *Analyse de l'article 22 de la loi LCEN*
- *Les logiciels « sociaux » sont-ils une menace ?*
- *Quels conseils peut-on donner aux professionnels du Marketing Direct, dans le cadre de la loi « pour la confiance dans l'économie numérique » ?*
- *Faut-il craindre les effets pervers des parades anti-spam ?*

Mais aussi les compte-rendu des conférences suivantes :

- *« Listes noires, listes blanches : efficacité et utilisation » (Paris, novembre 2004)*
- *« Techniques anti-spam : l'apport du monde du logiciel libre » (Paris, octobre 2004)*
- *« 2nd OECD Workshop on Spam » (Busan, septembre 2004)*
- *« Spam : Se plaindre... ou porter plainte ? » (Paris, septembre 2004)*
- *« Thematic Meeting on Countering Spam » (Genève, juillet 2004)*
- *« L'authentification des mèls : une solution au problème du spam ? » (Paris, juin 2004)*
- *« Spam Conference MIT » (Cambridge, décembre 2003)*
- *« Spam. The death of the e-mail ? » (Dublin, décembre 2003)*
- *« Spam Forum Paris » (Paris, novembre 2003)*
- *« Atelier Spam OCDE » (Bruxelles, octobre 2003)*

Les auteurs de cette étude sont consultants indépendants, spécialisés dans l'optimisation de l'usage d'Internet en entreprise : surf abusif, spam, cyberdépendance, création de charte d'utilisation, utilisation productive des messageries instantanées…. Forts d'une riche expérience de terrain, leur approche est globale et mêle aspects humains, légaux et techniques. Coauteurs de l'ouvrage de référence « Halte au Spam » (Eyrolles) et co-organisateurs de la première conférence française sur la problématique Spam (Spam Forum Paris), ils sont membres qualifiés du Groupe de contact « Spam » mis en place par le gouvernement français.

Son expérience autour des protocoles et leur impact sur les applications et la productivité a conduit Frédéric Aoun (Ingénieur réseaux diplômé de l'INT) à considérer globalement les outils techniques et leur utilisation. Son parcours en Amérique du Sud et aux Etats-Unis lui permet de voir d'un œil averti les différences et les particularités du marché français.

Précurseur dès 1985 de la compression de données, Bruno Rasle est à l'origine de l'introduction en France des premières solutions de qualité de service, aujourd'hui banalisées : équilibrage de charge, mesures de disponibilité et de performances de sites Web, accélération http, gestion des priorités… Il est à l'origine du « Nettoyage de Printemps des DNS », visant à améliorer le domaine .fr